



Junos Pulse Secure Access Service

Administration Guide

Release

7.4



Published: 2013-02-27
Part Number: , Revision 1

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986–1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Junos Pulse Secure Access Service Administration Guide

Revision History
June 2012—Beta

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Abbreviated Table of Contents

	About This Guide	xxxvii
Part 1	Getting Started	
Chapter 1	Initial Verification and Key Concepts	3
Chapter 2	Introduction to Secure Access Service	15
Part 2	Access Management Framework	
Chapter 3	General Access Management	71
Chapter 4	User Roles	105
Chapter 5	Resource Profiles	127
Chapter 6	Virtual Desktop Resource Profiles	137
Chapter 7	Resource Policies	143
Chapter 8	Authentication and Directory Servers	153
Chapter 9	SAML Single Sign-on	233
Chapter 10	Authentication Realms	305
Chapter 11	Sign-In Policies	321
Chapter 12	Single Sign-On	335
Chapter 13	Synchronizing User Records	363
Part 3	Endpoint Defense	
Chapter 14	Host Checker	373
Chapter 15	Cache Cleaner	445
Part 4	Remote Access	
Chapter 16	Hosted Java Applets Templates	453
Chapter 17	Citrix Templates	467
Chapter 18	Lotus iNotes Templates	477
Chapter 19	Microsoft OWA Templates	481
Chapter 20	Microsoft Sharepoint Templates	485
Chapter 21	Web Rewriting	489
Chapter 22	File Rewriting	561
Chapter 23	Secure Application Manager	583
Chapter 24	Telnet/SSH	631

Chapter 25	Terminal Services	641
Chapter 26	Junos Pulse Collaboration	691
Chapter 27	Email Client	725
Chapter 28	VPN Tunneling	733
Part 5	System Management	
Chapter 29	General System Management	789
Chapter 30	Certificates	837
Chapter 31	Elliptic Curve Cryptography	875
Chapter 32	System Archiving	889
Chapter 33	Logging and Monitoring	931
Chapter 34	Troubleshooting	959
Chapter 35	Clustering	977
Chapter 36	Delegating Administrator Roles	1005
Chapter 37	Instant Virtual System	1011
Chapter 38	IPv6 Support	1065
Chapter 39	Secure Access Service and IDP Interoperability	1081
Chapter 40	Routing AAA Over the Management Port for Virtual Appliances	1091
Part 6	System Services	
Chapter 41	Secure Access Service Serial Console	1097
Chapter 42	Customizable Admin and End-User UIs	1103
Chapter 43	SA6000 Series Appliance	1105
Chapter 44	SA4500 and SA6500 Series Appliances	1109
Chapter 45	Secure Access FIPS	1119
Chapter 46	SA4500 and SA6500 FIPS Appliances	1131
Chapter 47	FIPS Level 1 Support	1141
Chapter 48	Compression	1157
Chapter 49	Multi-Language Support	1161
Chapter 50	Handheld Devices and PDAs	1165
Chapter 51	Using IKEv2 with the Secure Access Service	1173
Chapter 52	Writing Custom Expressions	1181
Part 7	Index	
	Index	1207

Table of Contents

	About This Guide	xxxvii
	Objective	xxxvii
	Audience	xxxvii
	Document Conventions	xxxvii
	Documentation	xxxviii
	Obtaining Documentation	xxxviii
	Documentation Feedback	xxxviii
	Requesting Technical Support	xxxviii
	Self-Help Online Tools and Resources	xxxix
	Opening a Case with JTAC	xxxix
Part 1	Getting Started	
Chapter 1	Initial Verification and Key Concepts	3
	Verifying User Accessibility	3
	Creating a Test Scenario to Learn Secure Access Service Concepts and Best Practices	4
	Defining a User Role	5
	Defining a Resource Profile	6
	Defining an Authentication Server	7
	Defining an Authentication Realm	9
	Defining a Sign-In Policy	10
	Using the Test Scenario	12
	Default Settings for Administrators	13
Chapter 2	Introduction to Secure Access Service	15
	Secure Access Service Solution Overview	16
	Securing Traffic with Secure Access Service	18
	Authenticating Users with Existing Servers	19
	Fine-Tuning Access to Secure Access Service and the Resources It Intermediates	20
	Creating a Seamless Integration Between Secure Access Service and the Resources It Intermediates	21
	Protecting Against Infected Computers and Other Security Concerns	21
	Ensuring Redundancy in the Secure Access Service Environment	22
	Making the Secure Access Service Interface Match My Company's Look-and-Feel	23
	Enabling Users on a Variety of Computers and Devices to Use Secure Access Service	23
	Providing Secure Access for My International Users	24
	Configuring Secure Access Service	24

Network and Security Manager and the Secure Access Service	25
How Secure Access Service and NSM communicate	25
Available Services and Configuration Options	27
DMI Communication with the Secure Access Service	27
Configuring Secure Access for the Initial DMI Connection	28
Managing Large Binary Data Files	30
Uploading and Linking Large Binary Data Files with NSM	30
Importing Custom Sign-In Pages with NSM	31
Importing Antivirus LiveUpdate Settings with NSM	32
Importing Endpoint Security Assessment Plug-in (ESAP) Packages with NSM	33
Uploading a Third-Party Host Checker Policy with NSM	34
Linking to a Third-Party Host Checker Policy Shared Object with NSM	35
Linking to a Secure Virtual Workspace Wallpaper Image Shared Object with NSM	35
Importing Hosted Java Applets with NSM	36
Importing a Custom Citrix Client .cab File with NSM	37
Junos Pulse Overview	37
Session Migration	38
Location Awareness	38
Security Certificates on Junos Pulse	38
User Experience	39
Secure Access Service Gateway Deployment Options	39
Platform Support	40
Junos Pulse Configuration Overview	40
Configuring a Role for Junos Pulse	41
Pulse Connection Set Options for Pulse Secure Access Service	44
Junos Pulse Connection Options	46
Connection is Established Settings	48
Location Awareness Rules	49
Machine Connection Preferences	50
User Connection Preferences	50
Pre-login Connection Preferences	50
Creating a Client Connection Set	51
Configuring Connection Rules for Location Awareness	53
Junos Pulse Component Set Options	55
Creating a Client Component Set	56
Junos Pulse Client Installation Overview	57
Installing the Junos Pulse Client from the Web	58
Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File	59
Installing the Pulse Client Using Advanced Command-Line Options	60
Examples	62
Repairing a Pulse Installation on a Windows Endpoint	62
Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File	63
Installing the Pulse Client on OS X Endpoints Using Command-Line Options	64
Junos Pulse Command-line Launcher	64

	Using jamCommand to Import Junos Pulse Connections	67
Part 2	Access Management Framework	
Chapter 3	General Access Management	71
	Access Management Overview	71
	Policies, Rules & Restrictions, and Conditions Overview	72
	Accessing Authentication Realms	72
	Accessing User Roles	73
	Accessing Resource Policies	73
	Policies, Rules & Restrictions, and Conditions Evaluation	74
	Dynamic Policy Evaluation	77
	Understanding Dynamic Policy Evaluation	77
	Understanding Standard Policy Evaluation	78
	Enabling Dynamic Policy Evaluation	78
	Specifying Source IP Access Restrictions	79
	About Source IP Restrictions	79
	Specifying Source IP Restrictions at the Realm Level	80
	Specifying Source IP Restrictions at the Role Level	80
	Specifying Source IP Restrictions in Resource Policies	81
	Specifying Browser Access Restrictions	82
	Specifying Certificate Access Restrictions	84
	Specifying Password Access Restrictions	85
	Specifying Session Limits	86
	IF-MAP Federation Overview	89
	IF-MAP Federation Workflow	90
	IF-MAP Federation Details	91
	IF-MAP Logging	94
	Task Summary: Configuring IF-MAP Federation	94
	Configuring IF-MAP Server Settings	94
	Configuring the IF-MAP Federation Client	95
	IF-MAP Federation Network Timing Considerations	95
	Session-Export and Session-Import Policies	96
	Default Session-Export and Session-Import Policy Action	98
	Advanced Session-Export and Session-Import Policies	98
	Configuring Session-Export Policies	98
	Session-Import Policies	100
	Troubleshooting the IF-MAP Federation Network	101
	Viewing Active Users on the IF-MAP Client	101
	Trusted Server List	102
	Administrator and User Configuration	102
	White List Flow Chart	104
Chapter 4	User Roles	105
	User Roles Overview	105
	User Role Evaluation	106
	Permissive Merge Guidelines	108

	Configuration of User Roles	108
	Configuring General Role Options	109
	Role Restrictions	110
	Specifying Role-Based Source IP Aliases	111
	Specifying Role Session Options	111
	Customizing the Secure Access Service Welcome Page	115
	Secure Access Service Optimized Interface for the Apple iPad	120
	Defining Default Options for User Roles	122
	Customizing Messages	123
	Customizing UI Views for User Roles	124
Chapter 5	Resource Profiles	127
	Resource Profiles	127
	Resource Profile Components	128
	Defining Resource Profile Resources	130
	Defining Resource Profile Autopolicies	132
	Defining Resource Profile Roles	133
	Defining Resource Profile Bookmarks	134
	Resource Profile Templates	135
Chapter 6	Virtual Desktop Resource Profiles	137
	Virtual Desktop Resource Profile Overview	137
	Configuring a Citrix XenDesktop Resource Policy	138
	Configuring a VMware View Manager Resource Profile	139
	Defining Bookmarks for a Virtual Desktop Profile	140
	Configuring the Client Delivery	141
	Connecting to the Servers	142
Chapter 7	Resource Policies	143
	Resource Policies	143
	Resource Policy Components	144
	Specifying Resources for a Resource Policy	145
	General Notes About the Canonical Formats	145
	Specifying Server Resources	146
	Resource Policy Evaluation	147
	Creating Detailed Rules for Resource Policies	149
	Writing a Detailed Rule for Resource Policies	150
	Customizing Resource Policy UI Views	152
Chapter 8	Authentication and Directory Servers	153
	About Authentication and Directory Servers	154
	Task Summary: Configuring Authentication Servers	155
	About Anonymous Servers	156
	Anonymous Server Restrictions	157
	Defining an Anonymous Server Instance	157
	Using an RSA ACE/Server	158
	Defining an ACE/Server Instance	159
	Using an RSA ACE/Server with a Secure Access Service Cluster	161
	Using Active Directory or NT Domains	163
	Defining an Active Directory or Windows NT Domain Server Instance	164

Configuring a Role-Mapping Rule Based on the Active Directory LDAP Primary Group	168
Multi-Domain User Authentication	169
Windows 2000 and Windows 2003 Multi-Domain Authentication	169
Windows NT4 Multi-Domain Authentication	169
NT User Normalization	170
Join Domain for Active Directory-based Authentication Server Without Using a Domain Admin Account	170
Using the Kerberos Debugging Tool	172
Active Directory and NT Group Lookup Support	172
Active Directory Lookup Requirements	173
NT4 Group Lookup Requirements	173
Certificate Server	173
Configuring a Certificate Server Instance	174
Using an LDAP Server	175
Defining an LDAP Server Instance	176
Configuring LDAP Search Attributes for Meeting Creators	178
Enabling LDAP Password Management	179
Enabling LDAP Password Management	180
Supported LDAP Directories and Servers	180
Microsoft Active Directory	181
Sun iPlanet	181
General	181
Supported LDAP Password Management Functions	181
AD/NT Password Management Matrix	183
Troubleshooting LDAP Password Management on the Secure Access Service	183
Using a Local Authentication Server	184
Defining a Local Authentication Server Instance	184
Creating User Accounts on a Local Authentication Server	186
Creating User Accounts From the Secure Gateway Home Page	188
Configuring an NIS Server Instance	190
Configuring a RADIUS Server Instance	191
User Experience for RADIUS Users	191
Using CASQUE Authentication	192
Defining a Secure Access Service RADIUS Server Instance	192
Enabling RADIUS Accounting	195
General RADIUS Notes	206
Understanding Clustering Issues	207
Understanding the Interim Update Feature	207
eTrust SiteMinder Overview	207
Authentication Using Various Authentication Schemes	210
Determining the Username	210
Configuring SiteMinder to Work with the Secure Access Service	211
Configuring the SiteMinder Agent	212
Creating a SiteMinder Authentication Scheme for the Secure Access Service	213
Creating a SiteMinder Domain for the Secure Access Service	215
Creating a SiteMinder Realm for the Secure Access Service	215

	Creating a Rule/Response Pair to Pass Usernames to the Secure Access Service	216
	Configuring Secure Access to Work with SiteMinder	217
	Using SiteMinder User Attributes for Secure Access Role Mapping	227
	Defining a SiteMinder Realm for Automatic Sign-In	227
	Debugging SiteMinder and Secure Access Issues	228
	Defining a SAML Server Instance	229
Chapter 9	SAML Single Sign-on	233
	Junos Pulse Secure Access Service SAML 2.0 SSO Solutions	233
	Understanding SAML 2.0	233
	About SAML	233
	SAML Use Cases	234
	Secure Access Service SAML 2.0 Supported Features Reference	234
	Supported SAML SSO Deployment Modes	234
	Supported SAML SSO Profiles	240
	FIPS Support Notes	241
	Secure Access Service SAML 2.0 Configuration Tasks	242
	Configuring System-Wide SAML Settings	243
	Configuring Global SAML Settings	243
	Managing SAML Metadata Files	244
	Configuring Secure Access Service as a SAML 2.0 Service Provider	246
	Configuring Secure Access Service as a SAML 2.0 Identity Provider	250
	Configuration Overview	250
	Configuring Sign-in SAML Metadata Provider Settings	251
	Configuring Sign-in SAML Identity Provider Settings	251
	Configuring Peer SAML Service Provider Settings	255
	Configuring a SAML SSO Resource Policy for Gateway Mode Deployments	260
	Configuring a SAML SSO External Applications Policy	262
	Configuring a SAML 2.0 ACL Web Policy	264
	Example: Implementing SAML 2.0 Web Browser SSO for Google Apps	266
	Topology	266
	Configuring the Google Apps SAML service provider	268
	Configuring the Secure Access Service SAML Identity Provider	270
	Verifying the Google Apps SAML SSO Deployment	274
	Investigating a “No valid assertion found in SAML response” Error	275
	Junos Pulse Secure Access Service SAML 1.1 Support	280
	About SAML Version 1.1	280
	Understanding SAML 1.1	281
	Understanding SAML 1.1 Profiles	283
	Understanding SAML 1.1 Assertions	286
	Creating a Trust Relationship Between SAML 1.1 Systems	288
	Secure Access Service SAML Version 1.1 Configuration Tasks	292
	Creating a SAML 1.1 Server Instance	292
	Configuring SAML 1.1 SSO Profiles	294
	Creating a SAML 1.1 SSO POST Profile	298
	Creating a SAML 1.1 ACL Resource Policy	301

Chapter 10	Authentication Realms	305
	Authentication Realm Overview	305
	Creating an Authentication Realm	306
	Defining Authentication Access Policies	307
	Role Mapping Rules	308
	Specifying Role Mapping Rules for an Authentication Realm	309
	Machine Authentication for Junos Pulse Connections	311
	Junos Pulse Connection Realm and Role Preferences for Machine Authentication	312
	Using the LDAP Server Catalog	314
	Customizing User Realm UI Views	318
Chapter 11	Sign-In Policies	321
	About Sign-In Policies	321
	Task Summary: Configuring Sign In Pages	324
	About Configuring Sign In Policies	324
	Configuring User Sign In Policies	324
	About Sign-In Notifications	327
	Configuring and Implementing Sign-in Notifications	328
	Defining Authorization-Only Access Policies	330
	Defining Meeting Sign-In Policies	331
	Configuring Sign-In Pages	333
	Configuring Standard Sign-In Pages	333
Chapter 12	Single Sign-On	335
	About Single Sign-On	335
	About Multiple Sign-In Credentials	336
	Task Summary: Configuring Multiple Authentication Servers	337
	Task Summary: Enabling SSO to Resources Protected by Basic Authentication	337
	Task Summary: Enabling SSO to Resources Protected by NTLM	338
	Multiple Sign-In Credentials Execution	339
	Understanding SAML 1.1	344
	Configuring SAML 1.1 SSO Profiles	346
	Creating a SAML 1.1 SSO POST Profile	351
	Creating a SAML 1.1 ACL Resource Policy	354
	Creating a Trust Relationship Between SAML 1.1 Systems	357
	Configuring Trusted Application URLs	357
	Configuring an Issuer	358
	Configuring Certificates	358
	Configuring SSO Transactions: Artifact Profile	358
	Configuring SSO Transactions: POST Profile	359
	Configuring Access Control Transactions	360
	Configuring User Identity	361
Chapter 13	Synchronizing User Records	363
	About User Record Synchronization	363
	Enabling User Record Synchronization	365
	Configuring the User Record Synchronization Authentication Server	366
	Configuring the User Record Synchronization Server	367

	Configuring the User Record Synchronization Client	367
	Configuring the User Record Synchronization Database	368
	Scheduling User Record Synchronization Backup	369
Part 3	Endpoint Defense	
Chapter 14	Host Checker	373
	Host Checker and Trusted Network Computing	374
	Task Summary: Configuring Host Checker	376
	Creating Global Host Checker Policies	377
	Enabling Enhanced Endpoint Security Functionality	379
	Enabling Connection Control Host Checker Policies (Windows Only)	381
	Creating and Configuring New Client-side Host Checker Policies	382
	Checking for Third-Party Applications Using Predefined Rules (Windows Only)	383
	Configuring a Predefined Antivirus Rule with Remediation Options	384
	Configuring a Predefined Firewall Rule with Remediation Options (Windows Only)	386
	Configuring a Predefined AntiSpyware Rule (Windows Only)	387
	Configuring Virus Signature Version Monitoring and Patch Assessment Data Monitoring	388
	Patch Management Info Monitoring and Patch Deployment	390
	Additional Functionality with Pulse 2.0	391
	User Experience	392
	Using a System Management Server	392
	Specifying Customized Requirements Using Custom Rules	394
	Using a Wildcard or Environment Variable in a Host Checker Rule	399
	Configuring Patch Assessment Policies	401
	Using a System Management Server	402
	Configuring Patch Assessment Rules	403
	Using Third-party Integrity Measurement Verifiers	405
	Configuring a Remote IMV Server	406
	Implementing the Third-Party IMV Policy	411
	Implementing Host Checker Policies	412
	Executing Host Checker Policies	413
	Configuring Host Checker Restrictions	414
	Remediating Host Checker Policies	416
	General Host Checker Remediation User Experience	417
	Configuring General Host Checker Remediation	418
	Upgrading the Endpoint Security Assessment Plug-In	419
	Defining Host Checker Pre-Authentication Access Tunnels	421
	Specifying Host Checker Pre-Authentication Access Tunnel Definitions	422
	Specifying General Host Checker Options	425
	Specifying Host Checker Installation Options	426
	Client ActiveX Installation Delay	428
	Using Host Checker with the GINA Automatic Sign-In Function	428
	Installing Host Checker Automatically or Manually	429
	Using Host Checker Logs	430

	Configuring Host Checker for Windows Mobile	430
	Requiring Junos Pulse Mobile Security for Secure Access Service Gateway Access	431
	Host Checker for Apple iOS	432
	Host Checker for Pulse iOS Clients	432
	Configuring Host Checker for Pulse iOS Clients	433
	Implementing Host Checker Policies for Pulse for iOS Devices	435
	Using Proxy Exceptions	436
	Enabling the Secure Virtual Workspace	437
	Secure Virtual Workspace Restrictions and Defaults	438
	Configuring the Secure Virtual Workspace	439
	Defining Secure Virtual Workspace Permissions	439
	Defining a Secure Virtual Workspace Application Policy	441
	Defining a Secure Virtual Workspace Security Policy	442
	Defining Secure Virtual Workspace Environment Options	443
	Defining Secure Virtual Workspace Remediation Policy	444
Chapter 15	Cache Cleaner	445
	About Cache Cleaner	445
	Setting Global Cache Cleaner Options	445
	Implementing Cache Cleaner Options	448
	Specifying Cache Cleaner Restrictions	449
	About Cache Cleaner Logs	450
Part 4	Remote Access	
Chapter 16	Hosted Java Applets Templates	453
	About Hosted Java Applet Templates	453
	Task Summary: Hosting Java Applets	454
	Uploading Java Applets to Secure Access	454
	Signing Uploaded Java Applets	455
	Creating HTML Pages That Reference Uploaded Java Applets	456
	Accessing Java Applet Bookmarks	456
	Creating a Hosted Java Applet Resource Profile	457
	Configuring Hosted Java Applet Resource Profile Bookmarks	458
	Creating Hosted Java Applets Bookmarks Through the User Roles Page	460
	Required Attributes for Uploaded Java Applets	461
	Required Parameters for Uploaded Java Applets	462
	Use case: Creating a Citrix JICA 9.5 Java Applet Bookmark	463
Chapter 17	Citrix Templates	467
	About Citrix Templates	467
	Comparing Secure Access Access Mechanisms for Configuring Citrix	468
	Creating Resource Profiles Using Citrix Web Applications	471
Chapter 18	Lotus iNotes Templates	477
	Creating Resource Profiles Using the Lotus iNotes Template	477
Chapter 19	Microsoft OWA Templates	481
	Creating Resource Profiles Using the Microsoft OWA Template	481

Chapter 20	Microsoft Sharepoint Templates	485
	Creating Resource Profiles Using the Microsoft Sharepoint Template	485
Chapter 21	Web Rewriting	489
	Web Rewriting	490
	Silverlight Support	491
	Task Summary: Configuring the Web Rewriting Feature	492
	Remote SSO Overview	494
	Passthrough Proxy Overview	495
	Creating a Custom Web Application Resource Profile	496
	Defining a Web Access Control Autopolicy	499
	Defining a Single Sign-On Autopolicy	500
	Defining a Caching Autopolicy	503
	Defining a Java Access Control Autopolicy	505
	Defining a Rewriting Autopolicy	506
	Defining a Web Compression Autopolicy	510
	Defining Web Resource Profile Bookmarks	511
	Specifying Web Browsing Options	515
	Resource Policy Overview	519
	Writing a Web Access Resource Policy	521
	Defining Single Sign-On Policies	522
	About Basic, NTLM and Kerberos Resources	522
	Writing the Basic, NTLM and Kerberos Resources	523
	Writing a Basic Authentication, NTLM or Kerberos Intermediation Resource Policy	527
	Writing a Remote SSO Form POST Resource Policy	529
	Writing a Remote SSO Headers/Cookies Resource Policy	531
	Writing a Web Caching Resource Policy	533
	About OWA and Lotus Notes Caching Resource Policies	535
	Specifying General Caching Options	536
	Writing a Java Access Control Resource Policy	537
	Writing a Java Code Signing Resource Policy	538
	Creating a Selective Rewriting Resource Policy	540
	Creating a Passthrough Proxy Resource Policy	542
	Creating a Custom Header Resource Policy	544
	Creating an ActiveX Parameter Resource Policy	546
	Restoring the Default Secure Access Service ActiveX Resource Policies	548
	Creating Rewriting Filters	552
	Writing a Web Compression Resource Policy	552
	Defining an OWA Compression Resource Policy	553
	Writing a Web Proxy Resource Policy	554
	Specifying Web Proxy Servers	555
	Writing An HTTP 1.1 Protocol Resource Policy	555
	Creating a Cross Domain Access Policy	557
	Defining Resource Policies: General Options	558
	Managing Resource Policies: Customizing UI Views	559

Chapter 22	File Rewriting	561
	File Rewriting Overview	561
	Creating a File Rewriting Resource Profile	563
	Creating a File Access Control Autopolicy	564
	Creating a File Compression Autopolicy	564
	Creating a Single Sign-On Autopolicy (Windows Only)	565
	Configuring File Resource Profile Bookmarks	566
	Creating Windows File Bookmarks	568
	Creating Advanced Bookmarks to Windows Resources	569
	Creating Windows Bookmarks that Map to LDAP Servers	570
	Defining General Windows File Browsing Options	570
	Writing a File Resource Policy	570
	Windows File Resources Canonical Format	571
	Writing a Windows Access Resource Policy	572
	Writing a Windows SSO Resource Policy	573
	Writing a Windows Compression Resource Policy	574
	Defining General File Writing Options	575
	Creating UNIX File Bookmarks	576
	Creating Advanced Bookmarks to UNIX Resources	576
	Defining General UNIX File Browsing Options	577
	Defining UNIX/NFS File Resource Policies	578
	Canonical Format: UNIX/NFS File Resources	578
	Writing UNIX/NFS Resource Policies	579
	Writing a UNIX/NFS Compression Resource Policy	580
	Defining General UNIX/NFS File Writing Options	581
Chapter 23	Secure Application Manager	583
	Secure Application Manager Overview	584
	Task Summary: Configuring WSAM	584
	Launching VPN Tunneling During a WSAM Session	585
	Debugging WSAM Issues	586
	About WSAM Resource Profiles	586
	Creating WSAM Client Application Resource Profiles	587
	Creating WSAM Destination Network Resource Profiles	588
	Specifying Applications and Servers for WSAM to Secure	589
	Specifying Applications that Need to Bypass WSAM	591
	Specifying Role-Level WSAM Options	593
	Specifying Application Servers that Users Can Access	594
	Specifying Resource Level WSAM Options	596
	Using the WSAM Launcher	596
	JSAM Overview	600
	Task Summary: Configuring JSAM	601
	Using JSAM for Client/Server Communications	602
	Assigning IP Loopback Addresses to Servers	604
	Using Static Loopback Addresses	605
	IP Loopback Address Considerations When Merging Roles	605
	Resolving Host Names to Localhost	606
	Configuring a PC that Connects to the Secure Access Service Through a Proxy Web Server	607

	Determining the Secure Access Service-Assigned Loopback Address	607
	Configuring External DNS Servers and User Machines	608
	JSAM Linux and Macintosh Support	609
	Standard Application Support: MS Outlook	610
	Client/Server Communication Using JSAM	610
	Standard Application Support: Lotus Notes	612
	Client/Server Communication Using JSAM	612
	Configuring the Lotus Notes Client	613
	Standard Application Support: Citrix Web Interface for MetaFrame (NFuse Classic)	614
	Enabling Citrix Published Applications on the Citrix Native Client	614
	Enabling Citrix Secure Gateways	617
	Creating a JSAM Application Resource Profile	618
	Specifying Applications for JSAM to Secure	622
	Specifying Role Level JSAM Options	624
	Automatically Launching JSAM	625
	Specifying Application Servers that Users Can Access	627
	Specifying Resource Level JSAM Options	628
Chapter 24	Telnet/SSH	631
	About Telnet/SSH	631
	Task Summary: Configuring the Telnet/SSH Feature	632
	Creating a Telnet/SSH Resource Profile	633
	Associating Bookmarks with Telnet/SSH Resource Profiles	634
	Configuring General Telnet/SSH Options	637
	Writing a Telnet/SSH Resource Policy	638
Chapter 25	Terminal Services	641
	About Terminal Services	642
	Terminal Services User Experience	642
	Task Summary: Configuring the Terminal Services Feature	643
	Terminal Services Execution	645
	Configuring Citrix to Support ICA Load Balancing	646
	About Terminal Services Resource Profiles	648
	Configuring a Windows Terminal Services Resource Profile	649
	Defining a Hosted Java Applet Autopolicy	650
	Defining a Bookmark for a Windows Terminal Services Profile	653
	Creating a Windows Terminal Services Bookmark Through the User Roles Page	654
	Defining Display Options for the Windows Terminal Services Session	655
	Defining SSO Options for the Windows Terminal Services Session	656
	Defining Application Settings for the Windows Terminal Services Session	656
	Defining Device Connections for the Windows Terminal Services Session	657
	Defining Desktop Settings for the Windows Terminal Services Session	659
	Creating a Citrix Terminal Services Resource Profile Using Default ICA Settings	659
	Defining a Bookmark for a Citrix Profile Using Default ICA Settings	660
	Defining Display Options for the Citrix Terminal Services Session	663
	Defining SSO Options for the Citrix Terminal Services Session	663

	Defining Application, Auto-Launch, and Session Reliability Settings for the Citrix Terminal Services Session	664
	Defining Device Connections for the Citrix Terminal Services Session	665
	Creating a Citrix Resource Profile That Uses a Custom ICA File	666
	Defining a Bookmark for a Citrix Profile Using a Custom ICA File	668
	Creating a Citrix Profile That Lists Published Applications	669
	Defining a Bookmark for a Citrix Profile Listing Applications	670
	Creating Session Bookmarks to Your Terminal Server	672
	Creating Advanced Terminal Services Session Bookmarks	673
	Creating Links from an External Site to a Terminal Services Session Bookmark	679
	Specifying General Terminal Services Options	685
	Configuring Terminal Services Resource Policies	688
	Specifying the Terminal Services Resource Option	689
	Using the Remote Desktop Launcher	689
Chapter 26	Junos Pulse Collaboration	691
	Junos Pulse Collaboration Overview	691
	Task Summary: Configuring Junos Pulse Collaboration	693
	Scheduling Meetings Through the Secure Access Service End-User Console	694
	Scheduling Meetings Through Microsoft Outlook	695
	Sending Notification Emails	697
	Junos Pulse Collaboration Bridge Profile	698
	Junos Pulse Collaboration Bridge Profile Overview	698
	Creating a Junos Pulse Collaboration Bridge Profile	699
	Viewing, Editing and Deleting Your Junos Pulse Collaboration Bridge Profile	701
	Viewing the Contents of the Junos Pulse Collaboration Bridge Profile	701
	Editing a Junos Pulse Collaboration Bridge Profile	701
	Deleting a Junos Pulse Collaboration Bridge Profile	702
	Entering the Junos Pulse Collaboration Bridge Profile Conference and PIN IDs	702
	Joining Meetings	703
	Attending Meetings	705
	Conducting Meetings	706
	Presenting Meetings	707
	About Instant Meetings and Support Meetings	707
	About MyMeeting Meetings	709
	Joining MyMeeting Meetings	709
	Enabling and Configuring Junos Pulse Collaboration	710
	Permissive Merge Guidelines for Junos Pulse Collaboration	714
	Specifying Authentication Servers that Meeting Creators Can Access	714
	Configuring System-Level Meeting Settings	716
	Configuring a Junos Pulse Collaboration Meeting Server	718
	Junos Pulse Collaboration Meeting Server Use Cases	720
	Troubleshooting Junos Pulse Collaboration	721
	Known Issues with Junos Pulse Collaboration	722
	Monitoring Junos Pulse Collaboration	723

Chapter 27	Email Client	725
	About the E-Mail Client	725
	Choosing an E-Mail Client	726
	Working with a Standards-Based Mail Server	727
	Working with the Microsoft Exchange Server	728
	Exchange Server and IMAP Clients	728
	Exchange Server and POP Clients	729
	Exchange Server and Outlook Web Access	729
	About Lotus Notes and the Lotus Notes Mail Server	730
	Enabling the E-Mail Client at the Role Level	730
	Writing the E-Mail Client Resource Policy	731
Chapter 28	VPN Tunneling	733
	About VPN Tunneling	734
	VPN Tunneling on 64-Bit Linux Platforms	736
	Task Summary: Configuring VPN Tunneling	737
	VPN Tunneling Execution	739
	Automatically Signing into VPN Tunneling using GINA	740
	Using GINA Chaining	742
	Credential Provider for Windows Vista and Later	742
	Smart Card Credential Provider	744
	Credential Provider Authentication for Pulse Secure Access Service	745
	Launching VPN Tunneling During a Windows Secure Application Manager Session	749
	Logging In To Windows Through a Secure Tunnel	750
	VPN Tunneling Connection Profiles with Support for Multiple DNS Settings	751
	VPN Tunneling Incompatibility with Other VPN Client Applications	752
	Linux Client Requirements	752
	Client Side Logging	752
	VPN Tunneling Proxy Support	753
	VPN Tunneling Quality of Service	754
	VPN Tunneling Multicast Support	755
	Defining VPN Tunneling Role Settings	755
	About VPN Tunneling Resource Policies	759
	Defining VPN Tunneling Access Control Policies	760
	Creating VPN Tunneling Connection Profiles	761
	Defining Split Tunneling Network Policies	768
	VPN Tunneling Resource Policy Configuration Use Case	770
	About VPN Tunneling Bandwidth Management Policies	772
	User is Mapped to Multiple Roles	773
	Limitations	774
	Writing a VPN Tunneling Bandwidth Management Resource Policy	775
	Configuring the VPN Tunnel Server	776
	Specifying IP Filters	776
	Specifying the VPN Tunneling Server Base IP Address	776
	VPN Tunneling Installer Overview	777
	VPN tunneling Installation Process Dependencies	777
	VPN Tunneling Un-installation Process Dependencies	778
	Network Connect Launcher (NC Launcher) Overview	780

	Launching Network Connect On Other Platforms	782
	Troubleshooting Network Connect Errors	784
	nc.windows.app.23792	784
	Version Conflict on Downgrade	784
	Error When Connecting to a FIPS Appliance	785
Part 5	System Management	
Chapter 29	General System Management	789
	General Network Settings	790
	Internal and External Ports	791
	Bonding Ports on the SA 6000 SSL VPN Appliance	791
	Bonding Ports on the SA 6500 SSL VPN Appliance	792
	Configuring the Internal and External Ports	792
	Configuring the Internal Port	792
	Configuring the External Port	794
	Configuring SFP Ports on the SA Series 6000 SSL VPN Appliance	797
	Configuring the Management Port on the SA Series 6000 SSL VPN Appliance	798
	Using VLANs with Secure Access Service	799
	Creating a New VLAN Port	802
	Using Virtual Ports	802
	About Virtual Ports	802
	Creating Virtual Ports	803
	Associating a Device Certificate with a Virtual Port	803
	Associating a Virtual Port with a Role	803
	Using Virtual Ports with Client Certificate Authentication	804
	Creating Virtual Ports for a Cluster	804
	Configuring Static Routes for Network Traffic	805
	Creating ARP Caches	806
	Specifying Host Names for Secure Access Service to Resolve Locally	807
	Configuring System Utilities	807
	Reviewing System Data	807
	Upgrading or Downgrading the Secure Access Service Device	810
	Upgrading Virtual Appliances	810
	Changing Personalities	810
	Setting System Options	811
	Downloading Application Installers	813
	Obtaining, Entering and Upgrading Your License Keys	815
	Configuring License Options	818
	Upgrading License Keys	819
	About Subscription Licenses	821
	Available Subscription Licenses	822
	Activating and Deactivating Emergency Mode	822
	Setting Security Options	823
	Setting System-Wide Security Options	824
	Configuring Lockout Options	826
	Configuring NCP and JCP	827
	Installing a Juniper Software Service Package	828

	Configuring Your Management Port Network Settings From the Serial Console	829
	Configuring Management Port Network Settings	830
	Adding Static Routes to the Management Route Table	832
	Assigning Certificate to Management Port	833
	Controlling Administrator Sign-In Access	833
	Signing in Over the Management Port	834
	Setting Role-Mapping Rules Using Custom Expressions	834
	Troubleshooting the Management Port	835
	Using the Management Port on a Cluster	836
	Importing Configurations to a System with the Management Port Enabled	836
Chapter 30	Certificates	837
	About Using Certificates on Secure Access Service	838
	Using Device Certificates	839
	Importing Certificates Into the Secure Access Service	840
	Downloading a Device Certificate From the Secure Access Service	842
	Creating a Certificate Signing Request (CSR) for a New Certificate	843
	Using Intermediate Server CA Certificates	844
	Importing Intermediate Server CA Certificates	845
	Using Multiple Secure Access Service Certificates	845
	Task summary: Enabling Multiple Device Certificates	845
	Associating a Certificate With a Virtual Port	846
	Using a Trusted Client CA	846
	About Trusted CAs	846
	Enabling Trusted Client CAs	848
	Limitations	849
	Automatically Importing an Intermediate Trusted Client CA Certificate	849
	Manually Uploading CA Certificates	851
	Specifying Attributes for the Trusted Client CA Certificate	853
	Specifying Client-side Certificate Restrictions	855
	Enabling Client CA Hierarchies	857
	Enabling CRLs	858
	Using a Proxy Server for CRL Downloads and OCSP Status Checks	860
	Specifying CDP Options	861
	Enabling OCSP	863
	Using Trusted Server CAs	864
	Uploading Trusted Server CA Certificates	865
	Renewing a Trusted Server CA Certificate	866
	Viewing Trusted Server CA Certificate Details	867
	Restoring the Prepopulated Group of Trusted Server CA Certificates	867
	Using Code-signing Certificates	868
	Additional Considerations for SUN JVM Users	869
	Task Summary: Configuring the Secure Access Service to Sign or Re-Sign Java Applets	869
	Importing a Code-Signing Certificate	870
	About Two-Way SSL Authentication	870
	Task Summary: Configuring the Secure Access Service for Two-Way SSL Authentication	871

	Importing the Certificates for Two-Way SSL Handshake	872
	Mapping Resource Policies to the Certificate	873
	Mapping an Client Authentication Auto-Policy	874
Chapter 31	Elliptic Curve Cryptography	875
	Understanding ECC Certificates	875
	About Suite B	875
	Using ECC Certificates with Secure Access Service and Access Control Service	876
	Example: Assigning an ECC P-256 Certificate to an External Virtual Port and Giving Preference to Suite B Ciphers	877
	Configuring the External Port	877
	(optional) Configuring the Virtual Ports	878
	Creating the Certificate Signing Request for a New Certificate	878
	Importing the Signed Certificate Created from a CSR	880
	Presenting the Certificate on the Network	880
	Setting the Security Options	881
	Verifying the Certificate on the Client	883
	Using TCP Dump to View Cipher Information	885
Chapter 32	System Archiving	889
	About System Archiving	889
	Specifying Archive Schedules	891
	Specifying Archiving Parameters	891
	Archiving Debug Logs	892
	Archiving System Snapshots	893
	Creating Local Backups of Secure Access Service Configuration Files	894
	Importing and Exporting Secure Access Service Configuration Files	896
	Importing and Exporting IVS Configuration Settings	900
	Importing and Exporting XML Configuration Files	901
	Creating and Modifying XML Instances	903
	Integrity Constraints	906
	Mapping the XML Instance to UI Components	907
	Downloading the Schema File	908
	Strategies for Working With XML Instances	909
	Importing and Exporting XML Configuration Data	910
	System Restarts	916
	XML Import/Export Use Cases	918
	Importing to a System with the Management Port	922
	Using Operation Attributes	922
	General Import Rules	924
	Using the Push Configuration Feature	924
	Defining Push Configuration Targets	926
	Pushing Configuration Settings	928
	Archiving Junos Pulse Collaboration Meetings	929
Chapter 33	Logging and Monitoring	931
	Logging and Monitoring Overview	931
	Log File Severity Levels	933
	Custom Filter Log Files	933

	Dynamic Log Filters	933
	Viewing and Deleting User Sessions	934
	Configuring Log Monitoring Features	935
	Configuring Events, User Access, Admin Access, and Sensor Logs	935
	Creating, Resetting, or Saving a Dynamic Log Query	936
	Specifying Which Events to Save in the Log File	936
	Creating, Editing, or Deleting Log Filters	937
	Example: Using IP Address Filters	938
	Monitoring the Secure Access Service as an SNMP Agent	939
	Viewing System Statistics	947
	About Client-Side Logs	948
	Enabling Client-Side Logging and Global Options	948
	Enabling and Viewing Client-Side Log Uploads	949
	Viewing General Status	950
	Viewing System Capacity Utilization	950
	Specifying Time Range and Data to Display in Graphs	952
	Configuring Graph Appearance	952
	Viewing Critical System Events	953
	Downloading the Current Service Package	953
	Configuring the System Date and Time	954
	Monitoring Active Users	955
	Viewing and Cancelling Scheduled Meetings	956
	Adding Real Source IP Addresses to Log Messages	957
Chapter 34	Troubleshooting	959
	About Troubleshooting	959
	Simulating and Tracking Events	960
	Simulating Events That Cause a Problem	960
	Tracking Events Using Policy Tracing	962
	Recording a Trace File	963
	Creating System State Snapshot Files	964
	Creating TCP Dump Files	965
	Troubleshooting TCP and UDP Port Status	966
	Secure Access Service Network Connectivity Tools	969
	Address Resolution Protocol	969
	Ping or Ping6	970
	Traceroute or Traceroute6	970
	NSlookup	970
	AvgRTTs	970
	Using UNIX Commands to Test Network Connectivity	971
	Running NSLookup to Test Name Server Connectivity	971
	Running Debugging Tools Remotely	971
	Creating Debugging Logs	972
	Monitoring Cluster Nodes	973
	Configuring Group Communication Monitoring on a Cluster	974
	Configuring Network Connectivity Monitoring on a Cluster	974

Chapter 35	Clustering	977
	About Clustering	977
	Cluster Licensing	978
	Example 1: Licenses Distributed Equally Among Nodes	979
	Example 2: Licenses Distributed Unequally Among Nodes	979
	Example 3: Licenses Distributed Unequally Among Nodes (Extreme Case)	979
	Upgrading From Previous Versions	980
	Task Summary: Deploying a Cluster	981
	Defining and Initializing a Cluster	982
	Joining an Existing Cluster	983
	Re-adding a Node to a Cluster	984
	Deploying Two Nodes in an Active/Passive Cluster	985
	Failing Over the VIP to Another Node	986
	Deploying Two or More Units in an Active/Active Cluster	986
	Synchronizing the Cluster State	988
	Specifying Active/Passive, Active/Active, and Other Cluster Settings	990
	Adding Multiple Cluster Nodes	992
	General Cluster Maintenance	993
	Managing Network Settings for Cluster Nodes	993
	Upgrading Clustered Nodes	993
	Upgrading the Cluster Service Package	993
	Migrating Cluster Configurations to a Replacement Cluster	994
	Changing the IP Address of a Cluster Node	995
	Deleting a Cluster	996
	Restarting or Rebooting Clustered Nodes	996
	Configuring the External VIP for An Active/Passive Cluster	996
	Admin Console Procedures	997
	Monitoring Clusters	999
	Troubleshooting Clusters	1000
	“Management IP Address Differs From the Management IP Address” Error Message	1001
	Serial Console Procedures	1002
	Joining the Secure Access Service to a Cluster Through Its Serial Console	1002
	Disabling a Clustered Secure Access Service Using Its Serial Console	1004
Chapter 36	Delegating Administrator Roles	1005
	About Delegating Administrator Roles	1005
	Creating and Configuring Administrator Roles	1006
	Specifying Management Tasks to Delegate	1007
	Delegating System Management Tasks	1007
	Delegating User and Role Management	1008
	Delegating User Realm Management	1008
	Delegating Administrative Management	1008
	Delegating Resource Policy Management	1009
	Delegating Resource Profile Management	1009
	Delegating Access to IVS Systems	1009

Chapter 37	Instant Virtual System	1011
	Instant Virtual System (IVS) Overview	1012
	Deploying an IVS	1014
	Virtualized Secure Access Service Architecture	1016
	Signing In to the Root System or the IVS	1017
	Signing-In Using the Sign-In URL Prefix	1017
	Signing-In Over Virtual Ports	1019
	Signing-In Over a VLAN Interface	1020
	Navigating to the IVS	1020
	IVS Configuration Worksheet	1021
	Administering the Root System	1023
	Configuring the Root Administrator	1023
	IVS Provisioning Process Overview	1025
	Configuring Sign-In Ports for IVS	1026
	Virtual Local Area Network (VLAN) on Subscriber IVS	1028
	Configuring VLANs on the Virtualized Secure Access Service	1029
	Adding Static Routes to the VLAN Route Table	1030
	Deleting a VLAN	1031
	Loading the Certificates Server	1032
	Creating a Virtual System (IVS Profile)	1032
	IVS Initial Config Via Copy from the Root System or Another IVS	1034
	Use Cases for IVS Initial Config Via Copy	1035
	Signing In Directly to the IVS as an IVS Administrator	1036
	About Role-Based Source IP Aliasing	1037
	Associating Roles with Source IP Addresses in an IVS	1037
	Configuring Policy Routing Rules on the IVS	1038
	Routing Rules	1039
	Overlapping IP Address Spaces	1039
	Define Resource Policies	1039
	Clustering a Virtualized Secure Access Service	1040
	Accessing a DNS Server on the MSP Network	1041
	Accessing a DNS Server on a Subscriber Company Intranet	1042
	Configuring VPN Tunneling for Use on a Virtualized Secure Access Service	1043
	Configuring a Centralized DHCP Server	1046
	About Authentication Servers	1047
	Rules Governing Access to Authentication Servers	1048
	Configuring Authentication on a RADIUS Server	1048
	Configuring Authentication on Active Directory	1049
	Delegating Administrative Access to IVS Systems	1049
	Accessing Standalone Installers on an IVS System	1050
	Exporting and Importing IVS Configuration Files	1050
	Using XML Import and XML Export on IVS Systems	1052
	Monitoring Subscribers	1053
	Troubleshooting VLANs	1053
	IVS Use Case: Policy Routing Rules Resolution	1055
	Use Case: Configuring a Global Authentication Server for Multiple Subscribers	1060
	Use Case: Configuring a DNS/WINS Server IP Address per Subscriber	1061

	Use Case: Configuring Access to Web Applications and Web Browsing for Each Subscriber	1061
	Use Case: Configuring File Browsing Access for Each Subscriber	1062
	Use Case: Setting Up Multiple Subnet IP Addresses for a Subscriber's End-Users	1063
	Use Case: Configuring Multiple IVS Systems to Allow Access to Shared Server	1064
Chapter 38	IPv6 Support	1065
	Understanding IPv6	1065
	About IPv6	1065
	About IPv6 Address Types	1066
	About IPv6 Address Text Representation	1066
	About the IPv6 Unspecified Address	1067
	About the IPv6 Loopback Address	1067
	About IPv6 Address Prefixes	1067
	System Normalization of IPv6 Addresses	1067
	About Neighbor Discovery Protocol	1068
	IPv6 Support Overview	1069
	Client Access Summary	1069
	Network Topologies	1070
	IPv6 Support and Limitations for Secure Access Service Features	1071
	IPv6 Feature Configuration Task Summary	1075
	Managing the Neighbor Discovery Cache	1077
	Example: Creating a Cluster That Supports IPv6 Client Access	1077
	Overview	1077
	Before You Begin	1078
	Defining and Initializing a Cluster	1078
	Joining Nodes to the Cluster	1079
	Advanced Configuration	1080
Chapter 39	Secure Access Service and IDP Interoperability	1081
	About IDP	1081
	Licensing: IDP Availability	1082
	IDP Deployment Scenarios	1082
	Configuring the Secure Access Service to Interoperate with IDP	1083
	Interaction Between the IC Series and IDP	1084
	Configuring IDP Sensor Policies	1084
	Defining Automatic Response Sensor Event Policies	1086
	Identifying and Managing Quarantined Users Manually	1088
Chapter 40	Routing AAA Over the Management Port for Virtual Appliances	1091
	About Traffic Segregation	1091
	Configuring AAA Traffic Over the Management Port	1092
	Configuring AAA Traffic Through Both the Internal and Management Ports	1093

Part 6	System Services	
Chapter 41	Secure Access Service Serial Console	1097
	Using the Serial Console	1097
	Rolling Back to a Previous System State Through the Serial Console	1098
	Resetting a Secure Access Service Device to the Factory Setting Using the Serial Console	1099
	Performing Common Recovery Tasks with the Serial Console	1100
Chapter 42	Customizable Admin and End-User UIs	1103
	Customizable Admin and End-User UIs	1103
	Customizable End-User Interface Elements Overview	1104
Chapter 43	SA6000 Series Appliance	1105
	SA6000 Series Appliance	1105
	SA6000 Field-Replaceable Units	1106
Chapter 44	SA4500 and SA6500 Series Appliances	1109
	SA4500 and SA6500	1109
	Standard Hardware	1109
	SA Series 6500 Field-Replaceable Units	1110
	Device Status LED Behavior	1111
	Ethernet Port LED Behavior	1112
	Replacing the Cooling Fans	1113
	Replacing a Hard Drive	1114
	Replacing IOC Modules	1114
	Replacing a Power Supply	1116
Chapter 45	Secure Access FIPS	1119
	SA FIPS	1119
	SA FIPS Execution	1120
	Creating Administrator Cards	1121
	Deploying a Cluster in a Secure Access FIPS Environment	1122
	Creating a New Security World	1124
	Recovering an Archived Security World	1127
Chapter 46	SA4500 and SA6500 FIPS Appliances	1131
	FIPS Overview	1131
	Name and Password Restrictions	1132
	Initializing a Keystore	1133
	Reinitializing the Keystore	1133
	Joining a Cluster	1134
	Importing Device Certificates	1135
	Changing the Security Officer Password	1135
	Changing the Web User Password	1136
	Resetting the HSM Card In Case Of An Error	1137
	Upgrading the HSM Firmware	1137
	Binary Importing and Exporting of the Keystore	1138
	FIPS Device Status LED Behavior	1138

Chapter 47	FIPS Level 1 Support	1141
	Understanding Juniper Networks FIPS Level 1 Support	1141
	What Is FIPS?	1141
	What Is FIPS Level 1 Support?	1142
	FIPS Supported Platforms and Licensing	1142
	Enabling FIPS Level 1 Support	1143
	Turning Off FIPS Level 1 Support from the Serial Console	1146
	Installing a Self-Signed Certificate From the Serial Console	1147
	Supported Cipher Suites when FIPS Level 1 Support is Enabled and Disabled	1148
	Supported Cipher Suites When FIPS Level 1 Support is Disabled	1148
	Supported Cipher Suites When FIPS Level 1 Support is Enabled	1152
Chapter 48	Compression	1157
	About Compression	1157
	Enabling System-Level Compression	1159
Chapter 49	Multi-Language Support	1161
	About Multi-Language Support for the Secure Access Service	1161
	Encoding Files for Multi-Language Support	1162
	Localizing the User Interface	1162
	Localizing Custom Sign-In and System Pages	1163
Chapter 50	Handheld Devices and PDAs	1165
	Handheld Devices and PDAs	1165
	Task Summary: Configuring the Secure Access Service for PDAs and Handhelds	1166
	Defining Client Types	1168
	Enabling WSAM on PDAs	1169
	Enabling ActiveSync For Handheld Devices	1170
Chapter 51	Using IKEv2 with the Secure Access Service	1173
	About IKEv2	1173
	Extensible Authentication Protocol	1173
	Client Certificate-Based Authentication	1174
	Client Requirements	1174
	Supported Features	1175
	Task Summary: Configuring Secure Access for IKEv2	1176
	Defining the IKEv2 Role Mapping Rule	1177
	Enabling the IKEv2 Access Feature	1178
	Configuring the IKEv2 Ports	1178
Chapter 52	Writing Custom Expressions	1181
	Custom Expressions	1181
	Elements Used in Custom Expressions	1182
	Wildcard Matching	1185
	Distinguished Name Variables and Functions	1186
	System Variables and Examples	1186
	Using System Variables in Realms, Roles, and Resource Policies	1197
	Using Multi-Valued Attributes	1198
	Specifying Multi-valued Attributes in a Bookmark Name	1199
	Specifying Fetch Attributes in a Realm	1199

Specifying the homeDirectory Attribute for LDAP	1200
Using Custom Variables and Macros	1200
About Custom Variables and Macros	1200
Using Macros in Custom Expressions	1201
append	1202
daysdiff	1203
regmatch	1204

Part 7

Index

Index	1207
-------------	------

List of Figures

Part 1	Getting Started	
Chapter 2	Introduction to Secure Access Service	15
	Figure 1: Secure Access Service Working within a LAN	17
Part 2	Access Management Framework	
Chapter 3	General Access Management	71
	Figure 2: Security Checks Performed During a User Session	75
	Figure 3: Federation IF-MAP Topology	93
	Figure 4: Session-Import and Session-Export Policies	97
Chapter 4	User Roles	105
	Figure 5: Security Checks Performed by the Secure Access Service to Create a Session Role	106
Chapter 5	Resource Profiles	127
	Figure 6: Using Roles and Resource Policies to Configure Resources	129
	Figure 7: Using Resource Profiles to Configure Resources	130
Chapter 7	Resource Policies	143
	Figure 8: Resource Policy Evaluation Steps	148
Chapter 8	Authentication and Directory Servers	153
	Figure 9: User Admin Icon	188
	Figure 10: Creating a New Local User	189
Chapter 9	SAML Single Sign-on	233
	Figure 11: Secure Access Service as a SAML Service Provider in a Service-Provider-Initiated SSO Scenario	236
	Figure 12: Secure Access Service as a SAML Service Provider in an Identity-Provider-Initiated SSO Scenario	237
	Figure 13: Secure Access Service as a SAML Identity Provider (Gateway Mode)	238
	Figure 14: Secure Access Service as a SAML Identity Provider (Peer Mode) in a Service-Provider-Initiated SSO Scenario	239
	Figure 15: Secure Access Service as a SAML Identity Provider (Peer Mode) in an Identity-Provider-Initiated SSO Scenario	240
	Figure 16: Secure Access Service as a SAML identity provider (Gateway Mode)	261
	Figure 17: Secure Access Service as a SAML Identity Provider (Peer Mode) in a Service-Provider-Initiated SSO Scenario	267

	Figure 18: Secure Access Service as a SAML Identity Provider (Peer Mode) in an Identity-Provider-Initiated SSO Scenario	268
	Figure 19: Google Apps Advanced Tools: SSO	269
	Figure 20: SAML Global Settings	271
	Figure 21: SAML Identity Provider Settings	272
	Figure 22: Peer SP Settings	273
	Figure 23: External Applications Policy Settings	274
	Figure 24: Debug Log Page	276
	Figure 25: System Status Page	278
	Figure 26: Date and Time Page	279
	Figure 27: SAML Service Provider Configuration Page	280
	Figure 28: Artifact Profile	294
	Figure 29: POST Profile	298
	Figure 30: Access Control Policies	301
Chapter 10	Authentication Realms	305
	Figure 31: Junos Pulse Role Mapping Rule	313
	Figure 32: Server Catalog > Attributes Tab — Adding an Attribute for LDAP	315
	Figure 33: Server Catalog > Groups Tab — Adding LDAP Groups	316
	Figure 34: Server Catalog > Groups Tab — Adding Active Directory Groups	318
Chapter 12	Single Sign-On	335
	Figure 35: Collecting and Submitting Credentials from Multiple Servers	339
	Figure 36: Artifact Profile	347
	Figure 37: POST Profile	351
	Figure 38: Access Control Policies	354
Part 3	Endpoint Defense	
Chapter 14	Host Checker	373
	Figure 39: Host Checker Creates a Tunnel from a Client to a Policy Server Behind the Secure Access Service	422
Part 4	Remote Access	
Chapter 23	Secure Application Manager	583
	Figure 40: Java Secure Application Manager	603
	Figure 41: Java Secure Application Manager and Enhanced MS Exchange Support	611
	Figure 42: Java Secure Application Manager and Enhanced Lotus Notes Support	612
Chapter 26	Junos Pulse Collaboration	691
	Figure 43: Using the Junos Pulse Collaboration	695
	Figure 44: Using the Junos Pulse Collaboration Tab in the Options Window	696
	Figure 45: Online Meeting Button is Not Used	696
	Figure 46: Deleting the Meeting	697
Chapter 28	VPN Tunneling	733
	Figure 47: GINA Installation Process	741
	Figure 48: Pulse Logon Tile	745

	Figure 49: Credential Provider Log Information	749
Part 5	System Management	
Chapter 29	General System Management	789
	Figure 50: Example VLAN Use	801
	Figure 51: License Key Generation and Activation	816
Chapter 30	Certificates	837
	Figure 52: Defining Proxy Settings	860
Chapter 31	Elliptic Curve Cryptography	875
	Figure 53: Configuring the External Port for IPv4	877
	Figure 54: Creating the Virtual Port on the External Port	878
	Figure 55: Creating an ECC P-256 Certificate Signing Request	879
	Figure 56: CSR Successfully Created	879
	Figure 57: Pending CSR	880
	Figure 58: Associating the ECC P-256 With The External Virtual Port p_ecdsa256	881
	Figure 59: Setting Custom SSL Cipher Selections	882
	Figure 60: Confirming Custom Ciphers	883
	Figure 61: Connecting to a Port Using an ECC Curve P-256 Certificate	883
	Figure 62: Viewing the Connection Certificate Information	884
	Figure 63: Certificate Public Key	884
	Figure 64: Viewing the TCP Dump Output	885
	Figure 65: Issued to Certificate on the Device Certificates Pages	885
Chapter 32	System Archiving	889
	Figure 66: Archiving Debug Logs	893
	Figure 67: Including Debug Logs in System Snapshots	894
	Figure 68: Secure Access Service Object Referential Integrity Constraints	906
Chapter 33	Logging and Monitoring	931
	Figure 69: Using IP Address Filters	939
Chapter 34	Troubleshooting	959
	Figure 70: Successful TCP Port Probe	968
	Figure 71: Unsuccessful UDP Port Probe	969
Chapter 35	Clustering	977
	Figure 72: Active/Passive Cluster Pair	986
	Figure 73: Active/Active Configuration	988
Chapter 37	Instant Virtual System	1011
	Figure 74: MSP Deployment Scenario	1014
	Figure 75: IVS Architecture	1016
	Figure 76: Setting a Static Route in MSP Network DNS or Application Servers	1044
Chapter 38	IPv6 Support	1065
	Figure 77: IPv4 Endpoint Access to IPv6 Resources	1070
	Figure 78: IPv6 Endpoint Access to IPv4 Resources	1071
Chapter 39	Secure Access Service and IDP Interoperability	1081

Figure 79: Secure Access Service and IDP Topology Scenario 1 1083
Figure 80: Secure Access Service and IDP Topology Scenario 2 1083
Figure 81: Managing Quarantined Users 1089

Part 6

Chapter 47

System Services

FIPS Level 1 Support 1141
Figure 82: Enabling FIPS Level 1 Support 1144
Figure 83: Example of Allowed Encryption Strengths 1145
Figure 84: Events Log Entries for FIPS Level 1 1146
Figure 85: Admin Access Logs for FIPS Level 1 Encryption Strength Changes . . 1146

List of Tables

	About This Guide	xxxvii
	Table 1: Notice Icons	xxxviii
Part 1	Getting Started	
Chapter 2	Introduction to Secure Access Service	15
	Table 2: Pulse Connection Options	46
	Table 3: Pulse Launcher Arguments	65
	Table 4: Pulse Launcher Return Codes	66
Part 2	Access Management Framework	
Chapter 4	User Roles	105
	Table 5: Session Options	112
	Table 6: Configurable Options on the Apple iPad	121
	Table 7: View Menu Options	124
Chapter 5	Resource Profiles	127
	Table 8: Resource Profile Types and Configuration Information	130
Chapter 7	Resource Policies	143
	Table 9: DNS Hostname Special Characters	146
	Table 10: Port Possible Values	147
Chapter 8	Authentication and Directory Servers	153
	Table 11: Supported Password Management Functions	182
	Table 12: AD/NT Password Management Matrix	183
	Table 13: Attributes Common to both Start and Stop Messages	196
	Table 14: Start Attributes	197
	Table 15: Stop Attributes	197
	Table 16: RADIUS Role Mapping Attributes	198
	Table 17: eTrust SiteMinder Configuration Options	219
	Table 18: eTrust SiteMinder Advanced Configuration Options	224
	Table 19: SAML SP Profile (POST and Artifact)	229
Chapter 9	SAML Single Sign-on	233
	Table 20: Supported SAML 2.0 Deployment Profiles	240
	Table 21: SAML Support for FIPS Deployments	241
	Table 22: SAML Global Settings	243
	Table 23: SAML Metadata Provider Settings	245
	Table 24: SAML Service Provider Profile	247
	Table 25: Sign-in SAML Identity Provider Metadata Provider Settings	251

	Table 26: Sign-in SAML Identity Provider Settings	252
	Table 27: Peer Service Provider Configuration	255
	Table 28: SAML SSO Resource Policy Settings	262
	Table 29: SAML SSO External Applications Policy Settings	263
	Table 30: SAML ACL Web Policy Settings	264
	Table 31: Google Apps SSO Configuration	269
	Table 32: SAML Authentication Server (SAML 1.1)	292
Part 3	Endpoint Defense	
Chapter 14	Host Checker	373
	Table 33: Wildcard Characters for Specifying a File Name or Process Name . . .	399
	Table 34: Environment Variables for Specifying a Directory Path on Windows . .	400
	Table 35: Environment Variables for Specifying a Directory Path on Linux and Solaris	400
	Table 36: Environment Variables for Specifying a Directory Path on Macintosh	401
Part 4	Remote Access	
Chapter 17	Citrix Templates	467
	Table 37: Accessing the Citrix Web Interface Server using Web Resource Profile Templates	469
Chapter 21	Web Rewriting	489
	Table 38: DNS hostname special characters	498
	Table 39: Port possible values	498
	Table 40: Port Possible Values	506
	Table 41: Port Possible Values	520
	Table 42: OWA Caching Resource Policies	535
	Table 43: iNotes Caching Resource Policies	536
	Table 44: Predefined Resource Policies	548
Chapter 23	Secure Application Manager	583
	Table 45: WSAM Command Line Arguments	597
Chapter 25	Terminal Services	641
	Table 46: Case-Insensitive Terminal Services Session Bookmark Parameter Names	680
Chapter 28	VPN Tunneling	733
	Table 47: Installing Standard 32-Bit Libraries and Components	736
	Table 48: VPN tunneling Compatibility with Third-Party VPN Clients	752
	Table 49: VPN Tunneling Connection Profile Settings	762
	Table 50: Privilege Levels and Percent of Maximum Bandwidth	772
Part 5	System Management	
Chapter 29	General System Management	789
	Table 51: Internal Port Settings	793
	Table 52: External Port Settings	795

	Table 53: RAID and Hard Drive Status for the SA6000 and SA6500	809
	Table 54: RAID and Hard Drive Status for the MAG-SM360	809
	Table 55: Management Port Settings	830
Chapter 32	System Archiving	889
	Table 56: System Behavior When Editing Options	916
	Table 57: Legal Operation Attribute Relationships	923
Chapter 33	Logging and Monitoring	931
	Table 58: Configuration Objects	942
Chapter 34	Troubleshooting	959
	Table 59: Snapshot Configuration Options and Details	965
Chapter 35	Clustering	977
	Table 60: Cluster Status Page Information	997
	Table 61: Cluster Status	1000
Chapter 37	Instant Virtual System	1011
	Table 62: VLAN1 Route Table	1057
	Table 63: VLAN2 Route Table	1058
	Table 64: VLAN3 Route Table	1058
	Table 65: VLAN4 Route Table	1058
	Table 66: VLAN1 Route Table	1059
	Table 67: VLAN2 route table	1060
	Table 68: VLAN3 route table	1060
	Table 69: VLAN4 route table	1060
Chapter 38	IPv6 Support	1065
	Table 70: System Normalization of IPv6 Addresses	1067
	Table 71: Secure Access Service Release 7.4 Client Access Scenarios	1069
	Table 72: Summary of IPv6 Support	1072
	Table 73: IPv6 Feature Configuration Task Summary	1075
	Table 74: Secure Access Service Clusters: Advanced Configuration Guidelines	1080
Chapter 40	Routing AAA Over the Management Port for Virtual Appliances	1091
	Table 75: Configuring Traffic Segregation Options	1092
Part 6	System Services	
Chapter 44	SA4500 and SA6500 Series Appliances	1109
	Table 76: Device Status LEDs	1112
	Table 77: 4-Port Copper Gigabit Ethernet LEDs (available on IC4500 and IC6500)	1112
Chapter 46	SA4500 and SA6500 FIPS Appliances	1131
	Table 78: Security Officer Name and Username Requirements	1132
	Table 79: Status LED	1139
Chapter 47	FIPS Level 1 Support	1141
	Table 80: Supported Cipher Suites With FIPS Level 1 Support Off, Hardware Acceleration Enabled and RSA Server Certificates In Use	1148

	Table 81: Supported Cipher Suites With FIPS Level 1 Support Off, Hardware Acceleration Enabled and ECC Server Certificates In Use	1149
	Table 82: Supported Cipher Suites With FIPS Level 1 Support Off, Hardware Acceleration Enabled and RSA Server Certificates In Use	1150
	Table 83: Supported Cipher Suites With FIPS Level 1 Support Off, Hardware Acceleration Disabled and ECC Server Certificates In Use	1151
	Table 84: Supported Cipher Suites With FIPS Level 1 Support On and ECC Server Certificates In Use	1153
	Table 85: Supported Cipher Suites With FIPS Level 1 Support On and RSA Server Certificates In Use	1154
Chapter 52	Writing Custom Expressions	1181
	Table 86: Custom Expression Elements	1182
	Table 87: System Variables and Examples	1187

About This Guide

- Objective on page xxxvii
- Audience on page xxxvii
- Document Conventions on page xxxvii
- Documentation on page xxxviii
- Obtaining Documentation on page xxxviii
- Documentation Feedback on page xxxviii
- Requesting Technical Support on page xxxviii

Objective

This guide describes basic configuration procedures for Juniper Networks Secure Access Secure Access Service. This document was formerly titled *Secure Access Administration Guide*. This document is now part of the Junos Pulse documentation set.

Audience

This guide is designed for network administrators who are configuring and maintaining a Juniper Networks Secure Access Service device. To use this guide, you need a broad understanding of networks in general and the Internet in particular, networking principles, and network configuration. Any detailed discussion of these concepts is beyond the scope of this guide.

Document Conventions

Table 1 on page xxxviii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Documentation

For a list of related Secure Access Service documentation, see <http://www.juniper.net/support/products/sa/>. If the information in the latest Release Notes differs from the information in the documentation, follow the Release Notes.

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the products documentation page on the Juniper Networks web site at <http://www.juniper.net/techpubs>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf> .
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/> .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

PART 1

Getting Started

- [Initial Verification and Key Concepts on page 3](#)
- [Introduction to Secure Access Service on page 15](#)

CHAPTER 1

Initial Verification and Key Concepts

- [Verifying User Accessibility on page 3](#)
- [Creating a Test Scenario to Learn Secure Access Service Concepts and Best Practices on page 4](#)
- [Defining a User Role on page 5](#)
- [Defining a Resource Profile on page 6](#)
- [Defining an Authentication Server on page 7](#)
- [Defining an Authentication Realm on page 9](#)
- [Defining a Sign-In Policy on page 10](#)
- [Using the Test Scenario on page 12](#)
- [Default Settings for Administrators on page 13](#)

Verifying User Accessibility

You can easily create a user account in the system authentication server for use in verifying user accessibility to your Secure Access Service device. After creating the account through the admin console, sign in as the user on the Secure Access Service user sign-in page.

To verify user accessibility:

1. From the admin console, choose **Authentication > Auth. Servers**.
2. Select the **System Local** link.
3. Select the **Users** tab.
4. Click **New**.
5. Type **testuser1** as the username and enter a password, and then click **Save Changes**. Secure Access Service creates the testuser1 account.
6. Use another browser window to enter the machine's URL to access the user sign-in page. The URL is in the format: `https://a.b.c.d`, where `a.b.c.d` is the machine IP address you entered in the serial console when you initially configured your Secure Access Service.
7. Click **Yes** when prompted with the security alert to proceed without a signed certificate. The user sign-in page appears, indicating that you have successfully connected to your Secure Access Service.

8. Enter the username and password you created for the user account and then click **Sign In** to access the Secure Access Service home page for users.
9. Enter the URL to an internal Web server in the Address box and click **Browse**. Secure Access Service opens the Web page in the same browser window, so to return to the Secure Access Service home page, click the center button on the toolbar that appears on the target Web page.
10. Enter the URL to your external corporate site on the Secure Access Service home page, and click **Browse**. Secure Access Service opens the Web page in the same browser window, so use the button on the toolbar to return to the Secure Access Service home page.
11. Click **Browsing > Windows Files** on the Secure Access Service home page to browse through available Windows file shares or **Browsing > UNIX/NFS Files** to browse through available UNIX NFS file shares.

Related Documentation

- [Creating a Test Scenario to Learn Secure Access Service Concepts and Best Practices on page 4](#)
- [Defining a User Role on page 5](#)
- [Defining a Resource Profile on page 6](#)
- [Defining an Authentication Server on page 7](#)
- [Defining an Authentication Realm on page 9](#)
- [Defining a Sign-In Policy on page 10](#)
- [Using the Test Scenario on page 12](#)

[Creating a Test Scenario to Learn Secure Access Service Concepts and Best Practices](#)

Secure Access Service provides a flexible access management system that makes it easy to customize a user's remote access experience through the use of roles, resource policies, authentication servers, authentication realms, and sign-in policies. To enable you to quickly begin working with these entities, Secure Access Service ships with system defaults for each. you can create each access management entity by performing the following tasks:

- Define a user role
- Define a resource policy
- Define an authentication server
- Define an authentication realm
- Define a sign-in policy

Secure Access Service supports two types of users:

- **Administrators**—An administrator is a person who may view or modify Secure Access Service configuration settings. You create the first administrator account through the serial console.
- **Users**—A user is a person who uses Secure Access Service to gain access to corporate resources as configured by an administrator.

Related Documentation

- [Verifying User Accessibility on page 3](#)
- [Defining a User Role on page 5](#)
- [Defining a Resource Profile on page 6](#)
- [Defining an Authentication Server on page 7](#)
- [Defining an Authentication Realm on page 9](#)
- [Defining a Sign-In Policy on page 10](#)
- [Using the Test Scenario on page 12](#)

Defining a User Role

Secure Access Service is preconfigured with one user role called “Users.” This predefined role enables the Web and file browsing access features, enabling any user mapped to the Users role to access the Internet, corporate Web servers, and any available Windows and UNIX NFS file servers. You can view this role on the User Roles page.

After you enable an access feature for a role, configure the appropriate corresponding options that are accessible from the access feature’s configuration tab.

To define a user role:

1. In the admin console, choose **Users > User Roles**.
2. Click **New Role**.
3. Enter **Test Role** in the Name box and then click **Save Changes**.

Wait for Secure Access Service to display the Test Role page with the General tab and Overview link selected.

4. Select the **Web** check box under Access features and then click **Save Changes**.
5. Select **Web > Options**.
6. Select the **User can type URLs in the IVE browser bar** check box, and then click **Save Changes**.

After completing these steps, you have defined a user role. When you create resource profiles, you can apply them to this role. You can also map users to this role through role mapping rules defined for an authentication realm.

To quickly create a user role that enables Web and file browsing, duplicate the Users role, and then enable additional access features as desired.

Related Documentation

- [Verifying User Accessibility on page 3](#)
- [Creating a Test Scenario to Learn Secure Access Service Concepts and Best Practices on page 4](#)
- [Defining a Resource Profile on page 6](#)
- [Defining an Authentication Server on page 7](#)
- [Defining an Authentication Realm on page 9](#)
- [Defining a Sign-In Policy on page 10](#)
- [Using the Test Scenario on page 12](#)

Defining a Resource Profile

A resource profile is a set of configuration options that contains all of the resource policies, role assignments, and end-user bookmarks required to provide access to an individual resource.

Within a resource profile, a resource policy specifies the resources to which the policy applies (such as URLs, servers, and files) and whether Secure Access Service grants access to a resource or performs an action. Note that Secure Access Service is preconfigured with two types of resource policies:

- **Web Access**—The predefined Web Access resource policy, Initial Policy for Local Resources, allows access only to hosts belonging to domains within the secured network.
- **Windows Access**—The predefined Windows Access resource policy enables all users mapped to the Users role to access all corporate Windows file servers. By default, this resource policy applies to the Users role.



NOTE: Delete the Windows Access resource policies if you are concerned about users having access to all of your Web and file content.

To define a resource profile:

1. In the admin console, choose **Users > Resource Profiles > Web**.
2. Click **New Profile**.
The Web Applications Resource Profile page appears.
3. Fill in the following information:
 - a. In the Type box, keep the default option (Custom).
 - b. In the Name box, type **Test Web Access**.

- c. In the Base URL box, type **http://www.google.com**.
- d. Under Autopolicy: Web Access Control, select the check box next to the default policy created by Secure Access Service (http://www.google.com:80/*) and choose **Delete**.
- e. In Resource box, type **http://www.google.com**, select **Deny** from the Action list, and click **Add**.
- f. Click **Save and Continue**.

The Test Web Access page appears.

4. Click the **Roles** tab.
 - a. Select **Test Role** in the Available Roles box and click **Add** to move it to the Selected Roles box.
 - b. Click **Save Changes**.

Secure Access Service adds Test Web Access to the Web Application Resource Policies page and automatically creates a corresponding bookmark that links to google.com.

After completing these steps, you have configured a Web Access resource profile. Even though Secure Access Service comes with a resource policy that enables access to all Web resources, users mapped to Test Role are still prohibited from accessing <http://www.google.com>. These users are denied access because the autopolicy you created during the resource profile configuration takes precedence over the default Web access policy that comes with Secure Access Service.

Related Documentation

- [Verifying User Accessibility on page 3](#)
- [Creating a Test Scenario to Learn Secure Access Service Concepts and Best Practices on page 4](#)
- [Defining a User Role on page 5](#)
- [Defining an Authentication Server on page 7](#)
- [Defining an Authentication Realm on page 9](#)
- [Defining a Sign-In Policy on page 10](#)
- [Using the Test Scenario on page 12](#)

Defining an Authentication Server

An authentication server is a database that stores user credentials—username and password—and typically group and attribute information. When a user signs in to Secure Access Service, the user specifies an authentication realm, which is associated with an authentication server. Secure Access Service forwards the user's credentials to this authentication server to verify the user's identity.

Secure Access Service supports the most common authentication servers, including Windows NT Domain, Active Directory, RADIUS, LDAP, NIS, RSA ACE/Server, SAML Server, and eTrust SiteMinder, and enables you to create one or more local databases of users who are authenticated by Secure Access Service. Secure Access Service is preconfigured with one local authentication server for users called "System Local." This predefined local authentication server is a Secure Access Service database that enables you to quickly create user accounts for user authentication. This ability provides flexibility for testing purposes and for providing third-party access by eliminating the need to create user accounts in an external authentication server.

You can view the default local authentication server on the Authentication Servers page.



NOTE: Secure Access Service also supports authorization servers. An authorization server (or directory server) is a database that stores user attribute and group information. You can configure an authentication realm to use a directory server to retrieve user attribute or group information for use in role mapping rules and resource policies.

To define an authentication server:

1. In the admin console, choose **Authentication > Auth. Servers**.
2. Select **Local Authentication** from the New list and then click **New Server**.

The New Local Authentication page appears.

3. Enter **Test Server** in the Name box and then click **Save Changes**.

Wait for Secure Access Service to notify you that the changes are saved, after which additional configuration tabs appear.

4. Click the **Users** tab and then click **New**.

The New Local User page appears.

5. Enter **testuser2** in the Username box, enter a password, and then click **Save Changes** to create the user's account in the Test Server authentication server.

After completing these steps, you have created an authentication server that contains one user account. This user can sign in to an authentication realm that uses the Test Server authentication server.

The admin console provides last access statistics for each user account on the respective authentication servers pages, on the Users tab under a set of columns titled Last Sign-in Statistic. The statistics reported include the last successful sign-in date and time for each user, the user's IP address, and the agent or browser type and version.

Related Documentation

- [Verifying User Accessibility on page 3](#)
- [Creating a Test Scenario to Learn Secure Access Service Concepts and Best Practices on page 4](#)
- [Defining a User Role on page 5](#)

- [Defining a Resource Profile on page 6](#)
- [Defining an Authentication Realm on page 9](#)
- [Defining a Sign-In Policy on page 10](#)
- [Using the Test Scenario on page 12](#)

Defining an Authentication Realm

An authentication realm is a grouping of authentication resources, including:

- An authentication server, which verifies a user's identity. Secure Access Service forwards credentials submitted on a sign-in page to an authentication server.
- An authentication policy, which specifies realm security requirements that need to be met before Secure Access Service submits credentials to an authentication server for verification.
- A directory server, which is an LDAP server that provides user and group attribute information to Secure Access Service for use in role mapping rules and resource policies (optional).
- Role mapping rules, which are conditions a user must meet for Secure Access Service to map a user to one or more roles. These conditions are based on information returned by the realm's directory server, the person's username, or certificate attributes.

Secure Access Service is preconfigured with one user realm called "Users." This predefined realm uses the System Local authentication server, an authentication policy that requires a minimum password length of four characters, no directory server, and contains one role mapping rule that maps all users who sign in to the Users realm to the Users role. The "testuser1" account you created is part of the Users realm, because this account is created in the System Local authentication server. The "testuser2" account you created is not part of the Users realm, because you create the user account in the new "Test Server" authentication server, which is not used by the Users realm.

You can view the default user authentication realm on the User Authentication Realms page.

To define an authentication realm:

1. In the admin console, choose **Users > User Realms**.
The User Authentication Realms page appears.
2. Click **New**.
The New Authentication Realm page appears.
3. Enter **Test Realm** in the Name box.
4. Select **Test Server** from the Authentication list.
5. Click **Save Changes**.

Wait for Secure Access Service to notify you that the changes are saved and to display the realm's configuration tabs.

6. Click the **Role Mapping** tab if it is not already selected, and then click **New Rule**.

The Role Mapping Rule page appears.

7. Enter **testuser2** in the text box.
8. Under "...then assign these roles", select **Test Role** from the Available Roles list and click **Add** to move it to the Selected Roles box.
9. Click **Save Changes**.

After completing these steps, you have finished creating an authentication realm. This realm uses Test Server to authenticate users and a role mapping rule to map testuser2 to Test Role. Because the Test Web Access resource policy applies to Test Role, any user mapped to this role cannot access <http://www.google.com>.

Related Documentation

- [Verifying User Accessibility on page 3](#)
- [Creating a Test Scenario to Learn Secure Access Service Concepts and Best Practices on page 4](#)
- [Defining a User Role on page 5](#)
- [Defining a Resource Profile on page 6](#)
- [Defining an Authentication Server on page 7](#)
- [Defining a Sign-In Policy on page 10](#)
- [Using the Test Scenario on page 12](#)

Defining a Sign-In Policy

A sign-in policy is a system rule that specifies:

- A URL where a user may sign in to Secure Access Service.
- A sign-in page to display to the user.
- Whether or not the user needs to type or select an authentication realm to which Secure Access Service submits credentials.
- The authentication realms where the sign-in policy applies.

All Secure Access Service and SA Series FIPS appliances are preconfigured with one sign-in policy that applies to users: */. This default user sign-in policy (*/) specifies that when a user enters the URL to Secure Access Service, Secure Access Service displays the default sign-in page for the user and requires the user to select an authentication realm (if more than one realm exists). The */ sign-in policy is configured to apply to the Users authentication realm, therefore this sign-in policy does not apply to the authentication realm you created.

You can view the default user sign-in policy on the Signing In page. If your Secure Access Service has the Junos Pulse Collaboration Upgrade license, the */meeting sign-in policy

is also listed on this page. This policy enables you to customize the sign-in page for Junos Pulse Collaboration meetings.

To define a sign-in policy:

1. In the admin console, choose **Authentication > Signing in > Sign-in Policies**.
The Signing In page appears.
2. Click */ under User URLs.
The */ page appears.
3. Enter **test** after */ in the Sign-in URL box.
4. Under Authentication realm, select the **User picks from a list of authentication realms** option button, and then select **Test Realm** from the Available Realms list and click **Add** to move it to the Selected Realms box. (Repeat this process for the Users role if it is not already in the Selected Realms box.)
5. Click **Save Changes**.

After completing these steps, you have finished modifying the default users sign-in policy.

Optional Steps

You can perform these following optional steps to define a new sign-in page that is associated with the */test/ sign-in policy.

1. Select **Authentication > Signing In > Sign In Pages**, and then click **New Page**.
2. Enter **Test Sign-in Page** in the Name field, type **#FF0000** (red) in the Background color box, and then click **Save Changes**.
3. Select **Authentication > Signing In > Signing In Policies**, and then click **New URL**.
The New Sign-In Policy page appears.
4. Type ***/test/** in the Sign-in URL box, select **Default Sign-in Page** from the Sign-in Page list, and click **Save Changes**.
5. Select **Authentication > Signing In > Sign In Policies**, and then click ***/test/** under User URLs.
The */test/ page appears.
6. Select **Test Sign-in Page** from the Sign-in page list and then click **Save Changes**.

Related Documentation

- [Verifying User Accessibility on page 3](#)
- [Creating a Test Scenario to Learn Secure Access Service Concepts and Best Practices on page 4](#)
- [Defining a User Role on page 5](#)
- [Defining a Resource Profile on page 6](#)
- [Defining an Authentication Server on page 7](#)

- [Defining an Authentication Realm on page 9](#)
- [Using the Test Scenario on page 12](#)

Using the Test Scenario

The test scenario enables you to do the following tasks:

- Access the user console using the modified default sign-in policy.
- Sign in as the user created in the Test Server to map to the Test Realm.
- Test your Web browsing capabilities, which are dependent upon the proper configuration of Test Role and Test Web Access.

To use the test scenario:

1. In a browser, enter the machine's URL followed by **/test** to access the user sign-in page. The URL is in the format: `https://a.b.c.d/test`, where *a.b.c.d* is the machine IP address you entered in the serial console during initial configuration.
2. Click **Yes** when prompted with the security alert to proceed without a signed certificate. If the user sign-in page appears, you have successfully connected to your Secure Access Service device.



NOTE: If you performed the optional configuration steps in “Defining a Sign-In Policy”, the header color is red.

3. Enter the username and password you created for the user account in Test Server, type Test Realm in the Realm box, and then click Sign In to access the Secure Access Service home page for users.

Secure Access Service forwards the credentials to Test Realm, which is configured to use Test Server. Upon successful verification by this authentication server, Secure Access Service processes the role mapping rule defined for Test Realm, which maps testuser2 to Test Role. Test Role enables Web browsing for users.

4. In the browser Address box, enter the URL to your corporate Web site and click Browse. Secure Access Service opens the Web page in the same browser window, so to return to the Secure Access Service home page, click the center icon in the browsing toolbar that appears on the target Web page.
5. On the Secure Access Service home page, type **www.google.com** and click **Browse**. Secure Access Service displays an error message, because the Test Web Access resource policy denies access to this site for users mapped to Test Role.
6. Return to the Secure Access Service home page, click **Sign Out**, and then return to the user sign-in page.
7. Enter the credentials for testuser1, specify the Users realm, and then click **Sign In**.

8. On the Secure Access Service home page, type **www.google.com** and click **Browse**. Secure Access Service opens the Web page in the same browser window.
9. The test scenario demonstrates the basic Secure Access Service access management mechanisms. You can create very sophisticated role mapping rules and resource policies that control user access depending on factors such as a realm's authentication policy, a user's group membership, and other variables. To learn more about Secure Access Service access management, we recommend that you take a few minutes to review the online Help to familiarize yourself with its contents.

When you configure Secure Access Service for your enterprise, we recommend that you perform user access configuration. Before you make your Secure Access Service available from external locations, we recommend that you import a signed digital certificate from a trusted certificate authority (CA).

Related Documentation

- [Verifying User Accessibility on page 3](#)
- [Creating a Test Scenario to Learn Secure Access Service Concepts and Best Practices on page 4](#)
- [Defining a User Role on page 5](#)
- [Defining a Resource Profile on page 6](#)
- [Defining an Authentication Server on page 7](#)
- [Defining an Authentication Realm on page 9](#)
- [Defining a Sign-In Policy on page 10](#)

Default Settings for Administrators

Just like for users, Secure Access Service provides default settings that enable you to quickly configure accounts for administrators. This list summarizes the system default settings for administrators:

- Administrator roles—There are two built-in administrator roles.
 - .Administrators — This built-in role permits administrators to manage all aspects of Secure Access Service. The administrator user you create through the serial console is mapped to this role.
 - .Read-Only Administrators — This built-in role permits users mapped to the role to view (but not configure) all Secure Access Service settings. You need to map administrators to this role if you want to restrict their access.
- Administrators local authentication server — The Administrators local authentication server is an a Secure Access Service database that stores administrator accounts. You create the first administrator account in this server through the serial console. (Secure Access Service adds all administrator accounts created through the serial console to this server.) You cannot delete this local server.
- Admin Users authentication realm — The Admin Users authentication realm uses the default Administrators local authentication server, an authentication policy that requires

a minimum password length of four characters, no directory server, and one role mapping rule that maps all users who sign in to the Admin Users realm to the .Administrators role. The administrator account you create through the serial console is part of the Admin Users realm.

- [*/admin sign-in policy](#) — The default administrator sign-in policy ([*/admin](#)) specifies that when a user enters the URL to Secure Access Service followed by [/admin](#), Secure Access Service displays the default sign-in page for administrators. This policy also requires the administrator to select an authentication realm (if more than one realm exists). The [*/admin](#) sign-in policy is configured to apply to the Admin Users authentication realm, therefore this sign-in policy applies to the administrator account you create through the serial console.

**Related
Documentation**

- [Defining a User Role on page 5](#)

CHAPTER 2

Introduction to Secure Access Service

- [Secure Access Service Solution Overview on page 16](#)
- [Securing Traffic with Secure Access Service on page 18](#)
- [Authenticating Users with Existing Servers on page 19](#)
- [Fine-Tuning Access to Secure Access Service and the Resources It Intermediates on page 20](#)
- [Creating a Seamless Integration Between Secure Access Service and the Resources It Intermediates on page 21](#)
- [Protecting Against Infected Computers and Other Security Concerns on page 21](#)
- [Ensuring Redundancy in the Secure Access Service Environment on page 22](#)
- [Making the Secure Access Service Interface Match My Company's Look-and-Feel on page 23](#)
- [Enabling Users on a Variety of Computers and Devices to Use Secure Access Service on page 23](#)
- [Providing Secure Access for My International Users on page 24](#)
- [Configuring Secure Access Service on page 24](#)
- [Network and Security Manager and the Secure Access Service on page 25](#)
- [Configuring Secure Access for the Initial DMI Connection on page 28](#)
- [Managing Large Binary Data Files on page 30](#)
- [Uploading and Linking Large Binary Data Files with NSM on page 30](#)
- [Importing Custom Sign-In Pages with NSM on page 31](#)
- [Importing Antivirus LiveUpdate Settings with NSM on page 32](#)
- [Importing Endpoint Security Assessment Plug-in \(ESAP\) Packages with NSM on page 33](#)
- [Uploading a Third-Party Host Checker Policy with NSM on page 34](#)
- [Linking to a Third-Party Host Checker Policy Shared Object with NSM on page 35](#)
- [Linking to a Secure Virtual Workspace Wallpaper Image Shared Object with NSM on page 35](#)
- [Importing Hosted Java Applets with NSM on page 36](#)
- [Importing a Custom Citrix Client .cab File with NSM on page 37](#)
- [Junos Pulse Overview on page 37](#)

- [Junos Pulse Configuration Overview on page 40](#)
- [Configuring a Role for Junos Pulse on page 41](#)
- [Pulse Connection Set Options for Pulse Secure Access Service on page 44](#)
- [Junos Pulse Connection Options on page 46](#)
- [Creating a Client Connection Set on page 51](#)
- [Configuring Connection Rules for Location Awareness on page 53](#)
- [Junos Pulse Component Set Options on page 55](#)
- [Creating a Client Component Set on page 56](#)
- [Junos Pulse Client Installation Overview on page 57](#)
- [Installing the Junos Pulse Client from the Web on page 58](#)
- [Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 59](#)
- [Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 63](#)
- [Junos Pulse Command-line Launcher on page 64](#)
- [Using jamCommand to Import Junos Pulse Connections on page 67](#)

Secure Access Service Solution Overview

The Juniper Networks Secure Access Service enable you to give employees, partners, and customers secure and controlled access to your corporate data and applications including file servers, Web servers, native messaging and e-mail clients, hosted servers, and more from outside your trusted network using just a Web browser.

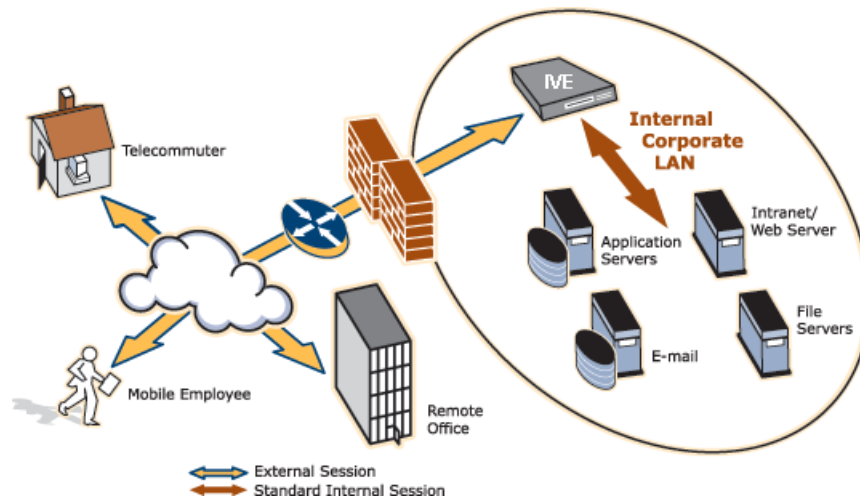
Secure Access Service provide robust security by intermediating the data that flows between external users and your company's internal resources. Users gain authenticated access to authorized resources through an extranet session hosted by the appliance. During intermediation, Secure Access Service receives secure requests from the external, authenticated users and then makes requests to the internal resources on behalf of those users. By intermediating content in this way, Secure Access Service eliminates the need to deploy extranet toolkits in a traditional DMZ or provision a remote access VPN for employees.

To access the intuitive Secure Access Service home page, your employees, partners, and customers need only a Web browser that supports SSL and an Internet connection. This page provides the window from which your users can securely browse Web or file servers, use HTML-enabled enterprise applications, start the client/server application proxy, begin a Windows, Citrix, or Telnet/SSH terminal session, access corporate e-mail servers, start a secured layer 3 tunnel, or schedule or attend a secure online meeting.



NOTE: These capabilities depend upon the Secure Access Service product and upgrade options you have purchased.

Figure 1: Secure Access Service Working within a LAN



You can configure Secure Access Service in the following ways:

- Provide users with secure access to a variety of resources. Secure Access Service intermediates access to multiple types of applications and resources such as Web-based enterprise applications, Java applications, file shares, terminal hosts, and other client/server applications such as Microsoft Outlook, Lotus Notes, the Citrix ICA Client, and pcAnywhere. Additionally, administrators can provision an access method that allows full Layer 3 connectivity, providing the same level of access that a user would get if they were on the corporate LAN.
- Fine-tune user access to the appliance, resource types, or individual resources based on factors such as group membership, source IP address, certificate attributes, and endpoint security status. For instance, you can use dual-factor authentication and client-side digital certificates to authenticate users to Secure Access Service and use LDAP group membership to authorize users to access individual applications.
- Assess the security status of your users' computers by checking for endpoint defense tools such as current antivirus software, firewalls, and security patches. You can then allow or deny users access to the appliance, resource types, or individual resources based on the computer's security status.

Secure Access Service acts as a secure, Application Layer gateway intermediating all requests between the public Internet and internal corporate resources. All requests that enter Secure Access Service are already encrypted by the end user's browser, using SSL/HTTPS 128-bit or 168-bit encryption—unencrypted requests are dropped. Because Secure Access Service provides a robust security layer between the public Internet and internal resources, administrators do not need to constantly manage security policies and patch security vulnerabilities for numerous different application and Web servers deployed in the public-facing DMZ.

Related Documentation

- [Securing Traffic with Secure Access Service on page 18](#)
- [Authenticating Users with Existing Servers on page 19](#)

- [Fine-Tuning Access to Secure Access Service and the Resources It Intermediates on page 20](#)
- [Creating a Seamless Integration Between Secure Access Service and the Resources It Intermediates on page 21](#)
- [Protecting Against Infected Computers and Other Security Concerns on page 21](#)
- [Ensuring Redundancy in the Secure Access Service Environment on page 22](#)
- [Making the Secure Access Service Interface Match My Company's Look-and-Feel on page 23](#)
- [Enabling Users on a Variety of Computers and Devices to Use Secure Access Service on page 23](#)
- [Providing Secure Access for My International Users on page 24](#)

Securing Traffic with Secure Access Service

Secure Access Service enables you to secure access to a wide variety of applications, servers, and other resources through its remote access mechanisms. Once you have chosen which resource you want to secure, you can then choose the appropriate access mechanism.

For instance, if you want to secure access to Microsoft Outlook, you can use the Secure Application Manager (SAM). The Secure Application Manager intermediates traffic to client/server applications including Microsoft Outlook, Lotus Notes, and Citrix. Or, if you want to secure access to your company Intranet, you can use the Web rewriting feature. This feature uses Secure Access Service's Content Intermediation Engine to intermediate traffic to Web-based applications and Web pages.

Secure Access Service includes remote access mechanisms that intermediate the following types of traffic:

- Web-based traffic, including Web pages and Web-based applications—Use the Web rewriting feature to intermediate this type of content. The Web rewriting feature includes templates that enable you to easily configure access to applications such as Citrix, OWA, Lotus iNotes, and Sharepoint. In addition, you can use the Web rewriting custom configuration option to intermediate traffic from a wide variety of additional Web-based applications and Web pages, including custom-built Web applications.
- Java applets, including Web applications that use Java applets—Use the hosted Java applets feature to intermediate this type of content. This feature enables you to host Java applets and the HTML pages that they reference directly on Secure Access Service rather than maintaining a separate Java server.
- File traffic, including file servers and directories—Use the file rewriting feature to intermediate and dynamically “webify” access to file shares. The file rewriting feature enables you to secure traffic to a variety of Windows and UNIX based servers, directories, and file shares.

- Client/server applications—Use the Secure Application Manager (SAM) feature to intermediate this type of content. SAM comes in two varieties (Windows and Java versions, or WSAM and JSAM). The WSAM and JSAM features include templates that enable you to easily configure access to applications such as Lotus Notes, Microsoft Outlook, NetBIOS file browsing, and Citrix. In addition, you can use the WSAM and JSAM custom configuration options to intermediate traffic from a wide variety of additional client/server applications and destination networks.
- Telnet and SSH terminal emulation sessions—Use the Telnet/SSH feature to intermediate this type of content. This feature enables you to easily configure access to a variety of networked devices that utilize terminal sessions including UNIX servers, networking devices, and other legacy applications.
- Windows Terminal Servers and Citrix server terminal emulation sessions— Use the Terminal Services feature to intermediate this type of content. This feature enables you to easily configure access to Windows Terminal Servers, Citrix MetaFrame Servers, and Citrix Presentation Servers (formerly known as Nfuse servers). You can also use this feature to deliver the terminal services clients directly from Secure Access Service, eliminating the need to use another Web server to host the clients.
- E-mail clients based on the IMAP4, POP3, and SMTP protocols—Use the email client feature to intermediate this type of content. This feature enables you to easily configure access to any corporate mail server based on the IMAP4, POP3, and SMTP protocols, such as Microsoft Exchange Server and Lotus Notes Mail servers.
- All network traffic—Use the VPN Tunneling feature to create a secure, Layer 3 tunnel over the SSL connection, allowing access to any type of application available on the corporate network. This feature enables you to easily connect remote users into your network by tunneling network traffic over port 443, enabling users full access to all of your network resources without configuring access to individual servers, applications, and resources.

**Related
Documentation**

- [Secure Access Service Solution Overview on page 16](#)

Authenticating Users with Existing Servers

You can easily configure Secure Access Service to use your company's existing servers to authenticate your end users—Users do not need to learn a new username and password to access the Secure Access Service device. Secure Access Service supports integration with LDAP, RADIUS, NIS, Windows NT Domain, Active Directory, eTrust SiteMinder, SAML, and RSA ACE/Servers.

Or, if you do not want to use one of these standard servers, you can store usernames and credentials directly on Secure Access Service and use Secure Access Service itself as an authentication server. In addition, you can choose to authenticate users based on attributes contained in authentication assertions generated by SAML authorities or client-side certificates. Or, if you do not want to require your users to sign into Secure Access Service, you can use the Secure Access Service anonymous authentication server, which allows users to access the Secure Access Service device without providing a username or password.

- Related Documentation**
- [Secure Access Service Solution Overview on page 16](#)
 - [About Authentication and Directory Servers on page 154](#)

Fine-Tuning Access to Secure Access Service and the Resources It Intermediates

In addition to using authentication servers to control access to Secure Access Service, you can control access to Secure Access Service and the resources it intermediates using a variety of additional client-side checks. Secure Access Service enables you to create a multilayered approach to protect Secure Access Service and your resources:

1. First, you can perform preauthentication checks that control user access to the Secure Access Service sign-in page. For instance, you might configure Secure Access Service to check whether or not the user's computer is running a particular version of Norton Antivirus. If it is not running, you can determine that the user's computer is unsecure and disable access to the Secure Access Service sign-in page until the user has updated the computer's antivirus software.
2. Once a user has successfully accessed the Secure Access Service sign-in page, you can perform realm-level checks to determine whether he can access the Secure Access Service end-user home page. The most common realm-level check is performed by an authentication server. (The server determines whether the user enters a valid username and password.) You can perform other types of realm-level checks, however, such as checking that the user's IP address is in your network or that the user is using the Web browser type that you specify.

If a user passes the realm-level checks that you specify, the user can access the Secure Access Service end-user home page. Otherwise, Secure Access Service does not enable the user to sign in, or Secure Access Service displays a "stripped down" version of the home page that you create. Generally, this stripped down version contains significantly less functionality than is available to your standard users because the user has not passed all of your authentication criteria. Secure Access Service provides extremely flexible policy definitions, enabling you to dynamically alter end-user resource access based on corporate security policies.

3. After Secure Access Service successfully assigns a user to a realm, the appliance maps the user to a role based on your selection criteria. A role specifies which access mechanisms a selected group of users can access. It also controls session and UI options for that group of users. You can use a wide variety of criteria to map users to roles. For instance, you can map users to different roles based on endpoint security checks or on attributes obtained from an LDAP server or client-side certificate.
4. In most cases, a user's role assignments control which individual resources the user can access. For instance, you might configure access to your company's Intranet page using a Web resource profile and then specify that all members of the Employees role can access that resource.

However, you can choose to further fine-tune access to individual resources. For instance, you may enable members of the Employees role to access your company's Intranet (as described earlier), but add a resource policy detailed rule that requires users to meet additional criteria to access the resource. For example, you may require users to be

members of the Employees role and to sign into Secure Access Service during business hours to access your company Intranet.

- Related Documentation**
- [Secure Access Service Solution Overview on page 16](#)
 - [Access Management Overview on page 71](#)

Creating a Seamless Integration Between Secure Access Service and the Resources It Intermediates

In a typical Secure Access Service configuration, you could add bookmarks directly to the Secure Access Service end-user home page. These bookmarks are links to the resources that you configure Secure Access Service to intermediate. Adding these bookmarks enables users to sign into a single place (Secure Access Service) and find a consolidated list of all of the resources available to them.

Within this typical configuration, you can streamline the integration between Secure Access Service and the intermediated resources by enabling single sign-on (SSO). SSO is a process that allows preauthenticated Secure Access Service users to access other applications or resources that are protected by another access management system without having to re-enter their credentials. During Secure Access Service configuration, you can enable SSO by specifying user credentials that you want the Secure Access Service to pass to the intermediated resources.

Or, if you do not want to centralize user resources on the Secure Access Service end-user home page, you could create links to the Secure Access Service-intermediated resources from another Web page. For instance, you can configure bookmarks on Secure Access Service, and then add links to those bookmarks from your company's Intranet. Your users can then sign into your company Intranet and click the links there to access the intermediated resources without going through the Secure Access Service home page. As with standard Secure Access Service bookmarks, you can enable SSO for these external links.

- Related Documentation**
- [Secure Access Service Solution Overview on page 16](#)
 - [About Single Sign-On on page 335](#)

Protecting Against Infected Computers and Other Security Concerns

Secure Access Service enables you to protect against viruses, attacks, and other security concerns using the Host Checker feature. Host Checker performs security checks on the clients that connect to Secure Access Service. For instance, you can use Host Checker to verify that end-user systems contain up-to-date antivirus software, firewalls, critical software hotfixes, and other applications that protect your users' computers. You can then enable or deny users access to the Secure Access Service sign-in pages, realms, roles, and resources based on the results that Host Checker returns. Or, you can display remediation instructions to users so they can bring their computers into compliance

You can also use Host Checker to create a protected workspace on clients running Windows 2000 or Windows XP. Through Host Checker, you can enable the Secure Virtual Workspace (SVW) feature to create a protected workspace on the client desktop, ensuring that any end user signing in to your intranet must perform all interactions within a completely protected environment. Secure Virtual Workspace encrypts information that applications write to disk or the registry and then destroys all information pertaining to itself or Secure Access Service session when the session is complete.

You can also secure your network from hostile outside intrusion by integrating your Secure Access Service with a Juniper Networks Intrusion Detection and Prevention (IDP) sensor. You can use IDP devices to detect and block most network worms based on software vulnerabilities, non-file-based Trojan horses, the effects of Spyware, Adware, and Key Loggers, many types of malware, and zero day attacks through the use of anomaly detection.

**Related
Documentation**

- [Secure Access Service Solution Overview on page 16](#)
- [Configuring the Secure Access Service to Interoperate with IDP on page 1083](#)

Ensuring Redundancy in the Secure Access Service Environment

You can ensure redundancy in your Secure Access Service environment using the clustering feature. With this feature, you can deploy two or more appliances as a cluster, ensuring no user downtime in the rare event of failure and stateful peering that synchronizes user settings, system settings, and user session data.

These appliances support active/passive or active/active configurations across a LAN. In Active/Passive mode, one Secure Access Service device actively serves user requests while the other Secure Access Service device runs passively in the background to synchronize state data. If the active Secure Access Service device goes offline, the passive Secure Access Service device automatically starts servicing user requests. In active/active mode, all the machines in the cluster actively handle user requests sent by an external load balancer. The load balancer hosts the cluster VIP and routes user requests to Secure Access Service defined in its cluster group based on source-IP routing. If a Secure Access Service device goes offline, the load balancer adjusts the load on the other active Secure Access Service device.



NOTE: WAN clustering is not supported on the MAG Series Junos Pulse Gateways, except as it relates to campus networks. In a well-connected campus network, where the connectivity is more LAN-like than WAN-like, the Junos Pulse Gateways can be clustered in separate buildings.

**Related
Documentation**

- [Secure Access Service Solution Overview on page 16](#)

Making the Secure Access Service Interface Match My Company's Look-and-Feel

Secure Access Service enables you to customize a variety of elements in the end-user interface. Using these customization features, you can update the look-and-feel of the Secure Access Service end-user console so it will resemble one of your standard company Web pages or applications.

For instance, you can easily customize the headers, background colors, and logos that Secure Access Service displays in the sign-in page and end-user console to match your company's style. You can also easily customize the order in which Secure Access Service displays bookmarks and the help system that Secure Access Service displays to users.

Or, if you do not want to display the Secure Access Service end-user home page to users (either in standard or customized form), you can choose to redirect users to a different page (such as your company Intranet) when users first sign into the Secure Access Service console. If you choose to use this option, you may want to add links to your Secure Access Service bookmarks on the new page.

If you want to further customize the Secure Access Service sign-in page, you can use the Secure Access Service's custom sign-in pages feature. Unlike the standard customization options that you can configure through the Secure Access Service admin console, the custom sign-in pages feature does not limit the number of customizations you can make to your pages. Using this feature, you can use an HTML editor to develop a sign-in page that exactly matches your specifications.

Related Documentation

- [Secure Access Service Solution Overview on page 16](#)
- [Creating a Seamless Integration Between Secure Access Service and the Resources It Intermediates on page 21](#)
- [Customizable Admin and End-User UIs on page 1103](#)

Enabling Users on a Variety of Computers and Devices to Use Secure Access Service

In addition to allowing users to access Secure Access Service from standard workstations and kiosks running Windows, Macintosh, and Linux operating systems, end users can access Secure Access Service from connected PDAs, handhelds and smart phones such as i-mode and Pocket PC. When a user connects from a PDA or handheld device, Secure Access Service determines which pages and functionality to display based on settings that you configure.

For more information about specifying which pages Secure Access Service displays to different devices, see the Secure Access Service supported platforms document available on the Juniper Networks Customer Support Center website.

Related Documentation

- [Secure Access Service Solution Overview on page 16](#)
- [Handheld Devices and PDAs on page 1165](#)

Providing Secure Access for My International Users

Secure Access Service supports English (US), French, German, Spanish, Simplified Chinese, Traditional Chinese, Japanese, and Korean. When your users sign into Secure Access Service, Secure Access Service automatically detects the correct language to display based on the user's Web browser setting. Or, you can use end-user localization and custom sign-in pages options to manually specify the language that you want to display to your end users.

Related Documentation

- [Secure Access Service Solution Overview on page 16](#)
- [About Multi-Language Support for the Secure Access Service on page 1161](#)

Configuring Secure Access Service

To enable users to start using Secure Access Service, you must complete the following basic steps:

1. Plug in the appliance, connect it to your network, and configure its initial system and network settings.
2. After you connect the Secure Access Service device to your network, you need to set the system date and time, upgrade to the latest service package, and install your product licenses. When you first sign into the admin console, Secure Access Service displays an initial configuration task guide that quickly walks you through this process.
3. After you install your product licenses, you need to set up your access management framework to enable your users to authenticate and access resources. Configuration steps include:
 - a. Define an authentication server that verifies the names and passwords of your users.
 - b. Create user roles that enable access mechanisms, session options, and UI options for user groups.
 - c. Create a user authentication realm that specifies the conditions that users must meet to sign into Secure Access Service.
 - d. Define a sign-in policy that specifies the URL that users must access to sign into Secure Access Service and the page that they see when they sign in.
 - e. Create resource profiles that control access to resources, specify which user roles can access them, and include bookmarks that link to the resources.

Secure Access Service includes a task guide in its admin console that quickly walks you through this process. To access this task guide, click the Guidance link located in the upper right corner of the admin console. Then, under Recommended Task Guides, select Base Configuration.

Once you have completed these basic steps, your Secure Access Service is ready for use. You can start using it as is, or configure additional advanced features such as endpoint defense and clustering.

- Related Documentation**
- [Creating a Test Scenario to Learn Secure Access Service Concepts and Best Practices on page 4](#)

Network and Security Manager and the Secure Access Service

Network and Security Manager (NSM) is Juniper Networks network management tool that allows distributed administration of network appliances. You can use the NSM application to centralize status monitoring, logging, and reporting, and to administer Secure Access Service configurations.

With NSM you can manage most of the parameters that you can configure through the Secure Access Service admin console. The configuration screens rendered through NSM are similar to the Secure Access Service's native interface.

NSM incorporates a broad configuration management framework that allows co-management using other methods. You can import and export XML via the Secure Access Service admin console interface, or you can manage from the Secure Access Service admin console.

How Secure Access Service and NSM communicate

Secure Access Service and the NSM application communicate through the Device Management Interface (DMI). DMI is a collection of schema-driven protocols that run on a common transport (TCP). DMI is designed to work with Juniper Networks platforms to make device management consistent across all administrative realms. The DMI protocols that are supported include NetConf (for inventory management, XML-based configuration, text-based configuration, alarm monitoring, and device specific commands), structured syslog, and threat flow for network profiling. DMI supports third-party network management systems that incorporate the DMI standard, however only one DMI-based agent per device is supported.

Secure Access Service's configuration is represented as a hierarchical tree of configuration items. This structure is expressed in XML that can be manipulated with NetConf. NetConf is a network management protocol that uses XML. DMI uses NetConf's generic configuration management capability and applies it to allow remote configuration of the device.

To allow NSM to manage Secure Access Service using the DMI protocol, NSM must import the schema and meta-data files from the Juniper Schema Repository, a publicly-accessible resource that is updated with each device release. In addition to downloading Secure Access Service's current schema, NSM may also download upgraded software.

The Schema Repository enables access to XSD and XML files defined for each device, model and software version.

Before attempting to communicate with NSM, you must first complete the initial configuration of Secure Access Service. Initial configuration includes network interface settings, DNS settings, licensing, and password administration.

If you have several Secure Access Service devices that will be configured in a clustering environment, the cluster abstraction must first be created in the NSM Cluster Manager. Then, you can add individual nodes. NSM cannot auto-detect cluster membership.

After you have completed the initial network configuration, you can configure Secure Access Service to communicate with NSM using the appropriate network information. Once Secure Access Service has been configured to communicate with NSM, Secure Access Service contacts NSM and establishes a DMI session through an initial TCP handshake.

All communications between Secure Access Service and NSM occur over SSH to ensure data integrity.

After Secure Access Service initially contacts NSM and a TCP session is established, interaction between Secure Access Service and NSM is driven from NSM, which issues commands to get hardware, software, and license details of Secure Access Service. NSM connects to the Schema Repository to download the configuration schema that is particular to Secure Access Service.

NSM then issues a command to retrieve configuration information from Secure Access Service. If NSM is contacted by more than one Secure Access Service device as a member of a cluster, information from only one of the cluster devices is gathered. NSM attempts to validate the configuration received from Secure Access Service against the schema from Juniper Networks.

Once Secure Access Service and NSM are communicating, Secure Access Service delivers syslog and event information to NSM.

After NSM and Secure Access Service are connected, you can make any configuration changes directly on Secure Access Service, bypassing NSM. NSM automatically detects these changes and imports the new configuration data. Changes to Secure Access Service cluster members will similarly be detected by NSM.

When you make changes to the Secure Access Service configuration through NSM you must push the changes to the device by performing an Update Device operation.

When you double-click the Secure Access Service icon in the Device Manager and select the Config tab, the configuration tree appears in the main display area in the same orientation as items appears on the Secure Access Service interface.

Available Services and Configuration Options

The following services and options are provided to NSM by Secure Access Service:

- **Inventory management service**—inventory management service enables management of Secure Access Service software, hardware, and licensing details. Adding or deleting licenses is not supported, however upgrading/downgrading software is supported.
- **Status monitoring service**—status monitoring service allows Secure Access Service status to be obtained, including name, domain, OS version, synchronization status, connection details, and current alarms.
- **Logging service**—logging service allow Secure Access Service logs to be obtained in a time-generated order. Logging configuration details that are set on Secure Access Service will apply to NSM.
- **XML-based configuration management service**—configuration management service enables NSM to manage the configuration of Secure Access Service. NSM uses the same XML Schema as Secure Access Service, so you can troubleshoot NSM using XML files downloaded from Secure Access Service.

The following device configuration items are not supported:

- Editing licensing information, (though licenses can be viewed)
- Creating clusters, joining nodes to clusters, or enabling or disabling cluster nodes
- Packaging log files or debug files for remote analysis
- Rebooting Secure Access Service

DMI Communication with the Secure Access Service

To configure the Secure Access Service to communicate with NSM you must coordinate actions between the Secure Access Service and NSM administrators. Items such as IP address, password, HMAC key (a one-time password), and the device ID must be shared between administrators of both the Secure Access device and NSM.

To connect the Secure Access Service and NSM you will need to do the following:

- Install and configure the Secure Access Service.
- Add the Secure Access Service as a device in NSM.
- Configure and activate the DMI agent on the Secure Access Service.
- Confirm connectivity and import the Secure Access Service configuration into NSM.

Related Documentation

- [Configuring Secure Access for the Initial DMI Connection on page 28](#)
- [Managing Large Binary Data Files on page 30](#)
- [Uploading and Linking Large Binary Data Files with NSM on page 30](#)

Configuring Secure Access for the Initial DMI Connection

To permit Secure Access and NSM to make an initial connection, you must add an NSM administrative user to the Secure Access configuration. This topic provides a summary of adding the NSM administrator and configuring the DMI agent to allow the Secure Access device and NSM to communicate. Complete configuration of the Secure Access device for authenticating users is outside the scope of this topic.

To initiate a DMI session for communication between Secure Access and NSM:

1. Ensure that basic connection information is configured on the Secure Access device (network address, DNS, password).
2. Ensure that the proper licenses are installed on the Secure Access device.
3. From the NSM UI client Device Manager, click the Add icon and select Device to open the Add Device wizard, and enter the applicable information required to add a Secure Access device to NSM. See the [Administration Guide](#).



NOTE: You must enter a unique NSM admin username and password on the NSM UI client. This username will be used on the Secure Access device as the username for the administrator account that will be used to manage the Secure Access device. NSM must have a unique account login to avoid interrupting the communication with Secure Access. NSM automatically generates a unique ID which is used for the HMAC key.

4. From the Secure Access admin console, select **Authentication > Auth. servers** and enter the username and password of the NSM admin using the credentials you entered on NSM in the applicable authentication server. Use the NSM username and password that you entered in the NSM UI Client.



NOTE: Only password-based authentication servers can be used. One-time password authentication is not supported.

5. Select **Administrators > Admin Roles** and create a DMI agent administrator role.
6. Select **Administrators > Admin Realms** and create a new DMI agent admin realm for the DMI agent on the Secure Access device and use role mapping to associate the DMI agent role and realm.
7. On the NSM interface, select the Domain menu and choose the domain to which the Secure Access device will be added.
8. In Device Manager, click the Add icon and select Device to open the Add Device wizard, and enter the applicable information required to add a Secure Access device to NSM. See the [Administration Guide](#).

**NOTE:**

- In a clustering environment, each cluster-node must have its own unique DMI agent and its own device-id and HMAC key, as each cluster node maintains its own persistent DMI connection to the management application.
- The HMAC key and the device id are hashed to identify individual devices to the application. Juniper recommends that you use a strong password for the HMAC key value to ensure that the key isn't guessed.

9. After you have added the Secure Access device to NSM, select **System > Configuration > DMI Agent** on the Secure Access admin console.
10. Under DMI connection, select the:
 - **Inbound Enabled** check box if you are using an SSH secure shell Command Line Interface (CLI) to manage the Secure Access device. The Secure Access device can also be managed by integrating an SSH-aware netconf that complies with Juniper Network's DMI specification.
 - **Outbound Enabled** check box if you are configuring the Secure Access device to communicate with NSM.



NOTE: When you enable or disable a connection, it takes a few minutes for the connection state to be updated.

11. Under DMI settings for inbound connections, enter the TCP port in which the Secure Access device should accept connections. This TCP port should not be used by any other Secure Access processes. We recommend you use the default port or a port number larger than 1024.
12. Under DMI settings for outbound connection, enter the NSM Primary Server IP address or hostname, Primary Port, Backup Server and Backup Port (if applicable), the Device ID, and the HMAC Key.
13. Select the Admin realm that you have configured for the DMI agent.
14. If you do not want DMI logging for both inbound and outbound DMI connections, uncheck the **DMI Logging** checkbox. By default, DMI logging is enabled.

The Secure Access device initiates a TCP connection to NSM. After the Secure Access device is identified to NSM through the HMAC key and device ID hash, the Secure Access device and NSM negotiate an SSH tunnel, and NSM requests authentication to the Secure Access device based on the username and password.

If you need to disconnect the device from NSM, you can either disable the DMI agent from the device, or you can delete the device from the NSM interface. If the DMI connection is later reestablished, NSM will automatically retrieve any configuration changes, as well as logs that have accumulated in the interim.

To add a Secure Access cluster in NSM, you first add the cluster, then you add each member. Adding a member is similar to adding a standalone Secure Access device. You must have a cluster object and all of the cluster members defined in NSM to allow NSM to access the cluster.

Managing Large Binary Data Files

Large binary data files that form a part of the configuration of the Secure Access Service are handled differently from the remainder of the configuration in NSM. The size of some of these binary files could cause configurations to be so large as to overload resources on the NSM server. Consequently, only the large binary files you specify get imported into NSM, and those files are configured as shared objects, which avoids duplication if applied to multiple devices.

With NSM, large binary data files are not imported with the rest of the configuration during a normal device import operation. Instead, the file is represented in the device configuration tree by a stub containing an MD5 hash and file length designation. If you need to manage such a file in NSM, you upload the file separately, and configure it as a shared object. To include the file as part of the device object in NSM, you must then establish a link between the node in the device configuration tree and the shared binary data object. When you establish the link, a pointer to the shared binary data object replaces the MD5 hash and length.

After you establish the link, an Update Device directive pushes all linked binary data files to the device along with the rest of the device configuration. No binary data is pushed for nodes that still contain the MD5 hash and length designators.

If you do not need to manage a large binary data file from NSM, then you do not need to include it in the device object configuration. For example, suppose you have a hosted Java applet that resides on a Secure Access Service, and you have no intention of updating this applet. In this case, no shared object creation or file upload is necessary. NSM device objects will contain only the MD5 hash stub for these endpoints. Any delta configuration operation between NSM and the device will indicate identical configurations because the MD5 hash in NSM will match the file on the device. For the same reasons, an Update Device directive will have no effect on the device.

Related Documentation

- [Uploading and Linking Large Binary Data Files with NSM on page 30](#)

Uploading and Linking Large Binary Data Files with NSM

This topic describes the complete procedure for downloading a large binary data file and linking that file into the Secure Access Service configuration tree.

To upload and link a large binary data file:

1. In the Device Manager, right-click the device icon and select Import Device from the list to Import the Secure Access Service configuration.

When the import job is finished, the device object configuration contains the MD5 stubs for each of the large binary data files.

2. Upload each required large binary data file onto the NSM client workstation.

You'll need to get some files from the Secure Access Service. Other files, such as ESAP configuration files, should be downloaded from the site of origin. Use the device Web UI to upload binary files from the Secure Access Service.

3. To create a shared object in the NSM Object Manager for the binary file:

- a. In the Configure panel of the NSM navigation tree, select **Object Manager > Binary data**, and then click the Add icon.

- b. In the Binary Data dialog box, enter a name for the object, select a color for the object icon, add a comment if desired, and select the file you uploaded in step 2. Click OK.

4. Link the shared object to the corresponding node in the device configuration tree:

- a. In the Device Manager, double-click the Secure Access Service to open the device editor, and then select the Configuration tab.

- b. Navigate to the node in the configuration where you want to load the binary file.

For example, to load an ESAP package, expand Authentication and then select Endpoint Security. In the Host Checker tab, select Endpoint Security Assessment Plug-Ins, and then click the Add icon.

- c. Select the shared object.

To continue the ESAP example, in the New Endpoint Security Assessment Plug-Ins dialog box, enter a version number, select a shared binary data object from the Path to Package list. This list includes all shared binary data objects. Click OK.

If the object you want is not in the list, you can add it to the shared binary data list by clicking the Add icon. The Binary Data dialog box appears as in step 3.

- d. Click OK to save the newly configured links.

Related Documentation • [Managing Large Binary Data Files on page 30](#)

Importing Custom Sign-In Pages with NSM

The customized sign-in pages feature is a licensed feature that enables you to use your own access pages rather than having to modify the sign-in page included with the Secure Access Service.

To create a link from a Secure Access Service configuration tree to a shared object containing a custom sign-in access page:

1. In the Device Manager, double-click the Secure Access Service to open the device editor, and then select the Configuration tab.
2. Expand Authentication.
3. Expand Signing-In.
4. Expand Sign-in Pages.
5. Select Users/Administrator Sign-in Pages, and then click the Add icon in the right pane.
6. Enter a name for the access page.
7. Select Custom Sign-in Pages.
8. Select a shared binary data object from the Custom Pages Zip File list.
9. Click OK once to save the link, and again to save the configuration.

To create a link from a Secure Access Service configuration tree to a shared object containing a custom sign-in meeting page:

1. In the Device Manager, double-click the Secure Access Service to open the device editor, and then select the Configuration tab.
2. Expand Authentication.
3. Expand Signing-In.
4. Expand Sign-in Pages.
5. Select Meeting Sign-in Pages, and then click the Add icon in the right pane.
6. Enter a name for the sign-in meeting page.
7. Select Custom Sign-in Page.
8. Select a shared binary data object from the Blob list.
9. Click OK once to save the link, and again to save the configuration.

**Related
Documentation**

- [Configuring Sign-In Pages on page 333](#)

Importing Antivirus LiveUpdate Settings with NSM

Retrieve the latest AV liveupdate file from the Juniper Downloads Web site at https://download.juniper.net/software/av/uac/epupdate_hist.xml.

Retrieve the latest patch file from the Juniper Download Web site at <https://download.juniper.net/software/hc/patchdata/patchupdate.dat>.

To create a link from a Secure Access Service configuration tree to a shared object containing an antivirus (AV) liveupdate file:

1. In the Device Manager, double-click the Secure Access Service to open the device editor, and then select the Configuration tab.
2. Expand Authentication.
3. Select Endpoint Security.
4. From the Host Checker tab, select Live Update Settings.
5. Select a shared binary data object from the Manually import virus signature list.
6. Click OK to save the configuration.

To create a link from a Secure Access Service configuration tree to a shared object containing an AV patch liveupdate file:

1. In the Device Manager, double-click the Secure Access Service to open the device editor, and then select the Configuration tab.
2. Expand Authentication.
3. Select Endpoint Security.
4. From the Host Checker tab, select Live Update Settings.
5. Select a shared binary data object from the Manually import patch management data list.
6. Click OK to save the configuration.

Related Documentation

- [Uploading a Third-Party Host Checker Policy with NSM on page 34](#)
- [Host Checker and Trusted Network Computing on page 374](#)

Importing Endpoint Security Assessment Plug-in (ESAP) Packages with NSM

The Endpoint Security Assessment Plug-in (ESAP) on the Secure Access Service checks third-party applications on endpoints for compliance with the predefined rules you configure in a Host Checker policy.

To download the Endpoint Security Assessment Plug-in from the Juniper Networks Customer Support Center to your NSM client computer:

1. Open the following page:
<http://www.juniper.net/support/products/esap/>
2. Click the Software tab.
3. Navigate to the ESAP release you want and click the link to download the package file to your computer.

To create a link from a Secure Access Service configuration tree to a shared object containing an ESAP package:

1. In the Device Manager, double-click the Secure Access Service to open the device editor, and then select the Configuration tab.
2. Expand Authentication.
3. Select Endpoint Security.
4. From the Host Checker tab, select Endpoint Security Assessment Plug-Ins, and then click the Add icon.
5. In the New Endpoint Security Assessment Plug-Ins dialog box, enter an ESAP version number.
6. Select a shared binary object from the Path to Package list.
7. Click OK once to save the link, and again to save the configuration.

Uploading a Third-Party Host Checker Policy with NSM

For the device to recognize a package definition file, you must:

1. Name the package definition file **MANIFEST.HCIF** and include it in a folder named **META-INF**.
2. Create a Host Checker policy package by creating a zip archive. The archive should include the META-INF folder that contains the MANIFEST.HCIF file along with the interface DLL and any initialization files.

For example, a Host Checker policy package might contain:

- META-INF/MANIFEST.HCIF
 - hcif-myPestPatrol.dll
 - hcif-myPestPatrol.ini
3. Upload the Host Checker package (or packages) to the NSM shared object. You can upload multiple policy packages to NSM shared objects, each containing a different MANIFEST.HCIF file.



NOTE: After you upload a Host Checker policy package to the NSM shared object, you cannot modify the package contents. Instead, you must modify the package on your local system and then upload the modified version to NSM.

4. Implement the policy at the realm, role, or resource policy levels using the options.

If you want to verify that the package itself is installed and running on the client computer (as opposed to a specific policy in the package passing or failing) you can use the name you specified when you uploaded the policy package (for example, myPestPatrol). To enforce a particular policy in the package, use the syntax

package-name.policy-name. For example, to enforce the FileCheck policy in the myPestPatrol package, use myPestPatrol.FileCheck.

- Related Documentation**
- [Host Checker and Trusted Network Computing on page 374](#)

Linking to a Third-Party Host Checker Policy Shared Object with NSM

To create a link from a Secure Access Service configuration tree to a shared object containing a third-party host checker policy:

1. In the Device Manager, double-click the Secure Access Service to open the device editor, and then select the Configuration tab.
2. Expand Authentication.
3. Select Endpoint Security.
4. From the Host Checker tab, select the Settings tab, and then click the Add icon in the Policies box.
5. From the Policy type list, select 3rd Party Policy.
6. Give the policy a name.
7. Select a shared binary data object from the Package list.
8. Click OK to save the configuration.

- Related Documentation**
- [Host Checker and Trusted Network Computing on page 374](#)

Linking to a Secure Virtual Workspace Wallpaper Image Shared Object with NSM

To create a link from a Secure Access Service configuration tree to a shared object containing a secure virtual workspace wallpaper image:

1. In the Device Manager, double-click the Secure Access Service to open the device editor, and then select the Configuration tab.
2. Expand Authentication.
3. Select Endpoint Security.
4. From the Host Checker tab, select the Settings tab, and then click the Add icon in the Policies box.
5. From the Policy type list, select Secure Virtual Workspace Policy.
6. Select the Options tab.
7. Select a shared binary data object from the Desktop wallpaper image list.
8. Click OK to save the configuration.

- Related Documentation**
- [Enabling the Secure Virtual Workspace on page 437](#)

Importing Hosted Java Applets with NSM

You can store Java applets of your choice as shared objects in NSM without using a separate Web server to host them. You can then use these applets to intermediate traffic to various types of applications through the Secure Access Service. For example, you can upload the 3270 applet, 5250 applet, or Citrix Java applet to shared NSM objects. These applets enable users to establish sessions to IBM mainframes, AS/400s, and Citrix MetaFrame servers through terminal emulators. To enable the Citrix Java ICA client through the Secure Access Service session, you must upload multiple Citrix .jar and .cab files or configure a Citrix Terminal Services resource profile to host the Java applets.

You can upload individual .jar and .cab files or .zip, .cab, or .tar archive files to NSM shared objects. Archive files can contain Java applets and files referenced by the applets. Within the .zip, .cab, or .tar file, the Java applet must reside at the top level of the archive.

To ensure compatibility with both Sun and Microsoft Java Virtual Machines (JVMs), you must upload both .jar and .cab files. The Sun JVM uses .jar files, whereas the Microsoft JVM uses .cab files.



NOTE: When you upload Java applets to NSM, NSM asks you to read a legal agreement before it finishes installing the applets. Please read this agreement carefully. It obligates you to take full responsibility for the legality, operation, and support of the Java applets that you upload.

Uploading Java applets requires signed ActiveX or signed Java applets to be enabled within the browser to download, install, and launch the client applications.

To create a link from a Secure Access Service configuration tree to a shared object containing a Java applet:

1. In the Device Manager, double-click the Secure Access Service to open the device editor, and then select the Configuration tab.
2. Expand Users.
3. Expand Resource Profiles.
4. Select Hosted Java Applets, and then click the Add icon in the right pane.
5. Give the applet and file each a name.
6. Select a shared binary data object from the Applet file to be uploaded list.
7. Click OK once to save the link, and then again to save the configuration.

- Related Documentation**
- [About Hosted Java Applet Templates on page 453](#)
 - [Task Summary: Hosting Java Applets on page 454](#)

Importing a Custom Citrix Client .cab File with NSM

The custom Citrix client file enables you to provision the Citrix client from the Secure Access Service instead of requiring that it be pre-installed on end-user machines or downloaded from some other web server.

To create a link from the Secure Access Service configuration tree to a shared object containing a Custom Citrix .cab file:

1. In the Device Manager, double-click the Secure Access Service to open the device editor, and then select the Configuration tab.
2. Expand Users.
3. Select User Roles.
4. Select the Global Role Options tab.
5. In the Global Terminal Services Role Options tab, select a shared binary data object from the Citrix Client CAB File list.
6. Click OK to save the configuration.

Related Documentation

- [Configuring a Citrix XenDesktop Resource Policy on page 138](#)
- [Creating Resource Profiles Using Citrix Web Applications on page 471](#)

Junos Pulse Overview

Junos[®] Pulse is an extensible multi service network client that supports integrated connectivity, location-aware network access, application acceleration, security, and selected third-party services. Junos Pulse simplifies the user experience by letting the network administrator configure, deploy, and control the Pulse client software on OS X and Windows and the Pulse connection configurations that reside on the endpoint.

Junos Pulse comprises client and server software. The client enables secure authenticated network connections to protected resources and services over local and wide area networks. The Junos Pulse client software can connect with the Junos Pulse Secure Access Service to provide remote access to enterprise and service provider networks. Pulse can provide application acceleration features when implemented with Junos Pulse Application Acceleration Service. Pulse also delivers secure, identity-enabled NAC for LAN-based network and application access when deployed with Junos Pulse Access Control Service. Pulse integrates third-party endpoint security applications such as anti spyware, anti malware, and patch management applications. Pulse also integrates with Junos Pulse Collaboration Suite for online meeting services.

Users of mobile devices (smartphones) can install the Pulse mobile device app from the respective app stores for secure connectivity to Junos Pulse Secure Access Service. Mobile device users can also enable an optional security component, the Junos Pulse Mobile Security Suite.

Session Migration

One of the primary benefits of Junos Pulse is that users can log in once through a device on the network, and then to access additional devices without needing reauthentication.

Using Junos Pulse, you can permit users to migrate from location to location without having the need for reauthentication. For example, a user can connect from home through the Secure Access Service, and then arrive at work and connect through an IC Series device without having to log in again. Session migration also enables users to access different resources within the network that are protected by Juniper Networks devices without repeatedly providing credentials. IF-MAP Federation is required to enable session migration for users.

Location Awareness

The location awareness feature enables you to define connections that are activated automatically based on the location of the endpoint. Pulse determines the location of the endpoint by evaluating *location awareness rules* that you define. Location awareness rules are based on the client's IP address and interface. For example, you can define rules to enable Junos Pulse to automatically establish a secure tunnel to the corporate network through a Secure Access Service only when the user is at home, and to establish a UAC connection when the user is connected to the corporate network over the LAN. You configure the location awareness feature by defining location awareness rules for individual connections.

Location awareness rules are available for connections that are defined on the access device and then distributed to endpoints. A user cannot configure the location awareness feature by manually creating a connection on the Junos Pulse client.



NOTE: Location awareness does not work when split tunneling is disabled.

Security Certificates on Junos Pulse

Users cannot add CA servers or manage the server list. Pulse handles certificates similar to how a browser handles certificates. If the Pulse dynamic certificate trust option is enabled for a connection, the user can accept or deny the certificate that is presented if it is one that is not from a certificate authority that is defined in the endpoint's certificate store.

An 802.1X connection enables on further layer of certificate verification. When you define an 802.1X connection on the access device, you can specify server certificate distinguished names for each CA.



NOTE: Certificate-based authentication may fail from a Windows mobile device if both expired and valid certificates with the same common name (CN) are present on the device.

User Experience

From the user perspective, Junos Pulse presents a clean, uncomplicated interface. The user can enter credentials, select a realm, save settings, and accept or reject the server certificate. When you configure the client, you can specify whether or not to permit end users to modify settings, such as to add connections.

The client displays the connection status until the connection is made. If a connection fails as a result of the endpoint failing a Host Checker policy, Host Checker reason strings and remediation options appear.

Secure Access Service Gateway Deployment Options

On the network side, the Junos Pulse configuration is integrated into the admin console of supported gateways. On the Secure Access Service, you can deploy all of the connections and components required for clients to connect to any supported gateway. Secure Access Service supports the following deployment options:

Junos Pulse Access Control Service and Pulse Secure Access Service support the following deployment options:

- **Web install**—Create all of the settings that a Windows or Mac OS X endpoint needs for connectivity and services, and install the software on endpoints that connect to the Pulse server's Web portal. Pulse servers include a default client connection set and client component set. The default settings enable you to deploy Junos Pulse to users without creating new connection sets or component sets. The default settings for the client permit dynamic connections and install only the components required for the connection.
- **Default installer**—A default Junos Pulse installer package (in .msi format for Windows and .dmg for Mac OS X) is included in the Pulse server software. You can distribute this default installer to endpoints, run it, and then let users create their own connections or have users browse to the Pulse server and authenticate through the server's Web portal to receive the initial configuration and bind the client to the server for future configuration updates. Users can automatically install connections to other Pulse servers (if the Pulse client's configuration allows dynamic connections) by browsing to the user Web portal of a Pulse server where a dynamic connection has been made available. A dynamic connection is a predefined set of connection parameters that enables a client to connect to the host server. If the user is able to log in to the Pulse server's user Web portal, the connection parameters are downloaded and installed on the Junos Pulse client. Dynamic connections are created as manual rather than automatic connections, which means that they are run only when the user initiates the connection or the user browses to a Pulse Server and launches Pulse from the server's Web interface.
- **Preconfigured installer**—Create the connections that an endpoint needs for connectivity and services, download the settings file (.jnprpreconfig), and download default Pulse installation program. For Windows endpoints you run the Pulse installation program by using an msixec command with the settings file as an option. For OS X endpoints, you run the default installer and then import the .jnprpreconfig file using a separate command.



NOTE: Junos Pulse for mobile devices uses a different deployment model than Pulse for Windows and Pulse for Mac endpoints.

Platform Support

The following Juniper Networks devices support Junos Pulse:

- Unified Access Control 4.0 or later
- Secure Access Service 7.0 or later
- App Acceleration Series JWOS 6.1 or later
- SRX Series 9.5 or later

For detailed information about supported platforms and installation requirements, see the *Junos Pulse Supported Platforms Guide*, which is available at <http://www.juniper.net/support/products/pulse>.



NOTE: The Junos Pulse for Windows client is not compatible with the Instant Virtual System (IVS) feature of Secure Access Service. In an IVS system, a Pulse client always takes its IP address from the root Secure Access Service address pool instead of using the pool defined for the virtualized Secure Access Service.

Related Documentation

- [Junos Pulse Configuration Overview on page 40](#)
- [Junos Pulse Connection Options on page 46](#)
- [Creating a Client Connection Set on page 51](#)
- [Configuring a Role for Junos Pulse on page 41](#)

Junos Pulse Configuration Overview

Configure the Secure Access Service and the Junos Pulse settings on the gateway so that when users request authentication, they are assigned a role based on the role mappings and optional security profile that you create. Access to specific resources is permitted only for users and devices that provide the proper credentials for the realm, that are associated with the appropriate roles, and whose endpoints meet security restrictions. If a user attempts to connect to the network from an endpoint that does not comply with the security restrictions you have defined, the user cannot access the realm or role.

As you plan your Pulse configuration, be sure you know how you want to deploy Junos Pulse. You can use one or more of the following Junos Pulse deployment options:

- Use the defaults or make changes to the Junos Pulse default component set and default connection set, and then download and distribute Pulse by having users log in

to the gateway's user Web portal and be assigned to a role. After the installation is complete, users have all the connections they need to access network resources.

- Create connections that an endpoint needs for connectivity and services, download the Pulse settings file (.jnprpreconfig), download default Pulse .msi installation program, and then run the .msi installation program by using an msiexec command with the settings file as an option. You can use the msiexec command to deploy Pulse using a standard software distribution process, such as SMS/SCCM.
- Distribute Junos Pulse with no preconfiguration. You can download the default Junos Pulse installation file (Mac or Win) from the Secure Access Service, and then distribute the file to endpoints using your organization's standard software distribution methods. Because the installer does not contain preconfigured connections, users must define network connections manually. Or you can create dynamic connections on each access gateway. These connections are automatically downloaded to the installed Pulse client when users provide their login credentials to the gateway's user Web portal.

The following tasks summarize how to configure Junos Pulse on the Secure Access Service:

- Create and assign user roles to control who can access different resources and applications on the network. If you are converting your access environment from agentless or a VPN Tunneling environment, you should create new roles that are specific for Junos Pulse.
- Define security restrictions for endpoints with Host Checker policies.
- Define user realms to establish authentication domains. If you are converting your access environment from agentless or a NC environment, typically you can use your existing realms.
- Associate the roles with appropriate realms to define your access control hierarchy using role mapping.
- Define Junos Pulse component sets, connection sets, and connections.
- Deploy Junos Pulse to endpoints.

Related Documentation

- [Junos Pulse Overview on page 37](#)
- [Junos Pulse Connection Options on page 46](#)
- [Creating a Client Connection Set on page 51](#)
- [Creating a Client Component Set on page 56](#)
- [Configuring a Role for Junos Pulse on page 41](#)

Configuring a Role for Junos Pulse

A user role defines session settings and options, personalization settings (user interface customization and bookmarks), and enabled access features (Web, file, application, Telnet/SSH, Terminal Services, network, meeting, and e-mail access). A user role does not specify resource access control or other resource-based options for an individual

request. For example, a user role can define whether or not a user can perform Web browsing. However, the individual Web resources that a user may access are defined by the Web resource policies that you configure separately.

The following procedure describes the role configuration options that apply to a role that employs Junos Pulse.

To create a role for Junos Pulse endpoints:

1. Select **Users > User Roles > New User Role** in the admin console, or select an existing role.
2. Enter a name for the role and, optionally, a description. This name appears in the list of Roles on the Roles page.
3. Click **Save Changes**. Role configuration tabs appear.

Configuring Role Options for Junos Pulse

All of the options for role configuration tabs are described in Access Management Framework.

To configure a role for Junos Pulse endpoints:

1. From the admin console, select **Users > User Roles**.
2. Click the role you want to configure.
3. On the General tab, click Overview and then under Options, select **Junos Pulse**.
4. Click the VPN Tunneling tab.
5. Under Split Tunneling Options, select your options:
 - **Split Tunneling**—Split tunneling options let you define how network traffic flows on the client.
 - **Enable**—Pulse modifies routes on the client so that traffic meant for the corporate intranet uses the virtual adapter created by Pulse (the Pulse tunnel) and all other traffic goes through the local physical adapter.
 - **Disable**—When the Pulse session is established, predefined local subnet and host-to-host routes that might cause split-tunneling behavior are removed, and all network traffic from the client goes through the Pulse tunnel. With split tunneling disabled, users cannot access local LAN resources during an active VPN session.



NOTE: Location awareness behavior is affected by split tunneling configuration. For example, if a location awareness rule relies on a address resolution made on the physical adapter, and split tunneling is disabled, the rule always resolves to FALSE after Pulse establishes the connection.

- **Route Precedence**—You can define which routing table takes precedence:

- **Tunnel routes**—The route table associated with the Pulse virtual adapter take precedence. Pulse overwrites the physical interface routes if there is conflict between the Pulse virtual adapter and the physical adapters. Pulse restores the original routes when the connection is ended.
 - **Endpoint routes**—Current IP routes take precedence.
 - **Route Monitor**—Pulse can monitor the route tables and take appropriate action.
 - **Yes**—Pulse ends the connection if a change is made to the routing tables.
 - **No**—Route tables are allowed to change on the client endpoint.
6. Under Auto Launch Options, select the **Auto-launch** check box to activate Pulse automatically when the endpoint is started.
 7. In the Options for Juniper client on Windows area, optionally specify a location for the following:
 - **Windows: Session start script**—Specify a script to run for users assigned to the role after Junos Pulse connects with the Secure Access Service. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources.
 - **Windows: Session end script**—Specify a script to run for users assigned to the role after Junos Pulse disconnects from the Secure Access Service. For example, you can specify a script that disconnects mapped network drives. If there is no start script defined, or the start script has not been run, the end script does not run.
 8. In the Options for Juniper client on Mac area, optionally specify a location for the following:
 - **Mac: Session start script**—Specify a script to run for users assigned to the role after Junos Pulse connects with the Secure Access Service.
 - **Mac: Session end script**—Specify a script to run for users assigned to the role after Junos Pulse disconnects from the Secure Access Service.
 9. Click **Save Changes**.

Host Checker options allow you to enable Host Checker policies, to choose one or more policies for the role, and to specify whether the endpoint must meet all or just one of the selected Host Checker policies. See Endpoint Defense for complete information on configuring endpoint security settings.

To configure Host Checker for a selected role:

1. For a selected role, select **General > Restrictions > Host Checker**.
2. Select the check box **Allow users whose workstations meet the requirements specified by these Host Checker policies**.
3. Click **Add** to move Host Checker policies from the Available Policies list to the Selected Policies list.

4. Select the check box **Allow access to the role...** to grant access if the endpoint passes any of the selected Host Checker policies.
5. Click **Save Changes**.

Related Documentation

- [Junos Pulse Connection Options on page 46](#)
- [Creating a Client Connection Set on page 51](#)
- [Creating a Client Component Set on page 56](#)

Pulse Connection Set Options for Pulse Secure Access Service

A Junos Pulse client connection set allows you to configure specific connection policies for client access to any Pulse server. The following options are applied to each connection added to the connection set.

- **Allow saving logon information**—Controls whether the Save Settings check box is available in login credential dialog boxes in the Junos Pulse client. If you clear this check box, the Junos Pulse client always requires users to provide credentials. If you select this check box, users have the option of saving their credentials.

The Junos Pulse client can retain *learned user settings*. These settings are retained securely on the endpoint, evolving as the user connects through different gateways and methods. The Junos Pulse client can save the following settings:

- Certificate acceptance
- Certificate selection
- Realm
- Username and password
- Proxy username/password
- Secondary username/password
- Role



NOTE: If the authentication server is an ACE server or a Radius server and authentication is set to Users authenticate using tokens or one-time passwords, Pulse ignores the Allow saving logon information option. If the user sees a username and token prompt and the Save Settings check box is disabled. Pulse supports soft token, hard token and smart card authentication.

When a user opts to save settings, that information is used for each subsequent connection without prompting. If a setting changes, (for example, if a user changes a password), the saved setting is invalid and connection attempts fail. In this case, the user must use the client's Forget Saved Settings feature. The Forget Saved Settings

feature clears all user saved settings, and Junos Pulse prompts the user for required information on connection attempts.

- **Allow user connections**—Controls whether connections can be added by the user.
- **Display splash screen**—Clear this check box to hide the Pulse splash screen that normally appears when the Pulse client starts.
- **Dynamic certificate trust**—Determines whether users can opt to trust unknown certificates. If you enable this check box, a user can ignore warnings about invalid certificates and connect to the target Pulse server.
- **Dynamic connections**—Allows connections within this connection set to be automatically updated or added to a Junos Pulse client when the user connects to the Pulse server through the user Web portal. Dynamic connections are created as manual rather than automatic connections, which means that they are run only when the user initiates the connection or the user browses to a Pulse Server and launches Pulse from the server's Web interface.
- **FIPS mode enabled**—Enable FIPS mode communications for all Pulse connections in the connection set. The Federal Information Processing Standard (FIPS) defines secure communications for the U.S. government. When a Pulse connection is operating in FIPS mode, **FIPS On** appears in the lower corner of the Pulse client interface. Application acceleration is not available for a connection that is operating in FIPS mode.
- **Wireless suppression**—Disables the endpoint's wireless access when a wired connection is available. Wireless suppression occurs only when the wired connection is connected and authorized.

If the wired connection is removed, Pulse enables the wireless connections with the following properties:

- Connect even if the network is not broadcasting.
- Authenticate as computer when computer information is available.
- Connect when this network is in range.



NOTE: If you enable wireless suppression, be sure to also configure a connection that enables the client to connect through a wired connection.

Related Documentation

- Junos Pulse Secure Access Service Overview
- Creating a Client Connection Set for Junos Pulse Secure Access Service
- [Junos Pulse Connection Options on page 46](#)
- [FIPS Overview on page 1131](#)

Junos Pulse Connection Options

When you create a connection for a connection set, you must choose a connection type.

[Table 2 on page 46](#) lists the options available for each connection type.

Table 2: Pulse Connection Options

UAC (802.1X) options	Adapter type —Specifies the type of adapter to use for authentication: wired or wireless.
Use this connection type to define authenticated connectivity to 802.1X devices, wired or wireless. Users cannot create 802.1X from the Pulse client interface. Users see 802.1X connections in the Pulse interface only when the connection has been deployed from the server and the specified network is available.	<p>Outer username—Enables a user to appear to log in anonymously while passing the actual login name (called the inner identity) through an encrypted tunnel. As a result, the user's credentials are secure from eavesdropping, and the user's inner identity is protected. In general, enter anonymous, which is the default value. In some cases, you might need to add additional text. For example, if the outer identity is used to route the user's authentication to the proper server, you might be required to use a format such as <code>anonymous@acme.com</code>.</p> <p>NOTE: If you leave the box blank, the client passes the user's login name (inner identity) as the outer identity.</p>
	<p>Scan list—If you selected wireless as the adapter type, the scan list box is available to specify the SSIDs to connect to in priority order. If you leave the list empty, the user can connect to any available wireless network.</p>
	<p>Support Non-broadcast SSID—Allow a user to connect to a non-broadcast wireless network from within the Pulse interface.</p>
Trusted Server List for 802.1X Connection	<p>Server certificate DN—If you are using certificate authentication, specify the server certificate distinguished name (DN) and its signing certificate authority (CA). An empty DN field allows a client to accept any server certificate signed by the selected CA.</p>

Table 2: Pulse Connection Options (*continued*)

SSL VPN or UAC (L3) options	<p>Allow user to override connection policy—Allows a user to override the connection policy by manually connecting or disconnecting. Typically, you leave this option selected to make sure that a user can establish a connection under all conditions. If you disable this check box, the user cannot change the endpoint's connection status, suspend or resume a connection to Pulse Secure Access Service, or shut down Junos Pulse.</p>
	<p>Support Remote Access (SSL VPN) or LAN Access (UAC) on this connection—Specifies that the connection is used for network connectivity. This option must be selected if this connection is for Pulse Access Control Service. If the connection is for Pulse Secure Access Service, you can disable this check box and use the connection for accessing Pulse Collaboration meetings only by also selecting Enable Junos Pulse Collaboration integration on this connection.</p>
	<p>Enable Junos Pulse Collaboration integration on this connection—Specifies that the connection is used for Pulse Collaboration Suite meetings. This option must be disabled if this connection is for Pulse Access Control Service. If the connection is for Pulse Secure Access Service, you can enable this check box and use the connection for accessing Pulse Collaboration meetings.</p>
	<p>You can enable a connection for Pulse Secure Access Service to be used for remote access only, for Pulse Collaboration integration only, or for both remote access and Pulse Collaboration integration. If you do not select either option, an error occurs when you save changes to this connection.</p>
	<p>This server—Specifies that you want the endpoint to connect to this Pulse server. Clear this check box to enable the edit box of the URL field and to specify a different Pulse server.</p>
	<p>URL—Allows you to specify a URL for a different Pulse server as the default connection. Specify a different server's URL to create connections for other Pulse servers in your network.</p>
SRX options	<p>Address—Specifies the location (hostname or IP address) of the firewall.</p>
	<p>Allow user to override connection policy—Allows a user to override the connection policy by manually connecting or disconnecting. Typically, you leave this option selected to make sure that a user can establish a connection under all conditions. If you disable this check box, the user cannot change the endpoint's connection status or shut down Junos Pulse.</p>
App Acceleration options	<p>Allow user to override connection policy—Allows a user to override the connection policy by manually connecting or disconnecting. Typically, you leave this option selected to make sure that a user can establish a connection under all conditions. If you disable this check box, the user cannot change the endpoint's connection status or shut down Junos Pulse.</p>
	<p>NOTE: For connections that use application acceleration, if Kaspersky software is installed on the Pulse client endpoint, it must be configured to allow traffic on UDP port 3578.</p>
	<p>Community string—The Junos Pulse client and the Pulse Application Acceleration Service can form an adjacency only if they belong to the same community as identified by the community string. When you create an App Acceleration connection, be sure the community string for the connection matches the community string defined in the Pulse Application Acceleration Service.</p>

Connection is Established Settings

For all connection types, you specify how the connection is established, manually or automatically. The options vary according to the type of connection. Automatic connections include machine authentication and credential provider connections.

Connections can be established using the following options:

- **Manually by the user**—When the endpoint is started, the Junos Pulse client software is started, but no connection is attempted. The user must use the Junos Pulse client user interface to select a connection.
- **Automatically after user signs into the desktop**—When the endpoint is started and the user has logged in to the endpoint, the Junos Pulse client software connects automatically. For App Acceleration connections, automatically is the default because Pulse forms an adjacency with Pulse Application Acceleration Service automatically if the service is available.



NOTE: All connections on an endpoint that are configured to start automatically attempt to connect to their target networks at startup time. To avoid multiple connection attempts, be sure that only one connection is configured to start automatically, or configure location awareness rules.

- **Automatically when the machine starts. Machine credentials used for authentication**—Enables machine authentication, which requires that Active Directory is used as the authentication server and that machine credentials are configured in Active Directory.



NOTE: If the machine and user have different roles, each role should map to the same connection set. Otherwise, after the user connects, the existing connection set might be replaced.

- **Automatically when the machine starts. Connection is authenticated again when the user signs in to the desktop**—Enables machine authentication for the initial connection. After the user connects with user credentials, the machine authentication is dropped. When the user logs out, the machine authentication connection is restored.
- **Automatically at user login**—Enables Pulse client interaction with the credential provider software on the endpoint. The user credentials are used to establish the authenticated Pulse connection to the network, log in to the endpoint, and log in to the domain server.



NOTE: This label changed at Pulse Secure Access Service R7.3. If you had selected the old label for a Pulse connection, **Automatically during desktop authentication. User is presented with the Junos Pulse credential tile at the logon screen**, it is automatically converted to the new label, **Automatically at user login** when you upgrade the system from R7.2.

- **Automatically when the machine starts. Connection is authenticated again at user login**—Enables Pulse client interaction with the credential provider software on the endpoint. Machine credentials are used to establish the authenticated Pulse connection to the network. When the user provides user credentials, the connection is authenticated again. In one typical use case, the machine credentials provide access to one VLAN, and the user credentials provide access to a different VLAN.

Location Awareness Rules

For connections that are set to have the connection established automatically, you can define location awareness rules.

According to location awareness rules—Location awareness rules enable an endpoint to connect conditionally. For example, the endpoint connects to Pulse Access Control Service if it is connected to the company intranet or it connects to Pulse Secure Access Service if it is in a remote location.

A Pulse connection uses the IP address of a specified interface on the endpoint to determine its network location. Each location awareness rule includes the following settings:

- **Name**—A descriptive name, for example, “corporate-DNS.” A name can include letters, numbers, hyphens, and underscores.
- **Action**—The method the connection uses to discover the IP address. Choose one of the following values:
 - **DNS Server**—Allows the endpoint to connect if the endpoint’s DNS server on the specified interface is set to one of the specified values. Use the condition box to specify IP addresses or address ranges.
 - **Resolve Address**—Allows the endpoint to connect if the hostname specified in the DNS Name box can be resolved by the DNS server for the specified interface. If one or more address ranges are specified in the Address Range box, the address must resolve to one of the ranges to satisfy the expression.
 - **Endpoint Address**—Allows the endpoint to connect if the IP address of the specified interface is within a range specified in the IP Address Range box.

Machine Connection Preferences

The Machine Connection Preferences appear if you have selected one of the machine authentication options for how the connection is established. Normally Pulse presents a selection dialog box if more than one realm or role is available to the user. However, a connection that is established through machine authentication fails if a dialog box is presented during the connection process. To suppress the selection dialogs, either ensure that only one role and realm is available to users, or specify a preferred realm and role for this connection.

- **Preferred Machine Realm**—Specify the realm that this connection uses when establishing the machine connection. The connection ignores any other realm available for the specified login credentials
- **Preferred Machine Role Set**—Specify the role or the name of the rule for the role set that this connection uses when establishing the machine connection. The role or rule name used must be a member of the preferred machine realm.

User Connection Preferences

The User Connection Preferences options enable you to specify a realm and role for automatic connections that would otherwise present a selection dialog box to the user. To suppress the selection dialogs, either ensure that only one role and realm is available to users or specify a preferred realm and role for this connection.

- **Preferred User Realm**—Specify the realm for this connection that is used when a user logs onto the endpoint. The connection ignores any other realm available for the user's login credentials
- **Preferred User Role Set**—Specify the preferred role or the name of the rule for the role set to be used for user authentication. The role or rule name must be a member of the preferred user realm.
- The **Select client certificate from machine certificate store** option enables you to specify the location of the client certificate on a Windows endpoint as part of a Pulse connection that verifies the identity of both the machine and the user before establishing a connection. When this check box is selected, the Pulse connection looks at client certificates located in the Local Computer personal certificate store. When this check box is not selected, the connection accesses the user certificate store a Windows endpoint. For more information, see Machine and User Authentication Through a Pulse Connection for Pulse Secure Access Service.

Pre-login Connection Preferences

The following Pre-login Connection Preferences appear if you select Automatically at user login or Automatically when machine starts. Connection is authenticated again at user login. as the Connection is established option:

- **Pre-login maximum delay**—The time period (in seconds) that a Windows client waits for an 802.1x connection to succeed during the login attempt. The range 1 to 120 seconds.

- **Pre-login user based virtual LAN**—If you are using VLANs for the machine login and the user login, you can enable this check box to allow the system to make the VLAN change.

Related Documentation

- Configuring Location Awareness Rules for Junos Pulse
- Creating a Client Connection Set for Junos Pulse Secure Access Service
- Preferred Realm and Role for Junos Pulse Machine Authentication
- Machine and User Authentication Through a Pulse Connection for Pulse Secure Access Service

Creating a Client Connection Set

To create a client configuration:

1. From the admin console, select **Users > Junos Pulse > Connections**.
2. Click the **New** button.
3. Enter a name and optional description for this connection set.



NOTE: You must enter a name, otherwise you cannot create a connection set.

4. Click **Save Changes**.
5. From the main Junos Pulse Connections page, select the connection set.
6. Under Options, select or clear the check box for each of the following items.
 - **Allow saving logon information**
 - **Allow user connections**
 - **Display Splash Screen**
 - **Dynamic certificate trust**
 - **Dynamic connections**
 - **Wireless suppression**
7. Under connections, click **New** to define a new connection.
8. Enter a name and an optional description for this connection.
9. Select a Type for the connection. The Type identifies the device type for the connections and can be any of the following:
 - **802.1X**
 - **SSL VPN or (UAC) L3**
 - **SRX**
 - **App Acceleration**

10. If you select **802.1X** from the type list enter a value or select or clear the following check boxes:
 - **Adapter type**
 - **Outer username**—Enter the outer username.
 - **Scan list**—Enter the SSIDs to connect to in your order of priority.
 - **Support Non-broadcast SSID**—Select this option to allow users to connect to non-broadcast networks.
11. Click **Save Changes**.
12. If you select **SSL VPN or (UAC) L3** after Options, select or clear the check box for each of the following items:
 - **Allow user to override connection policy**—Allows a user to override the connection policy by manually connecting or disconnecting. Typically, you leave this option selected to make sure that a user can establish a connection under all conditions. If you disable this check box, the user cannot change the endpoint's connection status or shut down Junos Pulse.
 - **Enable Junos Pulse Collaboration integration on this connection**—This option specifies that the connection is used for Pulse Collaboration Suite meetings. (Formerly called Secure Meeting.) This option must be disabled if this connection is for Pulse Access Control Service. If the connection is for Pulse Secure Access Service, you can enable this check box and use the connection for accessing Pulse Collaboration meetings.

You can enable a connection for Pulse Secure Access Service to be used for remote access only, for Pulse Collaboration integration only, or for both remote access and Pulse Collaboration integration. If you do not select either option, an error occurs when you save changes to this connection.
 - **Support Remote Access (SSL VPN) or LAN Access (UAC) on this connection**—This option must be selected if this connection is for Pulse Access Control Service. If the connection is for Pulse Secure Access Service, you can disable this check box and use the connection for accessing Pulse Collaboration meetings only by also selecting **Support Remote Access (SSL VPN) or LAN Access (UAC) on this connection**.
 - **Support Remote Access (SSL VPN) or LAN Access (UAC) on this connection**—This option must be disabled if this connection is for Pulse Access Control Service. If the connection is for Pulse Secure Access Service, you can enable this check box and use the connection for accessing Pulse Collaboration meetings.
 - **This Server**—This connection will use the URL of the server where you are creating the connection.
 - **URL**—If you did not enable the check box for This Server, you must specify the URL of the server for the connection.
13. If you select **SRX**, enter an IP address in the **Address** box.
14. From the Options list, select or clear the following check boxes:
 - **Address**—The network address for the firewall device.
 - **Allow user to override connection policy**

15. (Optional) You can enable location awareness by creating location awareness rules. Location awareness can force a connection to a particular interface.
16. If you select **App Acceleration**, select the **Connect Automatically** check box to permit the client to automatically connect to App Acceleration in the network.
17. After you have created the client connection set, create a client component set profile, and select this connection set.

Related Documentation

- [Junos Pulse Connection Options on page 46](#)
- [Junos Pulse Component Set Options on page 55](#)
- [Creating a Client Component Set on page 56](#)
- [Configuring Connection Rules for Location Awareness on page 53](#)

Configuring Connection Rules for Location Awareness

The location awareness feature enables a Pulse client to recognize its location and then make the correct connection. For example, a Pulse client that is started in a remote location automatically connects to the Secure Access Service. But that same client automatically connects to an IC Series appliance when it is started in the corporate office.



NOTE: Location awareness and session migration are similar because they both simplify connectivity for the user, but they do so under different conditions. With location awareness, the Pulse client makes a decision on where to connect when a user logs in to the computer. Session migration occurs when the user puts the computer into a stand by or hibernate mode without first logging off, and then opens the computer in a different network environment. Location awareness enables the Pulse client to intelligently start a new session. Session migration enables Pulse servers to intelligently migrate an existing session.

Location awareness relies on rules you define for each connection. If the conditions specified in the rules are true, Pulse attempts to make the connection. To set up the location awareness rules that select among many connections, you must define location awareness rules for each connection. Each location awareness rule is based on the endpoint's ability to reach an IP address or resolve a DNS name over a specified network interface.



NOTE: Location awareness behavior is affected by split tunneling configuration. For example, if a location awareness rule relies on a address resolution made on the physical adapter, and split tunneling is disabled, the rule always resolves to FALSE after Pulse establishes the connection.



NOTE: Connections can be set to manual, automatic, or controlled by location awareness rules. When the user logs in, the Pulse client attempts every connection in its connections list that is set to automatic or controlled by location awareness rules.

To configure location awareness rules:

1. If you have not already done so, create a connection or open an existing connection.
2. In the Connection is established area, select **According to location awareness rules**, and then click **New**.
3. Enter a name for this rule.
4. In the Action list, select one of the following:
 - **DNS server**—Connect if the DNS server associated with the endpoint's network properties is (or is not) set to a certain value or set of values. Specify the DNS server IP address in the IP address box. Also specify a network interface on which the condition must be satisfied:
 - **Physical**—The condition must be satisfied on the physical interfaces on the endpoint.
 - **Junos Pulse**—The condition must be satisfied on the virtual interface that Junos Pulse creates when it establishes a connection.
 - **Any**—Use any interface.
 - **Resolve address**—Connect if the configured host name or set of host names is (or is not) resolvable by the endpoint to a particular IP address. Specify the host name in the DNS name box and the IP address or addresses in the IP address box. Also specify a network interface on which the condition must be satisfied.



NOTE: The Pulse client software evaluates IP and DNS policies on network interface changes. DNS lookups occur on DNS configuration changes or when the time-to-live setting (10 minutes) expires for a particular host record. If Pulse cannot resolve the host for any reason, it polls the configured DNS server list every 30 seconds. If the host had been resolved successfully previously and the time-to-live timer has not expired, the polling continues until the timer expires. If the host had not been resolved successfully previously, the resolution attempt fails immediately.

5. Click **Save Changes**.
- **Endpoint Address**—Connect if a network adapter on the endpoint has an IP address that falls within or outside of a range or a set of ranges. Specify the IP address or addresses in the IP address box. Also specify a network interface on which the condition must be satisfied.

After you create the rule or rules, you must enable each rule you want to use for the connection. To enable a negative form of a rule, use a custom version of the rule. To enable location awareness rules:

1. In the list of connection awareness rules for a connection, select the check box next to each rule you want to enable.
2. To specify how to enforce the selected location awareness rules, select one of the following options:
 - **All of the above rules**—The condition is TRUE and the connection is attempted only when all selected location awareness rules are satisfied.
 - **Any of the above rules**—The condition is TRUE and the connection is attempted when any select location awareness rule is satisfied.
 - **Custom**—The condition is TRUE and the connection is attempted only when all selected location awareness rules are satisfied according to the Boolean logic you specify in the Custom box. Use the Boolean condition to specify a negative location rule. For example, connect to the Secure Access Service when Rule-1 is false and Rule-2 is true. The boolean logic in the custom box would be: NOT Rule-1 AND Rule-2. The accepted Boolean operators are AND, OR, NOT, and the use of ().
3. Click **Save Changes**.

Related Documentation

- [Creating a Client Connection Set on page 51](#)

Junos Pulse Component Set Options

A Junos Pulse component includes specific software components that provide Pulse connectivity and services.

A component set options includes the following options:

- **All components**—Includes all components. The Enhanced Endpoint Security (EES) component, which is available only if you have purchased an EES license, is included only if the user's assigned role requires it. Use the **All components** option only when you want client endpoints to be able to connect to all supported Pulse servers and to be able to use application acceleration. When you include the App Acceleration component, the disk space requirement for the Junos Pulse client installation increases to 300 MB.
- **No components**—Select this option to create an installer that only updates existing Pulse client installations, for example, to add a new connection. Do not use this option if you are creating an installer to add Pulse to endpoints that do not already have Pulse installed.
- **Minimal components**—Includes only the components needed to support the selected connections. For example, if the connection set you create includes an IC or Secure Access Service connection, the component set includes only the components required to connect to Pulse Access Control Service or Pulse Secure Access Service. The default

is Minimal components, which provides all needed components for the selected connections and limits the size of the Junos Pulse installation file.



NOTE: Selecting Pulse components applies to a Web installation only. The preconfigured installer always installs all components unless you specify the specific components you want using command line options. A preconfigured installer for an OS X endpoint always installs all components.

- Related Documentation**
- [Creating a Client Component Set on page 56](#)
 - [Configuring a Role for Junos Pulse on page 41](#)
 - The Client Installer Package

Creating a Client Component Set

To create a client component set:

1. From the admin console, select **Users > Junos Pulse > Components**.
2. Click **New** to create a new component set.
3. If you have not yet created a client connection set, select **Users > Pulse > Connections** and create a new connection set. Alternately, use the default client configuration, which permits dynamic connections, supports the outer username anonymous, and allows the client to connect automatically to an IC Series or Secure Access Service device.
4. Specify a **Name** for the client component set.
5. (Optional) Enter a **Description** for this client component set.
6. Select a connection set that you have created, or use the default connection set.
7. For Junos Pulse client components, select one of the following option buttons:
 - **All components**—The installer contains all Junos Pulse components, supporting all access methods and all features
 - **No components**—The preconfigured installer is a configuration update only, and works on endpoints that already have the Junos Pulse client installed.
 - **Minimal components**—Includes only the components needed to support the selected connections. For example, if the connection set you create includes an IC or SA connection, the component set includes only the components required to connect to Pulse Access Control Service or Pulse Secure Access Service. The Host Checker component is included as part of the minimal components configuration. The default is minimal components, which provides all needed components for the selected connections and limits the size of the Junos Pulse installation file.



NOTE: Do not deploy Pulse with minimal components and no connections. If you do so, the Pulse client is not able to connect to any devices and users are not able to create any connections from within the Pulse client interface.



NOTE: Selecting Pulse components applies to a Web installation only. A preconfigured installer for a Windows endpoint always installs all components unless you specify the specific components you want using MSIEXEC command options. A preconfigured installer for an OS X endpoint always installs all components.

8. Click **Save Changes**.
9. After you create a component set, distribute the client to users through a role. When users access the role, the installer automatically downloads to the endpoint. The installer components and connections are applied to the endpoint client.

If client connections associated with the component set for a role are changed even though the list of components has not, the existing configuration on the endpoint is replaced immediately if the endpoint is currently connected, or the next time the endpoint connects.

If a user is assigned to multiple roles and the roles include different component sets, the first role in an endpoint's list of roles is the one that determines which client (component set) is deployed.

Related Documentation

- [Junos Pulse Connection Options on page 46](#)
- [Creating a Client Connection Set on page 51](#)
- [Junos Pulse Component Set Options on page 55](#)
- [The Client Installer Package](#)
- [Configuring a Role for Junos Pulse on page 41](#)

Junos Pulse Client Installation Overview

The Secure Access Service include a default connection set and a default component set. These defaults enable you to deploy Junos Pulse to users without creating new connection sets or component sets. The default settings for the client permit dynamic connections, install only the components required for the connection, and permit an automatic connection to the Secure Access Service to which the endpoint connects.

In all deployment scenarios, you must have already configured authentication settings, realms, and roles.

You can deploy Junos Pulse to endpoints from Secure Access Service in the following ways:

- Web install—With a Web install, users log in to the access gateway's Web portal and are assigned to a role that supports a Pulse installation. When a user clicks the link to run Junos Pulse, the default installation program adds Pulse to the endpoint and adds the default component set and the default connection set. If you do not make any changes to the defaults, the endpoint receives a Pulse installation in which a connection to the gateway is set to connect automatically. You can edit the default connection set to add connections of other gateways and change the default options.



NOTE: A Web install requires that the user have Java installed and enabled for an installation through the Firefox browser or ActiveX enabled for an installation through Internet Explorer. If the browser does not meet this requirement, the user receives a descriptive message at the beginning of the installation process.

- Preconfigured installer—The preconfigured installer enables you to specify all connections that endpoints need, and then to create an installation program that you can distribute to endpoints using your local organization's standard software distribution method (such as Microsoft SCCM/SMS). After Pulse is installed on an endpoint, the user does not need to do any additional configuration.
- Default installer—You can download the default Pulse installation program in either .exe or .msi format and distribute it to endpoints using your local organization's standard software distribution method (such as Microsoft SMS/SCCM). The Junos Pulse client software is installed with all components and no connections. After users install a default Pulse installation, they can add new connections manually through the Pulse client user interface or by using a browser to access a gateway's Web portal. For the latter, the gateway's dynamic connection is downloaded automatically and the new connection is added to the Pulse client's connections list.

Installing the Junos Pulse Client from the Web

For a Web install, you direct users to the Web interface of the access gateway. After a successful login, a user is assigned to a role that includes an automatic download and installation of the Junos Pulse client software.



NOTE: A Web install requires that the user have Java installed and enabled for an installation through the Firefox browser or ActiveX enabled for an installation through Internet Explorer. If the browser does not meet this requirement, the user receives a descriptive message at the beginning of the installation process.

The default Junos Pulse installation settings includes minimal components and a connection to the access gateway. If you want a Web install that has customized settings, you can do any of the following:

- Edit the default connection set and add new connections. The default installer uses the default component set which includes the default connection set.
- Create a new connection set and edit the default component set to include the new connection set.
- Edit the role to specify a component set that includes the connections you want for the default installation.

Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File

The following procedures apply to Windows installations only.

After you create client connection sets and specify the connections to include within a client component set, you can create a preconfiguration file with all of the connections you want to distribute with the Pulse client. You specify the preconfiguration file as an option when you run the Pulse MSI installer program using an `msiexec` (`windows\system32\msiexec.exe`) command.

To create a preconfigured Pulse installer for distribution to Windows endpoints:

1. Select **Users > Junos Pulse > Connections** and create a connection set with the connections that you want to distribute.
2. Select **Users > Junos Pulse > Components**.
3. If necessary, create a new component set with the connection sets you want to distribute.

It does not matter which component option you select, All components, No components, or Minimal components. The Pulse installer installs all components unless you specify which components to install using one or more `ADDLOCAL` options in the command line. If you specify one or more `ADDLOCAL` options, the installer installs only the components you specify. Be sure that you specify all the components required to support the connections you have selected.

4. Select the check boxes next to the component sets that you want to distribute.
5. Click **Download Installer Configuration**.

You are prompted to save the preconfiguration. You can also specify the name of the target Pulse server for the connections, which enables you to create configuration files that are the same except for the target server.

The default filename of the `.jnprpreconfig` file is the name of the selected component set. Make note of the filename and location where you put the file. The preconfiguration file must be available to the clients either through a network share or distributed along with the Junos Pulse installation file.

6. Select **Maintenance > System > Installers**.

If necessary for your environment, download and install the Juniper Installer Service. To install Pulse, users must have appropriate privileges. The Juniper Installer Service allows you to bypass privilege restrictions and allow users with limited privileges to

install Pulse. See [“Downloading Application Installers” on page 813](#) for more information about Juniper Installer Service.

7. Download the appropriate Junos Pulse installer for your Windows environment:
 - Junos Pulse Installer (32-bit)
 - Junos Pulse Installer (64-bit)



NOTE: For a Windows installation (.msi) that uses an automated distribution mechanism and where the users do not have administrator privileges, you should ensure that the installation is run in the proper context, typically the USER context. To install in USER context, first advertise the .msi while in the SYSTEM context. For example, to advertise the 64-bit Windows installation to all users, use the following `msiexec` command:

```
msiexec /jm \JunosPulse.x64.msi
```

The advertisement allows the installation to be run in USER context even if the user is a restricted (non-admin) user. The location where the advertisement is run and where the actual installation is run *must* be the same. If the installation is an upgrade, you must advertise the upgrade version before running it. (Note that it is much easier to upgrade the Pulse client by not disabling the automatic upgrade feature on the Pulse server.) After the installation is run by the user, the Pulse client will use the correct user certificate and context.

Installing the Pulse Client Using Advanced Command-Line Options

The Junos Pulse installer includes the Pulse client and all the software components for all the Pulse services. The preconfiguration file contains the definitions of the Pulse connections that provide client access to specific Pulse servers and services.

Usage Notes:

- The preconfigured installer installs all Pulse components unless you specify the specific components you want using `ADDLOCAL` options. If you use one or more `ADDLOCAL` options, the preconfigured installer installs only the components specified by `ADDLOCAL`. A preconfigured installer ignores the component set you select when you create the preconfiguration file.
- When you use `ADDLOCAL` options, be sure that your `msiexec` command specifies *all* the components required for your connections. For example, if the connection requires 802.1X connectivity for a connection to Pulse Access Control Service, be sure to include both the 802.1X component and the Pulse Access Control Service component (`ADDLOCAL=PulseUAC,Pulse8021x`).
- When you run `msiexec`, you should append `/qn` or `/qb` (`msiexec` options) to the command line to suppress the installation program user interface. For example, the user interface lets the user choose a complete installation or a custom installation, which can override the components you specify with `ADDLOCAL` options. If the user selects Complete, the `msiexec` program ignores the `ADDLOCAL` options in the command

line and installs all components. The `/qn` option specifies a silent install, so no user interface appears. The `/qb` option also hides the user interface but it displays a progress bar.

- The procedures in this topic are valid with Windows installations only. For information about installing Pulse on OS X endpoints, see [“Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File”](#) on page 63.

You run the Pulse preconfigured installer program with `msiexec` (the command line for launching .msi programs on Windows platforms) and specify the following options.



NOTE: Command line options (`CONFIGFILE` and `ADDLOCAL`) are case sensitive and must be all caps.



NOTE: If the path to the `.jnpreconfig` file includes spaces, be sure to use quotes around the path.

- **CONFIGFILE**—This property specifies a configuration file to be imported into Pulse during installation. The property must include the full path to the configuration file. For example:

```
msiexec -i JunosPulse.msi CONFIGFILE="c:\temp\my configuration.jnpreconfig"
```

- **ADDLOCAL**—This optional property specifies which features and feature options (subfeatures) to install when you want to install only specific Pulse features. If you do not specify `ADDLOCAL` options, all Pulse components are installed. A feature comprises the components required to support client connections. When you use `ADDLOCAL`, you should append `msiexec` options `/qn` or `/qb` to the command line to suppress the installation program user interface.

Feature and subfeature names are case sensitive. To specify multiple features in a single command, separate each feature with a comma.

The `ADDLOCAL` property has the following features:

- **PulseSA**—Pulse components required for Pulse Secure Access Service.
- **PulseUAC**—Pulse components required for Pulse Access Control Service.
- **PulseSRX**—Pulse components required for SRX Series Gateways.
- **PulseAppAccel**—Pulse components required for Pulse Application Acceleration Service.

The `ADDLOCAL` property has the following optional subfeatures:

- **Pulse8021x**—Available with `PulseUAC`. Includes 802.1X connectivity components.
- **SAEndpointDefense**—Available with `PulseSA`. Includes Enhanced Endpoint Security (EES) components for connections to Pulse Secure Access Service.

- **SAHostChecker**—Available with PulseSA. Includes Host Checker components for connections to Pulse Secure Access Service.
- **UACEndpointDefense**—Available with PulseUAC. Includes EES components for connections to Pulse Access Control Service.
- **UACHostChecker**—Available with PulseUAC. Includes Host Checker components for connections to Pulse Access Control Service.
- **UACIPSec**—Available with PulseUAC. Includes components required to connect to Pulse Access Control Service using IPSec from 32-bit Windows endpoints. This feature is available in the 32-bit MSI only.
- **UACIPSec64**—Available with PulseUAC. Includes components required to connect to Pulse Access Control Service using IPsec from 64-bit Windows endpoints. This feature is available in the 64-bit MSI only.

Examples

When you use ADDLOCAL, you should append **msiexec** options **/qn** or **/qb** to the command line to suppress the installation program user interface. These examples use **/qb**.

To install PulseUAC with 802.1X and EES support on a Windows 32-bit endpoint using a configuration file:

```
msiexec -i JunosPulse.x86.msi CONFIGFILE=c:\pulse\Pulse-Connection-no.jnprpreconfig  
ADDLOCAL=PulseUAC,Pulse8021x,UACEndpointDefense /qb
```

To install PulseSA on a 32-bit Windows endpoint using a configuration file:

```
msiexec -i JunosPulse.x86.msi CONFIGFILE="c:\temp\myconfiguration.jnprpreconfig"  
ADDLOCAL=PulseSA /qb
```

To install PulseSA with EES and Host Checker on a 64-bit Windows endpoint using a configuration file:

```
msiexec -i JunosPulse.x64.msi CONFIGFILE="c:\temp\myconfiguration.jnprpreconfig"  
ADDLOCAL=PulseSA,SAEndpointDefense,SAHostChecker /qb
```

To install PulseAppAccel on a 64-bit Windows endpoint using a configuration file:

```
msiexec -i JunosPulse.x64.msi CONFIGFILE="c:\temp\myconfiguration.jnprpreconfig"  
ADDLOCAL=PulseAppAccel /qb
```

To install all Pulse components on a 64-bit Windows endpoint using a configuration file:

```
msiexec -i JunosPulse.x64.msi CONFIGFILE="c:\temp\myconfiguration.jnprpreconfig"  
/qb
```

Repairing a Pulse Installation on a Windows Endpoint

Junos Pulse uses an MSI installer, which supports a repair function. If problems with Pulse on a Windows endpoint indicate missing or damaged files or registry settings, the user can easily run the installation repair program. The repair program performs a reinstallation and replaces any missing files. The repair program does not install any files that were not part of the original installation. For example, if the file that holds Pulse connection configurations is damaged, the file installed by the repair program does not replace any

Pulse connections that were created by the user or deployed to the endpoint after the original Pulse installation.

To repair a Pulse installation on a Windows endpoint:

1. On the Windows endpoint where Pulse is installed, click **Start > Programs > Juniper Networks > Junos Pulse > Repair Junos Pulse**.
2. Follow the prompts for the installation wizard.

When the program is finished, you might be prompted to reboot the system.

**Related
Documentation**

- [Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 63](#)

Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File

The following procedures apply to OS X installations only.

After you create client connection sets and specify the connections to include within a client component set, you can create a preconfiguration file with all the connections you want to distribute with the Pulse client. After you run the Pulse installer on the endpoint, you run a special command that imports the settings from the preconfiguration file into Pulse.

To create a preconfigured Pulse installer for distribution to OS X endpoints:

1. Select **Users > Junos Pulse > Connections** and create a connection set with the connections that you want to distribute.
2. Select **Users > Junos Pulse > Components**.
3. If necessary, create a new component set with the connection sets you want to distribute.

It does not matter which component option you select, All components, No components, or Minimal components. The Pulse installation program for OS X always installs all components.

4. Select the check boxes next to the component sets that you want to distribute.
5. Click **Download Installer Configuration**.

You are prompted to save the preconfiguration. You can also specify the name of the target Pulse server for the connections, which enables you to quickly create multiple configuration files that are the same except for the target server.

The default filename of the `.jnprpreconfig` file is the name of the selected component set. Make note of the filename and location where you put the file. The preconfiguration file must be available to the clients either through a network share or distributed along with the Junos Pulse installer file.

6. Select **Maintenance > System > Installers**.
7. Download the Junos Pulse installer, **Junos Pulse Installer (Macintosh)**.

Installing the Pulse Client on OS X Endpoints Using Command-Line Options

The Junos Pulse installer includes the Pulse client and all of the software components for all of the Pulse services. The preconfiguration (**.jnprpreconfig**) file contains the definitions of the Pulse connections that provide client access to specific Pulse servers and services. After you distribute the Pulse installation package, you must first run the installer, and then run a separate program called `jamCommand`, which imports the settings from the **.jnprpreconfig** file. The `jamCommand` program is part of the Pulse installation.

The Pulse file you download from the Pulse server is in compressed (`.dmg`) format. You must unpack the file before you run the Pulse installation program.

The following steps include sample commands to install Pulse on an OS X endpoint and then import Pulse connections from a **.jnprpreconfig** file.

1. Run the Pulse installation program:

```
/usr/sbin/installer -pkg <full-path-to-the-pulse-install-package> -target  
CurrentUserHomeDirectory
```

2. Import the settings from the **.jnprpreconfig** file:

```
/Applications/Junos\ Pulse.app/Contents/Plugins/JamUI/jamCommand -importFile  
<full-path-to-the-jnprpreconfig-file>
```

Related Documentation

- [Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 59](#)

Junos Pulse Command-line Launcher

The Junos Pulse Launcher (`pulselauncher.exe`) is a standalone client-side command-line utility that allows you to launch Pulse and connect to or disconnect from a Pulse server (Pulse Secure Access Service or Pulse Access Control Service) without displaying the Pulse graphical user interface.

Pulse Launcher Usage Notes:

- Pulse Launcher runs on 32-bit and 64-bit endpoints.
- Pulse Launcher runs on the following platforms:
 - Windows XP
 - Windows Vista
 - Windows 7
- The Pulse Launcher program, `pulselauncher.exe`, is installed as part of a Pulse client installation in **Program Files\Common Files\Juniper Networks\Integration**.
- Pulse Launcher works only for the SA or IC connection type. The Pulse launcher does not support the Firewall or 802.1X connection types.

- The Pulse Launcher program does not support the role mapping option that prompts a user to select from a list of assigned roles. If you use the Pulse Launcher and more than one role can be assigned to a user, you must configure the role mapping settings for the realm to merge settings for all assigned roles. If the realm settings require the user to select a role, the Pulse Launcher command fails and exits with return code 2.
- The Pulse Launcher program does not support secondary authentication.

To use the Pulse Launcher program:

1. Write a script, batch file, or application.
2. Include a call to the Pulse Launcher executable, `pulselauncher.exe`.
3. Include logic in your script, batch file, or application to handle the possible return codes.

[Table 4 on page 66](#) lists the Pulse Launcher return codes.

The following command shows the complete `pulselauncher.exe` command syntax:

```
pulselauncher.exe [-version|-help|-stop] [-url <url> -u <user> -p <password> -r <realm>] [-d <DSID> -url <url>] [-cert <client certificate> -url <url> -r <realm>] [-signout -url <url>] [-t timeout]
```

Table 3: Pulse Launcher Arguments

Argument	Action
<code>-version</code>	Display the Pulse Launcher version information, then exit.
<code>-help</code>	Display available arguments information.
<code>-stop</code>	Stop Pulse and disconnect all active connections.
<code>-url <url></code>	Specify the Pulse server URL.
<code>-u <user></code>	Specify the username.
<code>-p <password></code>	Specify the password for authentication.
<code>-r <realm></code>	Specify the realm on the Pulse server.
<code>-d <DSID></code>	Passes a cookie to Pulse Launcher for a specified Pulse server from another authentication mechanism when Pulse Launcher starts. When you use the <code>-d</code> argument, you must also specify the <code>-url</code> argument to specify the Pulse server.

Table 3: Pulse Launcher Arguments (*continued*)

Argument	Action
-cert <client certificate>	<p>Specify the certificate to use for user authentication. For <client certificate> use the string specified in the Issued To field of the certificate. When using the -cert argument, you must also specify the -url and -r <realm> arguments.</p> <p>To use certificate authentication with the Pulse Launcher program, you must first configure the Pulse server to allow the user to sign in via user certificate authentication. You must also configure a trusted client CA on the Pulse server and install the corresponding client-side certificate in the Web browsers of end-users before running the Pulse Launcher.</p> <p>If the certificate is invalid, the Pulse Launcher displays an error message on the command line and logs a message in the log file.</p> <p>NOTE: If Pulse is launched through a browser, the browser handles certificate verification. If Pulse is launched through an application on Windows, the application handles certificate verification. If Pulse is launched through the Pulse Launcher on Windows, Pulse Launcher handles the expired or revoked client certificates.</p>
-signout	Disconnect and sign out from a specific server. Pulse can have multiple simultaneous connections so the -url argument is required when you use the -signout argument.
-timeout <time in seconds>	The amount of time allowed for the connection to take place before the attempt fails. Min = 45 (default), Max = 600.

The following table lists the possible return codes pulselauncher.exe returns when it exits.

Table 4: Pulse Launcher Return Codes

Code	Description
-1	Pulse is not running.
0	Success.
1	A parameter is invalid.
2	Connection has failed or Pulse is unable to connect to the specified gateway.
3	Connection established with error.
4	Connection does not exist. Example: the command attempts to sign out from a server that was not which has not been added on Pulse UI.
5	User cancelled connection.
6	Client certificate error.
7	Timeout error.
8	No user connection allowed from Pulse UI.

Table 4: Pulse Launcher Return Codes (*continued*)

Code	Description
9	No policy override from Pulse UI.
100	General error.

Examples

The following command is a simple login application that captures the credentials the user enters, and passes the credentials as arguments to `pulselauncher.exe`:

```
pulselauncher.exe -u JDoe -p my$Pass84 -url https://int-company.portal.com/usr -r
Users
pulselauncher return code: 0
```

The following Pulse Launcher example shows a certificate authentication:

```
pulselauncher.exe -url https://int-company.portal.com/usr -cert MyCert -url
https://int-company.portal.com/usr -r Users
pulselauncher return code: 0
```

The following example shows a command to use Pulse Launcher to specify a cookie (`-d`) for a specific Pulse server (`-url`):

```
pulselauncher.exe -d 12adf234nasu234 -url https://int-company.portal.com/usr
pulselauncher return code: 0
```

Related Documentation

- [Using jamCommand to Import Junos Pulse Connections on page 67](#)

Using jamCommand to Import Junos Pulse Connections

The `jamCommand.exe` program is a command line program that imports a `.jnprpreconfig` file into the Pulse client. The `jamCommand` program is available for Windows (XP, Vista, and Win7) and Mac OSX.



NOTE: The working name for Junos Pulse during the early development phase was Juniper Access Manager. Many Pulse filenames, directories, and other Junos Pulse elements include the acronym “jam.”

A `.jnprpreconfig` file includes Pulse connection parameters. You can create a `.jnprpreconfig` file on the Pulse server, and then use it as part of a Pulse installation to ensure that Pulse users have one or more Pulse connections when they start Pulse for the first time.



NOTE: One typical use case for `jamCommand` on a Windows endpoint is to first run `jamCommand` to import one or more Pulse connections from a `.jnprpredong` file, and then run `pulselauncher.exe` to start Pulse.

To install Pulse connections using jamCommand:

1. Create a .jnprpreconfig file on the Pulse server.
In the Pulse server admin console, click **Users > Junos Pulse > Components**.
2. Select the component sets you want, and then click **Download Installer Configuration**.
3. Distribute the .jnprpreconfig file to the Pulse endpoints.
4. Run jamCommand with the .jnprpreconfig file as an option. For example:

On Windows:

```
\Program Files\Common Files\Juniper Networks\JamUI\jamCommand -importfile  
myfile.jnprpreconfig
```

On Mac OSX:

```
/Applications/Junos Pulse/Contents/Plugins/JamUI/jamCommand -importfile  
myfile.jnprpreconfig
```

If the Pulse client is running when you run jamCommand, the new Pulse connection or connections appear immediately. The connection name appears as it was defined when you created the connection in the Pulse server admin console.

**Related
Documentation**

- [Junos Pulse Command-line Launcher on page 64](#)
- [Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 59](#)
- [Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 63](#)

PART 2

Access Management Framework

- [General Access Management on page 71](#)
- [User Roles on page 105](#)
- [Resource Profiles on page 127](#)
- [Virtual Desktop Resource Profiles on page 137](#)
- [Resource Policies on page 143](#)
- [Authentication and Directory Servers on page 153](#)
- [SAML Single Sign-on on page 233](#)
- [Authentication Realms on page 305](#)
- [Sign-In Policies on page 321](#)
- [Single Sign-On on page 335](#)
- [Synchronizing User Records on page 363](#)

CHAPTER 3

General Access Management

- [Access Management Overview on page 71](#)
- [Policies, Rules & Restrictions, and Conditions Overview on page 72](#)
- [Policies, Rules & Restrictions, and Conditions Evaluation on page 74](#)
- [Dynamic Policy Evaluation on page 77](#)
- [Specifying Source IP Access Restrictions on page 79](#)
- [Specifying Browser Access Restrictions on page 82](#)
- [Specifying Certificate Access Restrictions on page 84](#)
- [Specifying Password Access Restrictions on page 85](#)
- [Specifying Session Limits on page 86](#)
- [IF-MAP Federation Overview on page 89](#)
- [IF-MAP Federation Details on page 91](#)
- [Task Summary: Configuring IF-MAP Federation on page 94](#)
- [Configuring IF-MAP Server Settings on page 94](#)
- [Configuring the IF-MAP Federation Client on page 95](#)
- [IF-MAP Federation Network Timing Considerations on page 95](#)
- [Session-Export and Session-Import Policies on page 96](#)
- [Configuring Session-Export Policies on page 98](#)
- [Session-Import Policies on page 100](#)
- [Troubleshooting the IF-MAP Federation Network on page 101](#)
- [Viewing Active Users on the IF-MAP Client on page 101](#)
- [Trusted Server List on page 102](#)

Access Management Overview

The Secure Access Service enables you to secure your company resources using authentication realms, user roles, and resource policies. These three levels of accessibility allow you to control access from a very broad level (controlling who may sign into the Secure Access Service) down to a very granular level (controlling which authenticated users may access a particular URL or file). You can specify security requirements that users must meet to sign in to the Secure Access Service, to gain access to features, and

even to access specific URLs, files, and other server resources. The Secure Access Service enforces the policies, rules and restrictions, and conditions that you configure to prevent users from connecting to or downloading unauthorized resources and content.

To permit endpoints that are not directly connected to a Juniper Networks Security Device to access resources behind the firewall, you can configure a Unified Access Control to provision shared user sessions from any number of different Secure Access Service appliances and Infranet Controllers. IF-MAP Federation allows users to access resources protected by any number of Juniper Networks Firewalls (Infranet Enforcers) without requiring additional authentication.

The Secure Access Service access management framework is available on all Secure Access Service products. The access management features, including realms, roles, resource policies, and servers, are the base of the platform on which all Secure Access Service products are built.

- Related Documentation**
- [User Roles Overview on page 105](#)
 - [Authentication Realm Overview on page 305](#)

Policies, Rules & Restrictions, and Conditions Overview

The Secure Access Service enables you to secure your company resources using authentication realms, user roles, and resource policies. These three levels of accessibility allow you to control access from a very broad level (controlling who may sign into the Secure Access Service) down to a very granular level (controlling which authenticated users may access a particular URL or file).

Accessing Authentication Realms

Resource accessibility begins with the authentication realm. An authentication realm is a grouping of authentication resources, including:

- **An authentication server**—verifies that the user is who he claims to be. The Secure Access Service forwards credentials that a user submits on a sign-in page to an authentication server.
- **An authentication policy**—specifies realm security requirements that need to be met before the Secure Access Service submits a user's credentials to an authentication server for verification.
- **A directory server**—an LDAP server that provides user and group information to the Secure Access Service that the Secure Access Service uses to map users to one or more user roles.
- **Role mapping rules**—conditions a user must meet for the Secure Access Service to map the user to one or more user roles. These conditions are based on either user information returned by the realm's directory server or the user's username.

You can associate one or more authentication realms with the Secure Access Service sign-in page. When more than one realm exists for a sign-in page, a user must specify a realm before submitting her credentials. When the user submits her credentials, the

Secure Access Service checks the authentication policy defined for the chosen realm. The user must meet the security requirements you define for a realm's authentication policy or else the Secure Access Service does not forward the user's credentials to the authentication server.

At the realm level, you can specify security requirements based on various elements such as the user's source IP address or the possession of a client-side certificate. If the user meets the requirements specified by the realm's authentication policy, the Secure Access Service forwards the user's credentials to the appropriate authentication server. If this server successfully authenticates the user, then the Secure Access Service evaluates the role mapping rules defined for the realm to determine which roles to assign to the user.

Accessing User Roles

A role is a defined entity that specifies Secure Access Service session properties for users who are mapped to the role. These session properties include information such as session time-outs and enabled access features. A role's configuration serves as the second level of resource access control. Not only does a role specify the access mechanisms available to a user, but you can also specify restrictions with which users must comply before they are mapped to a role. The user must meet

At the role level, you can specify security requirements based on elements such as the user's source IP address and possession of a client-side certificate. If the user meets the requirements specified either by a role mapping rule or a role's restrictions, then the Secure Access Service maps the user to the role. When a user makes a request to the backend resources available to the role, the Secure Access Service evaluates the corresponding access feature resource policies.

Note that you may specify security requirements for a role in two places—in the role mapping rules of an authentication realm (using custom expressions) or by defining restrictions in the role definition. The Secure Access Service evaluates the requirements specified in both areas to make sure the user complies before it maps the user to a role.

Accessing Resource Policies

A resource policy is a set of resource names (such as URLs, host names, and IP address/netmask combinations) to which you grant or deny access or other resource-specific actions, such as rewriting and caching. A resource policy serves as the third level of resource access control. While a role may grant access to certain types of access features and resources (such as bookmarks and applications), whether or not a user can access a specific resource is controlled by resource policies. These policies may even specify conditions that, if met, either deny or grant user access to a server share or file. These conditions may be based on security requirements that you specify. The user must meet these security requirements or else the Secure Access Service does not process the user's request.

At the resource level, you can specify security requirements based elements such as the user's source IP address or possession of a client-side certificate. If the user meets the requirements specified by a resource policy's conditions, then the Secure Access Service either denies or grants access to the requested resource. You may enable Web access at the role level, for example, and a user mapped to the role may make a Web request.

You may also configure a Web resource policy to deny requests to a particular URL or path when Host Checker finds an unacceptable file on the user's machine. In this scenario, the Secure Access Service checks to see if Host Checker is running and indicates that the user's machine complies with the required Host Checker policy. If the user's machine complies, meaning the unacceptable file is not found, then the Secure Access Service grants the user access to the requested Web resource.

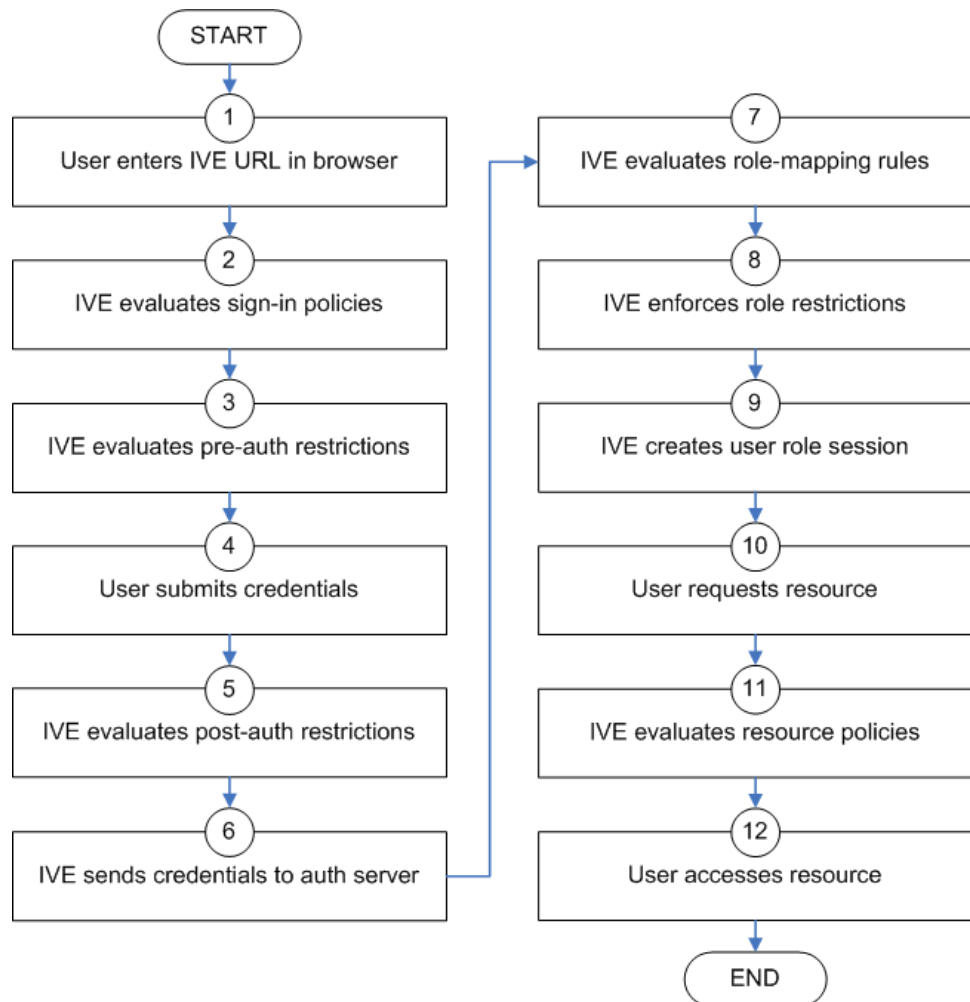
Note that you can create separate resource policies or you can create automatic resource policies (called autopolicies) during resource profile configuration (recommended).

- Related Documentation**
- [Policies, Rules & Restrictions, and Conditions Evaluation on page 74](#)
 - [Dynamic Policy Evaluation on page 77](#)

[Policies, Rules & Restrictions, and Conditions Evaluation](#)

The following diagram illustrates the access management security checks that the Secure Access Service performs when a user tries to access resources through the Secure Access Service. A detailed description of each step follows after the diagram.

Figure 2: Security Checks Performed During a User Session



1. The user enters the URL of the Secure Access Service end-user console (such as <http://employees.yourcompany.com/marketing>) in a Web browser.
2. The Secure Access Service evaluates its sign-in policies (starting with the administrator URLs and continuing to user URLs) until it matches the hostname entered by the user.
3. The Secure Access Service evaluates pre-authentication restrictions and determines if the user's system passes host checks and other requirements. If the pre-authentication checks fail, the Secure Access Service denies the user access. If the checks pass, the Secure Access Service prompts the user to enter the username and password for the realms whose preauthentication checks succeeded. (If required by the realm, the Secure Access Service prompts the user to enter two sets of credentials.) If more than one realm exists, the user must enter a realm or choose one from a list.
4. The Secure Access Service evaluates the post-authentication restrictions and determines whether the user's password conforms to specified limits and requirements. If the postauthentication checks fail, the Secure Access Service denies the user access.

If the checks pass, the Secure Access Service passes the user's credentials to the realm's authentication server.

5. The Secure Access Service forwards the user's username and password to the authentication server, which returns success or failure. (A RADIUS or SiteMinder authentication server also returns attributes for the Secure Access Service to use in role mapping.) If the authentication server returns failure, Secure Access denies the user access. If the server returns success, the Secure Access Service stores the user's credentials. If the realm has a separate LDAP authorization server, the Secure Access Service also queries the LDAP server for attribute and group information and saves the information returned by LDAP. If the realm includes a secondary authentication server, the Secure Access Service repeats this process with the secondary server.
6. The Secure Access Service evaluates the realm's role mapping rules and determines the roles for which the user is eligible. The Secure Access Service determines eligibility using information from the LDAP or RADIUS server or the user's username.
7. The Secure Access Service evaluates the restrictions of the eligible roles, enabling the user to access those roles whose restrictions the user's computer meets. Restrictions may include source IP, browser type, client-side certificate, Host Checker, and Cache Cleaner.
8. The Secure Access Service creates a "session role," determining the user's session permissions. If you enable permissive merging, the Secure Access Service determines session permissions by merging all valid roles and granting the allowed resources from each valid role. If you disable merging, the Secure Access Service assigns the user to the first role to which he is mapped.
9. When the user requests a resource, the Secure Access Service checks whether the corresponding access feature is enabled for the session user role. If not, the Secure Access Service denies the user access. If the access feature is enabled, the evaluates resource policies.
10. The Secure Access Service evaluates resource profiles and policies related to the user's request, sequentially processing each until it finds the profile or policy whose resource list and designated roles match the user's request. The Secure Access Service denies user access to the resource if specified by the profile or policy. Otherwise, the Secure Access Service intermediates the user request if the profile or policy enables access.
11. The Secure Access Service intermediates the user request, forwarding the user's request and credentials (if necessary) to the appropriate server. Then, the Secure Access Service forwards the the server's response to the user.
12. The user accesses the requested resource or application server. The user session ends when the user signs out or his session times out due to time limits or inactivity. The Secure Access Service may also force the user out if the session if you enable dynamic policy evaluation and the user fails a policy.



NOTE: If you enable dynamic policy evaluation, the Secure Access Service performs additional checks beyond the ones mentioned here.

Related Documentation • [Dynamic Policy Evaluation on page 77](#)

Dynamic Policy Evaluation

Dynamic policy evaluation allows you to automatically or manually refresh the assigned roles of users by evaluating a realm's authentication policy, role mappings, role restrictions, and resource policies. When the Secure Access Service performs a dynamic evaluation, it checks whether the client's status has changed. (For instance, the client's Host Checker status may have changed. Or, if the user is roaming, the computer's IP address may have changed.) If the status has changed, the Secure Access Service enables or denies the user access to the dependent realms, roles, or resource policies accordingly.

The Secure Access Service does not check for changes in user attributes from a RADIUS, LDAP, or SiteMinder server when performing dynamic policy evaluation. Instead, the Secure Access Service re-evaluates rules and policies based on the original user attributes that it obtained when the user signed into the Secure Access Service.

Understanding Dynamic Policy Evaluation

During dynamic policy evaluation, the Secure Access Service evaluates the following types of resource policies:

- Windows Secure Application Manager
- Java Secure Application Manager
- VPN Tunneling
- Telnet/SSH
- Terminal Services (Windows and Citrix)
- Java Access
- Code signing (for Java applets)



NOTE: Because the Secure Access Service evaluates Web and Files resource policies whenever the user makes a request for a resource, dynamic policy evaluation is unnecessary for Web and Files. The Secure Access Service does not use dynamic policy evaluation for Meetings resource policies and Email Client resource policies.

If the Secure Access Service determines after a dynamic policy evaluation that a user no longer meets the security requirements of a policy or role, the Secure Access Service terminates the connection immediately with the user. The user may see the closing of a TCP or application connection, or the termination of a user session for VPN Tunneling, Secure Application Manager, Terminal or Telnet/SSH. The user must take the necessary steps to meet the security requirements of the policy or role, and then sign into the Secure Access Service again.

The Secure Access Service logs information about policy evaluation and changes in roles or access in the Event log.

Understanding Standard Policy Evaluation

If you do not use dynamic policy evaluation, the Secure Access Service evaluates policies and roles only when the following events occur:

- When the user first tries to access the Secure Access Service sign-in page, the Secure Access Service evaluates the Host Checker policies (if any) for a realm.
- Immediately after the user's initial authentication, the Secure Access Service evaluates the user's realm restrictions in the authentication policy, role mapping rules, and role restrictions.
- When the user makes a request for a resource, the Secure Access Service evaluates resource access policies to determine if the associated role is allowed to access the resource.
- When the Host Checker status of the user's machine changes, the Secure Access Service evaluates the Host Checker policies (if any) for the role.

If you do not use dynamic policy evaluation and you make changes to an authentication policy, role mapping rules, role restrictions, or resource policies, the Secure Access Service enforces those changes only when the events described above occur.

If you use dynamic policy evaluation, the Secure Access Service enforces changes when the events described above occur, and it also enforces changes at the times you specify.

Enabling Dynamic Policy Evaluation

You can use dynamic policy evaluation in the following ways:

- **Evaluate all signed-in users in a realm**—You can automatically or manually refresh the roles of all currently signed-in users of a realm by using the General tab of the Administrators > Admin Realms > Select Realm or Users > User Realms > Select Realm page. You can trigger the Secure Access Service to perform a dynamic policy evaluation at the realm level based on:
 - **An automatic timer**—You can specify a refresh interval that determines how often the Secure Access Service performs an automatic policy evaluation of all currently signed-in realm users, such as every 30 minutes. When using the refresh interval, you can also fine-tune the Secure Access Service performance by specifying whether or not you want to refresh roles and resource policies as well as the authentication policy, role mapping rules, and role restrictions.
 - **On-demand**—At any time, you can manually evaluate the authentication policy, role mapping rules, role restrictions, and resource policies of all currently signed-in realm users. This technique is especially useful if you make changes to an authentication policy, role mapping rules, role restrictions, or resource policies and you want to immediately refresh the roles of a realm's users.

- **Evaluate all signed-in users in all realms**—At any time, you can manually refresh the roles of all currently signed-in users in all realms by using settings in the System > Status > Active Users page.
- **Evaluate individual users**—You can automatically refresh the roles of individual users by enabling dynamic policy evaluation for Host Checker on the Authentication > Endpoint Security > Host Checker page. Host Checker can trigger the Secure Access Service to evaluate resource policies whenever a user's Host Checker status changes. (If you do not enable dynamic policy evaluation for Host Checker, the Secure Access Service does not evaluate resource policies but it does evaluate the authentication policy, role mapping rules, and role restrictions whenever a user's Host Checker status changes.)

Related Documentation

- [Monitoring Active Users on page 955](#)

Specifying Source IP Access Restrictions

This topic describes options to enforce source IP restrictions for access to the corporate network or intranet resources. It includes the following information:

- [About Source IP Restrictions on page 79](#)
- [Specifying Source IP Restrictions at the Realm Level on page 80](#)
- [Specifying Source IP Restrictions at the Role Level on page 80](#)
- [Specifying Source IP Restrictions in Resource Policies on page 81](#)

About Source IP Restrictions

You can enforce access rules based on the source IP address of the request. You can configure rules related to sign-in, role-mapping, and resource access.

At the realm level, you can add source IP rules to the realms associated with sign-in pages. The user must sign in from a host with an IP address that is allowed by the source IP requirements for the authentication realm. If the source IP policy does not allow the host to access the realm, the Secure Access Service does not forward the user's credentials to the authentication server, and the user is denied access. You can set up multiple rules. For example, you can deny access to all users on a wireless network (10.64.4.100), and allow access to all other network users (0.0.0.0).

At the user role level, you can add source IP rules to the criteria that determine user role membership. If the source IP rule disqualifies a user from a role, subsequent role mapping rules are consulted.

In resource policies, you can add allow/deny rules based on source IP.

Specifying Source IP Restrictions at the Realm Level

To specify source IP restrictions:

1. Navigate to the administrator or user realm you want to configure:
 - **Administrators > Admin Realms > *Realm***
 - **Users > User Realms > *Realm***
2. Select **Authentication Policy > Source IP** to display the Source IP policy configuration page.
3. Choose one of the following options:
 - **Allow users to sign in from any IP address**—Essentially, this option turns off source IP restrictions.
 - **Allow or deny users from the following IP addresses**—Specifies source IP restrictions. If you select this option, use the policy table controls to create source IP rules.
4. Add a rule to the table:
 - a. Use the text boxes to specify source IP address match criteria:
 - For IPv4 clients, enter IPv4 address and netmask pairs.
 - For IPv6 clients, enter IPv6 address and prefix length pairs.
 - b. Use the Allow and Deny option buttons to specify the action when a rule matches.
 - c. Click **Add** to add the rule to the table.
 - d. Use the selection box and arrow buttons to order the list. Move the highest priority restrictions to the top of the list. For example, to deny access to all users on a wireless network (10.64.4.100) and allow access to all other network users (0.0.0.0), move the wireless network address (10.64.4.100) to the top of the list and move the (0.0.0.0) network below the wireless network.
5. Save the configuration.

Specifying Source IP Restrictions at the Role Level

To specify source IP restrictions:

1. Navigate to the administrator or user role you want to configure:
 - **Administrators > Admin Roles > *Role***
 - **Users > User Roles > *Role***
2. Select **General > Restrictions > Source IP** to display the Source IP policy configuration page.
3. Choose one of the following options:

- **Allow users to sign in from any IP address**—Essentially, this option turns off source IP restrictions.
 - **Allow or deny users from the following IP addresses**—Specifies source IP restrictions. If you select this option, use the policy table controls to create source IP rules.
4. Add a rule to the table:
 - a. Use the text boxes to specify source IP address match criteria:
 - For IPv4 clients, enter IPv4 address and netmask pairs.
 - For IPv6 clients, enter IPv6 address and prefix length pairs.
 - b. Use the Allow and Deny option buttons to specify the action when a rule matches.
 - c. Click **Add** to add the rule to the table.
 - d. Use the selection box and arrow buttons to order the list. Move the highest priority restrictions to the top of the list. For example, to deny access to all users on a wireless network (10.64.4.100) and allow access to all other network users (0.0.0.0), move the wireless network address (10.64.4.100) to the top of the list and move the (0.0.0.0) network below the wireless network.
 5. Save the configuration.

Specifying Source IP Restrictions in Resource Policies

A third way to use source IP restrictions is by creating custom rules in resource policies. The action for custom rules is either allow or deny. The match criteria include resources and conditions. One of the conditions you can set is source IP, so you can enforce source IP restrictions through resource policies. For example:

1. Navigate to **Users > Resource Policies**.
2. Select a policy. Click **Web Access Policies**, for example, to display its policies list.
3. Click the **Initial Policy for Local Resources** policy to edit it.
4. Click the **Detailed Rules** tab.
5. Under Conditions, expand the Prebuilt Conditions list, expand the **SourceIPStr** selections, select one of the example expressions, such as **SourceIPStr = "192.168.10.0/24"** or **SourceIPStr = "2001:DB8::15"**, and click **Insert Expression** to add the string to the Conditions box.
6. Modify the IP address. In other words, replace **192.168.10.0/24** with an IPv4 address / netmask pair; replace **2001:DB8::15** with an IPv6 address.
7. Specify the other match condition (resource) and specify the action (allow or deny).
8. Save the configuration.

Related Documentation

- [Role Restrictions on page 110](#)
- [Creating an Authentication Realm on page 306](#)

- [Specifying Browser Access Restrictions on page 82](#)
- [Specifying Certificate Access Restrictions on page 84](#)
- [Specifying Password Access Restrictions on page 85](#)
- [Configuring Host Checker Restrictions on page 414](#)

Specifying Browser Access Restrictions

Use a browser restriction to control from which Web browsers users can access a Secure Access Service sign-in page or be mapped to a role. If a user tries to sign in to the Secure Access Service using an unsupported browser, the sign-in attempt fails and a message displays stating that an unsupported browser is being used. This feature also enables you to ensure that users sign in to the Secure Access device from browsers that are compatible with corporate applications or are approved by corporate security policies.

You can restrict Secure Access Service and resource access by browser-type:

- **When administrators or users try to sign in to the Secure Access Service**—The user must sign in from a browser whose user-agent string meets the specified user-agent string pattern requirements for the selected authentication realm. If the realm “allows” the browser’s user-agent string, then the Secure Access Service submits the user’s credentials to the authentication server. If the realm “denies” the browser’s user-agent string, then the Secure Access Service does not submit the user’s credentials to the authentication server.
- **When administrators or users are mapped to a role**—The authenticated user must be signed in from a browser whose user-agent string meets the specified user-agent string pattern requirements for each role to which the Secure Access Service may map the user. If the user-agent string does not meet the “allowed” or “denied” requirements for a role, then the Secure Access Service does not map the user to that role.
- **When users request a resource**—The authenticated, authorized user must make a resource request from a browser whose user-agent string meets the specified “allowed” or “denied” requirements for the resource policy corresponding to the user’s request. If the user-agent string does not meet the “allowed” or “denied” requirements for a resource, then the Secure Access Service does not allow the user to access the resource.

The browser restrictions feature is not intended as a strict access control since browser user-agent strings can be changed by a technical user. It serves as an advisory access control for normal usage scenarios.

To specify browser restrictions:

1. Select the level at which you want to implement browser restrictions:
 - **Realm level**—Navigate to:
 - **Administrators > Admin Realms > *Select Realm* > Authentication Policy > Browser**
 - **Users > User Realms > *Select Realm* > Authentication Policy > Browser**
 - **Role level**—Navigate to:

- **Administrators > Admin Realms > Select Realm > Role Mapping > Select|Create Rule > Custom Expressions**
- **Administrators > Admin Roles > Select Role > General > Restrictions > Browser**
- **Users > User Realms > Select Realm > Role Mapping > Select|Create Rule > Custom Expression**
- **Users > User Roles > Select Role > General > Restrictions > Browser**

2. Choose one of the following options:

- **Allow all users matching any user-agent string sent by the browser**— Allows users to access the Secure Access Service or resources using any of the supported Web browsers.
- **Only allow users matching the following User-agent policy**—Allows you to define browser access control rules. To create a rule:
 - a. For the User-agent string pattern, enter a string in the format

`*<browser_string>*`

 where start (*) is an optional character used to match any character and <browser_string> is a case-sensitive pattern that must match a substring in the user-agent header sent by the browser. Note that you cannot include escape characters (\) in browser restrictions.
 - b. Select either:
 - **Allow** to allow users to use a browser that has a user-agent header containing the <browser_string> substring.
 - **Deny** to prevent users from using a browser that has a user-agent header containing the <browser_string> substring.
 - c. iii. Click **Add**.

3. Click **Save Changes** to save your settings.

Rules are applied in order, so the first matched rule applies.

Literal characters in rules are case sensitive, and spaces are allowed as literal characters.

For example, the string `*Netscape*` matches any user-agent string that contains the substring Netscape.

The following rule set grants resource access only when users are signed in using Internet Explorer 5.5x or Internet Explorer 6.x. This example takes into account some major non-IE browsers that send the 'MSIE' substring in their user-agent headers:

`*Opera*Deny`

`*AOL*Deny`

`*MSIE 5.5*Allow`

`*MSIE 6.*Allow`

* Deny

Specifying Certificate Access Restrictions

When you install a client-side certificate on the Secure Access Service through the System > Configuration > Certificates > Trusted Client CAs page of the admin console, you can restrict Secure Access Service and resource access by requiring client-side certificates:

- **When administrators or users try to sign in to the Secure Access Service**—The user must sign in from a machine that possesses the specified client-side certificate (from the proper certificate authority (CA) and possessing any optionally specified field/value pair requirements). If the user's machine does not possess the certificate information required by the realm, the user can access the sign-in page, but once the Secure Access Service determines that the user's browser does not possess the certificate, the Secure Access Service does not submit the user's credentials to the authentication server and the user cannot access features on the Secure Access Service.

To implement certificate restrictions at the realm level, navigate to:

- **Administrators > Admin Realms > *SelectRealm* > Authentication Policy > Certificate**
- **Users > User Realms > *SelectRealm* > Authentication Policy > Certificate**
- **When administrators or users are mapped to a role**—The authenticated user must be signed in from a machine that meets the specified client-side certificate requirements (proper certificate authority (CA) and optionally specified field/value pair requirements) for each role to which the Secure Access Service may map the user. If the user's machine does not possess the certificate information required by a role, then the Secure Access Service does not map the user to that role.
 - **Administrators > Admin Roles > *SelectRole* > General > Restrictions > Certificate**
 - **Users > User Realms > *Select Realm Role Mapping* > *Select|CreateRule* > *CustomExpression***
 - **Users > User Roles > *SelectRole* > General > Restrictions > Certificate**
- **When users request a resource**—The authenticated, authorized user must make a resource request from a machine that meets the specified client-side certificate requirements (proper certificate authority (CA) and optionally specified field/value pair requirements) for the resource policy corresponding to the user's request. If the user's machine does not possess the certificate information required by a resource, then the Secure Access Service does not allow the user to access the resource.
 - **Users > Resource Policies > *SelectResource* > *SelectPolicy* > Detailed Rules *Select|CreateRule* > *ConditionField***

Related Documentation

- [Dynamic Policy Evaluation on page 77](#)

Specifying Password Access Restrictions

You can restrict Secure Access Service and resource access by password-length when administrators or users try to sign in to the Secure Access Service. The user must enter a password whose length meets the minimum password-length requirement specified for the realm. Note that local user and administrator records are stored in the Secure Access Service authentication server. This server requires that passwords are a minimum length of 6 characters, regardless of the value you specify for the realm's authentication policy.

To specify password restrictions:

1. Select an administrator or user realm for which you want to implement password restrictions.

Navigate to:

- **Administrators > Admin Realms > Select Realm > Authentication Policy > Password**
- **Users > User Realms > Select Realm > Authentication Policy > Password**

2. Choose one of the following options:

- **Allow all users (passwords of any length)** — Does not apply password length restrictions to users signing in to the Secure Access Service.
- **Only allow users that have passwords of a minimum length** — Requires the user to enter a password with a minimum length of the number specified.



NOTE: This option is not applicable for IKEv2 users and therefore is not enforced for IKEv2 users.

3. Select **Enable Password Management** if you want to enable password management. You must also configure password management on the Secure Access Service authentication server configuration page (local authentication server) or through an LDAP server. For more information about password management,
4. If you have enabled a secondary authentication server, specify password length restrictions using the restrictions above as a guideline.
5. Click **Save Changes** to save your settings.

By default, the Secure Access Service requires that user passwords entered on the sign-in page be a minimum of four characters. The authentication server used to validate a user's credentials may require a different minimum length. The Secure Access Service local authentication database, for example, requires user passwords to be a minimum length of six characters.

Related Documentation

- [Dynamic Policy Evaluation on page 77](#)

Specifying Session Limits

In addition to the access management options you may specify for an authentication policy, you may also specify a limit for concurrent users. A user who enters a URL to one of this realm's sign-in pages must meet any access management and concurrent user requirements specified for the authentication policy before the Secure Access Service presents the sign-in page to the user.

Setting the minimum or maximum setting limit amount allows you to configure realms that are more likely to be available when the Secure Access Service is nearing the amount of licensed users.

Valid numbers for the minimum amount of sessions are between 0 and the license limit. A default of 0 means there are no limits. All of the realms minimum limits can add up to the license limit but cannot exceed it. You cannot modify an existing realm's minimum limit or add a new realm's minimum limit that exceeds the license limit. The maximum limit can be equal to or greater than the minimum limit for a particular realm. Value 0 for maximum limit means no user can log in to the realm.

You can also limit the number of concurrent users per session; a user can have multiple sessions. For example, if a user logs in from two machines in the same realm, an additional session is created. Each session counts towards the user license.

Users who enter through a realm with this feature enabled must have no more than the specified number of sessions open. If the user attempts to open a new session that exceeds the limit, a message appears and gives the user the option to continue or cancel.

When considering concurrent users per session, make note of the following:

- All session-related SSO attributes are saved in their respective session in the cache. These attributes are not shared with other sessions.
- All form-related SSO attributes are saved in their respective session in the cache. These attributes are not shared with other sessions.
- All Form-SSO related attributes will be saved in its respective session in the cache. The Form SSO state will not be shared with other sessions. The admin configured Form SSO values will be shared across all sessions.
- End-user's home page changes are reflected across all sessions. Any changes to the following will appear in the other concurrent sessions:
 - Bookmarks
 - Panel sorting (Preferences > User Home)
 - Email information, Daylight Saving Time, Junos Pulse Collaboration (Preferences > General)
 - Autostart Client Application Session session (Preferences > Applications)
 - Cached Email Info settings (Preferences > Advanced)

- Delete Cookies (Preferences > Advanced) now has options to let you remove cookies from the current session only or to remove cookies from all sessions.
- Delete Password (Preferences > Advanced) now has options to let you remove passwords from the current session only or to remove passwords stored by all sessions.
- Cache Cleaner and Host Checker information is saved in each session. They are not shared across concurrent sessions
- Log messages will contain session identifiers (concatenated at the end of the log message) to differentiate which session the message refers to.
- Only one session can host a scheduled meeting. users can not launch multiple scheduled meetings from concurrent sessions.
- Users can attend meetings from any sessions. However, since only one meeting client can be run per system, if a user wishes to attend more than one meeting, they must attend the other meetings from a different end-user system.
- Meeting host passes from one session to the other when you log out of a session. For example, suppose you are the meeting host, you join the meeting in user session A and then join the meeting again with user session B. User session A retains the meeting host. However, if you are the meeting host from user session A, exit the meeting from user session A and then join the meeting in user session B then user session B assumes the meeting host role.
- Each user session maintains its own VPN Tunneling information. This information is not shared between concurrent sessions. However, administrator network connect sessions are shared between concurrent sessions.
- If you log in to the Secure Access Service as administrator, the first session is edit mode. If you log in as an administrator in a concurrent session, that administrator is logged in as read-only mode.
- VPN Tunneling bandwidth allocation is enforced on a per-session basis. For example, if a user is allocated a 1M bandwidth then each user session has a 1M bandwidth. The total bandwidth for this user is the number of sessions of this user times 1M.
- Users can launch terminal services, JSAM or WSAM from any session. Session information is saved per each session, they are not shared across concurrent sessions. Multiple instances of terminal services, JSAM and WSAM can not be started on the same client.
- If a user has concurrent sessions and starts the email client from multiple sessions, the email client from the last session is the only one that can access the backend email server through Secure Access Service. For example, if a user has two concurrent sessions and starts the email client from both sessions, only the second session can access the email server.



NOTE: If you enable the multiple sessions per user feature, IKEv2 clients and VPN Tunneling clients may not be assigned the same IP address. For example, an IKEv2/VPN Tunneling client may be assigned a different VPN Tunneling VIP address each time they connect to the Secure Access Service when the Secure Access Service is obtaining the DHCP addresses from a DHCP server.

Use limits restrictions to set minimum and maximum concurrent users on the realm.

To specify the number of concurrent users limit restrictions:

1. Select an administrator or user realm for which you want to implement limits restrictions.
 - **Administrators > Admin Realms > *SelectRealm* Authentication Policy > Limits**
 - **Users > User Realms > *SelectRealm* > Authentication Policy > Limits**
2. To limit the number of concurrent users on the realm, select **Limit the number of concurrent users** and then specify limit values for these options:
 - **Guaranteed minimum**—You can specify any number of users between zero (0) and the maximum number of concurrent users defined for the realm, or you can set the number up to the maximum allowed by your license if there is no realm maximum.
 - **Maximum (optional)**—You can specify any number of concurrent users from the minimum number you specified up to the maximum number of licensed users. If you enter a zero (0) into the Maximum field, no users are allowed to login to the realm.
3. Click **Save Changes**.

To specify the number of concurrent users per session limit restriction:

1. Select **Authentication > Signing In > Sign-in Policies**.
2. Select the **Display open user session[s] warning notification** checkbox to determine when to display a message to the user. By displaying this message, users can log out of one of their existing sessions before continuing with the current log in if they have already met the maximum session count.

If you do not select this checkbox and the user attempts to log in when their maximum session count has already been met, the Secure Access Service terminates the session that has been idle the longest.

- Select **Always** to notify the user each time they log in when they already have another active session
 - Select **If the maximum session has been exceeded** to display the warning message only when the user's maximum session count has been met.
3. Select the **Enable multiple user sessions** checkbox.
 4. Select **Users > User Realms > *RealmName* > Authentication Policy > Limits**.

5. Specify the number of sessions permitted for users in the **Maximum number of sessions per user** text box.
6. Click **Save Changes**.



NOTE: If you do not select the **Enable multiple user sessions** checkbox, only one session per user is allowed regardless of the value you specify in the **Maximum number of sessions per user** text box.

Related Documentation

- [Dynamic Policy Evaluation on page 77](#)

IF-MAP Federation Overview

You can configure a Juniper Networks Unified Access Control (UAC) Infranet Controller to store user session information for other Infranet Controllers and Secure Access Services. Federation allows users to authenticate to a single Secure Access Service or Infranet Controller, and then access resources that are protected by any number of Juniper Networks firewall devices known as Infranet Enforcers that are controlled by different Infranet Controllers. Federation enhances network performance. If a user is required to login to multiple Secure Access Services or Infranet Controllers during the course of a day to access different resources, each device must perform authentication and Host-Checking, often with periodic Host Checker updates throughout the day. The overhead can lead to decreased performance not only on the devices, but also on the network and the endpoint. Imported IF-MAP sessions eliminate redundant logins and Host Checks.

Federation on the Secure Access Service uses the standard IF-MAP (Interface for Metadata Access Point) protocol to share session information and other data between connected devices over distributed networks. IF-MAP is a protocol defined by the Trusted Network Connect Working Group (TNC-WG) as a standard interface between different network elements and devices. Federation is accomplished using an IF-MAP server and IF-MAP clients.

It is important as an administrator to understand the fundamental underlying communication method for data transmission in a Federation network over IF-MAP. Policies that you configure on the Secure Access Service permit this communication.

In a federated network, the IF-MAP server functions as the repository, or data store for IF-MAP clients to use for publishing information regarding activity on the network. For example, Secure Access Service IF-MAP clients can publish information about sessions on the network, and Juniper Networks IDP devices can communicate information about potential threats to the IF-MAP client for publishing. IF-MAP clients can search for information about sessions or threats, and an IF-MAP client can establish a subscription so the IF-MAP server notifies the client when other clients publish new or changed information. In addition, IF-MAP clients can purge data that is no longer valid. All transactions are initiated by the IF-MAP client.

IF-MAP Federation is not supported for non-root IVSes on the Secure Access Service.

IF-MAP Federation is available on all Secure Access Services with version 6.4 or greater. No licensing is required.

1. The endpoint authenticates through the IF-MAP client (Secure Access Service). The IF-MAP client publishes session information to the IF-MAP server.
2. The endpoint attempts to access protected resources that are behind the Infranet Enforcer.
3. The Infranet Enforcer notifies the Infranet Controller (also an IF-MAP client). The IF-MAP client searches for session information on the IF-MAP server.
4. The Infranet Controller subscribes to session information about the endpoint's IP address.
5. The Infranet Controller notifies the Infranet Enforcer that session information exists for the IP address attempting to access resources, and the Infranet Enforcer provisions an auth table entry.
6. Access is granted to the protected resources. If any session information about the user changes, the authenticating IF-MAP client publishes the new information. Having subscribed to the user's session information, the Infranet Controller will be aware of any changes and provision access in accordance with the changed session information.

For details about configuring the Secure Access Service to work in an IF-MAP Federated network with the Infranet Controller, see IF-MAP Federation.

IF-MAP Federation Workflow

Configuring an IF-MAP federated network requires coordination between administrators of the different devices that will be in the federated network.

This document describes IF-MAP deployments that include only Juniper Networks devices: Infranet Controllers, Secure Access Services, Infranet Enforcer firewalls, and Juniper Networks IDP. For implementations that incorporate third-party components, contact Juniper Networks Technical Support.

The mix of devices in the federated network is important when planning the network. Will your network consist of only Infranet Controllers, or will you incorporate Secure Access Services? Do the devices in your network have similar role mapping policies, or is each device different?

Determine and understand your goals for the federated network. The big picture guides your implementation as it becomes more complex. Juniper Networks recommends that you begin slowly. For example, start with a single role on each device, and then build the network incrementally.

In the simplest model, you can use the default policies. Using this model, you can quickly establish a federated network, and session information will automatically be shared among distributed devices in the network. This simple model should be adequate for most implementations in which the devices in the federated network have identical or very similar role mapping policies.

If your configuration requires more complex policies, you will need to perform a number of tasks to achieve your intended results. The following guidelines will help you plan your workflow:

- Ensure that communications between IF-MAP servers and IF-MAP clients is established
- Determine the resources that will be shared among the different devices
- Define who can access specific resources
- Distribute resources and users into roles
- Establish a naming convention that is shared and implemented between all administrators and devices
- Create Session-Export and Session-Import policies that reflect the role designations that you have configured on the devices

**Related
Documentation**

- [IF-MAP Federation Details on page 91](#)
- [Task Summary: Configuring IF-MAP Federation on page 94](#)

IF-MAP Federation Details

You can configure the Secure Access Service as an IF-MAP client for an IF-MAP server. You configure an Infranet Controller as an IF-MAP server. Any endpoint sessions with an IP address created on an IF-MAP server are automatically published to that IF-MAP server.

You can create source IP policies for endpoints that authenticate to the Secure Access Service to permit access to resources behind Infranet Enforcers (ScreenOS Enforcers and JUNOS Enforcers). Session-Export policies that you configure on the IF-MAP clients allow the clients to publish endpoint user data to the IF-MAP server. Secure Access Services that are IF-MAP clients can subscribe to the information on an IF-MAP server.

When a user accesses the Secure Access Service that is configured as an IF-MAP client, the client publishes basic session information, including the IP address, user name and roles, to the IF-MAP server. The server stores the information as metadata. Other IF-MAP clients in the network can poll the server for metadata when session information is needed as a result of an endpoint attempting to access protected resources behind an Infranet Enforcer.

When an authenticated user from the Secure Access Service that is configured as an IF-MAP client attempts to access resources that are protected by an Infranet Enforcer for an Infranet Controller that is also configured as an IF-MAP client, the Infranet Controller automatically provisions an auth table entry for the user on the Infranet Enforcer to allow access without requiring the user to authenticate to the Infranet Controller.

The Infranet Enforcer as an IF-MAP client subscribes to session information and other data for the endpoint based on the originating IP address. The authenticating Secure Access Service (the original IF-MAP client) publishes any changes in session parameters to the IF-MAP server. Since the Infranet Controller that is protecting the accessed

resources subscribes to the metadata on the Federation server, session information is always current.

The Infranet Enforcer allows or denies traffic based on the resource access policies that are configured on the Infranet Controller to which it is connected.

You configure server settings on the Infranet Controller that will be the IF-MAP server. You configure client settings on each of the Secure Access Services and Infranet Controllers and that will be connected in the network.

In addition to the server and client settings, you configure Session-Export policies on Secure Access Services and Infranet Controllers that are IF-MAP clients. You configure and Session-Import policies on Infranet Controller IF-MAP clients that are connected to Infranet Enforcers.

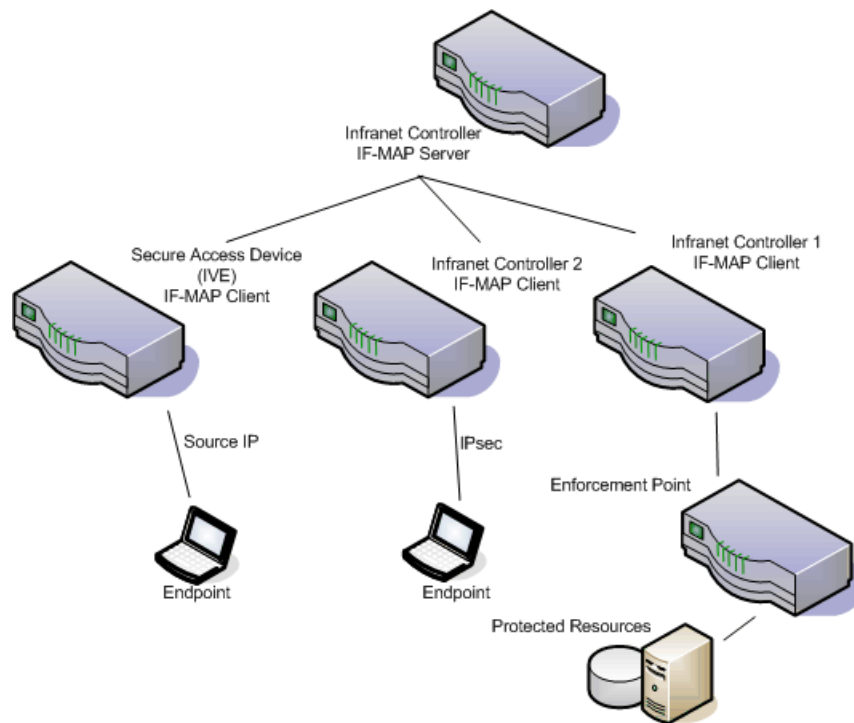
IF-MAP allows servers and clients to publish, search, poll, and subscribe to data within a network of IF-MAP servers and clients. All of the data from the Secure Access Services in the network that is published to the IF-MAP server uses the IF-MAP protocol. Session-Export and Session-Import policies that you configure on the Secure Access Service and Infranet Controller allow the devices to utilize the IF-MAP protocol to share session information.

Session-Export policies specify how to translate an endpoint's session on the Secure Access Service or the Secure Access Service into IF-MAP data. To translate session information into IF-MAP data, you enter detailed user information. The Secure Access Service evaluates the Export policies to determine a session's IF-MAP roles, capabilities, identities, and device attributes and publishes the data to the IF-MAP server.

The Session-Import policies that you configure on the Secure Access Service specify how the device should derive a username and a set of roles based on IF-MAP data that it receives from the IF-MAP server from other Secure Access Services. Import policies are similar to Role Mapping policies on a realm. You must be precise when configuring Export and Import policies, otherwise roles cannot be assigned properly.

The following figure depicts a scenario in which there are two Infranet Controllers configured as IF-MAP clients, one Secure Access Service configured as a IF-MAP client, and another Infranet Controller configured as the IF-MAP server. Endpoints that authenticate through any of the IF-MAP clients can access protected resources behind the enforcement point attached to Infranet Controller 1.

Figure 3: Federation IF-MAP Topology



The interaction between the endpoints, the clients and the server is as follows:

- An endpoint authenticates through the Secure Access Service depicted in the figure and starts VPN Tunneling or Junos Pulse.
- The Secure Access Service provisions an IP address for the endpoint to use on the internal network. Once the endpoint's IP address on the internal network is known, the Secure Access Service derives IF-MAP data from the endpoint's session.
- The Secure Access Service IF-MAP client publishes the session information as IF-MAP data to the IF-MAP server using Session-Export policies.
- When the user attempts to access resources behind the enforcement point, access is blocked since the Infranet Enforcer has no information about the endpoint. The Infranet Enforcer sends out a dynamic discovery message that includes the endpoint's source IP address.
- Infranet Controller 1 uses the IP address to retrieve session data from the IF-MAP server.
- The Infranet Controller uses Session-Import policies to retrieve session data from the IF-MAP server.

The endpoint authenticating to the Secure Access Service must be running VPN Tunneling.

Imported user sessions do not count against the maximum user count for either platform, as each user is counted on the Secure Access Service from which they authenticated.

For details on configuring an IF-MAP Federation network, see IF-MAP Federation.

IF-MAP Logging

IF-MAP related events are logged on both the IF-MAP server and the IF-MAP client.

Task Summary: Configuring IF-MAP Federation

The tasks listed in this topic are performed by an Access Control Service administrator, in conjunction with an administrator for the Secure Access Service. On the Secure Access Service, you configure Session-Export policies and you configure IF-MAP client settings. For details on configuring an IF-MAP Federation network, see IF-MAP Federation.

To use IF-MAP Federation, perform the following tasks on the Access Control Service and Secure Access Service:

1. Enable dynamic auth table provisioning on any connected Infranet Enforcers that you want to use with Federation.
2. On the Infranet Controller, configure IF-MAP server settings to permit the server to communicate with IF-MAP clients.
3. Configure IF-MAP client settings to permit clients to communicate with the IF-MAP server.
4. On the Access Control Service and Secure Access Service, coordinate Session-Import policies, Session-Export policies, roles, and resource access policies between all of the clients in the Federated network.
5. Configure Session-Export policies on Secure Access Services to define how sessions are translated into IF-MAP data.
6. Configure Session-Import policies on Secure Access Services that correspond with Export policies to translate IF-MAP data into Secure Access Service roles.
7. On the Infranet Controller, configure Source IP policies for Secure Access Service users who will use Source IP to access the network.

Related Documentation

- [Configuring IF-MAP Server Settings on page 94](#)
- [Configuring the IF-MAP Federation Client on page 95](#)
- [Session-Export and Session-Import Policies on page 96](#)
- [Troubleshooting the IF-MAP Federation Network on page 101](#)

Configuring IF-MAP Server Settings

You must add all IF-MAP clients to the Secure Access Service IF-MAP server. To add clients, you must specify the IP address and the security mechanism and credentials for the client.

For details on configuring an IF-MAP server, see IF-MAP Federation.

Related Documentation • [Troubleshooting the IF-MAP Federation Network on page 101](#)

Configuring the IF-MAP Federation Client

You must identify the IF-MAP server to each Secure Access Service IF-MAP client. To add the server, you specify the IF-MAP URL of the server and how to authenticate to the server. Match the URL and security settings to equal those on the IF-MAP server(s) to which the IF-MAP client will connect.

To configure IF-MAP client settings on the Secure Access Services that will be IF-MAP clients:

1. From the admin console select **System > IF-MAP Federation > Overview**.
2. Select the Enable IF-MAP Client option button.
3. Type the Server URL for IF-MAP Web service on the IF-MAP server. Append the server URL with **/dana-ws/soap/dsifmap** for all Juniper Networks IF-MAP servers.
4. Select the Client Authentication Method: Basic or Certificate.
 - a. If you select Basic, enter a Username and Password. This is the same as the information that was entered on the IF-MAP server.
 - b. If you select Certificate, select the Device Certificate to use.
 - c. Ensure that the certificate of the CA that signed the IF-MAP server certificate is added from the System > Configuration > Certificates > Trusted Server CA page.

The IF-MAP client validates the IF-MAP server certificate: if validation fails, the connection fails. Ensure that the hostname in the IF-MAP URL on the client machine matches the hostname of the server certificate on the IFMAP server, and that the CA that signed the server certificate is configured as a trusted server CA on the IF-MAP client.
5. Click **Save Changes**.

Related Documentation • [Configuring IF-MAP Server Settings on page 94](#)

IF-MAP Federation Network Timing Considerations

It is important that the time on all IF-MAP servers is correct, as timeout issues are critical to ensure that IF-MAP provides complete and timely information. The IF-MAP Federation is designed to fail secure. If any component in the network does not receive timely information, the IF-MAP metadata will be purged from the data stores.

The components are designed to fail-secure. If complete and timely information can not be provided, a user's session will be deleted. For example, if the chain of connections between an IF-MAP client that publishes a session and a client that grants access to a resource breaks, the client that granted access will remove the session. The fail-secure time limit is three minutes.

The timeout limit for IF-MAP is three minutes and applies to the following events:

- An IF-MAP server (or cluster) loses contact with one of its IF-MAP clients
- An IF-MAP server (or cluster) loses contact with one of its IF-MAP clients
- An IF-MAP server (cluster) loses contact with one of the other IF-MAP server (clusters) in the IF-MAP federation
- A Juniper IF-MAP client loses contact with its IF-MAP server (cluster) for too long

Related Documentation

- [Configuring IF-MAP Server Settings on page 94](#)
- [Configuring the IF-MAP Federation Client on page 95](#)
- [Session-Export and Session-Import Policies on page 96](#)
- [Troubleshooting the IF-MAP Federation Network on page 101](#)

Session-Export and Session-Import Policies

You configure Session-Export policies on all of the Secure Access Services and Infranet Controllers in the Federation network that are IF-MAP clients. These policies allow IF-MAP clients to translate outgoing session information into IF-MAP data and incoming IF-MAP data into session information. These translations enable sessions to be shared between Secure Access Services and Infranet Controllers even if the devices sharing sessions have different role configurations.

To accurately configure Session-Export and Session-Import policies you need a minimal understanding of IF-MAP identifiers and IF-MAP metadata. An identifier is a unique value required for all metadata operations. Each instance of metadata is associated with an identifier. Examples of identifiers include access-request, identity, IP address, and MAC address. Examples of metadata include capability, role, and device-attribute.

IF-MAP recognizes two metadata types that are similar to roles on the Secure Access Service: IF-MAP roles and IF-MAP capabilities. An IF-MAP role is an attribute assigned to a user in the organization. When IF-MAP metadata is published to the IF-MAP server, this information could be one way to identify individuals on the network. This is somewhat different from the concept of roles on the Secure Access Service. An IF-MAP capability is closer to the concept of a role on the Secure Access Service. An IFMAP capability is a collection of privileges assigned as a result of an access request. This is more analogous to the Secure Access Service role since they are derived through role mapping in an authentication realm.

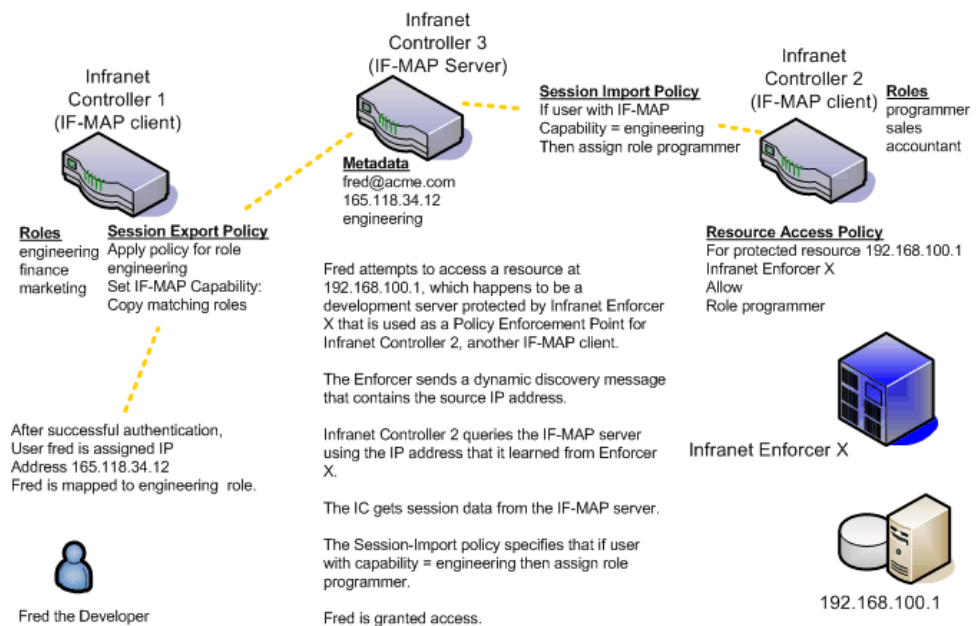
The data that is published to the IF-MAP server about a user session is derived by applying the Session-Export policies to the user session. The Session-Import policies are applied to the data from the IF-MAP server to assign a set of roles to the user.

When an endpoint attempts to access protected resources associated with the Secure Access Service, the device queries the IF-MAP server for data. The Infranet Controller uses Session- Import policies to derive roles and a user name from the IF-MAP data. For example, you could configure a Session-Import policy that looks for a specific Host

Checker policy (you specify the Host Checker policy in the Session-Import policy). If the Infranet Controller finds a match (in this case the Host Checker device attribute), the user can be assigned a role specified in the Session-Import policy.

All of the administrators who are configuring devices in the IF-MAP Federation network must agree on a set of capabilities, roles and device attributes and their meanings to be used with IF-MAP. Then, each administrator configures their device to map between local sessions and IF-MAP data. The following figure illustrates a coordinated IF-MAP Federated network configuration with policies that permit an example user to access protected resources.

Figure 4: Session-Import and Session-Export Policies



To further your understanding of Session-Import and Session-Export policies, please note the following Juniper Networks IF-MAP conventions:

- the Secure Access Service maps to the identical IF-MAP username.
- A role on the Secure Access Service is paired with an IF-MAP capability.
- Capabilities can have the same name as the roles they are paired with, or a different name.
- When different IF-MAP clients have different but equivalent role names (e.g. Legal and Law, both referring to members of the corporate legal department) a single IF-MAP capability must be chosen.
- Not every role needs to be paired with an IF-MAP capability: roles can be local to the Secure Access Service.

- After you decide on pairings between IF-MAP capabilities and the roles on the Secure Access Service, you create a session export policy for each pairing. On an Infranet Controller that controls Infranet Enforcers, you create a session import policy.
- The only parameters for the policies are the Secure Access Service roles and the IF-MAP capability; everything else is fixed.

Default Session-Export and Session-Import Policy Action

By default, Session-Import and Session-Export IF-MAP policies are configured to allow IF-MAP capabilities (the equivalent of Secure Access Service roles) to be published to the IF-MAP server and retrieved from the IF-MAP server, provided there are matching roles on each IF-MAP client. You can open new Session-Import and Session-Export policies on each device, and then name and close the policies. Any matching roles that the IF-MAP clients in the federated network have can be used to access resources.

Advanced Session-Export and Session-Import Policies

By default, advanced policy actions are not visible unless you click the advanced options links on the Session-Export and Session-Import policy pages. In default mode, you configure Session-Export and Session-Import policies using IF-MAP capabilities and Secure Access Service roles.

Device attributes, IF-MAP roles and identities can be accessed through the advanced options links. IF-MAP capabilities and Secure Access Service roles should provide the functionality that most Secure Access Service IF-MAP Federation requires.

Related Documentation

- [Configuring Session-Export Policies on page 98](#)
- [Session-Import Policies on page 100](#)

Configuring Session-Export Policies

Session-Export policies determine how users are identified on the IF-MAP server when their session is published via IF-MAP: the policy sets the IF-MAP identifiers. You define attributes for users that will be used to determine role matching on different Infranet Controllers. For example, you might configure a Session-Export policy to specify that any users that belong to the “engineering” role should be identified with the “engineering” IF-MAP capability on the IF-MAP server. That identity will be included in the session information to which other IF-MAP clients subscribe. You configure corresponding Session-Import Policies on Infranet Controllers to identify which roles the user should be assigned.

You configure Session-Export policies based on Infranet Controller or Secure Access Service roles, and users belonging to those roles can access resources on an Infranet Enforcer only if the role can be successfully matched with a role on the target Infranet Controller. You configure Session-Export policies on all Infranet Controllers and Secure Access Services for which you have users that will be allowed to access resources behind an Infranet Enforcer in the network.

When a user for whom Session-Export policies has been configured successfully authenticates to the network, the Session-Export policies are used to translate the user session into IF-MAP data which is then sent to the IF-MAP server. When the user attempts to access a resource that is protected by an Infranet Enforcer, the target Infranet Controller then attempts to translate the IF-MAP data for the user into a user name and roles using the Session-Import policies that are configured on the second Infranet Controller device.

Administrative Domains In Session-Export Policies

In a Layer 2 environment, session information on the IF-MAP server includes a MAC address. If an export policy specifies an Administrative Domain, the domain is associated with the MAC address published to the IF-MAP server (the administrative domain is also associated with the identity published to the IF-MAP server).

A DHCP server assigns an IP address to the endpoint after authentication. An IF-MAP enabled DHCP server publishes an ip-mac link to IF-MAP, associating the endpoint's IP address with its IF-MAP session information.

Including administrative domains in MAC addresses allows the ip-mac link to be created based on the administrative domain.

If your IF-MAP Federated network spans different administrative domains, you should configure separate Session-Export policies for each domain to prevent MAC address spoofing. Each administrative domain should have an associated DHCP server and unique Session-Export policies.

Other aspects of the Session-Export policies within the IF-MAP Federated network can overlap.

To configure a Session-Export policy:

1. From the admin console select **System > IF-MAP > Session-Export Policies**.
2. Click **New** to create a new policy.
3. Type a **Policy Name**, and optionally a **Description**.
4. Optionally, add **Available Roles** to the **Selected Roles** column to determine the roles for which this policy should apply. If you do not add any roles, the policy applies to all sessions. However, if you have non-interactive devices such as printers that do not need access, you may want to manually add roles and exclude those roles with non-interactive devices.
5. Under Policy Actions, Select **Set IF-MAP Capabilities** and choose the applicable roles.
 - **Copy Matching Roles**—Selecting this action copies all of the user roles that match the roles specified in the Roles section of this policy into the IF-MAP capabilities data.
 - **Copy all Roles**—Selecting this action copies all of the roles from the user session to the IF-MAP capabilities data.
 - **Set capabilities specified below**—Enter capabilities, one per line.

6. Select **Stop processing policies when this policy matches** to specify that when this policy is matched, no more Session-Export policies should be applied.
7. Select **Save Changes**, or continue to configure Advanced Actions.

To configure advanced options (generally not required for Infranet Controller and Secure Access Service IF-MAP Federation):

1. Select the **View Advanced Actions** link. Additional options appear on the page.
2. **Set IF-MAP Identity**—If this action is chosen, enter the Identity and select an Identity Type from the menu. Identity is normally specified as <NAME>, which assigns the user's login name. Any combination of literal text and context variables may be specified. If you choose other for Identity Type, enter a unique Identity Type in the text box.
3. Optionally type the **Administrative Domain** for the Session-Export policy. This optional field is applied to identity and MAC address data. One example for using this field is in a large network environment with several domains in which a username could be duplicated. By entering the domain, you ensure that the correct user is identified.
4. **Set IF-MAP Roles**—If this action is selected, select the applicable roles.
 - **Copy Matching Roles**—Selecting this action copies all of the user roles that match the roles specified in the Roles section of this policy into the IF-MAP capabilities data.
 - **Copy all Roles**—Selecting this action copies all of the roles from the user session to the IF-MAP capabilities data.
 - **Set capabilities specified below**—Enter capabilities, one per line.
5. **Set IF-MAP Device Attributes**—Device attributes represent a passed Host Checker policy on the Infranet Controller or Secure Access Service.
 - **Copy Host Checker policy names**—The name of each Host Checker policy that passed for the session is copied to a device attribute.
 - **Set Device Attributes**—Type Device Attributes, one per line, into the text box.
6. Select **Save Changes** to save this advanced Session-Export policy.

You must create corresponding Session-Import policies that allow IF-MAP client Infranet Controllers that are connected to an Infranet Enforcer in front of protected resources to collect IF-MAP data from the IF-MAP server.

**Related
Documentation**

- [Session-Export and Session-Import Policies on page 96](#)
- [Troubleshooting the IF-MAP Federation Network on page 101](#)

Session-Import Policies

The Session-Export policies that you create allow IF-MAP data that represents a session to be stored on the IF-MAP server. Session-Import policies specify how the Infranet Controller derives a set of roles and a username from the IF-MAP data in the IF-MAP

server. Session-Import policies establish rules for importing user sessions from the Secure Access Service. Import policies allow you to match authenticated users with corresponding roles on the target device. For example, you might configure an Import policy to specify that when IF-MAP data for a session includes the “Contractor” capability, the imported session should have the “limited” role. Session-Import policies allow the Infranet Controller to properly assign roles based on information that the IF-MAP server provides.

You configure Session-Import policies on IF-MAP client IVEs that are connected to an Infranet Enforcer in front of protected resources. For information about configuring Session-Import policies, see IF-MAP Federation.

Related Documentation

- [Troubleshooting the IF-MAP Federation Network on page 101](#)

Troubleshooting the IF-MAP Federation Network

Diagnostic tools on the Infranet Controller and Secure Access Service can assist you with troubleshooting a federated network.

IF-MAP Client User Messages—On the IF-MAP client, logs information that is published and removed from the IF-MAP server.

- Enable IF-MAP Client User Messages from **Log/Monitoring > User Access > Settings** on the Infranet Controller and Secure Access Service IF-MAP client.

IF-MAP Server Trace—On the IF-MAP server, logs the XML for all IF-MAP requests and responses.

- Enable the IF-MAP Server Trace from **Log/Monitoring > Events > Settings** on the IF-MAP server.

IF-MAP Server Trace should only be enabled for troubleshooting purposes, as running this diagnostic incurs a large performance impact.

Related Documentation

- [Viewing Active Users on the IF-MAP Client on page 101](#)

Viewing Active Users on the IF-MAP Client

On an IF-MAP client, you can view all of the sessions from other Infranet Controllers or Secure Access Services that currently access the client (the imported sessions). Session information that can be viewed includes the username, roles, the user’s endpoint IP address, and the IP address of the Infranet Controller or Secure Access Service that authenticated the user. You can select and remove sessions either temporarily or permanently. A temporarily removed session can be restored in response to a request for continued access. A permanently removed session cannot be restored.

To view, de-activate, or activate current sessions on an IF-MAP client:

1. Select **System > IF-MAP > Active Users** from the IF-MAP client admin console.
2. Select **Imported** or **Exported**.

3. Select **Activate** or **De-activate**.

Related Documentation

- [Troubleshooting the IF-MAP Federation Network on page 101](#)

Trusted Server List

The Secure Access Service uses two mechanisms to install and launch client software from a web browser:

- ActiveX controls (available only for Windows/IE)
- Java applets

With both mechanisms, the user is prompted to trust ActiveX controls and Java applets they have not run before. Inherent problems with these types of mechanisms are:

- When the user trusts an ActiveX control that control is trusted forever.
- When trusting a Java applet, users are trusting all code that is signed by the exact same code signing certificate.

To address the above, administrators can create a text file (called a whitelist) that contains a list of trusted Secure Access Services, fully qualified domain names or IP addresses, one per line. Administrators can configure two types of whitelists:

- Admin whitelist—The admin whitelist file can be modified only by the endpoint administrator. The administrator must use SMS or other mechanism to copy the admin whitelist file to the end-user's system. Admin whitelist files are located in:

`%ProgramFiles%\Juniper Networks\Whitelist.txt` (Windows)

`/usr/local/juniper/whitelist.txt` (Macintosh and Linux)

- User whitelist—Users can themselves make the decision to trust a Secure Access Service. When the user makes a decision to trust Secure Access Service, the Secure Access Service gets added to the user whitelist. User whitelist files are located in:

`%AppData%\Juniper Networks\Whitelist.txt` (Windows)

`~/Library/Application Support/Juniper Networks/whitelist.txt` (Macintosh)

`~/juniper_networks/whitelist.txt` (Linux)



NOTE: The trusted server list feature is for applications launched from a browser window. It does not apply to applications launched from the command-line or other means.

Administrator and User Configuration

The following is a snippet of a whitelist file:

```
qa.juniper.net
```

dev1.juniper.net
66.129.224.48



NOTE: Whitelist files are not deleted when the Secure Access Service software is removed.

There are two modes of enforcement:

- **Allow Admin List Only**—When software launches from the Secure Access Service that is not in the administrator whitelist, the launch fails and the user receives the error message “You are not allowed to launch software downloaded from <server>. Contact your system administrator for assistance.” If the Secure Access Service is in the administrator whitelist, the launch proceeds as requested.
- **Prompt**—When software launches from Secure Access Service that is not in the administrator whitelist or the user whitelist, the user is prompted if they want to launch the software with the message "Do you want to download, install and/or execute software from the following server". If the user declines, the launch fails. If the user accepts, the launch proceeds. The user also has the option to automatically add the Secure Access Service to the user whitelist file by selecting one of the following options from the message window:
 - **Always** —Add the server to the user whitelist file and download, install or launch the software
 - **Yes**—Download, install or launch the software but don't add the server to the user whitelist file
 - **No**—Don't download, install or launch software and don't add the server to the user whitelist file

If the first line of the whitelist file contains “AllowAdminListOnly” (case insensitive) then Allow Admin List Only enforcement mode is used. Otherwise, prompt mode enforcement is used.

A snippet of a whitelist file using Allow Admin List Only enforcement is shown here:

```
AllowAdminListOnly
qa.juniper.net
dev1.juniper.net
66.129.224.48
```



NOTE: Prompt enforcement is the default mode when you upgrade your Secure Access Service software to the latest revision.

To add clusters to the whitelist file:

- For Active/Passive clusters enter the VIP in the whitelist.
- For Active/Active clusters enter the load balancer hostname in the whitelist.

White List Flow Chart

The following steps outline the process for determining whether to launch the software

1. If the URL of the page initiating the launch does not begin with https, abort the launch and notify the user.
2. Else if the admin whitelist exists,
 - If the origin site is listed in the whitelist, proceed with the launch.
 - If the origin site is not in the whitelist and the whitelist starts with "AllowAdminListOnly", abort the launch and notify the user.
3. Else if the user whitelist exists,
 - If the origin site is in the user whitelist, proceed with the launch.
4. Prompt the user if they trust the origin site.
5. If the user agrees to trust the origin:
 - If they select Always then add the server to user whitelist file.
 - Proceed with the launch.
6. Abort the launch.

Related Documentation

- [Uploading Java Applets to Secure Access on page 454](#)

CHAPTER 4

User Roles

- [User Roles Overview on page 105](#)
- [Configuring General Role Options on page 109](#)
- [Role Restrictions on page 110](#)
- [Specifying Role-Based Source IP Aliases on page 111](#)
- [Specifying Role Session Options on page 111](#)
- [Customizing the Secure Access Service Welcome Page on page 115](#)
- [Secure Access Service Optimized Interface for the Apple iPad on page 120](#)
- [Defining Default Options for User Roles on page 122](#)
- [Customizing Messages on page 123](#)
- [Customizing UI Views for User Roles on page 124](#)

User Roles Overview

A user role is an entity that defines user session parameters (session settings and options), personalization settings (user interface customization and bookmarks), and enabled access features (Web, file, application, Telnet/SSH, Terminal Services, network, meeting, and e-mail access). A user role does not specify resource access control or other resource-based options for an individual request. For example, a user role may define whether or not a user can perform Web browsing. However, the individual Web resources that a user may access are defined by the Web resource policies that you configure separately.

The Secure Access Service access management framework supports two types of user roles:

- **Administrators**—An administrator role specifies Secure Access Service management functions and session properties for administrators who map to the role. You can customize an administrator role by selecting the Secure Access Service feature sets and user roles that members of the administrator role are allowed to view and manage. You can create and configure administrator roles through the Delegated Admin Roles page. Click **Administrators > Admin Roles** in the admin console.
- **Users**—A user role is an entity that defines user session parameters, personalization settings, and enabled access features. You can customize a user role by enabling specific Secure Access Service access features, defining Web, application, and session

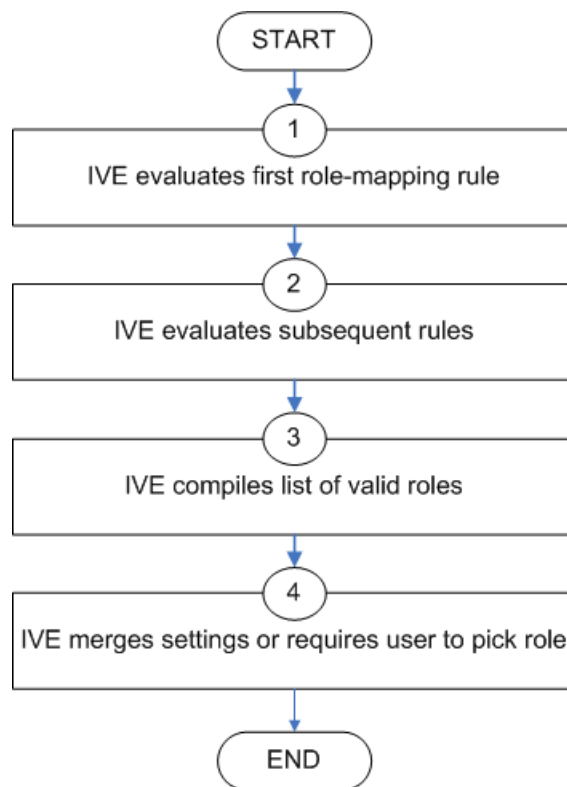
bookmarks, and configuring session settings for the enabled access features. You can create and configure user roles through the Roles page. Click Users > User Roles in the admin console.

User roles are an integral part of the Secure Access Service access management framework, and therefore are available on all Secure Access Service products. However, you can only access features through a user role if you are licensed for the feature. For instance, if you are using an SA-700 appliance and have not purchased a Core Clientless Access upgrade license, you cannot enable Web rewriting for a user role.

User Role Evaluation

The Secure Access Service's role mapping engine determines a user's session role, or combined permissions valid for a user session, as illustrated in the following figure. A detailed description of each step follows the diagram.

Figure 5: Security Checks Performed by the Secure Access Service to Create a Session Role



The Secure Access Service performs the following security checks to create a session role:

1. The Secure Access Service begins rule evaluation with the first rule on the Role Mapping tab of the authentication realm to which the user successfully signs in. During the evaluation, the Secure Access Service determines if the user meets the rule conditions. If so, then:
 - The Secure Access Service adds the corresponding roles to a list of “eligible roles” available to the user.
 - The Secure Access Service considers whether or not the “stop on match” feature is configured. If so, then the engine jumps to step 5.
2. The Secure Access Service evaluates the next rule on the authentication realm’s Role Mapping tab according to the process in Step 1 and repeats this process for each subsequent rule. When the Secure Access Service evaluates all role mapping rules, it compiles a comprehensive list of eligible roles.
3. The Secure Access Service evaluates the definition for each role in the eligibility list to determine if the user complies with any role restrictions. The Secure Access Service then uses this information to compile a list of valid roles, whose requirements the user also meets.

If the list of valid roles contains only one role, then the Secure Access Service assigns the user to that role. Otherwise, the Secure Access Service continues the evaluation process.
4. The Secure Access Service evaluates the setting specified on the Role Mapping tab for users who are assigned to more than one role:
 - **Merge settings for all assigned roles**—If you choose this option, then the Secure Access Service performs a permissive merge of all the valid user roles to determine the overall (net) session role for a user session.
 - **User must select from among assigned roles**—If you choose this option, then the Secure Access Service presents a list of eligible roles to an authenticated user. The user must select a role from the list, and the assigns the user to that role for the duration of the user session.
 - **User must select the sets of merged roles assigned by each rule**—If you choose this option, the Secure Access Service presents a list of eligible rules to an authenticated user (that is, rules whose conditions the user has met). The user must select a rule from the list, and the Secure Access Service performs a permiss merge of all the roles that map to that rule.



NOTE: If you use automatic (time-based) dynamic policy evaluation or you perform a manual policy evaluation, the Secure Access Service repeats the role evaluation process described in this section.

Permissive Merge Guidelines

A permissive merge is a merge of two or more roles that combines enabled features and settings following these guidelines:

- Any enabled access feature in one role takes precedence over the same feature set disabled in another role. For example, if a user maps to two roles, one of which disables Junos Pulse Collaboration while the other role enables Junos Pulse Collaboration, Secure Access Service allows the user to use Junos Pulse Collaboration for that session.
- In the case of Secure Application Manager, the Secure Access Service enables the version corresponding to the first role that enables this feature. Furthermore, the Secure Access Service merges the settings from all the roles that correspond to the selected version.



NOTE: If you are using Junos Pulse, then Junos Pulse is always enabled as the default client.

- In the case of user interface options, the Secure Access Service applies the settings that correspond to the user's first role.
- In the case of session timeouts, the Secure Access Service applies the greatest value from all of the roles to the user's session.
- If more than one role enables the Roaming Session feature, the Secure Access Service merges the netmasks to formulate a greater netmask for the session.
- When merging two roles that a user is mapped to—one in which bookmarks open in a new window and one in which bookmarks open in the same window—the merged role opens bookmarks in the same window.
- When merging two roles in which the first role disables the browsing toolbar and the second role enables either the framed or standard toolbar, the merged role uses the settings from the second role and displays the specified browsing toolbar.
- The merged role uses the highest value listed for the HTTP Connection Timeout. Click Users > User Roles > Select Role > Web > Options then click View advanced options.

Configuration of User Roles

To create a user role:

1. In the admin console, choose Users > User Roles.
2. Click New Role and then enter a name and optionally a description. This name appears in the list of Roles on the Roles page.

Once you have created a role, you can click the role's name to begin configuring it using the instructions in the following sections.



NOTE: When you delete a role, the personal bookmarks, SAM settings, and other settings may not be removed. Therefore, if you add a new role with the same name, any users added to that new role may acquire the old bookmarks and settings. In general, the Secure Access Service enforces referential integrity rules and does not allow you to delete any objects if they are referenced elsewhere. For example, if a role is used in any of the realm's role mapping rules, then the Secure Access Service rejects the deletion of the role unless you modify or delete the mapping rules.

When you create individual user accounts, you must add the users through the appropriate authentication server (not the role). Or for instructions on how to create users on third-party servers, see the documentation that comes with that product.

- Related Documentation**
- [Policies, Rules & Restrictions, and Conditions Overview on page 72](#)
 - [Configuring General Role Options on page 109](#)

Configuring General Role Options

Click Overview at the top of the General tab to edit a role's name and description, toggle session and user interface options on and off, and enable access features. When you enable an access feature, make sure to create corresponding resource policies.

To manage general role settings and options:

1. In the admin console, click **Users > User Roles > Role Name > General > Overview**.
2. Revise the name and description and then click **Save Changes** (optional).
3. Under Options, check the role-specific options that you want to enable for the role.

The Secure Access Service uses default settings for newly created roles or when you do not select role-specific options.

Role-specific options include:

- **VLAN/Source IP**—Select this option to apply the role settings configured on the General > VLAN/Source IP page.
 - **Session Options**—Select this option to apply the role settings in the General > Session Options page to the role.
 - **UI Options**—Select this option to apply the role settings in the General > UI Options page to the role.
4. Under Access features, check the features you want to enable for the role. Options include:
 - **Web**—intermediate Web URLs through the Content Intermediation Engine.
 - **Files (Windows or UNIX/NFS version)**—resource profile that controls access to resources on Windows server shares or UNIX servers.

- **Secure Application Manager (Windows version or Java version)**—provides secure, application-level remote access to enterprise servers from client applications.
 - **Telnet/SSH**—connect to internal server hosts in the clear using Telnet protocols or to communicate over an encrypted Secure Shell (SSH) session through a Web-based terminal session emulation.
 - **Terminal Services**—enable terminal emulation sessions on a Windows terminal server, Citrix NFuse server, or Citrix Metaframe server.
 - **Meetings**—securely schedule and hold online meetings between both Secure Access Service users and non-Secure Access Service users.
 - **Email Client**—enables users to use standards-based email clients to access corporate email securely from remote locations without the need for any additional software, such as a VPN client.
 - **VPN Tunneling**—provides secure, SSL-based network-level remote access to all enterprise application resources using the Secure Access Service.
5. Click **Save Changes** to apply the settings to the role.

**Related
Documentation**

- [Role Restrictions on page 110](#)
- [Specifying Role Session Options on page 111](#)

Role Restrictions

Click Restrictions at the top of the General tab to specify access management options for the role. The Secure Access Service considers these restrictions when determining whether or not to map a user to the role. The Secure Access Service does not map users to this role unless they meet the specified restrictions.

You may configure any number of access management options for the role. If a user does not conform to all of the restrictions, the Secure Access Service does not map the user to the role.

To specify access management options for the role:

1. In the admin console, click Users > User Roles > Role Name > General > Restrictions.
2. Click the tab corresponding to the option you want to configure for the role, and then configure it.

**Related
Documentation**

- [Specifying Source IP Access Restrictions on page 79](#)
- [Specifying Browser Access Restrictions on page 82](#)
- [Specifying Certificate Access Restrictions on page 84](#)

Specifying Role-Based Source IP Aliases

Click VLAN/Source IP at the top of the General to define role-based source IP aliases. If you want to direct traffic to specific sites based on roles, you can define a source IP alias for each role. You use these aliases to configure virtual ports you define for the internal interface source IP address. A back-end device can then direct end user traffic based on these aliases, as long as you configure the back-end device, such as a firewall, to expect the aliases in place of the internal interface source IP address. This capability enables you to direct various end users to defined sites based on their roles, even though all of the end user traffic has the same internal interface source IP address.



NOTE: You must define virtual ports to take advantage of the role-based source IP aliases.

To specify a source IP alias for the role:

1. In the admin console, click **Users > User Roles > Role Name > General > VLAN/Source IP**.
2. Select the VLAN you want to use from the VLAN list, if you have defined VLAN ports on your system.

If you have not defined VLAN ports, the option defaults to the Internal Port IP address. If you have provisioned IVS systems, and you have defined VLAN ports and you want any of those VLAN ports to appear in the VLAN list, then you must include the VLAN ports in the Selected VLANs text box on the Root IVS configuration page.

3. Select a source IP address from the list.
4. Click **Save Changes** to apply the settings to the role.



NOTE: If an end user is mapped to multiple roles and the Secure Access Service merges roles, the Secure Access Service associates the source IP address configured for the first role in the list with the merged role.

You can specify the same source IP address for multiple roles. You cannot specify multiple source IP addresses for one role.

Related Documentation

- [Using Virtual Ports on page 802](#)
- [Configuring the Internal and External Ports on page 792](#)

Specifying Role Session Options

Use the Session tab to specify session time limits, roaming capabilities, session and password persistency, request follow-through options, and idle timeout application

activity. Select the **Session Options** check box on the Overview tab to enable these settings for the role.

To configure general session options:

1. In the admin GUI, click **User > User Roles > RoleName > General > Session Options**.
2. Configure session options, as described in [Table 5 on page 112](#).
3. Save the configuration.

Table 5: Session Options

Option	Guidelines
Session lifetime	<ul style="list-style-type: none"> • For Idle Timeout, specify the number of minutes a nonadministrative user session may remain idle before ending. The minimum is five minutes. The default idle session limit is 10 minutes, which means that if a user's session is inactive for 10 minutes, the Secure Access Service ends the user session and logs the event in the system log (unless you enable session timeout warnings described later). • For Max. Session Length, specify the number of minutes an active nonadministrative user session may remain open before ending. The minimum is six minutes. The default time limit for a user session is 60 minutes, after which the Secure Access Service ends the user session and logs the event in the system log. During an end user session, prior to the expiration of the maximum session length, the Secure Access Service prompts the user to reenter authentication credentials, which avoids the problem of terminating the user session without warning. • For Reminder Time, specify when the Secure Access Service should prompt non-administrative users, warning them of an impending session or idle timeout. Specify the number of minutes before the timeout is reached. <p>NOTE: We recommend the difference between Idle Timeout and Reminder Time be greater than two minutes. This ensures that the reminder pop-up window appears at the correct time.</p>

Table 5: Session Options (*continued*)

Option	Guidelines
Enable session timeout warning	<p>Enable to notify non-administrative users when they are about to reach a session or idle timeout limit.</p> <p>These warnings prompt users to take the appropriate action when they are close to exceeding their session limits or idle timeouts, helping them save any in-progress form data that would otherwise be lost. Users approaching the idle timeout limit are prompted to reactivate their session. Users approaching the session time limit are prompted to save data.</p> <p>For example, a Secure Access Service user may unknowingly reach the idle timeout set for his role while using an e-mail client configured to work with the Secure Access Service, because the Secure Access Service does not receive data while the user composes e-mail. If the session timeout warning is enabled, however, the Secure Access Service prompts the user to reactivate his Secure Access Service session before the session times out and forces the user's Secure Access Service session to end. This warning gives the user the opportunity to save his partially composed e-mail.</p> <p>Optionally, select Display sign-in page on max session time out to display a new browser sign-in page to the end user when their session times out. This option only appears when you choose to enable the session timeout warning.</p> <p>NOTE: If you do not select the Enable session timeout warning option, the Secure Access Service only displays expiration messages to users—it does not give them the option to extend their sessions. Instead, users need to access the Secure Access Service sign-in page and authenticate into a new session.</p> <p>The Enable session timeout warning option only applies to expiration messages displayed by the end user's browser, not by other clients such as WSAM or VPN Tunneling.</p>
Roaming session	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • Enabled—Enables unlimited roaming sessions. An unlimited roaming session allows mobile users (laptop users) with dynamic IP addresses to sign in to the Secure Access Service from one location and continue working from another. Disable this feature to prevent users from accessing a previously established session from a new source IP address. This helps protect against an attack spoofing a user's session, provided the hacker was able to obtain a valid user's session cookie. If you enable unlimited session roaming, a session is maintained within an IPv4 network, within an IPv6 network, or from IPv4 to IPv6 and vice versa. • Limit to subnet—Limits the roaming session to the local subnet, specified by netmask for IPv4 subnets and prefix length for IPv6 subnets. Users may sign in from one IP address and continue using their sessions with another IP address as long as the new IP address is within the same subnet. If you configure limited session roaming, you can specify IPv4 or IPv6 subnets within which the session is maintained. However, with limited session roaming, you cannot allow sessions to roam from IPv4 to IPv6 networks, or vice versa. • Disabled—Disables roaming user sessions for users mapped to this role. Users who sign in from one IP address may not continue an active Secure Access Service session from another IP address; user sessions are tied to the initial source IP address.

Table 5: Session Options (*continued*)

Option	Guidelines
Persistent session	<p>By default, the Secure Access Service session cookie is flushed from the browser's memory when the browser is closed. The Secure Access Service session length is determined by both the idle timeout value and maximum session length value that you specify for the role. The Secure Access Service session does not terminate when a user closes the browser; a Secure Access Service session only terminates when a user signs out of the Secure Access Service.</p> <p>Enable the persistent session option to write the Secure Access Service session cookie to the client hard disk so that the user's Secure Access Service credentials are saved for the duration of the Secure Access Service session.</p> <p>Assume persistent session is enabled and a user starts a VPN Tunneling session from a browser. Later, the user quits the browser application. The next time the user opens a new browser window and logs in to the same Secure Access Service, the user is not prompted to enter his or her credentials again.</p> <p>NOTE: (Macintosh only) Persistent session applies only for browser login as stated earlier. If you start VPN Tunneling from the standalone launcher (by opening NetworkConnect.dmg) and later open a new browser and log in to that same Secure Access Service, you are prompted to reenter your credentials.</p> <p>NOTE: If you enable the Persistent session option and a user closes the browser window without signing out, any user can open another instance of the same browser to access the Secure Access Service without submitting valid credentials, posing a potential security risk. We recommend that you enable this feature only for roles whose members need access to applications that require Secure Access Service credentials and that you make sure these users understand the importance of signing out of the Secure Access Service when they are finished.</p>
Remove Browser Session Cookie	<p>Enable to remove the Secure Access Service session cookie and logs users out of their Secure Access Service Web session once the client component launches, enhancing security for your VPN Tunneling, WSAM and Pulse session.</p> <p>Disable to retain the Secure Access Service session cookie and keep users logged in to their Secure Access Service Web session once the client component starts.</p> <p>Because browser cookies are plain text files, they are susceptible to malicious attacks. The Remove Browser Session Cookie option removes the Secure Access Service session cookie, making your VPN Tunneling, WSAM and Junos Pulse sessions more secure. When enabled, users are logged out of their Secure Access Service Web session once the client component (for example, Junos Pulse) launches. Users are logged out of their Web session regardless of whether the client component launches successfully or not. If the client component does not successfully launch, users can restart their Web session and try launching their client component again. This option also prevents any client component from launching a browser through the client.</p> <p>NOTE: The Remove Browser Session Cookie removes only the Secure Access Service session cookie. It does not remove non-Secure Access Service cookies or other any other cookie.</p>

Table 5: Session Options (*continued*)

Option	Guidelines
Persistent password caching	<p>Enable to allow cached passwords to persist across sessions for a role.</p> <p>The Secure Access Service supports Windows NT LAN Manager (NTLM) authentication protocol and HTTP Basic Authentication and supports servers that are set up to accept both NTLM and anonymous sign-in. The Secure Access Service caches NTLM and HTTP Basic Authentication passwords provided by users so that the users are not repeatedly prompted to enter the same credentials used to sign in to the Secure Access Service server or another resource in the NT domain. By default, the Secure Access Service flushes cached passwords when a user signs out. A user can delete cached passwords through the Advanced Preferences page. After the end user logs in to the Secure Access Service, click Preferences and then click the Advanced tab.</p>
Browser request follow-through	Enable to allow the Secure Access Service to complete a user request made after an expired user session after the user reauthenticates.
Idle timeout application activity	Enable to ignore activities initiated by Web applications (such as polling for e-mails) when determining whether a session is active. If you disable this option, periodic pinging or other application activity may prevent an idle timeout.
Upload Logs	<p>Enable to allow the user to transmit (upload) client logs to the Secure Access Service.</p> <p>NOTE: Use the System > Log/Monitoring > Client Logs > Settings page to completely enable client-side logs for the user.</p>

Related Documentation • [Junos Pulse Collaboration Overview on page 691](#)

Customizing the Secure Access Service Welcome Page

Click **UI Options** at the top of the General tab to specify customized settings for the Secure Access Service welcome page and the browsing toolbar for users mapped to this role. The Secure Access Service welcome page (or home page) is the Web interface presented to authenticated Secure Access Service users. Click **Overview** at the top of the General tab, and then select the **UI Options** checkbox to enable custom settings for the role; otherwise, the Secure Access Service uses the default settings.

Personalization settings include the sign-in page, page header, page footer, and whether or not to display the browsing toolbar. If the user maps to more than one role, then the Secure Access Service displays the user interface corresponding to the first role to which a user is mapped.

To customize the Secure Access Service welcome page for role users:

1. Click **Users > User Roles > RoleName > General > UI Options**.
2. Under Header, specify a custom logo and alternate background color for the header area of the Secure Access Service welcome page (optional):
 - Click **Browse** and locate your custom image file. The new logo appears in the Current appearance box only after you save your changes.



NOTE: You can only specify a JPEG or GIF file for a custom logo image. Other graphics formats are not displayed properly in the JSAM status window on some OS platforms.

- Type the hexadecimal number for the background color or click the Color Palette icon and pick the desired color. The Current appearance box updates immediately.
3. Under Sub-headers, select new background and text colors (optional):
 - Type the hexadecimal number for the Background color or click the **Color Palette** icon and pick the desired color. The Current appearance box updates immediately.
 - Type the hexadecimal number for the Text color or click the **Color Palette** icon and pick the desired color. The Current appearance box updates immediately.
 4. Under Start page, specify the start page that you want users to see after they sign in and when they click the Home icon on the toolbar:
 - **Bookmarks page**—Select this option to display the standard Secure Access Service Bookmarks page.
 - **Meetings page**—Select this option to display the standard Secure Access Service meetings page.
 - **Custom page**—Select this option to display a custom start page and then specify the URL to the page. The Secure Access Service rewrites the URL and creates an access control rule to allow users access to the URL. (Note that users can also enter the custom URL in the Secure Access Service Browse field on the toolbar.) The Secure Access Service evaluates the access control rule after all other policies, which means another policy could deny access to the URL.
 - **Also allow access to directories below this url**—Select this option to allow users access to subdirectories of the custom-page URL. For example, if you specify `http://www.domain.com/`, users can also access `http://www.domain.com/dept/`.
 5. Under Bookmarks Panel Arrangement, arrange the panels as you want to display them on the user's bookmarks page:
 - a. To select the name of a panel, click in the Left Column or Right Column list.
 - b. To position a panel above or below the other panels, click Move Up or Move Down.
 - c. To move a panel to the other side of the user's bookmarks page, click Move > or < Move.



NOTE: The Secure Access Service displays all panels under Bookmarks Panel Arrangement for all licensed features regardless of whether or not you enable the corresponding feature for the role.

The maximum number of combined bookmarks a role can have is approximately 500. If a role has more than 500 bookmarks, some operations (for example, delete role, duplicate role) may not work correctly. The workaround is to split a role with a large number of bookmarks into multiple roles.

6. Under Help Page, select options to control the Help page that appears when users click the Help button on the toolbar:
 - **Disable help link**—Select this option to prevent users from displaying Help by removing the Help button from the toolbar.
 - **Standard help page**—Select this option to display the standard Secure Access Service end-user Help.
 - **Custom help page**—Select this option to display a custom Help page. Specify the URL to the custom help page, and then provide an optional width and height for the help page's window. The Secure Access Service rewrites the URL and creates an access control rule to allow users access to the URL. (Note that users can also enter the custom URL in the Secure Access Service Browse field on the toolbar.) The Secure Access Service evaluates the access control rule after all other policies, which means another policy could deny access to the URL. (Note that when you choose this option, the Secure Access Service disables the Tips link next to the Browse field.)
 - **Also allow access to directories below this url**—Select this option to allow users access to subdirectories of the custom help page URL. For example, if you specify `http://www.domain.com/help`, users can also access `http://www.domain.com/help/pdf/`.
7. Under User Toolbar, select options for the toolbar on the Secure Access Service Bookmarks page and other secure gateway pages on the Secure Access Service:
 - **Home**—Select this option to display the Home icon on the Secure Access Service Bookmarks page and other secure gateway pages on the Secure Access Service.
 - **Preferences**—Select this option to display the Preferences button.
 - **Session Counter**—Select this option to display a time value on the user toolbar that indicates the maximum remaining time allowed in the user's current session. Note that a period of user inactivity could also end the current session before this maximum time expires.
 - **Client Application Sessions**—Select this option to display the Client Apps button on the user toolbar. Users can click this button to display the Client Application Sessions page where they can start client applications such as VPN Tunneling or Secure Application Manager. If you do not select this option, the Secure Access Service

displays the Client Application Sessions panel on the Secure Access Service Bookmarks page.

8. Under Browsing toolbar, select options for the toolbar that users see when browsing pages not located on the Secure Access Service, such as external Web sites:
 - Show the browsing toolbar—Select this option to display the browsing toolbar.
 - Toolbar type—Select the type of browsing toolbar you want to display:
 - Standard—This toolbar can be moved to the top left or top right side of the browser window. Users can also collapse and expand the toolbar. When collapsed, the toolbar displays the custom logo only. The toolbar's default state is expanded and on the top right side of the browser window.
 - Framed—This toolbar remains fixed in a framed header section at the top of the page.



NOTE: We recommend that you do not use the top variable when working with a frame set because after the Secure Access Service intermediates the page, top might reference a different frame than you intend. This change might make the framed toolbar disappear or could cause your intermediated application to work erratically or incorrectly. See CIE Development,

- Toolbar logo and Toolbar logo (mobile)—Specify a custom logo (such as your company's logo) that you want to display on the standard and framed toolbars by browsing to the image file (optional). When the user clicks the logo, the page you specify for the Logo links to option appears. The current logo for the browsing toolbar appears next to these options.
- Logo links to— Select an option to link the browsing toolbar logo to a page that appears when users click the logo:
 - Bookmarks page—Links the logo to the Secure Access Service Bookmarks page.
 - "Start Page" settings—Links the logo to the custom start page you specified under the Start Page section.
 - Custom URL—Links the logo to the URL you enter in the associated text box (optional). This resource must be accessible to the Secure Access Service. The Secure Access Service rewrites the URL and creates an access control rule to allow users access to the URL. (Note that users can also enter the custom URL in the Secure Access Service Browse field on the toolbar.) The Secure Access Service evaluates the access control rule after all other policies, which means another policy could deny access to the URL.
 - Also allow access to directories below this url—Select this option to allow users access to subdirectories of the custom URL.
- Specify the items you want to display in the browsing toolbar:

- Enable "Home" link—Select this option to display the Home Page button, which is linked to the Secure Access Service Bookmarks page.
- Enable "Add Bookmark" link—Select this option to display the Bookmark this Page button.
- Enable "Bookmark Favorites" link—Select this option to display the Bookmark Favorites button. When the user clicks this button, the Secure Access Service displays a list of the bookmarks that the user specified as favorites on the Add Web Bookmark page of the secure gateway.
- Display Session Counter— Select this option to display a time value on the browsing toolbar that indicates the maximum remaining time allowed in the user's current session. Note that a period of user inactivity could also end the current session before this maximum time expires.
- Enable "Help" link—Select this option to display the Help button, which is linked to the Help page you specify for under Help page.



NOTE: If you click **Users > User Roles > Role Name > Web > Options** and clear the **User can add bookmarks** check box, then the Secure Access Service does not display the **Bookmark this Page** and **Bookmark Favorites** buttons on the browsing toolbar even if you select the **Enable "Add Bookmark" link** and **Enable "Bookmark Favorites" link** options.

- Use Iframe in Toolbar—Select this option if you are having problems with using iframes with JavaScript rewriting and with the Firefox web browser. This option resolves interoperability problems with the above.
9. Under **Personalized greeting**, specify a greeting and notification message on the Secure Access Service Bookmarks page (optional):
- Enabled—Select this option to display the personalized greeting. The Secure Access Service displays the username if the full name is not configured.
 - Show notification message—Select this option and enter a message in the associated text box (optional). The message appears at the top of the Secure Access Service Bookmarks page after you save changes and the user refreshes that page. You may format text and add links using the following HTML tags: `<i>`, ``, `
`, `` and `<a href>`. However, the Secure Access Service does not rewrite links on the sign-in page (because the user has not yet authenticated), so you should only point to external sites. Links to sites behind a firewall will fail. You may also use Secure Access Service system variables and attributes in this field.



NOTE: The length of the personalized greeting cannot exceed 12K, or 12288 characters.

If you use unsupported HTML tags in your custom message, the Secure Access Service may display the end user's home page incorrectly.

10. Under **Other**, specify whether or not you want the copyright notice and label shown in the footer (optional). This setting applies only to those users whose license permits disabling the copyright notice. For more information about this feature, call Juniper Networks Support.
11. Click **Save Changes**. The changes take effect immediately, but current user browser sessions may need to be refreshed to see the changes.
12. Click **Restore Factory Defaults** to reset all user-interface options back to factory defaults (optional).

Related Documentation • [Specifying Role Session Options on page 111](#)

Secure Access Service Optimized Interface for the Apple iPad

Secure Access Service is optimized for a number of platforms, including the Apple iPad. This optimization includes:

- Login pages – includes the login and logout pages as well as intermediate pages that appear after the user enters their credentials on the sign-in page and before the Home page appears. The following is a list of these customized login pages:
 - Cancel.shtml
 - Defender.shtml
 - ExceededConcurrent.shtml
 - GeneratePin.shtml
 - GraceLoginUsed.shtml
 - LoginPage.shtml
 - Logout.shtml
 - NewPin.shtml
 - NextToken.shtml
 - PasswordChange.shtml
 - PasswordExpiration.shtml
 - SelectRole.shtml
 - ShowSystemPin.shtml
 - SigninNotifPostAuth.shtml
 - SigninNotifPreAuth.shtml
 - SM-NewPinSelect.shtml
 - SM-NewPinSystem.shtml
 - SM-NewUserPin.shtml
 - SM-NextToken.shtml

- SSL.shtml
 - confirmation.shtml
 - confirmation_opensessions.shtml
 - user_unknown.shtml
- Home page – this home page displays the welcome panel and any applicable notification messages as well as the Web Bookmark panel, the File Bookmark (or Files) panel, the VPN and Preferences button.
 - Web Bookmark pages – located on the home page, the Web Bookmark panel lists each individual bookmarks and allows user to tap and browse the bookmark destination page. To to edit bookmarks, tap the **Edit** button on the panel header and the Edit Bookmark page appears. On this page, user can edit individual bookmarks, reorder bookmarks, and delete bookmarks. Editing is limited to user-created bookmarks.
 - File Bookmark pages – located on the home page, the File Bookmark panel lists each individual bookmarks. To edit bookmarks, tap the **Edit** button on the panel header and the Edit File Bookmark page will be displayed. On this page, user can edit individual bookmarks, reorder bookmarks, and delete bookmarks. Editing is limited to user-created file bookmarks.
 - Preferences page – located the home page is a Preferences button. When tapped, it displays the Preferences setting page, containing configuration options for changing username, delete cookies, delete session cookies and delete passwords.
 - Error pages – error pages that can be seen while using the features made available on the iPad are customized.
 - Company logos – Most pages display a company logo. These pages are capable of displaying custom logos if uploaded from the Secure Access Service admin GUI.

The following table lists the supported configurable options on the Apple iPad.

Table 6: Configurable Options on the Apple iPad

Custom User Interface Options	Supported
Header Logo Image	Yes
Header Background Color	No
Sub-Header Background Color	No
Sub-Header Text Color	No
Start Page Message (Welcome message)	Yes
Bookmark Panel Arrangement	No
Enable/Disable Help Link	Yes
Window Size of Help Page	No

Table 6: Configurable Options on the Apple iPad (*continued*)

Custom User Interface Options	Supported
Show/Hide Preferences Toolbar	No
Show/Hide Session Counter	Yes
Browsing Toolbar Items	Yes
Post-Auth Sign-In Notification	Yes
Personalized Greetings	Yes
Show Copyright Notice in Footer	No

Related Documentation

- Junos Pulse for Mobile Devices Overview

Defining Default Options for User Roles

You can define default options for all user roles, just as you can for delegated administrator roles. Default values are used for newly created roles or for roles where the session or UI option checkboxes are not selected in the User > User Roles > *UserName* > General > Overview window.

The default options include, but are not limited to:

- Session Options
 - **Session lifetime**—Define the idle timeout, maximum session length, and reminder time in minutes.
 - **Enable session timeout warning**—Determine whether to display warning and login page.
 - **Roaming Session**—Define level of mobility access.
 - **Persistent Session**—Define state across browser instances.
 - **Persistent password caching**—Define password state across sessions.
 - **Browser request follow-through**—Define response to browser session expiration.
 - **Idle timeout application activity**—Define Secure Access Service response to application session activity.
- UI Options
 - **Header**—Define the logo and background color.
 - **Sub-headers**—Define the background and text color.
 - **Start page**—Define which page appears after the user logs in.

- **Bookmarks Panel Arrangement**—Define the panels that appear on the user's bookmark page.
- **Help Page**—Display standard or custom help.
- **User Toolbar**—Define the links that appear on a user's home page.
- **Browsing toolbar**—Define the links that appear when a user is browsing an external website.
- **Personalized Greeting**—Display user's name and notification message on the user's welcome page.
- **Bookmarks Panel Arrangement Other**—Show copyright notice.

Defining Default Options for User Roles

To define the default options for all user roles:

1. Select **Users > User Roles**.
2. Click **Default Options**.
3. Modify settings in the **Session Options**, **UI Options**, and **Custom Messages** tabs.
4. Click **Save Changes**. These become the new defaults for all new user roles.

If you do not want user roles to see the copyright notice, you can also clear the Show copyright notice and "Secured by Juniper Networks" label in footers check box for user roles, in general. That way, all subsequent roles you create do not allow the notice to appear on the end user UI.

Related Documentation

- [Configuring General Role Options on page 109](#)
- [Role Restrictions on page 110](#)

Customizing Messages

You can customize basic messages that may be displayed to your end users when they sign in to the Secure Access Service. You can change the message text, and you can add internationalized versions of the messages in Chinese (Simplified), Chinese (Traditional), French, German, Japanese, Korean, and Spanish, in addition to English.

To customize messages:

1. Select **Users > User Roles**.
2. Click **Default Options**.
3. Select the **Custom Messages** tab.
4. Select the language to use from the menu.
5. Enter your text in the Custom Message box, below the default message you want to override.

6. Click **Save Changes**.
7. Repeat the process to create messages in additional languages.

Related Documentation

- [About Multi-Language Support for the Secure Access Service on page 1161](#)
- [Localizing the User Interface on page 1162](#)
- [Localizing Custom Sign-In and System Pages on page 1163](#)

Customizing UI Views for User Roles

You can use customization options on the Roles page to quickly view the settings that are associated with a specific role or set of roles. For instance, you can view all of the user roles and any Web bookmarks that you have associated with them. Additionally, you can use these customized views to easily link to the bookmarks and other configuration settings associated with a role.

To view a sub-set of data on the Roles page:

1. Click **Users > User Roles**.
2. Select an option from the View list at the top of the page. The following table describes these options.
3. Select one of the following options from the For list:
 - **All roles**—Displays the selected bookmarks for all user roles.
 - **Selected roles**—Displays the selected bookmarks for the user roles you choose. If you select this option, select one or more of the check boxes in the Role list.
4. Click **Update**.

Table 7: View Menu Options

Option	Description
Enabled Settings	Displays a graph outlining the remote access mechanisms and general options that you have enabled for the specified roles. Also displays links (the check marks) that you can use to access the corresponding remote access and general option configuration pages.
Restrictions	Displays Host Checker and Cache Cleaner restrictions that you have enabled for the specified roles. Also displays links you can use to access the corresponding Host Checker and Cache Cleaner configuration pages.
Meetings	Displays Junos Pulse Collaboration settings that you have configured for the specified roles. Also displays links you can use to access the corresponding Junos Pulse Collaboration configuration pages.
VPN Tunneling	Displays VPN Tunneling settings that you have configured for the specified roles. Also displays links you can use to access the corresponding VPN Tunneling configuration pages.

Table 7: View Menu Options (*continued*)

Role Mapping Rule & Realms	Displays the assigned authentication realms, role mapping rule conditions, and permissive merge settings for the specified roles. Also displays links you can use to access the corresponding realm and role mapping configuration pages.
Bookmarks: All	Displays the names and types of all of the bookmarks that you have enabled for the specified roles. Also displays links you can use to access the corresponding bookmark configuration pages. (Note that if you created a bookmark through a resource profile, the link appears in the Resource column. Otherwise, the link appears in the Bookmark column.)
Bookmarks: Web	Displays the Web bookmarks that you have enabled for the specified roles. Also displays links you can use to access the corresponding bookmark configuration pages. (Note that if you created a bookmark through a resource profile, the link appears in the Resource column. Otherwise, the link appears in the Web Bookmark column.)
Bookmarks: Files (Windows)	Displays the Windows File bookmarks that you have enabled for the specified roles. Also displays links you can use to access the corresponding bookmark configuration pages. (Note that if you created a bookmark through a resource profile, the link appears in the Resource column. Otherwise, the link appears in the Windows File Bookmark column.)
Bookmarks: Files (UNIX)	Displays the UNIX/NFS File bookmarks that you have enabled for the specified roles. Also displays links you can use to access the corresponding bookmark configuration pages. (Note that if you created a bookmark through a resource profile, the link appears in the Resource column. Otherwise, the link appears in the UNIX File Bookmark column.)
Bookmarks: Telnet	Displays the Telnet/SSH bookmarks that you have enabled for the specified roles. Also displays links you can use to access the corresponding bookmark configuration pages. (Note that if you created a bookmark through a resource profile, the link appears in the Resource column. Otherwise, the link appears in the Telnet/SSH Session column.)
Bookmarks: Terminal Services	Displays the Terminal Services bookmarks that you have enabled for the specified roles. Also displays links you can use to access the corresponding bookmark configuration pages. (Note that if you created a bookmark through a resource profile, the link appears in the Resource column. Otherwise, the link appears in the Terminal Services Session column.)
ACL Resource Policies: All	Displays the resource policies that are associated with the specified roles. Includes the type, name, description, action, and resources for each policy. Also displays links you can use to access the corresponding policy configuration pages.
ACL Resource Policies: Web	Displays the Web resource policies that are associated with the specified roles. Includes the type, name, description, action, and resources for each policy. Also displays links you can use to access the corresponding policy configuration pages.
ACL Resource Policies: Files (Windows)	Displays the Windows file resource policies that are associated with the specified roles. Includes the type, name, description, action, and resources for each policy. Also displays links you can use to access the corresponding policy configuration pages.
ACL Resource Policies: Files (UNIX)	Displays the UNIX file resource policies that are associated with the specified roles. Includes the type, name, description, action, and resources for each policy. Also displays links you can use to access the corresponding policy configuration pages.
ACL Resource Policies: SAM	Displays the JSAM and WSAM resource policies that are associated with the specified roles. Includes the type, name, description, action, and resources for each policy. Also displays links you can use to access the corresponding policy configuration pages.

Table 7: View Menu Options (*continued*)

ACL Resource Policies: Telnet	Displays the Telnet/SSH resource policies that are associated with the specified roles. Includes the type, name, description, action, and resources for each policy. Also displays links you can use to access the corresponding policy configuration pages.
ACL Resource Policies: Terminal Services	Displays the Terminal Services resource policies that are associated with the specified roles. Includes the type, name, description, action, and resources for each policy. Also displays links you can use to access the corresponding policy configuration pages.
ACL Resource Policies: VPN Tunneling	Displays the VPN Tunneling resource policies that are associated with the specified roles. Includes the type, name, description, action, and resources for each policy. Also displays links you can use to access the corresponding policy configuration pages.
Resource Profiles: All	Displays the resource profiles that are associated with the specified roles. Includes the type, name, bookmarks, and supporting policies for each profile. Also displays links you can use to access the corresponding resource profile configuration pages.
Resource Profiles: Web Applications	Displays the Web application resource profiles that are associated with the specified roles. Includes the name, bookmarks, and supporting policies for each profile. Also displays links you can use to access the corresponding resource profile configuration pages.
Resource Profiles: Web Hosted Java Applets	Displays the hosted Java applet resource profiles that are associated with the specified roles. Includes the name, bookmarks, and supporting policies for each profile. Also displays links you can use to access the corresponding resource profile configuration pages.
Resource Profiles: Files (Windows)	Displays the Windows file resource profiles that are associated with the specified roles. Includes the name, bookmarks, and supporting policies for each profile. Also displays links you can use to access the corresponding resource profile configuration pages.
Resource Profiles: Files (UNIX)	Displays the UNIX file resource profiles that are associated with the specified roles. Includes the name, bookmarks, and supporting policies for each profile. Also displays links you can use to access the corresponding resource profile configuration pages.
Resource Profiles: SAM Client Applications	Displays the JSAM and WSAM application resource profiles that are associated with the specified roles. Includes the name, bookmarks, and supporting policies for each profile. Also displays links you can use to access the corresponding resource profile configuration pages.
Resource Profiles: SAM WSAM destinations	Displays the WSAM destination resource profiles that are associated with the specified roles. Includes the name, bookmarks, and supporting policies for each profile. Also displays links you can use to access the corresponding resource profile configuration pages.
Resource Profiles: Telnet/SSH	Displays the Telnet/SSH resource profiles that are associated with the specified roles. Includes the name, bookmarks, and supporting policies for each profile. Also displays links you can use to access the corresponding resource profile configuration pages.
Resource Profiles: Terminal Services	Displays the Terminal Services resource profiles that are associated with the specified roles. Includes the name, bookmarks, and supporting policies for each profile. Also displays links you can use to access the corresponding resource profile configuration pages.

CHAPTER 5

Resource Profiles

- [Resource Profiles on page 127](#)
- [Resource Profile Components on page 128](#)
- [Defining Resource Profile Resources on page 130](#)
- [Defining Resource Profile Autopolicies on page 132](#)
- [Defining Resource Profile Roles on page 133](#)
- [Defining Resource Profile Bookmarks on page 134](#)
- [Resource Profile Templates on page 135](#)

Resource Profiles

A resource profile contains all of the resource policies, role assignments, and enduser bookmarks required to provide access to an individual resource. Resource profiles simplify resource configuration by consolidating the relevant settings for an individual resource into a single page within the admin console.

The Secure Access Service comes with two types of resource profiles:

- Standard resource profiles enable you to configure settings for a variety of resource types, such as Web sites, client/server applications, directory servers, and terminal servers. When you use this method, you choose a profile type that corresponds to your individual resource and then provide details about the resource.
- Resource profile templates enable you to configure settings for specific applications. When you use this method, you choose a specific application (such as the Citrix NFuse version 4.0). Then, the Secure Access Service pre-populates a variety of values for you based on your chosen application and prompts you to configure additional settings as necessary.

Resource profiles are an integral part of the Secure Access Service access management framework, and therefore are available on all Secure Access Service products. However, you can only access resource profile types that correspond to your licensed features. For instance, if you are using an SA700 Series appliance and have not purchased a Core Clientless Access upgrade license, you cannot create Web resource profiles.

To create resource profiles, you:

- Create user roles through the **Users > User Roles** page of the admin console.

- Create resource profiles through the **Users > Resource Profiles** page of the admin console. When creating the resource profile, specify the resource, create autopolicies, associate the profile with user roles, and create bookmarks as necessary.

- Related Documentation**
- [Resource Profile Components on page 128](#)
 - [Resource Profile Templates on page 135](#)

Resource Profile Components

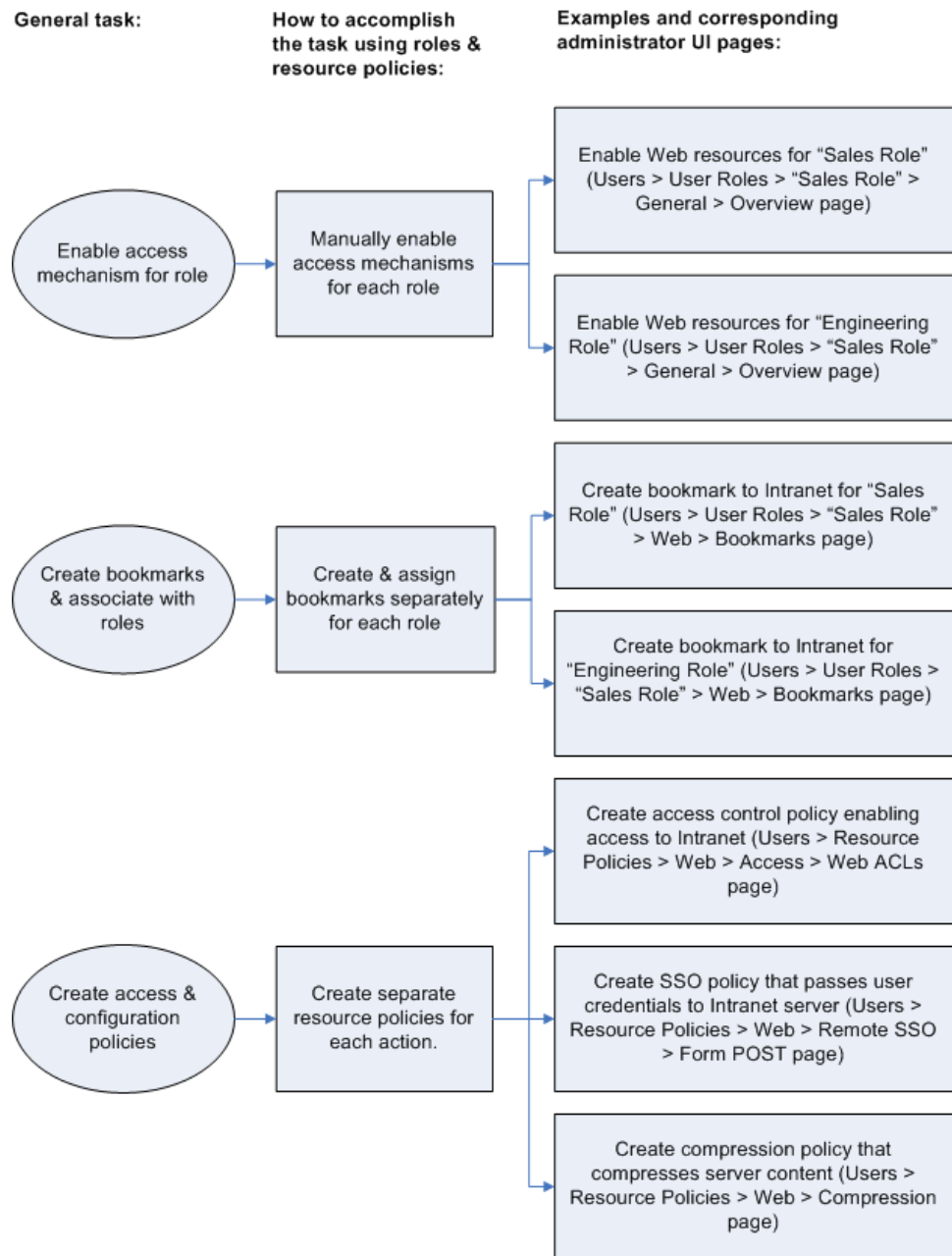
Resource profiles contain the following components:

- **Resources**—When you are defining a resource profile, you must specify the individual resource that you want to configure (such as your company Intranet site or a Lotus Notes application). All other major settings within the profile branch from this resource. You can configure a variety of resource types, including Web sites, client/server applications, directory servers, and terminal servers.
- **Autopolicies**—When you are defining a resource profile, you generally create autopolicies that establish the access requirements and other settings for the specified resource. The most common type of autopolicy enables access to the primary resource defined in the profile. Other policy types (such as compression and caching autopolicies) “fine-tune” how the Secure Access Service handles the data that it passes to and from the specified resource.
- **Roles**—When you are defining a resource profile, you generally associate the profile with user roles. The specified roles then inherit the autopolicies and (optionally) the bookmarks defined in the resource profile.
- **Bookmarks**—When you are defining a resource profile, you may optionally create a bookmark that links to the profile’s primary resource (such as your company intranet’s main page). You can also create additional bookmarks that link to various sites within the resource’s domain (such as the Sales and Marketing intranet pages). The Secure Access Service displays these bookmarks to users who are assigned to the user roles that you specify.

The following diagrams illustrate how resource profiles simplify the configuration of individual resources.

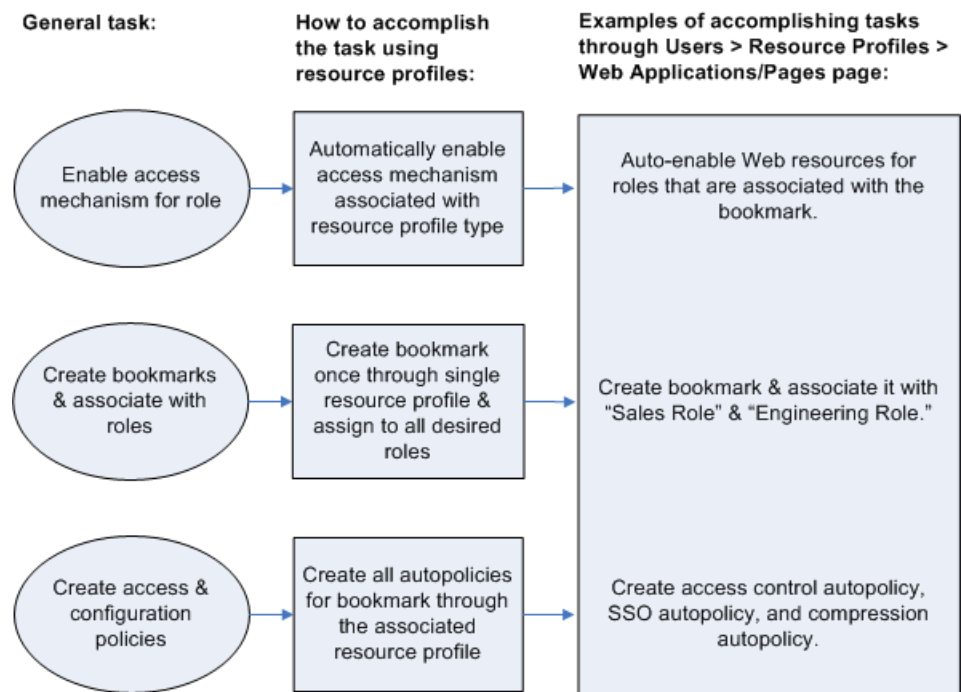
The following diagram shows how to configure resources using roles and resource policies. Note that to enable a bookmark for multiple user roles, you must manually re-create the bookmark and enable the appropriate access mechanism for each role. You must also use a variety of pages in the administrator console to create associated resource policies enabling access to the resource and other configuration options.

Figure 6: Using Roles and Resource Policies to Configure Resources



The following diagram shows how to configure resources using resource profiles. Note that you can create a bookmark, associate it with multiple user roles, and create the associated autopolicies enabling access to the resource and other configuration options through a single section in the administrator console. Also note that the Secure Access Service automatically enables the appropriate access mechanism to the roles to which you assign the bookmark.

Figure 7: Using Resource Profiles to Configure Resources



Related Documentation

- [Defining a Resource Profile on page 6](#)
- [Defining Resource Profile Autopolicies on page 132](#)
- [Defining Resource Profile Roles on page 133](#)
- [Defining Resource Profile Bookmarks on page 134](#)

Defining Resource Profile Resources

When you are defining a resource profile, you must specify the individual resource that you want to configure. Type type of profile that you choose is dependent on the type of resource you want to configure.

Table 8: Resource Profile Types and Configuration Information

Use this type of resource profile	To configure this type of resource
Web application/pages	URLs to Web applications, Web servers, and Web pages; Java applets that are stored on third party servers.
Host Java applet	Java applets that you upload directly to the Secure Access Service.
File browsing	Windows and UNIX/NFS servers, shares, and file paths
SAM client application	Client/server applications
WSAM destination	Destination networks or servers

Table 8: Resource Profile Types and Configuration Information (*continued*)

Telnet/SSH	Telnet or SSH servers
Terminal Services	Windows and Citrix terminal servers



NOTE: You cannot configure applications through VPN Tunneling using resource profiles. Instead, you must use roles and resource policies.

When defining resources, you can use Secure Access Service variables, such as <user> to dynamically link users to the correct resources. For instance, you can specify the following Web resource in order to direct users to their own individual intranet pages:

http://yourcompany.intranet/<user>

If the resource field of two different resource profiles are identical and both resource profiles are mapped to the same role, a user might view a resource policy from one profile and a resource policy from the other resource profile. For example, consider the following:

Resource Profile #1:

Resource Profile Name: Intranet

Resource Profile resource: http://intranet.company.com

Resource Profile Web ACL: http://intranet.company.com/sales/*

Mapped to Role: Sales

Resource Profile #2:

Resource Profile Name: Intranet for Sales

Resource Profile resource: http://intranet.company.com

Resource Profile Web ACL: http://intranet.company.com/sales/docs/*

The end-user that maps into the Sales role might see a bookmark name Intranet for Sales but the Web ACL enforcement will be http://intranet.company.com/sales/*:

This type of configuration is not supported.

Related Documentation

- [Defining a Resource Profile on page 6](#)
- [Defining Resource Profile Autopolicies on page 132](#)
- [Defining Resource Profile Roles on page 133](#)
- [Defining Resource Profile Bookmarks on page 134](#)

Defining Resource Profile Autopolicies

When you are defining a resource profile, you generally create autopolicies that establish the access requirements and other settings for the specified resource. The most common type of autopolicy enables access to the primary resource defined in the profile. Other policy types (such as compression and caching autopolicies) “fine-tune” how the Secure Access Service handles the data that it passes to and from the specified resource.

When creating resource profiles, the Secure Access Service only displays those autopolicies that are relevant to the resource profile type. For instance, you may choose to enable access to a client/server application through a WSAM resource profile. When you do, the Secure Access Service displays autopolicies that you can use to enable access to the specified application’s server. On the other hand, the Secure Access Service does not display Java access control autopolicies, since Java settings do not apply to WSAM.



NOTE: When defining access policies, you must explicitly list each hostname address. The policy checking system does not append or use the default domain or search domains in the Secure Access Service network settings.

Additionally, the Secure Access Service consolidates all of the relevant autopolicy options in a single page of the user interface, enabling you to understand all of the configuration possibilities and requirements for any given resource type.



NOTE: Access control autopolicies are generally based on the primary resource that you define in the resource profile. If you change the profile's primary resource, however, the Secure Access Service does not necessarily update the corresponding autopolicies. You should re-evaluate your autopolicies after changing the profile's primary resource.

For administrators who are accustomed to using a pre-5.3 version of the Secure Access Service product, note that autopolicies are resource policies. The Secure Access Service allows you to sort and order autopolicies along with standard resource policies in the Users > Resource Policies pages of the admin console. However, the Secure Access Service does not allow you to access more detailed configuration options for autopolicies through this section of the admin console. Instead, if you want to change the configuration of an autopolicy, you must access it through the appropriate resource profile.

For administrators who are accustomed to using a pre-5.3 version of the Secure Access Service product, note that you can also automatically create resource policies by enabling the Auto-allow option at the role level. However, note that we recommend that you use autopolicies instead, since they directly correspond to the resource you are configuring rather than all resources of a particular type. (You may also choose to enable the Auto-allow option for a role-level feature and create autopolicies for resources of the same type. When you do, the Secure Access Service creates policies for both and displays them in the appropriate resource policies page of the admin console.)

- Related Documentation**
- [Defining a Resource Profile on page 6](#)
 - [Defining Resource Profile Roles on page 133](#)
 - [Defining Resource Profile Bookmarks on page 134](#)

Defining Resource Profile Roles

Within a resource profile, you can assign user roles to the profile. For instance, you might create a resource profile specifying that members of the “Customers” role can access your company’s Support Center, while members of the “Evaluators” role cannot. When you assign user roles to a resource profile, the roles inherit all of the autopolicies and bookmarks defined in the resource profile.

Since the resource profile framework does not include options for creating roles, you must create user roles before you can assign them to resource profiles. However, the resource profile framework does include some user role configuration options. For instance, if you assign a user role to a Web resource profile, but you have not enabled Web rewriting for the role, the Secure Access Service automatically enables it for you.



NOTE: Note that you can assign roles to a resource profile through the Secure Access Service role framework as well as the resource profile framework.

- Related Documentation**
- [Defining a Resource Profile on page 6](#)
 - [Defining Resource Profile Autopolicies on page 132](#)
 - [Defining Resource Profile Bookmarks on page 134](#)

Defining Resource Profile Bookmarks

When you create a resource profile, the Secure Access Service generally creates a bookmark that links to the profile's primary resource (such as your company intranet's main page). Optionally, you may also create additional bookmarks that link to various sites within the primary resource's domain (such as the Sales and Marketing intranet pages). When you create these bookmarks, you can assign them to user roles, thereby controlling which bookmarks users see when they sign into the Secure Access Service end-user console.



NOTE: WSAM and JSAM resource profiles do not include bookmarks, since the Secure Access Service cannot launch the applications specified in the resource profiles.

For example, you may create a resource profile that controls access to your company intranet. Within the profile, you may specify:

- Resource profile name: Your Intranet
- Primary resource: `http://intranet.com`
- Web access control autopolicy: Allow access to `http://intranet.com:80/*`
- Roles: Sales, Engineering

When you create this policy, the Secure Access Service automatically creates a bookmark called "Your Intranet" enabling access to `http://intranet.com` and displays the bookmark to members of the Sales and Engineering roles.

You may then choose to create the following additional bookmarks to associate with the resource profile:

- "Sales Intranet" bookmark: Creates a link to the `http://intranet.com/sales` page and displays the link to members of the Sales role.
- "Engineering Intranet" bookmark: Creates a link to the `http://intranet.com/engineering` page and displays the link to members of the Engineering role.



NOTE: When configuring bookmarks, note that:

- You can only assign bookmarks to roles that you have already associated with the resource profile—not all of the roles defined on the Secure Access Service. To change the list of roles associated with the resource profile, use settings in its Roles tab.
- Bookmarks simply control which links the Secure Access Service displays to users—not which resources the users can access. For instance, in the example used above, a member of the Sales role would not see a link to the Engineering Intranet page, but he could access it by entering `http://intranet.com/engineering` in his Web browser's address bar. Similarly, if you delete a bookmark, users can still access the resource defined in the profile.
- The Secure Access Service allows you to create multiple bookmarks to the same resource. If you assign duplicate bookmarks to the same user role, however, the Secure Access Service only displays one of them to the users.
- Bookmarks link to the primary resource that you define in the resource profile (or a sub-directory of the primary resource). If you change the profile's primary resource, the Secure Access Service updates the corresponding bookmarks accordingly.

**Related
Documentation**

- [Defining a Resource Profile on page 6](#)
- [Defining Resource Profile Autopolicies on page 132](#)
- [Defining Resource Profile Roles on page 133](#)

Resource Profile Templates

Resource profile templates enable you to configure settings for specific applications. When you use this method, you choose a specific application (such as the Citrix NFuse version 4.0). Then, the Secure Access Service pre-populates a variety of values for you based on your chosen application and prompts you to configure additional settings as necessary.

Currently, the Secure Access Service includes templates for the following third-party applications:

- Citrix
- Lotus Notes
- Microsoft Outlook
- Microsoft Sharepoint
- NetBIOS file browsing

**Related
Documentation**

- [About Citrix Templates on page 467](#)
- [Creating Resource Profiles Using the Lotus iNotes Template on page 477](#)
- [Standard Application Support: MS Outlook on page 610](#)
- [Creating Resource Profiles Using the Microsoft Sharepoint Template on page 485](#)

CHAPTER 6

Virtual Desktop Resource Profiles

- [Virtual Desktop Resource Profile Overview on page 137](#)
- [Configuring a Citrix XenDesktop Resource Policy on page 138](#)
- [Configuring a VMware View Manager Resource Profile on page 139](#)
- [Defining Bookmarks for a Virtual Desktop Profile on page 140](#)
- [Configuring the Client Delivery on page 141](#)
- [Connecting to the Servers on page 142](#)

Virtual Desktop Resource Profile Overview

In addition to standard resource profiles and resource profile templates, you can configure virtual desktops as resource profiles.

As with the other resource profiles, a virtual desktop profile contains all of the role assignments and end-user bookmarks required to provide access to an individual resource. Unlike other resource profile types, there is no resource policy to configure for virtual desktops due to the dynamic nature of virtual desktops. The IP address and port of the system is not known until the end-user launches a session so dynamic ACLs are used.

Icons in the Virtual Desktops section on the end-user's home page represent desktops defined by the administrator. Clicking the icon launches the session using the Virtual Desktop Infrastructure (VDI) architecture.

A few of the main features of virtual desktop resource profiles are:

- SSO so that the user can sign on without having to enter their credentials
- Dynamic ACLs
- Client delivery mechanism for end-users who do not have the client already installed on their system
- Connection logging

Related Documentation

- [Configuring a Citrix XenDesktop Resource Policy on page 138](#)
- [Configuring a VMware View Manager Resource Profile on page 139](#)
- [Defining Bookmarks for a Virtual Desktop Profile on page 140](#)

- [Configuring the Client Delivery on page 141](#)
- [Connecting to the Servers on page 142](#)

Configuring a Citrix XenDesktop Resource Policy

The Citrix XenDesktop manages a pool of virtual desktops hosted on virtual machines and provides the connection management to those desktops. A list of XenDesktops is displayed to the end-user as bookmarks. When a desktop is selected, the Citrix client is launched and the user can access that desktop.

To configure a Citrix XenDesktop profile:

1. Select **Users > Resource Profiles > Virtual Desktops**.
2. Click **New Profile**.
3. Select **Citrix XenDesktop** from the Type drop-down list.
4. Enter a name and description (optional) to identify this profile.
5. Enter the name or IP address and port of the connection broker using the format *ip:port*. For example,

```
10.10.1.10:80  
xml.example.com:80
```

You can enter more than one IP address. Place each address on a separate line.

6. Select the **Use SSL for connecting to the Server** checkbox if SSL is required to connect to the server.
7. Enter the username to connect to the connection broker or use the <USERNAME> session variable.
8. Enter the password:
 - To use a variable password to connect to the connection broker, select **Variable Password** and enter the variable in the form of <PASSWORD> or <PASSWORD@SEcAuthServer>.
 - Select **Password** to use a static password to connect to the connection broker and enter the user credential's password.
9. Enter the domain where the connection broker is located.
10. Select **Enable Java support** to specify a Java applet to use to associate with the resource profile. The Secure Access Service uses this applet to intermediate traffic or falls back to this applet when ActiveX is not available on the user's system.
11. Click **Save and Continue**.
12. Select the roles to which this profile applies and click **Add**.

The Enabled Settings table under Users > User Roles also displays which roles have virtual desktops enabled.

13. Click **Save Changes**.
14. (Optional.) In the Bookmarks tab, modify the default bookmark created by the Secure Access Service and/or create new ones.

Related Documentation

- [Virtual Desktop Resource Profile Overview on page 137](#)
- [Configuring a VMware View Manager Resource Profile on page 139](#)
- [Defining Bookmarks for a Virtual Desktop Profile on page 140](#)
- [Configuring the Client Delivery on page 141](#)
- [Connecting to the Servers on page 142](#)

Configuring a VMware View Manager Resource Profile

VMware View Manager, formerly VMware VDI, lets you run virtual desktops in a datacenter that provide end-users a single view of all their applications and data in a personalized environment regardless of the device or location they log in from.

To configure a VMware View Manager profile:

1. Select **Users > Resource Profiles > Virtual Desktops**.
2. Click **New Profile**.
3. Select **VMware View Manager** from the Type drop-down list.
4. Enter a name and description (optional) to identify this profile.
5. Enter the name or IP address and port of the connection broker using the format *ip:port*. For example,
 - 10.10.1.10:80
 - xml.example.com:80

You can enter more than one IP address. Place each address on a separate line.
6. Select the **Use SSL for connecting to the Server** checkbox if SSL is required to connect to the server.
7. Enter the username to connect to the connection broker or use the <USERNAME> session variable.
8. Enter the password:
 - To use a variable password to connect to the connection broker, select **Variable Password** and enter the variable in the form of <PASSWORD> or <PASSWORD@SEcAuthServer>.
 - Select **Password** to use a static password to connect to the connection broker and enter the user credential's password.
9. Enter the domain where the View Manager server is located.
10. Click **Save and Continue**.

11. Select the roles to which this profile applies and click **Add**.

The Enabled Settings table under Users > User Roles also displays which roles have virtual desktops enabled.

12. Click **Save Changes**.
13. (Optional.) In the Bookmarks tab, modify the default bookmark created by the Secure Access Service and/or create new ones.

Related Documentation

- [Virtual Desktop Resource Profile Overview on page 137](#)
- [Configuring a Citrix XenDesktop Resource Policy on page 138](#)
- [Defining Bookmarks for a Virtual Desktop Profile on page 140](#)
- [Configuring the Client Delivery on page 141](#)
- [Connecting to the Servers on page 142](#)

Defining Bookmarks for a Virtual Desktop Profile

When you create a virtual desktop resource profile, the Secure Access Service automatically creates a bookmark that links to the server that you specified in the resource profile. The Secure Access Service allows you to modify this bookmark as well as create additional bookmarks to the same server.

These bookmarks are listed in the role bookmark pages (Users > User Roles > Role_Name > Virtual Desktop > Sessions) but you cannot add, modify or delete the bookmarks from the role bookmarks page. Bookmarks can only be added as part of the resource file.

To configure resource profile bookmarks for virtual desktop profiles:

1. Select **Users > Resource Profiles > Virtual Desktop**.
2. Click the name of the virtual desktop profile.
3. Click the Bookmark tab to modify an existing session bookmark. Or, click **New Bookmark** to create an additional session bookmark.
4. (Optional.) Change the name and description of the session bookmark. (By default, the Secure Access Service populates and names the session bookmark using the resource profile name.)
5. Specify whether all desktops or to a selected subset of desktops are available to the user.

The desktop list is retrieved from the connection broker using the credentials defined in the profile resource page.

6. Enter the credentials used to log in to the actual VMware or XenDesktop machine. The Secure Access Service passes these credentials to the server so that users can sign on without having to manually enter their credentials.
7. Specify how the window should appear to the user during a session by configuring options in the Settings area of the bookmark configuration page.

(XenDesktop) Under Preferred Client, you can select Automatic Detection, Citrix Client or Java. If you select Automatic Detection, the Secure Access Service checks to see if Citrix Client is present. If it is not present, the end-user is given the choice to download the Citrix Client or to use the alternate client, Java ICA Client.

8. Allow users to access local resources such as printers and drives through the terminal session by configuring options in the Connect Devices area of the bookmark configuration page.

(VMware) **Enable MMR**—Redirect certain multimedia codecs running on the remote desktop to the local client for rendering of full-motion video and audio.

(VMware) **Allow Desktop Reset**—Allow users to reset their desktop without administrative assistance. For example, if the desktop hangs, there is currently no way for the user to perform a hard reboot of the desktop. This option allows the users to restart their own virtual desktops thereby reducing the dependency on the administrator or helpdesk.

9. Specify how the terminal emulation window should appear to the user during a terminal session by configuring options in the Desktop Settings area.
10. Specify the roles to which you want to display the session bookmarks if you are configuring the session bookmark through the resource profile pages, under Roles:
 - **ALL selected roles**—Displays the session bookmark to all of the roles associated with the resource profile.
 - **Subset of selected roles**—Displays the session bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL Selected Roles list and click Add to move them to the Subset of selected roles list.
11. Click **Save Changes**.

Related Documentation

- [Defining Display Options for the Windows Terminal Services Session on page 655](#)
- [Virtual Desktop Resource Profile Overview on page 137](#)
- [Configuring a Citrix XenDesktop Resource Policy on page 138](#)
- [Configuring a VMware View Manager Resource Profile on page 139](#)
- [Configuring the Client Delivery on page 141](#)
- [Connecting to the Servers on page 142](#)

Configuring the Client Delivery

You can use the Virtual Desktop Configuration page to define the client delivery mechanism for end-users who do not have the client. The process is similar for both XenDesktop and VMware View Manager.

1. Choose **System > Configuration > Virtual Desktop**.
2. Select **Download from Secure Access Service** to download the client file from the Secure Access Service. Click **Browse** to locate the client file (.msi, .exe or .cab) and enter the version number.
3. Select **Download from a URL** to download the client file from the Internet. If desired, enter a new URL to override the default.
4. Check the **Access the URL through the Secure Gateway** checkbox if end-users can not directly access the specified web page. Selecting this option allows users to use the secure gateway to access the URL.
5. Under **Server Connection Timeout**, enter the number of seconds to wait for the server to respond before timing out.

- Related Documentation**
- [Virtual Desktop Resource Profile Overview on page 137](#)
 - [Connecting to the Servers on page 142](#)

Connecting to the Servers

When an end-user clicks a desktop icon, The Secure Access Service passes credentials to the server based on the desktop profile.

For XenDesktop, the Secure Access Service authenticates to the Citrix DDC server using credentials defined in the desktop profile. If successful, the list of available desktops is returned by the DDC server and is represented as bookmarks to the end-user. When an enduser clicks a XenDesktop icon, the Secure Access Service retrieves the ICA from the XenDesktop server and presents a desktop session to the user.

When an end-user clicks a VMware View Manager icon, the Secure Access Service authenticates to the View Manager using credentials defined in the desktop profile. If authentication is successful, a JSESSIONID cookie is returned by the View Manager, the Secure Access Service creates a tunnel using the cookie for the duration of the session.

If the desktop is unavailable, the client will continue to try to connect until the desktop is available or until a predefined timeout period occurs. An error message lets the user know the status, either that Secure Access Service is retrying the connection or that the desktop is unavailable. Similarly if the desktop is already in use by another enduser, an error message is presented to the user.

User logs are updated to show which VM machines are assigned to each user. Username, realm, VM IP, port, connection type, pool and connection broker are logged with each message.

The Active Virtual Desktops Sessions page (**System > Status > Virtual Desktop Sessions**) lists the active connections, including the connection broker, the VM machine assigned to the user and the connection type.

- Related Documentation**
- [Virtual Desktop Resource Profile Overview on page 137](#)
 - [Configuring the Client Delivery on page 141](#)

CHAPTER 7

Resource Policies

- [Resource Policies on page 143](#)
- [Resource Policy Components on page 144](#)
- [Specifying Resources for a Resource Policy on page 145](#)
- [Resource Policy Evaluation on page 147](#)
- [Creating Detailed Rules for Resource Policies on page 149](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)
- [Customizing Resource Policy UI Views on page 152](#)

Resource Policies

A resource policy is a system rule that specifies resources and actions for a particular access feature. A resource is either a server or file that can be accessed through Secure Access Service, and an action is to “allow” or “deny” a resource or to perform or not perform a function. Each access feature has one or more types of policies, which determine the Secure Access Service’s response to a user request or how to enable an access feature (in the case of Email Client). You may also define detailed rules for a resource policy, which enable you to evaluate additional requirements for specific user requests.

You can create the following types of resource policies through the Resource Policies pages of the Secure Access Service:

- **Web Resource Policies**—The Web resource policies specify the Web resources to which users may or may not browse. They also contain additional specifications such as header caching requirements, servers to which java applets can connect, code-signing certificates that the Secure Access Service should use to sign java applets, resources that the Secure Access Service should and should not rewrite, applications for which the Secure Access Service performs minimal intermediation, and single sign-on options.
- **File Resource Policies**—The file resource policies specify the Windows, UNIX, and NFS file resources to which users may or may not browse. They also contain additional specifications such as file resources for which users need to provide additional credentials.
- **Secure Application Manager Resource Policies**—The Secure Application Manager resource policies allow or deny access to applications configured to use JSAM or WSAM to make socket connections.

- **Telnet/SSH Resource Policies**—The Telnet/SSH resource policies allow or deny access to the specified servers.
- **Terminal Services Policies**—The Terminal Services resource policies allow or deny access to the specified Windows servers or Citrix Metaframe servers.
- **VPN Tunneling Resource Policies**—The VPN Tunneling resource policies allow or deny access to the specified servers and specify IP address pools.
- **Secure Email Client Resource Policies**—The Secure Email Client access resource policy allows you to enable or disable email client support. To allow end-users to open and save email attachments of different document types in OWA and iNotes, select the OWA or iNotes type when defining a Web Application Resource Profile.



NOTE: You can also create resource policies as part of the resource profile configuration process. In this case, the resource policies are called “advanced policies.”

Resource policies are an integral part of the Secure Access Service access management framework, and therefore are available on all Secure Access Service products. However, you can only access resource policy types that correspond to your licensed features. For instance, if you are using an SA700 Series appliance and have not purchased a Core Clientless Access upgrade license, you cannot create Web resource policy.

Related Documentation

- [Resource Policy Components on page 144](#)
- [Resource Policy Evaluation on page 147](#)
- [Creating Detailed Rules for Resource Policies on page 149](#)
- [Customizing Resource Policy UI Views on page 152](#)

Resource Policy Components

A resource policy contains the following information:

- **Resources**—A collection of resource names (URLs, host names, or IP address/netmask combinations) that specifies the resources to which the policy applies. You can specify a resource using a wildcard prefix to match host names. The default resource for a policy is star (*), meaning that the policy applies to all related resources.
- **Roles**—An optional list of user roles to which this policy applies. The default setting is to apply the policy to all roles.
- **Action**—The action for the Secure Access Service to take when a user requests the resource corresponding to the Resource list. An action may specify to allow or deny a resource or to perform or not perform an action, such as to rewrite Web content or allow Java socket connections.
- **Detailed Rules**—An optional list of elements that specifies resource details (such as a specific URL, directory path, file, or file type) to which you want to apply a different action or for which you want to evaluate conditions before applying the action. You

can define one or more rules and specify the order in which the Secure Access Service evaluates them.

Specifying Resources for a Resource Policy

The Secure Access Service platform's engine that evaluates resource policies requires that the resources listed in a policy's Resources list follow a canonical format. This section describes the canonical formats available for specifying Web, file, and server resources. When a user tries to access a specific resource, Secure Access Service compares the requested resource to the resources specified in the corresponding policies, starting with the first policy in a policy list. When the engine matches a requested resource to a resource specified in a policy's Resources list, it then evaluates further policy constraints and returns the appropriate action to the appliance (no further policies are evaluated). If no policy applies, then the appliance evaluates the auto-allow bookmarks (if defined); otherwise the default action for the policy is returned.



NOTE: You may not see the auto-allow option, if you are using a new installation, if you use resource profiles rather than resource policies, or if an administrator has hidden the option.

General Notes About the Canonical Formats

Please note the following when using canonical formats:

- If a path component ends with forward-slash_star (/*), then it matches the leaf node and everything below. If the path component ends with forwardslash_percent (/%), then it matches the leaf node and everything one-level below only. For example:

/intranet/* matches:

```
/intranet
/intranet/home.html
/intranet/eee/public/index.html
```

/intranet/% matches:

```
/intranet
/intranet/home.html
but NOT /intranet/eee/public/index.html
```

- A resource's host name and IP address are passed to the policy engine at the same time. If a server in a policy's Resources list is specified as an IP address, then the evaluation is based on the IP address. Otherwise, the engine tries to match the two host names—it does not perform a reverse-DNS-lookup to determine the IP.



NOTE: You cannot specify a host name for a VPN Tunneling resource policy. You can only specify an IP address.

- If a host name is not fully qualified in the hosts file, such as "juniper" instead of "intranet.juniper.net", and you are accessing a host name using the short name, then

the engine performs the resource matching against the short name. If, however, the short name is not in the hosts file and the host name resolution is done by DNS (by adding the domains listed in the Networks configuration page), then the fully qualified domain name (FQDN) is used for resource matching. In other words, for web resource policies a DNS lookup of the short name is performed. The result of the DNS lookup is a FQDN; the engine matches the FQDN with the ones entered in the UI.

Specifying Server Resources

When specifying server resources for Telnet/SSH, Terminal Services, or VPN Tunneling resource policies, note the following guidelines.

The canonical format is **[protocol://] host [:ports]**

The components are:

- Protocol (optional)—Possible case-insensitive values:
 - tcp
 - udp
 - icmp

If the protocol is missing, then all protocols are assumed. If a protocol is specified, then the delimiter “://” is required. No special characters are allowed.



NOTE: Available only to VPN Tunneling policies. For other access feature resource policies, such as Secure Application Manager and Telnet/SSH, it is invalid to specify this component.

- Host (required)—Possible values:
 - IP address/Netmask—The IP address needs to be in the format: *a.b.c.d*
The netmask may be in one of two formats:
 - Prefix: High order bits
 - IP: *a.b.c.d*
 For example: 10.11.149.2/24 or 10.11.149.2/255.255.255.0
No special characters are allowed.
 - DNS Hostname—For example: *www.juniper.com*
Special characters allowed include:

Table 9: DNS Hostname Special Characters

*	Matches ALL characters
%	Matches any character except dot (.)
?	Matches exactly one character



NOTE: You cannot specify a host name for a VPN Tunneling resource policy. You can only specify an IP address.

- Ports (optional)—Possible values:

Table 10: Port Possible Values

*	Matches ALL ports; no other special characters are allowed
port[,port]*	A comma-delimited list of single ports. Valid port numbers are [1- 65535]. Do not enter a space between port numbers. You can specify up to 15 ports.
[port1]-[port2]	A range of ports, from port1 to port2, inclusive.



NOTE: You may mix port lists and port ranges, such as: 80,443,8080-8090, except for in VPN Tunneling where mixing of port lists and port ranges is not supported.

If the port is missing, then the default port 80 is assigned for http, 443 for https. For VPN Tunneling, if the port is missing then the default port http is *. If a port is specified, then the delimiter ":" is required. For example:

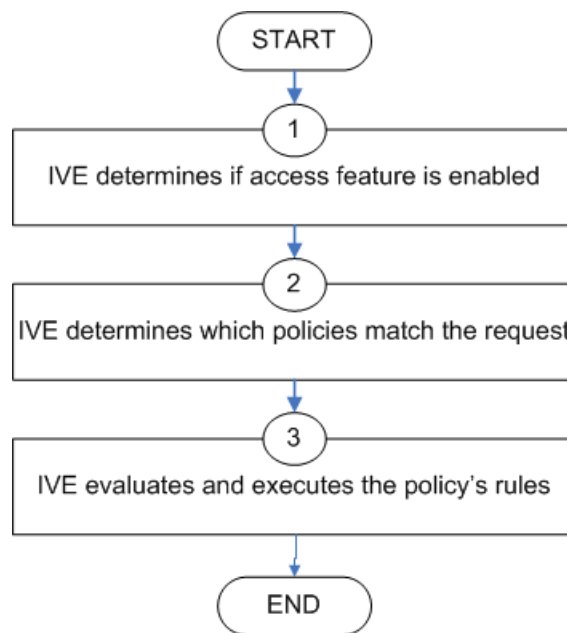
```
<username>.danastreet.net:5901-5910
tcp://10.10.149.149:22,23
tcp://10.11.0.10:80
udp://10.11.0.10:*
```

Resource Policy Evaluation

When Secure Access Service receives a user request, it evaluates the resource policies corresponding to the type of request. When it processes the policy that corresponds to the requested resource, it applies the specified action to the request. This action is defined on the policy's General tab or Detailed Rules tab. For example, if a user requests a Web page, the Secure Access Service knows to use the Web resource policies. In the case of Web requests, the Secure Access Service always starts with the Web Rewriting policies (Selective Rewriting and Pass through Proxy) to determine whether or not to handle the request. If none of these policies applies (or none is defined), the Secure Access Service then evaluates the Web Access policies until it finds one that pertains to the requested resource.

The Secure Access Service evaluates a set of resource policies for an access feature from the top down, meaning that it starts with the policy numbered one and then continues down the policy list until it finds a matching policy. If you defined detailed rules for the matching policy, the Secure Access Service evaluates the rules from the top down, starting with the rule numbered one and stopping when it finds a matching resource in the rule's Resource list. The following diagram illustrates the general steps of policy evaluation:

Figure 8: Resource Policy Evaluation Steps



Details regarding each evaluation step:

1. The Secure Access Service receives a user request and evaluates the user's session role to determine if the corresponding access feature is enabled. A user's "session role" is based on either the role or roles to which the user is assigned during the authentication process. The access features enabled for a user are determined by an authentication realm's role mapping configuration.
2. The Secure Access Service determines which policies match the request. The Secure Access Service evaluates the resource policies related to the user request, sequentially processing each policy until finding the one whose resource list and designated roles match the request. (If you configure the Secure Access Service using resource profiles, the Secure Access Service evaluates the advanced policies that you configure as part of the resource profile.)

The Web and file access features have more than one type of policy, so the Secure Access Service first determines the type of request (such as to a Web page, Java applet, or UNIX file) and then evaluates the policies related to the request. In the case of the Web access feature, the Rewriting policies are evaluated first for every Web request. The remaining five access features—Secure Application Manager, Secure Terminal Access, and Secure Email Client—have only one resource policy.

3. The Secure Access Service evaluates and executes the rules specified in the matching policies. You can configure policy rules to do two things:
 - Specify resources to which an action applies at a more granular level. For example, if you specify a Web server in the main policy settings for a Web Access resource policy, you can define a detailed rule that specifies a particular path on this server and then change the action for this path.

- Require the user to meet specific conditions written as boolean expressions or custom expressions in order to apply the action.
4. The Secure Access Service stops processing resource policies as soon as the requested resource is found in a policy's Resource list or detailed rule.



NOTE: If you use automatic (time-based) dynamic policy evaluation or you perform a manual policy evaluation, the Secure Access Service repeats the resource evaluation process described in this section.

Related Documentation

- [User Roles Overview on page 105](#)
- [Creating Detailed Rules for Resource Policies on page 149](#)
- [Dynamic Policy Evaluation on page 77](#)

Creating Detailed Rules for Resource Policies

The Web, file, Secure Application Manager, Telnet/SSH, and VPN Tunneling access features enable you to specify resource policies for individual Web, file, application, and telnet servers. The Email Client access features have one policy that applies globally. For these policies, you specify server settings that are used for every role that enables these access features. For all other access features, you can specify any number of resource policies, and for each, you can define one or more detailed rules.

A detailed rule is an extension of a resource policy that may specify:

- Additional resource information—such as a specific path, directory, file, or file type—for resources listed on the General tab. Note that you may also specify the same resource list (as on the General tab) for a detailed rule if the only purpose of the detailed rule is to apply conditions to a user request.
- An action different from that specified on the General tab (although the options are the same).
- Conditions that must be true in order for the detailed rule to apply.

In many cases, the base resource policy—that is, the information specified on the General tab of a resource policy—provides sufficient access control for a resource:

If a user belonging to the (defined_roles) tries to access the (defined_resources), DO the specified (resource_action).

You may want to define one or more detailed rules for a policy when you want to perform an action based on a combination of other information, which can include:

- A resource's properties, such as its header, content-type, or file type.
- A user's properties, such as the user's username and roles to which the user maps.

- A session's properties, such as the user's source IP or browser type, whether the user is running Host Checker or Cache Cleaner, the time of day, and certificate attributes.

Detailed rules add flexibility to resource access control by enabling you to leverage existing resource and permission information to specify different requirements for different users to whom the base resource policy applies.

Related Documentation

- [Writing a Detailed Rule for Resource Policies on page 150](#)

Writing a Detailed Rule for Resource Policies

Detailed rules add flexibility to resource access control by enabling you to leverage existing resource and permission information to specify different requirements for different users to whom the base resource policy applies.

To write a detailed rule for a resource policy:

1. On the New Policy page for a resource policy, enter the required resource and role information.
2. In the Action section, select **Use Detailed Rules** and then click **Save Changes**.
3. On the Detailed Rules tab, click **New Rule**.
4. On the Detailed Rule page:
 - In the Action section, specify:
 - **Disable SSO**—The Secure Access Service disables automatic SSO authentication for this user role and, instead, prompts the user for sign-in credentials.
 - **Basic**—This option specifies that the Secure Access Service use the Basic Authentication Intermediation method to control SSO behavior.

Enable Intermediation—Select the credentials to use. If this pull-down menu is blank, no basic authentication SSO settings are defined in the SSO General tab.

Disable Intermediation—When you select this option, the Secure Access Service does not intermediate the challenge/response sequence.



NOTE: The Secure Access Service always intermediates requests to Web proxies that require basic authentication, even if you select **Disable Intermediation**.

Although you are given an option to disable basic authentication intermediation, we do not recommend this option, as it is a very insecure authentication method and, in some cases, can transmit user credentials over the network in clear (unencrypted) text.

- **NTLM**—This option specifies that the Secure Access Service use the Microsoft NTLM Intermediation method to control SSO behavior.

Select the credentials to use. If this pull-down menu is blank, no NTLM SSO settings are defined in the SSO General tab.

Select the **Fallback to NTLM V1** option to try both NTLM V1 and NTLM V2. If you do not select this option, the Secure Access Service falls back only to NTLM V2. An intermediation page appear if SSO fails.

- **Kerberos**—This option specifies that the Secure Access Service use the Kerberos Intermediation method to control SSO behavior.

Select the credentials to use. If this pull-down menu is blank, no kerberos SSO settings are defined in the SSO General tab.

Select the **Fallback to NTLM V2** option to fallback only to NTLM V2 if kerberos fails. If you do not select this option, a Kerberos intermediation page appears if Kerberos SSO fails.

- **Constrained Delegation**—This option specifies that the Secure Access Service use the constrained delegation intermediation method to control SSO behavior.

Select the credentials to use. If this pull-down menu is blank, no constrained delegation SSO settings are defined in the SSO General tab.

Select the **Fallback to Kerberos** option fallback to Kerberos if constrained delegation fails. If you select this option, an intermediation page appears if constrained delegation fails. If you do not select this option and constrained delegation fails, an error page appears.

- In the Resources section, specify any of the following (required):
 - The same or a partial list of the resources specified on the General tab.
 - A specific path or file on the server(s) specified on the General tab, using wildcards when appropriate. For information about how to use wildcards within a Resources list, see the documentation for the corresponding resource policy.
 - A file type, preceded by a path if appropriate or just specify `*/*.file_extension` to indicate files with the specified extension within any path on the server(s) specified on the General tab.
- In the Conditions section, specify one or more expressions to evaluate in order to perform the action (optional):
 - Boolean expressions: Using system variables, write one or more boolean expressions using the NOT, OR, or AND operators.
 - Custom expressions: Using the custom expression syntax, write one or more custom expressions.



NOTE: You can use the <USER> substitution variable in ACLs for web pages, telnet, files, and SAM. You cannot use the variable in VPN Tunneling ACLs.

When specifying a time condition, the specified time range cannot cross midnight. The workaround is to break the time range into two conditions.

- Click **Save Changes**.
- 5. On the Detailed Rules tab, order the rules according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a rule's Resource list, it performs the specified action and stops processing rules (and other resource policies).

**Related
Documentation**

- [Writing the Basic, NTLM and Kerberos Resources on page 523](#)
- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)
- [Elements Used in Custom Expressions on page 1182](#)

Customizing Resource Policy UI Views

You can limit which resource policies the Secure Access Service displays on any given resource policy page based on user roles. For instance, you can configure the Users > Resource Policies > Web page of the admin console to only display those resource policies that are assigned to the "Sales" user role.

To control which resource policies the Secure Access Service displays:

1. Navigate to **Users > Resource Policies > Policy Type**.
2. From the Show all policies that apply to list, select **All Roles** or an individual role.
3. Click **Update**. The Secure Access Service displays resource policies that are assigned to the selected roles.

CHAPTER 8

Authentication and Directory Servers

- [About Authentication and Directory Servers on page 154](#)
- [Task Summary: Configuring Authentication Servers on page 155](#)
- [About Anonymous Servers on page 156](#)
- [Defining an Anonymous Server Instance on page 157](#)
- [Using an RSA ACE/Server on page 158](#)
- [Defining an ACE/Server Instance on page 159](#)
- [Using an RSA ACE/Server with a Secure Access Service Cluster on page 161](#)
- [Using Active Directory or NT Domains on page 163](#)
- [Defining an Active Directory or Windows NT Domain Server Instance on page 164](#)
- [Configuring a Role-Mapping Rule Based on the Active Directory LDAP Primary Group on page 168](#)
- [Multi-Domain User Authentication on page 169](#)
- [Join Domain for Active Directory-based Authentication Server Without Using a Domain Admin Account on page 170](#)
- [Using the Kerberos Debugging Tool on page 172](#)
- [Active Directory and NT Group Lookup Support on page 172](#)
- [Certificate Server on page 173](#)
- [Configuring a Certificate Server Instance on page 174](#)
- [Using an LDAP Server on page 175](#)
- [Defining an LDAP Server Instance on page 176](#)
- [Configuring LDAP Search Attributes for Meeting Creators on page 178](#)
- [Enabling LDAP Password Management on page 179](#)
- [Using a Local Authentication Server on page 184](#)
- [Defining a Local Authentication Server Instance on page 184](#)
- [Creating User Accounts on a Local Authentication Server on page 186](#)
- [Creating User Accounts From the Secure Gateway Home Page on page 188](#)
- [Configuring an NIS Server Instance on page 190](#)
- [Configuring a RADIUS Server Instance on page 191](#)

- [Defining a Secure Access Service RADIUS Server Instance on page 192](#)
- [Enabling RADIUS Accounting on page 195](#)
- [General RADIUS Notes on page 206](#)
- [eTrust SiteMinder Overview on page 207](#)
- [Configuring SiteMinder to Work with the Secure Access Service on page 211](#)
- [Configuring the SiteMinder Agent on page 212](#)
- [Creating a SiteMinder Authentication Scheme for the Secure Access Service on page 213](#)
- [Creating a SiteMinder Domain for the Secure Access Service on page 215](#)
- [Creating a SiteMinder Realm for the Secure Access Service on page 215](#)
- [Creating a Rule/Response Pair to Pass Usernames to the Secure Access Service on page 216](#)
- [Configuring Secure Access to Work with SiteMinder on page 217](#)
- [Using SiteMinder User Attributes for Secure Access Role Mapping on page 227](#)
- [Defining a SiteMinder Realm for Automatic Sign-In on page 227](#)
- [Debugging SiteMinder and Secure Access Issues on page 228](#)
- [Defining a SAML Server Instance on page 229](#)

About Authentication and Directory Servers

An authentication server is a database that stores user credentials—username and password—and typically group information. When a user signs in to the Secure Access Service appliance, the user specifies an authentication realm, which is associated with an authentication server. If the user meets the realm's authentication policy, the Secure Access Service forwards the user's credentials to the associated authentication server. The authentication server's job is to verify that the user exists and is who she claims to be. After verifying the user, the authentication server sends approval to the Secure Access Service and, if the realm also uses the server as a directory/attribute server, the user's group information or other user attribute information. The Secure Access Service then evaluates the realm's role mapping rules to determine to which user roles the user may be mapped.

The Secure Access Service appliance supports the most common authentication servers, including Windows NT Domain, Active Directory, RADIUS, LDAP, NIS, RSA ACE/Server, and eTrust SiteMinder, and enables you to create one or more local databases of users who are authenticated by the Secure Access Service.

A directory server is a database that stores user and typically group information. You can configure an authentication realm to use a directory server to retrieve user or group information for use in role mapping rules and resource policies. Currently, the Secure Access Service supports LDAP servers for this purpose, which means you can use an LDAP server for both authentication and authorization. You simply need to define one server instance, and then the LDAP server's instance name appears in both the Authentication and Directory/Attribute drop-down lists on a realm's General tab. You can use the same server for any number of realms.

In addition to LDAP, you can use a RADIUS or SiteMinder server for retrieving user attributes that can be used in role mapping rules. Unlike an LDAP server instance, however, a RADIUS or SiteMinder server instance name does not appear in a realm's Directory/Attribute drop-down list. To use a RADIUS or SiteMinder server to retrieve user information, you simply choose its instance name in the Authentication list and then choose Same as Above in the Directory/Attribute list. Then, you configure role mapping rules to use attributes from the RADIUS or SiteMinder server, which the Secure Access Service provides in an attribute list on the Role Mapping Rule page after you select Rule based on User attribute.

Authentication servers are an integral part of the Secure Access Service access management framework, and therefore available on all Secure Access Service products. Note, however, that the eTrust SiteMinder server is not available on the SA700 Series appliance.

**Related
Documentation**

- [Task Summary: Configuring Authentication Servers on page 155](#)

[Task Summary: Configuring Authentication Servers](#)

To specify an authentication server that a realm may use, you must first configure a server instance on the Authentication > Auth. Servers page. When you save the server's settings, the server name (the name assigned to the instance) appears on the realm's General tab in the Authentication drop-down list. If the server is a(n):

- **LDAP or Active Directory server**—The instance name also appears in the Directory/Attribute drop-down list on the realm's General tab. You may use the same LDAP or Active Directory server for both authentication and authorization for a realm, as well as use these servers for authorization for any number of realms that use different authentication servers.
- **RADIUS server**—The instance name also appears in the Accounting drop-down list on the realm's General tab. You may use the same RADIUS server for both authentication and accounting for a realm, as well as use these servers for accounting for any number of realms that use different authentication servers.

Use the Auth. Servers page to define authentication server instances. Authentication servers authenticate user credentials and authorization servers provide user information that the Secure Access Service uses to determine user privileges within the system. For example, you can specify a certificate server instance to authenticate users based on their client-side certificate attributes and then create an LDAP server instance to authorize the users based on values contained within a CRL (certificate revocation list).

To configure authentication servers:

1. Set up your authentication/authorization server using instructions from the provider.
2. Create an instance of the server starting at the **Authentication > Authentication > Auth. Servers** page in the admin console.

**NOTE:**

- An authentication server must be able to contact the Secure Access Service. If an authentication server such as RSA ACE/Server does not use IP addresses for the agent hosts, the authentication server must be able to resolve the Secure Access Service host name, either through a DNS entry or an entry in the authentication server's host file.
- You can only create one eTrust Siteminder server instance per the Secure Access Service.
- If you authenticate your Active Directory server with:
 - NTLM protocol—Choose Active Directory/Windows NT Domain.
 - LDAP protocol—Choose LDAP Server.
- If you are creating a local authentication server instance to authenticate user administrators, you must select **Local Authentication**.

- a. Select a server type from the **New** drop-down list.
 - b. Click **New Server**.
 - c. Depending on which server you selected, specify settings for the individual server instance.
3. Create an authentication realm using settings in the **Users > User Realms** or **Administrators > Admin Realms** page of the admin console.
 4. Local authentication servers only: Add users to the server using settings in the **Authentication > Auth. Servers > Select Local Server > Users** page of the admin console.
 5. Password management only: set up password management options.

Related Documentation

- [About Authentication and Directory Servers on page 154](#)

About Anonymous Servers

The anonymous server feature allows users to access the Secure Access Service without providing a username or password. Instead, when a user enters the URL of a sign-in page that is configured to authenticate against an anonymous server, the Secure Access Service bypasses the standard sign-in page, and immediately displays the welcome page to the user.

You may choose to use anonymous authentication if you think that the resources on the Secure Access Service do not require extreme security, or if you think that other security measures provided through the Secure Access Service are sufficient. For example, you may create a user role with limited access to internal resources, and then authenticate that role with a policy that only requires users to sign in from an IP address that resides within your internal network. This method presumes that if a user can access your internal network, s/he is qualified to view the limited resources provided through the user role.

Anonymous Server Restrictions

When defining and monitoring an anonymous server instance, note that:

- You can only add one anonymous server configuration.
- You cannot authenticate administrators using an anonymous server.
- During configuration, you must choose the anonymous server as both the authentication server and the directory/attribute server in the Users > User Realms > General tab.
- When creating role mapping rules through the Users > User Realms > Role Mapping tab, the Secure Access Service does not allow you to create mapping rules that apply to specific users (such as “Joe”), since the anonymous server does not collect username information. You can only create role mapping rules based on a default username (*), certificate attributes, or custom expressions.
- For security reasons, you may want to limit the number of users who sign in through an anonymous server at any given time. To do this, use the option on the Users > User Realms > [Realm] > Authentication Policy > Limits tab (where [Realm] is the realm that is configured to use the anonymous server to authenticate users).
- You cannot view and delete the sessions of anonymous users through a Users tab (as you can with other authentication servers), because the Secure Access Service cannot display individual session data without collecting usernames.

Related Documentation

- [Task Summary: Configuring Authentication Servers on page 155](#)
- [Defining an Anonymous Server Instance on page 157](#)

Defining an Anonymous Server Instance

To define an anonymous server:

1. In the admin console, select **Authentication > Auth. Servers**.
2. Do one of the following:
 - To create a new server instance on the Secure Access Service, select **Anonymous Server** from the New list, and then click **New Server**.
 - To update an existing server instance, click the appropriate link in the Authentication/Authorization Servers list.
3. Specify a name to identify the server instance.
4. Click **Save Changes**.
5. Specify which realms should use the server to authorize users.

Related Documentation

- [About Anonymous Servers on page 156](#)
- [Task Summary: Configuring Authentication Servers on page 155](#)

Using an RSA ACE/Server

When authenticating users with an RSA ACE/Server, users may sign in using two methods:

- **Using a hardware token and the standard Secure Access Service sign-in page**—The user browses to the standard Secure Access Service sign-in page, then enters the username and password (consisting of the concatenation of the PIN and the RSA SecurID hardware token's current value). The Secure Access Service then forwards the user's credentials to ACE/Server.
- **Using a software token and the custom SoftID Secure Access Service sign-in page**—The user browses to the SoftID custom sign-in page. Then, using the SoftID plug-in, the user enters the username and PIN. The SoftID plug-in generates a pass phrase by concatenating the user's PIN and token and passes the pass phrase to the Secure Access Service. For information about enabling the SoftID custom sign-in pages, see <http://www.juniper.net/techpubs/software/ive/admin/j-sa-sslvpn-7.0-customsigninpages.pdf>.

If the ACE/Server positively authenticates the user, the user gains access to the Secure Access Service. Otherwise, the ACE/Server:

- Denies the user access to the system if the user's credentials were not recognized.
- Prompts the user to generate a new PIN (New PIN mode) if the user is signing in to the Secure Access Service for the first time. Users see different prompts depending on the method they use to sign in. If the user signs in using the SoftID plug-in, they see the RSA prompts for creating a new pin; otherwise the user sees the Secure Access Service prompts.
- Prompts the user to enter the next token (Next Token mode) if the token entered by the user is out of sync with the token expected by ACE/Server. Next Token mode is transparent to users signing in using a SoftID token. The RSA SecurID software passes the token through the Secure Access Service to ACE/Server without user interaction.
- Redirects the user to the standard Secure Access Service sign-in page (SoftID only) if the user tries to sign-in to the RSA SecurID Authentication page on a computer that does not have the SecurID software installed.

When a user enters the New PIN or Next Token mode, they have three minutes to enter the required information before the Secure Access Service cancels the transaction and notifies the user to re-enter their credentials.

The Secure Access Service can handle a maximum of 200 ACE/Server transactions at any given time. A transaction only lasts as long as is required to authenticate against the ACE/Server. For example, when a user signs into the Secure Access Service, the ACE/Server transaction is initiated when the user submits the request for authentication and ends once the ACE/Server has finished processing the request. The user may then keep their Secure Access Service session open, even though her ACE/Server transaction is closed.

The Secure Access Service supports the following ACE/Server features: New PIN mode, Next Token mode, DES/SDI encryption, AES encryption, slave ACE/Server support, name

locking, and clustering. The Secure Access Service also supports the New PIN and Next Token modes of RSA SecurID through the RADIUS protocol.

Due to UNIX limitations of the ACE/Server library, you may define only one ACE/Server configuration.

The Secure Access Service does not support customizing the load balancing algorithm.

Related Documentation

- [Defining an ACE/Server Instance on page 159](#)
- [Using an RSA ACE/Server with a Secure Access Service Cluster on page 161](#)
- [Task Summary: Configuring Authentication Servers on page 155](#)

Defining an ACE/Server Instance

To define an ACE/Server:

1. Generate an ACE/Agent configuration file (sdconf.rec) for the Secure Access Service on the ACE server as follows:
 - a. Start the ACE/Server Configuration Management application and click **Agent Host**.
 - b. Click **Add Agent Host**.
 - c. For **Name**, enter a name for the Secure Access Service agent.
 - d. For **Network Address**, enter the IP address of the Secure Access Service.
 - e. Enter a **Site** configured on your ACE server.
 - f. For Agent Type, select **Communication Server**.
 - g. For Encryption Type, select **DES**.
 - h. Verify that **Sent Node Secret** is not selected (when creating a new agent).

The first time that the ACE server successfully authenticates a request sent by the Secure Access Service, the ACE server selects Sent Node Secret. If you later want the ACE server to send a new Node Secret to the Secure Access Service on the next authentication request, do the following:

- i. Click the **Sent Node Secret** check box to uncheck it.
- ii. Sign in to the admin console and choose **Authentication > Auth. Servers**.
- iii. Click the name of the ACE server in the Authentication/Authorization Servers list. If this is the initial configuration of the server, see instructions for creating the ACE server instance that follow this procedure.
- iv. Under Node Verification File, select the appropriate check box and click **Delete**. These steps ensure that the Secure Access Service and ACE server are in sync. Likewise, if you delete the verification file from the Secure Access Service, you should uncheck the **Sent Node Secret** check box on the ACE server.

If you use RSA ACE/Server authentication and change the Secure Access Service IP address, you must delete the node verification file on the Secure Access for ACE/Server authentication to work. Also, deselect the Sent Node Verification setting on the ACE/Server for the Secure Access Service.

- i. Click **Assign Acting Servers** and select your ACE server.
 - j. Click **Generate Config File**. When you add the ACE server to the Secure Access Service, you will import this configuration file.
2. In the admin console choose **Authentication > Auth. Servers**.
 3. Do one of the following:
 - To create a new server instance on the Secure Access Service, select **ACE Server** from the New list, and then click **New Server**.
 - To update an existing server instance, click the appropriate link in the Authentication/Authorization Servers list.
 4. Specify a name to identify the server instance.
 5. Specify a default port in the **ACE Port** field. Note that the Secure Access Service only uses this setting if no port is specified in the sdconf.rec file.
 6. Import the RSA ACE/Agent configuration file. Make sure to update this file on the Secure Access Service anytime you make changes to the source file. Likewise, if you delete the instance file from the Secure Access Service, go to the ACE Server Configuration Management application,
 7. Click **Save Changes**. If you are creating the server instance for the first time, the Settings and Users tabs appear.
 8. Specify which realms should use the server to authenticate and authorize administrators and users.

You can monitor and delete the sessions of users who are currently signed in through the server through the System > Status > Active Users page.

Related Documentation

- [Task Summary: Configuring Authentication Servers on page 155](#)
- [Using an RSA ACE/Server on page 158](#)
- [Using an RSA ACE/Server with a Secure Access Service Cluster on page 161](#)

Using an RSA ACE/Server with a Secure Access Service Cluster

There are six tasks required to integrate RSA SecurID with a Secure Access Service cluster (Active/Active or Active/Passive):

1. Add each Secure Access Service node as an Agent Host in the RSA Authentication Manager database.
2. Generate the **sdconf.rec** file.
3. Add the ACE server to the Secure Access Service configuration and import the **sdconf.rec** file.
4. Bind the ACE server to a Secure Access Service authentication realm.
5. Configure role mapping rules.
6. Verify the system functions as expected.

To integrate RSA SecurID with a Secure Access Service cluster:

1. Add each Secure Access Service node as an Agent Host in the RSA Authentication Manager database:
 - a. On the RSA Authentication Manager host computer, go to **Start > All Programs > RSA Security > RSA Authentication Manger Host Mode** to display the RSA Authentication Manager.
 - b. From the menu bar, select **Agent Host > Add Agent Host** to display the Edit Agent Host dialog box.
 - c. Complete the following settings:
 - For Name, type the hostname of the first Secure Access Service cluster node. Let's call this Node A.
 - For Network Address, type the Secure Access Service internal interface IP address.
 - For Agent Type, select **Communication Server**.
 - For Encryption Type, select your encryption method. The Secure Access Service supports SDI and DES encryption.
 - Assign users to the Agent Host either by selecting **Open to All Locally Known Users** or clicking **User Activations**.
 - d. Click **OK** to add the Secure Access Service as an Agent Host to the RSA Authentication Manager database.
 - e. Repeat the previous steps for the second Secure Access Service cluster node. Let's call this Node B.
2. Generate the **sdconf.rec** file:

- a. From the RSA Authentication Manager menu bar, select **Generate Configuration File > One Agent Host** to display the Generate Agent Host dialog box.
 - b. Select **One Agent Host** and click **OK** to display the Select Agent Host dialog box.
 - c. Select one of the Agent Host configurations you completed for the Secure Access Service cluster and click **OK**.
 - d. Save the **sdconf.rec** file to your localhost or to a location you can access when you use the Secure Access Service admin console. In the next step, you import this file into the Secure Access Service.
3. Add the ACE server to the Secure Access Service configuration and import the **sdconf.rec** file:
- a. In the Secure Access Service admin console, go to **Authentication > Auth. Servers**.
 - b. Do one of the following:
 - To create a new server instance, select **ACE Server** from the New list, and then click **New Server**.
 - To update an existing server instance, click the appropriate link in the Authentication/Authorization Servers list.
 - c. Complete the following settings.
 - For Name, enter a name to identify the ACE server instance.
 - For Port, change if necessary. The default is 5500. Note that the Secure Access Service only uses this setting if no port is specified in the **sdconf.rec** file.
 - For Import New Config File, click the **Browse** button and upload the **sdconf.rec** file.
 - d. Click **Save Changes**.



NOTE: Under Node Verification File on the ACE server configuration page, the Creation Time column is blank. This is not filled in until at least one user authenticates successfully to each of the nodes. You must log into the physical IP of each node to allow the Secure Access Service and the ACE server to negotiate a node secret on first successful login.

4. Bind the ACE server to a Secure Access Service authentication realm.
- a. In the admin console, go to **Users > Roles** and create a role for SecureID users based on your secure access policies.
 - b. Go to **Users > Realm > New** and enter the appropriate information for the authentication realm. Select the ACE server you created and click **Save Changes**.

5. Configure role mapping rules.
 - a. Go to **Users > Realm** and click the link for the user Realm you created.
 - b. Click the **Role-Mapping** tab.
 - c. Click **New Rule** and create a new rule.

Configuration is complete. SecurID authentication is enabled on the Secure Access Service. Users can log in with their username and SecureID passcode.

6. Verify the system is functioning as expected:
 - a. Open a browser to the Node A physical IP address and log in using your SecurID passcode.
 - b. In the admin console, go to **Authentication > Auth. Servers** and click the link for the ACE Server.
 - c. Under Node Verification File on the ACE server configuration page, note that the Creation Time column is no longer blank. It shows the timestamp for the first successful login using the ACE server. This indicates that the Secure Access Service and the ACE server negotiated a node secret on first successful login.
 - d. Repeat these verification steps for Node B.

Related Documentation

- [Using an RSA ACE/Server on page 158](#)
- [Creating an Authentication Realm on page 306](#)
- [Specifying Role Mapping Rules for an Authentication Realm on page 309](#)

Using Active Directory or NT Domains

When authenticating users with an NT Primary Domain Controller (PDC) or Active Directory, users sign in to the Secure Access Service using the same username and password they use to access their Windows desktops. The Secure Access Service supports Windows NT authentication and Active Directory using NTLM or Kerberos authentication.

If you configure a native Active Directory server, you may retrieve group information from the server for use in a realm's role mapping rules. In this case, you specify the Active Directory server as the realm's authentication server, and then you create a role mapping rule based on group membership. The Secure Access Service displays all groups from the configured domain controller and its trusted domains.

The Secure Access Service provides separate check boxes for each of the primary authentication protocols: Kerberos, NTLMv2, and NTLMv1, allowing you to select or ignore each of these protocols independent of one another. This more granular control of the authentication process avoids unnecessarily raising the failed login count policy in Active Directory and lets you fine-tune the protocols based on your system requirements.



NOTE:

- We do not support interoperation with Active Directory implementations that use the equal sign operator (=) in a group name, such as: "\=THIRD FLOOR GROUP". Authentication processing by the Secure Access Service involves search operations that use the equal sign operator (=) when parsing server catalogs to retrieve group names, user names and domain names, as well as user_SID and domain_SID values. You might encounter unexpected behavior that can affect normal processing of authentication services if a group name configured on your Active Directory server includes an equal sign operator (=).
- The Secure Access Service honors trust relationships in Active Directory and Windows NT environments.
- When sending user credentials to an Active Directory authentication server, the Secure Access Service uses whichever authentication protocol(s) you specify on the New Active Directory/Windows NT page. The Secure Access Service defaults to the authentication protocols in order. In other words, if you have selected the check boxes for Kerberos and NTLMv2, the Secure Access Service sends the credentials to Kerberos. If Kerberos succeeds, the Secure Access Service does not send the credentials to NTLMv2. If Kerberos is not supported or fails, the Secure Access Service uses NTLMv2 as the next protocol in order. The configuration sets up a cascading effect if you choose to use it by setting multiple check boxes.
- The Secure Access Service supports Domain Local Groups, Domain Global Groups, and Universal Groups defined in the Active Directory forest.
- The Secure Access Service allows only Active Directory security groups, not distribution groups. Security groups allow you to use one type of group for not only assigning rights and permissions, but also as a distribution list for email.
- If multiple Active Directory servers are configured on the Secure Access Service, each of the servers must be associated with a different and unique machine account name. The same machine account name should not be used for all servers.

Related Documentation

- [Defining an Active Directory or Windows NT Domain Server Instance on page 164](#)
- [About Basic, NTLM and Kerberos Resources on page 522](#)

Defining an Active Directory or Windows NT Domain Server Instance

To define an Active Directory or Windows NT Domain server:

1. In the admin console, choose **Authentication > Auth. Servers**.
2. Do one of the following:

- To create a new server instance on Secure Access Service, select **Active Directory/Windows NT** from the New list and then click **New Server**.
 - To update an existing server instance, click the appropriate link in the Authentication/Authorization Servers list.
3. Specify a name to identify the server instance.
 4. Specify the name or IP address for the primary domain controller or Active Directory server.
 5. (Optional). Specify the IP address of your back-up domain controller or Active Directory server.
 6. Enter the NetBios domain name of the Active Directory or Windows NT domain. For example, if the Active Directory domain name is us.amr.asgqa.net and you want to authenticate users who belong to the US domain, enter US in the domain field.
 7. Select the **Allow domain to be specified as part of username** check box to allow users to sign in by entering a domain name in the Username field in the format: domain\username
 8. Select the **Allow trusted domains** check box to get group information from all trusted domains within a forest.
 9. Select the **Domain Controller is a Windows 2008 server** check box if the backend domain controller is a Windows 2008 server. The Windows 2008 server has several enhancements to the Active Directory Server, which is now called Active Directory Domain Services.
 10. For **Admin Username** and **Admin Password**, enter an administrator username and password for the AD or NT server. Make sure the administrator you specify is a domain administrator in the same domain as the AD or NT server. Do not include a domain name with the server administrator username in the Admin Username field.
 11. Specify options under **Group Search with LDAP** if you want to retrieve group membership information from the LDAP server for users.



NOTE: When using LDAP group search the group lookup fails if the same user name is present in both the parent and child domain and if only the child domain user is part of a group. Native active directory group search works correctly.

Active directory group lookup using LDAP fails if a user from a different domain tree attempts to log in to Secure Access Service. Native Active Directory group lookup works correctly.

- Select **Enable Group Search With LDAP** to look up group information for a user.
- Select whether to use LDAP or LDAPS (LDAP communication using an SSL tunnel) protocol.

You enable LDAPS by installing a properly formatted certificate. If you select LDAPS, optionally select **Validate Server Certificate** to validate this certificate.

- For **Admin DN**, enter the administrator Distinguished Name.
 - Enter the **Base Search DN**. This is the point from where Secure Access Service starts searching for the user. Base DN will look something like `dc=juniper,dc=com`.
 - For **Nested Group Level**, enter how many levels within a group to search for the user. Note that higher numbers create longer queries or search time.
12. Under **Authentication Protocol**, specify which protocol Secure Access Service should use during authentication.
13. Under Kerberos Realm Name:
- Select **Use LDAP to get Kerberos realm name** if you want Secure Access Service to retrieve the Kerberos realm name from the Active Directory server using the specified administrator credentials.
 - Enter the Kerberos realm name in the Specify Kerberos realm name field if you know the realm name.
14. Expand the Advanced Options group and configure the following advanced options:
- **User may belong to Domain Local Groups across trust boundaries**—Specify if the trusted domains' Domain Local Groups must be searched to determine users' group memberships. This may impact performance.
 - **Container name**—Container path on the AD server where Secure Access Service joins. The default is **Computers**, which is a standard container created during installation of the AD server. The AD Computers container is the default location for new computer accounts created in the domain.

If desired, you may specify a different container or OU. Use the following format for nested OUs: **outer OU\inner OU**. Note the use of two backslash symbols (\): the first is the separator of the OUs, and the second is an escape sequence. For example, the following entry conforms with the required format: **CompObjects\SA**.
 - **Computer Name**—The name that Secure Access Service uses to join the specified Active Directory domain as a computer.

The computer name is pre-filled with an entry in the format of `vcNNNNHHHHHHHH`, where, in an IVS system, the `NNNN` is the IVS ID (assuming you have an IVS license) and the `HHHHHHHH` is a hex representation of the IP address of the Secure Access Service. You can change this to a unique name, either the one provided by default or one of your own choosing to more easily identify your systems in the Active Directory. In a non-IVS system, the first six characters of the name will be 'vc0000' because there is no IVS ID to display. For example, the name could be something like `vc0000a1018dF2` for a non-IVS system. The following entry conforms with the required format: **IVE_123**.

In a clustered environment with the same AD authentication server, this name is also unique among all cluster nodes, and Secure Access Service displays all of the identifiers for all attached cluster nodes.
15. Select the **Enable User Record Synchronization** checkbox to allow users to retain their bookmarks and individual preferences regardless of which Secure Access Service they log in to.

16. Click **Test Configuration** to verify the Active Directory server configuration settings, such as do the specified domain exist, are the specified controllers Active Directory domain controllers, does the selected authentication protocol work, and so forth. (optional)
17. Click **Save Changes**. If you are creating the server instance for the first time, the Settings and Users tabs appear. After you save changes, Secure Access Service masks the administrator password using five asterisk characters, regardless of the password length.
18. Click **Reset** to undo your edits and return all options on this page to their default value.

You can monitor and delete the sessions of users who are currently signed in through the server through the System > Status > Active Users page.

The admin console provides last access statistics for each user account on various Users tabs throughout the console, under a set of columns titled Last Sign-in Statistic. The statistics reported include the last successful sign-in date and time for each user, the user's IP address, and the agent or browser type and version.

**Related
Documentation**

- [About Basic, NTLM and Kerberos Resources on page 522](#)
- [Using Active Directory or NT Domains on page 163](#)

Configuring a Role-Mapping Rule Based on the Active Directory LDAP Primary Group

When the Secure Access Service queries the Active Directory LDAP server for a user's group membership details, the `memberOf` attribute is not populated with the user's Primary group. This is a known issue. See [Microsoft KB article 275523](#).

This topic describes how to work around this problem so that you can use the Active Directory LDAP primary group value as the basis for role mapping rules.

1. Use the [Active Directory® Service Interfaces Editor \(ADSI Edit\)](#) tool to find the RID (Relative Identifier) of the user's primary group.
 - a. Right-click the Domain Users group and select the properties of the Group.
 - b. Find the value assigned to the attribute `PrimaryGroupToken`. This value is the RID for that Group. In this example, let's say the assigned value is 513.
2. Update the Secure Access Service server catalog:
 - a. Go to Authentication > Auth. Servers > and click the link for your LDAP server configuration.
 - b. Under the "Determining group membership" group of settings, click the **Server Catalog** link.
 - c. Click the **Attribute** tab and use the controls to add a new attribute named **primaryGroupID**.
3. Create a new role mapping rule based on the RID user attribute:
 - a. Go to Users > User Realms and click the link of the realm you want to modify to display its configuration page.
 - b. Under Role Mapping, click **New Rule** to display the role mapping rule editor.
 - c. Select **User Attribute** from the "Rule based on" list and click **Update**.
 - d. Under Rule, select **primaryGroupID** from the list and set the rule matching to the RID value. In this example, you set the rule to match value 513. In your deployment, use the appropriate RID.
 - e. Complete the remaining role mapping rule configuration options according to your objectives and click **Save Changes**.

Related Documentation

- [Defining an LDAP Server Instance on page 176](#)
- [Specifying Role Mapping Rules for an Authentication Realm on page 309](#)

Multi-Domain User Authentication

Secure Access Service allows for multi-domain Active Directory and Windows NT authentication. Secure Access Service authenticates users in the domain you configure on the Authentication > Auth. Servers > New Active Directory / Windows NT page, users in child domains, and users in all domains trusted by the configured domain.

After you specify the address of a domain controller and a default domain in Secure Access Service Active Directory server configuration, users in the default domain authenticate to Secure Access Service using either just their username, or using the default domain plus username in the format defaultdomain\username.

When you enable trusted domain authentication, users in trusted or child domains authenticate to Secure Access Service using the name of the trusted or child domain plus the username in the format trusteddomain\username. Note that enabling trusted domain authentication adds to the server's response time.

Windows 2000 and Windows 2003 Multi-Domain Authentication

Secure Access Service supports Kerberos-based Active Directory authentication with Windows 2000 and Windows 2003 domain controllers. When a user logs in to Secure Access Service, it performs Kerberos authentication and attempts to fetch the Kerberos realm name for the domain controller, as well as all child and trusted realms, using LDAP calls.

You can alternately specify the Kerberos realm name when configuring an Active Directory authentication server, but we do not recommend this method for two reasons:

- You cannot specify more than one realm name. Secure Access Service cannot then authenticate against child or trusted realms of the realm you specify.
- If you misspell the realm name, Secure Access Service cannot authenticate users against the proper realm.

Windows NT4 Multi-Domain Authentication

Secure Access Service does not support Kerberos-based authentication in Windows NT4 domain controllers. Instead of Kerberos authentication, Secure Access Service uses NTLM authentication.



NOTE:

- For user authentication, Secure Access Service joins the default domain controller server using the machine name in the format *Secure Access-IPaddress*.
- If the DNS configuration on the Windows NT4 domain controller changes, make sure that Secure Access Service can still resolve names (child and trusted domains) using either WINS, DNS, or the Hosts file, that were able to resolve the names prior to the configuration change.

NT User Normalization

To support multi-domain authentication, Secure Access Service uses “normalized” NT credentials when contacting an Active Directory or NT4 domain controller for authentication. Normalized NT credentials include both the domain name and the username: domain\username. Regardless of how the user signs in to Secure Access Service, either using just a username or using the domain\username format, Secure Access Service always treats the username in the domain\username format.

When a user attempts to authenticate using only their username, Secure Access Service always normalizes their NT credentials as defaultdomain\username. Authentication succeeds only if the user is a member of the default domain.

For a user who signs to Secure Access Service using the domain\username format, Secure Access Service always attempts to authenticate the user as members of the domain the user specifies. Authentication succeeds only if the user-specified domain is a trusted or child domain of the default domain. If the user specifies an invalid or untrusted domain, authentication fails.

Two variables, <NTUser> and <NTDomain>, allow you to individually refer to domain and NT username values. Secure Access Service populates these two variables with the domain and NT username information.

When using pre-existing role mapping rules or writing a new role mapping rule for Active Directory authentication where USER = someusername, Secure Access Service treats this rule semantically as NTUser = someusername AND NTDomain = defaultdomain. This allows Secure Access Service to work seamlessly with preexisting role mapping rules.

Related Documentation

- [Using Active Directory or NT Domains on page 163](#)
- [Defining an Active Directory or Windows NT Domain Server Instance on page 164](#)

Join Domain for Active Directory-based Authentication Server Without Using a Domain Admin Account

With Active Directory on Windows Server 2000, Windows Server 2003 and Windows Server 2008, Secure Access Service can *join domain* (for an Active Directory based Authentication server) without using a domain administrator account.

1. Identify the user or group.
 - Identify the user or group to be granted permissions to perform AD operations on behalf of Secure Access Service. This can be any pre-existing user or group, or it can be a new one that you create.
 - If you use a group, be sure to add a user to the group with which you will configure the Secure Access Service Active Directory authentication server.
2. Open the Active Directory Users and Computers window.
 - a. Click **Start > Programs > Administrative Tools > Active Directory Users and Computers**.

- b. In the Active Directory Users and Computers interface, click **View**, and then select **Advanced Features**.
 3. Open the Access Control Settings for Computers dialog box.
 - a. In the Active Directory Users and Computers window, right-click **Computers** and then click **Properties**. The Computer Properties dialog appears.
 - b. Click the **Security** tab and then click **Advanced**. The Advanced Security Settings for Computers dialog box appears.
 4. Grant the user (or group) permission to Create Computer Objects and Delete Computer Objects in the Computers container.
 - a. In the Advanced Security Settings for Computers dialog box, click **Add**. The Select User, Computer, or Group dialog box appears.
 - b. Select or manually enter the name of the user or group you want to grant permissions to perform AD operations on behalf of Secure Access Service, and then click **OK**.
 - c. In the Permission Entry for Computers dialog box that appears, click **This object only** in the Apply onto list.
 - d. In the Permissions list, select the **Create Computer Objects** check box and the **Delete Computer Objects** check box, and then click **OK**.
 5. Grant the user (or group) permission to reset passwords and modify permissions on objects.
 - a. In the Active Directory Users and Computers window, right-click **Users** and then click **Properties**. The User Properties dialog box appears.
 - b. Click the **Security** tab and then click **Advanced**. The Advanced Security Settings for Users dialog box appears.
 - c. Click **Add**. The Select User, Computer, or Group dialog box appears.
 - d. Click or manually enter the name of the user (or group) you want to grant permissions to perform AD operations on behalf of Secure Access Service, and then click **OK**.
 - e. In the Permission Entry for Users dialog box, click **User objects** in the Apply onto list.
 - f. In the Permissions list, select the **Reset Password** checkbox, and then click **OK**.
 6. Verify there are no Deny entries that would affect the user (or group).
 7. Exit the Advanced Security Settings for Users dialog box.
 - a. In the Advanced Security Settings for Users dialog box, click **OK**.

- b. In the Users Properties dialog box, click **OK**.
8. Exit the Active Directory Users and Computers interface.
9. Configure the Secure Access Service Active Directory Authentication Server.
 - a. In the Administrator section of the Active Directory authentication server configuration, enter the user name you identified in Step 1 above and their password in the Admin Username and Admin Password fields respectively, and click **Save Changes**.
 - b. Restart the Secure Access Service services.

Using the Kerberos Debugging Tool

Use the Maintenance > Troubleshooting > Tools Kerberos window in the admin console to inspect the Kerberos ticket cache, probe the Kerberos infrastructure, and so forth. For example, Juniper Networks Technical Support may ask you to use this window to help debug Kerberos-related problems. You can also perform a quick check on Kerberos before setting up the Kerberos realms, credentials and policies.

The Kerberos window provides you with the following options:

- **Clear All Tickets**—Removes all tickets associated with the specified Secure Access Service username and realm. This action ensures that an active ticket does not remain on a computer when other users might have access to it. You must specify an account. You can not clear all tickets for all users.
- **Probe Kerberos DNS Setup**—Checks the DNS infrastructure for validity of the Kerberos realms and defined credentials. You must supply the Kerberos realm and site.
- **Verify Credential**—Verifies the Kerberos ticket is valid. For example, if you use Kerberos to verify the username and password provided by the user, this option verifies the credentials it obtains to make sure they belong to a trusted KDB site. The Server Realm and Server KDC fields are optional.
- **Verify Constrained Delegation Credential**—Verifies the Constrained Delegation ticket is valid. The Server Realm and Server KDC fields are reserved for future use. Any data entered in these fields are ignored.

Related Documentation

- [About Basic, NTLM and Kerberos Resources on page 522](#)

Active Directory and NT Group Lookup Support

Secure Access Service supports user group lookup in Domain Local, Domain Global, and Universal groups in the Active Directory forest, and Domain Local, and Domain Global groups for NT4 servers.

For the NT/AD group lookup to work, Secure Access Service first tries to join the domain using the default computer name. For this operation to succeed, you must specify valid

domain administrator credentials in the Active Directory server configuration on Secure Access Service.

Active Directory Lookup Requirements

Secure Access Service supports user group lookup in Domain Local, Domain Global, and Universal groups in the default domain, child domains, and all trusted domains. Secure Access Service obtains group membership using one of three methods that have different capabilities:

- **Group information in User's Security Context**—Returns information about a user's Domain Global groups.
- **Group information obtained using LDAP search calls**—Returns information about the user's Domain Global groups, and information about the user's Universal groups if Secure Access Service queries the Global Catalog Server.
- **Group information using native RPC calls**—Returns information about the user's Domain Local Group.

With respect to role mapping rules, Secure Access Service attempts group lookup in the following order:

- Secure Access Service checks for all Domain Global groups using the user's security context.
- If Secure Access Service has not found that the user is a member of some of the groups referenced in the role mapping rules, Secure Access Service performs an LDAP query to determine the user's group membership.
- If Secure Access Service has not found that the user is a member of some of the groups referenced in the role mapping rules, Secure Access Service performs an RPC lookup to determine the user's Domain Local group membership.

NT4 Group Lookup Requirements

Secure Access Service supports group lookup in the Domain Local and Domain Global groups created in the default domain, as well as all child, and other trusted domains. Secure Access Service obtains Domain Global group information from the user's security context, and Domain Local information using RPC calls. Secure Access Service uses no LDAP-based search calls in the NT4 environment.

Related Documentation

- [Using Active Directory or NT Domains on page 163](#)

Certificate Server

The certificate server feature allows users to authenticate based on attributes contained in client-side certificates. You may use certificate server by itself or in conjunction with another server to authenticate users and map them to roles.

For example, you may choose to authenticate users solely based on their certificate attributes. If Secure Access Service determines that the user's certificate is valid, it signs

the user in based on the certificate attributes you specify and does not prompt the user to enter a username or password.

Or, you may choose to authenticate users by passing their client-side certificate attributes to a second authentication server (such as LDAP). In this scenario, the certificate server first determines if the user's certificate is valid. Then, Secure Access Service can use realm-level role-mapping rules to compare the certificate attributes with the user's LDAP attributes. If it cannot find the proper match, Secure Access Service can deny or limit the user's access based on your specifications.



NOTE: When using client-side certificates, we strongly recommend that you train your end-users to close their Web browsers after signing out of Secure Access Service. If they do not, other users may be able to use their open browser sessions to access certificate-protected resources on the Secure Access Service without re-authenticating. (After loading a client-side certificate, both Internet Explorer and Netscape cache the certificate's credentials and private key. The browsers keep this information cached until the user closes the browser (or in some cases, until the user reboots the workstation). For details, see: <http://support.microsoft.com/?kbid=290345>.) To remind users to close their browsers, you may modify the sign out message in the Authentication > Authentication > Signing In Pages tab.

Related Documentation

- [Configuring User Sign In Policies on page 324](#)
- [Configuring a Certificate Server Instance on page 174](#)
- [Task Summary: Configuring Authentication Servers on page 155](#)

Configuring a Certificate Server Instance

When defining a certificate server on the Secure Access Service, you must perform the following steps:

1. Use settings in the System > Configuration > Certificates > CA Certificates tab to import the CA certificate used to sign the client-side certificates.
2. Create a certificate server instance:
 - a. Navigate to Authentication > Auth. Servers.
 - b. Select Certificate Server from the New list, and then click New Server.
 - c. Specify a name to identify the server instance.
 - d. In the User Name Template field, specify how the Secure Access Service should construct a username. You may use any combination of certificate variables contained in angle brackets and plain text.



NOTE: If you choose a certificate attribute with more than one value, the Secure Access Service uses the first matched value. For example, if you enter <certDN.OU> and the user has two values for the attribute (ou=management, ou=sales), the Secure Access Service uses the “management” value. To use all values, add the SEP attribute to the variable. For example, if you enter <certDN.OUT SEP=“:”> the Secure Access Service uses “management:sales”.

- e. Click Save Changes. If you are creating the server instance for the first time, the Settings and Users tabs appear.
3. If you want to verify certificate attributes against an LDAP server, use settings in the Authentication > Auth. Servers page to create an LDAP server instance. Note that you must use the Finding user entries section in the LDAP configuration page to retrieve the user-specific attributes that you want verify through the certificate.
4. Use settings in the Users > User Realms > RealmName > General tab or Administrators > Admin Realms > RealmName > General tab to specify which realms should use the certificate server to authenticate users. (You may also use settings in these tabs to specify realms that should use an LDAP server to verify certificate attributes.)
5. Use settings in the Authentication > Authentication > Signing In Policies page to associate the realms configured in the previous step with individual sign-in URLs.

Related Documentation

- [Specifying Client-side Certificate Restrictions on page 855](#)
- [Certificate Server on page 173](#)
- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)

Using an LDAP Server

The Secure Access Service supports two LDAP-specific authentication options:

- **Unencrypted**—in which the Secure Access Service sends the username and password to the LDAP Directory Service in clear, simple text.
- **LDAPS**—in which the Secure Access Service encrypts the data in the LDAP authentication session using Secure Socket Layer (SSL) protocol before sending it to the LDAP Directory Service.

The Secure Access Service performs substantial input validation for the following items:

- **LDAP Server**—The Secure Access Service provides a warning if the server is not reachable.
- **LDAP Port**—The Secure Access Service provides a warning if the LDAP server is not reachable.
- **Administrator credentials**—The Secure Access Service generates an error if the verification of admin credentials fails.

- **Base DN for users**—The Secure Access Service generates an error if the base-level search on the Base DN value fails.
- **Base DN for groups**—The Secure Access Service generates an error if the baselevel search on the Base DN value fails.

**Related
Documentation**

- [Task Summary: Configuring Authentication Servers on page 155](#)
- [Defining an LDAP Server Instance on page 176](#)
- [Enabling LDAP Password Management on page 179](#)

Defining an LDAP Server Instance

To define an LDAP server instance:

1. In the admin console, select **Authentication > Auth. Servers**.
2. Do one of the following:
 - To create a new server instance on Secure Access Service, select **LDAP Server** from the New list and then click **New Server**.
 - To update an existing server instance, click the appropriate link in the Authentication/Authorization Servers list.
3. Specify a name to identify the server instance.
4. Specify the name or IP address of the LDAP server that Secure Access Service uses to validate your users.
5. Specify the port on which the LDAP server listens. This port is typically 389 when using an unencrypted connection and 636 when using SSL.
6. Specify parameters for backup LDAP servers (optional). Secure Access Service uses the specified servers for failover processing; each authentication request is first routed to the primary LDAP server and then to the specified backup server(s) if the primary server is unreachable.



NOTE: Backup LDAP servers must be the same version as the primary LDAP server. Also, we recommend that you specify the IP address of a backup LDAP server instead of its host name, which may accelerate failover processing by eliminating the need to resolve the host name to an IP address.

7. Specify the type of LDAP server that you want to authenticate users against.
8. Specify whether or not the connection between Secure Access Service and LDAP Directory Service should be unencrypted, use SSL (LDAPS), or should use TLS.

If you select LDAPS, you have the option to require validation for the server certificate for the configured LDAP server(s) and its referral servers. If you enable validation for the referral servers, make sure your network DNS supports reverse lookup zone.

9. Specify how long you want Secure Access Service to wait for a connection to the primary LDAP server first, and then each backup LDAP server in turn.
10. Specify how long you want Secure Access Service to wait for search results from a connected LDAP server.
11. Click **Test Connection** to verify the connection between Secure Access Service and the specified LDAP server(s). (optional)
12. Select the **Authentication required?** check box if Secure Access Service needs to authenticate against the LDAP directory to perform a search or to change passwords using the password management feature. Then, enter an administrator DN and password.

For example: <CN=Administrator,CN=Users,DC=eng,DC=Juniper,DC=com>

13. Under **Finding user entries**, specify a:
 - **Base DN** at which to begin searching for user entries. For example:
<DC=eng,DC=Juniper,DC=com>
14. **Filter** if you want to fine-tune the search. For example:
<samAccountname=<username> or <cn=<username>>
 - Include <username> in the filter to use the username entered on the sign-in page for the search.
 - Specify a filter that returns 0 or 1 user DNs per user; Secure Access Service uses the first DN returned if more than 1 DN is returned.
15. Secure Access Service supports both static and dynamic groups. (Note that Secure Access Service only supports dynamic groups with LDAP servers.) To enable group lookup, you need to specify how Secure Access Service searches the LDAP server for a group. Under Determining group membership, specify a:
 - **Base DN** at which to begin searching for user groups.
 - **Filter** if you want to fine-tune the search for a user group.
 - **Member Attribute** to identify all the members of a static group. For example:
<member >
<uniquemember (iPlanet-specific)>
 - **Reverse group search** to start the search from the member instead of the group. This option is available only for Active Directory server types.
 - **Query Attribute** to specify an LDAP query that returns the members of a dynamic group. For example:
<memberURL>
 - **Nested Group Level** to specify how many levels within a group to search for the user. Note that the higher the number, the longer the query time, so we recommend that you specify to perform the search no more than 2 levels deep.
 - **Nested Group Search** to search by:

- **Nested groups in the LDAP Server Catalog.** This option is faster because it can search within the implicit boundaries of the nested group.
- **Search all nested groups.** With this option, Secure Access Service searches the Server Catalog first. If Secure Access Service finds no match in the catalog, then it queries LDAP to determine if a group member is a sub-group.



NOTE: Because Secure Access Service looks in the Server Catalog to determine if a member of a parent group is a user object or group object, you must add both the parent and all child (nested) groups to the Server Catalog.



NOTE: When the Secure Access Service queries the Active Directory LDAP server for a user's group membership details, the memberOf attribute is not populated with the user's Primary group. This is a known issue. See [Microsoft KB article 275523](#). To work around this issue, see “[Configuring a Role-Mapping Rule Based on the Active Directory LDAP Primary Group](#)” on page 168.

16. Under Bind Options, select:

- **Simple bind** to send a user's credentials in the clear (no encryption) to the LDAP Directory Service.
- **StartTLS bind** to encrypt a user's credentials using the Transport Layer Security (TLS) protocol before Secure Access Service sends the data to the LDAP Directory Service.

17. Click **Save Changes**. If you are creating the server instance for the first time, the Settings and Users tabs appear.

18. Specify which realms should use the server to authenticate and authorize administrators and users.



NOTE: Secure Access Service supports referral chasing if enabled on your LDAP server.

Related Documentation

- [Using the LDAP Server Catalog on page 314](#)
- [Using an LDAP Server on page 175](#)
- [Task Summary: Configuring Authentication Servers on page 155](#)

Configuring LDAP Search Attributes for Meeting Creators

Use options in the Meetings tab to specify individual LDAP attributes that a meeting creator may use to search for Secure Access Service users when scheduling a meeting.

To configure Junos Pulse Collaboration search attributes:

1. In the admin console, choose **Authentication > Auth. Servers**.
2. Click an LDAP server name (or create an LDAP server and then save it), and then choose the Meetings tab.
3. In the User Name field, enter the username attribute for this server. For example, enter SamAccountName for an Active Directory server or uid for an iPlanet server.
4. In the Email Address field, enter the email attribute for this server.
5. In the Display Name, Attributes field, enter any additional LDAP attributes whose contents you want to allow meeting creators to view (optional). (For example, to help the meeting creator easily distinguish between multiple invitees with the same name, you may want to expose an attribute that identifies the departments of individual users.) Enter the additional attributes one per line using the format: DisplayName,AttributeName. You may enter up to 10 attributes.
6. Click **Save Changes**.

**Related
Documentation**

- [Junos Pulse Collaboration Overview on page 691](#)

Enabling LDAP Password Management

The Secure Access Service password management feature enables users who authenticate through an LDAP server to manage their passwords through the Secure Access Service using the policies defined on the LDAP server. For example, if a user tries to sign in to the Secure Access Service with an LDAP password that is about to expire, the Secure Access Service catches the expired password notification, presents it to the user through the Secure Access Service interface, and then passes the user's response back to the LDAP server without requiring the user to sign in to the LDAP server separately.

Users, administrators, and help desk administrators who work in environments where passwords have set expiration times may find the password management feature very helpful. When users are not properly informed that their passwords are about to expire, they can change them themselves through the Secure Access Service rather than calling the Help Desk.

The password management feature enables users to change their passwords when prompted or at will. For example, during the sign-in process, the Secure Access Service may inform the user that his password is expired or about to expire. If expired, the Secure Access Service prompts the user to change his password. If the password has not expired, the Secure Access Service may allow the user to sign in to the Secure Access Service using his existing password. After he has signed in, he may change his password from the Preferences page.

Once enabled, the Secure Access Service performs a series of queries to determine user account information, such as when the user's password was last set, if his account is expired, and so forth. The Secure Access Service does this by using its internal LDAP or

Samba client. Many servers, such as Microsoft Active Directory or Sun iPlanet, offer an Administrative Console to configure account and password options.

The Secure Access Service enforces password policies by reading password attributes from the LDAP server. Therefore, for the Secure Access Service password management feature to work correctly, the password policy attributes on the back-end server need to be configured properly. The following configuration guidelines apply:

- For Active Directory in general, password policy attributes can be configured in the user entry container level or any organization level above the user container. If these attributes are configured at multiple levels, the level closest to the user node takes precedence.
- For Active Directory 2008, the Secure Access Service supports the Fine Grained Password Policy (FGP) configured in the AD user container.
- The Secure Access Service does not support customized password policies.
- The Secure Access Service does not support password management based on the Active Directory Global Catalog because password policy attributes are not fully populated on the Active Directory Global Catalog.

The Secure Access Service relies on the back-end server to pinpoint the cause of error when a password change operation fails. However, while LDAP servers may report errors accurately to human operators, they do not always do so when communicating programmatically to systems like the Secure Access Service. Therefore, reported errors may at times be generic or cryptic.

Enabling LDAP Password Management

To enable password management, you must first create an instance of the LDAP server. Next, you associate the LDAP server with the applicable realms. Finally, you select the enable password management feature at the realm level.

Supported LDAP Directories and Servers

The Secure Access Service supports password management with the following LDAP directories:

- Microsoft Active Directory/Windows NT
- Sun iPlanet
- Novell eDirectory

LDAP-based Password Management does not work on generic LDAP servers like OpenLDAP.

Additionally, the Secure Access Service supports password management with the following Windows servers:

- Microsoft Active Directory 2008
- Microsoft Active Directory 2003
- Windows NT 4.0

The following sections list specific issues related to individual server types.

- [Microsoft Active Directory on page 181](#)
- [Sun iPlanet on page 181](#)
- [General on page 181](#)
- [Supported LDAP Password Management Functions on page 181](#)
- [AD/NT Password Management Matrix on page 183](#)

Microsoft Active Directory

Changes on the Active Directory domain security policy may take 5 minutes or more to propagate among Active Directory domain controllers. Additionally, this information does not propagate to the domain controller on which it was originally configured for the same time period. This is a limitation of Active Directory.

When changing passwords in Active Directory using LDAP, the Secure Access Service automatically switches to LDAPS, even if LDAPS is not the configured LDAP method. To support LDAPS on the Active Directory server, you must install a valid SSL certificate into the server's personal certificate store. Note that the certificate must be signed by a trusted CA and the CN in the certificate's Subject field must contain the exact host name of the Active Directory server, for example: adsrv1.company.com. To install the certificate, select the Certificates Snap-In in the Microsoft Management Console (MMC).

The Account Expires option in the User Account Properties tab only changes when the account expires, not when the password expires. Microsoft Active Directory calculates the password expiration using the Maximum Password Age and Password Last Set values retrieved from the User object and Fine-Grained Password Policy objects or the Domain Security Policy LDAP objects.

Sun iPlanet

When you select the User must change password after reset option on the iPlanet server, you must also reset the user's password before this function takes effect. This is a limitation of iPlanet.

General

The Secure Access Service only displays a warning about password expiry if the password is scheduled to expire in 14 days or less. The Secure Access Service displays the message during each Secure Access Service sign in attempt. The warning message contains the remaining number of days, hours, and minutes that the user has to change his password before it expires on the server. The default value is 14 days; however, you may change it through the Administrators|Users > Admin Realms|User Realms> Authorization > Password configuration page of the admin console.

Supported LDAP Password Management Functions

The following matrix describes supported password management functions, their corresponding function names in the individual LDAP directories, and any additional relevant details. These functions must be set through the LDAP server itself before the Secure Access Service can pass the corresponding messages, functions, and restrictions

to end-users. The Active Directory attribute names shown are specific to the Domain Security Policy object. Similar attributes for the corresponding functions are used for the Active Directory 2008 Fine-Grained Password Policy. Refer to Microsoft documentation for details.

Table 11: Supported Password Management Functions

Function	Active Directory	iPlanet	Novell eDirectory
Authenticate user	unicodePwd	userPassword	userPassword
Allow user to change password if enabled	Server tells us in bind response (uses ntSecurityDescriptor)	If passwordChange == ON	If passwordAllowChange == TRUE
Log out user after password change	Yes	Yes	Yes
Force password change at next login	If pwdLastSet == 0	If passwordMustChange == ON	If pwdMustChange == TRUE
Password expired notification	userAccountControl == 0x80000	If Bind Response includes OID 2.16.840.1.113730.3.4.4 == 0	Check date/time value in
Password expiration notification (in X days/hours)	if pwdLastSet - now() < maxPwdAge - 14 days (is read from domain attributes) (the Secure Access Service displays warning if less than 14 days)	If Bind Response includes control OID 2.16.840.1.113730.3.4.5 (contains date/time) (the Secure Access Service displays warning if less than 14 days)	If now() - passwordExpirationTime < 14 days (the Secure Access Service displays warning if less than 14 days)
Disallow authentication if "account disabled/locked"	userAccountControl == 0x2 (Disabled) accountExpires userAccountControl == 0x10 (Locked) lockoutTime	Bind ErrorCode: 53 "Account Inactivated" Bind Error Code: 19 "Exceed Password Retry Limit"	Bind ErrorCode: 53 "Account Expired" Bind ErrorCode: 53 "Login Lockout"
Honor "password history"	Server tells us in bind response	Server tells us in bind response	Server tells us in bind response
Enforce "minimum password length"	If set, the Secure Access Service displays message telling user minPwdLength	If set, the Secure Access Service displays message telling user passwordMinLength	If set, the Secure Access Service displays message telling user passwordMinimumLength
Disallow user from changing password too soon	If pwdLastSet - now() < minPwdAge, then we disallow	If passwordMinAge > 0, then if now() is earlier than passwordAllowChangeTime, then we disallow	Server tells us in bind response

Table 11: Supported Password Management Functions (*continued*)

Function	Active Directory	iPlanet	Novell eDirectory
Honor "password complexity"	If pwdProperties == 0x1, then enabled. Complexity means the new password does not contain username, first or last name, and must contain characters from 3 of the following 4 categories: English uppercase, English lowercase, Digits, and Non-alphabetic characters (ex. !, \$, %)	Server tells us in bind response	Server tells us in bind response

AD/NT Password Management Matrix

The following matrix describes supported password management functions.

Table 12: AD/NT Password Management Matrix

Function	Active Directory	Active Directory 2003	Active Directory 2008 FGP	Windows NT
Authenticate user	Yes	Yes	Yes	Yes
Allow user to change password if enabled	Yes	Yes	Yes	Yes
Log out user after password change	Yes	Yes	Yes	Yes
Force password change at next login	Yes	Yes	Yes	Yes
Password expired notification	Yes	Yes	Yes	Yes
Account disabled	Yes	Yes	Yes	Yes
Account expired	Yes	Yes	Yes	Yes

Troubleshooting LDAP Password Management on the Secure Access Service

When troubleshooting, please provide any pertinent Secure Access Service logs, server logs, configuration information, and a TCP trace from the Secure Access Service. If you are using LDAPS, please switch to the "Unencrypted" LDAP option in the Secure Access Service LDAP server configuration while taking the LDAP TCP traces.

- Related Documentation**
- [Using an LDAP Server on page 175](#)
 - [Defining an LDAP Server Instance on page 176](#)

Using a Local Authentication Server

The Secure Access Service enables you to create one or more local databases of users who are authenticated by the Secure Access Service. You might want to create local user records for users who are normally verified by an external authentication server that you plan to disable or if you want to create a group of temporary users. Note that all administrator accounts are stored as local records, but you can choose to authenticate administrators using an external server.

When defining a new local authentication server instance, you need to give the server a unique name and configure password options and password management. These password options enable you to control the password length, character composition, and uniqueness. If desired, you can enable users to change their passwords and to force users to change passwords after a specified number of days. You can also prompt the user to change the password within a certain number of days of its expiration date.

Related Documentation

- [Task Summary: Configuring Authentication Servers on page 155](#)
- [Defining a Local Authentication Server Instance on page 184](#)

Defining a Local Authentication Server Instance

To define a local authentication server instance:

1. In the admin console, choose **Authentication > Auth. Servers**.
2. Do one of the following:
 - To create a new server instance on Secure Access Service, select **Local Authentication** from the New list and then click **New Server**.
 - To update an existing server instance, click the appropriate link in the Authentication/Authorization Servers list.
3. Specify a name to identify the new server instance or edit the current name for an existing server.
4. Specify password options:
 - a. Under **Password options**, set the minimum character length for passwords.
 - b. Set the maximum character length for passwords (optional). The maximum length cannot be less than the minimum length. There is no maximum limit to the length.

**NOTE:**

- If the maximum length set on the authentication server is shorter than the maximum length specified in the Secure Access Service, you may receive an error if you enter a password that is longer than that specified on the authentication server. The admin console allows you to enter passwords of any length, but your authentication server maximum determines the validity of the password length.
- If you want all passwords to be the same character length, set both the minimum and maximum lengths to the same value.

- Enable the **Password must have at least_digits** check box and specify the number of digits required in a password (optional). Do not require more digits than the value of the Maximum length option.
- Enable the **Password must have at least_letters** check box and specify the number of letters required in a password (optional). Do not require more letters than the value of the Maximum length option. If you enable the previous option, the combined total of the two options cannot exceed that of the value specified in the Maximum length option.
- Enable the **Password must have mix of UPPERCASE and lowercase letters** check box if you want all passwords to contain a mixture of upper- and lowercase letters (optional).



NOTE: Require passwords to contain at least two letters if you also require a mix of upper- and lowercase letters.

- Enable the **Password must be different from username** check box if the password cannot equal the username (optional).
- Enable the **New passwords must be different from previous password** check box if a new password cannot equal the previous password (optional).
- If you have configured open protocol sets for authentication, select the **Password stored as clear text** checkbox. IKEv2 EAP authentication works with local authentication servers only if this option is selected.



NOTE: Be aware of the security implications of storing passwords as clear text.

- Specify password management options:
 - Under Password management, enable the **Allow users to change their passwords** check box if you want users to be able to change their passwords (optional).

- b. Enable the **Force password change after _ days** check box and specify the number of days after which a password expires (optional).



NOTE: The default is 64 days, but you can set this value to any number you desire.

- c. Enable the **Prompt users to change their password _ days before current password expires** check box and provide the number of days before password expiration to prompt the user (optional).



NOTE: The default value is 14 days, but you can set the value to any number up to the number placed in the previous option.

6. If you are creating an account for a user administrator (user admin), refer to the section for configuring user admins.
7. Click **Save Changes**. If you are creating the server instance for the first time, the Users tab and Admin users tabs appear.

After you set password options and password management options, you also need to specify which realms should use the server to authenticate and authorize administrators and users. Use the Enable Password Management option on the Administrators|Users > Admin Realms|User Realms > Realm > Authentication Policy > Password page to specify whether or not the realm inherits password management settings from the local authentication server instance.

Related Documentation

- [Using a Local Authentication Server on page 184](#)
- [Specifying Password Access Restrictions on page 85](#)

Creating User Accounts on a Local Authentication Server

When you create a local authentication server instance, you need to define local user records for that database. A local user record consists of a username, the user's full name, and the user's password. You may want to create local user records for users who are normally verified by an external authentication server that you plan to disable or if you want to quickly create a group of temporary users.

To create local user records for a local authentication server:

1. In the admin console, choose **Authentication > Auth. Servers**.
2. Click the Secure Access Service local authentication server to which you want to add a user account.
3. Select the **Users** tab and click **New**.
4. Enter a **Username** and the user's **Full Name**.

- Do not include “~” in a username.
 - If you want to change a username after creating the account, you must create an entirely new account.
5. Enter the **Password** and **Confirm Password**. Make sure that the password you enter conforms to the password options specified for the associated local authentication server instance.
 6. Optionally, specify **Expiration Days** or **Expiration Hours** if this is a temporary account. You can later add additional time to extend the expiration date.
 7. **Select One-time use (disable account after the next successful sign-in)** if you want to limit the user to one login. After one successful login, the user’s login state is set to Disabled and the user receives an error message when attempting subsequent sign ins. However, you can manually reset this option in the admin console to allow the same user to login again. If you leave this option unchecked, it means that you are creating a permanent user.
 8. Select **Enabled** if not already selected. This option is used by the administrator to selectively enable or disable any user (one time or permanent). Selected by default. If the One-time use option is checked, this option changes to Disabled after the user logs in successfully. If a permanent or one-time user is logged in and you disable this option, the user is immediately logged out of the system and receives an error message.
 9. Select **Require user to change password at next sign in** if you want to force the user to change their password at the next login.



NOTE: If you force the user to change passwords, you must also enable the **Allow users to change their passwords** option. Use options on the **Administrators|Users > Admin Realms|User Realms > [Realm] > Authentication Policy > Password** page to specify which realms should inherit the server's password management capabilities.

10. Click **Save Changes**. The user record is added to the Secure Access Service database.



NOTE: The admin console provides last access statistics for each user account on various **Users** tabs throughout the console, under a set of columns titled **Last Signin Statistic**. The statistics reported include the last successful sign-in date and time for each user, the user’s IP address, and the agent or browser type and version.

Managing User Accounts

To manage a local user account:

1. In the admin console, choose **Authentication > Auth. Servers**.
2. Click the appropriate server link in the **Authentication/Authorization Servers** list.

3. Select the **Users** tab.
4. Perform any of the following tasks:
 - Enter a username in the **Show users named** field and click **Update** to search for a specific user.

Alternatively, you can use an asterisk (*) as a wildcard, where * represents any number of zero or more characters. For example, if you want to search for all usernames that contain the letters jo, enter *jo* in the Show users named field. The search is case-sensitive. To display the entire list of accounts again, either enter * or delete the field's contents and click **Update**.
 - Enter a number in the **Show N users field** and click **Update** to control the number of users displayed on the page.
 - Click the check box next to individual users and click **Delete** to terminate their Secure Access Service sessions.

Related Documentation

- [Using a Local Authentication Server on page 184](#)
- [Defining a Local Authentication Server Instance on page 184](#)
- [Creating User Accounts From the Secure Gateway Home Page on page 188](#)

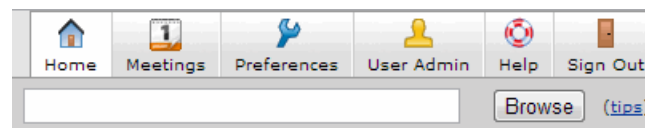
Creating User Accounts From the Secure Gateway Home Page

An end-user can be given rights for user administration for a local authentication server. When an admin user logs into an admin realm they can add a user on the local authentication server.

To create a user account:

1. Log in to the Secure Gateway home page as an admin user.
2. Click **User Admin** located in the upper right corner of the home page.

Figure 9: User Admin Icon



3. Click **New User**.

Figure 10: Creating a New Local User

The screenshot shows the Juniper Networks User Admin interface. The top navigation bar includes Home, Meetings, Preferences, User Admin, Help, and Sign Out. The main content area is titled 'New Local User' and shows the following form fields and options:

- Authentication Server: System Local
- Username:
- Full Name:
- Password:
- Confirm Password:
- One-time use (disable account after the next successful sign-in)
- Enabled
- Require user to change password at next sign in
- Buttons: Save Changes, Cancel

4. Enter a **Username** and the user's **Full Name**.
 - Do not include “~~” in a username.
 - If you want to change a username after creating the account, you must create an entirely new account.
5. Enter the **Password** and **Confirm Password**. Make sure that the password you enter conforms to the password options specified for the associated local authentication server instance.
6. **Select One-time use (disable account after the next successful sign-in)** if you want to limit the user to one login. After one successful login, the user's login state is set to Disabled and the user receives an error message when attempting subsequent sign ins. However, you can manually reset this option in the admin console to allow the same user to login again. If you leave this option unchecked, it means that you are creating a permanent user.
7. Select **Enabled** if not already selected. This option is used by the administrator to selectively enable or disable any user (one time or permanent). Selected by default. If the One-time use option is checked, this option changes to Disabled after the user logs in successfully. If a permanent or one-time user is logged in and you disable this option, the user is immediately logged out of the system and receives an error message.
8. Select **Require user to change password at next sign in** if you want to force the user to change their password at the next login.



NOTE: If you force the user to change passwords, you must also enable the Allow users to change their passwords option. Use options on the Administrators|Users > Admin Realms|User Realms > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities.

9. Click **Save Changes**. The user record is added to the Secure Access Service database.

Related Documentation

Configuring an NIS Server Instance

When authenticating users with a UNIX/NIS server, the Secure Access Service verifies that the username and password entered through the sign-in page correspond to a valid user ID and password pair in the NIS server. Note that the username submitted to the Secure Access Service cannot contain two consecutive tilde symbols (~~).



NOTE: You can only use NIS authentication with the Secure Access Service if your passwords are stored on the NIS server using Crypt or MD5 formats. Also note that you can only add one NIS server configuration to the Secure Access Service, but you can use that configuration to authenticate any number of realms.

To define an NIS server instance:

1. In the admin console, choose **Authentication > Auth. Servers**.
2. Do one of the following:
 - To create a new server instance on the Secure Access Service, select **NIS Server** from the New list, and then click **New Server**.
 - To update an existing server instance, click the appropriate link in the Authentication/Authorization Servers list.
3. Specify a name to identify the server instance.
4. Specify the name or IP address of the NIS server.
5. Specify the domain name for the NIS server.
6. Click **Save Changes**. If you are creating the server instance for the first time, the Settings and Users tabs appear.
7. Specify which realms should use the server to authenticate and authorize administrators and users.

Related Documentation

- [Task Summary: Configuring Authentication Servers on page 155](#)

- [Defining Authentication Access Policies on page 307](#)

Configuring a RADIUS Server Instance

A Remote Authentication Dial-In User Service (RADIUS) server is a type of server that allows you to centralize authentication and accounting for users. When using an external RADIUS server to authenticate Secure Access Service users, you need to configure it to recognize the Secure Access Service as a client and specify a shared secret for the RADIUS server to use to authenticate the client request.

The Secure Access Service also supports RADIUS proxy. You can configure your external RADIUS server as an inner or outer proxy target. When you specify RADIUS proxy, some fields in the RADIUS server configuration page are not applicable.

The Secure Access Service supports the standard RADIUS authentication schemes, including:

- Access-Request
- Access-Accept
- Access-Reject
- Access-Challenge

The Secure Access Service also supports the RSA ACE/Server using the RADIUS protocol and a SecurID token (available from Security Dynamics). If you use SecurID to authenticate users, users must supply their user ID and the concatenation of a PIN and the token value.

When defining a RADIUS server, the Secure Access Service gives administrators the ability to use either hard-coded (default) challenge expressions that support Defender 4.0 and some RADIUS server implementations (such as Steel-Belted RADIUS and RSA RADIUS) or to enter custom challenge expressions that allow the Secure Access Service to work with many different RADIUS implementations and new versions of the RADIUS server, such as Defender 5.0. The Secure Access Service looks for the response in the Access-Challenge packet from the server and issues an appropriate Next Token, New Pin, or Generic Passcode challenge to the user.

User Experience for RADIUS Users

The user experience varies depending on whether you are using a RADIUS server like Steel-Belted RADIUS, PassGo Defender RADIUS server or CASQUE authentication.

If you are using a PassGo Defender RADIUS Server, the user sign-in process is:

- The user signs in to the Secure Access Service with a username and password. The Secure Access Service forwards these credentials to Defender.
- Defender sends a unique challenge string to the Secure Access Service and the Secure Access Service displays this challenge string to the user.

- The user enters the challenge string in a Defender token and the token generates a response string.
- The user enters the response string on the Secure Access Service and clicks Sign In.

Using CASQUE Authentication

CASQUE authentication uses a token-based challenge/response authentication mechanism employing a CASQUE player installed on the client system. Once configured with CASQUE authentication, the RADIUS server issues a challenge with a response matching the custom challenge expression (:([0-9a-zA-Z/+]=]+):). The Secure Access Service then generates an intermediate page that automatically launches the CASQUE player installed on the user's system.



NOTE: If the CASQUE player does not launch automatically, click the Launch CASQUE Player link.

Users must then use their CASQUE Optical Responder tokens to generate the corresponding passcode, enter the passcode in the Response field, and click Sign In.

Related Documentation

- [Task Summary: Configuring Authentication Servers on page 155](#)
- [Enabling RADIUS Accounting on page 195](#)

Defining a Secure Access Service RADIUS Server Instance

To configure a connection to the RADIUS server on Secure Access Service:

1. In the admin console, choose **Authentication > Auth. Servers**.
2. Do one of the following:
 - To create a new server instance on Secure Access Service, select **RADIUS Server** from the New list, and then click **New Server**.
 - To update an existing server instance, click the appropriate link in the Authentication/Authorization Servers list.
3. At the top of the Radius Server page, specify a name to identify the server instance.
4. In the NAS-Identifier field, enter the name that identifies the Secure Access Service Network Access Server (NAS) client that communicates with the RADIUS server. If you leave this field empty, the Secure Access Service uses the value specified in the Hostname field of the System > Network > Overview page of the admin console. If no value is specified in Hostname field, the Secure Access Service uses the value "Juniper Secure Access."
5. Specify the name or IP address in the RADIUS server text box.
6. Enter the authentication port value for the RADIUS server. Typically this port is 1812, but some legacy servers might use 1645.

7. Enter a string for the shared secret. You also need to enter this string when configuring the RADIUS server to recognize the Secure Access Service as a client.
8. Enter the accounting port value for the RADIUS server. Typically this port is 1813, but some legacy servers might use 1646.
9. Enter the NAS IP Address. This allows you to control the NAS IP address value passed to RADIUS requests. If you leave this field empty, then the Secure Access Service's internal IP address will be passed to RADIUS requests. If you configure the NAS IP address, then the value will be passed, regardless of which cluster node sends the requests.
10. Enter the interval of time for the Secure Access Service to wait for a response from the RADIUS server before timing out the connection.
11. Enter the number of times for the Secure Access Service to try to make a connection after the first attempt fails.
12. Select the **Users authenticate using tokens or one-time passwords** option if you do not want to submit the password entered by the user to other SSO-enabled applications. You should generally select this option if the users submit one-time use passwords to the Secure Access Service.
13. In the Backup Server section, enter a secondary RADIUS server for the Secure Access Service to use if the primary server—the one defined in this instance—is unreachable. For the secondary server, enter the server:
 - a. Name or IP address
 - b. Authentication port
 - c. Shared secret
 - d. Accounting port
14. If you want to track Secure Access Service user activity using this instance of the RADIUS server, enter the following information in the Radius Accounting section:
 - a. In the **User-Name** field, specify the user information that the Secure Access Service should send to the RADIUS accounting server. Applicable variables include those that are set at the time after the user signs in and maps to a role. The default variables for this field are:
 - <username> logs the user's Secure Access Service username to the accounting server.
 - <REALM> logs the user's Secure Access Service realm to the accounting server.
 - <ROLE> logs the user's Secure Access Service role to the accounting server. If the user is assigned to more than one role, the Secure Access Service comma-separates them.

- b. Add an **Interim Update Level** (in minutes). The interim update level enables you to accomplish more precise billing for long-lived session clients and in case of a network failure.
15. Select the **Use NC assigned IP Address for FRAMED-IP-ADDRESS attribute value in Radius Accounting** checkbox to use the IP address returned from the Secure Access Service for the Framed-IP-Address attribute.

Two IP addresses are recorded: one prior to authenticating with the Secure Access Service, and one returned by VPN Tunneling after authentication. Select this option to use the VPN Tunneling IP address for the Framed-IP-Address attribute instead of the pre-authenticated (original) IP address.
16. (optional) Click **New Radius Rule** to add a custom challenge rule that determines the action to take for an incoming packet.

When a user enters his or her username and password, the initial authorization request is sent to the server. The server may respond with a Challenge or Reject packet. In the **Add Custom Radius Challenge Rule** window, you select the packet type (Challenge or Reject) and then specify what action to take. For example, you can show a login page with a specific error message to the user, or automatically send an ACCESS-REQUEST packet back to the server.

To create a custom challenge rule:

- a. Select the incoming packet type:
 - Access Challenge—sent by the RADIUS server requesting more information in order to allow access
 - Access Reject—sent by the RADIUS server rejecting access
- b. Specify an expression to evaluate, based on the Radius attribute, and click **Add**. If you specify more than one expression, the expressions are “ANDed” together. To remove an expression, click the delete icon next to the expression.
- c. Choose the action to take by selecting one of the following radio buttons:
 - show **NEW PIN** page—user must enter a new PIN for his/her token
 - show **NEXT TOKEN** page—user must enter the next tokencode
 - show **GENERIC LOGIN** page—display an additional page to the user in response to an Access Challenge sent by the server. Sometimes a Radius server returns a Challenge packet and requires the user to enter additional information to continue the login process. For example, a server receives the initial username and password and sends an SMS message to the user’s mobile phone with a one-time password (OTP). The user enters the OTP in the generic login page.
 - show **user login page with error**—display the standard login page with an embedded error message. This option lets you bypass the standard message string sent by the Secure Access Service and display a custom error message to

the user. Enter your custom message in the Error Message text box. There is no maximum character limit for this message.

- send ACCESS REQUEST with additional attributes—send an ACCESS-REQUEST packet with the specified attribute/value pair(s). Select an attribute, enter its value and click Add. To delete an attribute, click the delete icon next to the attribute/value pair.

You must set User-Password to <PASSWORD> otherwise an “Invalid username or password” message appears.

- d. Click Save Changes to save your edits, then click Close to close this window.

Your custom rules appear in the table under the Custom Radius Authentication Rule section. To delete a rule, select the checkbox next to the rule and click Delete.

17. Click **Save Changes**. If you are creating the server instance for the first time, the Settings and Users tabs appear.
18. Specify which realms should use the server to authenticate, authorize, or account for administrators and users.

Configuring the RADIUS Server to Recognize the Secure Access Service

You need to configure the RADIUS server to recognize the Secure Access Service by specifying:

- The host name given to the Secure Access Service.
- The network IP address of the Secure Access Service.
- The Secure Access Service client type—if applicable. If this option is available, select Single Transaction Server or its equivalent.
- The type of encryption to use for authenticating client communication. This choice should correspond to the client type.
- The shared secret you entered in the admin console for the RADIUS server on the Authentication > Auth. Servers > Radius Server page.

Related Documentation

- [Configuring a RADIUS Server Instance on page 191](#)
- [Enabling RADIUS Accounting on page 195](#)
- [System Variables and Examples on page 1186](#)

Enabling RADIUS Accounting

You can configure the Secure Access Service to send session start and stop messages to a RADIUS accounting server. The Secure Access Service recognizes two categories of sessions—user-sessions and sub-sessions. A user session may contain multiple sub-sessions. The Secure Access Service recognizes the following types of sub-sessions:

- JSAM

- WSAM
- VPN Tunneling (formerly called Network Connect)

The Secure Access Service sends a user-session start message after the user successfully signs in and the Secure Access Service maps him to a role. The Secure Access Service sends a sub-session start message when the sub-session becomes active; for example, after launching JSAM. The Secure Access Service sends a sub-session stop message when there is an explicit request from the user to terminate a sub-session, or if the user-session terminates.

Whenever a user session terminates, the Secure Access Service sends a user-session stop message to the accounting server. A user session terminates whenever the user:

- Manually signs out of the Secure Access Service
- Times out of the Secure Access Service either due to inactivity or because of exceeding the maximum session length
- Is denied access due to Host Checker or Cache Cleaner role-level restrictions
- Is manually forced out of the Secure Access Service by an administrator or due to dynamic policy evaluation.

The Secure Access Service also sends stop messages for all active sub-sessions. The stop-messages for the sub-sessions precede the stop-messages for the user-session.



NOTE: If users are signed into a Secure Access Service cluster, the RADIUS accounting messages may show the users signing in to one node and signing out of another.

The following three tables describe the attributes that are common to start and stop messages, attributes that are unique to start messages, and attributes that are unique to stop messages.

Table 13: Attributes Common to both Start and Stop Messages

Attribute	Description
User-Name (1)	String that the Secure Access Service administrator specifies during RADIUS server configuration
NAS-IP-Address (4)	Secure Access Service's IP address
NAS-Port (5)	The Secure Access Service sets this attribute to 0 if the user signed in using an internal port, or 1 if an external port.
Framed-IP-Address (8)	User's source IP address
NAS-Identifier (32)	Configured name for the Secure Access Service client under the RADIUS server configuration

Table 13: Attributes Common to both Start and Stop Messages
(continued)

Attribute	Description
Acct-Status-Type (40)	The Secure Access Service sets this attribute to 1 for a start message, or 2 for a stop message in a user-session or a sub-session
Acct-Session-Id (44)	Unique accounting ID that matches start and stop messages corresponding to a user-session or to a sub-session.
Acct-Multi-Session-Id (50)	Unique accounting ID that you can use to link together multiple related sessions. Each linked session must have a unique Acct-Session-Id and the same Acct-Multi-Session-Id.
Acct-Link-Count (51)	The count of links in a multi-link session at the time the Secure Access Service generates the accounting record

Table 14: Start Attributes

Attribute	Description
Acct-Authentic (45)	The Secure Access Service sets this attribute to: <ul style="list-style-type: none"> • RADIUS—if the user authenticated to a RADIUS server • Local—if the user authenticated to an Local Authentication Server • Remote—for anything else

Table 15: Stop Attributes

Attribute	Description
Acct-Session-Time (46)	Duration of the user-session or the sub-session
Acct-Terminate-Cause (49)	The Secure Access Service uses one of the following values to specify the event that caused the termination of a user session or a sub-session: <ul style="list-style-type: none"> • User Request (1) – User manually signs out • Idle Timeout (4) – User Idle time out • Session Timeout (5) – User Max Session Timeout • Admin Reset (6) – User Forced Out from Active Users page
Acct-Terminate-Cause (49)	The Secure Access Service uses one of the following values to specify the event that caused the termination of a user session or a sub-session: <ul style="list-style-type: none"> • User Request (1) – User manually signs out • Idle Timeout (4) – User Idle time out • Session Timeout (5) – User Max Session Timeout • Admin Reset (6) – User Forced Out from Active Users page

Table 15: Stop Attributes (*continued*)

Attribute	Description
Acct-Terminate-Cause (49)	The Secure Access Service uses one of the following values to specify the event that caused the termination of a user session or a sub-session: <ul style="list-style-type: none"> • User Request (1) – User manually signs out • Idle Timeout (4) – User Idle time out • Session Timeout (5) – User Max Session Timeout • Admin Reset (6) – User Forced Out from Active Users page
Acct-Input-Octets	Octet-based count of JSAM/WSAM/NC session level when session was terminated and of user session level when the session was terminated and the interim update time arrived. From the Secure Access Service to the client.
Acct-Output-Octets	Octet-based count of JSAM/WSAM/NC session level when session was terminated and of user session level when the session was terminated and the interim update time arrived. From client to the Secure Access Service.

To distinguish between a user-session and the sub-sessions it contains, examine the Acct-Session-Id and the Acct-Multi-Session-Id. In a user-session, both of these attributes are the same. In a sub-session, the Acct-Multi-Session-Id is the same as the one for the parent user-session, and the Secure Access Service indicates the sub-session by using one of the following suffixes in the Acct-Session-Id:

- “JSAM” for JSAM sessions
- “WSAM” for WSAM sessions
- “NC” for Network Connect or VPN Tunneling sessions

Supported RADIUS Attributes

The following RADIUS attributes are supported in RADIUS role mapping. For more information, see the full descriptions (from which these descriptions were derived) at the FreeRADIUS website located at <http://www.freeradius.org/rfc/attributes.html>.

Table 16: RADIUS Role Mapping Attributes

Attribute	Description
ARAP-Challenge-Response	Sent in an Access-Accept packet with Framed-Protocol of ARAP, and contains the response to the dial-in client's challenge.
ARAP-Features	Sent in an Access-Accept packet with Framed-Protocol of ARAP. Includes password information that the NAS must send to the user in an ARAP feature flags packet.

Table 16: RADIUS Role Mapping Attributes (*continued*)

Attribute	Description
ARAP-Password	Present in an Access-Request packet containing a Framed-Protocol of ARAP. Only one of User-Password, CHAP-Password, or ARAP-Password must be included in an Access-Request, or one or more EAP-Messages.
ARAP-Security	Identifies the ARAP Security Module to be used in an Access-Challenge packet.
ARAP-Security-Data	Contains a security module challenge or response, and is in Access-Challenge and Access-Request packets.
ARAP-Zone-Access	Indicates how to use the ARAP zone list for the user.
Access-Accept	Provides specific configuration information necessary to begin delivery of service to the user.
Access-Challenge	To send the user a challenge requiring a response, the RADIUS server must respond to the Access-Request by transmitting a packet with the Code field set to 11 (Access-Challenge).
Access-Reject	If any value of the received Attributes is not acceptable, then the RADIUS server must transmit a packet with the Code field set to 3 (Access-Reject).
Access-Request	Conveys information specifying user access to a specific NAS, and any special services requested for that user.
Accounting-Request	Conveys information used to provide accounting for a service provided to a user.
Accounting-Response	Acknowledges that the Accounting-Request has been received and recorded successfully.
Acct-Authentic	Indicates how the user was authenticated, whether by RADIUS, the NAS itself, or another remote authentication protocol.
Acct-Delay-Time	Indicates how many seconds the client has been trying to send this record.
Acct-Input-Gigawords	Indicates how many times the Acct-Input-Octets counter has wrapped around 2^{32} over the course of this service being provided.
Acct-Input-Octets	Indicates how many octets have been received from the port during the current session.
Acct-Input-Packets	Indicates how many packets have been received from the port during the session provided to a Framed User

Table 16: RADIUS Role Mapping Attributes (*continued*)

Attribute	Description
Acct-Interim-Interval	Indicates the number of seconds between each interim update in seconds for this specific session.
Acct-Link-Count	The count of links known to have been in a given multilink session at the time the accounting record is generated.
Acct-Multi-Session-Id	A unique Accounting ID to make it easy to link together multiple related sessions in a log file.
Acct-Output-Gigawords	Indicates how many times the Acct-Output-Octets counter has wrapped around 2^{32} during the current session.
Acct-Output-Octets	Indicates how many octets have been sent to the port during this session.
Acct-Output-Packets	Indicates how many packets have been sent to the port during this session to a Framed User.
Acct-Session-Id	A unique Accounting ID to make it easy to match start and stop records in a log file.
Acct-Session-Time	Indicates how many seconds the user has received service.
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop).
Acct-Terminate-Cause	Indicates how the session was terminated.
Acct-Tunnel-Connection	Indicates the identifier assigned to the tunnel session.
Acct-Tunnel-Packets-Lost	Indicates the number of packets lost on a given link.
CHAP-Challenge	Contains the CHAP Challenge sent by the NAS to a PPP Challenge-Handshake Authentication Protocol (CHAP) user.
CHAP-Password	The response value provided by a PPP Challenge-Handshake Authentication Protocol (CHAP) user in response to the challenge.
Callback-Id	The name of a location to be called, to be interpreted by the NAS.
Callback-Number	The dialing string to be used for callback.

Table 16: RADIUS Role Mapping Attributes (*continued*)

Attribute	Description
Called-Station-Id	Allows the NAS to send the phone number that the user called, using Dialed Number Identification (DNIS) or similar technology.
Calling-Station-Id	Allows the NAS to send the phone number that the call came from, using Automatic Number Identification (ANI) or similar technology.
Class	Sent by the server to the client in an Access-Accept and then sent unmodified by the client to the accounting server as part of the Accounting-Request packet, if accounting is supported.
Configuration-Token	For use in large distributed authentication networks based on proxy.
Connect-Info	Sent from the NAS to indicate the nature of the user's connection.
EAP-Message	Encapsulates Extended Access Protocol [3] packets to allow the NAS to authenticate dial-in users by means of EAP without having to understand the EAP protocol.
Filter-Id	The name of the filter list for this user.
Framed-AppleTalk-Link	The AppleTalk network number used for the serial link to the user, which is another AppleTalk router.
Framed-AppleTalk-Network	The AppleTalk Network number which the NAS can probe to allocate an AppleTalk node for the user.
Framed-AppleTalk-Zone	The AppleTalk Default Zone to be used for this user.
Framed-Compression	A compression protocol to be used for the link.
Framed-IP-Address	The address to be configured for the user.
Framed-IP-Netmask	The IP netmask to be configured for the user when the user is a router to a network.
Framed-IPX-Network	The IPX Network number to be configured for the user.
Framed-MTU	The Maximum Transmission Unit to be configured for the user, when it is not negotiated by some other means (such as PPP).
Framed-Pool	The name of an assigned address pool used to assign an address for the user.
Framed-Protocol	The framing to be used for framed access.

Table 16: RADIUS Role Mapping Attributes (*continued*)

Attribute	Description
Framed-Route	Routing information to be configured for the user on the NAS.
Framed-Routing	The routing method for the user, when the user is a router to a network.
Idle-Timeout	Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt.
Keep-Alives	Use SNMP instead of keep-alives.
Login-IP-Host	Indicates the system with which to connect the user, when the Login-Service Attribute is included.
Login-LAT-Group	Contains a string identifying the LAT group codes that this user is authorized to use.
Login-LAT-Node	Indicates the Node with which the user is to be automatically connected by LAT.
Login-LAT-Port	Indicates the Port with which the user is to be connected by LAT.
Login-LAT-Service	Indicates the system with which the user is to be connected by LAT.
Login-Service	Indicates the service to use to connect the user to the login host.
Login-TCP-Port	Indicates the TCP port with which the user is to be connected, when the Login-Service Attribute is also present.
MS-ARAP-Challenge	Only present in an Access-Request packet containing a Framed-Protocol Attribute with the value 3 (ARAP).
MS-ARAP-Password-Change-Reason	Indicates the reason for a server-initiated password change.
MS-Acct-Auth-Type	Represents the method used to authenticate the dial-up user.
MS-Acct-EAP-Type	Represents the Extensible Authentication Protocol (EAP) [15] type used to authenticate the dial-up user.
MS-BAP-Usage	Describes whether the use of BAP is allowed, disallowed or required on new multilink calls.
MS-CHAP-CPW-1	Allows the user to change password if it has expired.

Table 16: RADIUS Role Mapping Attributes (*continued*)

Attribute	Description
MS-CHAP-CPW-2	Allows the user to change password if it has expired.
MS-CHAP-Challenge	Contains the challenge sent by a NAS to a Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) user.
MS-CHAP-Domain	Indicates the Windows NT domain in which the user was authenticated.
MS-CHAP-Error	Contains error data related to the preceding MS-CHAP exchange.
MS-CHAP-LM-Enc-PW	Contains the new Windows NT password encrypted with the old LAN Manager password hash.
MS-CHAP-MPPE-Keys	Contains two session keys for use by the Microsoft Point-to-Point Encryption Protocol (MPPE).
MS-CHAP-NT-Enc-PW	Contains the new Windows NT password encrypted with the old Windows NT password hash.
MS-CHAP-Response	Contains the response value provided by a PPP Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) user in response to the challenge.
MS-CHAP2-CPW	Allows the user to change password if it has expired.
MS-CHAP2-Response	Contains the response value provided by an MS-CHAP-V2 peer in response to the challenge.
MS-CHAP2-Success	Contains a 42-octet authenticator response string.
MS-Filter	Used to transmit traffic filters.
MS-Link-Drop-Time-Limit	Indicates the length of time (in seconds) that a link must be underutilized before it is dropped.
MS-Link-Utilization-Threshold	Represents the percentage of available bandwidth utilization below which the link must fall before the link is eligible for termination.
MS-MPPE-Encryption-Policy	Signifies whether the use of encryption is allowed or required.
MS-MPPE-Encryption-Types	Signifies the types of encryption available for use with MPPE.
MS-MPPE-Recv-Key	Contains a session key for use by the Microsoft Point-to-Point Encryption Protocol (MPPE).

Table 16: RADIUS Role Mapping Attributes (*continued*)

Attribute	Description
MS-MPPE-Send-Key	Contains a session key for use by the Microsoft Point-to-Point Encryption Protocol (MPPE).
MS-New-ARAP-Password	Transmits the new ARAP password during an ARAP password change operation.
MS-Old-ARAP-Password	Transmits the old ARAP password during an ARAP password change operation.
MS-Primary-DNS-Server	Indicates the address of the primary Domain Name Server (DNS) [16, 17] server to be used by the PPP peer.
MS-Primary-NBNS-Server	Indicates the address of the primary NetBIOS Name Server (NBNS) [18] server to be used by the PPP peer.
MS-RAS-Vendor	Indicates the manufacturer of the RADIUS client machine.
MS-RAS-Version	Indicates the version of the RADIUS client software.
MS-Secondary-DNS-Server	Indicates the address of the secondary DNS server to be used by the PPP peer.
MS-Secondary-NBNS-Server	Indicates the address of the secondary DNS server to be used by the PPP peer.
NAS-IP-Address	Indicates the identifying IP Address of the NAS that is requesting authentication of the user, and must be unique to the NAS within the scope of the RADIUS server.
NAS-Identifier	Contains a string identifying the NAS originating the Access-Request.
NAS-Port	Indicates the physical port number of the NAS that is authenticating the user.
NAS-Port-Id	Contains a text string that identifies the port of the NAS that is authenticating the user.
NAS-Port-Type	Indicates the type of the physical port of the NAS that is authenticating the user.
Password-Retry	Indicates how many authentication attempts a user is allowed to attempt before being disconnected.
Port-Limit	Sets the maximum number of ports to be provided to the user by the NAS.

Table 16: RADIUS Role Mapping Attributes (*continued*)

Attribute	Description
Prompt	Indicates to the NAS whether it should echo the user's response as it is entered, or not echo it.
Proxy-State	A proxy server can send this attribute to another server when forwarding an Access-Request. The attribute must be returned unmodified in the Access-Accept, Access-Reject or Access-Challenge.
Reply-Message	Text that can be displayed to the user.
Service-Type	The type of service the user has requested, or the type of service to be provided.
Session-Timeout	Sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt.
State	A packet must have only zero or one State Attribute. Usage of the State Attribute is implementation dependent.
Telephone-number	Using the Calling-Station-Id and Called-Station-Id RADIUS attributes, authorization and subsequent tunnel attributes can be based on the phone number originating the call, or the number being called.
Termination-Action	The action the NAS should take when the specified service is completed.
Tunnel-Assignment-ID	Indicates to the tunnel initiator the particular tunnel to which a session is to be assigned.
Tunnel-Client-Auth-ID	Specifies the name used by the tunnel initiator during the authentication phase of tunnel establishment.
Tunnel-Client-Endpoint	Contains the address of the initiator end of the tunnel.
Tunnel-Link-Reject	Marks the rejection of the establishment of a new link in an existing tunnel.
Tunnel-Link-Start	Marks the creation of a tunnel link.
Tunnel-Link-Stop	Marks the destruction of a tunnel link.
Tunnel-Medium-Type	The transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports.

Table 16: RADIUS Role Mapping Attributes (*continued*)

Attribute	Description
Tunnel-Medium-Type	The transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports.
Tunnel-Password	A password to be used to authenticate to a remote server.
Tunnel-Preference	If the RADIUS server returns more than one set of tunneling attributes to the tunnel initiator, you should include this attribute in each set to indicate the relative preference assigned to each tunnel.
Tunnel-Private-Group-ID	The group ID for a particular tunneled session.
Tunnel-Reject	Marks the rejection of the establishment of a tunnel with another node.
Tunnel-Server-Auth-ID	Specifies the name used by the tunnel terminator during the authentication phase of tunnel establishment.
Tunnel-Server-Endpoint	The address of the server end of the tunnel.
Tunnel-Start	Marks the establishment of a tunnel with another node.
Tunnel-Stop	Marks the destruction of a tunnel to or from another node.
Tunnel-Type	The tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).
User-Name	The name of the user to be authenticated.
User-Password	The password of the user to be authenticated, or the user's input following an Access-Challenge.

Related Documentation

- [Configuring a RADIUS Server Instance on page 191](#)

General RADIUS Notes

Please note the following issues.

Understanding Clustering Issues

Accounting messages are sent to the RADIUS server by each cluster node without consolidation. RADIUS accounting follows these assumptions:

- If the cluster is active/passive, all users are connected to one node at a time.
- If the cluster is active/active and does not use a balancer, users are connected to different nodes but are static.
- If the cluster is active/active and uses a balancer, the balancer usually enforces a persistent source IP. In this case, users are always connected to the same node.

We do not support load balancing for RADIUS.

Understanding the Interim Update Feature

If you want a server to receive interim accounting messages, you can statically configure an interim value on the client, in which case, the locally-configured value overrides any value that might be included in the RADIUS Access-Accept message.

The octet count reported in the accounting messages is the cumulative total since the beginning of the user session.

The interim update byte count is only supported based on a user session, not on SAM or NC sessions.

The minimum interim update interval is 15 minutes. The data statistics (bytes in and bytes out) for RADIUS Accounting may not be sent for a J-SAM/W-SAM/NC session if the session is less than 30 seconds long and the applications keep the connections open all the time.

Related Documentation

- [Configuring a RADIUS Server Instance on page 191](#)

eTrust SiteMinder Overview

When you configure the Secure Access Service to authenticate users with an eTrust SiteMinder policy server, the Secure Access Service passes the user's credentials to SiteMinder during authentication. Once SiteMinder receives the credentials, it may use standard username and password authentication, ACE SecurID tokens, or clientside certificates to authenticate the credentials.

The Secure Access Service also passes a protected resource URL to SiteMinder during authentication in order to determine which SiteMinder realm it should use to authenticate the user. When the Secure Access Service passes the protected resource URL, SiteMinder authorizes the user's URL against the realm that is associated with the resource and allows the user to seamlessly access any resources whose protection levels are equal to or less than the resource the Secure Access Service passed.

The Secure Access Service enables single sign-on (SSO) from Secure Access to SiteMinder-protected resources using SMSESSION cookies. A SMSESSION cookie is a security token that encapsulates SiteMinder session information. Depending on your configuration, either the SiteMinder Web agent or the Secure Access Service creates a SMSESSION cookie and then posts the cookie to the following locations so the user does not have to re-authenticate if he wants to access additional resources:

- **The Secure Gateway:** If the user tries to access a SiteMinder resource from within his Secure Access Service session (for example, from the Secure Access Service file browsing page), the Secure Access Service passes its cached SMSESSION cookie to the Web agent for authentication.
- **The user's Web browser:** If the user tries to access a SiteMinder resource from outside of his Secure Access Service session (for example, when using a protected resource on a standard agent), SiteMinder uses the cached SMSESSION cookie stored in the user's Web browser to authenticate/authorize the user.

If you enable the Automatic Sign-In option the Secure Access Service can use an SMSESSION cookie generated by another agent to enable single sign-on from a SiteMinder resource to the Secure Access Service. When a user accesses the Secure Access Service sign-in page with an SMSESSION cookie, the Secure Access Service verifies the SMSESSION cookie. Upon successful verification, the Secure Access Service establishes a Secure Access Service session for the user. You can use the following authentication mechanisms when you enable automatic sign-in through the Secure Access Service:

- **Custom agent:** The Secure Access Service authenticates the user against the policy server and generates a SMSESSION cookie. When you select this option, you can enable SSO on other SiteMinder agents that use the same policy server. To enable SSO on these agents, update each of them to accept third party cookies. If you select this option and the user enters his Secure Access Service session with an SMSESSION cookie, the Secure Access Service attempts automatic sign-in when the user enters the Secure Access Service session.
- **HTML form post:** The Secure Access Service posts credentials to a standard Web agent that you have already configured. The Web agent then creates SMSESSION cookies. If you select this option, you cannot use SecurID New Pin and Next Token modes or client-side certificate authentication. If you select this option and the user enters his Secure Access Service session with an SMSESSION cookie, the Secure Access Service attempts automatic sign-in when the user enters the Secure Access Service session.
- **Delegated authentication:** The Secure Access Service delegates authentication to a standard agent. If this option is enabled, the Secure Access Service tries to determine the FCC URL associated with the protected resource. The Secure Access Service then redirects the user to the FCC URL with the Secure Access Service sign-in URL as the TARGET. Upon successful authentication, the user is redirected back to the Secure Access Service with an SMSESSION cookie and the Secure Access Service does an automatic sign-in for the user.



NOTE:

- At the time of this printing, Juniper Networks supports eTrust SiteMinder server version 6.0 and version 5.5 with standard agent versions 6 and 5QMR5. If you run older agents than the supported agents, you may experience cookie validation problems, including crossed log entries and intermittent user timeouts.
 - You can choose which eTrust SiteMinder server version you want to support when you create a server instance. You can choose version 5.5, which supports both versions 5.5 and 6.0, or you can choose version 6.0, which supports only version 6.0. There is no difference in the SiteMinder authentication server functionality based on which version you select. This option only controls the version of the Netegrity SDK to use. We recommend you match the compatibility mode with the version of the Policy Server.
 - When you use SiteMinder to authenticate, the primary and backup policy servers must run the same SiteMinder server software version. A mixed deployment (where the primary server runs a different server software version than the backup) is not supported.
 - SiteMinder does not store the IP address in the SMSESSION cookie, and therefore cannot pass it to the Secure Access Service.
 - SiteMinder sends the SMSESSION cookie to the Secure Access Service as a persistent cookie. To maximize security, the Secure Access Service resets the persistent cookie as a session cookie once authentication is complete.
 - When you use SiteMinder to authenticate, the Secure Access Service disregards any Secure Access Service session and idle timeouts and uses session and idle timeouts set through the SiteMinder realm instead.
 - When you use SiteMinder to authenticate, users must access the Secure Access Service using a fully-qualified domain name. This is because the SiteMinder SMSESSION cookie is only sent for the domain for which it is configured. If users access the Secure Access Service using an IP address, they may receive an authentication failure and will be prompted to authenticate again.
 - The Secure Access Service logs any SiteMinder error codes on the System > Log/Monitoring > User Access page. For information on the SiteMinder error codes, see the SiteMinder documentation.
-

Authentication Using Various Authentication Schemes

Within SiteMinder, an authentication scheme is a way to collect user credentials and determine the identity of a user. You may create different authentication schemes and associate different protection levels with each. For example, you may create two schemes—one that authenticates users based solely on the users' client-side certificates and provides them a low protection level, and a second that uses ACE SecurID token authentication and provides users a higher protection level. The Secure Access Service works with the following types of SiteMinder authentication schemes:

- **Basic username and password authentication**—The user's name and password are passed to the SiteMinder policy server. The policy server may then authenticate them itself or pass it to another server for authentication.
- **ACE SecurID token authentication**—The SiteMinder policy server authenticates users based on a username and password generated by an ACE SecurID token.
- **Client-side certificate authentication**—The SiteMinder policy server authenticates users based on their client-side certificate credentials. If you choose this authentication method, the Web browser displays a list of client certificates from which users can select.



NOTE:

- If you choose to authenticate users with this method, you must import the client certificate into the Secure Access Service through the System > Certificates > Trusted Client CAs tab.
 - If you do not want to display the standard Secure Access Service sign in page to users, you may change it using the customizable sign-in pages feature. For more information, see the *Custom Sign-In Pages Solution Guide*.
 - SiteMinder client-side certificate authentication is separate from Secure Access Service client-side certificate authentication. If you choose both, the Secure Access Service first authenticates using the Secure Access Service configuration parameters. If this succeeds, it then passes certificate values to SiteMinder for authentication.
-

Determining the Username

With the availability of different authentication schemes and sign-in points, the Secure Access Service may obtain a username from various sources, such as a policy server header, certificate attribute, or from the Secure Access Service sign-in page. Listed below are the various methods a user may employ to access the Secure Access Service and how the Secure Access Service determines the username for each. When a user:

- **Signs in through the standard Secure Access Service sign-in page**— The Secure Access Service first checks the username that the policy server returned in its OnAuthAccept response header. If SiteMinder does not define a username, the Secure Access Service uses the name that the user entered during sign-in. Otherwise, if neither

SiteMinder nor the user provide a username because the user authenticates using a client certificate, the Secure Access Service uses the UserDN value set by the policy server.

- **Automatically signs in to the Secure Access Service using SiteMinder credentials**—The Secure Access Service first checks the username that the policy server returned in its OnAuthAccept response header. If SiteMinder does not define a username, the Secure Access Service checks the SMSESSION cookie. Otherwise, if SiteMinder does not populate the response header or SMSESSION cookie with a username, the Secure Access Service checks the UserDN value in the SMSESSION cookie.

Once the Secure Access Service determines which username to use, it saves it in its session cache and references it when a user wants to access additional resources.

To consistently return the correct username to the Secure Access Service, you should configure the OnAuthAccept response on the SiteMinder policy server.

Related Documentation

- [Configuring Secure Access Service to Work with SiteMinder](#)
- [Creating a Rule/Response Pair to Pass Usernames to the Secure Access Service on page 216](#)
- [Creating a SiteMinder Realm for the Secure Access Service on page 215](#)
- [Creating a SiteMinder Domain for the Secure Access Service on page 215](#)
- [Creating a SiteMinder Authentication Scheme for the Secure Access Service on page 213](#)
- [Configuring the SiteMinder Agent on page 212](#)
- [Configuring SiteMinder to Work with the Secure Access Service on page 211](#)

Configuring SiteMinder to Work with the Secure Access Service

The following steps are required to configure a SiteMinder policy server to work with the Secure Access Service. These are not complete SiteMinder configuration instructions—they are only intended to help you make SiteMinder work with the Secure Access Service. For in-depth SiteMinder configuration information, refer to the documentation provided with your SiteMinder policy server.

- Configure the SiteMinder Agent.
- Create a SiteMinder authentication scheme for the Secure Access Service.
- Create a SiteMinder domain for the Secure Access Service.
- Create a SiteMinder realm for the Secure Access Service.
- Create a Rule/Response pair to pass usernames to the Secure Access Service.
- Create a SiteMinder Policy under the domain.

Related Documentation

- [eTrust SiteMinder Overview on page 207](#)
- [Configuring the SiteMinder Agent on page 212](#)

- [Creating a SiteMinder Authentication Scheme for the Secure Access Service on page 213](#)
- [Creating a SiteMinder Domain for the Secure Access Service on page 215](#)
- [Creating a SiteMinder Realm for the Secure Access Service on page 215](#)
- [Creating a Rule/Response Pair to Pass Usernames to the Secure Access Service on page 216](#)
- [Configuring Secure Access Service to Work with SiteMinder](#)

Configuring the SiteMinder Agent

A SiteMinder agent filters user requests to enforce access controls. For instance, when a user requests a protected resource, the agent prompts the user for credentials based on an authentication scheme, and sends the credentials to a SiteMinder policy server. A Web agent is simply an agent that works with a Web server. When configuring SiteMinder to work with the Secure Access Service, you must configure the Secure Access Service as a Web agent in most cases.



NOTE:

If you select the Delegate authentication to a standard agent option, you must set the following options in the agent configuration object of the standard Web agent host the FCC URL:

- `<EncryptAgentName=no>`
- `<FCCCompatMode=no>`

To configure the Secure Access Service as a Web agent on the SiteMinder policy server:

1. In the SiteMinder Administration interface, choose the **System** tab.
2. Right-click on **Agents** and choose **Create Agent**.
3. Enter a name for the Web agent and (optionally) a description. Note that you need to enter this name when creating a SiteMinder realm.
4. You must select the **Support 5.x agents** option for compatibility with the Secure Access Service.
5. Under Agent Type, select **SiteMinder** and then select **Web Agent** from the drop-down list. You must select this setting for compatibility with the Secure Access Service.
6. Under **IP Address** or **Host Name**, enter the name or IP address of the Secure Access Service.
7. In the **Shared Secret** field, enter and confirm a secret for the Web agent. Note that you need to enter this secret when configuring the Secure Access Service.
8. Click **OK**.

- Related Documentation**
- [eTrust SiteMinder Overview on page 207](#)
 - [Configuring SiteMinder to Work with the Secure Access Service on page 211](#)
 - [Creating a SiteMinder Authentication Scheme for the Secure Access Service on page 213](#)
 - [Creating a SiteMinder Domain for the Secure Access Service on page 215](#)
 - [Creating a SiteMinder Realm for the Secure Access Service on page 215](#)
 - [Creating a Rule/Response Pair to Pass Usernames to the Secure Access Service on page 216](#)
 - [Configuring Secure Access Service to Work with SiteMinder](#)

Creating a SiteMinder Authentication Scheme for the Secure Access Service

Within SiteMinder, an authentication scheme provides a way to collect credentials and determine the identity of a user.

To configure a SiteMinder authentication scheme for the Secure Access Service:

1. In the SiteMinder Administration interface, choose the **System** tab.
2. Right-click on **Authentication Schemes** and choose **Create Authentication Scheme**.
3. Enter a name for the scheme and (optionally) a description. Note that you need to enter this name when configuring the SiteMinder realm.
4. Under Authentication Scheme Type, select one of the following options:
 - **Basic Template**
 - **HTML Form Template**
 - **SecurID HTML Form Template** (If you are using SecurID authentication, you must choose SecurID HTML Form Template (instead of SecurID Template). Choosing this option enables the Policy Server to send ACE sign-in failure codes to the Secure Access Service).
 - **X509 Client Cert Template**
 - **X509 Client Cert and Basic Authentication**



NOTE:

- The Secure Access Service only supports the authentication scheme types listed here.
- You must select HTML Form Template if you want the Secure Access Service to handle re-authentication.
- If you select X509 Client Cert Template or X509 Client Cert and Basic Authentication, you must import the certificate into the Secure Access Service through the System > Certificates > Trusted Client CAs tab.

5. Enter a protection level for the scheme. Note that this protection level carries over to the SiteMinder realm that you associate with this scheme.
6. Select the **Password Policies Enabled for this Authentication Scheme** if you want to reauthenticate users who request resources with a higher protection level than they are authorized to access.
7. In the **Scheme Setup** tab, enter the options required by your authentication scheme type.

If you want the Secure Access Service to re-authenticate users who request resources with a higher protection level than they are authorized to access, you must enter the following settings:

- Under **Server Name**, enter the Secure Access Service host name (for example, sales.yourcompany.net).
- Select the Use SSL Connection checkbox.
- Under **Target**, enter the Secure Access Service sign-in URL defined in this step's first bullet plus the parameter "ive=1" (for example, /highproturl?ive=1). (The Secure Access Service must have a sign-in policy that uses */highproturl as the sign-in URL and only uses the corresponding SiteMinder authentication realm.)



NOTE: When you save changes, ive=1 disappears from the target. This is OK. The policy server includes ive=1 in the full authentication scheme URL that it sends to the Secure Access Service, as you can see in the in the **Parameter** field of the **Advanced** tab.

- De-select the **Allow Form Authentication Scheme to Save Credentials** checkbox.
 - Leave **Additional Attribute List** empty.
8. Click **OK**.

If you change a SiteMinder authentication scheme on the policy server, you must flush the cache using the **Flush Cache** option on the **Advanced** tab.

Related Documentation

- [Configuring Secure Access Service to Work with SiteMinder](#)
- [Creating a Rule/Response Pair to Pass Usernames to the Secure Access Service on page 216](#)
- [Creating a SiteMinder Realm for the Secure Access Service on page 215](#)
- [Creating a SiteMinder Domain for the Secure Access Service on page 215](#)
- [Configuring the SiteMinder Agent on page 212](#)
- [Configuring SiteMinder to Work with the Secure Access Service on page 211](#)
- [eTrust SiteMinder Overview on page 207](#)

Creating a SiteMinder Domain for the Secure Access Service

Within SiteMinder, a *policy domain* is a logical grouping of resources associated with one or more user directories. Policy domains contain realms, responses, and policies. When configuring the Secure Access Service to work with SiteMinder, you must give Secure Access Service users access to a SiteMinder resource within a realm, and then group the realm into a domain.

To configure a SiteMinder domain for the Secure Access Service:

1. Choose the **System** tab, right-click on **Domains** and choose **Create Domain**, or click on **Domains** and choose an existing SiteMinder domain.
2. Add a realm to the domain.

Related Documentation

- [Configuring SiteMinder to Work with the Secure Access Service on page 211](#)
- [Creating a SiteMinder Realm for the Secure Access Service on page 215](#)

Creating a SiteMinder Realm for the Secure Access Service

Within SiteMinder, a realm is a cluster of resources within a policy domain grouped together according to security requirements. When configuring SiteMinder to work with the Secure Access Service, you must define realms to determine which resources Secure Access Service users may access.

Within SiteMinder, a realm is a cluster of resources within a policy domain grouped together according to security requirements. When configuring SiteMinder to work with the Secure Access Service, you must define realms to determine which resources Secure Access Service users may access.

1. In the SiteMinder Administration interface, select the **Domains** tab.
2. Expand the domain that you created for the Secure Access Service.
3. Right-click on **Realms** and choose **Create Realm**.
4. Enter a name and (optionally) description for the realm.
5. In the Agent field, select the Web agent that you created for the Secure Access Service.
6. In the Resource Filter field, enter a protected resource. This resource inherits the protection level specified in the corresponding authentication scheme. For the default protection level, enter /ive-authentication. Note that you need to enter this resource when configuring the Secure Access Service. Or, if you use sign-in policies with nondefault URLs such as */nete or */cert, you must have corresponding resource filters in the SiteMinder configuration.
7. From the **Authentication Schemes** list, select the scheme that you created for the Secure Access Service.
8. Click **OK**.

- Related Documentation**
- [Configuring SiteMinder to Work with the Secure Access Service on page 211](#)
 - [Creating a SiteMinder Domain for the Secure Access Service on page 215](#)

Creating a Rule/Response Pair to Pass Usernames to the Secure Access Service

Within SiteMinder, you can use rules to trigger responses when authentication or authorization events take place. A response passes DN attributes, static text, or customized active responses from the SiteMinder policy server to a SiteMinder agent. When you configure SiteMinder to work with the Secure Access Service, you must create a rule that fires when a user successfully authenticates. Then, you must create a corresponding response that passes the user's username to the Secure Access Service Web agent.

To create a new rule:

1. In the SiteMinder Administration interface, choose the **Domains** tab.
2. Expand the domain that you created for the Secure Access Service, and then expand **Realms**.
3. Right-click on the realm that you created for the Secure Access Service, and choose **Create Rule under Realm**.
4. Enter a name and (optionally) description for the rule.
5. Under Action, choose **Authentication Events** and then select **OnAuthAccept** from the drop-down list.
6. Select **Enabled**.
7. Click **OK**.

To create a new response:

1. In the SiteMinder Administration interface, choose the **Domains** tab.
2. Expand the domain that you created for the Secure Access Service.
3. Right-click on **Responses** and select **Create Response**.
4. Enter a name and (optionally) a description for the response.
5. Select **SiteMinder** and then select the Secure Access Service Web agent.
6. Click **Create**.
7. From the Attribute list, select **WebAgent-HTTP-Header-Variable**.
8. Under Attribute Kind, select **Static**.
9. Under Variable Name, enter IVEUSERNAME.
10. Under Variable Value, enter a user name.
11. Click **OK**.

- Related Documentation**
- [Configuring SiteMinder to Work with the Secure Access Service on page 211](#)
 - [Configuring the SiteMinder Agent on page 212](#)

Configuring Secure Access to Work with SiteMinder

This section includes instructions for configuring Secure Access to work with a SiteMinder policy server.

Configuring Secure Access to Work with Multiple Authentication Schemes

To configure Secure Access to work with multiple SiteMinder authentication schemes, you must:

1. Configure the authentication schemes on the SiteMinder policy server.
2. Create one Secure Access instance of the SiteMinder policy server for all SiteMinder authentication schemes you want to use.
3. Specify which Secure Access realm should use the Secure Access instance of the SiteMinder policy server to authenticate and authorize administrators and users.
4. For each protected resource on the SiteMinder policy server, create a Secure Access sign-in policy. In the Authentication > Authentication > Signing In Policies > New Sign-In Policy page:
 - Specify a Secure Access sign-in URL that matches the SiteMinder protected resource URL on the policy server. Make the path portion of the URL match the SiteMinder resource filter in the SiteMinder realm configuration. For example, you can specify */ACE/ as a Secure Access sign-in URL to match a SiteMinder URL of XYZ/ACE, where XYZ is the name of a realm.
 - Select the Secure Access realm that you specified should use the SiteMinder policy server.

The user signs into Secure Access using one of the Secure Access sign-in URLs. Secure Access sends the protected resource URL to SiteMinder, and based on the resource, SiteMinder determines which type of scheme to use to authenticate the user. Secure Access collects the credentials that the authentication scheme requires, and then passes them to SiteMinder for authentication.

Configuring Secure Access to Grant Users Different Protected Resources

To configure Secure Access to grant users access to various SiteMinder protected resources (and by association, different protection levels), you must:

1. Define which resources the SiteMinder server should protect. Each of these resources inherits a protection level from a corresponding SiteMinder authentication scheme.
2. Create one Secure Access instance of the SiteMinder policy server for all protected resources and corresponding protection levels that you want to allow.

3. Specify which Secure Access realm should use the Secure Access instance of the SiteMinder policy server.
4. For each resource on the SiteMinder policy server, create a Secure Access sign-in policy for each realm-level resource filter. In the configuration page for the sign-in policy, specify:
 - A Secure Access sign-in URL that matches the protected resource URL on the policy server. Make the path portion of the URL match the SiteMinder resource filter. For example, you may define the following URLs:

https://employees.yourcompany.com/sales

https://employees.yourcompany.com/engineering

When users sign into the first URL, they can access the “sales” protected resource, and when they sign into the second URL, they can access the “engineering” protected resource.

To define a default resource (ive-authentication), enter * in the path portion of the URL.
 - Select the Secure Access realm that you specified should use the SiteMinder policy server.

During production, the user signs into Secure Access using one of the URLs. Secure Access extracts the protected resource from the URL and authenticates the user against the appropriate realm.

Defining an eTrust SiteMinder Server Instance

Within Secure Access, a SiteMinder instance is a set of configuration settings that defines how Secure Access interacts with the SiteMinder policy server. After defining the SiteMinder server instance, specify which Secure Access realm(s) should use the Secure Access instance of the SiteMinder policy server to authenticate and authorize administrators and users.

To define an eTrust SiteMinder server instance:

1. In the admin console, choose **Authentication > Auth. Servers**.
2. Do one of the following:
 - To create a new server instance on Secure Access, select **SiteMinder Server** from the New list, and then click **New Server**.
 - To update an existing server instance, click the appropriate link in the Authentication/Authorization Servers list.
3. Configure the server using the settings described in [Table 17 on page 219](#).
4. To add SiteMinder user attributes to the SiteMinder server instance:
 - a. Click **Server Catalog** to display the server catalog.
 - b. Enter the SiteMinder user attribute cookie name in the Attribute field in the server catalog and then click **Add Attribute**.

- c. When you are finished adding cookie names, click **OK**. Secure Access displays the names of the SiteMinder user attribute cookies in the Attribute list on the Role Mapping Rule page.
5. Click **Save Changes**.
6. Set advanced SiteMinder configuration options (optional) using the settings described in [Table 17 on page 219](#).

Table 17: eTrust SiteMinder Configuration Options

Option	Description
Name	Enter a name to identify the server instance.
Policy Server	Enter the name or IP address of the SiteMinder policy server that you want to use to authenticate users.
Backup Server(s), Failover Mode	<p>Enter a comma-delimited list of backup policy servers (optional). Then, choose a failover mode:</p> <ul style="list-style-type: none"> • Select Yes to have the Secure Access appliance use the main policy server unless it fails. • Select No to have the Secure Access appliance load balance among all the specified policy servers.
Agent Name, Secret	Enter the shared secret and agent name.. Note that these are case-sensitive.
Compatible with	Choose a SiteMinder server version. Version 5.5 supports versions 5.5 and 6.0. Version 6.0 supports only version 6.0 of the SiteMinder server API. Version 12.0 supports only version 12.0. The default value is 5.5 policy servers.
On logout, redirect to	<p>Specify a URL to which users are redirected when they sign out of Secure Access (optional). If you leave this field empty, users see the default Secure Access sign-in page.</p> <p><i>Note:</i> The On logout, redirect to field is included in the product release for backwards-compatibility, but is scheduled for discontinuance. If you want to redirect users to a different sign-in page when they sign out, we strongly recommend that you use the customizable sign-in pages feature instead. For more information, see the <i>Custom Sign-In Pages Solution Guide</i>.</p>
Protected Resource	<p>Specify a default protected resource. If you do not create sign-in policies for SiteMinder, Secure Access uses this default URL to set the user's protection level for the session. Secure Access also uses this default URL if you select the Automatic Sign-In option. If your users are signing in to the "*" URL (default Secure Access sign-in page), enter any URL ("/Secure Access-authentication" is the default) to set the protection level to the default Secure Access value. If you do create sign-in policies for SiteMinder, Secure Access uses those sign-in policies instead of this default URL.</p> <p><i>Note:</i> You must enter a forward slash (/) at the beginning of the resource (for example, "/ive-authentication").</p>

Table 17: eTrust SiteMinder Configuration Options (*continued*)

Option	Description
Resource Action	(Read-only) For new SiteMinder server instances, Secure Access sets the resource action to GET. If your SiteMinder instance is upgraded from a 3.x instance, Secure Access uses the resource action (for example, GET, POST, or PUT) that you previously chose. Note that to change an existing resource action to GET, you must delete the old SiteMinder server instance and then create a new instance that uses GET.
SMSESSION cookie settings	
Cookie Domain	<p>Enter the cookie domain for either the end-user or for the Secure Access Service. A <i>cookie domain</i> is a domain in which the user's cookies are active. For example, Secure Access sends cookies to the user's browser in this domain.</p> <p><i>Note:</i></p> <ul style="list-style-type: none"> Multiple domains should use a leading period and be comma-separated. For example: .sales.myorg.com, .marketing.myorg.com Domain names are case-sensitive. You cannot use wildcard characters. <p>For example, if you define ".juniper.net", the user must access the Secure Access device as "http://ive.juniper.net" in order to ensure that his SMSESSION cookie is sent back to the Secure Access Service.</p>
Protocol	(Read-only) Indicates that Secure Access uses HTTPS protocol to send cookies to the user's Web browser.
Secure Access Service Cookie Domain/IC Cookie Domain	Enter the Internet domain(s) to which Secure Access sends the SMSESSION cookie using the same guidelines outlined for the Cookie Domain field. (A Secure Access cookie domain enables single sign-on across multiple cookie domains. It allows a user's information to carry with him when he navigates from one domain to another.) If you have configured a cookie provider to enable single sign-on across multiple cookie domains, enter the domain of the cookie provider. Otherwise, enter the domain(s) of the Web agents for which single sign-on is desired. For example: .juniper.net
Protocol	Choose HTTPS to send cookies securely if other Web agents are set up to accept secure cookies, or HTTP to send cookies non-securely.
SiteMinder authentication settings	

Table 17: eTrust SiteMinder Configuration Options (*continued*)

Option	Description
Automatic Sign-In	<p>Select the Automatic Sign-In option to automatically sign in users who have a valid SMSESSION cookie in to Secure Access. Then, select the authentication realm to which the users are mapped. If you select this option, note that:</p> <ul style="list-style-type: none"> • If the protection level associated with a user's SMSESSION cookie is different from the protection level of the Secure Access realm, Secure Access uses the protection level associated with the cookie. • In order to enable single sign-on from another Web agent to Secure Access, Secure Access needs to validate an existing SMSESSION cookie created by a standard Web agent. • Secure Access supports the following realm and role limitations with the Automatic Sign-in feature: Host Checker, Cache Cleaner, IP address, browser, and concurrent user limit checks. Certificate and password restrictions are not supported since they are not applicable to automatically signed-in users. • Secure Access does not support the Automatic Sign in feature for administrator roles. This feature is only available for end-users. <p>When you select the Automatic Sign-In option, you must also configure the following sub-options:</p>
	<ul style="list-style-type: none"> • To assign user roles, use this authentication realm Select an authentication realm for automatically signed-in users. Secure Access maps the user to a role based on the role mapping rules defined in the selected realm.
	<ul style="list-style-type: none"> • If Automatic Sign In fails, redirect to Enter an alternative URL for users who sign into Secure Access through the Automatic Sign-In mechanism. Secure Access redirects users to the specified URL if Secure Access fails to authenticate and no redirect response is received from the SiteMinder policy server. If you leave this field empty, users are prompted to sign back in to Secure Access. <i>Note:</i> <ul style="list-style-type: none"> • Users who sign in through the Secure Access sign-in page are always redirected back to the Secure Access sign-in page if authentication fails. • If you are using the customizable UI (Custom Pages) option explained in the <i>Custom Sign-In Pages Solution Guide</i>, note that Secure Access redirects to welcome.cgi in two different cases. You must account for both of these special cases in your custom page: Session and idle timeouts: /dana-na/auth/welcome.cgi?p=timed-out Failed cookie validation: /dana-na/auth/welcome.cgi?p=failed <p>If you are using an authorization-only access policy, you must enter an alternative URL in this field regardless of whether you select the Automatic Sign In option. Users are redirected to this URL when SMSESSION cookie validation fails or if no SMSESSION cookie exists.</p>

Table 17: eTrust SiteMinder Configuration Options (*continued*)

Option	Description
Authenticate using custom agent	<p>Choose this option if you want to authenticate using the Secure Access custom Web agent. Note that if you select this option, you must also:</p> <ul style="list-style-type: none"> Update all of your standard Web agents to the appropriate Siteminder Agent Quarterly Maintenance Release (QMR) in order to accept the cookies created by Secure Access. If you are running SiteMinder version 5 Web agents, use the QMR5 hot fix. Secure Access is compatible with version 5.x and later SiteMinder agents. Older versions of SiteMinder agents are susceptible to cookie validation failures. Set the Accept Third Party Cookie attribute (AcceptTPCookie) to yes in the Web agent's configuration file (webagent.conf) or to 1 in the Windows Registry for the IIS Web server. The location of the attribute depends on the SiteMinder version and Web server you are using. For more information, please refer to the documentation provided with your SiteMinder server.
Authenticate using HTML form post	<p>Choose this option if you want to post user credentials to a standard Web agent that you have already configured rather than contacting the SiteMinder policy server directly. If you select this option, the Web agent contacts the policy server to determine the appropriate sign-in page to display to the user. In order to configure Secure Access to "act like a browser" that posts credentials to the standard Web agent, you must enter the information defined below. The easiest way to find this information is to:</p> <ol style="list-style-type: none"> Open a Web browser and enter the URL of the standard web agent that you want to use. For example, <code>http://webagent.juniper.net</code> Note the URL of the SiteMinder sign-in page that appears. For example: <code>http://webagent.juniper.net/siteminderagent/forms/login.fcc?TYPE=33554433&REALMOID=06-2525fa65-5a7f-11d5-9ee0-0003471b786c&GUID=&SMAUTHREASON=0&TARGET=\$SM\$http%3a%2f%2fwebagent%2ejuniper%2enet%2fportal%2findex%2ejsp</code> Extract information from the URL to enter in the fields that follow. <i>Note:</i> You cannot use SecurID New Pin and Next Token modes, client-side certificate authentication, or SNMP traps with the Authenticate using HTML form post option. The Authorize While Authenticating option is not applicable with the HTML form post option. You can authenticate users using this option, but if you want to authorize them as well, you must select Authenticate using custom agent. <p>When you select the Authenticate using HTML form post option, you must also configure the following sub-options:</p>

Table 17: eTrust SiteMinder Configuration Options (*continued*)

Option	Description
	<ul style="list-style-type: none"> Target URL on the external, eTrust-enabled Web server. In the Web agent sign-in page URL, the target appears after &TARGET=\$SMS\$. For example, in the URL shown in Authenticate Using HTML Form Post, the target is: <code>http%3a%2f%2fwebagent%2ejuniper%2enet%2fportal%2findex%2ejsp</code> After converting special characters (%3a=colon, %2f=backslash, %2e=period), the final target is: <code>http://webagent.juniper.net/portal/index.jsp</code>
	<ul style="list-style-type: none"> Protocol Protocol for communication between Secure Access and the specified Web agent. Use HTTP for non-secure communication or HTTPS for secure communication. In the Web agent sign-in page URL, the protocol appears first. For example, in the URL shown in Authenticate Using HTML Form Post, the protocol is HTTP.
	<ul style="list-style-type: none"> Web Agent Name of the Web agent from which Secure Access is to obtain SMSESSION cookies. An IP address is not allowed for this field. (Specifying the IP address as the Web agent prevents some browsers from accepting cookies.) In the Web agent sign-in page URL, the Web agent appears after the protocol. For example, in the URL shown above in Authenticate Using HTML Form Post, the Web agent is: <code>webagent.juniper.net</code>
	<ul style="list-style-type: none"> Port Port 80 for HTTP or port 443 for HTTPS.
	<ul style="list-style-type: none"> Path Path of the Web agent's sign-in page. Note that the path must start with a backslash (/) character. In the Web agent sign-in page URL, the path appears after the Web agent. For example, in the URL shown in Authenticate Using HTML Form Post, the path is: <code>/siteminderagent/forms/login.fcc</code>
	<ul style="list-style-type: none"> Parameters Post parameters to be sent when a user signs in. Common SiteMinder variables that you can use include <code>__USER__</code>, <code>__PASS__</code>, and <code>__TARGET__</code>. These variables are replaced by the username and password entered by the user on the Web agent's sign-in page and by the value specified in the Target field. These are the default parameters for login.fcc—if you have made customizations, you may need to change these parameters.

Table 17: eTrust SiteMinder Configuration Options (*continued*)

Option	Description
Delegate authentication to a standard agent	<p>Choose this option if you want to delegate authentication to a standard agent. When the user accesses the Secure Access sign-in page, Secure Access determines the FCC URL associated with the protected resource's authentication scheme. Secure Access redirects the user to that URL, setting the Secure Access sign-in URL as the target. After successfully authenticating with the standard agent, an SMSESSION cookie is set in the user's browser and he is redirected back to Secure Access. Secure Access then automatically signs in the user and establishes a Secure Access session.</p> <p>NOTE:</p> <ul style="list-style-type: none"> You must enable the Automatic Sign-In option in order to use this feature. If you enable this option and a user already has a valid SMSESSION cookie when he tries to access a resource, Secure Access tries to automatically sign in using the existing SMSESSION cookie. If the cookie is invalid, Secure Access clears the SMSESSION cookie and corresponding Secure Access cookies and presents the user with a "timeout" page. Secure Access successfully delegates authentication when the user clicks the "sign back in" option. If you select this option, your authentication scheme must have an associated FCC URL.

Table 18: eTrust SiteMinder Advanced Configuration Options

Option	Description
Poll Interval	Enter the interval at which Secure Access polls the Siteminder policy server to check for a new key.
Max. Connections	Controls the maximum number of simultaneous connections that Secure Access is allowed to make to the policy server. The default setting is 20.
Max. Requests/Connection	Controls the maximum number of requests that the policy server connection handles before Secure Access ends the connection. If necessary, tune to increase performance. The default setting is 1000.
Idle Timeout	Controls the maximum number of minutes a connection to the policy server may remain idle (the connection is not handling requests) before Secure Access ends the connection. The default setting of "none" indicates no time limit.

Table 18: eTrust SiteMinder Advanced Configuration Options (*continued*)

Option	Description
Authorize while Authenticating	<p>Specifies that Secure Access should look up user attributes on the policy server immediately after authentication to determine if the user is truly authenticated. For example, if your eTrust server authenticates users based on an LDAP server setting, you can select this option to indicate that Secure Access should authenticate users through the eTrust server and then authorize them through the LDAP server before granting them access. If the user fails authentication or authorization, he is redirected to the page configured on the policy server.</p> <p><i>Note:</i></p> <ul style="list-style-type: none"> If you do not select this option and you have authorization options setup through the Policy Users > Exclude tab of the policy server configuration utility, a user whom you have denied access may successfully authenticate into Secure Access. Not until the user tries to access a protected resource does Secure Access check his authorization rights and deny him access. Secure Access sends the same resource to the policy server for authorization as for authentication. This option is not supported with the Authenticate using HTML form post option or the Automatic sign-in.
Enable Session Grace Period, Validate cookie every N seconds	<p>You can eliminate the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that Secure Access should consider the cookie valid for a certain period of time. During that period, Secure Access assumes that its cached cookie is valid rather than re-validating it against the policy server. If you do not select this option, Secure Access checks the user's SMSESSION cookie on each request. Note that the value entered here does not affect session or idle timeout checking.</p>
Ignore Query Data	<p>By default, when a user requests a resource, Secure Access sends the entire URL for that resource to the policy server (including the query parameter, if present). For example, Secure Access may send the following URL to the policy server: http://foo/bar?param=value. (Query data appears after the ? character in the URL. Within this URL, param=value represents the query parameter.)</p> <p>Secure Access then caches the result of the authorization request for 10 minutes, including the query parameter. If the user then requests the same resource that is specified in the cached URL, the request fails since the query portion of the cached URL does not match the new request. Secure Access then has to re-contact the policy server to make a request that includes the new query parameter.</p> <p>If you select the Ignore Query Data option, Secure Access does not cache the query parameter in its URLs. Therefore, if a user requests the same resource as is specified in the cached URL, the request should not fail. For example, if you enable the Ignore Query Data option, both of the following URLs are considered the same resource:</p> <p>http://foo/bar?param=value1</p> <p>http://foo/bar?param=value2</p> <p>Enabling this option may improve performance.</p>

Table 18: eTrust SiteMinder Advanced Configuration Options (*continued*)

Option	Description
Accounting Port	The value entered in this field must match the accounting port value entered through the Policy Server Management Console. By default, this field matches the policy server's default setting of 44441.
Authentication Port	The value entered in this field must match the authentication port value entered through the Policy Server Management Console. By default, this field matches the policy server's default setting of 44442.
Authorization Port	The value entered in this field must match the authorization port value entered through the Policy Server Management Console. By default, this field matches the policy server's default setting of 44443.
Overlook Session for Methods	<p>Compares the request method to the methods listed here. If a match is found, Web Agent does not create a new or update an existing SMSESSION cookie, nor will it make any updates to the cookie provider for that request.</p> <p>You can enter multiple methods; use a comma to separate method names.</p> <p>If Overlook Session for Methods parameter is set but not Overlook Session for URLs, then all requests that match the methods defined in this parameter are processed (SMSESSION cookie creation/update is blocked).</p> <p>If both Overlook Session for Methods and Overlook Session for URLs parameters are set, both the method and the URL of the request are matched before proceeding. Then, all URLs with specified methods are processed (SMSESSION cookie creation/update is blocked).</p>
Overlook Session for URLs	<p>Compares the request URL to the URLs listed in this parameter. If a match is found, Web Agent does not create a new or update an existing SMSESSION cookie, nor will it make any updates to the cookie provider for that request.</p> <p>Specify a relative URL. For example: If the URL is <code>http://fqdn.host/MyDocuments/index.html</code>, enter /MyDocuments/index.html</p> <p>If Overlook Session for URLs is set but not Overlook Session for Methods, then all requests, regardless of the methods, matching the URLs defined in this parameter are processed (SMSESSION cookie creation/update is blocked).</p> <p>If both Overlook Session for Methods and Overlook Session for URLs parameters are defined, both the method and the URL of the request are matched before proceeding. Then, all URLs with specified methods are processed (SMSESSION cookie creation/update is blocked).</p>
Flush Cache	Use to delete the Secure Access resource cache, which caches resource authorization information for 10 minutes.

Related Documentation

Using SiteMinder User Attributes for Secure Access Role Mapping

After you create user attributes on a SiteMinder policy server, you can use them in role mapping rules for a realm that uses the SiteMinder policy server.

To use SiteMinder user attributes for Secure Access role mapping:

1. In the admin console, choose **Administrators > Admin Realms** or **Users > User Realms**.
2. On the General tab of the Authentication Realms page for the Secure Access realm that uses the SiteMinder policy server, choose **Same as Above** from the Directory/Attribute list.



NOTE: If you choose LDAP from the Directory/Attribute list instead of Same as Above, you can use both SiteMinder and LDAP attributes in role mapping rules.

3. On the Secure Access Role Mapping tab, create a rule based on Secure Access user attributes that references a SiteMinder user attribute cookie.

For example, to reference a SiteMinder user attribute cookie named department, add department to the list of Secure Access user attributes on the Secure Access Role Mapping tab. Then specify a value for the SiteMinder user attribute cookie, such as sales.

You can also use the following syntax to reference a SiteMinder user attribute cookie in a custom expression for a role mapping rule:

```
userAttr.<cookie-name>
```

For example:

```
<userAttr.department = ("sales" and "eng")>
```

Related Documentation

- [Creating an Authentication Realm on page 306](#)
- [Role Mapping Rules on page 308](#)

Defining a SiteMinder Realm for Automatic Sign-In

SiteMinder Automatic Sign In requires a realm whose authentication server is the SiteMinder server. If you perform an upgrade and you have already defined the Automatic Sign In realm that does not specify the SiteMinder server for authentication, and you have configured the SiteMinder server:

- The realms do not appear in the SiteMinder realm list under SiteMinder authentication settings in the admin console.

- The upgrade process creates a new realm called eTrust-Auto-Login-Realm which is based on your existing realm, but which configures the SiteMinder server as its authentication server.

To configure the SiteMinder realm on a new installation:

1. Select **Authentication > Auth. Servers**.
2. Choose **SiteMinder** from the New list and click **New Server**.
3. Specify the settings you want.
4. Click **Save Changes**.
5. Configure the realm, and select the SiteMinder server as the authentication server.
6. Select **Authentication > Auth. Servers**.
7. Choose the SiteMinder server you defined previously.
8. Under SiteMinder authentication settings, select the **Automatic Sign In** check box.
9. Choose the realm you just configured from the user authentication realm list.
10. Click **Save Changes**.



NOTE: The user authentication realm list on the SiteMinder server page only displays realms that are configured for SiteMinder. If you have not configured any SiteMinder realms, the drop down menu is empty.

**Related
Documentation**

- [Configuring SiteMinder to Work with the Secure Access Service on page 211](#)
- [Debugging SiteMinder and Secure Access Issues on page 228](#)

Debugging SiteMinder and Secure Access Issues

Problem At some point, you may encounter problems configuring the eTrust SiteMinder server interactions with Secure Access. You can use a number of debugging tools to identify and resolve problems:

- Solution**
- Review the Secure Access log file. Secure Access tracks failures of cookie validation, authorizing requests, and key rollovers.
 - Review the Policy Server Authentication log files.
 - Review the Standard Web Agent log file if you have selected the Authentication using HTML Form POST option.
 - Confirm that Secure Access contains the proper suffix that you defined in the Cookie Domain field. If Secure Access is not properly addressed, the browser may not forward the correct SMSESSION cookie to Secure Access and you may not be able to sign in. You must enter the Secure Access's FQDN on the browser, not the Secure Access IP address, otherwise, your login fails.

- Confirm that the Secure Access system time is synchronized with the SiteMinder server's system time. If the two system times are too divergent, the timeout settings may not function correctly, rejecting your attempts to sign in.
- In the SiteMinder server, confirm that you have defined the proper Session Timeout options max timeout and idle in the Siteminder Realm dialog.
- If you sign in to Secure Access and browse to a eTrust-protected Web agent, then reach the eTrust sign-in page instead of the single sign on (SSO) page, check the Secure Access Cookie Domain value to confirm that the domain matches the domain of the eTrust-protected Web agent. Review the setting for the Send Cookie Securely option. If Send Cookie Securely is set to yes, SSO works only with secure https:// sites. If Send Cookie Securely is set to no, SSO works with both http:// and https:// sites.

**Related
Documentation**

- [Configuring SiteMinder to Work with the Secure Access Service on page 211](#)

Defining a SAML Server Instance

This topic describes how to configure Secure Access Service as an Authentication Server for a SAML 2.0 deployment. For information on configuring an Authentication Server for a SAML 1.1 deployment, see [“Creating a SAML 1.1 Server Instance” on page 292](#).

To configure the Secure Access Service as a SAML SP:

1. In the admin console, select **Authentication > Auth. Servers**.
2. Select **SAML Server** from the New list and then click **New Server**.
3. Complete the settings as described in [Table 19 on page 229](#).
4. Click **Save Changes**.

After you save changes for the first time, the page is redisplayed and now has two tabs. The Settings tab allows you to modify any of the settings pertaining to the SAML Server instance. The Users tab lists valid users of the server.

Table 19: SAML SP Profile (POST and Artifact)

Setting	Guideline
Name	Specify a name to identify the server instance.
Settings	
SAML Version	Select 2.0 .
Secure Access Service Entity Id	This value is prepopulated. It is generated by the system, based on the value for the Host FQDN for SAML setting on the System > Configuration > SAML > Settings page.
Configuration Mode	Select Manual or Metadata . If a metadata file or location is available from the SAML IdP, use the metadata option to make configuration simpler and less prone to error. To upload or set the location for the published metadata file, go to System > Configuration > SAML and click the New Metadata Provider button.

Table 19: SAML SP Profile (POST and Artifact) (*continued*)

Setting	Guideline
Identity Provider Entity ID	<p>The IdP entity ID is sent as the Issuer value in the assertion generated by the SAML IdP.</p> <p>If you use the metadata option, this setting can be completed by selecting the IdP entity ID from the list. The list is populated by the IdP entities defined in metadata files added to the System > Configuration > SAML page.</p> <p>If you complete this setting manually, specify the Issuer value in assertions generated by the SAML IdP. Typically, you ask the SAML IdP administrator for this setting.</p>
Identity Provider Single Sign On Service URL	<p>The IdP SSO service URL is a URL provisioned by the SAML IdP. The setting is required to support SP-initiated SSO. If missing, the Secure Access Service cannot successfully redirect the user request.</p> <p>If you use the metadata option, this setting can be completed by selecting the SSO service URL from the list. The list is populated by the IdP entities defined in metadata files added to the System > Configuration > SAML page.</p> <p>If you complete this setting manually, ask the SAML IdP administrator for this setting.</p>
User Name Template	<p>Specify how the Secure Access Service is to derive the username from the assertion. If the field is left blank, it uses the string received in the NameID field of the incoming assertion as the username.</p> <p>If you choose a certificate attribute with more than one value, the Secure Access Service uses the first matched value. For example, if you enter <certDN.OU> and the user has two values for the attribute (ou=management, ou=sales), the Secure Access Service uses "management". To use all values, add the SEP attribute to the variable. For example, if you enter <certDN.OUT SEP=":">, the Secure Access Service uses "management:sales". The attributes received in the attribute statement in the incoming assertion are saved under userAttr. These variables can also be used with angle brackets and plain text. If the user name cannot be generated using the specified template, the login fails. If the NameID field of the incoming assertion is of type X509Nameformat, then the individual fields can be extracted using system variable "assertionNameDN".</p>
Allowed Clock Skew	<p>Specify the maximum allowed difference in time between the Secure Access Service clock and the SAML identity provider server clock.</p> <p>NOTE: SAML is a time sensitive protocol. The time-based validity of a SAML assertion is determined by the SAML identity provider. If the SAML identity provider and SAML service provider clocks are askew, the assertion can be determined invalid, and you will receive the following error:</p> <p>"SAML Transferred failed. Please contact your system administrator. Detail: Failure: No valid assertion found in SAML response."</p> <p>We recommend you use NTP to ensure the clocks are synchronized and that you set an Allowed Clock Skew value that accommodates any expected or permissible skew.</p>

Table 19: SAML SP Profile (POST and Artifact) (*continued*)

Setting	Guideline
Support Single Logout	<p>Single logout is a mechanism provided by SAML for logging out a particular user from all the sessions created by the IdP. Select this option if the Secure Access Service must receive and send single logout request for the peer SAML IdP.</p> <p>If you use the metadata option, the Single Logout Service URL setting can be completed by selecting the SLO service URL from the list. The list is populated by the IdP entities defined in metadata files added to the System > Configuration > SAML page. The Secure Access Service sends Single Logout requests to this URL.</p> <p>In addition, if you use the metadata option, the Single Logout Response URL setting is completed based on your selection for Single Logout Service URL. If the IdP has left this setting empty in its metadata file, the Secure Access Service sends the Single Logout response to the SLO service URL.</p> <p>If you complete these settings manually, ask the SAML IdP administrator for guidance.</p>
SSO Method	
Artifact	<p>When configured to use the Artifact binding, the Secure Access Service contacts the Artifact Resolution Services (ARS) to fetch the assertion using SOAP protocol. If the ARS is hosted on a HTTPS URL, then the certificate presented by the ARS is verified by the Secure Access Service. For this verification to pass successfully, the CA of the server certificate issued to the IdP ARS must be added to the Trusted Server CA on the Secure Access Service.</p> <p>Complete the following settings to configure SAML using the HTTP Artifact binding:</p> <ul style="list-style-type: none"> • Source ID. Enter the source ID for the IdP ARS. Source ID is Base64 encoded 20 byte identifier for the IdP ARS. If left blank, this value is generated by the Secure Access Service. • Source Artifact Resolution Service URL. For metadata-based configuration, this field is completed automatically from the metadata file and is not configurable. For manual configurations, enter the URL of the service to which the SP ACS is to send ArtifactResolve requests. ArtifactResolve requests are used to fetch the assertion from the artifact received by it. • SOAP Client Authentication. Select HTTP Basic or SSL Client Certificate and complete the related settings. If you use an SSL client certificate, select a certificate from the Secure Access Service device certificate list. • Select Device Certificate for Signing. Select the device certificate the Secure Access Service uses to sign the AuthnRequest sent to the IdP SSO service. If you do not select a certificate, the Secure Access Service does not sign AuthnRequest. • Select Device Certificate for Encryption. Select the device certificate the Secure Access Service uses to decrypt encrypted data received in the SAML response. The public key associated with the device certificate is used by the IdP for encryption.

Table 19: SAML SP Profile (POST and Artifact) (*continued*)

Setting	Guideline
POST	<p>When configured to use the POST binding, the Secure Access Service uses a response signing certificate to verify the signature in the incoming response or assertion. The certificate file must be in PEM or DER format. The certificate you select should be the same certificate used by the IdP to sign SAML responses.</p> <p>Complete the following settings to configure SAML using the HTTP POST binding:</p> <ul style="list-style-type: none"> • Response Signing Certificate. If you use the metadata-based configuration option, select a certificate from the list. The list is populated by the IdP entities defined in metadata files added to the System > Configuration > SAML page. If you configure these settings manually, browse to and upload the certificate to be used to validate the signature in the incoming response or assertion. If no certificate is specified, the certificate embedded in the response is used. • Enable Signing Certificate status checking. Select this option to check the validity of the signing certificate before verifying the signature. This setting applies to any certificate used for signature verification. If this option is enabled, the response will be rejected if the certificate is revoked, expired, or untrusted. If this option is selected, the certificate CA must be added to the Secure Access Service Trusted Client CA store. If this option is not enabled then the certificate is used without any checks. • Select Device Certificate for Signing. Select the device certificate the Secure Access Service uses to sign the AuthnRequest sent to the IdP SSO service. If you do not select a certificate, the Secure Access Service does not sign AuthnRequest. • Select Device Certificate for Encryption. Select the device certificate the Secure Access Service uses to decrypt encrypted data received in the SAML response. The public key associated with the device certificate is used by the IdP for encryption.
Service Provider Metadata Settings	
Metadata Validity	Enter the number of days the Secure Access metadata is valid. Valid values are 0 to 9999. 0 specifies the metadata does not expire.
Do Not Publish Secure Access Service Metadata	Select this option if you do not want the Secure Access Service to publish the metadata at the location specified by the Secure Access Service Entity ID field.
Download Metadata	This button appears only after you have saved the Authentication Server configuration. Use this button to download the metadata of the current SAML SP.
User Record Synchronization	
Enable User Record Synchronization	Allow users to retain their bookmarks and individual preferences regardless of which Secure Access Service device they log in to.

Related Documentation

- [Understanding SAML 2.0 on page 233](#)
- [Configuring Secure Access Service as a SAML 2.0 Service Provider on page 246](#)
- [Investigating a “No valid assertion found in SAML response” Error on page 275](#)

CHAPTER 9

SAML Single Sign-on

This chapter describes how to use the Junos Pulse Secure Access Service in a SAML single sign-on deployment. It includes the following sections:

- [Junos Pulse Secure Access Service SAML 2.0 SSO Solutions on page 233](#)
- [Secure Access Service SAML 2.0 Configuration Tasks on page 242](#)
- [Example: Implementing SAML 2.0 Web Browser SSO for Google Apps on page 266](#)
- [Investigating a “No valid assertion found in SAML response” Error on page 275](#)
- [Junos Pulse Secure Access Service SAML 1.1 Support on page 280](#)

Junos Pulse Secure Access Service SAML 2.0 SSO Solutions

This section provides a brief overview of the Security Assertion Markup Language (SAML) standard produced and approved by the Organization for the Advancement of Structured Information Standards (OASIS). It includes the following topics:

- [Understanding SAML 2.0 on page 233](#)
- [Secure Access Service SAML 2.0 Supported Features Reference on page 234](#)

Understanding SAML 2.0

This topic provides a reference to the Security Assertion Markup Language (SAML) standard and an overview of SAML 2.0 use cases. It includes the following information:

- [About SAML on page 233](#)
- [SAML Use Cases on page 234](#)

About SAML

SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. The standard defines the XML-based assertions, protocols, bindings, and profiles used in communication between SAML entities. SAML is used primarily to implement Web browser single sign-on (SSO). SAML enables businesses to leverage an identity-based security system like the Junos Pulse Secure Access Service to enforce secure access to websites and other resources without prompting the user with more than one authentication challenge.

For complete details on the SAML standard, see the OASIS website:

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

SAML Use Cases

This section provides a brief summary of the primary SAML use cases. It includes the following information:

- [SAML SSO on page 234](#)
- [SAML ACL on page 234](#)

SAML SSO

SAML is primarily used to enable Web browser single sign-on (SSO). The user experience objective for SSO is to allow a user to authenticate once and gain access to separately secured systems without resubmitting credentials. The security objective is to ensure the authentication requirements are met at each security checkpoint.

In an SSO transaction, the SAML services implemented at each secured system exchange requests and assertions to determine whether to allow access. The SAML assertions used in SSO transactions include authentication statements and attribute statements.

SAML ACL

SAML can also be used to enforce access control list (ACL) permissions. In an ACL transaction, the SAML services implemented for each secured system exchange assertions to determine whether a user can access the resource. The SAML assertions used in ACL transactions include authorization requests and authorization decision statements.

Related Documentation

- [Secure Access Service SAML 2.0 Supported Features Reference on page 234](#)
- [Configuring Secure Access Service as a SAML 2.0 Service Provider on page 246](#)
- [Configuring Secure Access Service as a SAML 2.0 Identity Provider on page 250](#)
- [Configuring a SAML 2.0 ACL Web Policy on page 264](#)

Secure Access Service SAML 2.0 Supported Features Reference

This topic provides an overview of Junos Pulse Secure Access Service support for Security Assertion Markup Language (SAML) single sign-on (SSO). It includes the following information related to SAML 2.0 support:

- [Supported SAML SSO Deployment Modes on page 234](#)
- [Supported SAML SSO Profiles on page 240](#)
- [FIPS Support Notes on page 241](#)

Supported SAML SSO Deployment Modes

In a SAML deployment, a SAML service provider is a secured resource (an application, website, or service) that is configured to request authentication from a SAML identity provider. The SAML identity provider responds with assertions regarding the identity, attributes, and entitlements (according to your configuration). The exchange enforces security and enables the SSO user experience.

The Secure Access Service can act as a SAML service provider, a SAML identity provider, or both. The following sections provide illustrations:

- [Secure Access Service as a SAML Service Provider on page 235](#)
- [Secure Access Service As a SAML Identity Provider \(Gateway Mode\) on page 237](#)
- [Secure Access Service as a SAML Identity Provider \(Peer Mode\) on page 238](#)

Secure Access Service as a SAML Service Provider

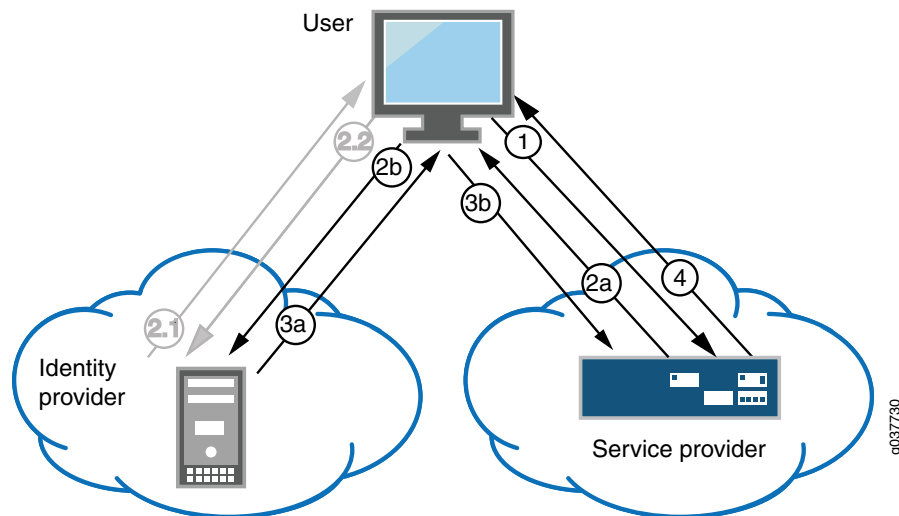
If you are working with a partner that has implemented a SAML identity provider, you can deploy the Secure Access Service as a SAML service provider to interoperate with it, thereby enabling SSO for users who should have access to resources in both networks. In this model, the user is authenticated by the SAML identity provider. The Secure Access Service uses the SAML response containing the assertion to make an authentication decision.

The choices the identity provider makes to implement SAML determine the Secure Access Service deployment choices, for example whether to use SAML 2.0 or SAML 1.1, whether to reference a published metadata configuration file, and whether to use a POST or artifact profile. When you deploy the Secure Access Service as a SAML service provider, you create a SAML authentication server that references the partner SAML identity provider, and a set of Secure Access Service access management framework objects (realm, role mapping rules, and sign-in policy) that reference the SAML authentication server.

When you configure the SAML service provider, some particular settings are necessary to support either identity-provider-initiated or service-provider-initiated SSO. The documentation for the configuration steps makes note of these settings. Regardless, you configure the SAML service provider to support both identity-provider-initiated and service-provider-initiated SSO.

[Figure 11 on page 236](#) illustrates the flow of network communication in a service-provider-initiated SSO scenario.

Figure 11: Secure Access Service as a SAML Service Provider in a Service-Provider-Initiated SSO Scenario



1 – The user clicks a link to access a resource.

2a – The service provider sends an HTTP redirect status code (HTTP 302) to the user. The SAML request and all other SAML details are sent as URL parameters in the URL Location header.

2b – The user sends an HTTP GET request to the identity provider. The SAML request and all other SAML details are sent as URL parameters.

If the user already has a session with the identity provider, steps 2.1 and 2.2 are skipped.

2.1 – If the user does not have a session, the identity provider sends an authentication challenge to the user.

2.2 – The user enters sign-in credentials.

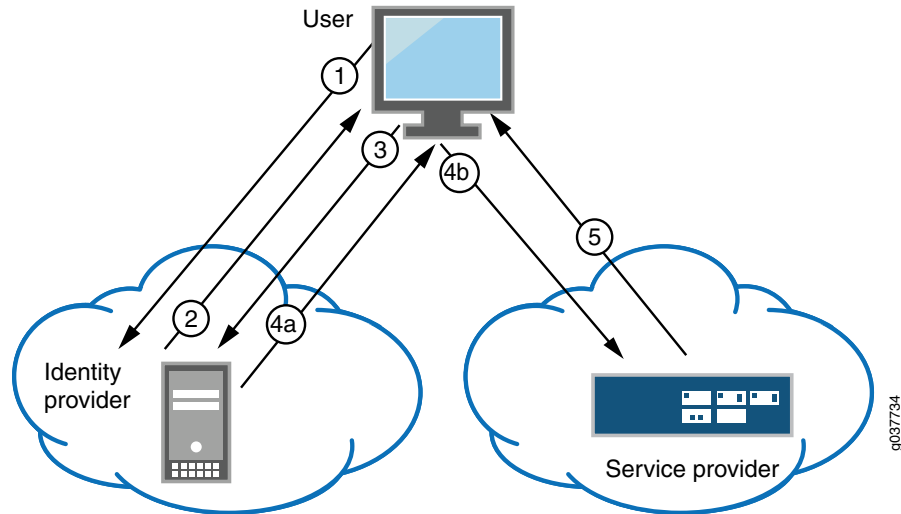
3a – The identity provider sends a successful status code (HTTP 200 OK) to the user with a form in the HTML body.

3b – The user sends the form to the service provider.

4 – The external resource is delivered to the user's browser.

Figure 12 on page 237 illustrates the flow of network communication in an identity-provider-initiated SSO scenario.

Figure 12: Secure Access Service as a SAML Service Provider in an Identity-Provider-Initiated SSO Scenario



1 – The user authenticates to the identity provider.

2 – The identity provider returns a portal page with links to external resources.

3 – The user clicks a link for an external resource.

4a – The identity provider sends a successful status code (HTTP 200 OK) to the user with a form in the HTML body.

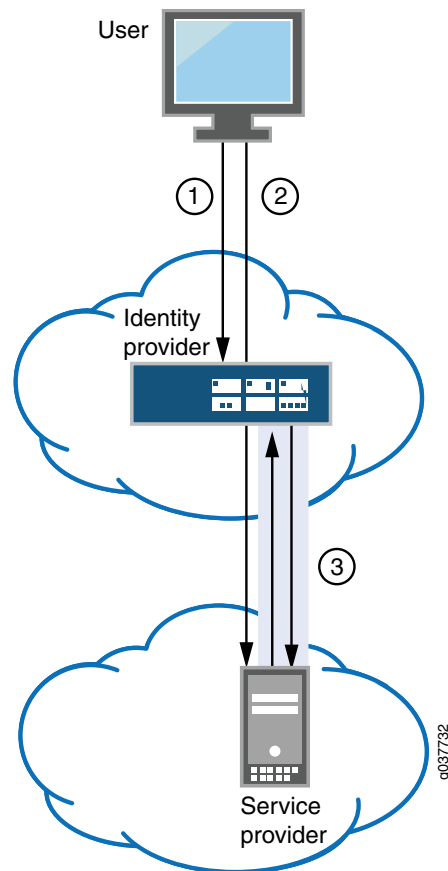
4b – The user sends the form to the service provider.

5 – The external resource is delivered to the user's browser.

Secure Access Service As a SAML Identity Provider (Gateway Mode)

When you deploy the Secure Access Service in front of enterprise resources that support SAML and have been configured as a SAML service provider, the Secure Access Service acts as a gateway for user access to the secured resource, just as it does with its other resource policies. The Secure Access Service maintains the session and uses its rewriting or pass-through proxy features to render data to the user. In the SAML exchange, the Secure Access Service acts as a SAML identity provider. When deployed as a gateway, the SAML SSO communication is always identity-provider-initiated. [Figure 13 on page 238](#) illustrates this scenario.

Figure 13: Secure Access Service as a SAML Identity Provider (Gateway Mode)



1 – A user logs into the Secure Access Service.

2 – The user clicks a link to a resource protected by a security system that supports SAML and has implemented a SAML service provider.

3 – The SAML identity provider initiates the SAML authentication request to the SAML service provider. Users are granted access to particular resources according to the Secure Access Service SAML SSO resource policy.

Secure Access Service as a SAML Identity Provider (Peer Mode)

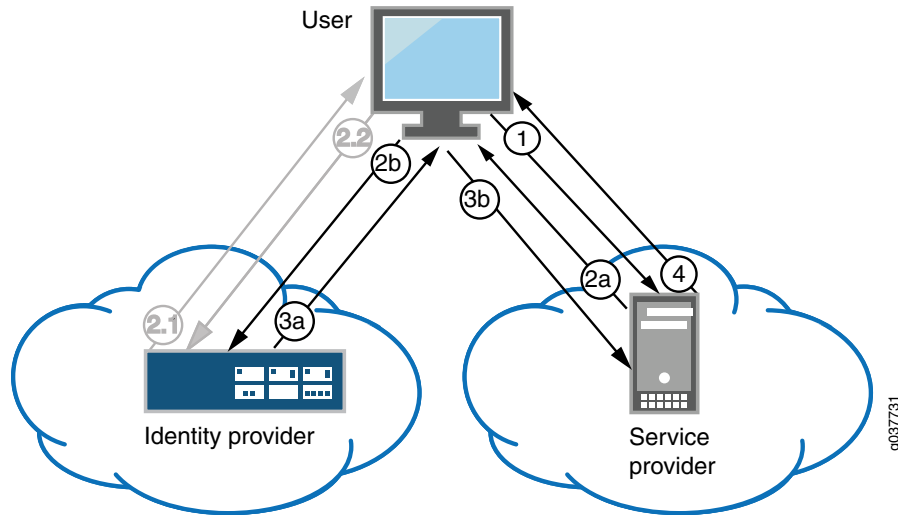
When deployed to support access to external resources (for example, public cloud resources), the Secure Access Service does not have to be a gateway to user access. The user can access the external resource directly, and the traffic does not flow through the Secure Access Service device. You configure the Secure Access Service as a SAML identity provider to correspond with the external SAML service provider, and you configure a SAML SSO external applications policy to determine the users and resources to which the SAML SSO experience applies.

When you configure the SAML identity provider, some settings are necessary to support either identity-provider-initiated or service-provider-initiated SSO. The documentation for the configuration steps makes note of these settings. Regardless, you configure the

SAML identity provider to support both identity-provider-initiated and service-provider-initiated SSO.

Figure 14 on page 239 illustrates the flow of network communication in a service-provider-initiated SSO scenario.

Figure 14: Secure Access Service as a SAML Identity Provider (Peer Mode) in a Service-Provider-Initiated SSO Scenario



1 – The user clicks a link to access a resource.

2a – The service provider sends an HTTP redirect status code (HTTP 302) to the user. The SAML request and all other SAML details are sent as URL parameters in the URL Location header.

2b – The user sends an HTTP GET request to the identity provider. The SAML request and all other SAML details are sent as URL parameters.

If the user already has a session with the identity provider, steps 2.1 and 2.2 are skipped.

2.1 – If the user does not have a session, the identity provider sends an authentication challenge to the user.

2.2 – The user enters sign-in credentials.

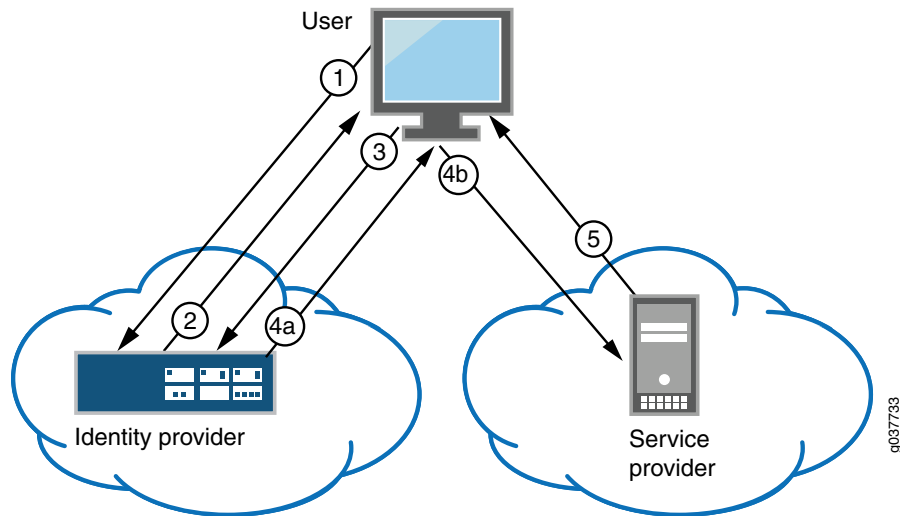
3a – The identity provider sends a successful status code (HTTP 200 OK) to the user with a form in the HTML body.

3b – The user sends the form to the service provider.

4 – The external resource is delivered to the user's browser.

Figure 15 on page 240 illustrates the flow of network communication in an identity-provider-initiated SSO scenario.

Figure 15: Secure Access Service as a SAML Identity Provider (Peer Mode) in an Identity-Provider-Initiated SSO Scenario



1 – The user authenticates to the identity provider.

2 – The identity provider returns a portal page with links to external resources.

3 – The user clicks a link for an external resource.

4a – The identity provider sends a successful status code (HTTP 200 OK) to the user with a form in the HTML body.

4b – The user sends the form to the service provider.

5 – The external resource is delivered to the user's browser.

Supported SAML SSO Profiles

Table 20 on page 240 summarizes support for SAML 2.0 deployment profiles.

Table 20: Supported SAML 2.0 Deployment Profiles

Profile	Message Flows	Binding	Service Provider	Identity Provider (Gateway)	Identity Provider (Peer)
Web browser SSO	<AuthnRequest> from service provider to identity provider	HTTP redirect	Supported	–	Supported
		HTTP POST	Not supported	–	Supported
		HTTP artifact	Not supported	–	Not supported
	Identity provider <Response> to service provider	HTTP POST	Supported	Supported	Supported
		HTTP artifact	Supported	Supported	Supported

Table 20: Supported SAML 2.0 Deployment Profiles (*continued*)

Profile	Message Flows	Binding	Service Provider	Identity Provider (Gateway)	Identity Provider (Peer)
Basic attribute profile	Simple <Attribute> statements (name-value pairs) as part of assertions	HTTP POST	Consumes and stores Attribute statements	Sends Attribute statements	Sends Attribute statements
		HTTP artifact			
Assertion query / request	Artifact resolution <ArtifactResolve> <ArtifactResponse>	SOAP	Supported	Supported	Supported
Single logout	Logout request	HTTP redirect	Supported	Not supported	Not supported
		HTTP POST	Not supported	Not supported	Not supported
		HTTP artifact	Not supported	Not supported	Not supported
		SOAP	Not supported	Not supported	Not supported
	Logout response	HTTP redirect	Supported	Not supported	Not supported
		HTTP POST	Not supported	Not supported	Not supported
		HTTP artifact	Not supported	Not supported	Not supported
		SOAP	Not supported	Not supported	Not supported



NOTE: Secure Access Service does not act as an Attribute Authority.

FIPS Support Notes

Historically, in FIPS deployments, private keys were managed in a way that can be problematic for SAML functionality that depends on access to the private key. [Table 21 on page 241](#) summarizes our support for SAML for FIPS deployments.

Table 21: SAML Support for FIPS Deployments

	SAML 2.0		SAML 1.1	
	Service Provider	Identity Provider	Consumer	Producer
7.4	Device certificate signing is supported; however, the ECDSA certificates is not supported. There are no other limitations.	Device certificate signing is supported; however, the ECDSA certificates is not supported. There are no other limitations.	No limitations	Artifact profile only

Table 21: SAML Support for FIPS Deployments (*continued*)

	SAML 2.0		SAML 1.1	
	Service Provider	Identity Provider	Consumer	Producer
7.3	Same as 7.2.	Same as 7.2.	No limitations	Artifact profile only
7.2	<p>The following configuration restrictions apply to the Authentication Server configuration:</p> <ul style="list-style-type: none"> Set Select Device Certificate for Signing to Not Applicable. Set Select Device Certificate for Encryption to Not Applicable. 	<p>The following configuration restrictions apply to the Sign-In SAML Identity Provider configuration:</p> <ul style="list-style-type: none"> Set Protocol Binding to Use for SAML Response to Artifact. POST is not supported. Set Signing Certificate to No Signing. Set Decryption Certificate to No Encryption. Clear the Enable Artifact Response Signing and Encryption check box. <hr/> <p>Support for valid 7.1 configurations (Legacy mode)</p>	No limitations	Artifact profile only
7.1	<p>The following configuration restrictions apply to the authentication server configuration:</p> <ul style="list-style-type: none"> Set Select Device Certificate for Signing to Not Applicable. Set Select Device Certificate for Encryption to Not Applicable. 	Artifact profile only	No limitations	Artifact profile only
7.0	–	–	No limitations	Artifact profile only

- Related Documentation**
- [Understanding SAML 2.0 on page 233](#)
 - [Configuring Secure Access Service as a SAML 2.0 Service Provider on page 246](#)
 - [Configuring Secure Access Service as a SAML 2.0 Identity Provider on page 250](#)

Secure Access Service SAML 2.0 Configuration Tasks

This section includes the tasks you perform to enable and configure SAML services. It includes the following information:

- [Configuring System-Wide SAML Settings on page 243](#)
- [Configuring Secure Access Service as a SAML 2.0 Service Provider on page 246](#)
- [Configuring Secure Access Service as a SAML 2.0 Identity Provider on page 250](#)
- [Configuring a SAML 2.0 ACL Web Policy on page 264](#)

Configuring System-Wide SAML Settings

This section describes tasks related to configuring system-wide SAML settings. It includes the following topics:

- [Configuring Global SAML Settings on page 243](#)
- [Managing SAML Metadata Files on page 244](#)

Configuring Global SAML Settings

The system-wide SAML settings impact all SAML service provider and identity provider instances.

To configure global SAML settings:

1. In the admin console, select **System > Configuration > SAML**.
2. Click the **Settings** button.
3. Complete the settings described in [Table 22 on page 243](#).
4. Click **Save Changes**.

Table 22: SAML Global Settings

Setting	Description
Timeout value for metadata fetch request	Specify the number of seconds after which a download request is abandoned. If the peer SAML entity publishes its metadata at a remote location, the Secure Access Service downloads the metadata file from the specified location.
Validity of uploaded/downloaded metadata file	Specify the maximum duration for which the Secure Access Service considers the metadata file of the peer SAML entity to be valid. If the metadata file provided by the peer SAML entity contains validity information, the lower value takes precedence.
Host FQDN for SAML	<p>Specify the fully qualified domain name for the Secure Access Service host. The value you specify here is used in the SAML entity ID and the URLs for SAML services, including:</p> <ul style="list-style-type: none"> • Entity ID for SAML service provider and SAML identity provider instances. The SAML entity ID is the URL where the Secure Access Service publishes its SAML metadata file. • Single sign-on service URL • Single logout service URL • Assertion consumer service URL • Artifact resolution service URL <p>BEST PRACTICE: The Secure Access Service uses HTTPS for these services. Therefore, we recommend that you assign a valid certificate to the interface that has the IP address to which this FQDN resolves so that users do not see invalid certificate warnings.</p>

Table 22: SAML Global Settings (*continued*)

Setting	Description
Alternate Host FQDN for SAML	<p>Optional.</p> <p>If you have enabled the Reuse Existing NC (Pulse) Session on the SAML Identity Provider Sign-In page, specify the fully qualified domain name used to generate the Secure Access Service SSO Service URL.</p> <p>Set up your DNS service to ensure that the alternate hostname resolves to a different IP address when a session is established and when not established. We recommend the following DNS behavior:</p> <ul style="list-style-type: none"> • If the NC (Pulse) session is not established, the IP address of the alternate hostname should resolve to the public IP address on the Secure Access Service external port. • If the NC (Pulse) session is established, the IP address of the alternate hostname should resolve to the private IP address on the Secure Access Service internal port. <p>BEST PRACTICE: The Secure Access Service uses HTTPS for this service. Therefore, we recommend that you assign a valid certificate to the interface that has the IP address to which this FQDN resolves so that users do not see invalid certificate warnings.</p>
Update Entity IDs	Use this button to regenerate the SAML entity IDs of all configured service providers and identity providers. Typically, you take this action when the Host FQDN for SAML is changed.

Related Documentation

- [Managing SAML Metadata Files on page 244](#)

Managing SAML Metadata Files

You use the System > Configuration > SAML pages to maintain a table of SAML metadata files for the SAML service providers and identity providers in your network. Using SAML metadata files makes configuration easier and less prone to error.

You can add the metadata files to the Secure Access Service by:

- Uploading a metadata file.
- Retrieving the metadata file from a well-known URL.

To add metadata files:

1. In the admin console, choose **System > Configuration > SAML**.
2. Click **New Metadata Provider**.
3. Complete the settings described in [Table 23 on page 245](#).
4. Click **Save Changes**.

Table 23: SAML Metadata Provider Settings

Setting	Description
Metadata Provider Location Configuration	<p>Use one of the following methods:</p> <ul style="list-style-type: none"> Local. Click Browse and locate the metadata file on your local host or file system. Remote. Enter the URL of the metadata file. Only http and https protocols are supported.
Metadata Provider Verification Configuration	<p>Select options:</p> <ul style="list-style-type: none"> Accept Untrusted Server Certificate. If you specify a URL for the metadata provider, select this option to allow the Secure Access Service to download the metadata file even if the server certificate is not trusted. This is necessary only for HTTPS URLs. Accept Unsigned Metadata. If this option is not selected, unsigned metadata is not imported. Signed metadata is imported only after signature verification. Signing Certificate. Click Browse and locate the certificate that verifies the signature in the metadata file. This certificate overrides the certificate specified in the signature of the received metadata. If no certificate is uploaded here then the certificate present in the signature of the received metadata is used. Enable Certificate Status Checking. Verify the certificate before using it. Certificate verification applies both to the certificate specified here and the certificate specified in the signature in the metadata file.
Metadata Provider Filter Configuration	<p>Select options and enter Entity IDs:</p> <ul style="list-style-type: none"> Roles. Select whether the metadata file includes configuration details for a SAML service provider, identity provider, or Policy Decision Point. You may select more than one. If you select a role that is not in the metadata file, it is ignored. If none of the selected roles are present in the metadata file, Secure Access Service returns an error. Entity IDs To Import. Enter the SAML Entity IDs to import from the metadata files. Enter only one ID per line. Leave this field blank to import all IDs. This option is available only for uploading local metadata files.

The Refresh button downloads the metadata files from the remote location even if these files have not been modified. This operation applies only to remote locations; local metadata providers are ignored if selected.

To refresh a metadata file:

1. In the admin console, choose **System > Configuration > SAML**.
2. Select the metadata file to refresh and click **Refresh**.

To delete a metadata file:

1. In the admin console, choose **System > Configuration > SAML**.
2. Select the metadata file to delete and click **Delete**.

Related Documentation

- [Configuring Peer SAML Service Provider Settings on page 255](#)

Configuring Secure Access Service as a SAML 2.0 Service Provider

This topic describes how to configure the Secure Access Service as a SAML service provider. When the Secure Access Service is a SAML service provider, it relies on the SAML identity provider authentication and attribute assertions when users attempt to sign in to the Secure Access Service. Note that authentication is only part of the Secure Access Service security system. The access management framework determines access to the Secure Access Service and protected resources.

Secure Access Service supports:

- HTTP Redirect binding for sending AuthnRequests
- HTTP Redirect binding for sending/receiving SingleLogout requests/responses
- HTTP POST and HTTP Artifact bindings for receiving SAML responses

Before you begin:

- Check to see whether the SAML identity provider uses HTTP POST or HTTP Artifact bindings for SAML assertions.
- Check to see whether the SAML identity provider has published a SAML metadata file that defines its configuration. If the SAML identity provider metadata file is available, configuration is simpler and less prone to error.
- Complete the Secure Access Service system-wide SAML settings if you have not already done so. Select **System > Configuration > SAML > Settings**. For details, see [“Configuring Global SAML Settings” on page 243](#).
- Add metadata for the SAML identity provider to the metadata provider list if you have not already done so. Select **System > Configuration > SAML**. For details, see [“Managing SAML Metadata Files” on page 244](#).

The sign-in URL for which a session needs to be established for Secure Access Service as a service provider is identified by the RelayState parameter (HTTP URL parameter for artifact and HTML form parameter for POST.) In a service provider initiated case, Secure Access Service populates RelayState as an HTTP URL parameter while sending AuthnRequest. In the IdP-Initiated scenario (Secure Access Service is a service provider and there is a third-party IdP), the IdP must be configured to set the appropriate Sign-in URL of Secure Access Service in the RelayState parameter of the HTML form containing the SAML response. For more information, see the SAML 2.0 specification.

To configure the Secure Access Service as a SAML service provider:

1. In the admin console, select **Authentication > Auth. Servers**.
2. Select **SAML Server** from the New list and then click **New Server**.
3. Complete the settings as described in [Table 24 on page 247](#).
4. Save the configuration.

After you save changes for the first time, the page is redisplayed and now has two tabs. The Settings tab allows you to modify any of the settings pertaining to the SAML server instance. The Users tab lists valid users of the server.

Next steps:

- Configure the access management framework to use the SAML authentication server. Start with realm and role mapping rules. For details, see [“Creating an Authentication Realm” on page 306](#) and [“Specifying Role Mapping Rules for an Authentication Realm” on page 309](#).
- Configure a sign-in policy. When using a SAML authentication server, the sign-in policy can map to a single realm only. For details, see [“Defining a Sign-In Policy” on page 10](#).

Table 24: SAML Service Provider Profile

Setting	Description
Name	Specify a name to identify the server instance.
Settings	
SAML Version	Select 2.0 .
SA Entity Id	This value is prepopulated. It is generated by the system, based on the value for the Host FQDN for SAML setting on the System > Configuration > SAML > Settings page.
Configuration Mode	Select Manual or Metadata . If a metadata file or location is available from the SAML identity provider, use the metadata option to make configuration simpler and less prone to error. To upload or set the location for the published metadata file, select System > Configuration > SAML and click the New Metadata Provider button.
Identity Provider Entity ID	<p>The identity provider entity ID is sent as the Issuer value in the assertion generated by the SAML identity provider.</p> <p>If you use the metadata option, this setting can be completed by selecting the identity provider entity ID from the list. The list is populated by the identity provider entities defined in metadata files added to the System > Configuration > SAML page.</p> <p>If you complete this setting manually, specify the Issuer value in assertions generated by the SAML identity provider. Typically, you ask the SAML identity provider administrator for this setting.</p>
Identity Provider Single Sign On Service URL	<p>The identity provider SSO service URL is a URL provisioned by the SAML identity provider. The setting is required to support service-provider-initiated SSO. If missing, the Secure Access Service cannot successfully redirect the user request.</p> <p>If you use the metadata option, this setting can be completed by selecting the SSO service URL from the list. The list is populated by the identity provider entities defined in metadata files added to the System > Configuration > SAML page.</p> <p>If you complete this setting manually, ask the SAML identity provider administrator for this setting.</p>

Table 24: SAML Service Provider Profile (*continued*)

Setting	Description
User Name Template	<p>Specify how the Secure Access Service is to derive the username from the assertion. If the field is left blank, it uses the string received in the NameID field of the incoming assertion as the username.</p> <p>If you choose a certificate attribute with more than one value, the Secure Access Service uses the first matched value. For example, if you enter <certDN.OU> and the user has two values for the attribute (ou=management, ou=sales), the Secure Access Service uses "management". To use all values, add the SEP attribute to the variable. For example, if you enter <certDN.OUT SEP=":">, the Secure Access Service uses "management:sales". The attributes received in the attribute statement in the incoming assertion are saved under userAttr. These variables can also be used with angle brackets and plain text. If the username cannot be generated using the specified template, the login fails. If the NameID field of the incoming assertion is of type X509Nameformat, then the individual fields can be extracted using system variable "assertionNameDN".</p>
Allowed Clock Skew (minutes)	<p>Specify the maximum allowed difference in time between the Secure Access Service clock and the SAML identity provider server clock.</p> <p>NOTE: SAML is a time sensitive protocol. The time-based validity of a SAML assertion is determined by the SAML identity provider. If the SAML identity provider and SAML service provider clocks are askew, the assertion can be determined invalid, and you will receive the following error:</p> <p>"SAML Transferred failed. Please contact your system administrator. Detail: Failure: No valid assertion found in SAML response."</p> <p>We recommend you use NTP to ensure the clocks are synchronized and that you set an Allowed Clock Skew value that accommodates any expected or permissible skew.</p>
Support Single Logout	<p>Single logout is a mechanism provided by SAML for logging out a particular user from all the sessions created by the identity provider. Select this option if the Secure Access Service must receive and send a single logout request for the peer SAML identity provider.</p> <p>If you use the metadata option, the Single Logout Service URL setting can be completed by selecting the SLO service URL from the list. The list is populated by the identity provider entities defined in metadata files added to the System > Configuration > SAML page. The Secure Access Service sends Single Logout requests to this URL.</p> <p>In addition, if you use the metadata option, the Single Logout Response URL setting is completed based on your selection for Single Logout Service URL. If the identity provider has left this setting empty in its metadata file, the Secure Access Service sends the Single Logout response to the SLO service URL.</p> <p>If you complete these settings manually, ask the SAML identity provider administrator for guidance.</p>
SSO Method	

Table 24: SAML Service Provider Profile (*continued*)

Setting	Description
Artifact	<p>When configured to use the Artifact binding, the Secure Access Service contacts the Artifact Resolution Service (ARS) to fetch the assertion using SOAP protocol. If the ARS is hosted on a HTTPS URL, then the certificate presented by the ARS is verified by the Secure Access Service. For this verification to pass successfully, the CA of the server certificate issued to the identity provider ARS must be added to the trusted server CA on the Secure Access Service.</p> <p>Complete the following settings to configure SAML using the HTTP Artifact binding:</p> <ul style="list-style-type: none"> • Source ID. Enter the source ID for the identity provider ARS. Source ID is Base64-encoded, 20-byte identifier for the identity provider ARS. If left blank, this value is generated by the Secure Access Service. • Source Artifact Resolution Service URL. For metadata-based configuration, this field is completed automatically from the metadata file and is not configurable. For manual configurations, enter the URL of the service to which the SP ACS is to send ArtifactResolve requests. ArtifactResolve requests are used to fetch the assertion from the artifact received by it. • SOAP Client Authentication. Select HTTP Basic or SSL Client Certificate and complete the related settings. If you use an SSL client certificate, select a certificate from the Secure Access Service device certificate list. • Select Device Certificate for Signing. Select the device certificate the Secure Access Service uses to sign the AuthnRequest sent to the identity provider SSO service. If you do not select a certificate, the Secure Access Service does not sign AuthnRequest. • Select Device Certificate for Encryption. Select the device certificate the Secure Access Service uses to decrypt encrypted data received in the SAML response. The public key associated with the device certificate is used by the identity provider for encryption.
POST	<p>When configured to use the POST binding, the Secure Access Service uses a response signing certificate to verify the signature in the incoming response or assertion. The certificate file must be in PEM or DER format. The certificate you select should be the same certificate used by the identity provider to sign SAML responses.</p> <p>Complete the following settings to configure SAML using the HTTP POST binding:</p> <ul style="list-style-type: none"> • Response Signing Certificate. If you use the metadata-based configuration option, select a certificate from the list. The list is populated by the identity provider entities defined in metadata files added to the System > Configuration > SAML page. If you configure these settings manually, browse to and upload the certificate to be used to validate the signature in the incoming response or assertion. If no certificate is specified, the certificate embedded in the response is used. • Enable Signing Certificate status checking. Select this option to check the validity of the signing certificate before verifying the signature. This setting applies to any certificate used for signature verification. If this option is enabled, the response will be rejected if the certificate is revoked, expired, or untrusted. If this option is selected, the certificate CA must be added to the Secure Access Service Trusted Client CA store. If this option is not enabled then the certificate is used without any checks. • Select Device Certificate for Signing. Select the device certificate the Secure Access Service uses to sign the AuthnRequest sent to the identity provider SSO service. If you do not select a certificate, the Secure Access Service does not sign AuthnRequest. • Select Device Certificate for Encryption. Select the device certificate the Secure Access Service uses to decrypt encrypted data received in the SAML response. The public key associated with the device certificate is used by the identity provider for encryption.

Service Provider Metadata Settings

Table 24: SAML Service Provider Profile (*continued*)

Setting	Description
Metadata Validity	Enter the number of days the Secure Access metadata is valid. Valid values are 0 to 9999. 0 specifies the metadata does not expire.
Do Not Publish SA Metadata	Select this option if you do not want the Secure Access Service to publish the metadata at the location specified by the Secure Access Service Entity ID field.
Download Metadata	This button appears only after you have saved the authentication server configuration. Use this button to download the metadata of the current SAML service provider.
User Record Synchronization	
Enable User Record Synchronization	Allow users to retain their bookmarks and individual preferences regardless of which Secure Access Service device they log in to.
Logical Auth Server Name	Specify the server name if you have enabled user record synchronization.

Related Documentation

- [Understanding SAML 2.0 on page 233](#)
- [Secure Access Service SAML 2.0 Supported Features Reference on page 234](#)
- [Investigating a “No valid assertion found in SAML response” Error on page 275](#)

Configuring Secure Access Service as a SAML 2.0 Identity Provider

This topic describes how to configure the Secure Access Service as a SAML identity provider. It includes the following sections:

- [Configuration Overview on page 250](#)
- [Configuring Sign-in SAML Metadata Provider Settings on page 251](#)
- [Configuring Sign-in SAML Identity Provider Settings on page 251](#)
- [Configuring Peer SAML Service Provider Settings on page 255](#)
- [Configuring a SAML SSO Resource Policy for Gateway Mode Deployments on page 260](#)
- [Configuring a SAML SSO External Applications Policy on page 262](#)

Configuration Overview

Implementing Secure Access Service as a SAML identity provider includes the following basic steps.

1. Configure system-wide SAML settings. Select **System > Configuration > SAML > Settings**. See “[Configuring Global SAML Settings](#)” on page 243.
2. Add SAML metadata provider files. Select **System > Configuration > SAML**. See “[Managing SAML Metadata Files](#)” on page 244.
3. Configure Sign-In SAML metadata provider settings. See “[Configuring Sign-in SAML Metadata Provider Settings](#)” on page 251.

4. Configure Sign-In SAML identity provider settings. See [“Configuring Sign-in SAML Identity Provider Settings” on page 251](#).
5. Configure peer service provider settings. See [“Configuring Peer SAML Service Provider Settings” on page 255](#).
6. Configure a resource policy:
 - For gateway mode deployments, configure a SAML SSO resource policy. See [“Configuring a SAML SSO Resource Policy for Gateway Mode Deployments” on page 260](#).
 - For peer mode deployments, configure a SAML SSO external applications policy. See [“Configuring a SAML SSO External Applications Policy” on page 262](#).

Configuring Sign-in SAML Metadata Provider Settings

Sign-in SAML metadata provider settings determine how Secure Access Service identity provider metadata is published.

To configure the identity provider metadata publication settings:

1. In the admin console, select **Authentication > Signing In > Sign-In SAML > Metadata Provider**.
2. Complete the settings described in [Table 25 on page 251](#).
3. Click **Save Metadata Provider** to save your changes.

Table 25: Sign-in SAML Identity Provider Metadata Provider Settings

Setting	Description
Entity ID	This value is prepopulated. It is generated by the system, based on the value for the Host FQDN for SAML setting on the System > Configuration > SAML > Settings page.
Metadata Validity	Specify the maximum duration for which a peer SAML entity can cache the Secure Access Service SAML metadata file. Valid values are 1 to 9999. The default is 365 days.
Do Not Publish SA Metadata	Select this option if you do not want the Secure Access Service to publish the metadata at the location specified by the Secure Access Service Entity ID field. You can use this option to toggle off publication without deleting your settings.
Download Metadata	Use this button to download the Secure Access Service SAML identity provider metadata.

Configuring Sign-in SAML Identity Provider Settings

The settings defined in this procedure are the default settings for Secure Access Service SAML identity provider communication with all SAML service providers. If necessary, you can use the peer service provider configuration to override these settings for particular service providers.

To configure sign-in SAML identity provider settings:

1. In the admin console, select **Authentication > Signing In > Sign-In SAML > Identity Provider**.
2. Complete the settings described in [Table 26 on page 252](#).
3. Click **Save Changes**.

Table 26: Sign-in SAML Identity Provider Settings

Setting	Description
Basic Identity Provider (IdP) Configuration (Published in Metadata)	
Protocol Binding to use for SAML Response	Select POST , Artifact , or both, depending on your total requirements.
Signing Certificate	Select the certificate used to sign the SAML messages sent by the Secure Access Service. The certificates listed here are configured on the System > Configuration > Certificate > Device Certificates page.
Decryption Certificate	Select the certificate used to decrypt the SAML messages sent by peer service providers. The public key associated with this certificate is used by the peer service provider to encrypt SAML messages exchanged with this identity provider. The decryption certificate must be configured if the peer service provider encrypts the SAML messages sent to the Secure Access Service. The certificates listed here are configured on the System > Configuration > Certificate > Device Certificates page.
Other Configurations	<p>Reuse Existing NC (Pulse) Session. This feature applies to an service-provider-initiated SSO scenario—that is, when a user clicks a link to log into the service provider site. The service provider redirects the user to the identity provider SSO Service URL.</p> <p>If this option is selected, a user with an active NC/Pulse session is not prompted to authenticate. The Secure Access Service uses information from the existing session to form the SAML response.</p> <p>Accept unsigned AuthnRequest. In an service-provider-initiated SSO scenario, the SP sends an AuthnRequest to the identity provider. This AuthnRequest could be either signed or unsigned. If this option is unchecked, the Secure Access Service rejects unsigned AuthnRequests. Note that the Secure Access Service also rejects signed AuthnRequests if signature verification fails.</p>
Service-Provider-Related IdP Configuration	
Relay State	SAML RelayState attribute sent to the service provider in an identity-provider-initiated SSO scenario. If left blank, the RelayState value is the URL identifier of the resource being accessed.
Session Lifetime	<p>Suggest a maximum duration of the session at the service provider created as a result of the SAML SSO. Select one of the following options:</p> <ul style="list-style-type: none"> • None. The identity provider does not suggest a session duration. • Role Based. Suggest the value of the session lifetime configured for the user role. • Customized. If you select this option, the user interface displays a text box in which you specify a maximum in minutes.

Table 26: Sign-in SAML Identity Provider Settings (*continued*)

Setting	Description
Sign-In Policy	<p>Select the sign-in URL to which the user is redirected in an service-provider-initiated scenario. The list is populated by the sign-in pages configured on the Authentication > Signing In > Sign-in Policies page.</p> <p>Note: The user is not redirected if he or she already has a session with the Secure Access Service and had authenticated through this sign-in policy.</p>
Force Authentication Behavior	<p>In an service-provider-initiated scenario, the service provider sends an AuthnRequest to the identity provider. If the service provider AuthnRequest includes the ForceAuthn attribute set to true and the user has a valid Secure Access Service session, this setting determines how the identity provider responds. Select one of the following options:</p> <ul style="list-style-type: none"> • Reject AuthnRequest. Do not honor the SAML SSO request. • Re-Authenticate User. Invalidate the user session and prompt for reauthentication. <p>Note: This setting prevails over the Pulse session reuse setting.</p>
User Identity	<p>Subject Name Format. Format of the NameIdentifier field in the generated assertion. Select one of the following options:</p> <ul style="list-style-type: none"> • DN. Username in the format of DN(distinguished name). • Email address. Username in the format of an email address. • Windows. Username in the format of a Windows domain qualified username. • Other. Username in an unspecified format. <p>Subject Name. Template for generating the username that is sent as the value of the NameIdentifier field in the assertion.</p> <p>You may use any combination of available system or custom variables contained in angle brackets and plain text.</p>
Web Service Authentication	<p>These settings apply when the HTTP Artifact binding is used.</p> <p>Authentication Type. Method used to authenticate the service provider assertion consumer service to the identity provider on the Secure Access Service system. Select one of the following options:</p> <ul style="list-style-type: none"> • None. Do not authenticate the assertion consumer service. • Username/Password. If you select this option, use the controls to specify username and password settings. • Certificate. For certificate-based authentication, the Client CA of the service provider should be present in Secure Access Service system Trusted Client CA list (located on the System > Configuration > Certificates > Trusted Client CAs page).
Artifact configuration	<p>These settings apply when the HTTP Artifact binding is used.</p> <p>Source ID. This is the Base64-encoded, 20-byte identifier of the Artifact Resolution Service on the identity provider.</p> <p>Enable Artifact Response Signing and Encryption. If checked, the identity provider signs and encrypts the artifact response.</p>

Table 26: Sign-in SAML Identity Provider Settings (*continued*)

Setting	Description
Attribute statement configuration	<p>Attributes to be sent in SAML Attribute statements can be specified manually as name-value pairs, or you can configure an option to fetch name-value pairs from an LDAP server (or you can specify both manual entries and LDAP entries).</p> <hr/> <p>To specify name-value pairs, enter values in the following boxes and click Add:</p> <ul style="list-style-type: none"> • Attribute Name—An ASCII string. • Friendly Name—A more readable friendly name for the attribute. This is optional (an option included in the SAML standard). • Attribute Value—The attribute value can be specified as a hard-coded string, a custom variable, or a user attribute variable. System conventions for specifying user and custom tokens and variables apply. The value can be a combination of a string and a user or custom variable. For example: Email::<customVar.email>. The value can also be a combination of user and custom variables and hardcoded text. For example: mydata=<USER><REALM><customVar.email>. • Value Type—Select Single-Valued or Multi-Valued. A single-valued attribute can be a combination of a string and a user or custom variable. If there are multiple single-valued attributes configured with the same attribute names, they are combined and sent as a multi-valued attribute. Select Multi-Value if you want every individual token defined in the Attribute Value column to be sent as a separate AttributeValue. For example: <pre><element ref="saml:AttributeValue" minOccurs="0" maxOccurs="unbounded"/></pre> <p>If the Attribute value is given as <USER>mars<REALM>jupiter<ROLE> and the value type is marked as Multi-Valued, then the values sent as part of attribute statement are sent as follows:</p> <pre>Username Realmname Role</pre> <p>Note that only the tokens ['<>'] will be considered when processing a Multi-Valued attribute marked. The remaining data (for example mars, jupiter) is discarded. Specifying the token <ROLE> will send only one role. To send all roles, specify the Attribute value with the syntax <ROLE SEP=";">. If you specify <ROLE SEP=";"> as a single-valued attribute, it is sent as a single string with ";" separated roles. If you specify <ROLE SEP=";"> as a multi-valued attribute, each role is sent in a separate <AttributeValue> element.</p> <p>NOTE: Encryption is set at the assertion level. You cannot encrypt individual attributes.</p>

Table 26: Sign-in SAML Identity Provider Settings (*continued*)

Setting	Description
	<p>To fetch attribute name-value pairs from an LDAP server, complete the following settings:</p> <ul style="list-style-type: none"> • Directory Server—Select the LDAP server from the list. You must add the LDAP server to the Authentication > Auth. Servers list before it can be selected. • Username for lookup—Enter a username template for LDAP lookup. The default is the variable <USERNAME>. The <USERNAME> variable stands for the login credential the user entered when logging in. The value can contain contextual characters as well as variables for substitution. • Attribute Name—Type an LDAP attribute name, such as cn. The attribute name is fetched from the LDAP server and sent as SAML Attribute statements as part of a SAML assertion. • Friendly Name—A more readable friendly name for the attribute. This is optional (an option included in the SAML standard). <p>NOTE: With the LDAP option, the SAML IdP sends attributes in the form configured on the backend LDAP server. If the LDAP server returns an attribute value in multi-valued form, then the SAML attribute statement will also be in multi-valued form.</p>

Configuring Peer SAML Service Provider Settings

The peer service provider list defines the set of service providers configured to communicate with the Secure Access Service SAML identity provider. When you add a peer service provider to the list, you can customize the SAML identity provider settings used to communicate with the individual service provider. If the service provider provides a SAML metadata file, you can use it to simplify configuration, or you can complete more detailed manual steps. If available, we recommend you use metadata so that configuration is simpler and less prone to error.

To configure peer SAML service provider settings:

1. In the admin console, select **Authentication > Signing In > Sign-In SAML > Identity Provider**.
2. Under Peer Service Provider Configuration, create a list of service providers that are SAML peers to the Secure Access Service SAML identity provider. To add a service provider to the list, click **Add SP**.
3. Complete the settings described in [Table 27 on page 255](#).
4. Click **Save Changes**.

Table 27: Peer Service Provider Configuration

Setting	Description
Configuration Mode	Select Manual or Metadata .
Service Provider Configuration - Metadata	
Entity Id	If you use metadata, select the SAML entity ID of the service provider. This list contains all the service providers specified in all the metadata files added to the System > Configuration > SAML page.

Table 27: Peer Service Provider Configuration (*continued*)

Setting	Description
Select certificates manually	<p>When you use the metadata configuration, the Secure Access Service SAML identity provider iterates through all the signature verification certificates specified when verifying the incoming SAML messages coming from the service provider. Similarly, when encrypting the SAML messages going out, the Secure Access Service SAML identity provider encrypts the messages with the first valid encryption certificate encountered in the metadata.</p> <p>Select this option to override this default behavior and select certificates manually.</p>
Signature Verification Certificate	If you select the Select certificates manually option, select the certificate to be used by the identity provider to verify the signature of incoming SAML messages.
Encryption Certificate	If you select the Select certificates manually option, select the certificate to be used if the assertions sent by the identity provider must be encrypted.
Service Provider Configuration - Manual	
Entity Id	If you are completing a manual configuration, ask the SAML service provider administrator for this setting.
Assertion Consumer Service URL	SAML service provider URL that receives the assertion or artifact sent by the identity provider.
Protocol Binding supported by the Assertion Consumer Service at the SP	Select POST , Artifact , or both. This setting must be consistent with the SAML identity provider configuration.
Default Binding	<p>If both POST and Artifact bindings are supported, which is the default?</p> <ul style="list-style-type: none"> • Post • Artifact <p>This setting must be consistent with the SAML identity provider configuration.</p>
Signature Verification Certificate	Upload the certificate to be used by the identity provider to verify the signature of incoming SAML messages. If no certificate is specified, the certificate embedded in the incoming SAML message is used for signature verification.
Encryption Certificate	Upload the certificate to be used if the assertions sent by the identity provider must be encrypted. If not certificate is specified, the assertions sent by the identity provider are not encrypted.
Certificate Attribute Configuration for Artifact Resolution Service	<p>Optional. Specify attributes that must be present in the certificate presented to the Artifact Resolution Service (ARS) at the identity provider by the service provider assertion consumer service.</p> <p>This option appears only if the SAML service provider supports the HTTP Artifact binding, the Secure Access Service SAML identity provider has been configured to support the HTTP Artifact binding, and the Web service authentication type specified for the service provider is Certificate.</p>
Certificate Status Checking Configuration	
Enable signature verification certificate status checking	Select this option to enable revocation checks for the signing certificate. Uses the configuration on the System > Configuration > Certificates > Trusted Client CAs page.

Table 27: Peer Service Provider Configuration (*continued*)

Setting	Description
Enable encryption certificate status checking	Select this option to enable revocation checks for the encryption certificate. Uses the configuration on the System > Configuration > Certificates > Trusted Client CAs page.
Customize identity provider Behavior	
Override Default Configuration	Select this option to set custom behavior of the Secure Access Service SAML identity provider for this SP instance. If you select this option, the user interface displays the additional options listed next.
Reuse Existing NC (Pulse) Session	This option cannot be enabled here if it is not selected for the sign-in SAML identity provider default settings.
Accept unsigned AuthnRequest	Individual service providers can choose to accept unsigned AuthnRequest.
Relay State	SAML RelayState attribute sent to the service provider in an identity-provider-initiated SSO scenario. If left blank, the RelayState value is the URL identifier of the resource being accessed.
Session Lifetime	Suggest a maximum duration of the session at the service provider created as a result of the SAML SSO. Select one of the following options: <ul style="list-style-type: none"> • None. The identity provider does not suggest a session duration. • Role Based. Suggest the value of the session lifetime configured for the user role. • Customized. If you select this option, the user interface displays a text box in which you specify a maximum in minutes.
Sign-In Policy	Select the Sign-In URL to which the user is redirected in an service-provider-initiated scenario. The list is populated by the sign-in pages configured in Authentication > Signing In > Sign-in Policies. Note: The user is not redirected if he or she already has a session with the Secure Access Service and had authenticated through this sign-in policy.
Force Authentication Behavior	In an service-provider-initiated scenario, the service provider sends an AuthnRequest to the identity provider. If the service provider AuthnRequest includes the ForceAuthn attribute set to true and the user has a valid Secure Access Service session, this setting determines how the identity provider responds. Select one of the following options: <ul style="list-style-type: none"> • Reject AuthnRequest. Do not honor the SAML SSO request. • Re-Authenticate User. Invalidate the user session and prompt for reauthentication. Note: This setting prevails over the Pulse session reuse setting.

Table 27: Peer Service Provider Configuration (*continued*)

Setting	Description
User Identity	<p>Subject Name Format. Format of NameIdentifier field in generated Assertion. Select one of the following options:</p> <ul style="list-style-type: none"> • DN. Username in the format of DN (distinguished name). • Email address. Username in the format of an e-mail address. • Windows. Username in the format of a Windows domain qualified username. • Other. Username in an unspecified format. <hr/> <p>Subject Name. Template for generating the username that is sent as the value of the NameIdentifier field in the assertion.</p> <p>You may use any combination of available system or custom variables contained in angle brackets and plain text.</p>
Web Service Authentication	<p>These settings apply when the HTTP Artifact binding is used.</p> <p>Authentication Type. Method used to authenticate the service provider assertion consumer service to the identity provider on the Secure Access Service system. Select one of the following options:</p> <ul style="list-style-type: none"> • None. Do not authenticate the assertion consumer service. • Username/Password. Use the controls to specify username and password settings. • Certificate. For certificate-based authentication, the client CA of the service providers should be present in the Secure Access Service system trusted client CA list (located on the System > Configuration > Certificates > Trusted Client CAs page).
Artifact configuration	<p>These settings apply when the HTTP Artifact binding is used.</p> <hr/> <p>Source ID. This is the Base64-encoded, 20-byte identifier of the Artifact Resolution Service on the identity provider.</p> <hr/> <p>Enable Artifact Response Signing and Encryption. If checked, the identity provider signs and encrypts the Artifact response.</p>
Attribute statement configuration	<p>Select Send Attribute Statements if the SAML SP requires additional attributes to be sent with SAML assertions. If you enable this option, select one of the following configuration options:</p> <ul style="list-style-type: none"> • Use IdP Defined Attributes—Send attributes based on the default settings for Secure Access Service SAML identity provider communication with all SAML service providers. • Customize IdP Defined Attributes—Selectively configure the attributes that are sent for this particular peer SAML SP. If you select this option, configure the settings described next.

Table 27: Peer Service Provider Configuration (*continued*)

Setting	Description
	<p>Attributes to be sent in SAML Attribute statements can be specified manually as name-value pairs, or you can configure an option to fetch name-value pairs from an LDAP server (or you can specify both manual entries and LDAP entries).</p> <hr/> <p>To specify name-value pairs, enter values in the following boxes and click Add:</p> <ul style="list-style-type: none"> • Attribute Name—An ASCII string. • Friendly Name—A more readable friendly name for the attribute. This is optional (an option included in the SAML standard). • Attribute Value—The attribute value can be specified as a hard-coded string, a custom variable, or a user attribute variable. System conventions for specifying user and custom tokens and variables apply. The value can be a combination of a string and a user or custom variable. For example: Email::<customVar.email>. The value can also be a combination of user and custom variables and hardcoded text. For example: mydata=<USER><REALM><customVar.email>. • Value Type—Select Single-Valued or Multi-Valued. A single-valued attribute can be a combination of a string and a user or custom variable. If there are multiple single-valued attributes configured with the same attribute names, they are combined and sent as a multi-valued attribute. Select Multi-Value if you want every individual token defined in the Attribute Value column to be sent as a separate AttributeValue. For example: <pre data-bbox="553 1026 1365 1052"><element ref="saml:AttributeValue" minOccurs="0" maxOccurs="unbounded"/></pre> If the Attribute value is given as <USER>mars<REALM>jupiter<ROLE> and the value type is marked as Multi-Valued, then the values sent as part of attribute statement are sent as follows: <pre data-bbox="553 1140 678 1215">Username Realmname Role</pre> Note that only the tokens ['<>'] will be considered when processing a Multi-Valued attribute marked. The remaining data (for example mars, jupiter) is discarded. Specifying the token <ROLE> will send only one role. To send all roles, specify the Attribute value with the syntax <ROLE SEP=";">. If you specify <ROLE SEP=";"> as a single-valued attribute, it is sent as a single string with ";" separated roles. If you specify <ROLE SEP=";"> as a multi-valued attribute, each role is sent in a separate <AttributeValue> element. <p>NOTE: Encryption is set at the assertion level. You cannot encrypt individual attributes.</p>

Table 27: Peer Service Provider Configuration (*continued*)

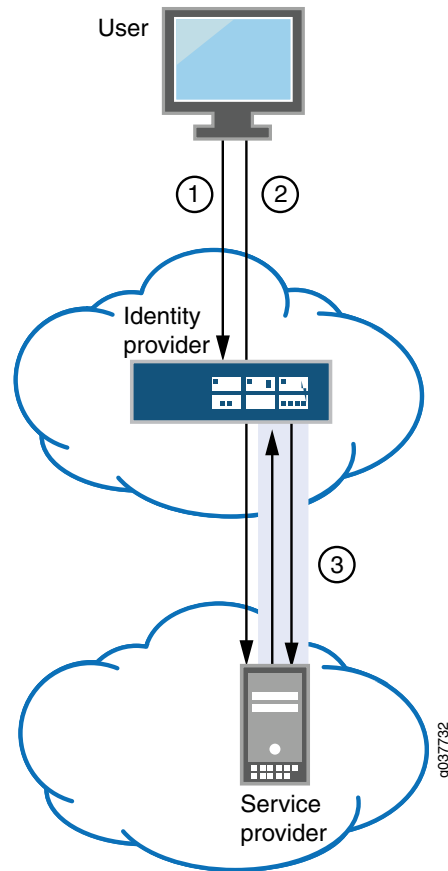
Setting	Description
	<p>To fetch attribute name-value pairs from an LDAP server, complete the following settings:</p> <ul style="list-style-type: none"> • Directory Server—Select the LDAP server from the list. You must add the LDAP server to the Authentication > Auth. Servers list before it can be selected. • Username for lookup—Enter a username template for LDAP lookup. The default is the variable <USERNAME>. The <USERNAME> variable stands for the login credential the user entered when logging in. The value can contain contextual characters as well as variables for substitution. • Attribute Name—Type an LDAP attribute name, such as cn. The attribute name is fetched from the LDAP server and sent as SAML Attribute statements as part of a SAML assertion. • Friendly Name—A more readable friendly name for the attribute. This is optional (an option included in the SAML standard). <p>NOTE: With the LDAP option, the SAML IdP sends attributes in the form configured on the backend LDAP server. If the LDAP server returns an attribute value in multi-valued form, then the SAML attribute statement will also be in multi-valued form.</p>

Configuring a SAML SSO Resource Policy for Gateway Mode Deployments

When deployed as a gateway in front of enterprise resources, the SAML SSO policy acts like other Secure Access Service resource policies. The Secure Access Service maintains the session and uses its rewriting or pass-through proxy features to render data to the user. You use a SAML SSO resource policy when the protected resource supports SAML SSO and has been configured as a SAML service provider. When deployed as a gateway, the SAML SSO communication is always identity-provider-initiated.

Figure 16 on page 261 illustrates a gateway mode deployment.

Figure 16: Secure Access Service as a SAML identity provider (Gateway Mode)



1 — A user logs into the Secure Access Service.

2 — The user requests a resource protected by a security system that supports SAML and has implemented a SAML service provider.

3 — The SAML identity provider initiates the SAML authentication request to the SAML service provider. Users are granted access to particular resources according to the Secure Access Service SAML SSO resource policy.

To configure a SAML SSO resource policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. Use the tabs to display the **SSO > SAML** page.

If your administrator view is not configured to show SAML policies, click the **Customize** button in the upper-right corner of the page and select the **SSO** and **SAML** check boxes.

3. Click **New Policy**.
4. Complete the settings described in [Table 28 on page 262](#).
5. Click **Save Changes**.

Table 28: SAML SSO Resource Policy Settings

Setting	Description
Name	Type a name for the policy.
Description	Type a description that would be meaningful to other administrators.
Resources	Specify the fully qualified domain name for the resources for which this policy applies. These are the resources protected at the SAML service provider.
Roles	Select one of the following options: <ul style="list-style-type: none"> • Policy applies to ALL roles. To apply this policy to all users • Policy applies to SELECTED roles. To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list. • Policy applies to all roles OTHER THAN those selected below. To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
Action	Select one of the following options: <ul style="list-style-type: none"> • Use the SAML SSO defined below. Typically, this is the setting you use for a SAML SSO resource policy. The Secure Access Service SAML identity provider makes the SSO request when a user tries to access a SAML resource specified in the Resources list. • Do NOT use SAML. Secure Access Service does not perform an SSO request. Use this if there is a problem with the SAML service provider and you want to allow access. • Use Detailed Rules. Use this option to configure advanced rules.
SAML SSO Details	SAML Version. Select 2.0 . <p>Service Provider Entity ID. Select the service provider entity ID. The service provider entity IDs listed here are configured on the Authentication > Signing In > Sign-in SAML > Identity Provider > Peer Service Provider pages.</p> <p>Cookie Domain. Enter a comma-separated list of domains to which Secure Access Service sends the SSO cookie.</p>



NOTE: The SAML SSO resource policy settings differ from Secure Access Service 7.1 to 7.2. Policies you created with Secure Access Service 7.1 are preserved in edit-only mode for legacy use.

Configuring a SAML SSO External Applications Policy

When deployed to support access to external resources (for example, public cloud resources), the Secure Access Service does not have to be a gateway to user access. The user can access the external resource directly, and the traffic does not flow through the Secure Access Service device. To enable SAML SSO in these deployments, you configure the Secure Access Service as a SAML identity provider to correspond with the external SAML service provider, and you configure an SSO SAML external applications policy to determine the users and resources to which the SAML SSO experience applies.

To configure a SAML External Apps resource policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. Use the tabs to display the **SSO > SAML External Apps** page.

If your administrator view is not configured to show SAML policies, click the **Customize** button in the upper-right corner of the page and select the **SSO** and **SAML** check boxes.

3. Click **New Policy**.
4. Complete the settings described in [Table 29 on page 263](#).
5. Click **Save Changes**.

Table 29: SAML SSO External Applications Policy Settings

Setting	Description
Name	Type a name for the policy.
Description	Type a description that would be meaningful to other administrators.
Resources	Specify the fully qualified domain name for the resources for which this policy applies. These are the resources protected at the SAML service provider.
Roles	Select one of the following options: <ul style="list-style-type: none"> • Policy applies to ALL roles. To apply this policy to all users. • Policy applies to SELECTED roles. To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list. • Policy applies to all roles OTHER THAN those selected below. To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
Action	Select one of the following actions: <ul style="list-style-type: none"> • Use the SAML SSO defined below. Typically, this is the setting you use for a SAML SSO resource policy. The Secure Access Service SAML identity provider makes the SSO request when a user tries to access to a SAML resource specified in the Resources list. • Do NOT use SAML. Secure Access Service does not perform an SSO request. Use this if there is a problem with the SAML service provider and you want to allow access. • Use Detailed Rules. Use this option to configure advanced rules.
SAML SSO Details	SAML Version. Select 2.0 . <hr/> Service Provider Entity ID. Select the service provider entity ID. The service provider entity IDs listed here are configured on the Authentication > Signing In > Sign-in SAML > Identity Provider > Peer Service Provider pages.

Related Documentation

- [Example: Implementing SAML 2.0 Web Browser SSO for Google Apps on page 266](#)

Configuring a SAML 2.0 ACL Web Policy

To configure the Secure Access Service as a policy enforcement point, you must create a SAML ACL web policy.

To configure a SAML ACL web policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. Use the tabs to display the Access > SAML ACL page.

If your administrator view is not configured to show SAML policies, click the Customize button in the upper-right corner of the page and select the **SAML ACL** check box.

3. On the SAML Access Control Policies page, click **New Policy**.
4. Complete the settings described in [Table 30 on page 264](#).
5. Click **Save Changes**.
6. On the SAML Access Control Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

Table 30: SAML ACL Web Policy Settings

Setting	Description
Name	Type a name for the policy.
Description	Type a description that would be meaningful to other administrators.
Resources	Specify the fully qualified domain name for the resources for which this policy applies. These are the resources protected at the SAML service provider.
Roles	Select one of the following options: <ul style="list-style-type: none"> • Policy applies to ALL roles. To apply this policy to all users. • Policy applies to SELECTED roles. To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list. • Policy applies to all roles OTHER THAN those selected below. To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
Action	Select one of the following options: <ul style="list-style-type: none"> • Use the SAML Access Control checks defined below. Secure Access Service performs an access control check to the specified URL using the data specified in the SAML Access Control Details section. • Do not use SAML Access. The Secure Access Service does not perform an access control check. • Use Detailed Rules. Use this option to configure advanced rules.

Table 30: SAML ACL Web Policy Settings (*continued*)

Setting	Description
SAML Access Control Details	<p>SAML Version. Select 2.0.</p> <hr/> <p>Configuration Mode. If you select manual, complete the SAML Access Control details. If you select Metadata, select the policy decision point to use.</p> <p>If the metadata option is disabled, you have not defined or uploaded a metadata file on the System > Configuration > SAML page.</p> <hr/> <p>SAML Web Service URL. Completed automatically if using metadata. If you configure manually, enter the URL of the access management system SAML server. For example, enter https://hostname/ws.</p> <hr/> <p>SAML Web Service Issuer. Enter the hostname of the issuer, typically the hostname of the access management system.</p> <p>NOTE: You must enter unique string that the SAML Web service uses to identify itself in authorization assertions.</p>
Authentication Type	<p>Select one of the following options:</p> <ul style="list-style-type: none"> • None—Do not authenticate the Secure Access Service. • Username—Authenticate using a username and password. Enter the username and password that the Secure Access Service must send the Web service. • Certificate Attribute—Authenticate using a certificate signed by a trusted certificate authority. If you have more than one certificate installed on the Secure Access Service, use the drop-down list to select which certificate to send to the Web service.
User Identity	<p>Subject Name Type—Specify which method the Secure Access Service and SAML Web service should use to identify the user. Select one the following options:</p> <ul style="list-style-type: none"> • DN—Send the username in the format of a DN (distinguished name) attribute. • Email Address—Send the username in the format of an e-mail address. • Windows—Send the username in the format of a Windows domain qualified username. • Other—Send the username in another format agreed upon by the Secure Access Service and the SAML Web service. <hr/> <p>Subject Name—Use variables to specify the username to the SAML Web service. Or, enter static text.</p> <p>NOTE: You must send a username or attribute that the SAML Web service will recognize.</p> <hr/> <p>Device Issuer—Enter a name that uniquely identifies the SAML authority, such as the device hostname.</p>
Maximum Cache Time	<p>You can eliminate the overhead of generating an authorization decision each time the user requests the same URL by indicating that the Secure Access Service must cache the access management system's authorization responses. Enter the amount of time the Secure Access Service should cache the responses (in seconds).</p>

Table 30: SAML ACL Web Policy Settings (*continued*)

Setting	Description
Ignore Query Data	By default, when a user requests a resource, the Secure Access Service sends the entire URL for that resource (including the query parameter) to the SAML Web service and caches the URL. You can specify that the Secure Access Service should remove the query string from the URL before requesting authorization or caching the authorization response.

- Related Documentation**
- [Understanding SAML 2.0 on page 233](#)
 - [Secure Access Service SAML 2.0 Supported Features Reference on page 234](#)

Example: Implementing SAML 2.0 Web Browser SSO for Google Apps

This example shows how to implement SAML 2.0 Web browser SSO for Google Apps. It includes the following sections:

- [Topology on page 266](#)
- [Configuring the Google Apps SAML service provider on page 268](#)
- [Configuring the Secure Access Service SAML Identity Provider on page 270](#)
- [Verifying the Google Apps SAML SSO Deployment on page 274](#)

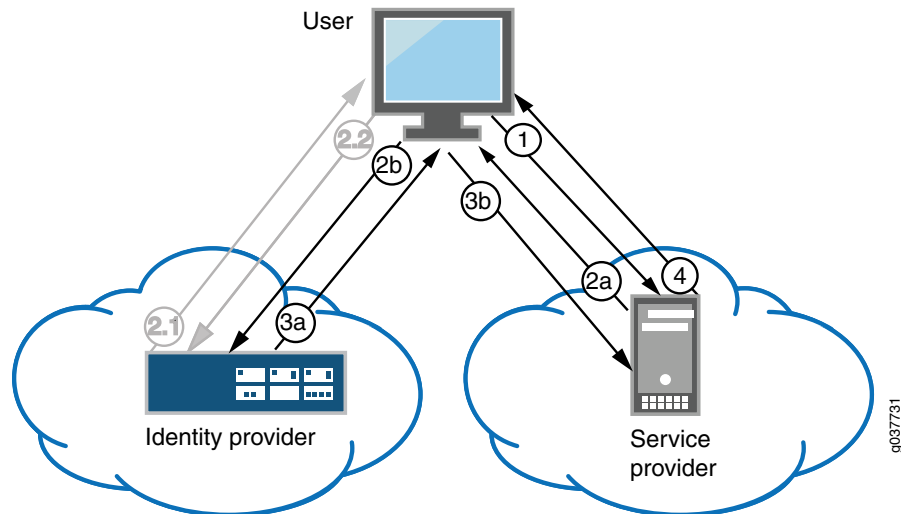
Topology

When deployed to support access to external resources (for example, public cloud resources), the Secure Access Service does not have to be a gateway to user access. The user can access the external resource directly, and the traffic does not flow through the Secure Access Service device. You configure the Secure Access Service as a SAML identity provider to correspond with the external SAML service provider, and you configure a SAML SSO external applications policy to determine the users and resources to which the SAML SSO experience applies.

When you configure the SAML identity provider, some settings are necessary to support either identity-provider-initiated or service-provider-initiated SSO. The documentation for the configuration steps makes note of these settings. Regardless, you configure the SAML identity provider to support both identity-provider-initiated and service-provider-initiated SSO.

[Figure 17 on page 267](#) illustrates the flow of network communication in a service-provider-initiated SSO scenario.

Figure 17: Secure Access Service as a SAML Identity Provider (Peer Mode) in a Service-Provider-Initiated SSO Scenario



1 – The user clicks a link to access a resource.

2a – The service provider sends an HTTP redirect status code (HTTP 302) to the user. The SAML request and all other SAML details are sent as URL parameters in the URL Location header.

2b – The user sends an HTTP GET request to the identity provider. The SAML request and all other SAML details are sent as URL parameters.

If the user already has a session with the identity provider, steps 2.1 and 2.2 are skipped.

2.1 – If the user does not have a session, the identity provider sends an authentication challenge to the user.

2.2 – The user enters sign-in credentials.

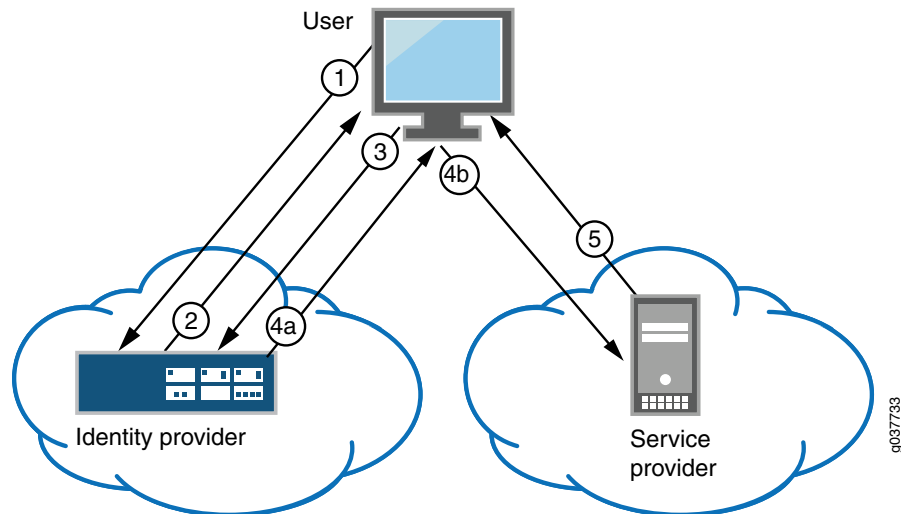
3a – The identity provider sends a successful status code (HTTP 200 OK) to the user with a form in the HTML body.

3b – The user sends the form to the service provider.

4 – The external resource is delivered to the user's browser.

Figure 18 on page 268 illustrates the flow of network communication in an identity-provider-initiated SSO scenario.

Figure 18: Secure Access Service as a SAML Identity Provider (Peer Mode) in an Identity-Provider-Initiated SSO Scenario



1 – The user authenticates to the identity provider.

2 – The identity provider returns a portal page with links to external resources.

3 – The user clicks a link for an external resource.

4a – The identity provider sends a successful status code (HTTP 200 OK) to the user with a form in the HTML body.

4b – The user sends the form to the service provider.

5 – The external resource is delivered to the user's browser.

Configuring the Google Apps SAML service provider

To configure the Google Apps SAML service provider:

1. Log into the Google Apps control panel. The URL is similar to the following:
<https://www.google.com/a/cpanel/acmegizmo.com>.
2. Click **Advanced Tools** in the menu bar.
3. Click the **Set up single sign-on (SSO)** link to display its configuration page, as shown in Figure 19 on page 269.
4. Configure the SAML service provider settings as described in Table 31 on page 269.
5. Click **Save Changes**.

Figure 19: Google Apps Advanced Tools: SSO

Dashboard
Organization & users
Groups
Domain settings
Reports
Advanced tools
Setup
Support
Settings
Help

Your settings have been saved.

[← Back to Advanced tools](#)

Set up single sign-on (SSO)

To set up SSO, please provide the information below. [SSO Reference](#)

Enable Single Sign-on

Sign-in page URL *
 URL for signing in to your system and Google Apps

Sign-out page URL *
 URL to redirect users to when they sign out

Change password URL *
 URL to let users change their password in your system; when defined here, this URL is shown even when Single Sign-on is not enabled

Verification certificate *
 A certificate file has been uploaded-[Replace certificate](#)

The certificate file must contain the public key for Google to verify sign-in requests. [Learn more](#)

Use a domain specific issuer

This must be checked if your domain uses an IDP Aggregator to handle SAML requests.
 If enabled, the issuer value sent in the SAML request will be **google.com/a/saml-ss0-example.com** instead of simply **google.com** [Learn more](#)

Network masks

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network.
 Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16)
 For ranges, use a dash. Example: (64.233.167-204.99/32)
 All network masks must end with a CIDR. [Learn more](#)

Table 31: Google Apps SSO Configuration

Setting	Description
Enable Single Sign-on	Select this option.
Sign-in page URL	Type the URL of the Secure Access Service SAML SSO service. The URL formed with the primary host FQDN for SAML has the following form: <pre style="color: #0070c0;">https://SAMLHostName/dana-na/auth/saml-ss0.cgi</pre> For example: <pre style="color: #0070c0;">https://i5.lab.juniper.net/dana-na/auth/saml-ss0.cgi</pre> The URL formed with the alternate host FQDN for SAML (to support Pulse/NC session detection) has the following form: <pre style="color: #0070c0;">https://i5pulse.lab.juniper.net/dana-na/auth/saml-ss0.cgi</pre>

Table 31: Google Apps SSO Configuration (*continued*)

Setting	Description
Sign-out page URL	<p>We recommend using the URL for the sign-in page for the realm associated with the Secure Access Service SAML identity provider. Users who already have a session will be directed to the sign-in page and can decide whether to log out from the Secure Access Service or not. The default sign-in URL has the form:</p> <p>https://FQDN</p> <p>For example:</p> <p>https://i5.lab.juniper.net/</p>
Change password URL	<p>We recommend using the URL for the sign-in page for the realm associated with the Secure Access Service SAML identity provider. Secure Access Service provides password management capabilities for some back-end auth servers (such as AD, LDAP, or Local Auth). When implemented, the password management capabilities are accessed from the sign-in page. The default sign-in URL has the form:</p> <p>https://FQDN</p> <p>For example:</p> <p>https://i5.lab.juniper.net/</p>
Verification certificate	<p>Click Browse and select the Secure Access Service device certificate. Then click Upload and ensure that the certificate is saved.</p>
Use a domain specific issuer	<p>Select this option.</p>
Network masks	<p>Do not select.</p>

Configuring the Secure Access Service SAML Identity Provider

You configure the Secure Access Service SAML identity provider settings to match the Google Apps SAML service provider settings.

To configure Secure Access Service SAM identity provider settings:

1. In the admin console, select **System > Configuration > SAML > Settings** to complete the global SAML settings. These settings apply to all of your SAML deployments.

[Figure 20 on page 271](#) shows an example of SAML global settings.

Figure 20: SAML Global Settings

SAML >
Settings

Metadata Server Configuration

Timeout value for metadata fetch request: seconds

Validity of uploaded/downloaded metadata file: days

Host FQDN for SAML:

Alternate Host FQDN for SAML:

Save changes?

2. Select **Authentication > Signing In > Sign-In SAML > Identity Provider** to configure SAML identity provider settings. These settings apply to all of your deployments where the Secure Access Service is a SAML identity provider. [Figure 21 on page 272](#) shows an example of SAML identity provider settings.

Figure 21: SAML Identity Provider Settings

Signing In

Sign-in Policies | Sign-in Pages | Sign-in Notifications | **Sign-in SAML**

Metadata Provider | **Identity Provider**

Basic Identity Provider (IdP) Configuration (Published in Metadata)

Protocol Binding to use for SAML Response

Post

Artifact

* Signing Certificate: Certificate to use for signing SAML n

Decryption Certificate: Certificate to use for decrypting the Provider (SP). This certificate is use

Other Configurations

Reuse Existing NC (Pulse) Session If enabled, the user's existing NC (P scenario, instead of authenticating th

Accept unsigned AuthnRequest Individual SPs can choose to accept

Service-Provider-related IdP Configuration

The following settings apply to all Service Providers by default. Can be overridden in Per

Relay State: 'RelayState' sent to SP in IdP-initiat resource being accessed is sent as '

* Session Lifetime: None Suggested maximum duration of the

Role Based

Customize

* SignIn Policy: The SignIn Policy used by this IdP to

* Force Authentication Behavior: Reject AuthnRequest SA behavior if SP sends an authentic browser session. Prevails over Pulse

Re-Authenticate User

User Identity

* Subject Name Format: Format of 'NameIdentifier' field in ge

* Subject Name: Template for generating user's identi

Save IdP configuration?

3. On the SAML Sign-In Identity Provider page, click **Add SP** and complete the settings for communication with Google Apps. Google Apps does not publish metadata, so the configuration is manually configured. The Google SAML service provider uses the HTTP POST binding and takes usernames in e-mail address format. [Figure 22 on page 273](#) shows an example of SP settings for Google Apps.

Figure 22: Peer SP Settings

Signing In >
New Peer Service Provider

* Configuration Mode: Manual Metadata If metadata is selected, uses metadata files uploaded by [Providers](#).

Service Provider Configuration

* Entity Id: Unique SAML Identifier of the SP.

* Assertion Consumer Service URL: URL of the service on SP that receives assertions.

Protocol Binding supported by the Assertion Consumer Service at the SP.

Post
 Artifact

* Default Binding: Post Artifact

Signature Verification Certificate: This certificate is used by IdP to verify outgoing Messages. If no certificate is specified incoming message is used to verify the message.

Issued To:
Issued By:
Valid:
Details: [Other Certificate Details](#)

Upload Certificate:

Encryption Certificate: The certificate to use if the the assertion is encrypted.

Issued To:
Issued By:
Valid:
Details: [Other Certificate Details](#)

Upload Certificate:

Certificate Status Checking Configuration

Enable signature verification certificate status checking Check this to enable revocation checks for the signature verification certificates of [Trusted Client CAs](#).

Enable encryption certificate status checking Check this to enable revocation checks for the encryption certificates of [Trusted Client CAs](#).

Customize IdP Behavior

Override Default Configuration

Reuse Existing NC (Pulse) Session If enabled, the user's existing NC (Pulse) session if any will be used instead of authenticating the user again.

Accept unsigned AuthnRequest

Relay State: 'RelayState' sent to SP in IdP-initiated SSO scenario. If left blank, the relay state being accessed is sent as 'RelayState'.

* Session Lifetime: None Role Based Customize Suggested maximum duration of the session at the SP created by this IdP.

* SignIn Policy: The SignIn Policy used by this IdP to authenticate the user.

* Force Authentication Behavior: Reject AuthnRequest Re-Authenticate User SA behavior if SP sends an authentication request with Force Authentication requested. Prevails over Pulse session re-use setting.

User Identity

* Subject Name Format: Format of 'NameIdentifier' field in generated Assertion.

* Subject Name: Template for generating user's identity as sent in 'NameIdentifier' field in generated Assertion.

Save SP configuration?

4. Select **Users > Resource Policies > Web > SSO > SAML SSO External Apps** and complete settings for the external applications policy that controls the users and the resources that can use the SSO implementation. [Figure 23 on page 274](#) shows an example of an SAML SSO external applications policy for Google Apps.

Figure 23: External Applications Policy Settings

New Policy

* Name: Required: Label to
 Description:

Resources

Specify the resources for which this policy applies, one per line. In order for you qualified domain name in your resource.

* Resources:
 Examples:
 http://*.domain.com/pub
 https://www.domain.com:
 10.10.10.10/255.255.2
 10.10.10.10/24:8000-5

Roles

Policy applies to ALL roles
 Policy applies to SELECTED roles
 Policy applies to all roles OTHER THAN those selected below

Available roles:

 Add->
Remove

Selected roles:

Action

Use the SAML SSO defined below
 Do not use SAML
 Use Detailed Rules (available after you click 'Save Changes')

SAML SSO Details

* SAML Version: 1.1 2.0

* Service Provider Entity ID:

Save changes?

Verifying the Google Apps SAML SSO Deployment

Access a Google Docs or Google Apps resource as a non-admin user to verify the solution works as expected.



TIP: Use a browser plugin such as HTTP Watch if you want to trace the SAML communication between the SAML service provider and SAML identity provider.

To verify service-provider-initiated SSO:

1. Make sure you are not logged into the Secure Access Service or Google.
2. Open a Web browser and open a location on Google Docs or Google Apps. Google Apps redirects you to the Secure Access Service sign-in page to authenticate.
3. Log in.

The Secure Access Service redirects you to the Google Docs or Google Apps location you had requested.

To verify Pulse/NC session detection for service-provider-initiated SSO:

1. Make sure you are not logged into the Secure Access Service or Google.
2. Use Pulse or VPN tunneling client to create an SSL VPN connection.
3. Open a Web browser and open a location on Google Docs or Google Apps.

You should not have to authenticate to access the Google Docs or Google Apps location.

To verify identity-provider-initiated SSO:

1. Use the Secure Access Service admin console to create a bookmark to a location on Google Docs or Google Apps.
2. As a user, log in to the Secure Access Service.
3. Click the bookmark link to the Google Docs or Google Apps location.

You should not have to authenticate to access the Google Docs or Google Apps location.

Related Documentation

- [Google Code: SAML Single Sign-on \(SSO\) Service for Google Apps](#)
- [Google Support: SSO \(Single Sign-on\)](#)
- [Configuring Secure Access Service as a SAML 2.0 Identity Provider on page 250](#)

Investigating a “No valid assertion found in SAML response” Error

Problem SAML is a time sensitive protocol. The time-based validity of a SAML assertion is determined by the SAML identity provider. If the SAML identity provider and SAML service provider clocks are askew, the assertion can be determined invalid, and authentication fails.

In the scenario described here, the Secure Access Service is deployed as a SAML service provider in a SAML 2.0 deployment.

In this scenario, the following error is returned to the user after the user has submitted credentials to the SAML identity provider:

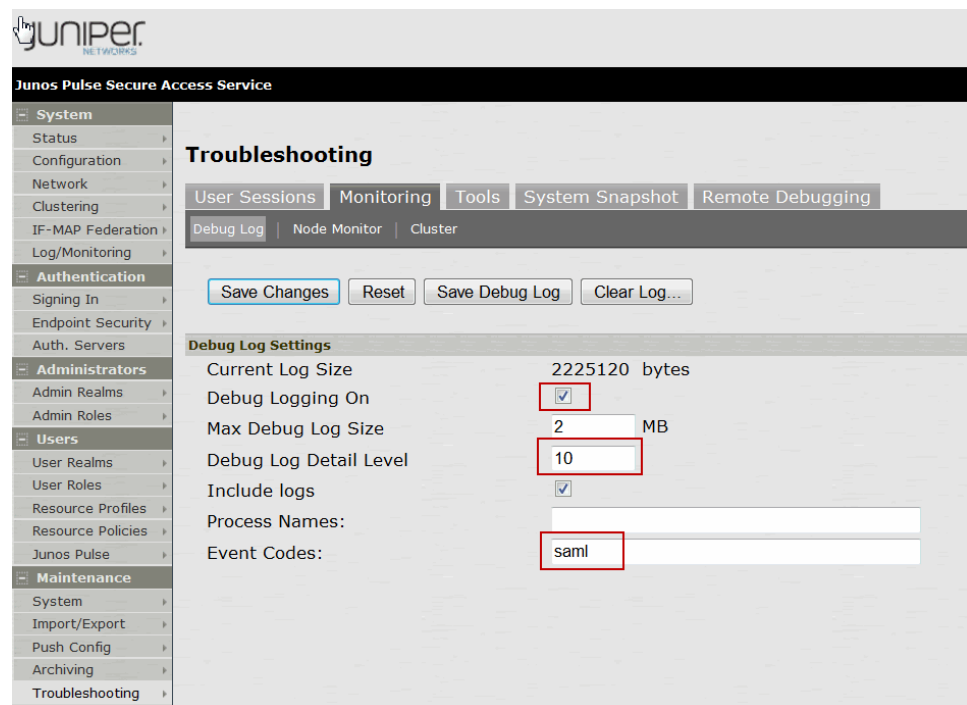
"SAML Transferred failed. Please contact your system administrator.

Detail: Failure: No valid assertion found in SAML response."

Cause To investigate the error:

1. Select **Maintenance > Troubleshooting > Monitoring > Debug Logs** to display the Debug Log configuration page, shown in [Figure 24 on page 276](#).

Figure 24: Debug Log Page



2. Turn debug logging on, set Debug Log Detail Level to **10**, and Event Codes to **saml**.
3. Reproduce the action that results in the error—in this case, user access to the resource associated with the SAML service provider that prompts the user to submit credentials to the SAML identity provider.
4. Click **Save Debug Log**.
The console displays the Save As dialog box.
5. Save the file to a location your local host or a location that you can access when sending mail. The file is an encrypted file, so do not try to open it and analyze it yourself.
6. Email the debug log to JTAC.

JTAC will use the file to diagnose the issue. In the debug log, the following log lines indicate issues with the time-based validity of the assertion:

```
verifySubjectConfirmationData: assertion has expired
```



```
processConditions: assertion has expired [NotOnOrAfter condition failed]
processConditions: assertion is not yet Valid [NotBefore condition failed]
```

These log lines indicate a clock sync issue only if failure of the time-based validity check is unexpected. The same log lines might appear in the debug log to indicate an assertion has expired as expected.

Solution We recommend you use NTP to ensure the clocks are synchronized and that you set an Allowed Clock Skew value that accommodates any expected or permissible skew. Properly synchronized clocks avoid unexpected failure.

To configure NTP:

1. Select **System > Status** to display the System Status page, shown in [Figure 25 on page 278](#).
2. Next to System Date & Time, click **Edit** to display the Date and Time page, shown in [Figure 26 on page 279](#).
3. Specify the settings for the same NTP server used by the SAML identity provider.
4. Save your configuration.

Figure 25: System Status Page

JUNIPER NETWORKS

Junos Pulse Secure Access Service

- System
 - Status
 - Configuration
 - Network
 - Clustering
 - IF-MAP Federation
 - Log/Monitoring
- Authentication
 - Signing In
 - Endpoint Security
 - Auth. Servers
- Administrators
 - Admin Realms
 - Admin Roles
- Users
 - User Realms
 - User Roles
 - Resource Profiles
 - Resource Policies
 - Junos Pulse
- Maintenance
 - System
 - Import/Export
 - Push Config
 - Archiving

System Status

Overview | Active Users | Maintenance

Critical Events

Page Settings

System Version
7.4R1:Internal (build 23292)
[Download Package](#)

Uptime
18 days, 4 hours,
58 minutes, 3 seconds

Last Config Update
Thu Jan 24 14:26:32 2013

System Date & Time [Edit](#)
2013-01-28
02:24:15 PM

Logging Disk: 0% Full

Max Licensed Users: 1000

Signed-In Users: 1

Figure 26: Date and Time Page

The screenshot shows the Juniper Pulse Secure Access Service configuration interface. The left sidebar contains a navigation menu with categories: System, Authentication, Administrators, Users, and Maintenance. The main content area is titled "Date and Time" and displays the following information:

- Status >**
- Date and Time**
- System Date: 1/28/2013
- System Time: 2:23:16 PM
- Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana

Under the "Time Source" section, the "Use NTP Server" option is selected. The configuration fields are:

- NTP Server: time.nist.gov
- Key: (optional)
- Secondary NTP Server: (optional)
- Key: (optional)
- Update Interval: 60 minutes (min: 1)

The "Set Time Manually" option is unselected. The manual settings are:

- Date: (mm/dd/yyyy)
- Time: (hh:mm:ss) AM

Buttons include "Get from Browser" and "Save Changes?". A "Save Changes?" section is also present at the bottom.

To set the Allowed Clock Skew value:

1. Select **Authentication > Auth. Servers**.
2. Select the SAML authentication server you want to configure to display its configuration page. A sample page is shown in [Figure 27 on page 280](#).
3. Specify a number of minutes in the **Allowed Clock Skew** to accommodate any expected or permissible skew.
4. Save your configuration.

Figure 27: SAML Service Provider Configuration Page

The screenshot shows the Junos Pulse Secure Access Service Administration interface. The left sidebar contains a navigation menu with categories like System, Authentication, Administrators, Users, and Maintenance. The main content area is titled 'New SAML Server' and includes a 'Server Name' field, a 'Settings' section with radio buttons for SAML Version (1.1 and 2.0), SA Entity Id, Configuration Mode (Manual and Metadata), Identity Provider Entity Id, Identity Provider Single Sign On Service URL, and User Name Template. A red box highlights the 'Allowed Clock Skew (minutes)' field. Below this field is a checkbox for 'Support Single Logout'. A small text box provides an example for the User Name Template: 'Example: <assertionNameDN.uid>, uid from X509Subject The entire assertion name identifier if not specified; Or <userAttr.attr>, attr from AttributeStatement attributes.'

Related Documentation

- [Archiving Debug Logs on page 892](#)
- [Configuring the System Date and Time on page 954](#)
- [Configuring Secure Access Service as a SAML 2.0 Service Provider on page 246](#)

Junos Pulse Secure Access Service SAML 1.1 Support

The trend in SAML deployments is converging on the SAML 2.0 specification. Junos Pulse Secure Access Service Release 7.2 continues to support SAML 1.1. The following sections reprint previous information we have provided about SAML 1.1 deployments:

- [About SAML Version 1.1 on page 280](#)
- [Secure Access Service SAML Version 1.1 Configuration Tasks on page 292](#)

About SAML Version 1.1

The following topics provide background information about SAML version 1.1:

- [Understanding SAML 1.1 on page 281](#)
- [Understanding SAML 1.1 Profiles on page 283](#)
- [Understanding SAML 1.1 Assertions on page 286](#)
- [Creating a Trust Relationship Between SAML 1.1 Systems on page 288](#)

Understanding SAML 1.1

The Secure Access Service enables you to pass user and session state information between the Secure Access Service and another trusted access management system that supports the Security Assertion Markup Language (SAML). SAML provides a mechanism for two disparate systems to create and exchange authentication and authorization information using an XML framework, minimizing the need for users to re-enter their credentials when accessing multiple applications or domains.

SAML exchanges are dependent upon a trusted relationship between two systems or domains. In the exchanges, one system acts as a SAML authority (also called an asserting party or SAML responder) that asserts information about the user. The other system acts as a relying party (also called a SAML receiver) that relies on the statement (also called an assertion) provided by the SAML authority. If it chooses to trust the SAML authority, the relying party authenticates or authorizes the user based on the information provided by the SAML authority.

The Secure Access Service supports two SAML use case scenarios:

- The Secure Access Service as the SAML authority—The user signs into a resource by way of the Secure Access Service first, and all other systems are SAML receivers, relying on the Secure Access Service for authentication and authorization of the user. Under this scenario, the Secure Access Service can use either an artifact profile or a POST profile.
- The Secure Access Service as the SAML receiver—The user signs into another system on the network first, and the Secure Access Service is the SAML receiver, relying on the other system for authentication and authorization of the user.

For example, in the first scenario, an authenticated Secure Access Service user named John Smith may try to access a resource protected by an access management system. When he does, the Secure Access Service acts as a SAML authority and declares “This user is John Smith. He was authenticated using a password mechanism.” The access management system (the relying party) receives this statement and chooses to trust the Secure Access Service (and therefore trust that the Secure Access Service has properly identified the user). The access management system may still choose to deny the user access to the requested resource (for instance, because John Smith has insufficient access privileges on the system), while trusting the information sent by the Secure Access Service.

In the second scenario, John Smith signs in to his company portal and is authenticated using an LDAP server sitting behind the company’s firewall. On the company’s secure portal, John Smith clicks a link to a resource protected by the Secure Access Service. The following process occurs:

1. The link redirects John Smith to an intersite transfer service on the company portal, which constructs an artifact URL. The artifact URL contains a reference to a SAML assertion stored in the company portal’s cache.
2. The portal sends the URL to the Secure Access Service, which can decide whether or not to link to the reference.

3. If the Secure Access Service links to the reference, the portal sends a SOAP message containing the SAML assertion (an XML message containing the user's credentials) to the Secure Access Service, which can then decide whether or not to allow the user access to the requested resource.



NOTE: SOAP requests generated by the Secure Access Service (when configured as a SAML 1.1 consumer) are not signed.

4. If the Secure Access Service allows the user access, the Secure Access Service presents to the user the requested resource.
5. If the Secure Access Service rejects the SAML assertion, or the user credentials, the Secure Access Service responds to the user with an error message.

When configuring the Secure Access Service, you can use SAML for:

- **Single sign-on (SSO) authentication**—In a SAML SSO transaction, an authenticated user is seamlessly signed into another system without resubmitting his credentials. In this type of transaction, the Secure Access Service can be either the SAML authority or the SAML receiver. When acting as the SAML authority, the Secure Access Service makes an authentication statement, which declares the user's username and how he was authenticated. If the relying party (called an assertion consumer service in SAML SSO transactions) chooses to trust the Secure Access Service, the user is seamlessly signed into the assertion consumer service using the username contained in the statement.

When acting as the SAML receiver, the Secure Access Service requests credential confirmation from the SAML authority, which is the other access management system, such as LDAP or another authentication server. The SAML authority sends an assertion by way of a SOAP message. The assertion is a set of XML statements that the Secure Access Service must interpret, based on criteria that the Secure Access Service administrator has specified in a SAML server instance definition. If the Secure Access Service chooses to trust the asserting party, the Secure Access Service allows the user to sign in seamlessly using the credentials contained in the SAML assertion.

- **Access control authorization**—In a SAML access control transaction, the Secure Access Service asks an access management system whether the user has access. In this type of transaction, the Secure Access Service is the relying party (also called a policy enforcement point in access control transactions). It consumes and enforces an authorization decision statement provided by the access management system (SAML authority), which declares what the user is allowed to access. If the SAML authority (also called a policy decision point in access control transactions) declares that the Secure Access Service user has sufficient access privileges, the user may access the requested resource

The Secure Access Service does not generate authorization decision statements—it only consumes them.

In addition to providing users access to a URL based on the authorization decision statement returned by a SAML authority, the Secure Access Service also allows you to define users' access rights to a URL using Secure Access Service-only mechanisms

(Users > Resource Profiles > Web Applications/Pages tab). If you define access controls through the Secure Access Service as well as through a SAML authority, both sources must grant access to a URL for a user to access it. For example, you may configure a Secure Access Service access policy that denies members of the “Users” role access to www.google.com, but configure another SAML policy that bases a user’s access rights on an attribute in an access management system. Even if the access management system permits users access to www.google.com, users are still denied access based on the Secure Access Service access policy.

When asked if a user may access a resource, access management systems that support SAML may return a response of permit, deny, or indeterminate. If the Secure Access Service receives an indeterminate response, it denies the user access.

The session timeouts on the Secure Access Service and your access management system may not coordinate with one another. If a user’s access management system session cookie times out before his Secure Access Service destination signaling identifier (DSID) cookie times out, then single sign-on between the two systems is lost. The user is forced to sign in again when he times out of the access management system.

**Related
Documentation**

- [Configuring SAML 1.1 SSO Profiles on page 294](#)

Understanding SAML 1.1 Profiles

The Secure Access Service accepts authentication assertions generated by a SAML authority using either an artifact profile or a POST profile. This feature allows a user to sign in to a source site or portal without going through the Secure Access Service first, and then to access the Secure Access Service with single sign-on (SSO) through the SAML consumer service.

As a result, the user who authenticates elsewhere can access resources behind the Secure Access Service without signing in again.

Using the Artifact Profile and POST Profile

The two supported profiles provide different methods of accomplishing the same task. The end user’s goal is to sign in to all desired resources once, without experiencing multiple sign-in pages for different resources or applications. Although the end user wants transparency, you, the administrator, want to ensure complete security across the resources on your system, regardless of the servers or sites represented.

The artifact profile requires that you construct an automated request-response HTTP message that the browser can retrieve based on an HTTP GET request.

The POST profile requires that you construct an HTML form that can contain the SAML assertion, and which can be submitted by an end user action or a script action, using an HTTP POST method.

Using the Artifact Profile Scenario

The SAML server generally supports the following artifact profile scenario:

1. The user accesses a source site through a browser. The source site might be a corporate portal using a non-Secure Access Service authentication access management system.
2. The source site challenges the user for username and password.
3. The user provides username and password, which the source site authenticates through a call to an LDAP directory or other authentication server.
4. The user then clicks a link on the source site, which points to a resource on a server that is protected behind the Secure Access Service.
5. The link redirects the user to the intersite transfer service URL on the source site. The source site pulls an authentication assertion message from its cache and encloses it in a SOAP message. The source site constructs a SAML artifact (a Base64 string) that it returns to the browser in a URI along with the destination and assertion address.
6. The destination site queries the authenticated assertion from the source site, based on the artifact it receives from the source site.
7. The Secure Access Service accepts the assertion as a valid authentication if the elapsed time falls within the allowable clock skew time. If the user also meets the other Secure Access Service policy restrictions, the Secure Access Service grants the user access to the requested resource.

The main tasks you are required to fulfill to support the Secure Access Service as the relying party with the artifact profile include:

- Implement the assertion consumer service, which:
 - Receives the redirect URL containing the artifact.
 - Generates and sends the SAML request.
 - Receives and processes the SAML response.
- Integrate the assertion consumer service with the existing Secure Access Service process, which:
 - Maps the SAML assertion to a local user.
 - Creates a Secure Access Service user session.
 - Performs local authorization.
 - Serves the resource or denies access.

Using the POST Profile Scenario

The SAML server generally supports the POST profile scenario, as follows:

1. The end user accesses the source website, hereafter known as the source site.
2. The source site verifies whether or not the user has a current session.

3. If not, the source site prompts the user to enter user credentials.
4. The user supplies credentials, for example, username and password.
5. If the authentication is successful, the source site authentication server creates a session for the user and displays the appropriate welcome page of the portal application.
6. The user then selects a menu option or link that points to a resource or application on a destination website.
7. The portal application directs the request to the local intersite transfer service, which can be hosted on the source site. The request contains the URL of the resource on the destination site, in other words, the TARGET URL.
8. The intersite transfer service sends an HTML form back to the browser. The HTML FORM contains a SAML response, within which is a SAML assertion. The response must be digitally signed. Typically the HTML FORM will contain an input or submit action that will result in an HTTP POST. This can be a user-clickable Submit button or a script that initiates the HTTP POST programmatically.
9. The browser, either due to a user action or by way of an auto-submit action, sends an HTTP POST containing the SAML response to the destination website's assertion consumer service.
10. The replying party's assertion consumer (in this case, on the destination website) validates the digital signature on the SAML response.
11. If valid, the assertion consumer sends a redirect to the browser, causing the browser to access the TARGET resource.
12. The Secure Access Service, on the destination site, verifies that the user is authorized to access the destination site and the TARGET resource.
13. If the user is authorized to access the destination site and the TARGET resource, the Secure Access Service returns the TARGET resource to the browser.

The main tasks you are required to fulfill to support the Secure Access Service as the relying party with the POST profile include:

- Implement the assertion consumer service, which receives and processes the POST form
- Integrate the assertion consumer service with the existing Secure Access Service process, which:
 - Maps the SAML assertion to a local user.
 - Creates a Secure Access Service user session.
 - Performs local authorization.
 - Serves the resource or denies access.

**Related
Documentation**

- [Understanding SAML 1.1 Assertions on page 286](#)

Understanding SAML 1.1 Assertions

Each party in the request-response communication must adhere to certain requirements. The requirements provide a predictable infrastructure so that the assertions and artifacts can be processed correctly.

- The artifact is a Base64-encoded string of 40 bytes. An artifact acts as a token that references an assertion on the source site, so the artifact holder—the Secure Access Service—can authenticate a user who has signed in to the source site and who now wants to access a resource protected by the Secure Access Service. The source site sends the artifact to the Secure Access Service in a redirect, after the user attempts to access a resource protected by the Secure Access Service. The artifact contains:
 - TypeCode—A 2-byte hex code of 0x0001 that identifies the artifact type.
 - SourceID—A Base64-encoded string of 20 bytes that determines the source site identity and location. You can use OpenSSL or similar Base64 encoding tool to generate the encoded string. The Secure Access Service maintains a table of SourceID values and the URL for the corresponding SAML responder. The Secure Access Service and the source site communicate this information in a back channel. On receiving the SAML artifact, the Secure Access Service decodes it and ensures that it is 20 bytes. It determines whether or not the SourceID belongs to a known source site, and, if it does, obtains the site location before sending a SAML request. The source site generates the SourceID by computing the SHA-1 hash of the source site's own URL.
 - AssertionHandle—A 20-byte random value that identifies an assertion stored or generated by the source site. At least 8 bytes of this value should be obtained from a cryptographically secure RNG or PRNG.
- The intersite transfer service is the identity provider URL on the source site (not the Secure Access Service). Your specification of this URL in the admin console enables the Secure Access Service to construct an authentication request to the source site, which holds the user's credentials in cache. The request is similar to the following example:

```
GET http://<intersite transfer hostname and
path>?TARGET=<Target>...<HTTP-Version><other HTTP 1.0 or 1.1 components>
```

In the preceding sample, <intersite transfer hostname and path> consists of the hostname, port number, and path components of the intersite transfer URL at the source and where Target=<Target> specifies the requested target resource at the destination (Secure Access Service protected) site. This request might look like:

```
GET http://10.56.1.123:8002/xferSvc?TARGET=http://www.dest.com/sales.htm
```

- The intersite transfer service redirects the user's browser to the assertion consumer service at the destination site—in this case, the Secure Access Service. The HTTP response from the source site intersite transfer service must be in the following format:

```
<HTTP-Version> 302 <Reason Phrase>
<other headers>
```

```
Location: http://<assertion consumer hostname and path>?<SAML
```

searchpart><other HTTP 1.0 or 1.1 components>

In the preceding sample, <assertion consumer hostname and path> provides the hostname, port number, and path components of an assertion consumer URL at the destination site and where <SAML searchpart>= ...TARGET=<Target> ...SAMLart=<SAML artifact>... consists of one target description, which must be included in the <SAML searchpart> component. At least one SAML artifact must be included in the SAML <SAML searchpart> component. The asserting party can include multiple SAML artifacts.



NOTE: You can use status code 302 to indicate that the requested resource resides temporarily under a different URI.

If <SAML searchpart> contains more than one artifact, all of the artifacts must share the same SourceID.

The redirect might look like:

HTTP/1.1 302 Found

Location:

http://www.ive.com:5802/artifact?TARGET=/www.ive.com/&SAMLart=artifact

- The user's browser accesses the assertion consumer service, with a SAML artifact representing the user's authentication information attached to the URL.

The HTTP request must appear as follows:

GET http://<assertion consumer hostname and path>?<SAML searchpart>
<HTTP-Version><other HTTP 1.0 or 1.1 request components>

In the preceding sample, <assertion consumer hostname and path> provides the hostname, port number, and path components of an assertion consumer URL at the destination site.

<SAML searchpart>= ...TARGET=<Taret>...SAMLart=<SAML artifact> ...

A single target description **MUST** be included in the <SAML searchpart> component. At least one SAML artifact **MUST** be included in the <SAML searchpart> component; multiple SAML artifacts **MAY** be included. If more than one artifact is carried within <SAML searchpart>, all the artifacts **MUST** have the same SourceID.

You should not expose the assertion consumer URL unless over SSL 3.0 or TLS 1.0. Otherwise, transmitted artifacts might be available in plain text to an attacker.

- The issuer value is typically the URL of the source site. You can specify the <ISSUER> variable, which will return the issuer value from the assertion.
- The username template is a reference to the SAML name identifier element, which allows the asserting party to provide a format for the username. The SAML specification allows for values in the following formats:

- Unspecified—Indicates that interpretation of the content is left up to the individual implementations. In this case, you can use the variable `assertionName`.
- Email Address—Indicates that the content is in the form of an e-mail address. In this case, you can use the variable `assertionName`.
- X.509 Subject Name—Indicates that the content is in the form of an X.509 subject name. In this case, you can use the variable `assertionNameDN.<RDN>`.
- Windows Domain Qualified Name—Indicates that the content is a string in the form of `DomainName\Username`.

You should define the username template to accept the type of username your SAML assertion contains.

- You can prevent eavesdropping on the SAML artifact by synchronizing the clocks on the source and destination sites. The Secure Access Service provides an Allowed Clock Skew attribute that dictates the maximum time difference allowed between the Secure Access Service and the source site. The Secure Access Service rejects any assertions whose timing exceeds the allowed clock skew.

Related Documentation

- [Understanding SAML 1.1 Profiles on page 283](#)
- [Creating a SAML 1.1 Server Instance on page 292](#)

Creating a Trust Relationship Between SAML 1.1 Systems

In order to ensure that SAML-enabled systems are only passing information between trusted sources, you must create a trust relationship between the applications that are sending and receiving information.

Configuring Trusted Application URLs

In a trust relationship, you must provide the SAML-enabled systems with the URLs they need to contact each other. In some transactions, only the system that initiates the transaction (the Secure Access Service) needs to know the URL of the other system. (The Secure Access Service uses the URL to initiate the transaction.) In other transactions (SSO transactions using artifact profiles), you need to configure each system with the URL of the other.

The following list shows the different transaction types and the URLs you must configure for each:

- SSO transactions: Artifact profile—On the Secure Access Service, you must enter the URL of the assertion consumer service. For example, use <https://hostname/acs>.

You must also enter the following URL for the Secure Access Service on the assertion consumer service. For example, use

<https://<SecureAccessHostname>/dana-ws/saml.ws>.

- SSO transactions: POST profile—On the Secure Access Service, you must enter the URL of the assertion consumer service. For example, use <https://hostname/acs>.

- Access control transactions—On the Secure Access Service, you must enter the URL of the SAML Web service. For example, use <https://hostname/ws>.

Configuring an Issuer

Before accepting a statement from another system, a SAML-enabled entity must trust the issuer of the statement. You can control which issuers a system trusts by specifying the unique strings of the trusted issuers during the system's configuration. (When sending a statement, an issuer identifies itself by including its unique string in the statement. SAML-enabled applications generally use hostnames to identify issuers, but the SAML standard allows applications to use any string.) If you do not configure a system to recognize an issuer's unique string, the system will not accept that issuer's statements.

The following list shows the different transaction types and the issuers you must configure for each:

- SSO transactions—You must specify a unique string on the Secure Access Service (typically its hostname) that it can use to identify itself and then configure the access management system to recognize that string.
- Access control transactions—You must specify a unique string on the access management system (typically its hostname) that it can use to identify itself and then configure the Secure Access Service to recognize that string.

Configuring Certificates

Within SSL transactions, the server must present a certificate to the client, and then the client must verify (at minimum) that it trusts the certificate authority who issued the server's certificate before accepting the information. You can configure all of the Secure Access Service SAML transactions to use SSL (HTTPS).

Configuring SSO Transactions: Artifact Profile

Artifact profile transactions involve numerous communications back and forth between the Secure Access Service and the access management system. The methods you use to pass data and authenticate the two systems affect which certificates you must install and configure.

The following list shows the different artifact profile configuration options that require special certificate configurations:

- All artifact profile transactions—Regardless of your artifact profile configuration, you must install the certificate of the CA that signed the Secure Access Service Web server certificate on the access management system. (The Secure Access Service requires the access management system to use an SSL connection when requesting an authentication statement. In an SSL connection, the initiator must trust the system to which it is connecting. By installing the CA certificate on the access management system, you ensure that the access management system will trust the CA that issued the Secure Access Service certificate.)
- Sending artifacts over an SSL connection (HTTPS GET requests)—If you choose to send artifacts to the access management system using an SSL connection, you must install the access management system's root CA certificate on the Secure Access

Service. (In an SSL connection, the initiator must trust the system to which it is connecting. By installing the access management system's CA certificate on the Secure Access Service, you ensure that the Secure Access Service will trust the CA that issued the access management system's certificate.) You can install the root CA from the System > Configuration > Certificates > Trusted Client CAs page in the admin console. If you do not want to send artifacts over an SSL connection, you do not need to install any additional certificates.

To enable SSL-based communications from the Secure Access Service to the access management system, enter a URL that begins with HTTPS in the SAML Assertion Consumer Service URL field during the Secure Access Service configuration. You may also need to enable SSL on the access management system.

- Transactions using certificate authentication—If you choose to authenticate the access management system using a certificate, you must:
 - Install the access management system's root CA certificate on the Secure Access Service. You can install the root CA from the System > Configuration > Certificates > Trusted Client CAs page in the admin console.
 - Specify which certificate values the Secure Access Service should use to validate the access management system. You must use values that match the values contained in the access management server's certificate.

If you do not choose to authenticate the access management system, or if you choose to use username/password authentication, you do not need to install any additional certificates.

Configuring SSO Transactions: POST Profile

In a POST profile transaction, the Secure Access Service sends signed authentication statements to the access management system. Generally, it sends them over an SSL connection (recommended), but in some configurations, the Secure Access Service may send statements through a standard HTTP connection.

The following list shows the different POST profile configuration options that require special certificate configurations:

- All POST profile transactions—Regardless of your POST profile configuration, you must specify which certificate the Secure Access Service should use to sign its statements. You can choose a certificate in the Users > Resource Policies > Web > SSO SAML > [Policy] > General page in the admin console. Then, you must install the Secure Access Service device certificate on the access management system. You can download the Secure Access Service certificate from the System > Configuration > Certificates > Device Certificates > [Certificate] > Certificate Details page.
- Sending POST data over an SSL connection (HTTPS)—If you choose to send statements to the access management system using an SSL connection, you must install the access management system's root CA certificate on the Secure Access Service. (In an SSL connection, the initiator must trust the system to which it is connecting. By installing the access management system's certificate on the Secure Access Service, you ensure that the Secure Access Service will trust the CA that issued the access management system's certificate.) You can install the root CA from the

System > Configuration > Certificates > Trusted Client CAs page in the admin console. If you do not want to post statements over an SSL connection, you do not need to install any additional certificates.

To enable SSL-based communications from the Secure Access Service to the access management system, enter a URL that begins with HTTPS in the SAML assertion consumer service URL field during the Secure Access Service configuration. You may also need to enable SSL on the access management system.

Configuring Access Control Transactions

In an access control transaction, the Secure Access Service posts an authorization decision query to the access management system. To ensure that the access management system responds to the query, you must determine which certificate options are required by your configuration.

The following list shows the different access control configuration options that require special certificate configurations:

- Sending authorization data over an SSL connection—If you choose to connect to the access management system using an SSL connection, you must install the access management system's root CA on the Secure Access Service. (In an SSL connection, the initiator must trust the system to which it is connecting. By installing the access management system's certificate on the Secure Access Service, you ensure that the Secure Access Service will trust the CA that issued the access management system's certificate.) You can install the root CA from the System > Configuration > Certificates > Trusted Client CAs page in the admin console.
- Transactions using certificate authentication—If you choose to use certificate authentication, you must configure the access management system to trust the CA that issued the Secure Access Service certificate. Optionally, you may also choose to accept the certificate based on the following additional options:
 - Upload the Secure Access Service certificate public key to the access management system.
 - Validate the Secure Access Service using specific certificate attributes.

These options require that you specify which certificate the Secure Access Service should pass to the access management system. You can choose a certificate in the Users > Resource Policies > Web > SAML ACL > [Policy] > General page in the admin console.

To determine how to configure your access management system to validate the Secure Access Service certificate, see your access management system's documentation. If your access management system does not require certificate authentication, or if it uses username/password authentication, you do not need to configure the Secure Access Service to pass the access management server a certificate. If you do not specify a trust method, your access management system may accept authorization requests from any system.

Configuring User Identity

In a trust relationship, the two entities must agree on a way to identify users. You may choose to share a username across systems, select an LDAP or certificate user attribute to share across systems, or hardcode a user ID. (For example, you may choose to set the Subject Name field to “guest” to easily allow access across systems.)

To ensure that the two systems are passing common information about users, you must specify which information the Secure Access Service should pass using options in the User Identity section of the Users > Resource Policies > Web > SAML SSO > [Policy] > General page and the Users > Resource Policies > Web > SAML ACL > [Policy] > General page. Choose a username or attribute that the access management system will recognize.

Related Documentation

- [Using a Trusted Client CA on page 846](#)
- [Understanding SAML 1.1 on page 281](#)
- [Configuring SAML 1.1 SSO Profiles on page 294](#)
- [Configuring General Role Options on page 109](#)

Secure Access Service SAML Version 1.1 Configuration Tasks

The following topics describe how to configure the Secure Access Service features that support SAML version 1.1:

- [Creating a SAML 1.1 Server Instance on page 292](#)
- [Configuring SAML 1.1 SSO Profiles on page 294](#)
- [Creating a SAML 1.1 SSO POST Profile on page 298](#)
- [Creating a SAML 1.1 ACL Resource Policy on page 301](#)

Creating a SAML 1.1 Server Instance

To create a new SAML server instance:

1. In the admin console, choose **Authentication > Auth. Servers**.
2. Select **SAML Server** from the New list, and then click **New Server**.
3. Complete the settings as described in [Table 32 on page 292](#).
4. Click **Save Changes**.

After you save changes for the first time, the page is redisplayed and now has two tabs. The Settings tab allows you to modify any of the settings pertaining to the SAML Server instance. The Users tab lists valid users of the server.

Table 32: SAML Authentication Server (SAML 1.1)

Setting	Guideline
Name	Specify a name to identify the server instance.

Table 32: SAML Authentication Server (SAML 1.1) (continued)

Setting	Guideline
Settings	
SAML Version	Select 1.1.
Source Site Inter-Site Transfer Service URL	User is redirected to this URL in destination first scenario.
Issuer Value for Source Site	Typically the URI or hostname of the issuer of the assertion.
User Name Template	Enter the mapping string from the SAML assertion to a Secure Access Service user realm. For example, enter <code><assertionNameDN.CN></code> to derive the username from the CN value in the assertion.
Allowed Clock Skew	The maximum allowed difference in time between the Secure Access Service clock and the source site clock.
SSO Method	
Artifact	<ul style="list-style-type: none"> Source ID. A Base64-encoded string of 20 bytes that the Secure Access Service uses to recognize an assertion from a given source site. Source SOAP Responder Service URL SOAP Client Authentication. Select HTTP Basic or SSL Client Certificate and complete the related settings. <p>NOTE: SOAP requests generated by the Secure Access Service (when configured as a SAML 1.1 consumer) are not signed.</p>
POST	<ul style="list-style-type: none"> Response Signing Certificate. Enter the name of, or browse to locate, the PEM-formatted signing certificate, which is loaded for the SAML response signature verification. The certificate you select should be the same certificate used for signing the SAML response at the source site. The source site may send this certificate along with the SAML response, depending on the source site configuration. By default, the system performs signature verification of the SAML response first on the locally configured certificate. If a certificate is not configured locally in the SAML authentication server, then the system performs the signature verification on the certificate included in the SAML response from the source site. Enable Signing Certificate status checking. Select this option to check the validity of the signing certificate configured in the SAML authentication server POST profile. It is possible that the certificate has already expired or has been revoked.
User Record Synchronization	
Enable User Record Synchronization	Allow users to retain their bookmarks and individual preferences regardless of which Secure Access Service device they log in to.
Logical Auth Server Name	

**Related
Documentation**

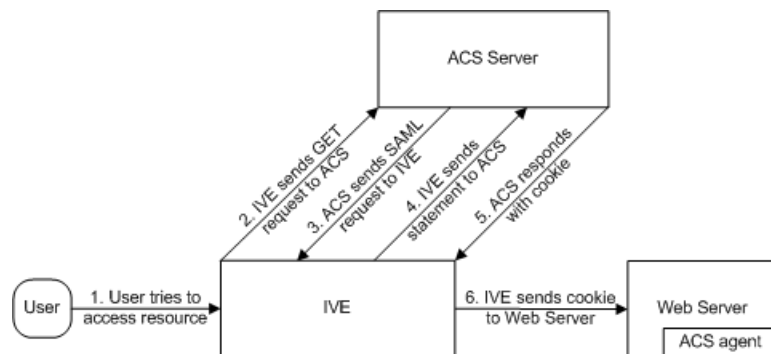
Configuring SAML 1.1 SSO Profiles

When enabling SSO transactions to a trusted access management system, you must indicate whether the access management system should “pull” user information from the Secure Access Service or whether the Secure Access Service should “push” it to the access management system. You indicate which communication method the two systems should use by selecting a profile during configuration. A *profile* is a method that two trusted sites use to transfer a SAML statement. When configuring the Secure Access Service, you may choose to use an artifact or POST profile.

When you choose to communicate using the *artifact profile* (also called browser/artifact profile), the trusted access management server “pulls” authentication information from the Secure Access Service.

Figure 28 on page 294 shows the SAML communication process when the implementation uses the artifact profile.

Figure 28: Artifact Profile



The Secure Access Service and an assertion consumer service (ACS) use the following process to pass information:

1. The user tries to access a resource—A user is signed into the Secure Access Service and tries to access a protected resource on a Web server.
2. The Secure Access Service sends an HTTP or HTTPS GET request to the ACS—the Secure Access Service intercepts the request and checks whether it has already performed the necessary SSO operation to honor the request. If not, the Secure Access Service creates an authentication statement and passes an HTTP query variable called an artifact to the assertion consumer service.

An artifact profile is a Base64-encoded string that contains the source ID of the source site (that is, a 20-byte string that references the Secure Access Service) and a randomly generated string that acts as a handle to the authentication statement. (Note that a handle expires 5 minutes after the artifact is sent, so if the assertion consumer service responds after 5 minutes, the Secure Access Service does not send a statement. Also note that the Secure Access Service discards a handle after its first use to prevent the handle from being used twice.)

3. The ACS sends a SAML request to the Secure Access Service—The assertion consumer service uses the source ID sent in the previous step to determine the location of the

Secure Access Service. Then the assertion consumer service sends a statement request wrapped in a SOAP message to the following address on the Secure Access Service:

`https://<<ivehostname>/danaws/saml.ws`

The request includes the statement handle passed in the previous step.



NOTE: The Secure Access Service only supports type 0x0001 artifacts. This type of artifact passes a reference to the source site's location (that is, the source ID of the Secure Access Service), rather than sending the location itself. To handle type 0x0001 artifacts, the assertion consumer service must maintain a table that maps source IDs to the locations of partner source sites.


4. The Secure Access Service sends an authentication statement to the ACS—the Secure Access Service uses the statement handle in the request to find the correct statement in the Secure Access Service cache and then sends the appropriate authentication statement back to the assertion consumer service. The unsigned statement contains the user's identity and the mechanism he used to sign into the Secure Access Service.
5. The ACS sends a cookie to the Secure Access Service—The assertion consumer service accepts the statement and then it sends a cookie back to the Secure Access Service that enables the user's session.
6. The Secure Access Service sends the cookie to the Web server—the Secure Access Service caches the cookie to handle future requests. Then the Secure Access Service sends the cookie in an HTTP request to the Web server whose domain name matches the domain in the cookie. The Web server honors the session without prompting the user for credentials.



NOTE: If you configure the Secure Access Service to use artifact profiles, you must install the Secure Access Service Web server certificate on the assertion consumer service.

To write a SAML SSO artifact profile resource policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show SAML policies, make the following modifications:
 - a. Click the **Customize** button in the upper right corner of the page.
 - b. Select the **SSO** check box.
 - c. Select the **SAML** check box below the SSO check box.
 - d. Click **OK**.
3. Use the tabs to display the **SSO > SAML** page.

4. Click **New Policy**.
 5. On the New Policy page, enter:
 - a. A name to label this policy.
 - b. A description of the policy (optional).
 6. In the Resources section, specify the resources to which this policy applies.
 7. In the Roles section, specify:
 - **Policy applies to ALL roles**—To apply this policy to all users.
 - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
 - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
 8. In the Action section, specify:
 - **Use the SAML SSO defined below**—The Secure Access Service performs a single-sign on (SSO) request to the specified URL using the data specified in the SAML SSO details section. The Secure Access Service makes the SSO request when a user tries to access a SAML resource specified in the Resources list.
 - **Do NOT use SAML**—The Secure Access Service does not perform a SSO request.
 - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
 9. In the SAML SSO Details section, specify:
 - **SAML Assertion Consumer Service URL**—Enter the URL that the Secure Access Service should use to contact the assertion consumer service (that is, the access management server). For example, `https://<hostname>:<port>/dana-na/auth/saml-consumer.cgi`. (Note that the Secure Access Service also uses this field to determine the SAML recipient for its assertions.)
-
- 
- NOTE:** If you enter a URL that begins with HTTPS, you must install the assertion consumer service's root CA on the Secure Access Service.
-
- **Profile**—Select **Artifact** to indicate that the assertion consumer service should “pull” information from the Secure Access Service during SSO transactions.
 - **Source ID**—Enter the source ID for the Secure Access Service. It must be a Base64-encoded string. The Secure Access Service decodes it and ensures that it is 20 bytes. You can use OpenSSL or other Base64 tool to generate the Base64-encoded string.



NOTE: The Secure Access Service identifier (that is, the source ID) must map to the following URL on the assertion consumer service:
`https://<ivehostname>/dana-ws/saml.ws`

- **Issuer**—Enter a unique string that the Secure Access Service can use to identify itself when it generates assertions (typically its hostname).



NOTE: You must configure the assertion consumer service to recognize the Secure Access Service unique string.

10. In the User Identity section, specify how the Secure Access Service and the assertion consumer service should identify the user:

- **Subject Name Type**—Specify which method the Secure Access Service and assertion consumer service should use to identify the user:
 - **DN**—Send the username in the format of a DN (distinguished name) attribute.
 - **Email Address**—Send the username in the format of an email address.
 - **Windows**—Send the username in the format of a Windows domain qualified username.
 - **Other**—Send the username in another format agreed upon by the Secure Access Service and the assertion consumer service.
- **Subject Name**—Use variables to specify the username that the Secure Access Service should pass to the assertion consumer service. Or, enter static text.



NOTE: You must send a username or attribute that the assertion consumer service will recognize.

11. In the Web Service Authentication section, specify the authentication method that the Secure Access Service should use to authenticate the assertion consumer service:

- **None**—Do not authenticate the assertion consumer service.
- **Username**—Authenticate the assertion consumer service using a username and password. Enter the username and password that the assertion consumer service must send the Secure Access Service.
- **Certificate Attribute**—Authenticate the assertion consumer service using certificate attributes. Enter the attributes that the assertion consumer service must send the Secure Access Service (one attribute per line). For example, use `cn=sales`. You must use values that match the values contained in the assertion consumer service certificate.



NOTE: If you select this option, you must install the assertion consumer service root CA on the Secure Access Service.

12. **Cookie Domain**—Enter a comma-separated list of domains to which we send the SSO cookie.
13. Click **Save Changes**.
14. On the SAML SSO Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

Related Documentation

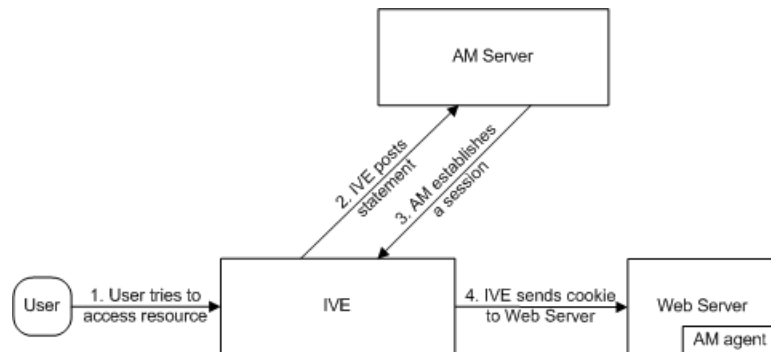
- [About Using Certificates on Secure Access Service on page 838](#)

Creating a SAML 1.1 SSO POST Profile

When you choose to communicate using a POST profile (also called browser/POST profile), the Secure Access Service “pushes” authentication data to the access management system using an HTTP POST command over an SSL 3.0 connection.

Figure 29 on page 298 shows the SAML communication process when the implementation uses the POST profile.

Figure 29: POST Profile



The Secure Access Service and an access management system use the following process to pass information:

1. The user tries to access a resource—A user is signed into the Secure Access Service and tries to access a protected resource on a Web server.
2. The Secure Access Service posts a statement—the Secure Access Service intercepts the request and checks whether it has already performed the necessary SSO operation to honor the request. If not, the Secure Access Service creates an authentication statement, digitally signs it, and posts it directly to the access management server. Since the statement is signed, the access management server must trust the certificate authority that was used to issue the certificate. Note that you must configure which certificate the Secure Access Service uses to sign the statement.

3. The AM establishes a session—If the user has the proper permissions, the access management server sends a cookie back to the Secure Access Service that enables the user's session.
4. The Secure Access Service sends the cookie to the Web server—the Secure Access Service caches the cookie to handle future requests. Then the Secure Access Service sends the cookie in an HTTP request to the Web server whose domain name matches the domain in the cookie. The Web server honors the session without prompting the user for credentials.



NOTE: If you configure the Secure Access Service to use POST profiles, you must install the assertion consumer service's root CA on the Secure Access Service and determine which method the assertion consumer service uses to trust the certificate.

To write a SAML SSO POST profile resource policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show SAML policies, make the following modifications:
 - a. Click the **Customize** button in the upper right corner of the page.
 - b. Select the **SSO** check box.
 - c. Select the **SAML** check box below the SSO check box.
 - d. Click **OK**.
3. Use the tabs to display the **SSO > SAML** page.
4. Click **New Policy**.
5. On the SAML SSO Policy page, enter:
 - A name to label this policy.
 - A description of the policy (optional).
6. In the Resources section, specify the resources to which this policy applies.
7. In the Roles section, specify:
 - **Policy applies to ALL roles**—To apply this policy to all users.
 - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
 - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:

- **Use the SAML SSO defined below**—The Secure Access Service performs a single-sign on (SSO) request to the specified URL using the data specified in the SAML SSO details section. The Secure Access Service makes the SSO request when a user tries to access a SAML resource specified in the Resources list.
 - **Do NOT use SAML**—The Secure Access Service does not perform an SSO request.
 - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. In the SAML SSO Details section, specify:
- **SAML Assertion Consumer Service URL**—Enter the URL that the Secure Access Service should use to contact the assertion consumer service (that is, the access management server). For example, use <https://hostname/acs>.
 - **Profile**—Select POST to indicate that the Secure Access Service should “push” information to the assertion consumer service during SSO transactions.
 - **Issuer**—Enter a unique string that the Secure Access Service can use to identify itself when it generates assertions. Typically, the issuer string is a hostname.



NOTE: You must configure the assertion consumer service to recognize the Secure Access Service unique string.

- **Signing Certificate**—Specify which certificate the Secure Access Service should use to sign its assertions.
10. In the User Identity section, specify how the Secure Access Service and the assertion consumer service should identify the user:
- **Subject Name Type**—Specify which method the Secure Access Service and assertion consumer service should use to identify the user:
 - **DNDN**—Send the username in the format of a DN (distinguished name) attribute.
 - **Email Address**—Send the username in the format of an e-mail address.
 - **Windows**—Send the username in the format of a Windows domain qualified username.
 - **Other**—Send the username in another format agreed upon by the Secure Access Service and the assertion consumer service.
 - **Subject Name**—Use variables to specify the username that the Secure Access Service should pass to the assertion consumer service. Or, enter static text.



NOTE: You must send a username or attribute that the assertion consumer service will recognize.

- **Cookie Domain**—Enter a comma-separated list of domains to which we send the SSO cookie.

11. Click **Save Changes**.
12. On the SAML SSO Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

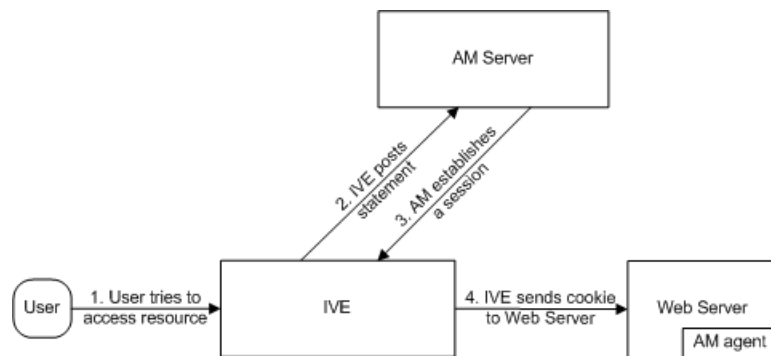
Related Documentation

- [About Using Certificates on Secure Access Service on page 838](#)
- [Writing a Web Proxy Resource Policy on page 554](#)

Creating a SAML 1.1 ACL Resource Policy

When enabling access control transactions to a trusted access management system, the Secure Access Service and trusted access management system exchange information using the method shown in [Figure 30 on page 301](#).

Figure 30: Access Control Policies



The Secure Access Service and an access management system use the following process to pass information:

1. The user tries to access a resource—A user is signed into the Secure Access Service and tries to access a protected resource on a Web server.
2. The Secure Access Service posts an authorization decision query—If the Secure Access Service has already made an authorization request and it is still valid, the Secure Access Service uses that request. (The authorization request is valid for the period of time specified in the admin console.) If it does not have a valid authorization request, the Secure Access Service posts an authorization decision query to the access management system. The query contains the user's identity and the resource that the access management system needs to authorize.
3. The access management system posts an authorization decision statement—The access management system sends an HTTPS POST containing a SOAP message that contains the authorization decision statement. The authorization decision statement contains a result of permit, deny, or indeterminate.
4. The Secure Access Service sends the request to the Web browser—If the authorization decision statement returns a result of permit, the Secure Access Service allows the

user access. If not, the Secure Access Service presents an error page to the user telling him that he does not have the proper access permissions.



NOTE: If you configure the Secure Access Service to use access control transactions, you must install the SAML Web service root CA on the Secure Access Service.

To create a SAML access control resource policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show SAML policies, make the following modifications:
 - a. Click the **Customize** button in the upper right corner of the page.
 - b. Select the **SAML ACL** check box below the Access check box.
 - c. Click **OK**.
3. Use the tabs to display the Access > SAML ACL page.
4. On the SAML Access Control Policies page, click **New Policy**.
5. On the New Policy page, enter:
 - a. A name to label this policy.
 - b. A description of the policy (optional).
6. In the Resources section, specify the resources to which this policy applies.
7. In the Roles section, specify:
 - **Policy applies to ALL roles**—To apply this policy to all users.
 - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
 - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
 - **Use the SAML Access Control checks defined below**—The Secure Access Service performs an access control check to the specified URL using the data specified in the SAML Access Control Details section.
 - **Do not use SAML Access**—The Secure Access Service does not perform an access control check.
 - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. In the SAML Access Control Details section, specify:

- **SAML Web Service URL**—Enter the URL of the access management system’s SAML server. For example, use <https://hostname/ws>.
- **Issuer**—Enter the hostname of the issuer, which in most cases is the hostname of the access management system.



NOTE: You must enter a unique string that the SAML Web service uses to identify itself in authorization assertions.

10. In the User Identity section, specify how the Secure Access Service and the SAML Web service should identify the user:

- **Subject Name Type**—Specify which method the Secure Access Service and SAML Web service should use to identify the user:
 - **DN**—Send the username in the format of a DN (distinguished name) attribute.
 - **Email Address**—Send the username in the format of an e-mail address.
 - **Windows**—Send the username in the format of a Windows domain qualified username.
 - **Other**—Send the username in another format agreed upon by the Secure Access Service and the SAML Web service.
- **Subject Name**—Use variables to specify the username that the Secure Access Service should pass to the SAML Web service. Or, enter static text.



NOTE: You must send a username or attribute that the SAML Web service will recognize.

11. In the Web Service Authentication section, specify the authentication method that the SAML Web service should use to authenticate the Secure Access Service:

- **None**—Do not authenticate the Secure Access Service.
- **Username**—Authenticate the Secure Access Service using a username and password. Enter the username and password that the Secure Access Service must send the Web service.
- **Certificate Attribute**—Authenticate the Secure Access Service using a certificate signed by a trusted certificate authority. If you have more than one certificate installed on the Secure Access Service, use the drop-down list to select which certificate to send to the Web service.



NOTE: If you select this option, you must install the Secure Access Service Web server certificate on the access management system Web server and determine which method the SAML Web service uses to trust the certificate.

12. In the Options section, specify:
 - **Maximum Cache Time**—You can eliminate the overhead of generating an authorization decision each time the user requests the same URL by indicating that the Secure Access Service must cache the access management system's authorization responses. Enter the amount of time the Secure Access Service should cache the responses (in seconds).
 - **Ignore Query Data**—By default, when a user requests a resource, the Secure Access Service sends the entire URL for that resource (including the query parameter) to the SAML Web service and caches the URL. You can specify that the Secure Access Service should remove the query string from the URL before requesting authorization or caching the authorization response.
13. Click **Save Changes**.
14. On the SAML Access Control Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

**Related
Documentation**

- [About Using Certificates on Secure Access Service on page 838](#)
- [Writing a Web Proxy Resource Policy on page 554](#)

Authentication Realms

- [Authentication Realm Overview on page 305](#)
- [Creating an Authentication Realm on page 306](#)
- [Defining Authentication Access Policies on page 307](#)
- [Role Mapping Rules on page 308](#)
- [Specifying Role Mapping Rules for an Authentication Realm on page 309](#)
- [Machine Authentication for Junos Pulse Connections on page 311](#)
- [Junos Pulse Connection Realm and Role Preferences for Machine Authentication on page 312](#)
- [Using the LDAP Server Catalog on page 314](#)
- [Customizing User Realm UI Views on page 318](#)

Authentication Realm Overview

An authentication realm specifies the conditions that users must meet in order to sign into the Secure Access Service. A realm consists of a grouping of authentication resources, including:

- An authentication server — verifies that the user is who he claims to be. The Secure Access Service forwards credentials that a user submits on a sign-in page to an authentication server.
- A directory server—an LDAP server that provides user and group information to the Secure Access Service that the Secure Access Service uses to map users to one or more user roles.
- An authentication policy—specifies realm security requirements that need to be met before the Secure Access Service submits a user's credentials to an authentication server for verification.
- Role mapping rules—conditions a user must meet in order for the Secure Access Service to map the user to one or more user roles. These conditions are based on either user information returned by the realm's directory server or the user's username.

Authentication realms are an integral part of the Secure Access Service access management framework, and therefore are available on all Secure Access products. Note, however that custom expressions are not available on the Secure Access Service

700 appliance and are only available on all other Secure Access products by special license. Therefore, when creating a realm, not all administrators can create advanced role-mapping rules using custom expressions.

**Related
Documentation**

- [About Sign-In Policies on page 321](#)
- [Defining Authentication Access Policies on page 307](#)
- [Creating an Authentication Realm on page 306](#)

Creating an Authentication Realm

To create an authentication realm:

1. In the admin console, choose **Administrators > Admin Realms** or **Users > User Realms**.
2. On the respective Authentication Realms page, click **New**. Or, select a realm and click **Duplicate** to base your realm on an existing realm.
3. Enter a name to label this realm and (optionally) a description.
4. If you are copying an existing realm, click **Duplicate**. Then, if you want to modify any of its settings, click the realm's name to enter into edit mode.
5. Select **When editing, start on the Role Mapping page** if you want the Role Mapping tab to be selected when you open the realm for editing.
6. Under Servers, specify:
 - An authentication server to use for authenticating users who sign in to this realm.
 - A directory/attribute server to use for retrieving user attribute and group information for role mapping rules and resource policies. (optional)
 - A RADIUS accounting server to use to track when a user signs in and out of the Infranet Controller (optional).
7. If you want to submit secondary user credentials to an SSO-enabled resource or enable two-factor authentication to access the Secure Access device, select **Additional authentication server**. Then:
 - a. Select the name of the secondary authentication server. Note that you cannot choose an anonymous server, certificate server, or eTrust SiteMinder server.
 - b. Select **Username** is specified by user on sign-in page if you want to prompt the user to manually submit his username to the secondary server during the Secure Access sign-in process. Otherwise, if you want to automatically submit a username to the secondary server, enter static text or a valid variable in the predefined as field. By default, Secure Access submits the <username> session variable, which holds the same username used to sign in to the primary authentication server.
 - c. Select **Password** is specified by user on sign-in page if you want to prompt the user to manually submit his password to the secondary server during the Secure Access

sign-in process. Otherwise, if you want to automatically submit a password to the secondary server, enter static text or a valid variable in the predefined as field.

- d. Select **End session if authentication against this server fails** if you want to control access to Secure Access based on the successful authentication of the user's secondary credentials. If selected, authentication fails if the user's secondary credentials fails.
8. If you want to use dynamic policy evaluation for this realm select **Dynamic policy evaluation** to enable an automatic timer for dynamic policy evaluation of this realm's authentication policy, role mapping rules, and role restrictions. Then:
 - a. Use the Refresh interval option to specify how often you want the Infranet Controller to perform an automatic policy evaluation of all currently signedin realm users. Specify the number of minutes (5 to 1440).
 - b. Select **Refresh roles** to also refresh the roles of all users in this realm. (This option does not control the scope of the Refresh Now button.)
 - c. Select **Refresh resource policies** to also refresh the resource policies (not including Meeting and Email Client) for all users in this realm. (This option does not control the scope of the Refresh Now button.)
 - d. Click **Refresh Now** to manually evaluate the realm's authentication policy, role mapping rules, role restrictions, user roles, and resource policies of all currently signed-in realm users. Use this button if you make changes to an authentication policy, role mapping rules, role restrictions, or resource policies and you want to immediately refresh the roles of this realm's users.
 9. Click **Save Changes** to create the realm on the Secure Access device. The General, Authentication Policy, and Role Mapping tabs for the authentication realm appear.
 10. Perform the next configuration steps:
 - a. Configure one or more role mapping rules.
 - b. Configure an authentication policy for the realm.

Related Documentation

- [Defining Authentication Access Policies on page 307](#)
- [Configuring User Sign In Policies on page 324](#)
- [Dynamic Policy Evaluation on page 77](#)

Defining Authentication Access Policies

An authentication policy is a set of rules that controls one aspect of access management—whether or not to present a realm's sign-in page to a user. An authentication policy is part of an authentication realm's configuration, specifying rules for Secure Access to consider before presenting a sign-in page to a user. If a user meets the requirements specified by the realm's authentication policy, then Secure Access presents the corresponding sign-in page to the user and then forwards the user's

credentials to the appropriate authentication server. If this server successfully authenticates the user, then Secure Access moves on to the role evaluation process.

To specify authentication realm access policies:

1. In the admin console, choose **Administrators > Admin Realms or Users > User Realms**.
2. On the respective Authentication Realms page, click Specifying RADIUS Request Attributes a realm and then click the **Authentication Policy** tab.
3. On the Authentication Policy page, configure one or more of the access management options described in the Related Topics section.

**Related
Documentation**

- [Specifying Source IP Access Restrictions on page 79](#)
- [Specifying Password Access Restrictions on page 85](#)
- [Specifying Certificate Access Restrictions on page 84](#)
- [Specifying Browser Access Restrictions on page 82](#)
- [Specifying Session Limits on page 86](#)

Role Mapping Rules

Role mapping rules are conditions a user must meet in order for Secure Access to map the user to one or more user roles. These conditions are based on either user information returned by the realm's directory server or the user's username. You must specify role mapping directives in the following format: If the specified condition is|is not true, then map the user to the selected roles.

You create a role mapping rule on Role Mapping tab of an authentication realm. When you click New Rule on this tab, the Role Mapping Rule page appears with an inline editor for defining the rule. This editor leads you through the three steps of creating a rule:

- Specify the type of condition on which to base the rule. Options include:
 - Username
 - User attribute
 - Certificate or certificate attribute
 - Group membership
 - Custom expressions
- Specify the condition to evaluate, which consists of:
 - One or more usernames, user attributes, certificate attributes, groups (LDAP), or expressions depending on the type of condition you selected.
 - To what the value(s) should equate, which may include a list of usernames, user attribute values from a RADIUS or LDAP server, client-side certificate values (static or compared to LDAP attributes), LDAP groups, or pre-defined custom expressions.

- Specify the roles to assign to the authenticated user.

Secure Access compiles a list of eligible roles to which a user may be mapped, which are roles specified by the role mapping rules to which the user conforms. Next, Secure Access evaluates the definition for each role to determine if the user complies with any role restrictions. Secure Access uses this information to compile a list of valid roles, which are roles for which the user meets any additional requirements. Finally, Secure Access either performs a permissive merge of the valid roles or presents a list of valid roles to the user, depending on the configuration specified on the realm's Role Mapping tab.

Related Documentation

- [User Roles Overview on page 105](#)

Specifying Role Mapping Rules for an Authentication Realm

When creating a new rule that uses LDAP or SiteMinder user attributes, LDAP group information, or custom expressions, you must use the server catalog.

To specify role mapping rules for an authentication realm:

1. In the admin console, choose **Administrators > Admin Realms** or **Users > User Realms**.
2. On the respective Authentication Realms page, select a realm and then click the **Role Mapping** tab.
3. Click **New Rule** to access the Role Mapping Rule page. This page provides an inline editor for defining the rule.
4. In the Rule based on list, choose one of the following:
 - **Username**—Username is the Secure Access username entered on the sign-in page. Choose this option if you want to map users to roles based on their Secure Access usernames. This type of rule is available for all realms.
 - **User attribute**—User attribute is a user attribute from a RADIUS, LDAP, or SiteMinder server. Choose this option if you want to map users to roles based on an attribute from the corresponding server. This type of rule is available only for realms that use a RADIUS server for the authentication server, or that use an LDAP or SiteMinder server for either the authentication server or directory server. After choosing the User attribute option, click Update to display the Attribute list and the Attributes button. Click the Attributes button to display the server catalog.
 - To add SiteMinder user attributes, enter the SiteMinder user attribute cookie name in the Attribute field in the server catalog, and then click Add Attribute. When you are finished adding cookie names, click OK. Secure Access displays the names of the SiteMinder user attribute cookies in the Attribute list on the Role Mapping Rule page.
 - For information on how to use the server catalog to add LDAP user attributes.
 - **Certificate or Certificate attribute**—Certificate or Certificate attribute is an attribute supported by the users' client-side certificate. Choose this option if you want to map users to roles based on certificate attributes. The Certificate option is available for all realms; the Certificate attribute option is available only for realms that use

LDAP for the authentication or directory server. After choosing this option, click Update to display the Attribute text box.

- **Group membership**—Group membership is group information from an LDAP or native Active Directory server that you add to the server catalog Groups tab. Choose this option if you want to map users to roles based on either LDAP or Active Directory group information. This type of rule is available only for realms that use an LDAP server for either the authentication server or directory server or that use an Active Directory server for authentication. (Note that you cannot specify an Active Directory server as an authorization server for a realm.)
- **Custom Expressions**—Custom Expressions is one or more custom expressions that you define in the server catalog. Choose this option if you want to map users to roles based on custom expressions. This type of rule is available for all realms. After choosing this option, click Update to display the Expressions lists. Click the Expressions button to display the Expressions tab of the server catalog.



NOTE: If you add more than one custom expression to the same rule, Secure Access creates an “OR” rule for the expressions. For example, you might add the following expressions to a single rule:

- Expression 1: cacheCleanerStatus = 1
- Expression 2: loginTime = (8:00AM TO 5:00PM)

Based on these expressions, a user would match this rule if Cache Cleaner was running on his system OR if he signed into the Secure Access device between 8:00 and 5:00.

5. Under Rule, specify the condition to evaluate, which corresponds to the type of rule you select and consists of:
 - a. Specifying one or more usernames, SiteMinder user attribute cookie names, RADIUS or LDAP user attributes, certificate attributes, LDAP groups, or custom expressions.
 - b. Specifying to what the value(s) should equate, which may include a list of Secure Access usernames, user attribute values from a RADIUS, SiteMinder, or LDAP server, client-side certificate values (static or LDAP attribute values), LDAP groups, or custom expressions.

For example, you can choose a SiteMinder user attribute cookie named department from the Attribute list, choose is from the operator list, and then enter "sales" and "eng" in the text box.

Or, you can enter a custom expression rule that references the SiteMinder user attribute cookie named department:

```
<userAttr.department = ("sales" and "eng")>
```

6. Under ...then assign these roles:
 - a. Specify the roles to assign to the authenticated user by adding roles to the **Selected Roles list**.

- b. Check **Stop processing rules when this rule matches** if you want Secure Access to stop evaluating role mapping rules if the user meets the conditions specified for this rule.
7. Click **Save Changes** to create the rule on the Role Mapping tab. When you are finished creating rules:

Make sure to order role mapping rules in the order in which you want Secure Access to evaluate them. This task is particularly important when you want to stop processing role mapping rules upon a match.

Related Documentation

- [Role Mapping Rules on page 308](#)
- [Policies, Rules & Restrictions, and Conditions Overview on page 72](#)

Machine Authentication for Junos Pulse Connections

Junos Pulse supports machine authentication. Machine authentication uses machine credentials (machine name and password or machine certificate) to authenticate the endpoint. You can enable machine authentication for Pulse Secure Access Service as part of a Junos Pulse connection and distribute the connection to endpoints through the normal Pulse distribution methods.

The following describes the requirements for a machine authentication environment:

- Machine authentication for Pulse Secure Access Service is available for Pulse layer 3 connections only.
- The authentication server used by the Pulse connection must be Active Directory/Windows NT for machine name/password authentication or a certificate server for machine certificate authentication.
- The endpoint must be a member of a Windows domain and the machine credentials must be defined in Active Directory. Typically, during login, the user must enter domain/user in the username box.
- The Pulse connection must be configured so that no prompts are presented during the login process. For example, prompts for realm or role selection or a server certificate trust prompt cause the connection to fail.
- For machine certificate authentication, the domain workstation logon certificate must be issued by the domain certificate authority. The root certificate (CA) must be in the Machine Trusted Certificate store instead of the certificate store for a particular user.

To enable a Pulse connection for machine authentication:

1. Click **Users > Junos Pulse > Connections** and create or select a connection set.
2. Create or edit a connection. Machine authentication is available for connection type **SSL VPN or UAC (L3)** only.
3. Under Connection is established, select one of the following options:

- **Automatically when the machine starts. Machine credentials used for authentication**—This option enables machine-only authentication. Machine credentials are used to connect to the Pulse Secure Access Service before the user logs on. The user does not need to be logged in. The connection is maintained when a users logs on, logs off, or switches to a different logon.
- **Automatically when the machine starts. Connection is authenticated again when the user signs in into the desktop**—This option enables user-after-desktop authentication. Machine credentials are used to authenticate the endpoint when no user is logged on. When a user logs on, the machine authentication connection is dropped and the user login is used instead. When the user logs off, the machine connection is reestablished.

Junos Pulse Connection Realm and Role Preferences for Machine Authentication

When a Junos Pulse connection is configured to use machine authentication, any prompts that occur during the login process cause the connection to fail. For example, if the Pulse server authentication policy allows a user to select a realm or a role during the login process, Pulse presents a dialog box to the user and prompts for the realm or role selection. To avoid failed connections due to prompts during machine authentication you can specify a preferred role and realm for a Pulse connection.

For a Pulse connection that is used for machine authentication, you *do not* need to specify the preferred role if any of the following conditions are true:

- Users are mapped to only one role.
- Users are mapped to more than one role, but the realm's role mapping properties are set to merge settings for all assigned roles.

For a Pulse connection that is used for machine authentication, you *must* specify the preferred realm if the authentication sign-in policy allows the user to select a realm. If that realm maps to only one role, you do not need to specify the role.

For a Pulse connection that is used for machine authentication, you *must* specify the preferred role if any of the following conditions are true:

- The realm that the user connects to maps to more than one role and the realm's role mapping properties are set to require that the user must select a role. The preferred role set must be the name of a role assigned in that realm.
- The realm that the user connects to maps to more than one role and the realm's role mapping properties are defined by role mapping rules. You specify the preferred role by specifying the name of a **rule** that assigns the role set. [Figure 31 on page 313](#) shows a role mapping rule with the rule name highlighted.

Figure 31: Junos Pulse Role Mapping Rule

User Authentication Realms >
PulseFullClient

General Authentication Policy Role Mapping

Specify how to assign roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

New Rule... Duplicate Delete Save Changes

	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/>	1. matches expression "Not-Employee-or-Not-Appvd-Contractor"	→ IT Deny Access (Not FTE / Appr. PVC or Authorised tester)	Not-Employee-or-Not-Appvd-Contractor	✓
<input type="checkbox"/>	2. attribute "userAccountControl" is "614", "646", "66054" or "66084"	→ IT Disabled Account	Disabled Account	✓

When more than one role is assigned to a user:

- Merge settings for all assigned roles
- User must select from among assigned roles
- User must select the sets of merged roles assigned by each rule

When you create a Pulse connection for machine authentication, you must use the connection type **SSL VPN or UAC (L3)**. To identify the connection as a machine authentication connection, you specify how the connection is established using one of the following options:

- **Automatically when the machine starts. Machine credentials used for authentication**

This option uses the machine credentials defined in Active Directory for the machine login process and uses the same credentials for user login. When you select this option, the Realm and Role Set Preferences enable you to specify the following options:

- **Preferred Machine Realm**—Type the realm name that maps to the role you want to assign.
- **Preferred Machine Role Set**—Type the name of the role. The role must be one that is identified in the realm's role mapping properties. Or specify the name of a role mapping rule that assigns the role set.

- **Automatically when the machine starts. Connection is authenticated again when the user signs in into the desktop**

This option uses the Active Directory machine credentials for the machine login process. When machine login is complete, Pulse drops that connection and then uses the user credentials for user login. When you select this option, the Realm and Role Set Preferences enable you to specify the following options:

- **Preferred Machine Realm**—Type the realm name that maps to the role you want to assign.
- **Preferred Machine Role Set**—Type the name of the role. The role must be one that is identified in the realm's role mapping properties. Or specify the name of a role mapping rule that assigns the role set.

- **Preferred User Realm**—Type the realm name that maps to the role you want to assign.
- **Preferred User Role Set**—Type the name of the role. The role must be one that is identified in the realm's role mapping properties. Or specify the name of a role mapping rule that assigns the role set.



NOTE: Realm and role prompts are not the only prompts that are possible during the login process. If the Pulse connection has the Dynamic Certificate Trust option enabled, and there is an issue with the server certificate, Pulse asks the user if it is Ok to proceed. That certificate prompt causes a machine connection to fail. Note that the Pulse prompt for upgrading Pulse software is presented after the user connection is established and it will not affect a machine authentication connection.

Related Documentation

- [Role Mapping Rules on page 308](#)
- [Policies, Rules & Restrictions, and Conditions Overview on page 72](#)

Using the LDAP Server Catalog

The LDAP server catalog is a secondary window through which you specify additional LDAP information for Secure Access to use when mapping users to roles, including:

- **Attributes**—The Server Catalog Attributes tab shows a list of common LDAP attributes, such as cn, uid, uniquemember, and memberof. This tab is accessible only when accessing the Server Catalog of an LDAP server. You can use this tab to manage an LDAP server's attributes by adding custom values to and deleting values from its Secure Access server catalog. Note that Secure Access maintains a local copy of the LDAP server's values; attributes are not added to or deleted from your LDAP server's dictionary.
- **Groups**—The Server Catalog Groups tab provides a mechanism to easily retrieve group information from an LDAP server and add it to the server's Secure Access server catalog. You specify the BaseDN of your groups and optionally a filter to begin the search. If you do not know the exact container of your groups, you can specify the domain root as the BaseDN, such as dc=juniper, dc=com. The search page returns a list of groups from your server, from which you can choose groups to enter into the Groups list.



NOTE: The BaseDN value specified in the LDAP server's configuration page under "Finding user entries" is the default BaseDN value. The Filter value defaults to (cn=*).

You can also use the Groups tab to specify groups. You must specify the Fully Qualified Distinguished Name (FQDN) of a group, such as cn=GoodManagers, ou=HQ, ou=Juniper, o=com, c=US, but you can assign a label for this group that appears in the Groups list. Note that this tab is accessible only when accessing the Server Catalog of an LDAP server.

- **Expressions**—The Server Catalog Expressions tab provides a mechanism to write custom expressions for the role mapping rule.

To display the LDAP server catalog:

- After choosing the User attribute option on the Role Mapping Rule page, click **Update** to display the Attribute list and the Attributes button.
- Click the **Attributes** button to display the LDAP server catalog. (You can also click **Groups** after choosing the Group membership option, or click **Expressions** after choosing the Custom Expressions option.)

Figure 32: Server Catalog > Attributes Tab — Adding an Attribute for LDAP

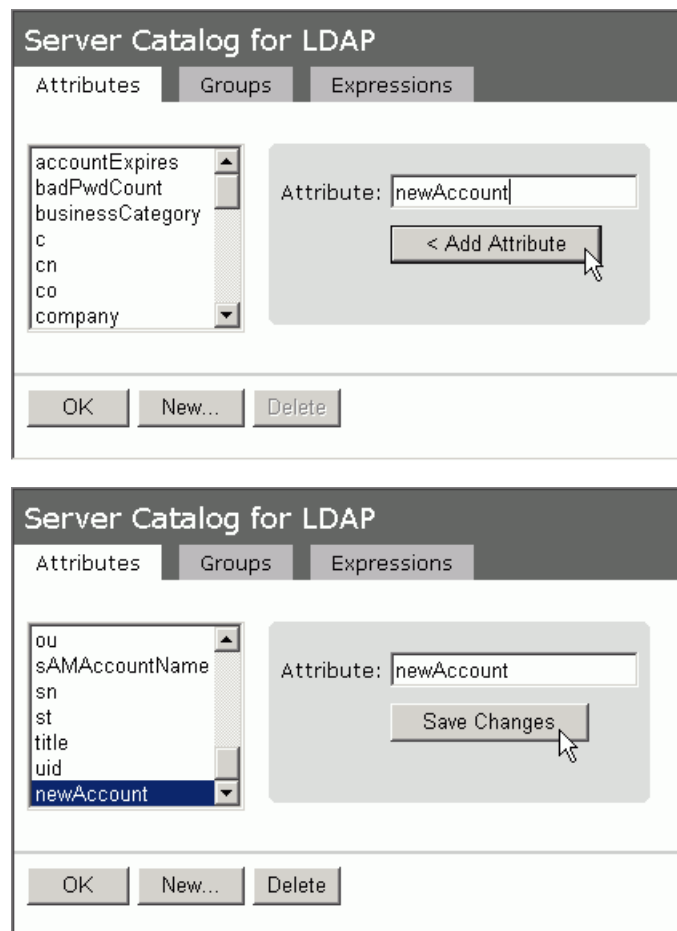


Figure 33: Server Catalog > Groups Tab — Adding LDAP Groups

Server Catalog for Win2K QA Active Directory Server

Attributes Groups Expressions

To add a group, type a name and click Add Group. To edit an existing group, select it, make your changes and click Save Changes. When you are done, click OK.

(none)

Name:

Group:

Enter group as DOMAIN/GroupName

< Add Group

OK New... Delete Search...

Group search for LDAP

To search the LDAP server, specify a base DN and a filter, and click Search.

Base DN:

Filter:

Search

Add Selected Back

Matching DNs		Type
<input type="checkbox"/>	CN= vmware ,CN=Users,DC=QA,DC=danastreet,DC=net	static
<input checked="" type="checkbox"/>	CN=Account Operators,CN=Builtin,DC=QA,DC=danastreet,DC=net	static
<input type="checkbox"/>	CN=Administrators,CN=Builtin,DC=QA,DC=danastreet,DC=net	static
<input type="checkbox"/>	CN=AutoTest,DC=QA,DC=danastreet,DC=net	static
<input checked="" type="checkbox"/>	CN=Backup Operators,CN=Builtin,DC=QA,DC=danastreet,DC=net	static
<input type="checkbox"/>	CN=Cert Publishers,CN=Users,DC=QA,DC=danastreet,DC=net	static

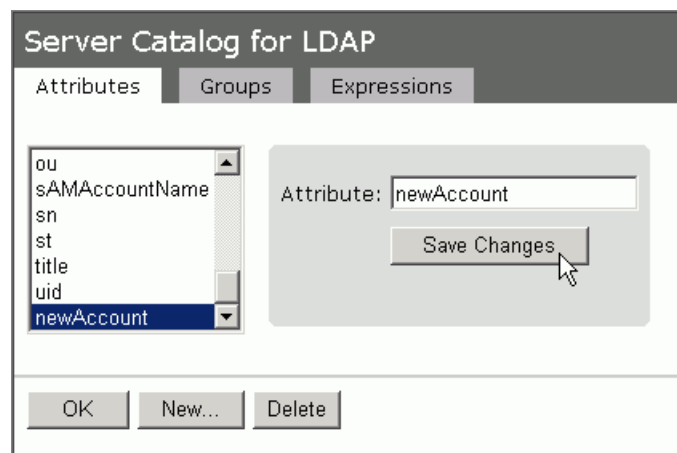
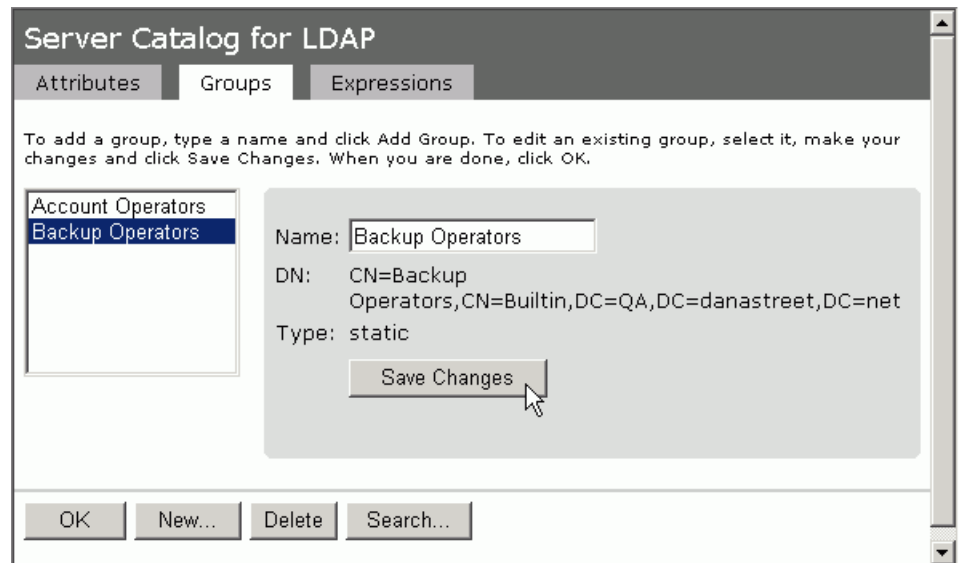
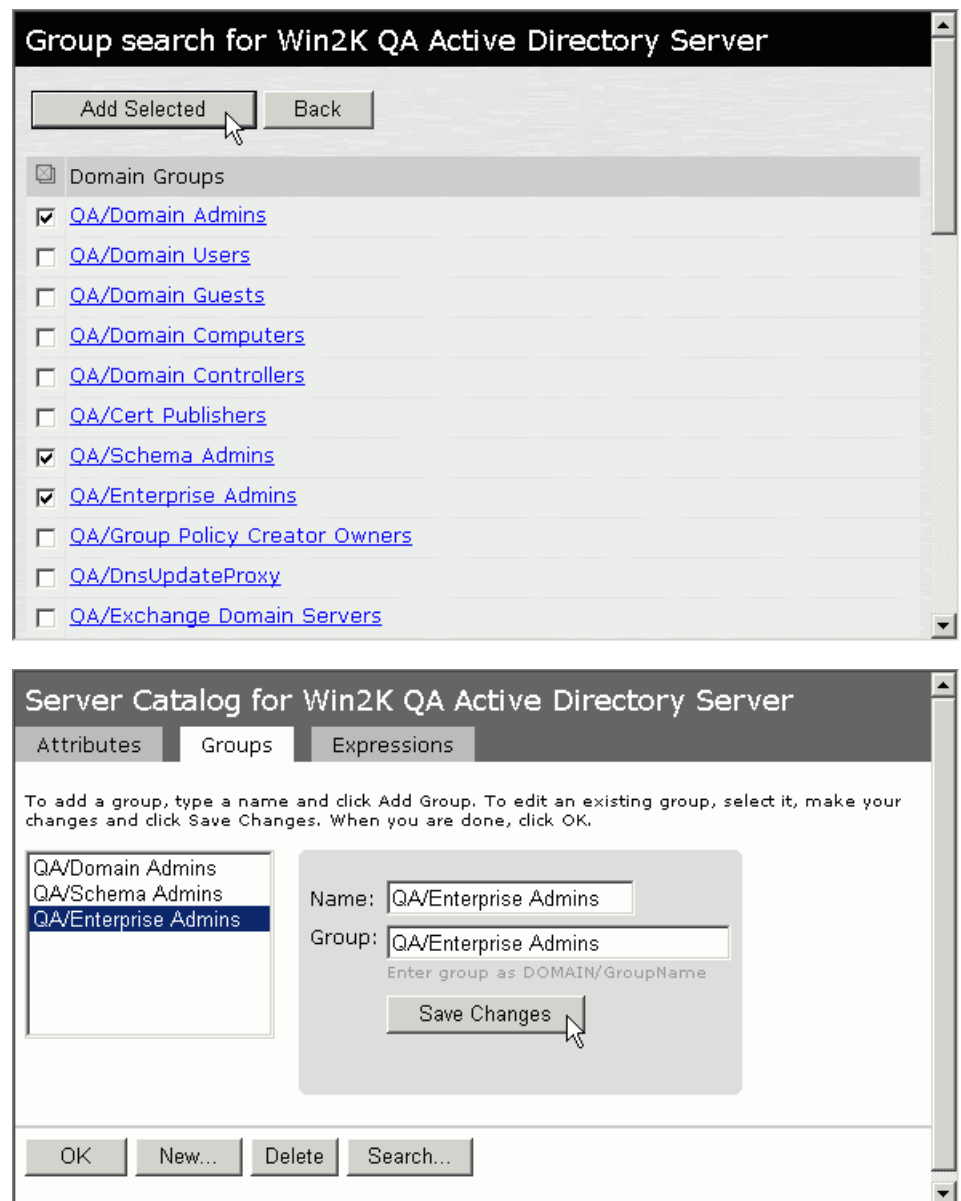


Figure 34: Server Catalog > Groups Tab — Adding Active Directory Groups



Related Documentation

- [Specifying Role Mapping Rules for an Authentication Realm on page 309](#)
- [Custom Expressions on page 1181](#)

Customizing User Realm UI Views

You can use customization options on the User Authentication Realms page to quickly view the settings that are associated with a specific realm or set of realms. For instance, you can view the role-mapping rules that you have associated with all your user realms.

Additionally, you can use these customized views to easily link to the authentication policies, servers, role-mapping rules, and roles associated with a user realms.

To view a sub-set of data on the User Authentication Realms page:

1. Select one of the following options from the View menu:
 - **Overview**—Displays the authentication servers and dynamic policy evaluation settings that you have set for the specified user realms. You may also use this setting to link to the specified server configuration pages.
 - **Authentication Policy**—Displays Host Checker and Cache Cleaner restrictions that you have enabled for the specified user realms. You may also use this setting to link to the specified Host Checker and Cache Cleaner configuration pages.
 - **Role Mapping**—Displays rule conditions and corresponding role assignments that you have enabled for the specified user realms. You may also use this setting to link to the specified rule conditions and role assignments configuration pages.
 - **Servers**—Displays authentication server names and corresponding types that you have enabled for the specified user realms. You may also use this setting to link to the specified server configuration pages.
 - **Roles**—Displays role assignments and corresponding permissive merge settings that you have enabled for the specified user realms.
2. Select one of the following options from the for list:
 - **All realms**—Displays the selected settings for all user realms.
 - **Selected realms**—Displays the selected settings for the user realms you choose. If you select this option, select one or more of the check boxes in the Authentication Realm list.
3. Click **Update**.

Sign-In Policies

- [About Sign-In Policies on page 321](#)
- [Task Summary: Configuring Sign In Pages on page 324](#)
- [About Configuring Sign In Policies on page 324](#)
- [Configuring User Sign In Policies on page 324](#)
- [About Sign-In Notifications on page 327](#)
- [Configuring and Implementing Sign-in Notifications on page 328](#)
- [Defining Authorization-Only Access Policies on page 330](#)
- [Defining Meeting Sign-In Policies on page 331](#)
- [Configuring Sign-In Pages on page 333](#)

About Sign-In Policies

Sign-in policies define the URLs that users and administrators use to access the Secure Access Service and the sign-in pages that they see. The Secure Access Service has two types of sign-in policies—one for users and one for administrators. When configuring sign-in policies, you associate realms, sign-in pages, and URLs.

For example, in order to allow all users to sign in to the Secure Access Service, you must add all user authentication realms to the user sign-in policy. You may also choose to modify the standard URL that the end-users use to access the Secure Access Service and the sign-in page that they see. Or, if you have the proper license, you can create multiple user sign-in policies, enabling different users to sign into different URLs and pages.

Additionally, appliances equipped with a Junos Pulse Collaboration license come with a meeting URL. You can use this URL to control the sign-in page that users see when they sign into a meeting on the Secure Access Service. If you have the proper license, you may also create additional meeting sign-in pages, enabling different Junos Pulse Collaboration users to sign into different URLs and pages.

You can create multiple sign-in policies, associating different sign-in pages with different URLs. When configuring a sign-in policy, you must associate it with a realm or realms. Then, only members of the specified authentication realm(s) may sign in using the URL defined in the policy. Within the sign-in policy, you may also define different sign-in pages to associate with different URLs.

For example, you can create sign-in policies that specify:

- Members of the “Partners” realm can sign in to the Secure Access Service using the URLs: **partner1.yourcompany.com** and **partner2.yourcompany.com**. Users who sign into the first URL see the “partners1” sign-in page; users who sign into the second URL see the “partners2” sign-in page.
- Members of the “Local” and “Remote” realms can sign into the Secure Access Service using the URL: **employees.yourcompany.com**. When they do, they see the “Employees” sign-in page.
- Members of the “Admin Users” realm can sign into the Secure Access Service using the URL: **access.yourcompany.com/super**. When they do, they see the “Administrators” sign-in page.

When defining sign-in policies, you may use different host names (such as **partners.yourcompany.com** and **employees.yourcompany.com**) or different paths (such as **yourcompany.com/partners** and **yourcompany.com/employees**) to differentiate between URLs.



NOTE: If a user attempts to sign in while there is another active user session with the same sign-in credentials, the Secure Access Service displays a warning page showing the IP address of the existing session and two buttons: Continue and Cancel. By clicking the Cancel button, the user terminates the current sign-in process and redirects the user back to the Sign-in page. By clicking the Continue button, the Secure Access Service creates the new user session and terminates the existing session.



NOTE: When enabling multiple sign-in URLs, note that in some cases the Secure Access Service must use cookies on the user's machine to determine which sign-in URL and corresponding sign-in page to display to the user. The Secure Access Service creates these cookies when the user signs into the Secure Access Service. (When a user signs into the Secure Access Service, the Secure Access Service responds with a cookie that includes the sign-in domain of the URL. The Secure Access Service then attaches this cookie to every Secure Access Service request the user makes.) Generally, these cookies ensure that the Secure Access Service displays the correct sign-in URL and page to the user. For example, if a user signs into the Secure Access Service using the URL `http://yourcompany.net/employees` and then her session times out, the Secure Access Service uses the cookie to determine that it must display the `http://yourcompany.net/employees` sign-in URL and corresponding page to the user when she requests another Secure Access Service resource.

However, in isolated cases, the cookie on the user's machine may not match the resource she is trying to access. The user may sign into one URL and then try to access a resource that is protected by a different URL. In this case, the Secure Access Service displays the sign-in URL and corresponding sign-in page that the user signed into most recently. For example, a user may sign into the Secure Access Service using the sign-in URL

`http://yourcompany.net/employees`. Then she may try to access the Secure Access Service resource using a link on an external server, such as `https://yourcompany.net/partners/dana/term/winlaunchterm.cgi?host=<termsrvIP>`. Or, she may try to open a bookmark that she created during a different session, such as

`https://yourcompany.net/partners/DanaInfo=.awxyBmszGr3xt1r5O3v.,SSO=U+`. In these cases, the Secure Access Service would display the

`http://yourcompany.net/employees` sign-in URL and page to the user, rather than the sign-in URL or page that is associated with the external link or saved bookmark that she is trying to access.

Sign-in policies and pages are an integral part of the Secure Access Service access management framework, and therefore are available on all Secure Access products. However, note that the following advanced sign-in features are not available on the SA 700:

- The ability to create multiple sign-in policies.
- The ability to create sign-in pages for Junos Pulse Collaboration users.
- The ability to create and upload custom sign-in pages to the Secure Access Service.

Related Documentation

- [Task Summary: Configuring Sign In Pages on page 324](#)
- [Defining Meeting Sign-In Policies on page 331](#)
- [Configuring User Sign In Policies on page 324](#)

Task Summary: Configuring Sign In Pages

To configure sign-in policies, you must:

1. Create an authentication realm through the Administrators > Admin Realms or the Users > User Realms page of the admin console.
2. (Optional) Modify an existing sign-in page or create a new one using options in the Authentication > Signing In > Sign-in Pages page of the admin console.
3. (Optional) Modify an existing sign-in page or create a new one using options in the Authentication > Signing In > Sign-in Pages page of the admin console.
4. Specify a sign-in policy that associates a realm, sign-in URL, and sign-in page using settings in the Authentication > Signing In > Sign-in Policies page of the admin console.
5. If you differentiate between URLs using host names, you must associate each host name with its own certificate or upload a wildcard certificate into Secure Access using options in the System > Configuration > Certificates > Device Certificates page.

Related Documentation

- [About Configuring Sign In Policies on page 324](#)
- [Configuring User Sign In Policies on page 324](#)
- [Defining Meeting Sign-In Policies on page 331](#)

About Configuring Sign In Policies

User sign-in policies also determine the realm(s) that users and administrators can access.

Depending on whether a sign-in policy is for endpoints (users) or administrators, the configuration options are different. For users, different authentication protocol sets can be configured, and realm selection is based on the authentication method that is associated with the realm.

Related Documentation

- [Configuring User Sign In Policies on page 324](#)
- [Defining Meeting Sign-In Policies on page 331](#)

Configuring User Sign In Policies

To create or configure user sign-in policies:

1. In the admin console, select **Authentication > Signing In > Sign-in Policies**.
2. To create a new sign-in policy, click **New URL**. Or, to edit an existing policy, click a URL in the **Administrator URLs** or **User URLs** column.
3. Select Users or Administrators to specify which type of user can sign into Secure Access using the access policy.

4. In the **Sign-in URL** field, enter the URL that you want to associate with the policy. Use the format `<host>/<path>` where `<host>` is the host name of the Secure Access device, and `<path>` is any string you want users to enter. For example: `partner1.yourcompany.com/outside`. To specify multiple hosts, use the `*` wildcard character.

To specify that all administrator URLs should use the sign-in page, enter `*/admin`.



NOTE:

- You may only use wildcard characters (`*`) in the beginning of the host name portion of the URL. Secure Access does not recognize wildcards in the URL path.
- SAML authentication does not support sign-in URLs that contain multiple realms. Instead, map each sign-in URL to a single realm.

5. (optional) Enter a Description for the policy.
6. From the Sign-in Page list, select the sign-in page that you want to associate with the policy. You may select the default page that comes with Secure Access, a variation of the standard sign-in page, or a custom page that you create using the customizable UI feature.
7. (User URLs only) In the Meeting URL field, select the meeting URL that you want to associate with this sign-in policy. Secure Access applies the specified meeting URL to any meeting created by a user who signs into this user URL.
8. Under Authentication realm, specify which realm(s) map to the policy, and how users and administrators should pick from amongst realms. If you select:
 - User types the realm name—Secure Access maps the sign-in policy to all authentication realms, but does not provide a list of realms from which the user or administrator can choose. Instead, the user or administrator must manually enter his realm name into the sign-in page.
 - User picks from a list of authentication realms—Secure Access only maps the sign-in policy to the authentication realms that you choose. Secure Access presents this list of realms to the user or administrator when he signs-in to Secure Access and allows him to choose a realm from the list. (Note that Secure Access does not display a drop-down list of authentication realms if the URL is only mapped to one realm. Instead, it automatically uses the realm you specify.)



NOTE: If you allow the user to pick from multiple realms and one of those realms uses an anonymous authentication server, Secure Access does not display that realm in the drop-down realm list. To effectively map your sign-in policy to an anonymous realm, you must add only that realm to the Authentication realm list.

9. Click **Save Changes**.

Enabling and Disabling Sign-In Policies

To enable and disable sign-in policies:

1. In the admin console, choose **Authentication > Signing In > Sign-in Policies**.
2. To enable or disable:
 - **An individual policy**—Select the check box next to the policy that you want to change, and then click Enable or Disable.
 - **All user and meeting policies**—Select or deselect the **Restrict access to administrators only** check box at the top of the page.

If you select this option, all user sessions are immediately terminated. If this device is part of a cluster, all user sessions across all nodes in the cluster are immediately terminated.

3. Click **Save Changes**.

Specifying the Order in Which Sign-In Policies are Evaluated

Secure Access evaluates sign-in policies in the same order that you list them on the Sign-in Policies page. When it finds a URL that matches exactly, it stops evaluating and presents the appropriate sign-in page to the administrator or user. For example, you may define two administrator sign-in policies with two different URLs:

- The first policy uses the URL `*/admin` and maps to the default administrator sign-in page.
- The second policy uses the URL `yourcompany.com/admin` and maps to a custom administrator sign-in page.

If you list the policies in this order on the Sign-in Policies page, Secure Access never evaluates or uses the second policy because the first URL encompasses the second. Even if an administrator signs in using the `yourcompany.com/admin` URL, Secure Access displays the default administrator sign-in page. If you list the policies in the opposite order, however, Secure Access displays the custom administrator sign-in page to those administrators who access Secure Access using the `yourcompany.com/admin` URL.

Note that Secure Access only accepts wildcard characters in the host name section of the URL and matches URLs based on the exact path. For example, you may define two administrator sign-in policies with two different URL paths:

- The first policy uses the URL `*/marketing` and maps to a custom sign-in page for the entire Marketing Department.
- The second policy uses the URL `*/marketing/joe` and maps to a custom sign-in page designed exclusively for Joe in the Marketing Department.

If you list the policies in this order on the Sign-in Policies page, Secure Access displays Joe's custom sign-in page to him when he uses the `yourcompany.com/marketing/joe` URL to access Secure Access. He does not see the Marketing sign-in page, even though it is listed and evaluated first, because the path portion of his URL does not exactly match the URL defined in the first policy.

To change the order in which administrator sign-in policies are evaluated:

1. In the admin console, choose **Authentication > Signing In > Sign-in Policies**.
2. Select a sign-in policy in the **Administrator URLs**, **User URLs** or **Meeting URLs** list.
3. Click the up and down arrows to change the selected policy's placement in the list.
4. Click **Save Changes**.

**Related
Documentation**

- [About Configuring Sign In Policies on page 324](#)

About Sign-In Notifications

With sign-in notifications, you can create and configure detailed notification messages that appear for Pulse clients and for agentless access endpoints when the user attempts to sign in. For example, you could configure a notification message that explains terms of use, company-specific policies, a welcome page, an end user license agreement (EULA), or a message of the day (MOTD).

For a browser-based (agentless) login, the notification message appears in a separate page either before (pre-auth) or after (post-auth) user authentication during the sign-in process. For a Pulse client login, the notification messages appear in a Pulse message box. The user is expected to read the content of the sign-in notification message and acknowledge by clicking a Proceed button. The user can indicate disagreement by clicking a Decline button, which ends the login attempt.

You can configure a sign-in policy to use a sign-in notification either as pre-auth or post-auth (or both). In the case of post-auth configuration, you can either use a common message for all roles or use separate messages for each role.

You can create a multi-language sign-in notification package that relies on the language setting of the endpoint. You can customize the sign-in notification page appearance for browser-based logins by modifying the related fields in a sign-in page in the Admin UI or by using a custom sign-in page.

Notes:

- Sign-in notifications are supported on Windows, Mac, and for browser-based access on mobile devices. However, sign-in notifications might not work well with all mobile devices due to device limitations.
- Sign-in notifications (including uploaded packages) are included in XML exports.
- If a Pulse session is resumed or extended, the pre-auth notification message is not shown again. However, if the user switches roles when resuming a session, and that role change results in a new notification, Pulse displays the message. You can configure the post-auth message to be skipped if it has already been seen. If the post-auth message is not marked to be skipped, then it always appears.

**Related
Documentation**

- [Configuring and Implementing Sign-in Notifications on page 328](#)

Configuring and Implementing Sign-in Notifications

Sign-in notifications appear for Pulse client and for browser-based logins when the user attempts to sign in.

To configure and implement sign-in notifications:

1. In the admin console, select **Authentication > Signing In > Sign-in Notifications**.
2. Click **New Notification**.
3. Specify a Name for the notification. This name appears in the sign-in policies page, and in the UI Options page for a selected role.
4. Select **Text** or **Package** in the Type box.
 - If you select **Text**, type the desired sign-in notification message, or copy and paste the relevant text into the Text field.
 - If you select **Package**, click the **Browse** button and navigate to a previously prepared .zip file. A package is typically used to provide different language versions of the notification message.
 - The zip file should include a default.txt file and one or more <language>.txt files (Example: en.txt).
 - Language-abbreviations should be strings that can appear in Accept-Language header of an HTTP request.
 - The character encoding supported is UTF-8.



NOTE: When you create a zip file, do not add the folder containing the files, but add the files directly.

5. Click **Save Changes**.

To enable sign-in notifications:

1. In the admin console, click **Authentication > Signing In > Sign-in Policies**.
2. Select an existing URL or create a new URL.
3. Under Configure Sign-in Notifications, select the check box for **Pre-Auth Sign-in Notification**, **Post-Auth Sign-in Notification**, or both.
 - After Pre-Auth Sign-in Notification, select a previously configured sign-in notification from the drop-down menu.
 - After Post-Auth Sign-in Notification, select the option for **Use a common Sign-in Notification for all roles** or **Use the Sign-in Notification associated to the assigned role**.
 - If you select **Use a common Sign-in Notification for all roles**, select a previously configured sign-in notification from the drop-down menu.

- If you select **Use the Sign-in Notification associated to the assigned role**, the sign-in notification configured for the assigned role will be used.
 - Prevent the Post-Auth sign-in notification from being displayed to users who have seen it before, by selecting the **Skip if already shown** check box. (This is only a hint to the system and might not be honored in all environments.)
4. Click **Save Changes**.
 5. You can customize the appearance of the sign-in notification message by selecting **Authentication > Signing In > Sign-in Pages** and creating a sign-in page or using an existing page.
 6. Under Sign-in Notification appearance, customize UI options for Pre-Auth Notifications and Post-Auth Notifications by changing the following items:
 - For **Notification Title** enter the text that appears at the top of the sign-in notification page.
 - In the **Proceed Button** box, enter the text for the button that the user clicks to proceed with the sign-in.

This text applies to browser-based logins only. A Pulse client login always displays Proceed.
 - Optionally, clear the check box for **Display "Decline" Button**. If this box is not checked, the user does not have the option to decline.
 - In the **Decline Button** box, enter the text for the button that the user clicks to decline.

This text applies to browser-based logins only. A Pulse client login always displays Decline.
 - In the **Message on Decline** box, enter the text that you would like to appear when a user clicks the Decline button.
 7. Click **Save Changes**.



NOTE: If you enabled **Use the Sign-in Notification associated to the assigned role** you must complete the implementation by selecting the sign-in notification on the **Users > User Roles > Role Name > General > UI Options** page or **Administrators > Admin Roles > Role Name > General > UI Options** page, as applicable.

If more than one role is available to a user, the sign-in notification associated with the first role assigned is displayed.

8. Add the sign-in page in which you have customized the sign-in notification appearance to the sign-in policy.

Related Documentation

- [About Sign-In Notifications on page 327](#)

Defining Authorization-Only Access Policies

Authorization-only access is similar to a reverse proxy. Typically, a reverse proxy is a proxy server that is installed in front of web servers. All connections coming from the Internet addressed to one of the web servers are routed through the proxy server, which may either deal with the request itself or pass the request wholly or partially to the main web server. Up to 1000 concurrent connections is supported on an SA 6500.

With an authorization-only access, you select a user role. Secure Access then acts as reverse proxy server and performs authorization against the Netegrity SiteMinder server for each request.

For example, the authorization-only access feature satisfies the following business needs:

- If you have a third-party AAA policy management server (like Netegrity), Secure Access acts as an authorization-only agent.
- If your user sessions are managed by a third-part session management system, there is no need to duplicate the user session management in Secure Access.

With authorization-only access, there is no SSO from Secure Access. SSO is controlled by your third-party AAA infrastructure.



NOTE: Before defining this policy, you must first configure your Netegrity server and define your hostnames in the Network Configuration page.

You must also specify settings in the SiteMinder authorization settings section of the SiteMinder authentication server page. Users are redirected to the URL specified in the If Automatic Sign In fails, redirect to field when the SMSESSION cookie validation fails or if no SMSESSION cookie exists. Users are redirected to the URL specified in the If authorization fails, redirect to field when an access denied error occurs.

To create or configure authorization-only access policies:

1. In the admin console, choose **Authentication > Signing In > Sign-in Policies**.
2. To create a new authorization only access policy, click **New URL** and select **authorization only access**. Or, to edit an existing policy, click a URL in the Virtual Hostname column.
3. In the Virtual Hostname field, enter the name that maps to Secure Access's IP address. The name must be unique among all virtual hostnames used in pass-through proxy's hostname mode. The hostname is used to access backend application entered in the Backend URL field. Do not include the protocol (for example, http:) in this field.

For example, if the virtual hostname is myapp.ivehostname.com, and the backend URL is http://www.xyz.com:8080/, a request to https://myapp.ivehostname.com/test1 via Secure Access is converted to a request to http://www.xyz.com:8080/test1. The response of the converted request is sent to the original requesting web browser.

- In the Backend URL field, enter the URL for the remote server. You must specify the protocol, hostname and port of the server. For example, `http://www.mydomain.com:8080/*`.

When requests match the hostname in the Virtual Hostname field, the request is transformed to the URL specified in the Backend URL field. The client is directed to the backend URL unaware of the redirect.

- (optional) Enter a Description for this policy.
- Select the server name or **No Authorization** from the Authorization Server drop down menu. If you select a server, ensure that the front-end server provides the SMSESSION cookie otherwise you will receive an error.
- Select a user role from the Role Option drop down menu.

Only the following user role options are applicable for authorization-only access.

- Allow browsing un-trusted SSL websites (Users > User Roles > *RoleName* > Web > Options > View advanced options)
- HTTP Connection Timeout (Users > User Roles > *RoleName* > Web > Options > View advanced options)
- Source IP restrictions (Users > User Roles > *RoleName* > General > Restrictions)
- Browser restrictions (Users > User Roles > *RoleName* > General > Restrictions)

Ensure the user role you select has an associated Web Access policy.

- Select the **Allow ActiveSync Traffic only** option to perform a basic of validation of the HTTP header to ensure the request is consistent with ActiveSync protocol. If you select this option only ActiveSync protocol requests can be processed. If validation fails, a message is created in the user's event log. If you do not select this option, both ActiveSync and non-ActiveSync requests are processed.
- Click **Save Changes** to save your edits.

The System Status Overview page displays the number of current active concurrent connections and a histogram of the active concurrent connections (Authorization Only Access Active Connections plot in the Concurrent SSL Connections graph).

Related Documentation

- [eTrust SiteMinder Overview on page 207](#)
- [Specifying Web Browsing Options on page 515](#)
- [Specifying Browser Access Restrictions on page 82](#)

Defining Meeting Sign-In Policies

To create or configure meeting sign-in policies:

- In the admin console, choose **Authentication > Authentication > Signing In Policies**.
- To create a new sign-in policy, click **New URL**. Or, to edit an existing policy, click a URL in the Meeting URLs column.

3. Select **Meeting**.

4. In the Sign-in URL field, enter the URL that you want to associate with the meeting policy. Use the format <host>/<path> where <host> is the host name of the Secure Access device, and <path> is any string you want users to enter. For example: Partner1.YourCompany.com/OnlineConference. When creating the meeting URL, note that:

- You cannot modify the URL of the default meeting URL (* /meeting) that comes with the product.
- If you want to enable users to sign into meetings using all of the host names defined in the associated user URL, use the * wildcard character in your meeting URL definition. For example, you might associate the following hosts with your user URL:
 - YourInternalServer.YourCompany.net
 - YourExternalServer.YourCompany.com

Then, if you create an */OnlineConference meeting URL definition and associate it with the user URL, users can access the meeting sign-in page using either of the following URLs:

- <http://YourInternalServer.YourCompany.net/OnlineConference>
- <http://YourExternalServer.YourCompany.com/OnlineConference>
- If you create a meeting URL that includes the * wildcard character and enable email notifications, Secure Access constructs the meeting URL in the notification email using the host name specified by the user when signing into Secure Access. For instance, a user might sign into Secure Access using the following URL from the previous example:

<http://YourInternalServer.YourCompany.net>

Then, if the user creates a meeting, Secure Access specifies the following sign-in URL for that meeting in the email notification:

<http://YourInternalServer.YourCompany.net/OnlineConference>

Note that since the email link references an internal server, out-of-network users cannot access the meeting.

- If you only want to enable users to sign into meetings using a sub-set of the host names defined in the associated user URL, or if you want to require users to use a completely different URL to sign into meetings, do not include the * wildcard character in your meeting URL definition. Instead, create a unique and specific meeting URL definition.

For instance, you can create the following meeting URL definition and associate it with the user URL from the previous example in order to specify that all meetings contain links to the external server only:

YourExternalServer.YourCompany.com/OnlineConference

5. (optional) Enter a Description for the policy.

6. From the Sign-in Page list, select the sign-in page(s) that you want to appear to users who access meetings using this policy. You may select the default pages that come with Secure Access, a variation of the standard sign-in pages, or customized pages that you create using the customizable UI feature.
7. Click **Save Changes**.

Related Documentation

- [Configuring Sign-In Pages on page 333](#)

Configuring Sign-In Pages

A *sign-in page* defines the customized properties in the end-user's welcome page such as the welcome text, help text, logo, header, and footer. The Secure Access Service allows you to create two types of sign-in pages to present to users and administrators:

- **Standard sign-in pages**—Standard sign-in pages are produced by Juniper and are included with all versions of the Secure Access Service. You can modify standard sign-in pages through the Authentication > Signing In > Sign-in Pages tab of the admin console.
- **Customized sign-in pages**—Customized sign-in pages are THTML pages that you produce using the Template Toolkit and upload to the Secure Access Service in the form of an archived ZIP file. The customized sign-in pages feature enables you to use your own pages rather than having to modify the sign-in page included with the Secure Access Service.

For more information on customized sign-in pages, see

http://www.juniper.net/techpubs/en_US/release-independent/sa/information-products/pathway-pages/sa-series/product/.

Configuring Standard Sign-In Pages

Standard sign-in pages that come with the Secure Access Service include:

- **Default Sign-In Page**—the Secure Access Service displays this page to users when they sign into the Secure Access Service.
- **Meeting Sign-In Page**—the Secure Access Service displays this page to users when they sign into a meeting. This page is only available if you install a Junos Pulse Collaboration license on the Secure Access Service.

You can modify the default sign-in page that the Secure Access Service displays to users when they sign into the Secure Access Service. You can also create new standard sign-in pages that contain custom text, logo, colors, and error message text using settings in the Authentication > Signing In > Sign-in Pages tab of the admin console.

To create or modify a standard sign-in page:

1. In the admin console, select **Authentication > Signing In > Sign-in Pages**.
2. If you are:

- **Creating a new page**—Click **New Page**.
 - **Modifying an existing page**—Select the link corresponding to the page you want to modify.
3. (New pages only) Under Page Type, specify whether this is an administrator/user access page or a meeting page.
 4. Enter a name to identify the page.
 5. In the Custom text section, revise the default text used for the various screen labels as desired. When adding text to the Instructions field, note that you may format text and add links using the following HTML tags: `<i>`, ``, `
`, ``, and `<a href>`. However, the Secure Access Service does not rewrite links on the sign-in page (since the user has not yet authenticated), so you should only point to external sites. Links to sites behind a firewall will fail.

If you use unsupported HTML tags in your custom message, the Secure Access Service may display the end-user's Secure Access Service home page incorrectly.
 6. In the Header appearance section, specify a custom logo image file for the header and a different header color.
 7. In the Custom error messages section, revise the default text that is displayed to users if they encounter certificate errors.

You can include `<<host>>`, `<<port>>`, `<<protocol>>`, and `<<request>>` variables and user attribute variables, such as `<<userAttr.cn>>` in the custom error messages. Note that these variables must follow the format `<variable>` to distinguish them from HTML tags which have the format `<tag>`.
 8. To provide custom help or additional instructions for your users, select **Show Help button**, enter a label to display on the button, and specify an HTML file to upload to the Secure Access Service. Note that the Secure Access Service does not display images and other content referenced in this HTML page. (Not available for the Junos Pulse Collaboration sign-in page.)
 9. Click **Save Changes**. The changes take effect immediately, but users with active sessions might need to refresh their Web browsers.

Click **Restore Factory Defaults** to reset the sign-in page, Secure Access Service user home page, and admin console appearance.

**Related
Documentation**

- Custom Text HTML Tags

Single Sign-On

- [About Single Sign-On on page 335](#)
- [Task Summary: Configuring Multiple Authentication Servers on page 337](#)
- [Task Summary: Enabling SSO to Resources Protected by Basic Authentication on page 337](#)
- [Task Summary: Enabling SSO to Resources Protected by NTLM on page 338](#)
- [Multiple Sign-In Credentials Execution on page 339](#)
- [Understanding SAML 1.1 on page 344](#)
- [Configuring SAML 1.1 SSO Profiles on page 346](#)
- [Creating a SAML 1.1 SSO POST Profile on page 351](#)
- [Creating a SAML 1.1 ACL Resource Policy on page 354](#)
- [Creating a Trust Relationship Between SAML 1.1 Systems on page 357](#)

About Single Sign-On

Single sign-on (SSO) is a process that allows pre-authenticated Secure Access users to access other applications or resources that are protected by another access management system without having to re-enter their credentials.

Secure Access provides several integration mechanisms that allow you to configure SSO connections from the Secure Access to other servers, applications, and resources. SSO mechanisms include:

- **Remote SSO**—Secure Access provides loose integration with any application that uses a static POST action within an HTML form to sign in users. You can configure Secure Access to post Secure Access credentials, LDAP attributes, and certificate attributes to a Web-enabled application, as well as set cookies and headers, allowing users to access the application without re-authenticating.
- **SAML**—Secure Access provides loose integration with selected access management systems that use the Security Assertion Markup Language (SAML) to communicate with other systems. You can enable users to sign in to Secure Access and then sign in to and access resources protected by the access management system without re-authenticating. You can also enable users to sign in to another access management system and then access resources protected by Secure Access, without re-authenticating.

- Basic authentication and NTLM intermediation to Intranet sites—Secure Access allows you to automatically submit Secure Access user credentials to other Web sites and proxies within the same Intranet zone. When you enable basic authentication intermediation through the Users > Resource Profiles > Web Applications/Pages page of the admin console, Secure Access submits the cached credentials to Intranet Web sites whose host names end in the DNS suffix configured in the System > Network > Overview page. To maximize security, you may also configure Secure Access to use base-64 encoding to protect the cached credentials.
- Active Directory server—Secure Access allows you to automatically submit Active Directory SSO credentials to other Web sites and Windows file shares within the same Intranet zone that are protected by native NTLM authentication. When you enable this option, Secure Access submits cached credentials to NTLM-protected Web sites whose host names end in the DNS suffix configured in the System > Network > Overview page of the admin console.
- eTrust SiteMinder policy server—When you authenticate Secure Access users using a eTrust SiteMinder policy server, you can enable them access to SiteMinder protected resources without re-authenticating (provided they are authorized with the correct protection level). Additionally, you can re-authenticate users through Secure Access if they request resources for which their current protection level is inadequate and you can enable users to sign into the policy server first and then access Secure Access without re-authenticating.
- Terminal Sessions—When you enable the Terminal Services feature for a role, you allow users to connect to applications that are running on a Windows terminal server or Citrix MetaFrame server without re-authenticating. You may also pass a username to the Telnet/SSH server.
- Email clients—When you enable the Email Client feature for a role and then create a corresponding resource policy, you allow users to access standards-based email such as Outlook Express, Netscape Communicator, or Qualcomm's Eudora without re-authenticating.

Secure Access determines which credentials to submit to the SSO-enabled server, application, or resource based on the mechanism you use to connect. Most mechanisms allow you to collect user credentials for up to two authentication servers in the Secure Access sign-in page and then submit those credentials during SSO.

The remaining mechanisms (SAML, eTrust SiteMinder, and the Email Client) use unique methods for enabling SSO from Secure Access to the supported application.

About Multiple Sign-In Credentials

When configuring an authentication realm, you can enable up to two authentication servers for the realm. Enabling two authentication servers allows you to require two different sets of credentials—one for Secure Access and another for your SSO-enabled resource—without requiring the user to enter the second set of credentials when accessing the resource. It also allows you to require two-factor authentication in order to access Secure Access.

- Related Documentation**
- [Remote SSO Overview on page 494](#)
 - [Understanding SAML 1.1 on page 281](#)
 - [Defining a Single Sign-On Autopolicy on page 500](#)
 - [Defining an Active Directory or Windows NT Domain Server Instance on page 164](#)
 - [eTrust SiteMinder Overview on page 207](#)
 - [About Terminal Services on page 642](#)
 - [About the E-Mail Client on page 725](#)
 - [Multiple Sign-In Credentials Execution on page 339](#)

Task Summary: Configuring Multiple Authentication Servers

To enable multiple authentication servers:

1. Create authentication server instances through the Authentication > Auth. Servers page of the admin console.
2. Associate the authentication servers with a realm using settings in the following pages of the admin console:
 - Users > User Realms > *Select Realm* > General
 - Administrators > Admin Realms > *Select Realm* > General
3. (Optional) Specify password length restrictions for the secondary authentication server using settings in the following pages of the admin console:
 - Users > User Realms > *Select Realm* > Authentication Policy > Password
 - Administrators > Admin Realms > *Select Realm* > Authentication Policy > Password

- Related Documentation**
- [Authentication Realm Overview on page 305](#)
 - [Specifying Password Access Restrictions on page 85](#)

Task Summary: Enabling SSO to Resources Protected by Basic Authentication

To enable single sign-on to Web servers and Web proxies that are protected by basic authentication, you must:

1. Specify a Secure Access host name that ends with the same prefix as your protected resource using settings in the System > Network > Overview page of the admin console. (Secure Access checks the host names to ensure that it is only enabling SSO to sites within the same Intranet.)
2. Enable users to access Web resources, specify the sites to which you want Secure Access to submit credentials, create autopolicies that enable basic authentication intermediation single sign-on, and create bookmarks to the selected resources using

settings in the Users > Resource Profiles > Web Application/Pages > [Profile] page of the admin console.

3. If you want users to access Web servers through a proxy, configure Secure Access to recognize the appropriate servers and proxies using settings in the following pages of the admin console:
 - Use settings in Users > Resource Policies > Web > Web proxy > Servers page to specify which Web servers you want to protect with the proxy.
 - Use settings in the Users > Resource Policies > Web > Web proxy > Policies page to specify which proxies you want to use and which servers (above) you want the proxies to protect. You may specify individual resources on the server or the entire server.

Related Documentation

- [Task Summary: Enabling SSO to Resources Protected by NTLM on page 338](#)

Task Summary: Enabling SSO to Resources Protected by NTLM



NOTE: Secure Access supports web proxies that perform NTLM authentication. However, the following case is not supported: a proxy exists between Secure Access and the back-end server and the back-end server performs the NTLM authentication.

To enable single sign-on to Web servers, Windows file servers, and Web proxies that are protected by NTLM, you must:

1. Specify a Secure Access host name that ends with the same suffix as your protected resource using settings in the System > Network > Overview page of the admin console. (Secure Access checks the host names to ensure that it is only enabling SSO to sites within the same Intranet.)
2. Enable users to access the appropriate type of resource (Web or file), specify the sites or servers to which you want the Secure Access Service to submit credentials, create autopolicies that enable NTLM single sign-on, and create bookmarks to the selected resources using settings in the following pages of the admin console:
 - Users > Resource Profiles > Web Application/Pages > [Profile]
 - Users > Resource Profiles > File Browsing Resource Profiles > [Profile]
3. If you want users to access Web servers through a proxy, configure Secure Access to recognize the appropriate servers and proxies using settings in the following pages of the admin console:
 - a. Use settings in Users > Resource Policies > Web > Web proxy > Servers page to specify which Web servers you want to protect with the proxy.
 - b. Use settings in the Users > Resource Policies > Web > Web proxy > Policies page to specify which proxies you want to use and which servers (above) you want the

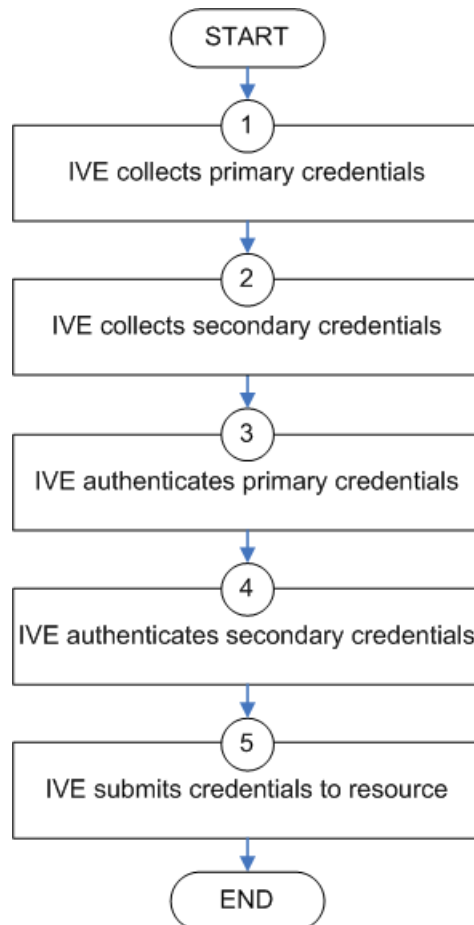
proxies to protect. You may specify individual resources on the server or the entire server.

- Related Documentation**
- [Task Summary: Enabling SSO to Resources Protected by Basic Authentication on page 337](#)

Multiple Sign-In Credentials Execution

The following diagram illustrates the process that Secure Access uses to collect and authenticate multiple user credentials and submit them to SSO-enabled resources. Each of the steps in the diagram are described in further detail in the sections that follow.

Figure 35: Collecting and Submitting Credentials from Multiple Servers



Step 1: Secure Access Collects the User's Primary Credentials

When the user signs in to Secure Access, Secure Access prompts him to enter his primary server credentials. Secure Access saves these credentials to submit to the SSO resource later, if necessary. Note that Secure Access saves the credentials exactly as the user

enters them—it does not pre-pend or append them with additional information such as the user's domain.

Step 2: Secure Access Collects or Generates the User's Secondary Credentials

You may configure Secure Access to either manually collect or automatically generate the user's secondary set of credentials. If you configure Secure Access to:

- Manually collect the user's secondary credentials—The user must enter his secondary credentials directly after entering his primary credentials.
- Automatically generate the user's credentials—Secure Access submits the values you specified in the administration console during setup. By default, Secure Access uses the <username> and <password> variables, which hold the username and password entered by the user for the primary authentication server.

For example, you may configure an LDAP server as your primary authentication server and an Active Directory server as your secondary authentication server. Then, you may configure Secure Access to infer the user's Active Directory username but require the user to manually enter his Active Directory password. When Secure Access infers the Active Directory username, it simply takes the name entered for the LDAP server (for example, JDoe@LDAPServer) and resubmits it to the Active Directory (for example, JDoe@ActiveDirectoryServer).

Step 3: Secure Access Authenticates the Primary Credentials

After Secure Access collects all required credentials, it authenticates the user's first set of credentials against the primary authentication server. Then:

- If the credentials successfully authenticate, Secure Access stores them in the <username> and <password> session variables and continues on to authenticate the secondary credentials.



NOTE: If you authenticate against a RADIUS server that accepts dynamic, time-sensitive passwords, you may choose to not store user passwords using the Secure Access session variable.

- If the credentials do not successfully authenticate, Secure Access denies the user access to the Secure Access appliance.

Step 4: Secure Access Authenticates the Secondary Credentials

After authenticating the primary credentials, Secure Access authenticates the secondary credentials. Then:

- If the credentials successfully authenticate, Secure Access stores them in the <username[2]> and <password[2]> session variables and allows the user access to Secure Access. You may also access these variables using the syntax <username@SecondaryServer> and <password@SecondaryServer>.



NOTE: If you authenticate against a RADIUS server that accepts dynamic, time-sensitive passwords, you may choose to not store user passwords using the Secure Access session variable.

- If the credentials do not successfully authenticate, Secure Access does not save them. Depending on how you configure your authentication realm, Secure Access may allow or deny the user access to Secure Access if his secondary credentials do not successfully authenticate.

You can detect that secondary authentication failed by creating a custom expression that checks for an empty `user@secondaryAuth` variable. You may want to do this so that you can assign users to roles based on successful authentication. For example, the following expression assigns users to the “MoreAccess” role if they successfully authenticate against the “ACE server” secondary authentication server:

`user@{ACE Server} != "" then assign role MoreAccess`

Note “Ace server” is shown in curly braces since the authentication server’s name contains spaces.

Step 5: Secure Access Submits Credentials to an SSO-Enabled Resource

After the user successfully signs in to Secure Access, he may try to access an SSO-enabled resource using a pre-configured bookmark or other access mechanism. Then, depending on which type of resource the user is trying to access, Secure Access submits different credentials. If the user is trying to access a:

- Web SSO, Terminal Services, or Telnet/SSH resource—Secure Access submits the credentials that you specify through the admin console, such as `<username>` (which submits the user’s primary credentials to the resource) or `<username[2]>` (which submits the user’s secondary credentials to the resource). Or, if the user has entered a different username and password through the end user console, Secure Access submits the user-specified credentials.



NOTE: Secure Access does not support submitting ACE server, certificate server, or anonymous server credentials to a Web SSO, terminal services, or Telnet/SSH resource. If you configure Secure Access to submit credentials from one of these types of primary authentication servers, Secure Access submits credentials from the user’s secondary authentication server instead. If these credentials fail, Secure Access prompts the user to manually enter his username and password.

- Resource protected by a Web server, Windows server, or Web proxy that is using NTLM authentication—Secure Access submits credentials to the backend server or proxy that is protecting the Web or file resource. Note that you cannot disable NTLM authentication through Secure Access—If a user tries to access a resource that is protected by NTLM, Secure Access automatically intermediates the authentication challenge and submits credentials in the following order:

- (Windows file resources only) Administrator-specified credentials—If you create a resource profile that specifies credentials for a Windows file resource and the user then accesses the specified resource, Secure Access submits the specified credentials.
- Cached credentials—If Secure Access does not submit administrator-specified credentials or the credentials fail, Secure Access determines whether it has stored credentials for the specified user and resource in its cache. (See below for information about when Secure Access caches credentials.) If available, Secure Access submits its stored credentials.
- Primary credentials—If Secure Access does not submit cached credentials or the credentials fail, Secure Access submits the user's primary Secure Access credentials provided that following conditions are true:
 - The resource is in the same Intranet zone as Secure Access (that is, the resource's host name ends in the DNS suffix configured in the System > Network > Overview page of the admin console).
 - (Web proxies only) You have configured Secure Access to recognize the Web proxy through settings in the Users > Resource Policies > Web > Web Proxy pages of the admin console.
 - The credentials are not ACE credentials.
 - (RADIUS credentials only) You specify in the RADIUS configuration page that the RADIUS server does not accept one-time passwords.
- Secondary credentials—If the primary credentials fail, Secure Access determines whether it has secondary credentials for the user. If available, Secure Access submits the user's secondary Secure Access credentials provided that the conditions described for primary credentials are true.
- Last-entered credentials—If Secure Access does not submit secondary credentials or if the credentials fail, Secure Access determines whether it has stored credentials for the specified user and a different resource in its cache. (See below for information about when Secure Access caches credentials.) If available, Secure Access submits its stored credentials provided the conditions described for primary credentials are true.
- User-specified credentials (prompt)—If Secure Access does not submit last-entered credentials or if the credentials fail, Secure Access prompts the user to manually enter his credentials in the intermediate sign-in page. If the user selects the "Remember password?" checkbox, Secure Access caches the user-specified credentials and, if necessary, resubmits them when the user tries to access the same resource again. Note that when Secure Access caches these credentials, it remembers the specific user and resource, even after the user signs out of Secure Access.
- Resource protected by a Web server or Web proxy using basic authentication—Secure Access submits credentials in the following order to the backend server or proxy that is protecting the Web resource:

- **Cached credentials**—If Secure Access does not submit administrator-specified credentials or the credentials fail, Secure Access determines whether it has stored credentials for the specified user and resource in its cache. If available, Secure Access submits its stored credentials.
- **Primary credentials**—If Secure Access does not submit cached credentials or the credentials fail, Secure Access submits the user's primary Secure Access credentials provided that following conditions are true:
 - The resource is in the same Intranet zone as Secure Access (that is, the resource's host name ends in the DNS suffix configured in the System > Network > Overview page of the admin console).
 - (Web proxies only) You have configured Secure Access to recognize the Web proxy through settings in the Users > Resource Policies > Web > Web Proxy pages of the admin console.
 - The credentials are not ACE credentials.
 - (RADIUS credentials only) You specify in the RADIUS configuration page that the RADIUS server does not accept one-time passwords.
- **Secondary credentials**—If the primary credentials fail, Secure Access determines whether it has secondary credentials for the user. If available, Secure Access submits the user's secondary Secure Access credentials provided that the conditions described for primary credentials are true.
- **Last-entered credentials**—If Secure Access does not submit secondary credentials or if the credentials fail, Secure Access determines whether it has stored credentials for the specified user and a different resource in its cache. If available, Secure Access submits its stored credentials provided the conditions described for primary credentials are true.
- **User-specified credentials (prompt)**—If Secure Access does not submit last-entered credentials or if the credentials fail, Secure Access prompts the user to manually enter his credentials in the intermediate sign-in page. If the user selects the "Remember password?" checkbox, Secure Access caches the user-specified credentials and, if necessary, resubmits them when the user tries to access the same resource again. Note that when Secure Access caches these credentials, it remembers the specific user and resource, even after the user signs out of Secure Access.



NOTE: Secure Access does not support the multiple credential authentication mechanism described in this section with the Email client and SAML SSO mechanisms.

You cannot define an anonymous server, certificate server, SAML or eTrust SiteMinder server as a secondary authentication server.

If you define an eTrust SiteMinder server as your primary authentication server, you cannot define a secondary authentication server.

Secure Access supports basic authentication and NTLM challenge/response scheme for HTTP when accessing web applications, but does not support HTTP-based cross-platform authentication via the negotiate protocol.

Related Documentation • [Configuring a RADIUS Server Instance on page 191](#)

Understanding SAML 1.1

The Secure Access Service enables you to pass user and session state information between the Secure Access Service and another trusted access management system that supports the Security Assertion Markup Language (SAML). SAML provides a mechanism for two disparate systems to create and exchange authentication and authorization information using an XML framework, minimizing the need for users to re-enter their credentials when accessing multiple applications or domains.

SAML exchanges are dependent upon a trusted relationship between two systems or domains. In the exchanges, one system acts as a SAML authority (also called an asserting party or SAML responder) that asserts information about the user. The other system acts as a relying party (also called a SAML receiver) that relies on the statement (also called an assertion) provided by the SAML authority. If it chooses to trust the SAML authority, the relying party authenticates or authorizes the user based on the information provided by the SAML authority.

The Secure Access Service supports two SAML use case scenarios:

- The Secure Access Service as the SAML authority—The user signs into a resource by way of the Secure Access Service first, and all other systems are SAML receivers, relying on the Secure Access Service for authentication and authorization of the user. Under this scenario, the Secure Access Service can use either an artifact profile or a POST profile.
- The Secure Access Service as the SAML receiver—The user signs into another system on the network first, and the Secure Access Service is the SAML receiver, relying on the other system for authentication and authorization of the user.

For example, in the first scenario, an authenticated Secure Access Service user named John Smith may try to access a resource protected by an access management system.

When he does, the Secure Access Service acts as a SAML authority and declares “This user is John Smith. He was authenticated using a password mechanism.” The access management system (the relying party) receives this statement and chooses to trust the Secure Access Service (and therefore trust that the Secure Access Service has properly identified the user). The access management system may still choose to deny the user access to the requested resource (for instance, because John Smith has insufficient access privileges on the system), while trusting the information sent by the Secure Access Service.

In the second scenario, John Smith signs in to his company portal and is authenticated using an LDAP server sitting behind the company’s firewall. On the company’s secure portal, John Smith clicks a link to a resource protected by the Secure Access Service. The following process occurs:

1. The link redirects John Smith to an intersite transfer service on the company portal, which constructs an artifact URL. The artifact URL contains a reference to a SAML assertion stored in the company portal’s cache.
2. The portal sends the URL to the Secure Access Service, which can decide whether or not to link to the reference.
3. If the Secure Access Service links to the reference, the portal sends a SOAP message containing the SAML assertion (an XML message containing the user’s credentials) to the Secure Access Service, which can then decide whether or not to allow the user access to the requested resource.



NOTE: SOAP requests generated by the Secure Access Service (when configured as a SAML 1.1 consumer) are not signed.

4. If the Secure Access Service allows the user access, the Secure Access Service presents to the user the requested resource.
5. If the Secure Access Service rejects the SAML assertion, or the user credentials, the Secure Access Service responds to the user with an error message.

When configuring the Secure Access Service, you can use SAML for:

- Single sign-on (SSO) authentication—In a SAML SSO transaction, an authenticated user is seamlessly signed into another system without resubmitting his credentials. In this type of transaction, the Secure Access Service can be either the SAML authority or the SAML receiver. When acting as the SAML authority, the Secure Access Service makes an authentication statement, which declares the user’s username and how he was authenticated. If the relying party (called an assertion consumer service in SAML SSO transactions) chooses to trust the Secure Access Service, the user is seamlessly signed into the assertion consumer service using the username contained in the statement.

When acting as the SAML receiver, the Secure Access Service requests credential confirmation from the SAML authority, which is the other access management system, such as LDAP or another authentication server. The SAML authority sends an assertion by way of a SOAP message. The assertion is a set of XML statements that the Secure

Access Service must interpret, based on criteria that the Secure Access Service administrator has specified in a SAML server instance definition. If the Secure Access Service chooses to trust the asserting party, the Secure Access Service allows the user to sign in seamlessly using the credentials contained in the SAML assertion.

- Access control authorization—In a SAML access control transaction, the Secure Access Service asks an access management system whether the user has access. In this type of transaction, the Secure Access Service is the relying party (also called a policy enforcement point in access control transactions). It consumes and enforces an authorization decision statement provided by the access management system (SAML authority), which declares what the user is allowed to access. If the SAML authority (also called a policy decision point in access control transactions) declares that the Secure Access Service user has sufficient access privileges, the user may access the requested resource

The Secure Access Service does not generate authorization decision statements—it only consumes them.

In addition to providing users access to a URL based on the authorization decision statement returned by a SAML authority, the Secure Access Service also allows you to define users' access rights to a URL using Secure Access Service-only mechanisms (Users > Resource Profiles > Web Applications/Pages tab). If you define access controls through the Secure Access Service as well as through a SAML authority, both sources must grant access to a URL for a user to access it. For example, you may configure a Secure Access Service access policy that denies members of the "Users" role access to www.google.com, but configure another SAML policy that bases a user's access rights on an attribute in an access management system. Even if the access management system permits users access to www.google.com, users are still denied access based on the Secure Access Service access policy.

When asked if a user may access a resource, access management systems that support SAML may return a response of permit, deny, or indeterminate. If the Secure Access Service receives an indeterminate response, it denies the user access.

The session timeouts on the Secure Access Service and your access management system may not coordinate with one another. If a user's access management system session cookie times out before his Secure Access Service destination signaling identifier (DSID) cookie times out, then single sign-on between the two systems is lost. The user is forced to sign in again when he times out of the access management system.

**Related
Documentation**

- [Configuring SAML 1.1 SSO Profiles on page 294](#)

Configuring SAML 1.1 SSO Profiles

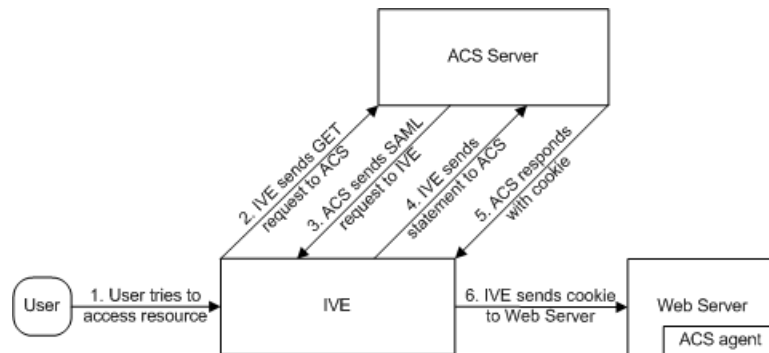
When enabling SSO transactions to a trusted access management system, you must indicate whether the access management system should "pull" user information from the Secure Access Service or whether the Secure Access Service should "push" it to the access management system. You indicate which communication method the two systems should use by selecting a profile during configuration. A *profile* is a method that two

trusted sites use to transfer a SAML statement. When configuring the Secure Access Service, you may choose to use an artifact or POST profile.

When you choose to communicate using the *artifact profile* (also called browser/artifact profile), the trusted access management server “pulls” authentication information from the Secure Access Service.

Figure 28 on page 294 shows the SAML communication process when the implementation uses the artifact profile.

Figure 36: Artifact Profile



The Secure Access Service and an assertion consumer service (ACS) use the following process to pass information:

1. The user tries to access a resource—A user is signed into the Secure Access Service and tries to access a protected resource on a Web server.
2. The Secure Access Service sends an HTTP or HTTPS GET request to the ACS—the Secure Access Service intercepts the request and checks whether it has already performed the necessary SSO operation to honor the request. If not, the Secure Access Service creates an authentication statement and passes an HTTP query variable called an artifact to the assertion consumer service.

An artifact profile is a Base64-encoded string that contains the source ID of the source site (that is, a 20-byte string that references the Secure Access Service) and a randomly generated string that acts as a handle to the authentication statement. (Note that a handle expires 5 minutes after the artifact is sent, so if the assertion consumer service responds after 5 minutes, the Secure Access Service does not send a statement. Also note that the Secure Access Service discards a handle after its first use to prevent the handle from being used twice.)

3. The ACS sends a SAML request to the Secure Access Service—The assertion consumer service uses the source ID sent in the previous step to determine the location of the Secure Access Service. Then the assertion consumer service sends a statement request wrapped in a SOAP message to the following address on the Secure Access Service:

`https://<<ivehostname>/danaws/saml.ws`

The request includes the statement handle passed in the previous step.



NOTE: The Secure Access Service only supports type 0x0001 artifacts. This type of artifact passes a reference to the source site's location (that is, the source ID of the Secure Access Service), rather than sending the location itself. To handle type 0x0001 artifacts, the assertion consumer service must maintain a table that maps source IDs to the locations of partner source sites.

4. The Secure Access Service sends an authentication statement to the ACS—the Secure Access Service uses the statement handle in the request to find the correct statement in the Secure Access Service cache and then sends the appropriate authentication statement back to the assertion consumer service. The unsigned statement contains the user's identity and the mechanism he used to sign into the Secure Access Service.
5. The ACS sends a cookie to the Secure Access Service—the assertion consumer service accepts the statement and then it sends a cookie back to the Secure Access Service that enables the user's session.
6. The Secure Access Service sends the cookie to the Web server—the Secure Access Service caches the cookie to handle future requests. Then the Secure Access Service sends the cookie in an HTTP request to the Web server whose domain name matches the domain in the cookie. The Web server honors the session without prompting the user for credentials.



NOTE: If you configure the Secure Access Service to use artifact profiles, you must install the Secure Access Service Web server certificate on the assertion consumer service.

To write a SAML SSO artifact profile resource policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show SAML policies, make the following modifications:
 - a. Click the **Customize** button in the upper right corner of the page.
 - b. Select the **SSO** check box.
 - c. Select the **SAML** check box below the SSO check box.
 - d. Click **OK**.
3. Use the tabs to display the **SSO > SAML** page.
4. Click **New Policy**.
5. On the New Policy page, enter:
 - a. A name to label this policy.

- b. A description of the policy (optional).
6. In the Resources section, specify the resources to which this policy applies.
 7. In the Roles section, specify:
 - **Policy applies to ALL roles**—To apply this policy to all users.
 - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
 - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
 8. In the Action section, specify:
 - **Use the SAML SSO defined below**—The Secure Access Service performs a single-sign on (SSO) request to the specified URL using the data specified in the SAML SSO details section. The Secure Access Service makes the SSO request when a user tries to access a SAML resource specified in the Resources list.
 - **Do NOT use SAML**—The Secure Access Service does not perform a SSO request.
 - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
 9. In the SAML SSO Details section, specify:
 - **SAML Assertion Consumer Service URL**—Enter the URL that the Secure Access Service should use to contact the assertion consumer service (that is, the access management server). For example, `https://<hostname>:<port>/dana-na/auth/saml-consumer.cgi`. (Note that the Secure Access Service also uses this field to determine the SAML recipient for its assertions.)



NOTE: If you enter a URL that begins with HTTPS, you must install the assertion consumer service's root CA on the Secure Access Service.

- **Profile**—Select **Artifact** to indicate that the assertion consumer service should “pull” information from the Secure Access Service during SSO transactions.
- **Source ID**—Enter the source ID for the Secure Access Service. It must be a Base64-encoded string. The Secure Access Service decodes it and ensures that it is 20 bytes. You can use OpenSSL or other Base64 tool to generate the Base64-encoded string.



NOTE: The Secure Access Service identifier (that is, the source ID) must map to the following URL on the assertion consumer service:
`https://<ivehostname>/dana-ws/saml.ws`

- **Issuer**—Enter a unique string that the Secure Access Service can use to identify itself when it generates assertions (typically its hostname).



NOTE: You must configure the assertion consumer service to recognize the Secure Access Service unique string.

10. In the User Identity section, specify how the Secure Access Service and the assertion consumer service should identify the user:

- **Subject Name Type**—Specify which method the Secure Access Service and assertion consumer service should use to identify the user:
 - **DN**—Send the username in the format of a DN (distinguished name) attribute.
 - **Email Address**—Send the username in the format of an email address.
 - **Windows**—Send the username in the format of a Windows domain qualified username.
 - **Other**—Send the username in another format agreed upon by the Secure Access Service and the assertion consumer service.
- **Subject Name**—Use variables to specify the username that the Secure Access Service should pass to the assertion consumer service. Or, enter static text.



NOTE: You must send a username or attribute that the assertion consumer service will recognize.

11. In the Web Service Authentication section, specify the authentication method that the Secure Access Service should use to authenticate the assertion consumer service:

- **None**—Do not authenticate the assertion consumer service.
- **Username**—Authenticate the assertion consumer service using a username and password. Enter the username and password that the assertion consumer service must send the Secure Access Service.
- **Certificate Attribute**—Authenticate the assertion consumer service using certificate attributes. Enter the attributes that the assertion consumer service must send the Secure Access Service (one attribute per line). For example, use cn=sales. You must use values that match the values contained in the assertion consumer service certificate.



NOTE: If you select this option, you must install the assertion consumer service root CA on the Secure Access Service.

12. **Cookie Domain**—Enter a comma-separated list of domains to which we send the SSO cookie.

13. Click **Save Changes**.
14. On the SAML SSO Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

Related Documentation

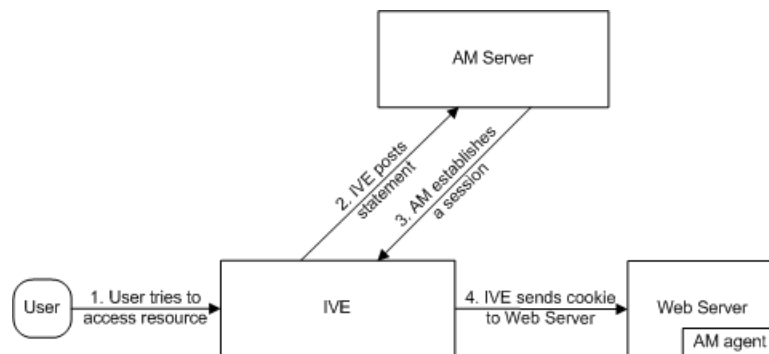
- [About Using Certificates on Secure Access Service on page 838](#)

Creating a SAML 1.1 SSO POST Profile

When you choose to communicate using a POST profile (also called browser/POST profile), the Secure Access Service “pushes” authentication data to the access management system using an HTTP POST command over an SSL 3.0 connection.

Figure 29 on page 298 shows the SAML communication process when the implementation uses the POST profile.

Figure 37: POST Profile



The Secure Access Service and an access management system use the following process to pass information:

1. The user tries to access a resource—A user is signed into the Secure Access Service and tries to access a protected resource on a Web server.
2. The Secure Access Service posts a statement—the Secure Access Service intercepts the request and checks whether it has already performed the necessary SSO operation to honor the request. If not, the Secure Access Service creates an authentication statement, digitally signs it, and posts it directly to the access management server. Since the statement is signed, the access management server must trust the certificate authority that was used to issue the certificate. Note that you must configure which certificate the Secure Access Service uses to sign the statement.

3. The AM establishes a session—If the user has the proper permissions, the access management server sends a cookie back to the Secure Access Service that enables the user's session.
4. The Secure Access Service sends the cookie to the Web server—the Secure Access Service caches the cookie to handle future requests. Then the Secure Access Service sends the cookie in an HTTP request to the Web server whose domain name matches the domain in the cookie. The Web server honors the session without prompting the user for credentials.



NOTE: If you configure the Secure Access Service to use POST profiles, you must install the assertion consumer service's root CA on the Secure Access Service and determine which method the assertion consumer service uses to trust the certificate.

To write a SAML SSO POST profile resource policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show SAML policies, make the following modifications:
 - a. Click the **Customize** button in the upper right corner of the page.
 - b. Select the **SSO** check box.
 - c. Select the **SAML** check box below the SSO check box.
 - d. Click **OK**.
3. Use the tabs to display the **SSO > SAML** page.
4. Click **New Policy**.
5. On the SAML SSO Policy page, enter:
 - A name to label this policy.
 - A description of the policy (optional).
6. In the Resources section, specify the resources to which this policy applies.
7. In the Roles section, specify:
 - **Policy applies to ALL roles**—To apply this policy to all users.
 - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
 - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:

- **Use the SAML SSO defined below**—The Secure Access Service performs a single-sign on (SSO) request to the specified URL using the data specified in the SAML SSO details section. The Secure Access Service makes the SSO request when a user tries to access a SAML resource specified in the Resources list.
 - **Do NOT use SAML**—The Secure Access Service does not perform an SSO request.
 - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. In the SAML SSO Details section, specify:
- **SAML Assertion Consumer Service URL**—Enter the URL that the Secure Access Service should use to contact the assertion consumer service (that is, the access management server). For example, use <https://hostname/acs>.
 - **Profile**—Select POST to indicate that the Secure Access Service should “push” information to the assertion consumer service during SSO transactions.
 - **Issuer**—Enter a unique string that the Secure Access Service can use to identify itself when it generates assertions. Typically, the issuer string is a hostname.



NOTE: You must configure the assertion consumer service to recognize the Secure Access Service unique string.

- **Signing Certificate**—Specify which certificate the Secure Access Service should use to sign its assertions.
10. In the User Identity section, specify how the Secure Access Service and the assertion consumer service should identify the user:
- **Subject Name Type**—Specify which method the Secure Access Service and assertion consumer service should use to identify the user:
 - **DNDN**—Send the username in the format of a DN (distinguished name) attribute.
 - **Email Address**—Send the username in the format of an e-mail address.
 - **Windows**—Send the username in the format of a Windows domain qualified username.
 - **Other**—Send the username in another format agreed upon by the Secure Access Service and the assertion consumer service.
 - **Subject Name**—Use variables to specify the username that the Secure Access Service should pass to the assertion consumer service. Or, enter static text.



NOTE: You must send a username or attribute that the assertion consumer service will recognize.

- **Cookie Domain**—Enter a comma-separated list of domains to which we send the SSO cookie.

11. Click **Save Changes**.
12. On the SAML SSO Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

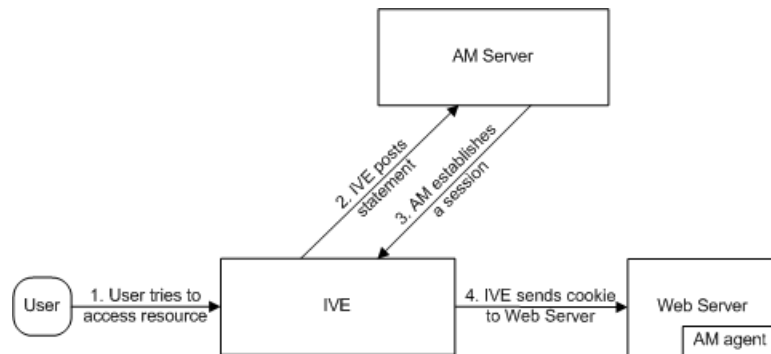
Related Documentation

- [About Using Certificates on Secure Access Service on page 838](#)
- [Writing a Web Proxy Resource Policy on page 554](#)

Creating a SAML 1.1 ACL Resource Policy

When enabling access control transactions to a trusted access management system, the Secure Access Service and trusted access management system exchange information using the method shown in [Figure 30 on page 301](#).

Figure 38: Access Control Policies



The Secure Access Service and an access management system use the following process to pass information:

1. The user tries to access a resource—A user is signed into the Secure Access Service and tries to access a protected resource on a Web server.
2. The Secure Access Service posts an authorization decision query—If the Secure Access Service has already made an authorization request and it is still valid, the Secure Access Service uses that request. (The authorization request is valid for the period of time specified in the admin console.) If it does not have a valid authorization request, the Secure Access Service posts an authorization decision query to the access management system. The query contains the user's identity and the resource that the access management system needs to authorize.
3. The access management system posts an authorization decision statement—The access management system sends an HTTPS POST containing a SOAP message

that contains the authorization decision statement. The authorization decision statement contains a result of permit, deny, or indeterminate.

4. The Secure Access Service sends the request to the Web browser—If the authorization decision statement returns a result of permit, the Secure Access Service allows the user access. If not, the Secure Access Service presents an error page to the user telling him that he does not have the proper access permissions.



NOTE: If you configure the Secure Access Service to use access control transactions, you must install the SAML Web service root CA on the Secure Access Service.

To create a SAML access control resource policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show SAML policies, make the following modifications:
 - a. Click the **Customize** button in the upper right corner of the page.
 - b. Select the **SAML ACL** check box below the Access check box.
 - c. Click **OK**.
3. Use the tabs to display the Access > SAML ACL page.
4. On the SAML Access Control Policies page, click **New Policy**.
5. On the New Policy page, enter:
 - a. A name to label this policy.
 - b. A description of the policy (optional).
6. In the Resources section, specify the resources to which this policy applies.
7. In the Roles section, specify:
 - **Policy applies to ALL roles**—To apply this policy to all users.
 - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
 - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
 - **Use the SAML Access Control checks defined below**—The Secure Access Service performs an access control check to the specified URL using the data specified in the SAML Access Control Details section.

- **Do not use SAML Access**—The Secure Access Service does not perform an access control check.
 - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. In the SAML Access Control Details section, specify:
- **SAML Web Service URL**—Enter the URL of the access management system's SAML server. For example, use <https://hostname/ws>.
 - **Issuer**—Enter the hostname of the issuer, which in most cases is the hostname of the access management system.



NOTE: You must enter a unique string that the SAML Web service uses to identify itself in authorization assertions.

10. In the User Identity section, specify how the Secure Access Service and the SAML Web service should identify the user:
- **Subject Name Type**—Specify which method the Secure Access Service and SAML Web service should use to identify the user:
 - **DN**—Send the username in the format of a DN (distinguished name) attribute.
 - **Email Address**—Send the username in the format of an e-mail address.
 - **Windows**—Send the username in the format of a Windows domain qualified username.
 - **Other**—Send the username in another format agreed upon by the Secure Access Service and the SAML Web service.
 - **Subject Name**—Use variables to specify the username that the Secure Access Service should pass to the SAML Web service. Or, enter static text.



NOTE: You must send a username or attribute that the SAML Web service will recognize.

11. In the Web Service Authentication section, specify the authentication method that the SAML Web service should use to authenticate the Secure Access Service:
- **None**—Do not authenticate the Secure Access Service.
 - **Username**—Authenticate the Secure Access Service using a username and password. Enter the username and password that the Secure Access Service must send the Web service.
 - **Certificate Attribute**—Authenticate the Secure Access Service using a certificate signed by a trusted certificate authority. If you have more than one certificate installed on the Secure Access Service, use the drop-down list to select which certificate to send to the Web service.



NOTE: If you select this option, you must install the Secure Access Service Web server certificate on the access management system Web server and determine which method the SAML Web service uses to trust the certificate.

12. In the Options section, specify:
 - **Maximum Cache Time**—You can eliminate the overhead of generating an authorization decision each time the user requests the same URL by indicating that the Secure Access Service must cache the access management system's authorization responses. Enter the amount of time the Secure Access Service should cache the responses (in seconds).
 - **Ignore Query Data**—By default, when a user requests a resource, the Secure Access Service sends the entire URL for that resource (including the query parameter) to the SAML Web service and caches the URL. You can specify that the Secure Access Service should remove the query string from the URL before requesting authorization or caching the authorization response.
13. Click **Save Changes**.
14. On the SAML Access Control Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

Related Documentation

- [About Using Certificates on Secure Access Service on page 838](#)
- [Writing a Web Proxy Resource Policy on page 554](#)

Creating a Trust Relationship Between SAML 1.1 Systems

In order to ensure that SAML-enabled systems are only passing information between trusted sources, you must create a trust relationship between the applications that are sending and receiving information.

Configuring Trusted Application URLs

In a trust relationship, you must provide the SAML-enabled systems with the URLs they need to contact each other. In some transactions, only the system that initiates the transaction (the Secure Access Service) needs to know the URL of the other system. (The Secure Access Service uses the URL to initiate the transaction.) In other transactions (SSO transactions using artifact profiles), you need to configure each system with the URL of the other.

The following list shows the different transaction types and the URLs you must configure for each:

- SSO transactions: Artifact profile—On the Secure Access Service, you must enter the URL of the assertion consumer service. For example, use <https://hostname/acs>.

You must also enter the following URL for the Secure Access Service on the assertion consumer service. For example, use

<https://<SecureAccessHostname>/dana-ws/saml.ws>.

- SSO transactions: POST profile—On the Secure Access Service, you must enter the URL of the assertion consumer service. For example, use <https://hostname/acs>.
- Access control transactions—On the Secure Access Service, you must enter the URL of the SAML Web service. For example, use <https://hostname/ws>.

Configuring an Issuer

Before accepting a statement from another system, a SAML-enabled entity must trust the issuer of the statement. You can control which issuers a system trusts by specifying the unique strings of the trusted issuers during the system's configuration. (When sending a statement, an issuer identifies itself by including its unique string in the statement. SAML-enabled applications generally use hostnames to identify issuers, but the SAML standard allows applications to use any string.) If you do not configure a system to recognize an issuer's unique string, the system will not accept that issuer's statements.

The following list shows the different transaction types and the issuers you must configure for each:

- SSO transactions—You must specify a unique string on the Secure Access Service (typically its hostname) that it can use to identify itself and then configure the access management system to recognize that string.
- Access control transactions—You must specify a unique string on the access management system (typically its hostname) that it can use to identify itself and then configure the Secure Access Service to recognize that string.

Configuring Certificates

Within SSL transactions, the server must present a certificate to the client, and then the client must verify (at minimum) that it trusts the certificate authority who issued the server's certificate before accepting the information. You can configure all of the Secure Access Service SAML transactions to use SSL (HTTPS).

Configuring SSO Transactions: Artifact Profile

Artifact profile transactions involve numerous communications back and forth between the Secure Access Service and the access management system. The methods you use to pass data and authenticate the two systems affect which certificates you must install and configure.

The following list shows the different artifact profile configuration options that require special certificate configurations:

- All artifact profile transactions—Regardless of your artifact profile configuration, you must install the certificate of the CA that signed the Secure Access Service Web server

certificate on the access management system. (The Secure Access Service requires the access management system to use an SSL connection when requesting an authentication statement. In an SSL connection, the initiator must trust the system to which it is connecting. By installing the CA certificate on the access management system, you ensure that the access management system will trust the CA that issued the Secure Access Service certificate.)

- Sending artifacts over an SSL connection (HTTPS GET requests)—If you choose to send artifacts to the access management system using an SSL connection, you must install the access management system's root CA certificate on the Secure Access Service. (In an SSL connection, the initiator must trust the system to which it is connecting. By installing the access management system's CA certificate on the Secure Access Service, you ensure that the Secure Access Service will trust the CA that issued the access management system's certificate.) You can install the root CA from the System > Configuration > Certificates > Trusted Client CAs page in the admin console. If you do not want to send artifacts over an SSL connection, you do not need to install any additional certificates.

To enable SSL-based communications from the Secure Access Service to the access management system, enter a URL that begins with HTTPS in the SAML Assertion Consumer Service URL field during the Secure Access Service configuration. You may also need to enable SSL on the access management system.

- Transactions using certificate authentication—If you choose to authenticate the access management system using a certificate, you must:
 - Install the access management system's root CA certificate on the Secure Access Service. You can install the root CA from the System > Configuration > Certificates > Trusted Client CAs page in the admin console.
 - Specify which certificate values the Secure Access Service should use to validate the access management system. You must use values that match the values contained in the access management server's certificate.

If you do not choose to authenticate the access management system, or if you choose to use username/password authentication, you do not need to install any additional certificates.

Configuring SSO Transactions: POST Profile

In a POST profile transaction, the Secure Access Service sends signed authentication statements to the access management system. Generally, it sends them over an SSL connection (recommended), but in some configurations, the Secure Access Service may send statements through a standard HTTP connection.

The following list shows the different POST profile configuration options that require special certificate configurations:

- All POST profile transactions—Regardless of your POST profile configuration, you must specify which certificate the Secure Access Service should use to sign its statements. You can choose a certificate in the Users > Resource Policies > Web > SSO SAML > [Policy] > General page in the admin console. Then, you must install the Secure Access Service device certificate on the access management system. You can download the

Secure Access Service certificate from the System > Configuration > Certificates > Device Certificates > [Certificate] > Certificate Details page.

- Sending POST data over an SSL connection (HTTPS)—If you choose to send statements to the access management system using an SSL connection, you must install the access management system's root CA certificate on the Secure Access Service. (In an SSL connection, the initiator must trust the system to which it is connecting. By installing the access management system's certificate on the Secure Access Service, you ensure that the Secure Access Service will trust the CA that issued the access management system's certificate.) You can install the root CA from the System > Configuration > Certificates > Trusted Client CAs page in the admin console. If you do not want to post statements over an SSL connection, you do not need to install any additional certificates.

To enable SSL-based communications from the Secure Access Service to the access management system, enter a URL that begins with HTTPS in the SAML assertion consumer service URL field during the Secure Access Service configuration. You may also need to enable SSL on the access management system.

Configuring Access Control Transactions

In an access control transaction, the Secure Access Service posts an authorization decision query to the access management system. To ensure that the access management system responds to the query, you must determine which certificate options are required by your configuration.

The following list shows the different access control configuration options that require special certificate configurations:

- Sending authorization data over an SSL connection—If you choose to connect to the access management system using an SSL connection, you must install the access management system's root CA on the Secure Access Service. (In an SSL connection, the initiator must trust the system to which it is connecting. By installing the access management system's certificate on the Secure Access Service, you ensure that the Secure Access Service will trust the CA that issued the access management system's certificate.) You can install the root CA from the System > Configuration > Certificates > Trusted Client CAs page in the admin console.
- Transactions using certificate authentication—If you choose to use certificate authentication, you must configure the access management system to trust the CA that issued the Secure Access Service certificate. Optionally, you may also choose to accept the certificate based on the following additional options:
 - Upload the Secure Access Service certificate public key to the access management system.
 - Validate the Secure Access Service using specific certificate attributes.

These options require that you specify which certificate the Secure Access Service should pass to the access management system. You can choose a certificate in the Users > Resource Policies > Web > SAML ACL > [Policy] > General page in the admin console.

To determine how to configure your access management system to validate the Secure Access Service certificate, see your access management system's documentation. If your access management system does not require certificate authentication, or if it uses username/password authentication, you do not need to configure the Secure Access Service to pass the access management server a certificate. If you do not specify a trust method, your access management system may accept authorization requests from any system.

Configuring User Identity

In a trust relationship, the two entities must agree on a way to identify users. You may choose to share a username across systems, select an LDAP or certificate user attribute to share across systems, or hardcode a user ID. (For example, you may choose to set the Subject Name field to "guest" to easily allow access across systems.)

To ensure that the two systems are passing common information about users, you must specify which information the Secure Access Service should pass using options in the User Identity section of the Users > Resource Policies > Web > SAML SSO > [Policy] > General page and the Users > Resource Policies > Web > SAML ACL > [Policy] > General page. Choose a username or attribute that the access management system will recognize.

Related Documentation

- [Using a Trusted Client CA on page 846](#)
- [Understanding SAML 1.1 on page 281](#)
- [Configuring SAML 1.1 SSO Profiles on page 294](#)
- [Configuring General Role Options on page 109](#)

Synchronizing User Records

- [About User Record Synchronization on page 363](#)
- [Enabling User Record Synchronization on page 365](#)
- [Configuring the User Record Synchronization Authentication Server on page 366](#)
- [Configuring the User Record Synchronization Server on page 367](#)
- [Configuring the User Record Synchronization Client on page 367](#)
- [Configuring the User Record Synchronization Database on page 368](#)
- [Scheduling User Record Synchronization Backup on page 369](#)

About User Record Synchronization

The user record synchronization feature promotes a more consistent user experience by allowing users to retain their bookmarks and individual preferences regardless of which Secure Access they log in to.

User record synchronization relies on client-server pairings. The client is the Secure Access appliance that users log in to start their remote access. Each client is associated with one primary server and one backup server to store user record data. Clients can be individual appliances or a node within a cluster.

A server in this instance is the Secure Access appliance that stores the user data records. Each server can be configured to replicate its user record data to one or more peer servers. Servers are identified by a user-defined logical name. The same logical name can be assigned to more than one authentication server to let you associate authentication servers of different types to the same user. For example, SA1 is an ACE authentication server with user1 who creates a bookmark to www.juniper.net. SA2 is an Active Directory authentication server with the same user1. For the www.juniper.net bookmark to be transferred from SA1/ACE/user1 to SA2/AD/user1 you would assign the logical name “Logical1” to both the ACE server on SA1 and the Active Directory server on SA2.



NOTE: Cluster VIPs can not be used as the IP for synchronizing between clients and peers servers.

As long as the logical name is the same, the authentication servers can be different types and different server names and still be associated with a common user. The username

must be the same for user record data to be synchronized across the servers. The logical authentication server (LAS) and username combination is what uniquely identifies a user record.

The following user records are synchronized between the client and server:

- Bookmarks
 - Web
 - File
 - Terminal Services
 - JSAM
- Preferences
- Persistent cookies
- Cached passwords

User session data is not synchronized. Persistent cookies, if changed, are synchronized when the user session terminates. All other modifications to the user records are synchronized immediately. User records are stored in cache on the client node prior to being pushed to the servers.

When a user logs in to a client, their data is pulled from the associated server. The pull is performed in the background and does not delay the login process. Users using browsers that do not support JavaScript must manually refresh the index page for updated bookmarks and preferences to appear. For browsers that support JavaScript, users may see a spinning progress indicator and their home page will refresh automatically with updated bookmarks and preferences.

Clients and servers need not be installed with the same Secure Access software version as long as they are using version 7.2 or later.



NOTE: User record synchronization uses port 17425. This port number is not configurable. If you are deploying across a firewall, configure your firewall to allow traffic on this port.

To set up user record synchronization, you perform the following tasks:

1. Enable user record synchronization for each participating client and server, identify which ones are the client and which ones are the server and assign a node name to each client and server.
2. Create a shared secret which is used to authenticate the client with the server and the server to its peer servers.
3. On each server, define which clients and peers are allowed to communicate with the server.
4. On each client, define the servers that handle records for each LAS server.

When enabling this feature, you have several options to initialize the user record database. You can:

- populate the database using user records located in the cache of the client systems.
- populate the database use user records located in the cache of the server systems.
- don't pre-populate the database but populate it as users log in and out of the client system.

If you choose the last option, users may not be able to view their saved bookmarks and preferences until the next time they log in, depending on which client they log in to.



NOTE: User records may not synchronize if the time clocks on the Secure Access appliances are not in sync. We recommend that you use the same NTP server for each node participating in user record synchronization to keep Secure Access times accurately adjusted.

The user record synchronization feature will not start automatically after importing a system configuration that has this feature enabled. The workaround is to disable user record synchronization and then enable user record synchronization from the user interface after the configuration import.

Related Documentation

- [Enabling User Record Synchronization on page 365](#)
- [Configuring the User Record Synchronization Authentication Server on page 366](#)
- [Configuring the User Record Synchronization Server on page 367](#)
- [Configuring the User Record Synchronization Client on page 367](#)
- [Configuring the User Record Synchronization Database on page 368](#)

Enabling User Record Synchronization

The first step in enabling user record synchronizing is to define the node name and the shared secret used to authenticate between the clients and the servers:

1. Select **System > Configuration > User Record Synchronization > General**.
2. Select the **Enable User Record Synchronization** checkbox.
3. Enter a unique node name. This name is used when associating a client with a server and is different from the logical name assigned to a server. This node name is also not the same as the cluster node name.
4. Enter the shared secret and confirm it.

The shared secret is the password used to authenticate the client with its servers and the primary server with its peer servers. Use the same shared secret for all clients and servers participating in user record synchronization.

5. Select whether this node is client only or if this node acts as both a client and server.
6. Click **Save Changes**.



NOTE: If you need to make any changes in this window at a later time, you must deselect the Enable User Record Synchronization checkbox and click Save Changes. Make your edits, select the Enable User Record Synchronization checkbox and save your changes.

Once you enter a name and shared secret, you can not clear these fields.

**Related
Documentation**

- [Configuring the User Record Synchronization Authentication Server on page 366](#)
- [Configuring the User Record Synchronization Server on page 367](#)
- [Configuring the User Record Synchronization Client on page 367](#)
- [Configuring the User Record Synchronization Database on page 368](#)

Configuring the User Record Synchronization Authentication Server

To set up the authentication server you must define it's logical name:

1. Select **Authentication > Auth Servers**.
2. Click the name of the authentication server you want assign a LAS name.

By assigning the authentication server a LAS name, all users that authenticate using the authentication server are associated with this LAS. In this instance, we are referring to the client nodes, not the user record synchronization server nodes.

3. Select the **User Record Synchronization** checkbox.
4. Enter a logical name to identify this server.

This allows you to share user record data across authentication servers on different Secure Access gateways. By assigning a LAS name to an authentication server, you are implicitly assigning it to all users that authenticate with that auth server. The combination of the user's login name and their LAS name uniquely identifies the user's user record across all user record synchronization servers.

5. Click **Save Changes**.

**Related
Documentation**

- [Configuring the User Record Synchronization Client on page 367](#)
- [Configuring the User Record Synchronization Database on page 368](#)

Configuring the User Record Synchronization Server

To set up the user record synchronization server you must define its peer nodes (optional) and the clients that can access this server.

1. Select **System > Configuration > User Record Synchronization > This Server**.
2. Enter the peer server's node name and IP address, then click **Add**. To specify more than one peer server, enter each server's node name and IP address individually and click **Add**. There is no limit on the number of peer servers you can add.

Data is replicated from the primary or backup server to its peer servers. If the primary is not available, user data is sent to the backup. User data is then replicated to the peer servers.

3. For each client you want synchronized with this server, enter the client's name and IP address and click **Add**.

Once added, peer servers will have a colored icon next to their name indicating their connection status. Node status is provided to client nodes and LAS mapping servers as well.

Color	Description
Green	Connected
Yellow	Connecting
Gray	Not connected

Related Documentation

- [Configuring the User Record Synchronization Authentication Server on page 366](#)
- [Configuring the User Record Synchronization Client on page 367](#)
- [Configuring the User Record Synchronization Database on page 368](#)

Configuring the User Record Synchronization Client

To set up the client, you select the primary and backup server you want this client to synchronize with:

1. Select **System > Configuration > User Record Synchronization > This Client**.
2. Select the LAS name you want to synchronize and enter the primary IP of the user record server that will server the user records. If you prefer to synchronize with any available server, select **Any LAS**.
3. Enter the primary and optionally a backup server's IP address and then click **Add**.

Even if you select Any LAS, you must enter a primary server IP address.

Once added, the primary and backup servers have a colored icon next to their name indicating their connection status.

- Related Documentation**
- [Configuring the User Record Synchronization Authentication Server on page 366](#)
 - [Configuring the User Record Synchronization Server on page 367](#)
 - [Configuring the User Record Synchronization Database on page 368](#)

Configuring the User Record Synchronization Database

With the Database tab, you can delete inactive records from the client cache, retrieve statistics about the database, export and import the data and remove user data from the server's database.

To configure the database:

1. Select **System > Configuration > User Record Synchronization > Database**.
2. Select **Auto-delete inactive synchronized user records from the Cache** to remove inactive user records from the cache. This option does not remove user records from the user record database.

When this option is selected, Secure Access performs a check every 15 minutes and deletes user records that meet all of the following criteria:

- There are no active user sessions associated with the user record.
 - The user record does not have any custom settings or the latest version of the user record has been synchronized with the user record database.
 - The authentication server associated with the user record database does not have type "local". For example, the "System Local" auth server that is part of the default configuration of Secure Access has a "local" type, so any user records associated with that auth server will not be auto-deleted. However, user records associated with external authentication servers like Radius or LDAP may be deleted, depending on the two prior criteria.
3. Select **Auto-delete user records from the local synchronization database that have been idle for X days** to permanently remove user records from the database located on the server. Enter the number of days user records must be inactive before being deleted.

In this instance, "inactive" means that no client has pulled the user record or pushed any modifications to the user record in X days.

4. Click **Retrieve Statistics** to display the number of records in the database. You can not edit or view records in the database.
5. Under **Export**, you export user records to a file. The user records can be exported from the user record database, or from the cache. The exported file can be used to pre-populate the user record database on another node.
 - Enter the LAS name of the user records you want to export. If you leave this field blank, all user records are exported. If you enter a LAS name, only user records with the entered LAS name are exported.
 - To encrypt the exported data, select the **Encrypt the exported data with password** checkbox and enter the password.

- Click **Export** to export the user records from the specified source (cache or database). You will be prompted where to save the file.
6. Under Import, you import user records into the synchronization database. The user records can be imported from a file or from the cache. Use the Import operation to pre-populate the user record database with user records exported from another node, or with user records from the cache.
- Click **Browse** to locate the exported file and enter the password if the exported file was encrypted with a password.
 - Select the **Override Logical Auth Servers in imported user records with** checkbox to replace the LAS name in each imported user record with the LAS name entered.
For example, you change the LAS name, use this option to update the user records with the new name.
 - Click **Import**.
7. Under Delete, specify which user records to permanently remove from the user record database. The options you select apply only to the user record database associated with this server.
- Select **User record with login name and Logical Auth Server** to remove a specific record. The login name and LAS name together uniquely identify a user record. Select this option to remove that record (if it exists).
 - Select **User records with Logical Auth Server** to delete all user records with the specified LAS name.
 - Select **All user records** to permanently remove user records from the database on this node.
 - Click **Delete**.

Related Documentation

- [Configuring the User Record Synchronization Authentication Server on page 366](#)
- [Configuring the User Record Synchronization Server on page 367](#)
- [Configuring the User Record Synchronization Client on page 367](#)

Scheduling User Record Synchronization Backup

You can configure periodic backups of the user record database. User record synchronization backup can be enabled only on a user record synchronization server.

To backup the user record database:

1. Ensure the system is set up as a user record synchronization server. See [System > Configuration > User Record Synchronization](#).
2. Select **Maintenance > Archiving > Archiving Servers**.
3. Select the **Archive User Record Synchronization Database** check box.

4. Specify an archive schedule. Through the options, schedule archives on any combination of weekdays including weekends.



NOTE: If you schedule an archival operation to occur during the hour that your system switches to Daylight Savings Time (DST) the operation may not occur as scheduled. For example, if your system is set to change to DST at 1:00 a.m. and you have scheduled an archival operation to occur at anytime between 1:01 a.m. and 1:59 a.m., the operation is not accomplished, because at 1:00 a.m. the system clock is moved forward to 2:00 a.m. and the system never reaches your archival time for that date.

5. Define a specific time when you want Secure Access Service to archive data or elect to archive data every hour, which produces twenty-four files with unique timestamps.



NOTE: We recommend you schedule an archival operation during hours when traffic is light in order to minimize its impact to your users. The automatic archiving process compresses files and, if the system is busy, can degrade performance for users. Also, a cluster node may appear unresponsive if the system is busy with traffic and performing archiving simultaneously.

6. Provide a password if you want to encrypt system configuration or user account archives with a password (optional).
7. Click **Save Changes**.

**Related
Documentation**

- [Configuring the User Record Synchronization Database on page 368](#)

PART 3

Endpoint Defense

- [Host Checker on page 373](#)
- [Cache Cleaner on page 445](#)

Host Checker

- Host Checker and Trusted Network Computing on page 374
- Task Summary: Configuring Host Checker on page 376
- Creating Global Host Checker Policies on page 377
- Enabling Enhanced Endpoint Security Functionality on page 379
- Enabling Connection Control Host Checker Policies (Windows Only) on page 381
- Creating and Configuring New Client-side Host Checker Policies on page 382
- Checking for Third-Party Applications Using Predefined Rules (Windows Only) on page 383
- Configuring a Predefined Antivirus Rule with Remediation Options on page 384
- Configuring a Predefined Firewall Rule with Remediation Options (Windows Only) on page 386
- Configuring a Predefined AntiSpyware Rule (Windows Only) on page 387
- Configuring Virus Signature Version Monitoring and Patch Assessment Data Monitoring on page 388
- Patch Management Info Monitoring and Patch Deployment on page 390
- Specifying Customized Requirements Using Custom Rules on page 394
- Using a Wildcard or Environment Variable in a Host Checker Rule on page 399
- Configuring Patch Assessment Policies on page 401
- Configuring Patch Assessment Rules on page 403
- Using Third-party Integrity Measurement Verifiers on page 405
- Configuring a Remote IMV Server on page 406
- Implementing the Third-Party IMV Policy on page 411
- Implementing Host Checker Policies on page 412
- Configuring Host Checker Restrictions on page 414
- Remediating Host Checker Policies on page 416
- Configuring General Host Checker Remediation on page 418
- Upgrading the Endpoint Security Assessment Plug-In on page 419
- Defining Host Checker Pre-Authentication Access Tunnels on page 421
- Specifying Host Checker Pre-Authentication Access Tunnel Definitions on page 422

- [Specifying General Host Checker Options on page 425](#)
- [Specifying Host Checker Installation Options on page 426](#)
- [Client ActiveX Installation Delay on page 428](#)
- [Using Host Checker with the GINA Automatic Sign-In Function on page 428](#)
- [Installing Host Checker Automatically or Manually on page 429](#)
- [Using Host Checker Logs on page 430](#)
- [Configuring Host Checker for Windows Mobile on page 430](#)
- [Host Checker for Apple iOS on page 432](#)
- [Using Proxy Exceptions on page 436](#)
- [Enabling the Secure Virtual Workspace on page 437](#)
- [Defining Secure Virtual Workspace Permissions on page 439](#)
- [Defining a Secure Virtual Workspace Application Policy on page 441](#)
- [Defining a Secure Virtual Workspace Security Policy on page 442](#)
- [Defining Secure Virtual Workspace Environment Options on page 443](#)
- [Defining Secure Virtual Workspace Remediation Policy on page 444](#)

Host Checker and Trusted Network Computing

Host checker is a client-side agent that performs endpoint health and security checks for hosts that attempt to connect to the Secure Access Service.

The Trusted Computing Group (TCG) is a not-for-profit organization formed in 2003 to develop, define, and promote open standards for hardware-enabled trusted computing and security technologies across multiple platforms, peripherals, and devices. The TCG has over 100 members that include component vendors, software developers, systems vendors, and network companies.

Trusted Network Connect (TNC) is a subgroup of the TCG that created an architecture and set of standards for verifying endpoint integrity and policy compliance during or after a network access request. Many of the TCG members participated in the definition and specification of the TNC's architecture. The TNC defined several standard interfaces that enable components from different vendors to securely operate together. The TNC architecture is designed to build on established standards and technologies, such as 802.1X, RADIUS, IPsec, EAP, and TLS/SSL. For more information about TNC, see www.trustedcomputinggroup.org.

Using technology based on the TNC architecture and standards, the Host Checker component of the Unified Access Control solution provides a comprehensive approach to assess the trust worthiness of endpoints.

You can use Host Checker to perform endpoint checks on hosts before allowing them to connect to the Secure Access Service and access protected resources. Host Checker can check for third party applications, files, process, ports, registry keys, and custom DLLs on hosts. Based on the results of the checks, it can then deny or allow access to protected resources. For example, you may choose to check for virus detection software before allowing a user access to any of the Secure Access Service realms, launch the software

on the user's system if necessary, map the user to roles based on individual policies defined in your own DLL, and then further restrict access to individual resources based on the existence of spyware detection software. When a user's computer does not meet the requirements you specify, you can display remediation instructions to users so they can bring their computers into compliance.



NOTE: If you configure a large number of Host Checker policies, and the Secure Access Service is under a heavy load, the server process inside the device could get overloaded. When this happens, a message appears in the event log (Log/Monitoring > Events > Log).

Host Checker supports TNC-based integrity measurement collectors (IMCs) and integrity measurement verifiers (IMVs). IMCs are software modules that run on the host and collect information such as antivirus, antispyware, patch management, firewall, and other configuration and security information about the host. IMVs are software modules that run on the Secure Access Service and verify a particular aspect of an host's integrity. Each IMV on the Secure Access Service works with the corresponding IMC on the host to verify that the host meets the requirements of the integrity measurement custom rule(s) that you configure. IMCs frequently scan the client machine for changes in security status. Some IMCs can detect a change in status (for example, if the user turns off virus checking) and then trigger a new check to make sure the modified system complies with the requirements of the Host Checker policy. You can configure Host Checker to monitor third-party IMCs installed on client computers by using third-party IMVs that are installed on a remote IMV server.

You can invoke Host Checker at the role level, or the realm level to specify access requirements for endpoints attempting to authenticate.

All Host Checker rules are implemented through IMCs and IMVs based on the TNC open architecture. IMCs are software modules that Host Checker runs on the client machine.

IMCs are responsible for collecting information, such as antivirus, antispyware, patch management, firewall, and other configuration and security information for a client machine.

IMVs are software modules running on the Secure Access Service that are responsible for verifying a particular aspect of an endpoint's integrity.

The Secure Access Service and Host Checker manage the flow of information between the corresponding pairs of IMVs and IMCs. Each IMV on the Secure Access Service works with the corresponding IMC on the client machine to verify that the client meets the Host Checker rules.

You can also configure Host Checker to monitor third-party IMCs installed on client computers by using third-party IMVs that are installed on a remote IMV server.

Related Documentation

- [Creating Global Host Checker Policies on page 377](#)
- [Task Summary: Configuring Host Checker on page 376](#)

Task Summary: Configuring Host Checker



NOTE: Ensure that user endpoints have signed ActiveX components or signed Java applets enabled within their browsers to permit Host Checker to download, install, and launch.

To configure a Host Checker policy, perform these tasks:

1. Create and enable Host Checker policies through the **Authentication > Endpoint Security > Host Checker** page of the admin console.
 - a. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
 - b. Under Policies, click **New**.
 - c. Enter a name in the Policy Name field and then click **Continue**. (Users see this name on the Host Checker remediation page if you enable custom instructions for this policy.)
 - d. Create one or more rules to associate with the policy.
2. Configure additional system-level options on the **Authentication > Endpoint Security > Host Checker** page of the admin console as necessary:
 - If you want to display remediation information to users if they fail to meet the requirements of a Host Checker policy, configure remediation options through the **Authentication > Endpoint Security > Host Checker** page of the admin console.
 - For Windows clients, determine whether you need to use a pre-authentication access tunnel between the clients and policy server(s) or resources. If necessary, create a manifest.hcif file with the tunnel definition and upload it through the **Authentication > Endpoint Security > Host Checker** page of the admin console.
 - To change default Host Checker settings, configure settings through the **Authentication > Endpoint Security > Host Checker** page of the admin console.
3. Determine the level you that you want to enforce Host Checker policies:
 - To enforce Host Checker policies when the user initially accesses Secure Access, implement the policy at the realm level by selecting the policy at the **Users > User Realms > Select Realm > Authentication Policy > Host Checker** page of the admin console.
 - To allow or deny users access to specific roles based on compliance with Host Checker policies, implement the policies at the role level by using the **Users > User Roles > Select Role > General > Restrictions > Host Checker** page of the admin console.

- To map users to roles based on their compliance with Host Checker policies, use custom expressions in the **Users > User Realms > Select Realm > Role Mapping** page of the admin console.
 - To allow or deny users access to individual resources based on their compliance with Host Checker policies, use conditions in the **Users > Resource Policies > Select Resource > Select Policy > Detailed Rules > Select|Create Rule** page of the admin console.
4. Specify how users can access the Host Checker client-side agent that enforces the policies you define:
 - To enable automatic installation of the Host Checker client-side agent on all platforms, use the **Administrators > Admin Realms > Select Realm > Authentication Policy > Host Checker** page or the **Users > User Realms > Select Realm > Authentication Policy > Host Checker** page of the admin console.
 - To download the Host Checker installer and manually install it on your Windows users' systems, use the **Maintenance > System > Installers** page of the admin console.
 5. Determine whether you want to create client-side logs. If you enable client-side logging through the **System > Log/Monitoring > Client Logs** page of the admin console, the Secure Access appliance creates log files on your users' systems and writes to the file whenever Host Checker runs.

If more than one valid Secure Access session exists from the same system, and Host Checker is used in those sessions, all of the valid sessions are terminated if a user signs out from any of the sessions. To prevent this, turn off Host Checker for those sessions that do not need Host Checker.

**Related
Documentation**

- [Junos Pulse Overview on page 37](#)
- [Creating Global Host Checker Policies on page 377](#)

Creating Global Host Checker Policies

To use Host Checker as a policy enforcement tool for managing endpoints, you create Host Checker policies through the **Authentication > Endpoint Security > Host Checker** page of the admin console, and then implement the policies at the realm, role, and resource policy levels.

Secure Access provides many options that you can use to enable, create, and configure Host Checker policies:

- **Pre-defined policies (prevent in-network attacks or downloads malware detection software)**—Secure Access comes equipped with two types of pre-defined client-side Host Checker policies that you simply need to enable, not create or configure, in order to use them. The Connection Control policy prevents attacks on Windows client computers from other infected computers on the same network. The EES policies download malware protection software to client computers before users sign into Secure Access. Note that these policies only work on Windows systems.
- **Pre-defined rules (check for third party applications)**—Host Checker contains a wide array of pre-defined rules that check for antivirus software, firewalls, malware, spyware, and specific operating systems from a variety of industry leaders. You can enable one or more of these rules within a Host Checker client-side policy to ensure that the integrated third party applications that you specify are running on your users' computers.
- **Custom rules (check for additional requirements)**—In addition to Predefined rules, you can create custom rules within a Host Checker policy to define requirements that user endpoints must meet. Using custom rules, you can:
 - Configure Host Checker to check for custom third party DLLs that perform customized client-side checks.
 - Verify that certain ports are open or closed on the user's computer.
 - Confirm that certain processes are or are not running on the user's computer.
 - Check that certain files are or are not present on the client machine.
 - Evaluate the age and content of required files through MD5 checksums.
 - Confirm that registry keys are set on the client machine (Windows only).
 - Check the NetBIOS name, MAC addresses, or certificate of the client machine (Windows only).
 - Assess the client operating system and application service packs to ensure they are up to date (Windows only).
 - Perform application and version checks to ensure that endpoints are running the correct software (Windows only).
- **Custom integrated applications (implement through server API)**—For Windows clients, you can upload a third-party J.E.D.I. DLL to Secure Access.
- Within a single policy, you can create different Host Checker requirements for Windows, Macintosh and Linux, checking for different files, processes, and products on each operating system. You can also combine any number of host check types within a single policy and check for alternative sets of rules.

**Related
Documentation**

- [Configuring a Remote IMV Server on page 406](#)
- [Implementing Host Checker Policies on page 412](#)

Enabling Enhanced Endpoint Security Functionality

Host Checker includes integrated antispymware functionality that can detect and remediate Windows endpoints. Enhanced Endpoint Security (EES) ensures that the following malware, spyware, viruses, or worms are not present on endpoints that attempt to connect to Secure Access, and you can restrict or quarantine these endpoints depending on your Host Checker policy configuration.

- Adware
- Dialers
- Hijack
- Spy Cookie
- Commercial System Monitor
- System Monitor (detects spyware, keyloggers, screenscrapers and any malware that monitors the system)
- Trojan Downloader
- Trojan Phisher
- Trojan Horse
- Worm

EES can scan processes that are loaded in memory on endpoints and provide real-time file system write and execution shield to automatically remediate machines that are not in compliance. As part of the remediation status, EES reports any threats that are detected but not remediated. In some cases the end user may be directed to reboot the machine to achieve compliance.

EES uses a signature database that is automatically downloaded to endpoints from Web Root Spy Sweeper servers on the Internet. The signature database is not hosted on Secure Access.

Endpoints must have access to the Internet for EES to successfully run, as live signature updates must be permitted to download. Additionally, if you configure default remediation roles you should ensure that endpoints that are directed to remediation roles can access `*webroot.com`, `*cloudfront.net`, `*edgesuite.net` and `*akamai.net`.

You can configure the age of the database on Secure Access to determine the acceptable age of the signature database. The age of the database is the threshold used to determine if a user can access resources by passing a Host Checker policy. For example, if signatures are five days old, and you configure the age as six days, the user is allowed to access resources. If you configure the age as four days, the user fails the Host Checker policy. If a user passes the initial EES Host Checker policy, signature updates are performed regularly, so endpoints should generally have the most current updates.

If Internet connectivity is not available to an endpoint prior to connecting to Secure Access and you have chosen to implement the option to check for signature age, the policy will

not pass if the signatures are too old. For example, if a user has not accessed the endpoint for several days and the signatures are not up to date, the endpoint cannot authenticate to Secure Access. In this case, you can create a default remediation role that allows limited access to the Internet for signature updates at `*webroot.com`.

EES antispayware functionality is available on Windows platforms (including Vista) with VPN Tunneling.

You configure EES on the Endpoint Security > Host Checker main page to ensure that multiple policies are not created, and that the same policy is used across all realms and roles for which you have enabled it. When you create a realm or a role, you can enable EES restrictions in addition to any other Host Checker policies.



NOTE: The trial package of 25 AED users has been replaced by the trial pack of 2 EES users. Trial packs are intended for proof-of-concept and trial tests. They are not intended for production use. A lab license key does not add or subtract any EES capacity.

User Experience

For endpoints that do not have VPN Tunneling or Junos Pulse already installed, the EES plugin initializes before the EES policy can be evaluated. An informational page displays on the user's endpoint to communicate the assessment status.

A significant amount of data is downloaded (approximately 5 MB for the installer and approximately 12 MB for the signatures) followed by the memory scan.

After installation, signatures are updated and the memory scan is performed to establish that no spyware is loaded in memory. If it is determined that the endpoint does not have active spyware in memory, the policy passes.

The initial installation and scan on endpoints takes some time. You should warn end users to wait for the operation to complete.

Any threat detected is automatically remediated by Host Checker and not reported. If threats cannot be remediated, the endpoint reports back to the server. Roles and user sessions can be adjusted based on endpoint compliance. A number of user strings automatically notify the end user of compliance status.

To enable and use EES antispayware:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. Under Options, select the **Advanced Endpoint Protection: Malware Protection** tab.
3. Select the **Enable Advanced Endpoint Protection: Malware Protection** check box.
4. Set the age of the signature definitions database by selecting the **Signature definitions should not be older than** check box. Enter the frequency in days (3 - 30). This function

does not change the frequency of updates. This number determines the maximum permissible age of signatures.

5. Click **Save Changes**.

When you create or configure realm or role Host Checker restrictions, you can select **Enhanced Endpoint Security: Malware Protection** to apply to that role or realm.

Related Documentation

- [Configuring Host Checker Restrictions on page 414](#)

Enabling Connection Control Host Checker Policies (Windows Only)

The pre-defined connection control Host Checker policy prevents attacks on Windows client computers from other infected computers on the same physical network.



NOTE: The Host Checker connection control policy is not supported on Windows Vista or Windows 7.

The Host Checker connection control policy blocks all incoming TCP, UDP and ICMP connections. This policy allows all outgoing TCP and VPN Tunneling traffic, as well as all connections to DNS servers, WINS servers, DHCP servers, proxy servers, and Secure Access.



NOTE: Users must have administrator privileges in order for Host Checker to enforce the connection control policy on the client computer.

To enable the pre-defined Host Checker connection control policy:

1. In the admin console, choose **Authentication > Endpoint Security > Host Checker**.
2. Under Options, select the **Create Host Checker Connection Control Policy** checkbox.
3. Click **Save Changes**. Secure Access enables the Host Checker connection control policy.



NOTE: Note that you cannot modify this policy—only enable or disable it. Also note that since you cannot modify this policy, Secure Access does not display it in the Policies section of the **Authentication > Endpoint Security > Host Checker** page with other configurable policies.

4. Implement the Host Checker connection control policy at the realm, role, or resource policy levels.

You must evaluate or enforce the connection control policy at the realm level to make the policy effective on client computers.

- Related Documentation**
- [Configuring Host Checker Restrictions on page 414](#)

Creating and Configuring New Client-side Host Checker Policies

You can create a variety of policies through the Host Checker client that check for antivirus software, firewalls, malware, spyware, and specific operating systems from a wide variety of industry leaders. You can also create checks for custom third-party DLLs, ports, processes, files, registry keys and the NetBIOS name, MAC addresses, or certificate of the client machine.



NOTE: We recommend you check for multiple MAC addresses in a single policy instead of creating a policy for each MAC address. If you create policies for each MAC address, unexpected results may occur if there are more than 100 policies due to browser cookie size limitations.

When creating the policies, you must define the policy name, and either enable pre-defined rules, or create custom rules that run the specified checks. Optionally, you can specify how Host Checker should evaluate multiple rules within a single policy.

To create a standard client-side policy:

1. In the admin console, choose **Authentication > Endpoint Security > Host Checker**.
2. Under Policies, click **New**.
3. Enter a name in the Policy Name field and then click **Continue**. (Users see this name on the Host Checker remediation page if you enable custom instructions for this policy.)
4. Create one or more rules to associate with the policy.
5. Specify how Host Checker should evaluate multiple rules within the policy.
6. (Recommended) Specify remediation options for users whose computers do not meet the requirements specified in the policy. (If you do not create remediation instructions and the policy fails, your users will not know why they cannot access their resources.)
7. Implement the policy at the realm, role, or resource policy levels.

- Related Documentation**
- [Checking for Third-Party Applications Using Predefined Rules \(Windows Only\) on page 383](#)
 - [Specifying Customized Requirements Using Custom Rules on page 394](#)
 - [Configuring General Host Checker Remediation on page 418](#)
 - [Configuring Host Checker Restrictions on page 414](#)

Checking for Third-Party Applications Using Predefined Rules (Windows Only)

Host Checker comes pre-equipped with a vast array of pre-defined rules that check for antivirus software, firewalls, malware, spyware, and specific operating systems from a wide variety of industry leaders. You can enable one or more of these rules within a Host Checker client-side policy to ensure that the integrated third party applications that you specify are running on your users' computers in accordance with your specifications. For firewall and antivirus rules, you can specify remediation actions to automatically bring the endpoint into compliance.

To view the currently supported applications, go to Authentication > Endpoint Security > Host Checker and create a new policy. You can choose predefined rule types from the Select Rule Type drop down list box to see a list of the supported applications within that category. The lists of applications can be quite extensive and are updated at each support release, so it is useful to check the list periodically.

The following predefined rule types are available:

- **Predefined: AntiVirus**—Select this option to create a rule that checks for the antivirus software that you specify, and to specify remediation options.
- **Predefined: Firewall**—Select this option to create a rule that checks for the firewall software that you specify, and to specify remediation options.
- **Predefined: Malware**—Select this option to create a rule that checks for the malware protection software that you specify.
- **Predefined: AntiSpyware**—Select this option to create a rule that checks for the anti-spyware protection software that you specify.
- **Predefined: OS Checks**—Select this option to create a rule that checks for the Windows operating systems and minimum service pack versions that you specify. (Any service pack whose version is greater than or equal to the version you specify satisfies the policy.)



NOTE: If the underlying TNCC service is killed or stopped, the endpoint can remain on the network, potentially out of compliance, until the next Host Checker policy refresh.

This section details Predefined Malware and Predefined OS check. Predefined Antivirus, Firewall and Malware checks are defined in sections that follow.

To create a Host Checker rule using Predefined Malware or Predefined OS Check rules:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy or click on an existing policy in the Policies section of the page.
3. Under Rule Settings, choose one of the following options and click **Add**:
 - Predefined Malware

- Predefined OS Checks

The predefined rule page opens.

4. In the **Rule Name field**, enter an identifier for the rule.
5. Under Criteria, select the specific malware or operating systems that you want to check for and click **Add**. (When checking for an operating system, you may also specify a service pack version.)



NOTE: When you select more than one type of software within a pre-defined rule, Host Checker considers the rule satisfied if any of the selected software applications are present on the user's machine.

6. Under Optional, select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, Secure Access initiates a new handshake to re-evaluate realm or role assignments.
7. Click **Save Changes**.
8. Optionally add additional rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

Related Documentation

- [Creating and Configuring New Client-side Host Checker Policies on page 382](#)
- [Configuring a Predefined Firewall Rule with Remediation Options \(Windows Only\) on page 386](#)
- [Configuring a Predefined Antivirus Rule with Remediation Options on page 384](#)
- [Implementing Host Checker Policies on page 412](#)

Configuring a Predefined Antivirus Rule with Remediation Options

You can configure antivirus remediation actions with Host Checker. You can specify a requirement for the age (in days) of the last successful virus scan, and you can specify that virus signatures installed on client machines should not be older than a specified number of updates.

You can also monitor policies to ensure that logged-in endpoints maintain compliance status, and remediate the endpoint to another role or realm depending on the current status.

If a client attempts to log in, and the client machine does not meet the requirements you specify, Host Checker can attempt to correct the deficiencies to allow the client to successfully log in. With Host Checker antivirus remediation, you can prompt the endpoint to download the latest virus signature files, turn on antivirus protection, and initiate an antivirus scan.

All of the remediation options are not supported for all antivirus software vendors' products. All available vendors and products that are supported are displayed when you select the Require any supported product option button.

Alternately, you can select the Require specific products/vendors option button and select either the Require any supported product from a specific vendor or Require specific products check boxes, then add an available type to Selected Types. The remediation options appear, and you can determine which remediation options are available for specific products or vendors

To configure a Predefined Antivirus rule:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy or click on an existing policy in the **Policies** section of the page.
3. Under Rule Settings, choose **Predefined: Antivirus** and click **Add**.
4. Enter the **Rule Name** for this antivirus rule.
5. To determine if your software vendor's product is supported for the System Scan check, click **these Antivirus products**. A new window will open with a list of all of the products that support the feature.
6. Select or clear the check box next to **Successful System Scan must have been performed in the last _ days**, and enter the number of days in the field.

If you select this check box, a new option appears. If the remediation action to start an antivirus scan has been successfully begun, you can override the previous check.

7. Select or clear the check box next to **Consider this rule as passed if 'Full System Scan' was started successfully as remediation**.
8. Select or clear the check box next to **Virus definition files should not be older than _ updates**. Enter a number between 1 and 10. If you enter 1, the client must have the latest update. You must import the virus signature list for the supported vendor.
9. Select your antivirus vendor(s) and product(s) by using either the **Require any supported product** or **Require specific products/vendors** option buttons.

Require any supported product allows you to check for any product (rather than requiring you to select every product separately). This option button reveals a list of products in the remediation section to allow you to enable remediation options which are product specific.

Require specific products/vendors allows you to define compliance by allowing any product by a specific vendor (for example, any Symantec product).

Require specific products provides functionality that allows you to select individual products to define compliance.

After you select your vendor(s) and product(s), remediation options will appear on the page.

For each of the following remediation actions:

- **Download latest virus definition files**—obtains the latest available file for the specified vendor from the vendor’s website
- **Turn on Real Time Protection**—launches the virus scanning mechanism for the specified vendor
- **Start Antivirus Scan**—performs a real-time virus scan for the specified vendor
the check box is active (clickable) if the action is supported for your product.

If your antivirus product is not supported, you can click the remediation column headers to determine what vendors and products are supported.

10. If your product is supported, select the check box for any or all of the remediation actions that you want to apply.
11. Under Optional, select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, Secure Access initiates a new handshake to re-evaluate realm or role assignments.
12. Click **Save Changes** to save the antivirus rule and enforce antivirus remediation.
13. Optionally add additional rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

Related Documentation

- [Configuring Virus Signature Version Monitoring and Patch Assessment Data Monitoring on page 388](#)
- [Creating and Configuring New Client-side Host Checker Policies on page 382](#)
- [Implementing Host Checker Policies on page 412](#)

Configuring a Predefined Firewall Rule with Remediation Options (Windows Only)

You can configure firewall remediation actions with Host Checker after you create a Host Checker firewall rule that requires the endpoint to have a specific firewall installed and running prior to connecting to the network.

After you enforce the Host Checker rule with firewall remediation actions, if an endpoint attempts to log in without the required firewall running, Host Checker can attempt to enable the firewall on the client machine.

The remediation option is not supported for all firewall products. All available products are displayed by using the Require any supported product or Require specific products/vendors option buttons.

To configure a Host Checker Predefined Firewall rule:

1. In the admin console, choose **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy or click an existing policy in the Policies section of the page.

3. Under Rule Settings, choose **Predefined: Firewall** and click **Add**.
4. Enter a **Rule Name** for the firewall rule.
5. Select your firewall vendor(s) and product(s) by using either the **Require any supported product** or **Require specific products/vendors** option buttons.

Require any supported product allows you to check for any product (rather than requiring you to select every product separately). This option button reveals a list of products in the remediation section to allow you to enable remediation options which are product specific.

When you add an available product to Selected Products, the remediation option appears, and you can determine if the remediation option is available for your selected firewall.

Require specific products/vendors allows you to define compliance by allowing any product by a specific vendor (for example, any Symantec product).

Require specific products provides functionality that allows you to select individual products to define compliance.

After you select your vendor(s) and product(s), the remediation options will appear on the page. The Turn on Firewall check box is active (clickable) if the action is supported for your product.

6. If your firewall is supported, select the check box to **Turn on Firewall**.
7. Under Optional, select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, Secure Access initiates a new handshake to re-evaluate realm or role assignments.
8. Click **Save Changes** to save the firewall rule and enforce firewall remediation.
9. Optionally add additional rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

**Related
Documentation**

- [Creating and Configuring New Client-side Host Checker Policies on page 382](#)
- [Implementing Host Checker Policies on page 412](#)

Configuring a Predefined AntiSpyware Rule (Windows Only)

You can configure Host Checker to check for installed antispyware on endpoints.

After you enforce the Host Checker rule, if an endpoint attempts to log in without the required spyware, the Host Checker rule will fail.

The option is not supported for all spyware products. All available products are displayed by using the Require any supported product or Require specific products/vendors option buttons.

To configure a Host Checker Predefined Spyware rule:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy or click an existing policy in the Policies section of the page.
3. Under Rule Settings, choose **Predefined: AntiSpyware** and click **Add**.
4. Enter a **Rule Name** for the firewall rule.
5. Select one of the following options:
 - Select the **Require any supported product** option button to check for any product (rather than requiring you to select every product separately).
 - Select the **Require specific products/vendors** option button to specify the spyware that you want to check for.
 - Choose either the **Require any supported product from a specific vendor** or **Require specific products** to specify spyware.
 - Add antispyware from Available Products to Selected Products.
6. Under Optional, select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, Secure Access initiates a new handshake to re-evaluate realm or role assignments.
7. Click **Save Changes**.
8. Optionally add additional rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

Related Documentation

- [Creating and Configuring New Client-side Host Checker Policies on page 382](#)
- [Implementing Host Checker Policies on page 412](#)

Configuring Virus Signature Version Monitoring and Patch Assessment Data Monitoring

You can configure Host Checker to monitor and verify that the virus signatures, operating systems, software versions, and patches installed on client computers are up to date, and remediate those endpoints that do not meet the specified criteria. Host Checker uses the current virus signatures and patch assessment versions from the vendor(s) you specify for pre-defined rules in a Host Checker policy.

You can automatically import the current Virus signature version monitoring or Patch Management Info Monitoring lists from the Juniper Networks staging site at a specified interval, or you can download the files from Juniper and use your own staging server.

You can also configure a proxy server as a staging site between Secure Access and the Juniper site. To use a proxy server, you enter the servers network address, port and authentication credentials, if applicable.

To access the Juniper Networks staging site for updates, you must enter the credentials for your Juniper Networks Support account.

To configure Secure Access to automatically import the current virus signature version monitoring and patch management version monitoring list(s) from the Juniper staging site:

1. Choose **Authentication > Endpoint Security > Host Checker**.
2. Click **Virus signature version monitoring**, or **Patch Management Info Monitoring**.
3. Select **Auto-update virus signatures list** or **Auto-update Patch Management data**.
4. For **Download path**, leave the existing URL(s) of the staging site(s) where the current list(s) are stored. The default URLs are the paths to the Juniper Networks staging site:
https://download.juniper.net/software/av/uac/epupdate_hist.xml
 (for auto-update virus signatures list)
<https://download.juniper.net/software/hc/patchdata/patchupdate.dat>
 (for auto-update patch management)
5. For **Download interval**, specify how often you want Secure Access to automatically import the current list(s).
6. For **Username** and **Password**, enter your Juniper Networks Support credentials.
7. Click **Save Changes**.

To manually import the current virus signature version monitoring and patch management version monitoring list(s):

1. Choose **Authentication > Endpoint Security > Host Checker**.
2. Click **Virus signature version monitoring**, or **Patch Management Info Monitoring**.
3. Download the list(s) from the Juniper staging site to a network server or local drive on your computer by entering the Juniper URLs in a browser window.
https://download.juniper.net/software/av/uac/epupdate_hist.xml
<https://download.juniper.net/software/hc/patchdata/patchupdate.dat>
4. Under **Manually import virus signatures list**, click **Browse**, select the list, and then click **OK**.
5. Click **Save Changes**.



NOTE: If you use your own staging site for storing the current list(s), you must upload the trusted root certificate of the CA that signed the staging's server certificate to Secure Access.

To use a proxy server as the auto-update server:

1. Choose **Authentication > Endpoint Security > Host Checker**.
2. Click **Virus signature version monitoring**, or **Patch Management Info Monitoring**.
3. Select **Auto-update virus signatures list** or **Auto-update Patch Management data**.

4. For **Download path**, leave the existing URL(s) of the staging site(s) where the current list(s) are stored. The default URLs are the paths to the Juniper Networks staging site:
`https://download.juniper.net/software/av/uac/epupdate_hist.xml`
(for auto-update virus signatures list)
`https://download.juniper.net/software/hc/patchdata/patchupdate.dat`
(for auto-update patch management)
5. For **Download interval**, specify how often you want Secure Access to automatically import the current list(s).
6. For **Username** and **Password**, enter your Juniper Networks Support credentials.
7. Select the check box for **Use Proxy Server**.
8. Enter the **IP Address** of your proxy server.
9. Enter the **Port** that the Juniper Networks Support site will use to communicate with your proxy server.
10. If your proxy server is password protected, type the **Username** and **Password** of the proxy server.
11. Click **Save Changes**.

Related Documentation

- [Uploading Trusted Server CA Certificates on page 865](#)
- [Implementing Host Checker Policies on page 412](#)

Patch Management Info Monitoring and Patch Deployment

You can configure Host Checker policies that check for Windows endpoint's operating system service pack, software version, or desktop application patch version compliance. Host Checker uses a list of the most current patch versions from the vendor for predefined rules in the Host Checker policy. Host Checker does not scan for non-security patches.

You obtain the most current patch version information from a Juniper Networks staging site. You can manually download and import the list into the Secure Access Service, or you can automatically import the list from the Juniper Networks staging site or your own staging site at a specified interval.

Monitoring is based on either one or more specified products or on specific patches, though not in the same policy. For example, you could check for Internet Explorer Version 7 with one policy, and Patch MSOO-039: SSL Certificate Validation Vulnerabilities with a second policy. Then, apply both policies to endpoints at the role or realm level to ensure that the user has the latest browser version with a specific patch. In addition, for Microsoft products, you can specify the severity level of patches that you wish to ignore. For example, you could ignore low or moderate threats.

The Secure Access Service can send remediation instructions (such as a message describing what patches or software are non-compliant, and a link to where the endpoint can obtain the patch). The Secure Access Service does not autoremediate in the event

of a non-compliant endpoint. However, you can send the items to the client for manual remediation of managed machines.

When an endpoint first connects to the Secure Access Service, the latest versions of the data files and libraries of the IMC are downloaded to the host computer. The initial check takes 10- 20 seconds to run, depending on the link speed. If the files are outdated, they are automatically updated at subsequent checks. If this is the first time the endpoint has connected to the Secure Access Service with the patch assessment policy, and the connection is a Layer 2 connection, the IMC required to run the Patch Assessment check cannot download. In this case, you should configure a remediation role that displays instructions to direct the user to retry with a Layer 3 connection or contact the administrator.

Note that in non-English installations, the English version of local patches is displayed.

Additional Functionality with Pulse 2.0

With Pulse 2.0, additional functionality is provided for Patch Info Monitoring and Deployment.

Endpoints with Pulse 2.0 that are not in compliance with specified patch policies can be updated with the required patches and brought into compliance automatically. This is achieved through a new patch deployment engine. The patch deployment engine executes on endpoints, downloads specified patches, and installs patches that are required through the Host Checker policy. The patch deployment engine provides a new means of remediating endpoints that do not meet the patch assessment policies defined on the Secure Access Service. This functionality is available for Windows XP, and Vista and Windows 7 32 bit and 64 bit versions.

The Host Checker IMC on the endpoint interfaces with the patch deployment engine to download and install missing patches reported by the IMV. When the patch installation is complete, the IMC signals the TNC client to start a new handshake with the Secure Access Service, and enables the Secure Access Service to make access control decisions based on the result of the handshake.

Endpoints without Pulse 2.0 can still use the legacy basic patch remediation mechanism, in which a pre-installed SMS client is triggered to get patches from a pre-configured SMS server. This mechanism installs only those patches that are published on the SMS server. If the SMS client is not installed, or the server doesn't host the patches required by the policies on Secure Access Service, the endpoint cannot be fully remediated.

The patch deployment engine is an executable file that is hosted on the Secure Access Service. The executable can be downloaded to any endpoint that you would like to remediate. Unlike the SMS client, one can specify what patches need to be applied. The patch deployment engine directly downloads missing patches from vendor websites, without going through the Secure Access Service. Therefore, Internet connectivity is needed for Shavlik remediation to work. The patch deployment engine does not work with Layer 2 without Layer 3 connectivity. You can configure a remediation VLAN for post authentication. Once Layer 3 connectivity is obtained, endpoints can remediate successfully. With Layer 3 connectivity, the patch deployment engine downloads missing patches.

A separate license is required for patch info monitoring and deployment functionality. It is not available as part of the endpoint solution.

All of the files required for patch deployment are a part of a ESAP packages beginning with Secure Access Service software version 7.1. The default ESAP package shipped with Series SSL VPN Appliance software version 7.1 contains the required patch deployment files. Any older ESAP packages fail to update on these devices.

The IMC and IMV for patch monitoring is backward compatible. Since this feature is available from Pulse 2.0 onward, a new Pulse communicating with an older IMV (with Pulse support), or a new IMV communicating to an older IMC exhibit the same behavior as today. There should be no change in the patch assessment, and Shavlik's deployment engine is not invoked for remediation.

User Experience

Patch remediation can take a good deal of time, and policies continue to fail until the process is completed. When an update is required, the user is given an option to proceed with patch deployment. If the user decides not to deploy the patch(es) and proceed, the user may not have connectivity or may have limited connectivity, depending on the Secure Access Service administration configuration. If any patches require a reboot subsequent to installation, the application informs Host Checker, and Pulse notifies the user. In this case, until the machine is rebooted, patches continue to be reported as missing in subsequent patch assessments. If a reboot is required, any further patch deployment is not carried out until the machine is rebooted. The user is notified if a reboot is required.

Pulse notifies the user that patches need to be installed, and provides status as the download is occurring. When the installation is complete, the client presents the login dialogue.

Using a System Management Server

You can use a System Management Server (SMS) to provide a method for automatic updates to non-compliant software.

Pulse 2.0 can support either the SMS download method or the patch deployment engine for patch deployment, depending on the configuration on the Secure Access Service. If the Secure Access Service is configured for the SMS method for patch deployment, the client machine should have the SMS client already installed in the machine for deployment to begin, otherwise remediation fails.

Endpoints configured with SMS for software management typically poll the server for updates every fifteen minutes or longer. In a worst-case scenario, clients that are not in compliance with existing Host Checker software requirements might have to wait until the next update interval to login.

Using the SMS download method, you can force the client to initiate the software update immediately after the patch assessment check.

If a user attempts to log in, and the endpoint does not have a required software version for compliance with a Host Checker patch assessment policy, Host Checker immediately

notifies the client to poll the server for an immediate update. The client receives notification that an SMS update has started.

To configure SMS to update the client when notified, set the advertisement time on the SMS to As soon as possible. The following process then occurs:

- The Secure Access Service patch assessment policy specifies the required software.
- When an endpoint attempts to authenticate, Host Checker evaluates the client and sends the results back to the Secure Access Service.
- The Secure Access Service evaluates the results and sends reason strings and remediation information to the client, including a message that directs the client to poll the server for software advertisements immediately.
- The SMS client queries the SMS server for software advertisements.
- The server identifies what patches should be advertised to the client (this is configured on the server, Host Checker does not interact with the server).
- The SMS client receives the advertisement and applies the required patch(es).

You assign clients to a particular group or collection on the server. Then the SMS server can advertise patches for that collection. You can configure roles on the Secure Access Service that correspond to collections, and SMS can send the appropriate patches for a particular role.

You must have the SMS client installed and configured correctly on endpoints, and the SMS server must be reachable. In a Layer 2 network, Host Checker is performed before the endpoint is connected to the network. Host Checker can obtain the IP address of the SMS server configured for the client. If the endpoint is out of compliance and remediation is necessary, Host Checker pings the server IP address every 15 seconds until the server can be notified to update the client.

It is important as an administrator to inform users of the expected behavior if this feature is enabled, as there is no notification to the user until the SMS sends back the advertisement.

Juniper Networks recommends only one patch deployment on the endpoint at any point in time. However, there is no way to determine if an SMS update is in progress, and so it may be possible that the patch deployment engine is started while a SMS Update is also occurring (this could happen if Pulse is connected to two IC Series or Secure Access Services with one using SMS remediation and the other using the patch deployment engine). Given the fact that most patches will not allow two instances to be running, one of the remediations fail, depending on which began first.

The Admin Console allows you to select only one of the remediation options (either SMS or patch deployment engine) for all the policies.

If Pulse is connected to more than one IC Series or Secure Access Service, and one requires patch deployment engine remediation and the other requires SMS remediation, both requests are met. If both require the patch deployment engine method, the requests are queued.

Specifying Customized Requirements Using Custom Rules

In addition to the predefined policies and rules that come with Secure Access, you can create custom rules within a Host Checker policy to define requirements that your users' computers must meet. Using custom rules, you can:

- Configure remote integrity measurement verifiers (IMVs) to perform customized client-side checks.
- Configure Host Checker to check for custom DLLs that perform customized client-side checks.
- Verify that certain ports are open or closed on the user's computer.
- Confirm that certain processes are or are not running on the user's computer.
- Check that certain files are or are not present on the client machine.
- Evaluate the age and content of required files through MD5 checksums.
- Confirm that registry keys are set on the client machine.
- Confirm the NETBIOS name of the client machine.
- Confirm the MAC addresses of the client machine.
- Check the validity of the machine certificate that is installed on the user's computer.



NOTE: You can only check for registry keys, third-party DLLs, NETBIOS names, MAC addresses, and machine certificates on Windows computers.

To create a client-side Host Checker policy:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy or click an existing policy in the Policies section of the page.
3. Click the tab that corresponds to the operating system for which you want to specify Host Checker options—Windows, Mac, Linux or Solaris. In the same policy, you can specify different Host Checker requirements on each operating system. For example, you can create one policy that checks for different files or processes on each operating system.



NOTE: You must explicitly create policies for each operating system you want to allow. For example, if you create a Windows Host Checker policy, but don't create one for Mac or Linux, users who sign into Secure Access from a Mac or Linux machine will not comply with the Host Checker policy and therefore will not be able to access the realm, role, or resource on which you enforce Host Checker.

4. Under Rule Settings, choose the options in the following sections and click **Add**. The Add Custom Rule page for the rule type appears.

- **Custom: Remote IMV**—Use this rule type to configure integrity measurement software that a client must run to verify a particular aspect of the client's integrity, such as the client's operating system, patch level, or virus protection.
- **3rd Party NHC Check (Windows only)**—Use this rule type to specify the location of a custom DLL. Host Checker calls the DLL to perform customized client-side checks. If the DLL returns a success value to Host Checker, then Secure Access considers the rule met. In the 3rd Party NHC Check configuration page:
 - a. Enter a name and vendor for the 3rd Party NHC Check rule
 - b. Enter the location of the DLL on client machines (path and file name).
 - c. Click **Save Changes**.

The 3rd Party NHC Check feature is primarily provided for backwards compatibility. We recommend that you use IMCs and IMVs instead
- **Ports**—Use this rule type to control the network connections that a client can generate during a session. This rule type ensures that certain ports are open or closed on the client machine before the user can access Secure Access. In the Ports configuration page:
 - a. Enter a name for the port rule.
 - b. Enter a comma delimited list (without spaces) of ports or port ranges, such as: 1234,11000-11999,1235.
 - c. Select **Required** to require that these ports are open on the client machine or **Deny** to require that they are closed.
 - d. Under Optional, select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, Secure Access initiates a new handshake to re-evaluate realm or role assignments.
 - e. Click **Save Changes**.
- **Process**—Use this rule type to control the software that a client may run during a session. This rule type ensures that certain processes are running or not running on the client machine before the user can access resources protected by Secure Access. In the Processes configuration page:
 - a. Enter a name for the process rule.
 - b. Enter the name of a process (executable file), such as: good-app.exe.



NOTE: For Linux, Macintosh and Solaris systems, the process that is being detected must be started using an absolute path.

You can use a wildcard character to specify the process name.

For example: good*.exe

- c. Select **Required** to require that this process is running or **Deny** to require that this process is not running.
 - d. Specify the MD5 checksum value of each executable file to which you want the policy to apply (optional). For example, an executable may have different MD5 checksum values on a desktop, laptop, or different operating systems. On a system with OpenSSL installed—many Macintosh, Linux and Solaris systems have OpenSSL installed by default—you can determine the MD5 checksum by using this command: `openssl md5 <processFilePath>`
 - e. Click **Save Changes**.
- **File**—Use this rule type to ensure that certain files are present or not present on the client machine before the user can access Secure Access. You may also use file checks to evaluate the age and content (through MD5 checksums) of required files and allow or deny access accordingly. In the Files configuration page:
 - a. Enter a name for the file rule.
 - b. Enter the name of a file (any file type), such as: `c:\temp\bad-file.txt` or `/temp/bad-file.txt`.

You can use a wildcard character to specify the file name. For example:

*.txt

You can also use an environment variable to specify the directory path to the file. (You cannot use a wildcard character in the directory path.) Enclose the variable between the `<%` and `%>` characters. For example:

`<%windir%>\bad-file.txt`

- c. Select **Required** to require that this file is present on the client machine or **Deny** to require that this file is not present.
- d. Specify the minimum version of the file (optional). For example, if you require notepad.exe to be present on the client, you can enter 5.0 in the field. Host Checker accepts version 5.0 and above, of notepad.exe.
- e. Specify the maximum age (File modified less than n days) (in days) for a file (optional). If the file is older than the specified number of days, then the client does not meet the attribute check requirement.



NOTE: You can use the maximum age option to check the age of virus signatures. Make sure you specify the path to a file in the File Name field whose timestamp indicates when virus signatures were last updated, such as a virus signature database or log file that updates each time the database updates. For example, if you use TrendMicro, you may specify:

`C:\Program Files\Trend Micro\OfficeScan Client\TmUpdate.ini`

- f. Specify the MD5 checksum value of each file to which you want the policy to apply (optional). On Macintosh, Linux and Solaris, you can determine the MD5 checksum by using this command: `openssl md5<filePath>`
 - g. Select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change in compliance status on an endpoint that has successfully logged in occurs, Secure Access initiates a new handshake to re-evaluate realm or role assignments.
 - h. Click **Save Changes**.
- **Registry Setting (Windows only)**—Use this rule type to control the corporate PC images, system configurations, and software settings that a client must have to access Secure Access. This rule type ensures that certain registry keys are set on the client machine before the user can access Secure Access. You may also use registry checks to evaluate the age of required files and allow or deny access accordingly. In the Registry Settings configuration page:
 - a. Enter a name for the registry setting rule.
 - b. Select a root key from the drop-down list.
 - c. Enter the path to the application folder for the registry subkey.
 - d. Enter the name of the key's value that you want to require (optional). This name appears in the Name column of the Registry Editor.
 - e. Select the key value's type (String, Binary, or DWORD) from the dropdown list (optional). This type appears in the Type column of the Registry Editor.
 - f. Specify the required registry key value (optional). This information appears in the Data column of the Registry Editor.

If the key value represents an application version, select Minimum version to allow the specified version or newer versions of the application. For example, you can use this option to specify version information for an antivirus application to make sure that the client antivirus software is current. Secure Access uses lexical sorting to determine if the client contains the specified version or higher. For example:

3.3.3 is newer than 3.3

4.0 is newer than 3.3

4.0a is newer than 4.0b

4.1 is newer than 3.3.1



NOTE: If you specify only the key and subkey, Host Checker simply verifies the existence of the subkey folder in the registry.

- g. Under Optional, select **Monitor this rule for change in result** to continuously monitor the policy compliance of endpoints. If this check box is selected, and a change

in compliance status on an endpoint that has successfully logged in occurs, Secure Access initiates a new handshake to re-evaluate realm or role assignments.

You can configure registry setting remediation actions with Host Checker. If a client attempts to login, and the client machine does not meet the requirements you specify, Host Checker can attempt to correct the discrepancies to allow the client to login.

h. Select the check box for **Set Registry value specified in criteria**.

i. Click **Save Changes**.

- **NetBIOS (Windows only, does not include Windows Mobile)**—Use this rule type to check the NetBIOS name of the client machine before the user can access Secure Access. In the NetBIOS configuration page:

a. Enter a name for the NetBIOS rule.

b. Enter a comma-delimited list (without spaces) of NetBIOS names. The name can be up to 15 characters in length. You can use wildcard characters in the name and it is not case-sensitive. For example, md*, m*xp and *xp all match MDXP.

c. Select **Required** to require that NETBIOS name of the client machine match one of the names you specify, or **Deny** to require that the name does not match any name.

d. Click **Save Changes**.

- **MAC Address (Windows only)**—Use this rule type to check the MAC addresses of the client machine before the user can access Secure Access. In the MAC Address configuration page:

a. Enter a name for the MAC address rule.

b. Enter a comma-delimited list (without spaces) of MAC addresses in the form XX:XX:XX:XX:XX:XX where the X's are hexadecimal numbers. For example:

00:0e:1b:04:40:29

You can use a * wildcard character to represent a two-character section of the address. For example, you can use a * to represent the "04", "40", and "29" sections of the previous example address:

00:0e:1b:*:*

But you cannot use a * to represent a single character. For example, the * in the following address is not allowed:

00:0e:1b:04:40:*9

c. Select **Required** to require that a MAC address of the client machine matches any of the addresses you specify, or **Deny** to require that the all addresses do not match. A client machine will have at least one MAC address for each network connection, such as Ethernet, wireless, and VPN. This rule's requirement is met

if there is a match between any of the addresses you specify and any MAC address on the client machine.

- d. Click **Save Changes**.



NOTE: Since the MAC address is changeable on some network cards, this check may not guarantee that a client machine meets the requirements of your Host Checker policy.

- **Machine Certificate (Windows only)**—Use this rule type to check that the client machine is permitted access by validating the machine certificate stored on the client machine. In the Machine Certificate configuration page:
 - a. Enter a name for the machine certificate rule.
 - b. From the Select Issuer Certificate list, select the certificate that you want to retrieve from the user's machine and validate. Or, select Any Certificate to skip the issuer check and only validate the machine certificate based on the optional criteria that you specify below.
 - c. From the Optional fields (Certificate field and Expected value), specify any additional criteria that Host Checker should use when verifying the machine certificate.
 - d. Click **Save Changes**.



NOTE: If more than one certificate is installed on the client machine that matches the specified criteria, The Host Checker client passes the first certificate it finds to Secure Access for validation.

5. Optionally add additional rules to the policy, specify how Host Checker should evaluate multiple rules within the policy, and define remediation options.

Related Documentation

- [Implementing Host Checker Policies on page 412](#)
- [Task Summary: Configuring Host Checker on page 376](#)
- [Using a Wildcard or Environment Variable in a Host Checker Rule on page 399](#)

Using a Wildcard or Environment Variable in a Host Checker Rule

You can use the following wildcards to specify a file name in a **Custom File** rule or a process name in a **Custom Process** rule:

Table 33: Wildcard Characters for Specifying a File Name or Process Name

Wildcard Character	Description	Example
*	Matches any character	*.txt

Table 33: Wildcard Characters for Specifying a File Name or Process Name (continued)

Wildcard Character	Description	Example
?	Matches exactly one character	app-?.exe

In a **Custom File** rule for Windows, you can use the following environment variables to specify the directory path to a file:

Table 34: Environment Variables for Specifying a Directory Path on Windows

Environment variable	Example Windows Value
<%APPDATA%>	C:\Documents and Settings\jdoe\Application Data
<%windir%>	C:\WINDOWS
<%ProgramFiles%>	C:\Program Files
<%CommonProgramFiles%>	C:\Program Files\Common Files
<%USERPROFILE%>	C:\Documents and Settings\jdoe
<%HOMEDRIVE%>	C:
<%Temp%>	C:\Documents and Settings\ <user name="">\Local Settings\Temp</user>

In a **Custom File** rule for Linux and Solaris, you can use the following environment variables to specify the directory path to a file:

Table 35: Environment Variables for Specifying a Directory Path on Linux and Solaris

Environment variable	Example Linux and Solaris Values
<%java.home%>	/local/local/java/j2sdk1.4.1_02/jre
<%java.io.tmpdir%>	/tmp
<%user.dir%>	/home-shared/cknouse
<%user.home%>	/home/cknouse

In a **Custom File** rule for Macintosh, you can use the following environment variables to specify the directory path to a file.

Table 36: Environment Variables for Specifying a Directory Path on Macintosh

Environment variable	Example Macintosh Value
<%HOME%>	/Users/admin where <i>admin</i> is the logged in user name
<%USER%>	Maps to the login name of the MAC machine



NOTE: Although environment variables are formatted in the same way as Toolkit Template directives, they are not interchangeable and you should not confuse them.

Related Documentation

- [Specifying Customized Requirements Using Custom Rules on page 394](#)
- [Implementing Host Checker Policies on page 412](#)

Configuring Patch Assessment Policies

You can configure Host Checker policies that check for Windows endpoint's operating system service pack, software version, or desktop application patch version compliance.

Host Checker uses a list of the most current patch versions from the vendor for predefined rules in the Host Checker policy.

You obtain the most current patch version information from a staging site at Juniper Networks. You can manually download and import the current list into the Secure Access Service, or you can automatically import the current list from the Juniper Networks staging site or your own staging site at the specified interval.

Checks can be based on one or more specified products or on specific patches, though not in the same policy. For example, you could check for Internet Explorer version 7 with one policy, and Patch MSOO-039: SSL Certificate Validation Vulnerabilities with a second policy. Then, apply both policies to endpoints at the role or realm level to ensure that the user has the latest browser version with a specific patch. Additionally, you can specify the severity level of patches that you wish to ignore for Microsoft products; for example, you could choose to ignore low or moderate threats.

The Secure Access Service can send remediation instructions (e.g. a message describing what patches or software are non-compliant, and a link to where the endpoint can obtain the patch). The Secure Access Service does not auto-remediate in the event of a non-compliant endpoint. However, you can choose to send the items to the client for manual remediation of managed machines.

When an endpoint first connects to the Secure Access Service, the latest versions of the data files and libraries of the IMC are downloaded to the host computer. The initial check takes 10- 20 seconds to run, depending on the link speed. If outdated, these files are automatically updated at subsequent checks. If this is the first time the endpoint has connected to the Secure Access Service with the patch assessment policy, and the

connection is a Layer 2 connection, the IMC required to run the Patch Assessment check cannot download. In this case, you should configure a remediation role which displays instructions to direct the user to retry with a Layer 3 connection or contact the administrator.

Note that in non-English installations, the English version of local patches is displayed.

Using a System Management Server

For Windows clients, you can use a System Management Server (SMS) to provide a method for automatic updates to non-compliant software.

Endpoints configured with SMS for software management typically poll the server for updates every fifteen minutes or longer. In a worst-case scenario, clients that are not in compliance with existing Host Checker software requirements may have to wait until the next update interval to login.

Using the SMS remediation feature, you can force the client to initiate the software update immediately after the patch assessment check.

If a user attempts to log in, and the endpoint does not have a required software version for compliance with a Host Checker patch assessment policy, Host Checker immediately notifies the client to poll the server for an immediate update. The client receives notification that an SMS update has started.

To have the SMS update the client when notified, set the advertisement time on the SMS to As soon as possible.

- The Secure Access Service patch assessment policy specifies the required software.
- When an endpoint attempts to authenticate, Host Checker evaluates the client and sends the results back to the Secure Access Service.
- The Secure Access Service evaluates the results and sends reason strings and remediation information to the client, including a message that directs the client to poll the server for software advertisements immediately.
- The SMS client queries the SMS server for software advertisements.
- The server identifies what patches should be advertised to the client (this is configured on the server, Host Checker does not interact with the server).
- The SMS client receives the advertisement and applies the required patch(es).

You assign clients to a particular group or collection on the server, then the SMS can advertise patches for that collection. You can configure roles on the Secure Access Service that correspond to collections, and SMS can send the appropriate patches for a particular role.

You must have the SMS client installed and configured correctly on endpoints, and the SMS server must be reachable. In a Layer 2 network, Host Checker is performed before the endpoint is connected to the network. Host Checker can obtain the IP address of the SMS server configured for the client. If the endpoint is out of compliance and remediation

is necessary, Host Checker pings the server IP address every 15 seconds until the server can be notified to update the client.

It is important as an administrator to inform users of the expected behavior if this feature is enabled, as there is no notification to the user until SMS sends back the advertisement.

**Related
Documentation**

- [Configuring Patch Assessment Rules on page 403](#)

Configuring Patch Assessment Rules

To configure a patch assessment custom rule:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. Create a new policy or click on an existing policy in the Policies section of the page.
3. Click the **Windows** tab.
4. Under Rule Settings, choose **Custom: Patch assessment**.
5. Click **Add** under Rule Settings. The Add Custom Rule:Patch assessment page appears.
6. Enter a name for the integrity measurement rule.



NOTE: If a selection that is not applicable is included in a policy, i.e. the endpoint does not have the targeted software, the rule will be ignored and the check for that particular selection will pass.

7. Select either **Scan for specific products** or **Scan for specific patches**.

If you select Scan for specific products you must further select either All Products or Specific Products.

If you select All Products, Host Checker checks for all of the exposed patches on the endpoint.

To configure a policy based on specific products:

- a. Choose the **All Products** option button.
- b. Optionally, select specific patches that you wish to ignore for all products by clicking the **Add** button under Ignore following patches.
- c. Click **Save Changes**.
- d. Optionally, for Microsoft products, clear the check boxes to determine the severity level of the patches that you wish to ignore. For example, if you wanted to check for only critical patches for the selections, clear the check boxes for **Important**, **Moderate**, **Low**, and **Unspecified**.
- e. Click **Save Changes**.

If you select **Specific Products**, two new dialogs open. You can select from an extensive listing of products and versions, and you can choose to ignore specific patches.

For example, if you add Internet Explorer 6 to the Selected Products list, you can choose to ignore any patches that you do not consider critical for the product. You can further fine-tune the severity level of specific patches to be ignored by clearing the severity check boxes for Microsoft products.

To configure a policy based on specific products:

- a. Choose the **Specific Products** option button.
- b. Select software from the Available products window and add to the Selected products window.
- c. Click **Save Changes**.
- d. Optionally, select specific patches that you wish to ignore for the chosen products by clicking the **Add** button under Ignore following patches.

When you click the Add button, a new dialog opens, displaying all of the available patches for the software you have selected.

- e. Select specific patches that you wish to ignore from the Available patches window and add to the Selected patches window.
- f. Click the **Add** button under Add.

When you click the Add button, the Ignore following patches window is populated with the patches you have chosen.

- g. Optionally, for Microsoft products, clear the check boxes to determine the severity level of the patches that you wish to ignore. For example, if you wanted to check for only critical patches for the selections, clear the check boxes for **Important**, **Moderate**, **Low**, and **Unspecified**.



NOTE: The severity level check boxes only apply to Microsoft products. For other vendors, such as Adobe, the Unspecified check box determines whether or not the check will be run.

- h. Click **Save Changes**.

The Scan for specific patches option allows you to choose from a list of all available patches.

To configure a policy based on patches:

- a. Choose the **Scan for specific patches** option button.

When you select the Scan for specific patches option a new dialog opens, allowing you to add specific patches.

- b. Click the **Add** button.

- c. Select specific patches that you wish to check for from the Available patches window and add to Selected patches.
 - d. Click the **Add** button.
 - e. Click **Save Changes**.
8. Click **Save Changes**.
 9. To direct the Secure Access Service to notify the SMS server to update the client in the event of a failed Patch Assessment rule, select Enable SMS patch update. SMS remediation will be triggered each time Host Checker detects that an endpoint is not compliant.
 10. Click **Save Changes**.

You can display remediation information for users based on which patch/version needs to be updated. For example, you can configure a reason string to display information about a patch that is missing and specify a link to take the user to the web page to get the patch.
 11. To display remediation information to users, select the Send Reason Strings option under Remediation on the main Host Checker Policy page.

**Related
Documentation**

- [Configuring Patch Assessment Policies on page 401](#)
- [Implementing Host Checker Policies on page 412](#)

Using Third-party Integrity Measurement Verifiers

The Trusted Network Connect (TNC) standard enables the enforcement of security requirements for endpoints connecting to networks. The client-side components of the TNC are the IMCs and the TNC-client (TNCC). The TNCC compiles the IMC measurements and sends them to the server. At the server, there is a corresponding set of components: the TNC-server (TNCS) and the IMVs. The TNCS manages the messages between the IMVs and the IMCs and sends the recommendations, based on the IMVs, to the policy engine. This type of rule is available for Host Checker policies on all platforms.

Secure Access and Host Checker comply with the standards produced by the TNC. For more information about the TNC, IMVs and IMCs, see www.trustedcomputinggroup.org.

You can configure Host Checker to monitor third-party TNC-compliant IMCs installed on client computers. To do so, you must:

1. Run the Third-party Integrity Measurement Verifier (IMV) Server installer on the system designated as the remote IMV server. Install the third-party IMVs and create the server certificates.
2. Specify the remote IMV server so that Secure Access can communicate with it.
3. Implement the Host Checker policy.

- Related Documentation**
- [Configuring a Remote IMV Server on page 406](#)
 - [Implementing the Third-Party IMV Policy on page 411](#)

Configuring a Remote IMV Server



NOTE:

- In an Active/Passive cluster, the Active/Passive nodes' individual IP addresses must be added to the RIMV as the Secure Access IP addresses.
- The successful addition of remote IMV server is not logged in the event log.
- When Host Checker fails, custom instructions are not displayed. There is no user access log on Secure Access about Host Checker failure.

During this step, you install third-party IMVs. Third-party IMVs are installed on the remote IMV server, not on Secure Access.

During this step, you also obtain a server certificate for the remote IMV server. You import the trusted root CA certificate of the CA that generated the server certificate onto Secure Access. Secure Access then authenticates with the remote IMV server through the certificate. If you do not have a certificate authority, install and use OpenSSL to generate a CA certificate.

To install, configure, and implement the server software:

1. In the admin console of Secure Access, choose **Maintenance > System > Installers** and download the Third-party Integrity Measurement Verifier (IMV) Server installer.
2. Run the installer on the system designated as the remote IMV server.
3. Install the third-party IMVs on the remote IMV server and the corresponding IMCs on the client systems.
4. Generate a server certificate from a certificate authority for the remote IMV server. The server's certificate Subject CN value must contain the actual host name or IP address of the remote IMV server.

The server certificate and the private key must be combined into a single PKCS#12 file and encrypted with a password.

If you do not have a certificate authority, you can use the following steps to create a CA and then create a server certificate for the remote IMV server.



NOTE: Install the full version of OpenSSL. The "light" version of OpenSSL will not work.

Follow the steps below to set up OpenSSL:

- a. Download and install OpenSSL from this site:

<http://www.slproweb.com/products/Win32OpenSSL.html>

- b. At the Windows command prompt, type the following commands:

```
cd \openssl
md certs
cd certs
md demoCA
md demoCA\newcerts
edit demoCA\index.txt
```

- c. Press the **ALT-F** keys and then the **S** key to save the file.
- d. Press the **ALT-F** keys and then the **X** key to exit the editor.
- e. At the Windows command prompt, type the following commands:

```
edit demoCA\serial
```
- f. Type the following in the document window: **01**
- g. Press the **ALT-F** keys and then the **S** key to save the file.
- h. Press the **ALT-F** keys and then the **X** key to exit the editor.
- i. At the Windows command prompt, type the following commands:

```
set path=c:\openssl\bin;%path%
```

Follow the steps below to create a CA key:

- a. To create a CA key, type the following command at the Windows command prompt in the c:\openssl\certs directory:

```
openssl genrsa -out ca.key 1024
```

The following output should appear:

```
Loading 'screen' into random state - done
Generating RSA private key, 1024 bit long modulus
.....++++++
.+++++
e is 65537 (0x10001)
```

Follow the steps below to create a CA Certificate:

- a. Type the following command at the Windows command prompt in the c:\openssl\certs directory:

```
openssl req -new -x509 -days 365 -key ca.key -out
demoCA/cacert.pem
```

- b. Enter the appropriate Distinguished Name (DN) information for the CA certificate. You can leave some fields blank by entering a period.

For example:

```
Country Name: US
State or Province Name: CA
Locality Name: Sunnyvale
Organization Name: XYZ
Org. Unit Name: IT
Common Name: ic.xyz.com
Email Address: user@xyz.com
```

- c. To set up the CA, type the following command at the Windows command prompt in the directory c:\openssl\certs:

```
copy ca.key demoCA
notepad demoCA.cnf
```

- d. When prompted to create a new file, press the **yes** button.

- e. Type the following lines in the document, pressing the Enter key at the end of each line.

```
[ca]
default_ca = demoCA
[demoCA]
dir = ./demoCA
database = $dir/index.txt
new_certs_dir = $dir/newcerts
certificate = $dir/cacert.pem
serial = $dir/serial
private_key = $dir/ca.key
default_days = 365
default_md = md5
policy = policy_any
```

```

email_in_dn = no
name_opt = ca_default
name_opt = ca_default
copy_extensions = none
[ policy_any ]
countryName = supplied
stateOrProvinceName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress = optional

```

f. Save the file and close notepad.

g. Type the following command to generate an RSA private key for the remote IMV server:

```
openssl genrsa -out rimvs_key.pem 1024
```

h. Type the following command to generate a CSR for the remote IMV server:

```
openssl req -new -key rimvs_key.pem -out rimvs_csr.pem
```

i. Type the following lines:

```

Country Name:
State or Province Name:
Locality Name:
Organization Name:
Organizational Unit Name:
Common Name: [IPAddress]
Email Address:
A challenge password:
An optional company name:

```

You may enter any value you like for most fields, but the Common Name field must contain the IP address of the machine running the remote IMV server. This machine should have a static IP address.

j. Type the following command to generate a certificate for the remote IMV server:

```
openssl ca -config demoCA.cnf -in rimvs_csr.pem -out rimvs_cert.pem
```

k. Type 'y' twice when prompted to generate the certificate. This certificate is valid for 365 days by default. If you want a different certificate lifetime, change the default_days parameter in the demoCA.cnf file, or use the -days parameter to the openssl ca command to specify a different lifetime.

l. Type the following command to place the remote IMV server key and certificate in a PKCS#12 file (substitute your password):

```
openssl pkcs12 -export -in rimvs_cert.pem -inkey rimvs_key.pem -passout
pass:<password>-out rimvs_p12.pem
```

5. On the remote IMV server, choose **Programs > Juniper Networks > Remote IMV Server > Remote IMV Server Configurator** from the Start menu.
6. Under Client Info, click **Add**.
7. Configure the port to service SOAP requests from Secure Access.
8. Enter the client's IP address, the number of addresses to use, and the shared secret used by both Secure Access and the remote IMV server.

9. Change logging settings if you choose (log is generated in the install directory).
10. Browse and find the PKCS#12 file you generated in the filesystem.
11. Specify the password associated with the certificate.
12. In the admin console of Secure Access, use the **System > Configuration > Certificates > Trusted Server CAs** tab to import the trusted root CA certificate of the CA that issued the certificate for the remote IMV server.

If you used OpenSSL to generate the Remote IMV Server's server certificate is:
demoCA\cacert.pem.

If you did not use OpenSSL to generate this certificate, ensure that the file you import has the CA certificate (not the root certificate).

13. Click **Import Trusted Server CA** and browse for the server certificate used on the remote IMV server.
14. Add the new remote IMV server:

To specify the remote IMV server so that Secure Access can communicate with it:

- a. In the admin console, choose **Authentication > Endpoint Security > Host Checker**.
- b. Under Remote IMV, click **New Server**.
- c. In the New Server page:
 - i. Create a label for the server using the **Name** and (optional) **Description** fields.
 - ii. In the **Hostname** field, enter either the IP address or host name as defined in the server certificate.
 - iii. In the **Port** field, enter the unique port number Secure Access uses to communicate with the remote IMV server. Ensure that no other service is using this port number.

The default port number is the same as the default https port number. If you are running a web server on the same system as the Remote IMV Server, enter a new port number in the Port field.
 - iv. In the **Shared Secret** field, enter the same shared secret used in the client information entry on the remote IMV server.
 - v. Click **Save Changes**.
- d. Under Remote IMV, click **New IMV** to specify the third-party IMV.
- e. In the New IMV page:
 - i. Create a label for the IMV using the **Name** and (optional) **Description** fields.
 - ii. In the **IMV Name** field, enter the name of the IMV. This name must match the "human readable name" in the IMV's well-known registry key on the remote IMV server. For more information about human readable names and the well-known registry key, see www.trustedcomputinggroup.org.

- iii. From the Primary Server pop-up menu, select the remote IMV server where this IMV is installed.
- iv. (Optional) From the Secondary Server pop-up menu, select the secondary remote IMV server where this IMV is installed. The secondary server acts as a failover in case the primary server becomes unavailable.

Secure Access continues to try to re-establish connection to the primary remote IMV Server, and uses the primary Remote IMV Server on subsequent handshakes once it becomes available.

- v. Click **Save Changes**.
- f. Click **Save Changes**.

Related Documentation

- [Implementing the Third-Party IMV Policy on page 411](#)
- [Using Third-party Integrity Measurement Verifiers on page 405](#)

Implementing the Third-Party IMV Policy

To use Host Checker as a policy enforcement tool for managing endpoints, you must create global Host Checker policies at the system level through the Authentication > Endpoint Security > Host Checker page of the admin console, and then implement the policies at the realm and role levels.



NOTE: The **Custom: Remote IMV** option does not appear until you add the **Remote IMV New Server and New IMV** on the main Host Checker page.

To implement the third-party IMV policy:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. Under Policies, click **New**.
3. Enter a name in the **Policy Name** field and then click **Continue**. (Users see this name on the Host Checker remediation page if you enable custom instructions for this policy.)
4. Under Rule Settings, choose **Custom: Remote IMV** and click **Add**.
5. In the Add Custom Rule: Remote IMV page:
 - a. In the **Rule Name** field, enter an identifier for the rule.
 - b. Under **Criteria**, select the third-party IMV to be associated with this rule.
 - c. Click **Save Changes**.
6. Specify how Host Checker should evaluate multiple rules within the policy.
7. (Recommended) Specify remediation options for users whose computers do not meet the requirements specified in the policy

8. Click **Save Changes**.
9. Implement the policy at the realm or role level.

Related Documentation

- [Using Third-party Integrity Measurement Verifiers on page 405](#)
- [Configuring a Remote IMV Server on page 406](#)
- [Implementing Host Checker Policies on page 412](#)

Implementing Host Checker Policies

After you create global policies through the Authentication > Endpoint Security > Host Checker page of the admin console, you can restrict Secure Access and resource access by requiring Host Checker in a:

- **Realm authentication policy**—When administrators or users try to sign in to Secure Access or launch a Virtual Workspace session, Secure Access evaluates the specified realm's authentication policy to determine if the pre-authentication requirements include Host Checker. You can configure a realm authentication policy to download Host Checker, launch Host Checker and enforce Host Checker policies specified for the realm, or not require Host Checker. The user must sign in using a computer that adheres to the Host Checker requirements specified for the realm. If the user's computer does not meet the requirements, then Secure Access denies access to the user unless you configure remediation actions to help the user bring his computer into compliance. You can configure realm-level restrictions through the Administrators > Admin Realms > *SelectRealm* > Authentication Policy > Host Checker page or the Users > User Realms > *SelectRealm* > Authentication Policy > Host Checker page of the admin console.
- **Role**—When Secure Access determines the list of eligible roles to which it can map an administrator or user, it evaluates each role's restrictions to determine if the role requires that the user's computer adheres to certain Host Checker policies. If it does and the user's computer does not follow the specified Host Checker policies, then Secure Access does not map the user to that role unless you configure remediation actions to help the user bring his computer into compliance. You can configure role-mapping using settings in the Users > User Realms > *SelectRealm* > Role Mapping page. You can configure role-level restrictions through the Administrators > Admin Roles > *SelectRole* > General > Restrictions > Host Checker page of the admin console or the Users > User Roles > *SelectRole* > General > Restrictions > Host Checker page. If you have enabled Advanced Endpoint Defense Malware Protection, you can select to implement this feature for any role.
- **Resource policy**—When a user requests a resource, Secure Access evaluates the resource policy's detailed rules to determine if the resource requires that the user's computer adheres to certain Host Checker policies. Secure Access denies access to the resource if the user's computer does not follow the specified Host Checker policies unless you configure remediation actions to help the user bring his computer into compliance. To implement Host Checker restrictions at the resource policy level, use settings in the Users > Resource Policies > *SelectResource* > *SelectPolicy* > Detailed Rules page.

You may specify that Secure Access evaluate your Host Checker policies only when the user first tries to access the realm, role, or resource that references the Host Checker policy. Or, you may specify that Secure Access periodically re-evaluate the policies throughout the user's session. If you choose to periodically evaluate Host Checker policies, Secure Access dynamically maps users to roles and allows users access to new resources based on the most recent evaluation.

Executing Host Checker Policies

When the user tries to access Secure Access, Host Checker evaluates its policies in the following order:

1. **Initial evaluation**—When a user first tries to access the Secure Access sign-in page, Host Checker performs an initial evaluation. Using the rules you specify in your policies, Host Checker verifies that the client meets your endpoint requirements and returns its results to Secure Access. Host Checker performs an initial evaluation regardless of whether you have implemented Host Checker policies at the realm, role, or resource policy level.

If the user navigates away from the Secure Access sign-in page after Host Checker starts running but before signing in to Secure Access, Host Checker continues to run on the user's machine until the Host Checker process times out.

If Secure Access does not receive a result from Host Checker for any reason (including because the user manually terminated Host Checker), Secure Access displays an error and directs the user back to the sign-in page.

Otherwise, if the Host Checker process returns a result, Secure Access goes on to evaluate the realm level policies.

2. **Realm-level policies**—Secure Access uses the results from Host Checker's initial evaluation to determine which realms the user may access. Then, Secure Access displays or hides realms from the, only allowing the user to sign into those realms that you enable for the sign-in page, and if the Host Checker requirements for each realm are met. If the user cannot meet the Host Checker conditions required by any of the available realms, Secure Access does not display the sign-in page. Instead, it displays an error stating the user has no access unless you have configured remediation actions to help the user bring the endpoint into compliance.

Note that Host Checker only performs realm-level checks when the user first signs into the Secure Access. If the state of the user's system changes during his session, Secure Access does not remove him from the current realm or allow him access to a new realm based on his new system state.

3. **Role-level policies**—After the user signs into a realm, Secure Access evaluates role-level policies and maps the user to the role or roles if he meets the Host Checker requirements for those role(s). Then, Secure Access displays the Secure Access homepage to the user and enables those options that the mapped role(s) allow.

If Host Checker returns a different status during a periodic evaluation, Secure Access dynamically remaps the user to roles based on the new results. If the user loses rights to all available roles during one of the periodic evaluations, Secure Access disconnects

the user's session unless you have configured remediation actions to help the user bring the endpoint into compliance.

4. **Resource-level policies**—After Secure Access allows the user to access the homepage, the user may try to access a resource that is controlled by a resource policy. When he does, Secure Access determines whether or not to perform the action specified in the resource policy based on the last status returned by Host Checker.

If Host Checker returns a different status during a periodic evaluation, the new status only impacts new resources that the user tries to access. For example, if the user successfully initiates a VPN Tunneling session and then fails his next resource-level host check, he may continue to access the open VPN Tunneling session. Secure Access only denies him access if he tries to open a new VPN Tunneling session. Secure Access checks the last status returned by Host Checker whenever the user tries to access a new Web resource or open a new Secure Application Manager, VPN Tunneling, or Secure Terminal Access session.

With either a success or fail result, Host Checker remains on the client. Windows users may manually uninstall the agent by running `uninstall.exe` in the directory where Host Checker is installed. If you enable client-side logging through the System > Log/Monitoring > Client Logs page, this directory also contains a log file, which Secure Access rewrites each time Host Checker runs.

If you enable dynamic policy evaluation for Host Checker, Secure Access evaluates resource policies implemented at the realm level whenever a user's Host Checker status changes. If you do not enable dynamic policy evaluation for Host Checker, Secure Access does not evaluate resource policies but it does evaluate the authentication policy, role mapping rules, and role restrictions whenever a user's Host Checker status changes.

**Related
Documentation**

- [Configuring Host Checker Restrictions on page 414](#)
- [Specifying General Host Checker Options on page 425](#)
- [Role Restrictions on page 110](#)
- [Defining Authentication Access Policies on page 307](#)

Configuring Host Checker Restrictions

To specify Host Checker restrictions:

1. Navigate to: **Authentication > Endpoint Security > Host Checker** and specify global options for Host Checker to apply to any user for whom Host Checker is required in an authentication policy, a role mapping rule, or a resource policy.
2. If you want to implement Host Checker at the realm level:
 - a. Navigate to:
 - **Administrators > Admin Realms > *Select Realm* > General > Restrictions > Host Checker.**
 - **Users > User Realms > *Select Realm* > General > Restrictions > Host Checker.**

- b. Choose one of the following options for either all available policies or for individual policies listed in the **Available Policies** column:
 - **Evaluate Policies**—Evaluates without enforcing the policy on the client and allows user-access. This option does not require Host Checker to be installed during the evaluation process; however, Host Checker is installed once the user signs in to Secure Access.
 - **Require and Enforce**—Requires and enforces the policy on the client in order for the user to log in to the specified realm. Requires that Host Checker is running the specified Host Checker policies in order for the user to meet the access requirement. Requires Secure Access to download Host Checker to the client machine. If you choose this option for a realm’s authentication policy, then Secure Access downloads Host Checker to the client machine after the user is authenticated and before the user is mapped to any roles in the system. Selecting this option automatically enables the Evaluate Policies option.
 - c. Select the **Allow access to realm if any ONE of the selected “Require and Enforce” policies is passed** check box if you do not want to require users to meet all of the requirements in all of the selected policies. Instead, the user can access the realm if he meets the requirements of any one of the selected Host Checker policies. Note that Cache Cleaner policies are not part of the “requirement” decision process. Users can access the realm as long as they meet the other requirements regardless of whether they meet the Cache Cleaner policy.
3. If you want to implement Host Checker at the role level:
 - a. Navigate to:
 - **Administrators > Admin Roles > Select Role > General > Restrictions > Host Checker.**
 - **Users > User Roles > Select Role > General > Restrictions > Host Checker.**
 - b. Choose one of the following options:
 - **Allow all users** — Does not require Host Checker to be installed in order for the user to meet the access requirement.
 - **Allow only users whose workstations meet the requirements specified by these Host Checker policies** — Requires that Host Checker is running the specified Host Checker policies in order for the user to meet the access requirement.
 - Select the **Allow access to role if any ONE of the selected “Require and Enforce” policies is passed** check box if you do not want to require users to meet all of the requirements in all of the selected policies. Instead, the user can access the role if he meets the requirements of any one of the selected Host Checker policies.
 4. If you want to create role-mapping rules based on a user’s Host Checker status:
 - a. Navigate to: **Users > User Realms > Select Realm > Role Mapping.**
 - b. Click **New Rule**, select **Custom Expressions** from the Rule based on list, and click **Update**. Or, to update an existing rule, select it from the **When users meet these conditions** list.

- c. Click **Expressions**.
 - d. Write a custom expression for the role mapping rule to evaluate Host Checker's status using the `hostCheckerPolicy` variable. For help writing the custom expressions, use tips in the Expressions Dictionary.
 - e. In the **...then assign these roles** section, select the roles that Secure Access should map users to when they meet the requirements specified in the custom expression and click **Add**.
 - f. Select the **Stop processing rules when this rule matches** if you want Secure Access to stop evaluating role mapping rules if the user successfully meets the requirements defined in this rule.
5. If you want to implement Host Checker at the resource policy level:
- a. Navigate to: **Users > Resource Policies > Select Resource > Select Policy > Detailed Rules**.
 - b. Click **New Rule** or select an existing rule from the Detailed Rules list.
 - c. Write a custom expression for the detailed rule to evaluate Host Checker's status using the `hostCheckerPolicy` variable.

These options allow you to control which version of an application or service runs on client machines.

Remediating Host Checker Policies

You can specify general remediation actions that you want Host Checker to take if an endpoint does not meet the requirements of a policy. For example, you can display a remediation page to the user that contains specific instructions and links to resources to help the user bring their endpoint into compliance with Host Checker policy requirements.

You can also choose to include a message to users (called a reason string) that is returned by Host Checker or an integrity measurement verifier (IMV) and explains why the client machine does not meet the Host Checker policy requirements.

For example, the user may see a remediation page that contains the following custom instructions, a link to resources, and reason strings:

Your computer's security is unsatisfactory.

Your computer does not meet the following security requirements. Please follow the instructions below to fix these problems. When you are done click Try Again. If you choose to **Continue** without fixing these problems, you may not have access to all of your intranet servers.

1. Symantec

Instructions: You do not have the latest signature files. **Click here to download the latest signature files**. Reasons: The AntiVirus Product Version is too low.

The age of the Virus Definitions is not acceptable.

For each Host Checker policy, you can configure two types of remediation actions:

- **User-driven**—Using custom instructions, you can inform the user about the failed policy and how to make his computer conform. The user must take action to successfully re-evaluate the failed policy. For instance, you can create a custom page that is linked to a policy server or Web page and enables the user to bring his computer into compliance.
- **Automatic (system-driven)**—You can configure Host Checker to automatically remediate the user's computer. For example, when the initial policy fails, you can kill processes, delete files, or allow automatic remediation by an IMV. On Windows, you can also call the `HCIF_Module.Remediate()` API function as part of a third-party J.E.D.I. DLL. Host Checker does not inform users when performing automatic actions. (You could, however, include information in your custom instructions about the automatic actions.)

General Host Checker Remediation User Experience

Users may see the remediation page in the following situations:

- Before the user signs in:
 - If you enable custom instructions for a policy that fails, Secure Access displays the remediation page to the user. The user has two choices:
 - Take the appropriate actions to make the endpoint conform to the policy and then click the Try Again button on the remediation page. Host Checker checks the user's computer again for compliance with the policy.
 - Leave the endpoint in its current state and click the Continue button to sign in to Secure Access. The user cannot access the realm, role, or resource that requires compliance with the failed policy.

If you do not configure Secure Access with at least one realm that allows access without enforcing a Host Checker policy, the user must bring the endpoint into compliance before signing into Secure Access.
 - If you do not enable custom instructions for a policy that fails, Host Checker does not display the remediation page to the user. Instead, Secure Access displays the sign-in page but does not allow the user to access any realms, roles, or resources that have a failed Host Checker policy.
- After the user signs in:
 - (Windows only) During a session, if a user's Windows computer becomes non-compliant with the requirements of a Host Checker policy, an icon appears in the system tray along with a pop-up message that informs the user of the non-compliance. The user can then click the pop-up message to display the remediation page.

- (Macintosh or Linux) During a session, if a user's Macintosh or Linux computer becomes non-compliant with the requirements of a Host Checker policy, Secure Access displays the remediation page to inform the user of the non-compliance.



NOTE: If the user hides the remediation page by setting a user preference, he may only continue using the secure gateway if you configure other realms and roles that do not enforce a Host Checker policy.

Related Documentation

- [Configuring General Host Checker Remediation on page 418](#)
- [Configuring a Predefined Antivirus Rule with Remediation Options on page 384](#)
- [Configuring a Predefined Firewall Rule with Remediation Options \(Windows Only\) on page 386](#)
- [Specifying Customized Requirements Using Custom Rules on page 394](#)

Configuring General Host Checker Remediation

To specify remediation actions for a Host Checker policy:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. Create or enable Host Checker policies.
3. Specify the remediation actions that you want Host Checker to perform if a user's computer does not meet the requirements of the current policy:
 - **Enable Custom Instructions**—Enter the instructions you want to display to the user on the Host Checker remediation page. You can use the following HTML tags to format text and add links to resources such as policy servers or web sites: `<i>`, ``, `
`, ``, and `<a href>`. For example:

You do not have the latest signature files.

```
<a href="www.company.com">Click here to download the latest signature files.</a>
```



NOTE: For Windows clients, if you include in the instructions a link to a Secure Access-protected policy server, define a pre-authentication access tunnel.

- **Enable Custom Actions**—You can select one or more alternate policies that you want Host Checker to evaluate if the user's computer does not meet the current policy requirements. The alternate policy must be either a third-party policy that uses a J.E.D.I. package or a Secure Virtual Workspace policy. For example, you can use a J.E.D.I. package to launch an application if the user's computer does not meet the current policy requirements. Select the alternate policy in the HC Policies list and then click Add.

- **Remediate**—(Third party DLLs only) You can select this option to perform remediation actions specified by means of the Remediate () API function in a third-party J.E.D.I. DLL.



NOTE: The Remediate feature is primarily provided for backwards compatibility. We recommend that you use IMCs and IMVs instead.

- **Kill Processes**—On each line, enter the name of one or more processes you want to kill if the user's computer does not meet the policy requirements. You can include an optional MD5 checksum for the process. (You cannot use wildcards in the process name.) For example:

keylogger.exe

MD5: 6A7DFAF12C3183B56C44E89B12DBEF56

- **Delete Files**—Enter the names of files you want to delete if the user's computer does not meet the policy requirements. (You cannot use wildcards in the file name.) Enter one file name per line. For example:

c:\temp\bad-file.txt

/temp/bad-file.txt

- **Send reason strings**—Select this option to display a message to users (called a reason string) that is returned by Host Checker or integrity measurement verifier (IMV) and explains why the client machine does not meet the Host Checker policy requirements. This option applies to predefined rules, custom rules, and to third-party IMVs that use extensions in the Juniper Networks TNC SDK. For example, an antivirus IMV might display the following reason string:

The AntiVirus Product Version is too low. The age of the Virus Definitions is not acceptable.



NOTE: By sending reason strings, you are disclosing to users what the IMV is checking on the client machine.

4. Click **Save Changes**.

Related Documentation

- [Remediating Host Checker Policies on page 416](#)

Upgrading the Endpoint Security Assessment Plug-In

The Endpoint Security Assessment Plug-in (ESAP) on Secure Access checks third-party applications on endpoints for compliance with the pre-defined rules you configure in a Host Checker policy. This plug-in is included in the Secure Access system software package.

Juniper Networks frequently adds enhancements, bug fixes, and support for new third-party applications to the plug-in. New plug-in releases are available independently and more frequently than new releases of the Secure Access system software package. If necessary, you can upgrade the plug-in on Secure Access independently of upgrading the Secure Access system software package.

You can upload up to four versions of the plug-in to Secure Access, but Secure Access uses only one version at a time (called the active version). If necessary, you can rollback to a previously active version of the plug-in.

To upgrade the Endpoint Security Assessment Plug-in:

1. Download the Endpoint Security Assessment Plug-in from the Juniper Networks Customer Support Center to your computer:
 - a. Open the following page:
<http://www.juniper.net/support/products/esap/>
 - b. Click the Software tab.
 - c. Navigate to the ESAP release you want and click the link to download the package file to your computer.
2. Select **Authentication > Endpoint Security > Host Checker**.
3. At the bottom of the Host Checker page under Manage Endpoint Security Assessment Plug-In Versions:
 - a. If you have previously uploaded four versions of the component software, you must delete one of the versions before you can upload another one. Select the version you want to delete and click **Delete**.
 - b. If you want Secure Access to actively begin using the new component software immediately after you upload it, select the Set as active after upload option.
 - c. Click **Browse**, select the plug-in file you want to upload to Secure Access, and click **OK**.
 - d. Click **Upload**. While Secure Access uploads and decrypts the plugin .zip file, the message "Loading..." appears in the plug-in list under Manage Endpoint Security Assessment Plug-In Versions. If Secure Access is a member of a cluster, Secure Access displays the message "Loading..." while the plug-in is transferred to the other cluster nodes. After the plug-in is installed, the date and time of the plug-in installation appears in the plug-in list.
 - e. If you did not select the Set as active after upload option, activate the plug-in you want to use by selecting the version in the plug-in list and clicking **Activate**.



NOTE:

- If you attempt to activate a version of the plug-in that does not support all of the pre-defined rules already configured in all Host Checker policies, Secure Access does not allow activation of that plug-in version. For example, if a Host Checker policy is configured to use a pre-defined rule to check for a version of antivirus software, and you attempt to activate a plug-in version that does not support that particular version of the antivirus software, Secure Access does not allow you to activate that plug-in version. To view the list of supported products for a particular plug-in version, click the plug-in's version number under Manage Endpoint Security Assessment Plug-In Versions.
- You can rollback to an older plug-in version after upgrading to a later version by selecting the older version as the active version. But, if you modified any Host Checker policies after upgrading to the later version, the rollback may not succeed. Rollback is guaranteed to succeed only if the policies did not change.
- If you upgrade the Secure Access system software to a newer version, or you import a user configuration file, the currently active plug-in version does not change. If you want to use a different plug-in version after upgrading or importing a user configuration file, you must manually activate that plug-in version.
- If Secure Access already has four versions of the plug-in installed when you upgrade the Secure Access system software to a newer version, Secure Access automatically deletes the oldest plug-in version and installs, but does not activate, the plug-in included with the new Secure Access system software.

Related Documentation • [Implementing Host Checker Policies on page 412](#)

Defining Host Checker Pre-Authentication Access Tunnels

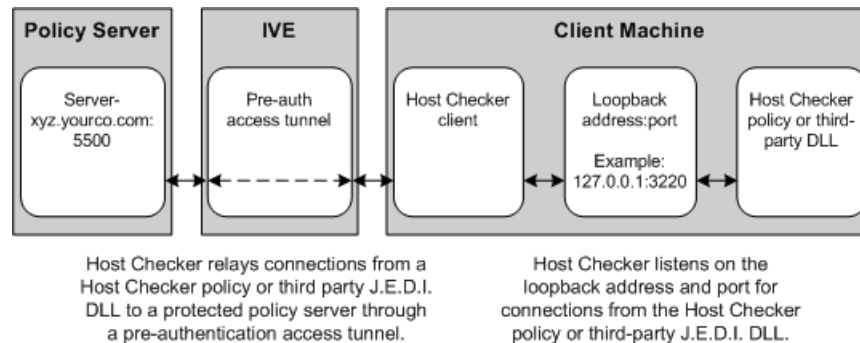
If your policies require Host Checker rules or third-party J.E.D.I. DLLs to access a policy server (or other resource) to check compliance before users are authenticated, you can use one of the following methods to make the resource available to the Host Checker Windows clients:

- **Deploy the policy server in a DMZ where Host Checker rules or third-party J.E.D.I. DLLs can access the server directly instead of going through Secure Access**—This deployment is the simplest solution because you do not have to define a Host Checker pre-authentication access tunnel through Secure Access between clients and the policy server.
- **Deploy the policy server in a protected zone behind Secure Access (Windows only)**—This deployment requires you to define a pre-authentication access tunnel. A pre-authentication access tunnel enables Host Checker rules or third-party J.E.D.I. DLLs

to access the Secure Access-protected policy server or resource before Secure Access authenticates users. To define a pre-authentication access tunnel, you associate a loopback address (or host name) and port on the client with an IP address and port on the policy server. You add one or more tunnel definitions to a MANIFEST.HCIF file, which you then upload to Secure Access. You can upload multiple MANIFEST.HCIF files to Secure Access. For all third-party policies enabled on a realm, Host Checker creates tunnels for all of the tunnel definitions in all of the MANIFEST.HCIF files, assuming the definitions are unique.

While running on a Windows client, Host Checker listens for a connection on each loopback address and port you specify in the tunnel definitions. The connections can originate from the integrated Host Checker rules and from client-side or server-side J.E.D.I. DLLs. Host Checker uses the pre-authentication access tunnel(s) to forward the connections through Secure Access to the policy server(s) or other resource.

Figure 39: Host Checker Creates a Tunnel from a Client to a Policy Server Behind the Secure Access Service



NOTE: Host Checker pre-authentication access tunnels are supported on Windows only.

Related Documentation

- [Specifying Host Checker Pre-Authentication Access Tunnel Definitions on page 422](#)

Specifying Host Checker Pre-Authentication Access Tunnel Definitions

For Windows clients, you can define a pre-authentication access tunnel that enables Host Checker methods or third-party J.E.D.I. DLLs to access a Secure Access-protected policy server (or other resource) before users are authenticated.

A definition for a Host Checker pre-authentication access tunnel configures access to one policy server or other resource. Each tunnel definition consists of a pair of IP addresses and ports: one loopback IP address and port on the client, and one IP address and port on the policy server.

You specify one or more tunnel definition(s) in a Host Checker policy package definition file. The package definition file, which must be named MANIFEST.HCIF, defines the name of an interface DLL, the Host Checker policies defined in the DLL, and the

pre-authentication access tunnel definitions. Note that if you do not include policies in your package, Host Checker simply enforces that the package has run on the client. If you do declare policies through this file, they become available through the admin console where you can implement them at the realm, role, and resource policy levels.

Within the MANIFEST.HCIF file, you must include one definition per line, with a blank line between each definition, using the following format:

```
HCIF-Main: <DLLName>
HCIF-Policy: <PolicyName>
HCIF-IVE-Tunnel: <client-loopback>:port <policy-server>:port
```

where:

<DLLName> is the name of the interface DLL, such as myPestPatrol.dll. Even if you are not using an interface DLL, you must include a dummy DLL as a placeholder file that has this exact name.

<PolicyName> is the name of a policy defined in the DLL, such as myFileCheck. You can define multiple policies by using the HCIF-Policy statement for each policy. If you are not using an interface DLL, you can use any policy name as a placeholder.

The syntax of a Host Checker tunnel definition is:

```
HCIF-IVE-Tunnel: <client-loopback>:port <policy-server>:port
```

where:

<client-loopback> is a loopback address that begins with 127. and takes any of the following forms:

- An IP address and port that takes the form of 127.*.*:port. To avoid conflicts with JSAM, do not use 127.0.0.1 with port 80, but you can use 127.0.0.1 with other ports. For example: 127.0.0.1:3220
- A host name that resolves to a loopback address that begins with 127. You can use a local hosts file on each client computer or a DNS server to resolve the loopback address.
- A host name that does not resolve to a loopback address, or resolves to a non-loopback address. In these cases, Host Checker allocates a loopback address and updates the local hosts file on the client with the mapping. Note that the user must have administrator privileges in order for Host Checker to modify the local hosts file. If the user does not have administrator privileges, Host Checker cannot update the hosts file and cannot open the pre-authentication access tunnel. In that case, Host Checker logs an error.

<policy-server> is the IP address or host name of the back-end policy server. Secure Access resolves the host name you specify.

For example, in the following tunnel definition, 127.0.0.1:3220 is the client loopback address and port, and mysygate.company.com:5500 is the policy server host name and port:

```
HCIF-IVE-Tunnel: 127.0.0.1:3220 mysygate.company.com:5500
```

Or you can use a host name for the client, as in this example:

```
HCIF-IVE-Tunnel: mysygate.company.com:3220 mysygate.company.com:5500
```

Keep the following in mind when specifying tunnel definitions:

- You must add a blank line between each line in the MANIFEST.HCIF file, and you can use a semi-colon at the beginning of a line to indicate a comment. For example:

```
HCIF-Main: myPestPatrol.dll
HCIF-Policy: myFileCheck
HCIF-Policy: myPortCheck
; Tunnel definitions
HCIF-IVE-Tunnel: 127.0.0.1:3220 mysygate.company.com:5500
HCIF-IVE-Tunnel: 127.1.1.1:3220 mysygate2.company.com:5500
HCIF-IVE-Tunnel: mysygate.company.com:3220 mysygate3.company.com:5500
```

- Host Checker pre-authentication access tunnels are supported on Windows only.
- If <client-loopback> is a non-loopback address, then Host Checker cannot open the pre-authentication access tunnel and logs an error instead.
- If you use a loopback address other than 127.0.0.1 (such as 127.0.0.2 and above), clients who are using Windows XP Service Pack 2 must install the XP SP2 Hot Fix. See:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;884020>



NOTE: If you are deploying a client-side or server-side third-party DLL, keep the following in mind:

- Unzip the server-side third-party DLL package and add the tunnel definitions to the MANIFEST.HCIF file that contain the policies for the third-party DLL. (The DLL must use the same <client-loopback> address and port or host name that you specify in the MANIFEST.HCIF file.)
- Since a pre-authentication access tunnel is open only while Host Checker is running, a third-party DLL can access its Secure Access protected policy server only while Host Checker is running.
- If a third-party DLL uses HTTPS to connect to its policy server via a host name that resolves properly to the loopback address, no server certificate warnings appear. However, if the third-party DLL connects explicitly via a loopback address, then server certificate warnings do appear because the host name in the certificate does not match the loopback address. (The developer of the third-party DLL can configure the DLL to ignore these warnings.)

Related Documentation

- [Defining Host Checker Pre-Authentication Access Tunnels on page 421](#)

Specifying General Host Checker Options

You can specify global options for Host Checker that apply to any user for whom Host Checker is required in an authentication policy, a role mapping rule, or a resource policy.

To specify general Host Checker options:

1. In the admin console, choose **Authentication > Endpoint Security > Host Checker**.
2. Under Options:
 - In the **Perform check every X minutes** field, specify the interval at which you want Host Checker to perform policy evaluation on a client machine. If the client machine fails to meet the requirements of the Host Checker policies required by a role or resource policy, then Secure Access denies the associated user requests.

For example, you may require that a user runs a specific third-party antivirus application in order to map to Role A, which enables network connections from an external location. If the user's client machine is running the required antivirus application when the user signs in to Secure Access, then the user maps to Role A and is granted all access features enabled for Role A. If the antivirus application stops running during the user session, however, the next time Host Checker runs, the user fails to meet the security requirements for Role A and therefore loses all access privileges for Role A.

When an end-user logs into a Realm, Host Checker performs an initial policy check, regardless of whether or not the policy is enforced at the Realm, Role, and/or Resource level. The initial policy check establishes a start time. Host Checker evaluates policies at the frequency set by the Perform check every X minutes option starting the clock at the initial policy check. Although the frequency setting is set globally for all Host Checker policy checking, it is not synchronized for all end-user clients connected to Secure Access. Each client performs its own initial policy check and starts its own X minute countdown. If you configure the authentication policy within a realm where Host Checker enforces policies (versus installing), the enforcement occurs only during the pre-authentication phase. After an end-user signs in and for the duration of the user's session, any subsequent Host Checker policy checks have no impact on realm access, meaning that there is no concept of removing an end-user session from a realm once an end-user successfully authenticates into that realm.

If you configure a role restriction where Host Checker enforces policies, the enforcement occurs just after authentication during role mapping. Role restrictions are enforced periodically during the end-user session at an interval specified using the Host Checker frequency setting. If the end-user successfully passes the Host Checker evaluation during role mapping but later fails X minutes after login, that specific user loses rights to that role. If the end-user loses rights to all available roles due to Host Checker policy evaluation, the end-user session is disconnected.

If you configure a resource-based policy rule where Host Checker enforces policies, the enforcement occurs when the end-user attempts to access the resource/backend server. For web resources, the Host Checker evaluation occurs at each request. For SAM and STA resources, the Host Checker evaluation occurs

when Secure Access activates the connection to the backend application/server. For VPN Tunneling access, the Host Checker evaluation occurs when Secure Access initiates VPN Tunneling. Existing connections of applications running by way of SAM, Telnet/SSH connection, and VPN Tunneling connections are not affected by further Host Checker evaluations. Only new Web requests, new applications across SAM, new instances of STA, and launching VPN Tunneling are affected. The Host Checker evaluation is based on the most recent policy check that occurred X minutes ago. Example, if you configure the frequency setting to Perform check every five minutes and the end-user attempts to access a protected resource or attempts to launch VPN Tunneling four minutes after the last check, then the policy evaluation is based on the state of the client machine four minutes ago, not at the moment the end-user attempted to access the resource.



NOTE: If you enter a value of zero, Host Checker only runs on the client machine when the user first signs into Secure Access.

- For the Client-side process, login inactivity timeout option, specify an interval to control timing out in the following situations:
 - If the user navigates away from the Secure Access sign-in page after Host Checker starts running but before signing in to Secure Access, Host Checker continues to run on the user's machine for the interval you specify.
 - If the user is downloading Host Checker over a slow connection, increase the interval to allow enough time for the download to complete.
 - Select Perform dynamic policy reevaluation to automatically refresh the roles of individual users by enabling dynamic policy evaluation for Host Checker. Host Checker can trigger Secure Access to evaluate resource policies whenever a user's Host Checker status changes. (If you do not select this option, Secure Access does not evaluate resource policies but it does evaluate the authentication policy, role mapping rules, and role restrictions whenever a user's Host Checker status changes.)
3. Click **Save Changes**.

Related Documentation

- [Configuring Host Checker Restrictions on page 414](#)

Specifying Host Checker Installation Options

If you implement any policy at the realm, role, or resource policy level that requires Host Checker, you must provide a mechanism by which Secure Access or the user can install Host Checker on the client machine. Otherwise, when Secure Access evaluates the Host Checker policy, the user's machine fails because the Host Checker client is not available to return a success status.

You can use two methods to install Host Checker on a user's system:

- Secure Access automatically installs Host Checker—Enable automatic installation through the Users/Administrators > User Realms/Administrator Realms > [Realm] >

Authentication Policy > Host Checker page of the admin console. When you do, Secure Access evaluates the realm-level option when the user accesses the Secure Access sign-in page and then determines if the current version of Host Checker is installed on the user's machine. If Host Checker is not installed, Secure Access attempts to install it using either an ActiveX or a Java delivery method.

When a Windows user signs in to Secure Access, Secure Access attempts to install an ActiveX control on the user's system. If Secure Access successfully installs the ActiveX control, the control manages the installation of the Host Checker program.

If Secure Access cannot install the ActiveX control because ActiveX is turned off on the user's system, Secure Access attempts to install Host Checker using Java. For Linux hosts, Secure Access always uses the Java delivery method. The Java delivery method requires only user privileges, but Java must be enabled on the user's system. For the Firefox browser on Linux, the Java runtime and plug-in must be installed.



NOTE: Due to some anomalies with Microsoft JVM, Host Checker may not install and an error box appears. If this occurs, click **Try Again**. The subsequent installation should succeed.

If Secure Access cannot use the Java delivery method because Java is disabled on the user's system, Secure Access displays a no-access error message.



NOTE: If Microsoft Vista is running on the user's system, the user must click the setup link that appears during the installation process to continue installing the setup client and Host Checker. On all other Microsoft operating systems, the setup client and Host Checker install automatically.

- The user or administrator manually installs Host Checker (Windows only)—Download the Host Checker installer from the Maintenance > System > Installers page of the admin console and use it to manually install Host Checker on the user's system.



NOTE: To install Host Checker, users must have appropriate privileges, as described in the *Client-side Changes Guide* on the Juniper Networks Customer Support Center. If the user does not have these privileges, use the Juniper Installer Service available from the Maintenance > System > Installers page of the admin console to bypass this requirement.

Removing the Juniper ActiveX Control

If Microsoft Windows XP is running on the user's system and you want to remove the Juniper set-up ActiveX control:

1. Open Internet Explorer.
2. Click the **Tools** button and then click **Internet Options**.

3. Click **Settings**, then **View Objects**.
4. Select **JuniperSetupSP1** and press **Delete**.

If Microsoft Vista is running on the user's system and you want to remove the Juniper set-up ActiveX control:

1. Open Internet Explorer.
2. Click the **Tools** button and then click **Manage Add-ons**.
3. In the Show list, click **Downloaded ActiveX controls** to display all ActiveX controls.
4. Click **JuniperSetupClient** and then click **Delete**.

**Related
Documentation**

- [Installing Host Checker Automatically or Manually on page 429](#)

Client ActiveX Installation Delay

During end-user sign-in, the setup client is delivered through either ActiveX or Java, depending on the client system's capability. By default, Internet Explorer blocks ActiveX content and displays an information bar that lets the user decide whether to install the new ActiveX control.



NOTE: For restricted users, the information bar displays help information only, it does not allow installation of new ActiveX controls.

The Secure Access SSL VPN Series Appliance displays to end-users an intermediate page with a 15-second delay to interact with the information bar content. End-users can choose to skip the installation (and the 15-second delay) by clicking the "click here" link. If end-users choose to skip the installation, they are not prompted again unless they clear their browser cookies.

Administrators can customize the message and locale displayed in this intermediate page by clicking the Custom Messages tab in the Default Options for User Roles page and filling out information under the User Login Messages section.

**Related
Documentation**

- [Customizing Messages on page 123](#)

Using Host Checker with the GINA Automatic Sign-In Function

Using Host Checker in conjunction with the Windows Graphical Identification and Authorization (GINA) sign-in function for VPN Tunneling requires that you pay particular attention to the type, level, and number of items to verify on the client before granting or rejecting access to Secure Access. Since the GINA sign-in function takes place before Windows has completely launched on the client, and therefore, before the user profile on Windows is created, we recommend you adopt the following practices when creating

Host Checker policies you plan to use for Windows clients featuring the GINA sign-in function:

- You can check system-level processes at both realm enforce and realm evaluate. You can check user-level processes only at realm evaluate.
- If you have user-level processes at realm evaluate, create a separate VPN Tunneling role featuring only system-level policy checks that can be performed before Windows has completely launched on the client. Ensure that this role allows connectivity to the Windows Domain infrastructure in your secure network to support drive mapping, software updates, and group policies, for example. Mapping your users to this role allows the GINA authentication to complete. This role is in addition to the final role that you want the user to be mapped.

**Related
Documentation**

- [About VPN Tunneling on page 734](#)

Installing Host Checker Automatically or Manually

To automatically install Host Checker on client computers:

1. In the admin console, choose **Authentication > Endpoint Security > Host Checker**.
2. Under Options, select **Auto-upgrade Host Checker** if you want Secure Access to automatically download the Host Checker application to a client computer when the version of Host Checker on Secure Access is newer than the version installed on the client. Here is a summary of what happens when the Auto-upgrade Host Checker option is selected or not selected:
 - If Host Checker is not installed on the client computer, Host Checker is installed automatically regardless of whether the Auto-upgrade Host Checker option is selected or not selected.
 - If the Auto-upgrade Host Checker option is selected and a previous version of Host Checker is installed, Host Checker is upgraded on the client automatically.
 - If the Auto-upgrade Host Checker option is not selected and a previous version of Host Checker is installed, Host Checker is not upgraded the client automatically.

If you select the Auto-upgrade Host Checker option, note the following:

- On Windows, the user must have administrator privileges in order for Secure Access to automatically install the Host Checker application on the client. For more information, see the *Client-side Changes Guide* on the Juniper Networks Customer Support Center.
 - If a user uninstalls Host Checker and then signs in to Secure Access for which the Auto-upgrade Host Checker option is not enabled, the user no longer has access to Host Checker.
3. Click **Save Changes**.

The Maintenance > System > Installers page of the admin console provides several applications and a service for download. You can download an application or service as a Windows executable file, which enables you to:

- Distribute the file to client machines using software distribution tools. This option enables you to install an application or service on client machines whose users do not have Administrator privileges, which are required to install the application or service.
- Post the executable in a secure repository so that users with the proper administrator right may download and install the appropriate version.
- Download and execute a script that automatically retrieves the proper version of the installer from an FTP server.

**Related
Documentation**

- [Specifying Host Checker Installation Options on page 426](#)

Using Host Checker Logs

Use the System > Log/Monitoring > Client Logs > Settings tab to enable client-side logging for the Host Checker. When you enable this option, Secure Access writes a client-side log to any client that uses Host Checker. Secure Access appends to the log file each time the feature is invoked during subsequent user sessions. This feature is useful when working with the support team to debug problems with the respective feature.

Since these settings are global, Secure Access writes a log file to all clients that use the feature for which you enable client-side logging. Also, Secure Access does not remove client-side logs. Users need to manually delete log files from their clients. For information about where Secure Access installs log files, see the *Client-side Changes Guide* on the Juniper Networks Customer Support Center.

To specify global client-side logging settings:

1. In the admin console, choose **System > Log/Monitoring > Client Log > Settings**.
2. Select the desired features for which Secure Access writes client-side logs.
3. Click **Save Changes** to save these settings globally.

**Related
Documentation**

- [Implementing Host Checker Policies on page 412](#)

Configuring Host Checker for Windows Mobile

You can configure Host Checker to enforce policies for handheld devices, such as PDAs and smart phones, that run the Windows Mobile operating system.



NOTE: Currently only Windows Mobile versions 5 and 6 are supported.

Host Checker rules include checks for ports, processes, files, registry key settings, operating system version, and certificates on the handheld device. You can also load and use installed third-party IMCs to perform vendor-specific checks. Once the policy is created, Host Checker deploys automatically when the user connects to the Secure Access Service gateway.

Host Checker does not require any configuration on the handheld device itself. When the server determines the device is out of compliance, Host Checker displays a notification icon in the system tray. Clicking this icon opens a browser page that contains reasons for the compliance failure and remediation instructions.

Host Checker remains on the handheld device and does not need to be downloaded each time the user connects to the gateway. When the gateway upgrades to a newer version of Host Checker, the handheld device automatically updates the next time the user connects to the gateway. To remove Host Checker from the handheld device, use the Remove Programs applet in the Settings panel of the device.

Host Checker policies for Windows Mobile are configured through the Authentication > Endpoint Security > Host Checker page of the admin console.

Requiring Junos Pulse Mobile Security for Secure Access Service Gateway Access

Junos Pulse Mobile Security is an optional licensed feature of the Pulse mobile device app. A Secure Access Service administrator can configure the Secure Access Service gateway to perform a host check and require that Pulse Mobile Security be activated on mobile devices before granting access to the device through the Secure Access Service gateway.



NOTE: The Pulse Mobile security check feature is available on Secure Access Service software Release 7.0 Release 2 or higher.

To require Pulse Mobile Security software on the device:

1. On the Secure Access Service gateway admin console, select **Users > User Realms**.
2. Select the realm you created for mobile devices. If necessary, create a new one now.
3. On the Authentication Policy tab, select **Host Checker**.
4. Select the **Enable Mobile Security Check** check box, and then click **Save Changes**.

The Mobile Security Check is now applied to all realm users. If you have created more than one realm for mobile device access, enable this check box on each realm.

When you select the **Enable Mobile Security Check** check box, Junos Pulse connects to the Secure Access Service gateway only when the following criteria is met:

- Security Suite feature is enabled on Junos Pulse.
- There is no un-quarantined virus on the device.

Mobile device users must perform the following tasks:

- Download and install the Pulse client software app for the particular device type. The Pulse Mobile Security client software is bundled with the VPN app.
- Start Pulse Mobile Security by tapping the Pulse icon.
- If the device is not registered, respond to the prompts for registration information, including a license key.

**Related
Documentation**

- [Implementing Host Checker Policies on page 412](#)
- [Specifying Customized Requirements Using Custom Rules on page 394](#)

Host Checker for Apple iOS

- [Host Checker for Pulse iOS Clients on page 432](#)
- [Configuring Host Checker for Pulse iOS Clients on page 433](#)
- [Implementing Host Checker Policies for Pulse for iOS Devices on page 435](#)

Host Checker for Pulse iOS Clients

Host Checker is a component of Junos Pulse that reports the integrity of iOS endpoints that are attempting to connect to Pulse Secure Access Service. Host Checker runs as a Trusted Network Connect (TNC) client on the endpoint. The client evaluates the endpoint according to predefined criteria and reports to the Trusted Network Connect server, which is a part of Pulse Secure Access Service. If the endpoint is not in compliance with the Host Checker policies, then the user might not get access to the network or might get limited access to the network depending upon the enforcement policies configured by the administrator.

For iOS clients, Host Checker can evaluate client compliance based on the following predefined criteria:

- **OS Checks**—You can specify the iOS version or minimal version that must be installed on the device.
- **Jail Breaking Detection**—Jail breaking is a process that allows Apple iPhone, iPad and iPod Touch users to gain root access to the iOS operating system and bypass usage and access limitations imposed by Apple. With a jail broken device, an iOS user can install applications that are not available through the Apple App Store. Jail broken devices expose the device to a greater risk of running malicious applications.
- **Mobile Security Suite**—Pulse Mobile Security Suite (MSS) for iOS supports features that help protect the iOS device if it is lost or stolen: remote wipe, remote lock, and locate. Pulse MSS also allows the MSS administrator to provide VPN configurations to the device and enforce other usage practices such as requiring a lock password and specifying the password strength. Host Checker enables you to require that an iOS device have the Pulse Mobile Security Suite installed and enabled.



NOTE: The Pulse MSS check on the client is based on the presence of a valid client certificate issued by the Mobile Security Gateway. Therefore, to configure this Host Checker item, you need to add the CA used by MSS in the Certificates section of the Pulse Secure Access Service admin console.

Host Checker evaluation policies can be part of a larger Host Checker configuration that applies to many different types of clients or to iOS devices only.

Related Documentation

- [Configuring Host Checker for Pulse iOS Clients on page 433](#)
- [Implementing Host Checker Policies for Pulse for iOS Devices on page 435](#)

Configuring Host Checker for Pulse iOS Clients

Host Checker policies can be part of a larger Host Checker configuration that applies to many different types of clients or to iOS devices only. However, you might find it easiest to create a separate Host Checker policy specifically for iOS devices.



NOTE: One type of iOS Host Checker rule, the Pulse Mobile Security Suite (MSS) check, requires that an iOS device be registered with the MSS. To create this type of rule, you must specify the same trusted client certificate authority (CA) that is configured on the Pulse Mobile Security Gateway (MSG). This means that the CA must already be defined in the Certificates section of the Pulse Secure Access Service admin console before you can create this type of Host Checker rule.

To create a Host Checker policy for iOS devices:

1. From the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. In the Policies section, click **New** to open a New Host Checker Policy page.
3. Specify a name for the new policy and then click **Continue** to open the Host Checker Policy page.

The name appears in lists when you implement the policy so be sure to use a descriptive name, such as **iOS HC Policy**.

4. Click the Mobile tab, and then click the iOS tab.
5. In the Rule Settings section, click **Select Rule Type** and select one of the following options and then click **Add**:
 - **OS Checks**—To specify the iOS version that must be installed on the device:
 - a. Specify a descriptive name for this rule. For example **Must-Be-iOS-4.1-or-higher**. Rule names cannot include spaces.
 - b. Specify the criteria. For example, to enforce iOS 4.1 or higher, create two conditions: Equal to 4.1 and Above 4.1.

Host Checker supports iOS versions 4.1 through 4.3.X.

- c. Click **Save Changes**.
 - **Jail Breaking Detection**—Jail breaking is a process that allows Apple iPhone, iPad and iPod Touch users to gain root access to the iOS operating system, and bypass usage and access limitations imposed by Apple. With a jail broken device, an iOS user can install applications that are not available through the Apple App Store. Jail broken devices possess a greater risk of running malicious applications.
 - a. Specify a descriptive name for this rule. For example **No-iOS-Jailbreak**.
 - b. The **Don't allow Jail Broken devices** check box is enabled by default.
 - c. Click **Save Changes**.
 - **Mobile Security Suite**—Pulse Mobile Security Suite (MSS) for iOS supports features that help protect the iOS device if it is lost or stolen: remote wipe, remote lock, and locate. Pulse MSS also allows the MSS administrator to provide VPN configurations to the device. An MSS rule allows you to require that an iOS device have MSS installed and enabled.
 - a. Specify a descriptive name for this rule. For example **iOS-MSS**.
 - b. In the Criteria section, the **Enable Mobile Security Suite on the device** check box is enabled by default.
 - c. Click the **MDM Trusted client CA** box to choose a certificate authority.

MDM (Mobile Device Management) enables remote configuration and management of mobile devices. Secure Access Service verifies registration with Pulse MSS through the presence of a valid client certificate issued by the Mobile Security Gateway. Therefore, to configure this Host Checker item, you need to know the client certificate authority that is used by the Pulse Mobile Security Gateway. The certificate authorities listed in the box are defined in the System > Configuration section of the Pulse Secure Access Service admin console.
 - d. Optionally, specify additional criteria (the certificate field and expected value), and then click **Add**.
 - e. Click **Save Changes**.
6. After you have configured all of your rules, specify how you want to enforce them by choosing one of the following options:
 - All of the rules
 - Any of the rules
 - Custom

For Custom requirements, you can specify a custom expression using Boolean operators AND and OR and also group and nest conditions using parenthesis.
 7. Specify remediation options:

- **Enable custom instructions**—If you enable this check box, a text box appears and allows you to type information that appears on the user's device if Host Checker discovers an issue. For example, if you enabled the MSS rule that terminates the VPN session of Host Checker discovers a virus, you can instruct the user to run a virus scan to clear the issue before trying to connect.
- **Send reason strings**—Select this option to display a message to users (called a reason string) that explains why the client machine does not meet the Host Checker policy requirements. For example, if the jailbreak detection policy fails, Pulse appears, **A jailbroken device is not allowed to access the network. Please contact your network administrator.**

8. When you are finished, click **Save Changes**.

A host checker policy configured for a VPN tunnel is not triggered if the VPN tunnel is launched automatically by VPN on Demand on an Apple iOS device. If the VPN session is started through the Pulse client, the host checker policy is applied correctly. A VPN on Demand configuration enables an iOS device to automatically initiate a VPN connection when any application running on the phone initiates a connection to a host in a predefined set of hosts. A VPN on Demand connection uses client certificate-based authentication so the user does not have to provide credentials every time a VPN connection is initiated.

Related Documentation

- [Host Checker for Pulse iOS Clients on page 432](#)
- [Implementing Host Checker Policies for Pulse for iOS Devices on page 435](#)

Implementing Host Checker Policies for Pulse for iOS Devices

After you create one or more Host Checker policies for iOS devices, you must implement them. Pulse Secure Access Service can use Host Checker policies at the realm or the role level.

Realm Authentication—You can configure a realm authentication policy to download and run Host Checker with a particular Host Checker policy. If the iOS device does not meet the Host Checker requirements, then Pulse Secure Access Service can deny access. You can provide remediation information in the Host Checker policy to describe the requirement and help users take steps to solve the issue.

To enable a Host Checker policy for a realm:

1. From the admin console, select **Users > User Realms > SelectRealm > Authentication Policy > Host Checker**. The Host Checker page displays all of the available Host Checker policies.
2. Select the check box next to each policy you want to include. Select one or both of the following check boxes next to the policy:
 - **Evaluate Policies**—Evaluates without enforcing the policy on the iOS device and allows access.
 - **Require and Enforce**—Requires that the iOS device be in compliance with the Host Checker policy. Pulse Secure Access Service downloads Host Checker to the iOS device after the user is authenticated and before the user is mapped to any roles

in the system. Selecting this option automatically enables the Evaluate Policies option.

3. Optionally select **Allow access to realm if any ONE of the selected “Require and Enforce” policies is passed**. This check box is available if you selected more than one Host Checker policy. If you enable this check box, an iOS device is allowed access if it passes any of the Require and Enforce policies. The Cache Cleaner policy does not apply to iOS devices.
4. Click **Save Changes**.

Role—You can configure a role to download and run Host Checker with a particular Host Checker policy. If the iOS device does not meet the Host Checker requirements, then Secure Access can deny access or assign the user to a remediation role that has limited access. You can provide remediation information in the Host Checker policy to help users take steps to solve the issue.

To enable a Host Checker policy for a role:

1. From the admin console, select **Users > User Roles > SelectRole > General > Restrictions > Host Checker**. The Host Checker page displays all of the available Host Checker policies.
2. Select **Allow users whose workstations meet the requirements specified by these Host Checker policies**.
3. In the Available Policies list, select the policies that you want to apply to select them, and then click Add to move them to the Selected Policies list. To select a policy click it. So select more than one policy, use Ctrl+click.
4. Optionally select **Allow access to the role if any ONE of the selected policies (except cache-cleaner) is passed**. This check box is available if you selected more than one Host Checker policy. If you enable this check box, an iOS device is allowed access if it passes any of the Require and Enforce policies. The Cache Cleaner policy does not apply to iOS devices.
5. Click **Save Changes**.

Related Documentation

- [Host Checker for Pulse iOS Clients on page 432](#)
- [Configuring Host Checker for Pulse iOS Clients on page 433](#)

Using Proxy Exceptions

Secure Access Service clients parse Internet Explorer’s static proxy exception list. We support most exceptions that Internet Explorer supports with the following limitations:

- For IP address exception, we support n.***; n.n.**; n.n.n.*. For example, 10.***; 10.10.**; 10.10.10.*; or 10.10.10.10. We do not support 10* or 10.*10.* even though Internet Explorer may support them.

- For string expression, we support specific strings such as my.company.net, or a wild card at front of the string, for example, *.my.company.net or *.company.net. We do not support *.company.*, *.company*, *.company. *.com, *.net *.com and so forth.

Enabling the Secure Virtual Workspace

The Secure Virtual Workspace guarantees the integrity of Secure Access session data on a client machine running Windows 2000 or Windows XP by creating a protected workspace on the client desktop. By enabling the Secure Virtual Workspace, you ensure that any end-user signing in to your intranet must perform all interactions within a completely protected environment. If the user's applications and interactions result in data being written to disk or to the registry, the Secure Virtual Workspace encrypts that information. When the Secure Access session is complete, the Secure Virtual Workspace destroys all information pertaining to itself or to the session, by default. However, you can configure the state of this type of information to suit your particular needs. For example, you might decide to allow data to persist across Secure Virtual Workspace sessions.

Secure Access follows the DoD 5220.M cleaning and sanitization standard for securely deleting Secure Virtual Workspace data that is stored on the hard disk.

The Secure Virtual Workspace:

- Removes workspace data and resources when the session ends.
- Ensures that no browser Helper Objects latch onto an Internet Explorer process before launching IE.
- Prohibits desktop search products from intercepting Web traffic and indexing the contents.
- Enters all of its configuration and run-time operations in Secure Access logs.

Secure Access hosts the Secure Virtual Workspace binary, which the client system downloads from Secure Access whenever a user connects. The Secure Virtual Workspace creates a virtual file system and a virtual registry on the client.

You define and configure the applications that are allowed to run within the Secure Virtual Workspace. For example, you can configure the following types of application configurations:

- Restrict launching of Internet Explorer and Outlook to the Secure Virtual Workspace.
- Restrict application installations and executions within a Secure Virtual Workspace session. This ensures that even the application binaries are completely removed from the client machine after the session ends.



NOTE: Secure Virtual Workspace does not work when IBM Sametime 7.5 is running in the default desktop. IBM Sametime 7.5 automatically switches users to the default desktop from the virtual workspace.

For Windows Vista and later, certain processes, like regedit, require elevated privileges. SVW does not currently allow the running of elevated privilege processes.

Secure Access implementation of the Secure Virtual Workspace:

- Does not require the client desktop user to have administrator privileges to download and run the Secure Virtual Workspace.
- Supports the use of the Secure Virtual Workspace in conjunction with Host Checker, which will automatically launch in the secure workspace, when initiated.
- Provides the Secure Virtual Workspace as a J.E.D.I. module, to allow you to create Secure Virtual Workspace policies at the user role or realm level.

Secure Virtual Workspace Restrictions and Defaults

The Secure Virtual Workspace imposes certain restrictions on its use, and establishes defaults, which you may be able to modify.

- SVW does not support Cache Cleaner.
- By default, a platform-specific browser is allowed to run in the SVW, unless explicitly restricted by the administrator.
- Secure Access does not allow software applications that update the HKLM registry entries on installation to operate within the SVW.
- Secure Access does not support the standard JSAM applications Outlook and Netbios file browsing through SVW, since these applications require registry key changes. However, Secure Access does support the Citrix and Lotus Notes JSAM standard applications through SVW.
- By default, Secure Access does not allow access to external storage or printing devices by some applications running in the SVW. You can enable access to these devices on a role or realm basis, if needed.
- By default, end-users are unable to access network shares, unless you configure access to network shares in the SVW policy.
- If your end-users use firewalls or other applications that run in the kernel space, they may experience problems when trying to download the Secure Access client components in SVW. Low-level administrative applications may display message boxes requiring user interaction. If you set the option to allow switching to the default or real desktop, the user may be able to dismiss the message boxes. If the switching option is disabled, users may be unable to fix the problem.
- The Secure Virtual Workspace does not support 16-bit applications.

- Some Windows keyboard shortcuts may not work properly inside an SVW session.
- To display the Windows Task Manager while in SVW, you cannot use the standard keyboard shortcut Ctrl+Alt+Del. You must right-click on the Windows taskbar (typically on the bottom of the screen, unless you have moved it) to display a popup menu, from which you can select Task Manager.
- If you set the Host Checker status update interval to a value of zero (0), Host Checker will perform the status check once and then quit. If Host Checker quits, SVW also quits. As a result, the end-user is unable to initiate an SVW session. Set the Host Checker status update interval to a non-zero value.
- SVW only scans for file system drives when the user first starts his session. If the user starts a session and then adds a drive (such as a USB drive), he will not be able to access the drive during that session.
- The Logoff On Connect feature is not supported within SVW.

Configuring the Secure Virtual Workspace

You configure the Secure Virtual Workspace within the context of a Host Checker policy and all Secure Virtual Workspace policies you define appear in a list at Authentication > Endpoint Security > Secure Virtual Workspace.

Because the Secure Virtual Workspace session data is stored on the end-user's real desktop, you should implement the persistence feature only if each of your end-users always uses the same client machine.



NOTE: No provision has been made to ensure that you cannot configure a sign-in URL mapping to more than one realm configured with an SVW policy. If you configure multiple mappings to more than one realm, the results are unpredictable. You must explicitly configure the secure virtual desktop to allow only one SVW policy to be evaluated at the user end.

Related Documentation

- [Defining Secure Virtual Workspace Permissions on page 439](#)
- [Defining a Secure Virtual Workspace Application Policy on page 441](#)
- [Defining a Secure Virtual Workspace Security Policy on page 442](#)
- [Defining Secure Virtual Workspace Environment Options on page 443](#)
- [Defining Secure Virtual Workspace Remediation Policy on page 444](#)

Defining Secure Virtual Workspace Permissions

You can specify which devices and resources the end-user can access when using the Secure Virtual Workspace.

To define a new Secure Virtual Workspace permissions policy:

1. In the admin console, choose **Authentication > Endpoint Security > Secure Virtual Workspace**.
2. Click **New Secure Virtual Workspace Policy**.
3. Enter a name for the policy.
4. Under Permissions, check the appropriate checkboxes for the items to which you want to grant permissions:
 - Printers—Select to allow end-user access to network printers.
 - Restricted View of Files—When Restricted View is set, only the directories Documents and Settings, Program Files, and the Windows system folders on the system drive (typically c:) are available within SVW.



NOTE: If you set the Restricted View of Files option, and your end-users configure partitioned drives, they will be unable to access any applications or files residing on any drive other than the system (c:) drive. If you allow your end-users to partition drives, you should not use the Restricted View.

- Removable Drives—Select to allow end-user access to removable drives on the end-user's client machine.

If an end-user installs a USB removable storage device he may experience the two following behaviors, depending also on how you set this option:

- If the user connects the USB device before initiating an SVW session, the device will appear to be a fixed hard drive and the user will not be able to read or write to the device during an SVW session, even when you have set the Removable Drives option.
- If the user connects the USB device after initiating an SVW session, the device appears to be removable media and the user can access it, if you have set the Removable Drives option when configuring SVW.
- Network Share Access—Select to allow end-user access to network share drives.
- Switch to Real Desktop—Select to allow end-user to toggle between the Secure Virtual Workspace and the end-user's client desktop.
- Desktop Persistence—Select to allow end-users to maintain a Secure Virtual Workspace across client sessions on NTFS file systems only.



NOTE: Desktop persistence and switching are not supported on FAT16 or FAT32 file systems.

If you select this option, note that multiple users using the same password to encrypt their SVW workspace on the same host could gain access to the persistent data storage protected by that static password. We recommend that your users employ strong password when securing their SVW persistent data store on multi-user systems.

- Virtual File Execution—Select to allow virtualized file applications to run within a Secure Virtual Workspace environment. By default, downloading an executable within Secure Virtual Workspace encrypts that executable and prevents it from being run. Selecting this option allows executables to be downloaded without encrypting them.
5. Continue to define the policy or click **Save Changes**.

Related Documentation

- [Enabling the Secure Virtual Workspace on page 437](#)

Defining a Secure Virtual Workspace Application Policy

You can specify which applications the end-user can install or run when using the Secure Virtual Workspace.

To define a new Secure Virtual Workspace application policy:

1. In the admin console, choose **Authentication > Endpoint Security > Secure Virtual Workspace**.
2. Click **New Secure Virtual Workspace Policy** or click the hyperlinked name of an existing Secure Virtual Workspace policy.
3. Enter a name for the policy.
4. Under Applications, select the checkboxes for the types of applications you want to enable:
 - Control panel—Select to allow the end-user to access the Windows control panel while in the Secure Virtual Workspace.
 - Run menu—Select to allow the end-user to access the Windows run menu while in the Secure Virtual Workspace.
 - Registry editor—Select to allow the end-user to access the Windows registry editor (regedt32.exe) while in the Secure Virtual Workspace.
 - Task manager—Select to allow the end-user to access the Windows Task Manager (taskmgr.exe) and system processes while in the Secure Virtual Workspace.
 - Command window—Select to allow the end-user to access the Windows Command window (cmd.exe) and execute commands while in the Secure Virtual Workspace.

- Custom applications—You can identify custom applications that the end-user is allowed to run while in the Secure Virtual Workspace. For example, you might include in-house applications, non-default browsers, and other types of applications. Enter one application, including the .exe extension per line in the multiline text box. You can also use the * wildcard for an entire class of applications, and you can include an optional MD5 hash value following the executable name and a comma, telnet.exe,0414ea8.
- Applications to deny—You can identify applications you want to restrict from end-user use while in the Secure Virtual Workspace. Enter one application, including the extension for each executable per line in the multiline text box.



NOTE: Any custom application that is not listed in the Custom applications field is denied by default.

If you add the same application to the Custom applications text box and to the Applications to deny text box, the deny action takes precedence and users will be denied access to the application SVW sessions. Be aware that this can happen if you use wildcards to specify applications in both lists. For example, if you specify *plore.exe in the allow list and iex*.exe in the deny list, then iexplore.exe will be denied.

5. Continue to define the policy or click **Save Changes**.

After you define one or more Virtual Workspace policies, you must enable them as Realm authentication policies at the user level.

Related Documentation

- [Implementing Host Checker Policies on page 412](#)
- [Defining a Secure Virtual Workspace Security Policy on page 442](#)
- [Defining Secure Virtual Workspace Remediation Policy on page 444](#)

Defining a Secure Virtual Workspace Security Policy

You can specify encryption levels and can control the use of 3rd-party extensions in Internet Explorer and Outlook.

To specify security options for a new Secure Virtual Workspace policy:

1. In the admin console, choose **Authentication > Endpoint Security > Secure Virtual Workspace**.
2. Click **New Secure Virtual Workspace Policy** or click the hyperlinked name of an existing Secure Virtual Workspace policy.
3. Enter a name for the policy.
4. Specify the type of AES encryption key the Secure Access Service uses to enable the Secure Virtual Workspace on the client. The available options are 128, 192, and 256-bit encryption keys.

5. Identify the IE or Outlook extensions you want to allow by including each allowable DLL on a separate line in the IE/Outlook extensions to allow text box. Any extension that is not listed is denied, by default.

These extensions are small applications that are passed into and out of the Secure Virtual Workspace session.

6. Continue to define the policy or click **Save Changes**.

Related Documentation

- [Defining a Secure Virtual Workspace Application Policy on page 441](#)
- [Defining Secure Virtual Workspace Remediation Policy on page 444](#)

Defining Secure Virtual Workspace Environment Options

To specify environment options for a new Secure Virtual Workspace policy:

1. In the admin console, choose **Authentication > Endpoint Security > Secure Virtual Workspace**.
2. Click **New Secure Virtual Workspace Policy** or click the hyperlinked name of an existing Secure Virtual Workspace policy.
3. Enter a name for the policy.
4. Under Options, specify:
 - The maximum length of time (in minutes) a client's Secure Virtual Workspace session can remain idle before the connection to Secure Access times out.
 - The desktop wallpaper image (Optional).
 - The desktop background color (Optional).
 - The sign-in URL to use to access the SVW.

The available URLs include the default User sign-in URL and any URLs you have defined in Authentication > Signing in > Sign-in Policies. The first time SVW puts the user into the virtual workspace and initiates a browser, it takes the user to Secure Access using a sign-in URL. By default, this sign-in URL is the same one that the user has entered to start their Secure Access session. You can configure a different sign-in URL through this option.



NOTE: Secure Access does not support host names that contain a wildcard, such as `*host.com/[path]`.

- The string to display in the toolbar title. By default, "SVW Title" is displayed.
 - To allow users to hide the toolbar, select the **Autohide Toolbar** option. When users choose to hide the toolbar (by clicking the thumbtack icon in the toolbar), they must scroll to the top of their desktop in order to make the toolbar reappear.
5. Continue to define the policy or click **Save Changes**.

- Related Documentation**
- [Enabling the Secure Virtual Workspace on page 437](#)

Defining Secure Virtual Workspace Remediation Policy

To specify remediation options for a new Secure Virtual Workspace policy:

1. In the admin console, choose **Authentication > Endpoint Security > Secure Virtual Workspace**.
2. Click **New Secure Virtual Workspace Policy** or click the hyperlinked name of an existing Secure Virtual Workspace policy.
3. Enter a name for the policy.
4. Under Remediation, select remediation options for users whose computers do not meet the requirements specified in the policy.



NOTE: If you do not create remediation instructions and the policy fails, your users will not know why they cannot launch the Secure Virtual Workspace or access local resources.

- **Enable Custom Instructions**—Select to expand text box in which you can enter custom instructions, using either text or HTML, that will be presented to end-users when the Secure Virtual Workspace encounters a remediation problem.
 - **Enable Custom Actions**—You can select one or more alternate policies that you want Host Checker to evaluate if the user's computer does not meet the current policy requirements. The alternate policy must be either a third-party policy that uses a J.E.D.I. package or another Secure Virtual Workspace policy. For example, you can use a J.E.D.I. package to launch an application if the user's computer does not meet the current policy requirements. Select the alternate policy in the HC Policies list and then click Add.
 - **Kill Processes**—Select to open text box in which you enter application processes and MD5 hash values for the processes you want killed. For example:


```
Application.exe
MD5: 6A7DFAF12C3183B56C44E89B12DBEF56
MD5: 9S3AJ912CC3183B56C44E89B12DI2AC9
```
 - **Delete Files**—Select to open text box in which you can enter file names, one per line, of files you want deleted.
 - **Send reason strings**—Select to send remediation information.
5. Click **Save Changes**.

- Related Documentation**
- [Configuring General Host Checker Remediation on page 418](#)

Cache Cleaner

- [About Cache Cleaner on page 445](#)
- [Setting Global Cache Cleaner Options on page 445](#)
- [Implementing Cache Cleaner Options on page 448](#)
- [Specifying Cache Cleaner Restrictions on page 449](#)
- [About Cache Cleaner Logs on page 450](#)

About Cache Cleaner

Cache Cleaner is a Host Checker policy that removes residual data, such as temporary files or application caches, left on a user's machine after a Secure Access session. For example, when a user signs in to Secure Access from an Internet kiosk and opens a Microsoft Word document using a browser plug-in, Cache Cleaner can remove the temporary copy of the Word file stored in the browser cache (Windows folder) when the session terminates. By removing the copy, Cache Cleaner prevents other kiosk users from finding and opening the Word document after the Secure Access user concludes the session.

Cache Cleaner can also prevent Web browsers from permanently storing the usernames, passwords, and Web addresses that users enter in Web forms. By preventing browsers from improperly caching this information, Cache Cleaner keeps confidential user information from being stored on untrusted systems.



NOTE: Cache cleaner does not currently support Secure Virtual Workspace (SVW).

Related Documentation

- [Setting Global Cache Cleaner Options on page 445](#)
- [Implementing Cache Cleaner Options on page 448](#)

Setting Global Cache Cleaner Options

When you enable Cache Cleaner, it clears all content downloaded through Secure Access' Content Intermediation Engine from a user's system. In addition, you can use settings in

the Authentication > Endpoint Security > Cache Cleaner page of the admin console to clear content from the following places:

- Specified hosts and domains—If you enable WSAM or JSAM, you may want to configure Cache Cleaner to clear additional hosts and domains. When users browse the Internet outside Secure Access using WSAM or JSAM, Internet files appear in their temporary Internet file folder. To delete these files using Cache Cleaner, you must specify the appropriate hostname (for example, www.yahoo.com).
- Specified files and folders—If you enable your users to access client-server applications on their local systems, you may want to configure Cache Cleaner to clear the temporary files and folders that the applications create on the users' systems.



NOTE: If you configure Cache Cleaner to remove files from a directory, Cache Cleaner clears all files, including those that the user has explicitly saved to the directory and files that were in the directory prior to the Secure Access session.

Only one Cache Cleaner policy is allowed. You can neither delete the default Cache Cleaner policy (named "Cache Cleaner Policy") nor create a new one.

To specify global Cache Cleaner options:

1. Select **Authentication > Endpoint Security > Cache Cleaner** in the admin console.
2. Under Options:
 - a. Specify how often Cache Cleaner runs in the Cleaner Frequency field. Valid values range from 1 to 60 minutes. Each time Cache Cleaner runs, it clears all content downloaded through the Secure Access Content Intermediation Engine plus the browser cache, files, and folders you specify under the Browser Cache and Files and Folders sections.
 - b. Select the **Disable AutoComplete of web addresses** check box to prevent the browser from using cached values to automatically fill in Web addresses during the user's Secure Access session. When you select this option, Secure Access sets the following Windows registry value to 0 during the user's Secure Access session:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\AutoComplete.
Then, at the end of the session, Secure Access restores the registry value to its original setting.
 - c. Select the **Disable AutoComplete of usernames and passwords** check box to prevent Internet Explorer from automatically filling in user credentials in Web forms using cached values. Selecting this option also disables the "Save Password?" prompt on Windows systems. When you select this option, Secure Access sets the following Windows registry values to 0:
 - HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FormSuggest Passwords

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\FormSuggest Passwords\FormSuggest PW Ask
 - HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ DisablePasswordCaching
- d. Select the **Flush all existing AutoComplete Passwords** check box to clear any cached passwords that Internet Explorer has cached on the user's system. When you select this option, Secure Access sets the following Windows registry value to 0:
- ```
HKEY_CURRENT_USER \Software\Microsoft\Internet Explorer\IntelliForms\SPW
```
- Then, select one of the following options:
- Select the **For Secure Gateway session only** option button to specify that Secure Access should restore the user's cached passwords at the end of his Secure Access session.
  - Select the **Permanently** option button to permanently delete the user's cached passwords.
- e. Select the **Empty Recycle Bin and Recent Documents list** check box to empty the recycle bin and clear the recent documents list. The entire contents are removed, not just the files related to the user's sessions.
3. Under Browser Cache, enter one or more hostnames or domains (wildcards are permitted). When a user session ends, Cache Cleaner removes any content in the browser cache that originates from these servers. Cache Cleaner also removes this content when it runs at the specified cleaner frequency interval. Note that Secure Access does not resolve hostnames, so enter all possible representations of a server, such as its hostname, FQDN, and IP address.
4. Under Files and Folders:
- a. Specify either:
    - The name of a file that you want Cache Cleaner to remove.
    - The complete directory path to a folder whose contents you want Cache Cleaner to remove. If you specify a directory, select Clear Subfolders to also clear the contents of any subdirectories within this directory.
  - b. Select the **Clear folders only at the end of session** check box if you want Cache Cleaner to clear directory contents only at the end of the user session. Otherwise, Cache Cleaner also clears files and folders at the specified cleaner frequency interval



**NOTE:** When specifying files and folders to clear, note the following:

Cache Cleaner uses a cookie called DSPREAUTH to send the client's status to Secure Access. If you delete this cookie from the user's client, Cache Cleaner does not work properly. To avoid problems, do not specify Internet Explorer directories such as <userhome>\Local Settings\Temporary Internet Files\\* under File or folder path. Note that Cache Cleaner still clears all of the Internet Explorer cache downloaded from the Secure Access host and the other hosts specified in the Hostnames box, regardless of what directories you specify under Files and Folders.

For the Firefox browser, Cache Cleaner clears only those directories you specify under Files and Folders.

5. Click **Save Changes** to save these settings globally.

If more than one valid Secure Access session exists from the same system and Cache Cleaner is used in those sessions, all sessions are terminated when a user signs out from one of the sessions. To prevent this, turn off Cache Cleaner for those sessions that do not need Cache Cleaner.



**NOTE:** If multiple administrators or end users to a single Secure Access are signed in from the same client system and at least one of them deploys Cache Cleaner, unexpected results may occur. For example, Cache Cleaner might shut down, role privileges might be lost, and forced disconnections might occur.

**Related Documentation** • [Implementing Cache Cleaner Options on page 448](#)

## Implementing Cache Cleaner Options

After you specify which hosts, domains, files, and folders to clear using settings in the Authentication > Endpoint Security > Cache Cleaner page of the admin console, you can restrict Secure Access and resource access by requiring Cache Cleaner in the following options:

- **Realm authentication policy**—When users try to sign in to Secure Access, Secure Access evaluates the specified realm's authentication policy to determine if the pre-authentication requirements include Cache Cleaner. You can configure a realm authentication policy to evaluate whether to require and enforce the Cache Cleaner policy in order for the user to log in to the specified realm. If the user's computer does not meet the requirements, then the user is denied access to Secure Access. As a post-authentication requirement, you can evaluate without enforcing the Cache Cleaner policy on the client and allow user access. You configure realm-level restrictions through

the Users > User Realms > *Realm* > Authentication Policy > Host Checker page of the admin console.

- **Role**—When Secure Access determines the list of eligible roles to which it can map an administrator or user, it evaluates each role’s restrictions to determine if the role requires Cache Cleaner to run on the user’s workstation. If it does and the user’s machine is not already running Cache Cleaner, then Secure Access does not map the user to that role. You can control which roles Secure Access maps a user to by using settings in Users > User Realms > *Realm* > Role Mapping. Select or create a rule and then select Custom Expressions. You can configure role-level restrictions through the Users > User Roles > *Role* > General > Restrictions > Host Checker page of the admin console.
- **Resource policy**—When a user requests a resource, Secure Access evaluates the resource policy’s detailed rules to determine whether or not Cache Cleaner needs to be installed or running on the user’s workstation. Secure Access denies access to the resource if the user’s machine does not meet the Cache Cleaner requirement. You can implement Cache Cleaner restrictions at the resource policy level through the Condition Field box of the Rules window. Select Users > Resource Policies > *Resource* > *Policy* > Detailed Rules and set `hostCheckeryPolicy = ‘Cache Cleaner policy’`.

You may specify that Secure Access evaluate your Cache Cleaner policies only when the user first tries to access the realm, role, or resource that references the Cache Cleaner policy. Or, you can use settings in the Authentication > Endpoint Security > Cache Cleaner tab to specify that Secure Access periodically re-evaluate the policies throughout the user’s session. If you choose to periodically evaluate Cache Cleaner policies, Secure Access dynamically maps users to roles and allows users access to new resources based on the most recent evaluation.

When the user tries to access Secure Access, Host Checker evaluates its policies (Cache Cleaner is a Host Checker policy) in the following order:

- Initial evaluation
- Realm-level policies
- Role-level policies
- Resource-level policies

**Related Documentation**

- [Setting Global Cache Cleaner Options on page 445](#)

## Specifying Cache Cleaner Restrictions

To specify Cache Cleaner restrictions:

1. Select **Authentication > Endpoint Security > Cache Cleaner** and specify global options for Cache Cleaner to apply to any user for whom Cache Cleaner is required in an authentication policy, a role mapping rule, or a resource policy.
2. Implement Cache Cleaner at the realm level and role level as you would with Host Checker.

3. Create role-mapping rules based on a user's Cache Cleaner status as you would with Host Checker.
4. To implement Cache Cleaner at the resource policy level:
  - a. Select **Users > Resource Policies > Select Resource > Select Policy > Detailed Rules**.
  - b. Click **New Rule** or select an existing rule from the Detailed Rules list.
  - c. Create a custom expression in a detailed rule that sets `hostCheckeryPolicy = 'Cache Cleaner policy'`.

- Related Documentation**
- [Configuring Host Checker Restrictions on page 414](#)
  - [Custom Expressions on page 1181](#)

## About Cache Cleaner Logs

---

Since Cache Cleaner is a Host Checker policy, it is included in the Host Checker logs. Use the **System > Log/Monitoring > Client Logs > Settings** tab to enable client-side logging for Host Checker. When you enable this option, Secure Access writes a client-side log to any client that uses Host Checker. Secure Access appends to the log file each time the feature is invoked during subsequent user sessions. This feature is useful when working with the support team to debug problems with the respective feature.

## PART 4

# Remote Access

- Hosted Java Applets Templates on page 453
- Citrix Templates on page 467
- Lotus iNotes Templates on page 477
- Microsoft OWA Templates on page 481
- Microsoft Sharepoint Templates on page 485
- Web Rewriting on page 489
- File Rewriting on page 561
- Secure Application Manager on page 583
- Telnet/SSH on page 631
- Terminal Services on page 641
- Junos Pulse Collaboration on page 691
- Email Client on page 725
- VPN Tunneling on page 733





# Hosted Java Applets Templates

- [About Hosted Java Applet Templates on page 453](#)
- [Task Summary: Hosting Java Applets on page 454](#)
- [Uploading Java Applets to Secure Access on page 454](#)
- [Signing Uploaded Java Applets on page 455](#)
- [Creating HTML Pages That Reference Uploaded Java Applets on page 456](#)
- [Accessing Java Applet Bookmarks on page 456](#)
- [Creating a Hosted Java Applet Resource Profile on page 457](#)
- [Configuring Hosted Java Applet Resource Profile Bookmarks on page 458](#)
- [Creating Hosted Java Applets Bookmarks Through the User Roles Page on page 460](#)
- [Required Attributes for Uploaded Java Applets on page 461](#)
- [Required Parameters for Uploaded Java Applets on page 462](#)
- [Use case: Creating a Citrix JICA 9.5 Java Applet Bookmark on page 463](#)

## About Hosted Java Applet Templates

---

The Secure Access Java applet upload feature enables you to store the Java applets of your choice directly on Secure Access without employing a separate Web server to host them. When you use this feature, you simply upload the applets to Secure Access (along with additional files that the applets reference) and create a simple Web page through Secure Access that references the files. Then, Secure Access intermediates the Web page and Java applet content using its Content Intermediation Engine.

For example, you might want to use Secure Access to intermediate traffic between an IBM AS/400 system on your network and individual 5250 terminal emulators on your users' computers. To configure Secure Access to intermediate this traffic, obtain the 5250 terminal emulator's Java applet. Then you can upload this applet to Secure Access and create a simple Web page that references the applet. After you create the Web page through Secure Access, Secure Access creates a corresponding bookmark that users can access through their home pages.

Secure Access enables you to host Java applets using Web resource profile templates (described in these topics) as well as through Terminal Services resource profiles.

The hosted Java applets feature is a standard feature on all Secure Access appliances except the SA 700. If you are using an SA-700 appliance, you must install a Core Clientless Access upgrade license to access the hosted Java applets feature.

**Related Documentation**

- [Task Summary: Hosting Java Applets on page 454](#)

---

## Task Summary: Hosting Java Applets

---

The Secure Access Service Java applet upload feature enables you to store the Java applets of your choice directly on the Secure Access Service without employing a separate Web server to host them.

To host Java applets on the Secure Access Service:

1. Specify which applets you want to upload, create Secure Access Service bookmarks that reference the uploaded applets, and specify which roles can access the bookmarks using settings in the Users > Resource Profiles > Web page of the admin console.
2. (Optional.) To sign your Java applets, Select System > Configuration > Certificates > Code-Signing Certificates in the admin console to upload the Java certificate to the Secure Access Service. If you choose to skip this step, the user sees an untrusted certificate warning each time he accesses the corresponding bookmark.
3. (Optional.) To improve the performance of your Java applications:
  - a. Select Enable Java instrumentation caching on the Maintenance > System > Options page of the admin console. This option can improve the performance of downloading Java applications.
  - b. After you finish configuring the Secure Access Service, cache your Java applet and access it as an end user. This action eliminates the performance hit that occurs through the intermediation engine when the first end user accesses the applet.

**Related Documentation**

- [Using Code-signing Certificates on page 868](#)
- [Uploading Java Applets to Secure Access on page 454](#)
- [Signing Uploaded Java Applets on page 455](#)
- [Creating HTML Pages That Reference Uploaded Java Applets on page 456](#)

---

## Uploading Java Applets to Secure Access

---

You can use Java applets to intermediate traffic to various types of applications through Secure Access. For example, you can upload the 3270 applet, 5250 applet, or Citrix Java applet to Secure Access. These applets enable users to establish sessions to IBM mainframes, AS/400s, and Citrix MetaFrame servers through terminal emulators. (Note that to enable the Citrix Java ICA client through a Secure Access session, you must upload multiple Citrix .jar and .cab files to Secure Access.

Secure Access enables you to upload individual .jar and .cab files or .zip, .cab, or .tar archive files. Archive files can contain Java applets and files referenced by the applets. Within the .zip, .cab, or .tar file, the Java applet must reside at the top level of the archive. You can upload any number of files to Secure Access as long as their combined size does not exceed 100 MB.

To ensure compatibility with both Sun and Microsoft Java Virtual Machines (JVMs), you must upload both .jar and .cab files to Secure Access. (The Sun JVM uses .jar files, whereas the Microsoft JVM uses .cab files.)



**NOTE:** When you upload Java applets to Secure Access, Secure Access asks you to read a legal agreement before it finishes installing the applets. Read this agreement carefully—it obligates you to take full responsibility for the legality, operation, and support of the Java applets that you upload.

You can only upload 100 MB of Java applets to Secure Access. Secure Access displays the size of each applet that you upload to Secure Access on the Java Applets page so you can determine, if necessary, which applets you want to delete.

Uploading Java applets requires signed ActiveX or signed Java applets to be enabled within the browser to download, install, and launch the client applications.

**Related Documentation**

- [Task Summary: Hosting Java Applets on page 454](#)

## Signing Uploaded Java Applets

Unlike other Java applets that users can access through Secure Access, you do not have to create a separate code-signing policy for the Java applets that you upload to Secure Access. Secure Access automatically signs (or re-signs) them using the appropriate code-signing certificate. A code-signing certificate (also called an applet certificate) is a type of server-side certificate that re-signs Java applets intermediated by Secure Access.

Secure Access automatically signs (or resigns) your hosted Java applets with the code-signing certificate that you install through the System > Configuration > Certificates > Code-signing Certificates page of the admin console. If you do not install a code-signing certificate on Secure Access, Secure Access uses its self-signed applet certificate to sign or re-sign the applets. In this case, users see an “untrusted certificate issuer” warning whenever they access the Java applets through Secure Access.



**NOTE:** Secure Access re-instruments and re-signs your uploaded Java applets whenever you change (that is, import, renew, or delete) the corresponding code-signing certificate on Secure Access.

- Related Documentation**
- [Task Summary: Hosting Java Applets on page 454](#)

## Creating HTML Pages That Reference Uploaded Java Applets

---

When uploading a Java applet to Secure Access, you must create a simple Web page that references the applet. Users can access this Web page through a bookmark on their Secure Access home pages or from external Web servers.

The Web page must contain a simple HTML page definition that references the uploaded Java applet. The Web page can also contain any additional HTML and JavaScript that you choose. Secure Access can generate some of the Web page for you, including the HTML page definition and the references to your Java applet. (Note, however, that Secure Access is not aware of all the applet-specific parameters that are required by your applet—you must find and fill these parameters in yourself.) When Secure Access generates this HTML, it creates placeholders for any undefined values and prompts you to fill in the necessary values.

You can create these Web pages through Java applet upload resource profiles.

- Related Documentation**
- [Task Summary: Hosting Java Applets on page 454](#)
  - [Accessing Java Applet Bookmarks on page 456](#)

## Accessing Java Applet Bookmarks

---

Users can access the applets you upload to Secure Access using two methods:

- Bookmarks on the Secure Access end-user console—When you create a Web page that references your uploaded Java applets, Secure Access creates a corresponding link to the Web page and displays that link in the Bookmarks section of the Secure Access end-user console. Users who map to the appropriate role can simply click the link to access the Java applet.
- Links on external Web servers—Users can link to the Java applet bookmarks from an external Web server by simply using the correct URLs. When the user enters a bookmark's URL (or clicks an external link that contains the URL), Secure Access prompts the user to enter his Secure Access username and password. If he properly authenticates, Secure Access allows him to access the bookmark. You can construct the URL to the Java applet bookmark using the syntax described in either of the following lines:

```
https://SecureAccessGateway_hostname/dana/home/launchwebapplet.cgi?bmname=bookmarkName
```

```
https://SecureAccessGateway_hostname/dana/home/launchwebapplet.cgi?resourceID=<resourceID>&bmname=bookmarkName
```

You can determine the ID for a Java applet bookmark by accessing it through the Secure Access home page and then extracting the ID from the Web browser's address bar.



**NOTE:** Although Secure Access enables you to create multiple bookmarks with the same name, we strongly recommend that you use a unique name for each. If multiple bookmarks have the same name and a user accesses one of these bookmarks using a URL that includes the `bmname` parameter, Secure Access randomly picks which of the identically named bookmarks to display to the user. Also note that the `bmname` parameter is case-sensitive.

If you create links on external servers to Java applet bookmarks on Secure Access and you are using multiple customized sign-in URLs, some restrictions occur.

**Related Documentation**

- [Configuring Hosted Java Applet Resource Profile Bookmarks on page 458](#)
- [Creating Hosted Java Applets Bookmarks Through the User Roles Page on page 460](#)

## Creating a Hosted Java Applet Resource Profile

To create a hosted Java applet resource profile:

1. Select **Users > Resource Profiles > Web** in the admin console.
2. Click **New Profile**.
3. Select **Hosted Java Applet** from the Type list.
4. Enter a unique name and optionally a description for the resource profile.
5. Select the Java applet that you want to associate with the resource profile from the Applet to use list. Or, if the applet that you want to use is not currently available in the list, click Edit Applet. Then:
  - a. Click New Applet to add an applet to this list. Or, select an existing applet and click Replace (to replace an existing applet with a new applet) or Delete (to remove an applet from Secure Access)



**NOTE:** If you replace an existing archive, make sure that the new applet archive contains all of the necessary files for the applet to successfully launch and run. If the associated HTML for the applet refers to files that do not exist in the new archive, then the applet will not function correctly.

Secure Access only allows you to delete applets that are not currently in use by a Web or Terminal Services resource profile.

- b. Enter a name to identify the applet in the Name box (for new and replaced applets only).

- c. Browse to the applet that you want to upload to Secure Access. You can upload applets (.jar or .cab files) or archives (.zip, .jar, and .tar files) that contain applets and all of the resources that the applets need (for new and replaced applets only).
- d. Select the **Uncompress jar/cab file** check box if the file that you selected is an archive that contains the applet (New and replaced applets only).
- e. Click **OK** and then click **Close Window**.



**NOTE:** When you select an applet in the Java Applets dialog box, you are loading third-party software onto the Juniper product. By clicking OK, you are agreeing to the following terms on behalf of yourself (as purchaser of the equipment) or the organization that purchased the Juniper product, as applicable.

By loading third party software onto the Juniper Networks product, you are responsible for obtaining all rights necessary for using, copying, and/or distributing such software in or with the Juniper Networks product. Juniper is not responsible for any liability arising from use of such third party software and will not provide support for such software. The use of third party software may interfere with the proper operation of the Juniper Networks product and/or Juniper Networks software, and may void any warranty for the Juniper Networks product and/or Juniper Networks software.

6. Use settings in the Autopolicy: Java Access Control section to enable access if your Java applets need to make socket connections.
7. Click **Save and Continue**.
8. Select the roles to which the resource profile applies In the Roles tab and click Add.  
The selected roles inherit the autopolicies and bookmarks created by the resource profile. If it is not already enabled, Secure Access also automatically enables the Web option in the Users > User Roles > Select\_Role > General > Overview page of the admin console and the Allow Java Applets option Users > User Roles > Select\_Role > Web > Options page of the admin console for all of the roles you select.
9. Click **Save Changes**.
10. Create bookmarks in the Bookmarks tab.

**Related Documentation**

- [Configuring Hosted Java Applet Resource Profile Bookmarks on page 458](#)

---

## Configuring Hosted Java Applet Resource Profile Bookmarks

You must create bookmarks to your hosted Java applets to enable end users to access the applets.

To configure hosted Java applet resource profile bookmarks:

1. Select **Users > Resource Profiles > Web > Select Resource Profile > Bookmarks** in the admin console.
2. Click the appropriate link in the Bookmark column if you want to modify an existing bookmark. Or, click New Bookmark to create an additional bookmark.



**NOTE:** Although it is generally easiest to create a resource profile session bookmark through the resource profile configuration page, you can choose to create one through the user roles page as well if you have already created a resource profile.

3. Enter a name and optionally a description for the bookmark. This information displays on the Secure Access home page. (By default, Secure Access names the bookmark the same name as the corresponding resource profile.)



**NOTE:** We strongly recommend that you use a unique name for each bookmark to make it clear to users which link they are accessing.

4. Click Generate HTML to create an HTML page definition that includes references to your Java applets. Then, fill in any required attributes and parameters.

If you are using HTML generated by Secure Access, make sure to search the HTML code for “\_\_PLEASE\_SPECIFY\_\_” and update the code as necessary.

You can also add more HTML or JavaScript to this Web page definition. Secure Access rewrites all of the code that you enter in this field



**NOTE:** Make sure to enter unique HTML in this field. If you create two bookmarks with the same HTML code, Secure Access deletes one of the bookmarks in the end-user view. You will still be able to see both bookmarks, however, in the administrator console.

5. List those attributes in the Multi-Valued User Attributes box if your HTML code contains attributes that may expand to multiple values (such as userAttr.hostname or userAttr.ports), . When the user signs into Secure Access, Secure Access evaluates these attributes and creates separate bookmarks as necessary based on each of the individual values. If you use an attribute that expands to multiple values, but do not enter that attribute in this box, Secure Access creates a single bookmark based on the attribute's first value.
6. Under Display options, click Bookmark opens new window to enable Secure Access to automatically open the Web resource in a new browser window. Note that this functionality applies only to role bookmarks and not bookmarks created by users. Next, select the following options if you want to hide UI elements from the user:

- Do not display the browser address bar—Select this option to remove the address bar from the browser window. This feature forces all Web traffic through Secure Access by precluding users in the specified role from typing a new URL in the address bar, which circumvents Secure Access.
  - Do not display the browser toolbar—Select this option to remove the menu and toolbar from the browser. This feature removes all menus, browsing buttons, and bookmarks from the browser window so that the user browses only through Secure Access.
7. Under **Roles**, specify the roles to which you want to display the bookmark if you are configuring the bookmark through the resource profile pages:
    - **ALL selected roles**—Select this option to display the bookmark to all of the roles associated with the resource profile.
    - **Subset of selected roles**—Select this option to display the bookmark to a subset of the roles associated with the resource profile. Then select roles from the **ALL Selected Roles** list and click **Add** to move them to the **Subset of selected roles** list.
  8. Click **Save Changes**.

**Related Documentation**

- [Defining Resource Profile Bookmarks on page 134](#)
- [Creating Hosted Java Applets Bookmarks Through the User Roles Page on page 460](#)
- [Creating HTML Pages That Reference Uploaded Java Applets on page 456](#)
- [Required Attributes for Uploaded Java Applets on page 461](#)
- [Required Parameters for Uploaded Java Applets on page 462](#)

---

## Creating Hosted Java Applets Bookmarks Through the User Roles Page

---

It is generally easiest to create a hosted Java applets bookmark through the resource profile configuration pages, as explained in previous topic. However, you can choose to create a resource profile session bookmark through the user roles page using the following instructions:

1. Select **Users > Roles > Select\_Role > Web > Bookmarks** in the admin console.
2. Click **New Bookmark**.
3. Select **Pick a Web Resource Profile** from the Type list. (Secure Access does not display this option if you have not already created a hosted Java applet resource profile.)
4. Select an existing resource profile.
5. Click **OK**. (If you have not already associated the selected role with the resource profile, Secure Access automatically makes the association for you. Secure Access also enables any access control policies for the role that are required by the resource profile.)
6. If this role is not already associated with the selected resource profile, Secure Access displays an informational message. If you see this message, click **Save Changes** to



add this role to the resource profile's list of roles and to update the profile's autopolicies as required. Then, repeat the previous steps to create the bookmark.

7. Configure the bookmark settings.



**NOTE:** When you create a resource profile bookmark through the user roles page (instead of the standard resource profiles page), Secure Access only associates the generated bookmark with the selected role. Secure Access does not assign the bookmark to all of the roles associated with the selected resource profile.

**Related Documentation**

- [Accessing Java Applet Bookmarks on page 456](#)
- [Configuring Hosted Java Applet Resource Profile Bookmarks on page 458](#)

## Required Attributes for Uploaded Java Applets

When you create a Java applets bookmark through Secure Access, you must define the following attributes and their corresponding values. If you use the Generate HTML feature, Secure Access populates some of this information for you and adds PLEASE\_SPECIFY to those attributes whose values you must specify. When specifying attributes and their corresponding values, use the attribute="value" format.



**NOTE:** Secure Access generates parameters that it knows are required. Note, however, that Secure Access is not aware of all the applet-specific parameters that are required by your applet—you must find and fill in these parameters yourself.

Attributes that are required by Secure Access include:

- code—Indicates which class file to invoke in your Java applet. Use this value to point to your Java applet's main function. Example:
 

```
applet code="com.citrix.JICA"
```
- codebase—Indicates where the Web browser can fetch the applet. Use the <<CODEBASE>> variable, which points to the location on Secure Access where Secure Access stores the Java applet. When entering a path to a file, note that <<CODEBASE>> includes a trailing slash, which means the following example works:

```

```

This example does not work:

```

```

- archive—Indicates which archive file (that is, .jar, .cab, or .zip file) the Web browser should fetch. Example:

```
archive="JICAEngN.jar"
```

In addition to the required attributes listed earlier, you may also use the following optional attributes when creating a Java applet bookmark:

- name—Specifies a label for the Java applet. Example:

```
name="CitrixJICA"
```

- host—Specifies, for terminal sessions, the server to which Secure Access should connect.
- port—Specifies, for terminal sessions, the port to which Secure Access should connect.
- width and height—Indicates the size of the Java applet window. Example:

```
width="640" height="480"
```

- align—Indicates the Java applet window's alignment within the browser window. Example:

```
align="top"
```



**NOTE:** When defining attributes and their corresponding values, note the following:

- We strongly recommend that you not include `useslibrarycabbase` parameter in the HTML, because it causes the cab file to be permanently installed on the user's machine. If you later change a cab file on Secure Access, all users will have to manually delete the cab files on their machines to get the new version from Secure Access.
- We do not support applet tags that are constructed through the `document.write` function because the dynamic HTML interferes with the Secure Access parser.
- We do not support relative links to URLs, documents, or images in your HTML. If you do, the links will break when the user tries to access them from the Secure Access end-user console. Instead, you should include absolute links. If you are linking to a document or image included in your zip file, use the `<<CODEBASE>>` variable to indicate that Secure Access can find the file in zip archive uploaded to Secure Access. For example:

```

```

**Related Documentation**

- [Required Parameters for Uploaded Java Applets on page 462](#)

## Required Parameters for Uploaded Java Applets

When you create a Java applets bookmark through Secure Access, you must specify parameters and values that Secure Access should pass to the Java applet. These parameters are completely applet-specific. When specifying parameters and their corresponding values, use the following format:

```
<param name="parameterName" value="valueName">
```

Where all of the text is literal except *parameterName* and *valueName*.

You can use Secure Access variables to pass values to the Java applet by enclosing the variable names in double-brackets. For example, you might choose to pass the <<username>> and <<password>> values to the Java applet.



**NOTE:** When using the Java applet upload feature, if you include the <password> token within the generated HTML, it appears as cleartext if you view the source in the browser window that launches the applet. This behavior cannot be changed because Secure Access does not control how the Java applet processes the password. We strongly discourage the use of the <password> token in the HTML code.

If you find a Web page that contains an applet that you want to use, go to the demonstration site and view the source on the page that runs the Java applet. Within the source, look at the applet tag. Pick out the code attribute in the source and determine if it contains any special parameters that you need to pass to the browser. In most cases, you should be able to copy and paste the code attribute and its corresponding parameters directly into the HTML field for your Secure Access bookmark. Note, however, that if a parameter references a resource on the local Web server, you cannot copy and paste the reference into the Secure Access bookmark because Secure Access does not have access to the other Web server's local resources. When copying and pasting parameters from another source, always check the values of the parameters.

**Related  
Documentation**

- [Required Attributes for Uploaded Java Applets on page 461](#)

## Use case: Creating a Citrix JICA 9.5 Java Applet Bookmark

This topic discusses how to enable access to a Citrix Metaframe server through Secure Access using the 9.5 Java version of the Citrix ICA client (JICA).



**NOTE:** In addition to the method described here, you can also use Terminal Services resource profiles to host the Java versions of Citrix ICA clients on Secure Access.

Secure Access supports several mechanisms for intermediating traffic between a Citrix server and client, including the Terminal Services, JSAM, WSAM, VPN Tunneling, and hosted Java applets features.

To enable the Citrix JICA 9.5 client using the Java applet upload feature:

1. Import code-signing certificates.
2. Download **JICAcomponents.zip** from the citrix.com downloads page.

3. Create a hosted Java applet resource profile through the Users > Resource Profiles > Web page of the admin console. When defining the resource profile:
  - a. Upload the archived Citrix container file to Secure Access.
  - b. When uploading the applet, select the **Uncompress jar/cab file** check box because the container file contains multiple jar and cab files.
  - c. Specify any Metaframe servers to which these applets may connect.
  - d. Assign the resource profile to the appropriate roles.
4. Generate the Web page for the bookmark in the resource profile's Bookmarks tab. Secure Access automatically inserts all of the .jar files into the corresponding Web page. (JICA 95 supports only Sun JVM, so no cab files are present.) Then, specify parameters for the Citrix client using the following examples as a guide. (Note that the bookmark in the following example can contain references to the jar and cab files that are in the zip file.

#### JICA 9.5 Applet Example

```
<html>
<head>
<title>jica95 Applet</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>
```

```
<!--
```

```
Notes:
```

1) << CODEBASE >> is a system value that will get replaced at the time the applet is launched. Please do not modify this value.

2) Please modify the remaining values as needed.

3) Please make sure all attribute names/values are enclosed in double quotes.

```
-->
```

```
<body>
```

```
 <applet code="com.citrix.JICA"
 codebase="<< CODEBASE >>"
```

```
 archive="<< CODEBASE >>:jica95.jar"
 width="640" height="480"
 name="jica95" align="top">
```

```
 <param name="code" value="com.citrix.JICA">
```

```
 <param name="codebase" value="<< CODEBASE >>">
```

```
 <param name="archive"
 value="<< CODEBASE >>:jica95.jar"
 <param name="cabbase" value="">
```

```
 <param name="name" value="jica95">
```

```
 <param name="width" value="640">
```

```
 <param name="height" value="480">
```

```
 <param name="align" value="top">
```

```
<!--
```

```
Please specify additional params here after the comment.
```

```
<param name="paramname" value="paramvalue">
```

```
-->
```

```

 <param name="Address" value="__PLEASE_SPECIFY__">
 <param name="Username" value="<< user >>">
 <param name="password" value="<< password >>">
 <param name="EncryptionLevel" value="1">
 <param name="BrowserProtocol" value="HTTPOnTCP">
 </applet>
</body>
</html>

```

### JICA 8.x Applet Example

The following sample includes generated HTML code for the 8.x JICA client, which supported both Sun and MS JVMs:

```

<html>
<head>
<title>CitrixJICA Applet.</title>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1">
</head>
<!--
Notes:
1) << CODEBASE >> is a system value that will get
replaced at the time the applet is launched.
Please do not modify this value.
2) Please modify the remaining values as needed.
3) Please make sure all attribute names/values are
enclosed in double quotes.
-->
<body>
 <applet code="com.citrix.JICA"
 codebase="<< CODEBASE >>"
 archive="JICAEngN.jar,JICA-sicaN.jar,cryptojN.jar,JICA-configN.jar,JICA-coreN.jar"

 width="640" height="480"
 name="CitrixJICA" align="top">
 <param name="code" value="com.citrix.JICA">
 <param name="codebase" value="<< CODEBASE >>">
 <param name="archive"
value="JICAEngN.jar,JICA-sicaN.jar,cryptojN.jar,JICA-configN.jar,JICA-coreN.jar">
 <param name="cabbase"
value="cryptojM.cab,JICA-configM.cab,JICAEngM.cab,JICA-sicaM.cab,JICA-coreM.cab">

 <param name="name" value="CitrixJICA">
 <param name="width" value="640">
 <param name="height" value="480">
 <param name="align" value="top">
 <!--
Please specify additional params here after the comment.
 <param name="paramname" value="paramvalue">
 -->
 <param name="Address" value="__PLEASE_SPECIFY__">
 <param name="Username" value="<< user >>">
 <param name="password" value="<< password >>">
 <param name="EncryptionLevel" value="1">
 <param name="BrowserProtocol" value="HTTPOnTCP">
 </applet>

```

```
</body>
</html>
```

- Related Documentation**
- [Accessing Java Applet Bookmarks on page 456](#)
  - [Configuring Hosted Java Applet Resource Profile Bookmarks on page 458](#)

# Citrix Templates

- [About Citrix Templates on page 467](#)
- [Comparing Secure Access Access Mechanisms for Configuring Citrix on page 468](#)
- [Creating Resource Profiles Using Citrix Web Applications on page 471](#)

## About Citrix Templates

---

Secure Access supports several mechanisms for intermediating traffic between a Citrix server and client, including the Juniper Networks Citrix Terminal Services proxy, JSAM, WSAM, VPN Tunneling, and the hosted Java applets feature.

The Citrix Web template enables you to easily configure access to a Citrix server using the Juniper Networks Citrix Terminal Services proxy, JSAM, or WSAM. The Citrix Web template is a resource profile that controls access to Citrix applications and configures Citrix settings as necessary. Citrix Web templates significantly reduce your configuration time by consolidating configuration settings into one place and by prepopulating a variety of resource policy settings for you depending on the type of Citrix setup you select. You should use the Citrix Web template if you have the Citrix Web Interface already installed in your environment or if you are using a Web server to host your ICA files.

Because of their highly simplified configurations, templates are the ideal Citrix configuration method if you want to deliver ActiveX or Java applets from a third-party Web server through Secure Access.

Citrix Web templates simplify your configuration by automatically detecting whether the Citrix Web client or the Citrix Java applet is being used and employing the appropriate Secure Access access mechanism accordingly. For instance, if you have configured the Citrix Web Interface to deliver a Java client, Secure Access automatically uses its Java rewriting engine to tunnel traffic. If you have configured the Citrix Web Interface to deliver an ActiveX client, Secure Access uses its Citrix Terminal Services feature, JSAM, or WSAM (depending on the option you select) to tunnel traffic.

We strongly recommend using Citrix templates instead of the traditional role and resource policy configuration options available through Secure Access.



**NOTE:** Juniper Networks does not support saving a Citrix application shortcut to the desktop through Secure Access when the loopback IP address is running on the client. Double-clicking this shortcut returns an error as it does not use WSAM or JSAM.

---

**Related  
Documentation**

- [About Hosted Java Applet Templates on page 453](#)
- [Creating WSAM Client Application Resource Profiles on page 587](#)
- [Creating a JSAM Application Resource Profile on page 618](#)
- [Creating Resource Profiles Using Citrix Web Applications on page 471](#)

---

## Comparing Secure Access Access Mechanisms for Configuring Citrix

---

Secure Access supports several mechanisms for intermediating traffic between a Citrix server and client, including the Citrix Terminal Services proxy, JSAM, WSAM, VPN Tunneling, and the hosted Java applets feature.

The following table describes key differences when accessing a Citrix Metaframe Server through a Citrix Web Interface server. The descriptions in this table focus on configuring Citrix Terminal Services, JSAM, and WSAM through Web resource profile templates (Select Users > Resource Profiles > Web, click New Profile and select Citrix Web interface/JICA from the Type list.)



**NOTE:** If you want to configure access to a Citrix Metaframe server through a Citrix Web Interface server, you must use Web resource profile templates. If you want to configure access to a Citrix Metaframe server without using a Citrix Web Interface server, you must use a standard Citrix Terminal Services or WSAM resource profile or role.

---



Table 37: Accessing the Citrix Web Interface Server using Web Resource Profile Templates

Requirement	Terminal Services	JSAM	WSAM
User experience	<ol style="list-style-type: none"> <li>The user clicks a Citrix Web Interface bookmark in the Web Bookmarks section of the Secure Access end user console.</li> <li>The user is taken to the Citrix Web Interface (WI) sign-in page (assuming you do not configure FORM POST SSO).</li> <li>Once the user signs into the WI portal (either manually or automatically through SSO), he is taken to the Citrix WI portal page, which contains the list of published applications in icon form.</li> <li>When the user clicks the published application, the Juniper Networks Citrix Terminal Services (CTS) proxy launches and the ICA traffic is tunneled through the Juniper Networks CTS proxy.</li> </ol>	<ol style="list-style-type: none"> <li>The user launches JSAM.</li> <li>The user clicks a Citrix Web Interface bookmark in the Web Bookmarks section of the Secure Access end user console.</li> <li>The user is taken to the Citrix Web Interface (WI) sign-in page (assuming you do not configure FORM POST SSO).</li> <li>Once the user signs into the WI portal (either manually or automatically through SSO), he is taken to the Citrix WI portal page, which contains the list of published applications in icon form.</li> <li>When the user clicks the published application, the ICA traffic is tunneled through JSAM.</li> </ol>	<ol style="list-style-type: none"> <li>The user launches WSAM.</li> <li>The user clicks a Citrix Web Interface bookmark in the Web Bookmarks section of the Secure Access end user console.</li> <li>The user is taken to the Citrix Web Interface (WI) sign-in page (assuming you do not configure FORM POST SSO).</li> <li>Once the user signs into the WI portal (either manually or automatically through SSO), he is taken to the Citrix WI portal page, which contains the list of published applications in icon form.</li> <li>When the user clicks the published application, the ICA traffic is tunneled through WSAM.</li> </ol>
Accessing published applications from Mac or Linux	Not supported on Mac and Linux.	Supported on Mac and Linux.	Not supported on Mac and Linux.
Configuring ports	Secure Access automatically monitors all traffic on port 1494 if session reliability is turned off on the server. Secure Access monitors port 2598 if session reliability is turned on. You do not need to specify which ports to monitor or which applications to intermediate.	You must specify which ports Secure Access monitors. This enables you to access published applications that use ports other than 1494.	You do not need to specify which ports to monitor or which applications to intermediate. WSAM works in app mode and monitors all traffic coming from certain Citrix executables.
Administrator privileges	<p>If a Citrix Web client is not installed on the user's desktop, administrator privileges are required.</p> <p>This is a limitation of the installation of the Citrix client. To install and run the Juniper Networks Citrix Terminal Services proxy client, administrator privileges are not required.</p>	<p>If a Citrix Web client is not installed on the user's desktop, administrator privileges are required.</p> <p>This is a limitation of the installation of the Citrix client. To run JSAM, administrator privileges are not required.</p>	Requires administrator privileges to install WSAM.
Modifying host file	Does not require modification of the etc/hosts file.	Does not require modification of the etc/hosts file.	Does not require modification of the etc/hosts file.

The following table describes key differences when accessing a Citrix Metaframe Server without using a Citrix Web Interface server. The descriptions in this table focus on configuring Citrix Terminal Services, JSAM, and WSAM through standard resource profiles (Select Users > Resource Profiles > SAM or Terminal Services.)

Requirement	Terminal Services	JSAM	WSAM
User experience	The user launches the published application by clicking the bookmark or icon in the Terminal Services section of the Secure Access end user console.	<ol style="list-style-type: none"> <li>1. JSAM auto-launches when the user signs into Secure Access or the user launches JSAM manually.</li> <li>2. The user launches the published application using standard methods such as the Windows Start menu or a desktop icon.</li> </ol>	<ol style="list-style-type: none"> <li>1. WSAM auto-launches when the user signs into Secure Access or the user launches WSAM manually.</li> <li>2. The user launches the published application using standard methods such as the Windows Start menu or a desktop icon.</li> </ol>
Accessing published applications from Mac or Linux	Macintosh and Linux users cannot access published applications from a Citrix Metaframe server.	Macintosh and Linux users can access published applications from a Citrix Metaframe server.	Macintosh and Linux users cannot access published applications from a Citrix Metaframe server.
Admin configuration	You can specify which ports Secure Access intermediates. Or, if you do not configure this information, Secure Access automatically monitors ports 1494 and 2598.	You cannot configure Citrix as a standard application. Instead, you need to create a custom JSAM application, provide the server names of all Metaframe servers, and specify which ports Secure Access monitors. This enables you to use applications such as Citrix Secure Gateways (CSGs) and published applications that use ports other than 1494.	You must specify which ports and applications Secure Access monitors. This enables you to use applications such as Citrix Secure Gateways (CSGs) and published applications that use ports other than 1494.
Administrator privileges	<p>If a Citrix Web client is not installed on the user's desktop, administrator privileges are required.</p> <p>This is a limitation of the installation of the Citrix client. To install and run the Juniper Networks Citrix Terminal Services proxy client, administrator privileges are not required.</p>	Requires administrator privileges to run JSAM because etc/hosts file modifications are required.	Requires administrator privileges to install WSAM.
Modifying host file	Does not require modification of the etc/hosts file.	Requires modification of the etc/hosts file.	Does not require modification of the etc/hosts file.

- Related Documentation**
- [About Citrix Templates on page 467](#)
  - [Creating Resource Profiles Using Citrix Web Applications on page 471](#)

## Creating Resource Profiles Using Citrix Web Applications

The Citrix Web template enables you to easily configure Citrix access using the Juniper Networks Citrix Terminal Services proxy, JSAM, or WSAM.

To create a resource profile using the Citrix template:

1. Select **Users > Resource Profiles > Web** in the admin console.
2. Click **New Profile**.
3. Select Citrix Web Interface/JICA from the Type list.
4. Enter a unique name and optionally a description for the Citrix resource profile.
5. Enter the URL of the Web server that hosts your ICA files in the Web Interface (NFuse) URL field. Use the format: [protocol://]host[:port][[/path]]. For instance, enter the URL of an NFuse server, the Web interface for a Citrix Metaframe Presentation Server, or a Web server from which Secure Access can download Citrix Java applets or Citrix cab files. (Secure Access uses the specified URL to define the default bookmark for the Citrix resource profile.) You may enter a directory URL or a file URL.
6. Specify which type of Citrix implementation you are using in your environment by selecting one of the following options:
  - Java ICA Client with Web Interface (NFuse)—Select this option if you have deployed the Citrix Web Interface for MPS (that is, NFuse) to deliver Java ICA clients.
  - Java ICA Client without Web Interface (NFuse)—Select this option if you have deployed a generic Web server to deliver Java ICA clients.
  - Non-Java ICA Client with Web Interface (NFuse)—Select this option if you have deployed the Citrix Web Interface for MPS (that is, NFuse) to use any of the different clients (Java, ActiveX, local).
  - Non-Java ICA Client without Web Interface (NFuse)—(Read only) If you have deployed a non-Java ICA client without the Citrix Web Interface for MPS (that is, NFuse), you cannot create a Citrix resource profile through this template. Instead, click the client application profile link beneath this option. The link brings you to the Client Application Profiles page, where you can create a SAM resource profile.
7. From the Web Interface (NFuse) version list, select which Citrix version you are using. (Secure Access uses this value to pre-populate the Forms POST SSO values in your single sign-on autopolicy.
8. Specify the Metaframe Servers to which you want to control access in the MetaFrame servers area. Then click **Add**. When specifying servers, you can enter wildcards or IP ranges.

Secure Access uses the values that you enter to automatically create a corresponding resource policy that enables access to the necessary resources:

- If you select either **Java ICA Client with** or **without Web Interface**, Secure Access creates a corresponding Java ACL resource policy that enables Java applets to connect to the specified Metaframe servers.

- If you select **Non-Java ICA Client with Web Interface**, and then you select **ICA client connects over WSAM or JSAM**, Secure Access creates a corresponding SAM resource policy that enables users to access the specified Metaframe servers.
  - If you select **Non-Java ICA Client with Web Interface**, and then you select **ICA client connects over CTS**, Secure Access creates corresponding Terminal Services and Java resource policies that enable users to access the specified Metaframe servers.
9. (Java ICA clients only.) If you deployed Citrix using a Java ICA Client, select the **Sign applets with uploaded code-signing certificate(s)** check box to re-sign the specified resources using the certificate uploaded through the System > Configuration > Certificates > Code-signing Certificates page of the admin console.

When you select this option, Secure Access uses all of the “allow” values that you enter in the resource profile’s Web access control autopolicy to automatically create a corresponding code-signing resource policy. Within this policy, Secure Access uses the specified Web resources to create a list of trusted servers.

10. (Non-Java ICA clients only) If you have deployed Citrix using a non-Java ICA Client with a Web interface, you must use the Juniper Networks Citrix Terminal Services proxy, Secure Application Manager, or VPN Tunneling to secure traffic to your Metaframe servers instead of the Content Intermediation Engine.

To secure traffic through the Juniper Citrix Terminal Services proxy or the Secure Application Manager, select one of the following options in the ICA Client Access section:

- ICA client connects over CTS Client—Select this option to secure your Citrix traffic through the Secure Access Citrix Terminal Services client (if your users are using Active X clients) or Java rewriting engine (if your users are using Java clients). (When you select this option, Secure Access automatically enables the Terminal Services option on the Users > User Roles > *Select\_Role* > General > Overview page of the admin console.)



**NOTE:** If you are using a third-party Web server such as your company’s Intranet server to deliver the ICA file, make sure the Content-Type of the HTTP Response header is application/x-ica. Only then does Secure Access automatically intermediate the ICA file and launch its Citrix Terminal Services client to tunnel the traffic.



**NOTE:** If you select this option, we recommend that you disable Citrix client downloads through the Citrix Web Interface. Otherwise, users could inadvertently start two different windows downloading two versions of the Citrix client simultaneously—one through Secure Access (which automatically attempts to download the Citrix client if one is not present on the user’s computer) and one through the Citrix Web Interface.

- ICA client connects over WSAM—Select this option to secure traffic using WSAM. (When you select this option, Secure Access automatically enables the Secure Application Manager option on the Users > User Roles > *Select\_Role* > General > Overview page of the admin console.)
- ICA client connects over JSAM—Select this option to secure traffic using JSAM. Then, configure the following options:
  - Number of Servers/Applications—Enter the lesser of the following two numbers: maximum number of Citrix servers in your environment or the maximum number of published applications that a user can open simultaneously. For instance, if your environment contains one server and five published applications, enter 1 in this field. Or, if your environment contains 20 servers and 10 published applications, enter 10 in this field. The maximum value this field accepts is 99.
  - Citrix Ports—Specify the ports on which the Metaframe servers listen.

When you select the ICA client connects over JSAM option, Secure Access automatically enables the Secure Application Manager option on the Users > User Roles > *Select\_Role* > General > Overview page of the admin console.



**NOTE:** You cannot enable WSAM and JSAM for the same role. Therefore, if you try to create a Citrix resource profile that uses one of these access mechanisms (for instance, JSAM) and another profile associated with role already uses the other access mechanism (for instance, WSAM), Secure Access does not enable the new access mechanism (JSAM) for the role. Also note that you can only use WSAM or JSAM to configure access to one Citrix application per user role.

11. (Non-Java ICA Client with Web Interface only.) If you want to allow users to access local resources such as printers and drives through their Citrix Web Interface sessions, select the **Configure access to local resources** check box. Then, select from the following options:
  - Select **Connect printers** if you want to enable the user to print information from the terminal server to his local printer.
  - Select **Connect drives** if you want to enable the user to copy information from the terminal server to his local client directories.
  - Select **Connect COM Ports** if you want to enable communication between the terminal server and devices on the user's serial ports.



**NOTE:** To control access to local resources exclusively through your Citrix Metaframe server settings, clear the Configure access to local resources check box. When you clear the option, the Metaframe server settings take effect. Or, if you want to selectively override Citrix Metaframe server settings for the bookmark, select the Configure access to local resources check box and then specify the local resources to which you want to enable or disable access. Note that if you enable access to a local resource through Secure Access, however, you still must enable access to it through the Metaframe server as well.

When you enable local resources through the terminal server, each user can only access his own local resources. For instance, user 1 cannot see user 2's local directories.

12. Select the **Autopolicy: Web Access Control** check box to create a policy that allows or denies users access to the resource specified in the Web Interface (NFuse) URL field. (By default, Secure Access automatically creates a policy for you that enables access to the resource and all of its subdirectories.)
13. If you selected one of the Web interface options above, update the SSO policy created by the Citrix template. Select the **Autopolicy: Single Sign-on** check box. (Single sign-on autopolicies configure Secure Access to automatically pass Secure Access data such as usernames and passwords to the Citrix application. Secure Access automatically adds the most commonly used values to the single sign-on autopolicy based on the Citrix implementation you choose.)

When you select single sign-on, the WIClientInfo and WINGSession cookies are prepopulated automatically in addition to the POST Resource and URL.

Or, if you selected the non-Web interface option, you may optionally create your own single sign-on autopolicy.

14. Click **Save and Continue**.
15. Select the roles in the Roles tab to which the Citrix resource profile applies and click **Add**.

The selected roles inherit the autopolicies and bookmarks created by the Citrix resource profile. If it is not already enabled, Secure Access also automatically enables the Web option in the Users > User Roles > *Select\_Role* > General > Overview page of the admin console and the Allow Java Applets option in the Users > User Roles > *Select\_Role* > Web > Options page of the admin console for all of the roles you select.

16. Click **Save Changes**.
17. (Optional.) In the Bookmarks tab, modify the default bookmark created by Secure Access and/or create new ones.

By default, Secure Access creates a bookmark to the Web interface (NFuse) URL defined in the Web Interface (NFuse) URL field and displays it to all users assigned to the role specified in the Roles tab.

**Related  
Documentation**

- [About Citrix Templates on page 467](#)
- [Creating WSAM Client Application Resource Profiles on page 587](#)
- [Creating a JSAM Application Resource Profile on page 618](#)





# Lotus iNotes Templates

- [Creating Resource Profiles Using the Lotus iNotes Template on page 477](#)

## Creating Resource Profiles Using the Lotus iNotes Template

---

A Lotus iNotes template is a resource profile that controls access to the Web application and configures iNotes settings as necessary. Lotus iNotes templates significantly reduce your configuration time by consolidating settings into one place and by prepopulating a variety of resource policy settings for you depending on the type of setup you select.

Secure Access supports intermediating traffic to Lotus iNotes through a Web rewriting resource profile template, JSAM, WSAM, and VPN Tunneling. This topic describes how to configure access using the Web rewriting template. The prepopulated values vary depending on the version of iNotes you select and are based on the most common deployment of the servers.

To create a resource profile using the Lotus iNotes template:

1. Select **Users > Resource Profiles > Web** in the admin console.
2. Click **New Profile**.
3. Select the Lotus Notes version from the Type list.
4. Enter a unique name and optionally a description for the Lotus Notes resource profile.
5. Enter the URL of the Lotus iNotes resource to which you want to control access in the Base URL box. Use the format: [protocol://]host[:port][/path]. Secure Access uses the specified URL to define the default bookmark for the Lotus iNotes resource profile. You may enter a directory URL or a file URL.
6. Under iNotes setting, select **Allow caching on client** to let Web browsers store non-user data, such as Javascript and CSS files, on a user's machine. Select **Minimize caching on client** to allow Secure Access to send a cache-control:no-store header or a cache-control:no-cache header based on the user's Web browser and content type. This is the same as smart caching.

The Allow caching on client option caches content that the backend iNotes server typically caches. This caching option improves performance by using the cached content instead of retrieving the content from the server the next time the page displays. The Minimize caching on client option provides security by sending a cache-control:no-store header or a cache-control:no-cache header to either not store

content or to re-validate the cached content each time it is requested. With both caching option, you can choose to either allow or prevent the uploading or downloading of attachments.

7. Select the **Prevent download of attachments** check box to prohibit users from downloading attachments to their systems. Select the **Prevent upload of attachments** check box (available only for Lotus iNotes 6.5 and Lotus iNotes 7) to prevent users from transmitting (uploading) attachments to Secure Access.
8. Select the **Autopolicy: Web Access Control** check box to create a policy that allows or denies users access to the Web resource (and all of its subdirectories) listed in the Resource field.
  - a. In the Resource box, specify the Web server or HTML page to which you want to control access using the format: [protocol://]host[:port][/path].
  - b. From the Action list, select **Allow** to enable access to the specified resource or **Deny** to block access to the specified resource.
  - c. Click **Add**.
9. Select the **Autopolicy: Caching** check box to specify the resources to which this policy applies in the Resource box.



**NOTE:** The correct caching resource policy must be configured to allow end users to open and save e-mail attachments of different document types in iNotes. For example, if the caching policy is set to Smart, end users cannot save .htm or .html attachments to disk.

10. Select the **Autopolicy: Web Compression** check box to create a policy that specify which types of Web data Secure Access should and should not compress.
  - a. In the Resources field, specify the resources to which this policy applies.
  - b. Select one of the following options from the Action list:
    - Compress—Secure Access compresses the supported content types from the specified resource.
    - Do not compress—Secure Access does not compress the supported content types from the specified resource.
  - c. Click **Add**.
11. Select the **Autopolicy: Single Sign-On** check box to pass Secure Access data such as the username and password to the Lotus iNotes application.
12. Click **Save and Continue**.
13. Select the roles to which the Lotus iNotes resource profile applies in the Roles tab and click **Add**.

The selected roles inherit the autopolicies and bookmarks created by the Lotus iNotes resource profile. If it is not already enabled, Secure Access also automatically enables

the Web option in the Users > User Roles > *Select Role* > General > Overview page of the admin console.

14. Click **Save Changes**.

15. (Optional.) In the Bookmarks tab, modify the default bookmark created by Secure Access and/or create new ones

**Related  
Documentation**

- [About Hosted Java Applet Templates on page 453](#)
- [Creating WSAM Client Application Resource Profiles on page 587](#)
- [Creating a JSAM Application Resource Profile on page 618](#)
- [Creating Resource Profiles Using Citrix Web Applications on page 471](#)



# Microsoft OWA Templates

- [Creating Resource Profiles Using the Microsoft OWA Template on page 481](#)

## Creating Resource Profiles Using the Microsoft OWA Template

---

A Microsoft Outlook Web Access (OWA) template is a resource profile that controls access to the application and configures OWA settings as necessary. OWA templates significantly reduce your configuration time by consolidating configuration settings into one place and by prepopulating a variety of resource policy settings for you depending on the type of setup you select.

Secure Access supports intermediating traffic to Microsoft OWA through a Web rewriting resource profile template, JSAM, WSAM, and VPN Tunneling. This topic describes how to configure access using the Web rewriting template. The prepopulated values vary depending on the version of OWA you select and are based on the most common deployment of the servers.

To create a resource profile using the Microsoft OWA template:

1. Select **Users > Resource Profiles > Web Applications/Pages** in the admin console.
2. Click **New Profile**.
3. Select your Microsoft OWA version from the Type list.
4. Enter a unique name and optionally a description for the Citrix resource profile.
5. Enter the URL of the OWA resource to which you want to control access in the Base URL box. Use the format: [protocol://]host[:port][/path]. Secure Access uses the specified URL to define the default bookmark for the OWA resource profile. You may enter a directory URL or a file URL.

6. Under OWA settings select the following options,
  - a. (OWA 2000 and OWA 2003.) Select **Allow caching on client** to let Web browsers store non-user data, such as Javascript and CSS files, on a user's machine.

The Allow caching on client option caches content the backend OWA server typically caches. This caching option improves performance by using the cached content instead of retrieving the content from the server the next time the page displays.
  - b. (OWA 2000 and OWA 2003.) Select **Minimize caching on client** to allow Secure Access to send a cache-control:no-store header or a cache-control:no-cache header (do not store content or revalidate the cached content each time it is requested) based on the user's Web browser and content type. This is the same as smart caching.
  - c. (OWA 2007.) Select **Managed Device** to cache files. If you configure a Form post SSO, the trusted parameter is set to 4. This indicates the end user's device is private.
  - d. (OWA 2007.) Select **Unmanaged Device** to not cache files. If you configure a Form post SSO, the trusted parameter is set to 0. This indicates the end user's device is public.



**NOTE:** If it is necessary to download an attachment, the file is cached even though you select Unmanaged Device.

- e. Select **Prevent download of attachments** to prohibit users from downloading attachments to their systems.
  - f. Select **Prevent upload of attachments** to prevent users from transmitting (uploading) attachments to Secure Access.
7. Under Autopolicy: Web Access Control, create a policy that allows or denies users access to the Web resource (and all of its subdirectories) listed in the Resource field.
  - a. Specify the Web server or HTML page to which you want to control access in the Resource field. Use the format: [protocol://]host[:port][/path].
  - b. Select **Allow** to enable access to the specified resource or **Deny** to block access to the specified resource from the Action list.
  - c. Click **Add**.
8. Under Autopolicy: Caching, specify the resources to which this policy applies in the Resource box.



**NOTE:** The correct caching resource policy must be configured to allow end users to open and save e-mail attachments of different document types in OWA. For example, if the caching policy is set to Smart, end users cannot save .htm or .html attachments to disk.

9. Under Autopolicy: Web Compression, create a policy that specifies which types of Web data Secure Access should and should not compress.
  - a. Specify the resources to which this policy applies in the Resources box.
  - b. Select one of the following options from the Action list:
    - Compress—Secure Access compresses the supported content types from the specified resource.
    - Do not compress—Secure Access does not compress the supported content types from the specified resource.
  - c. Click **Add**.
10. Select the **Autopolicy: Single Sign-On** check box to pass Secure Access data such as the username and password to the OWA application.
11. Click **Save and Continue**.
12. Select the roles to which the resource profile applies in the Roles tab and click **Add**.

The selected roles inherit the autopolicies and bookmarks created by the Microsoft OWA resource profile. If it is not already enabled, Secure Access also automatically enables the Web option in the Users > User Roles > Select\_Role > General > Overview page of the admin console.
13. Click **Save Changes**.
14. (Optional.) Modify the default bookmark created by Secure Access in the Bookmarks tab, and/or create new ones.

**Related Documentation**

- [About Hosted Java Applet Templates on page 453](#)
- [Creating WSAM Client Application Resource Profiles on page 587](#)
- [Creating a JSAM Application Resource Profile on page 618](#)
- [Creating Resource Profiles Using Citrix Web Applications on page 471](#)





# Microsoft Sharepoint Templates

- [Creating Resource Profiles Using the Microsoft Sharepoint Template on page 485](#)

## Creating Resource Profiles Using the Microsoft Sharepoint Template

---

A Microsoft Sharepoint template is a resource profile that controls access to the application and configures Sharepoint settings as necessary. Microsoft Sharepoint templates significantly reduce your configuration time by consolidating configuration settings into one place and by pre-populating a variety of resource policy settings for you depending on the type of setup you select.

Secure Access supports intermediating traffic to Microsoft Sharepoint through a Web rewriting resource profile template, JSAM, WSAM, and VPN Tunneling. This topic describes how to configure access using the Web rewriting template.

SharePoint 2010 is supported with the following caveats:

- Office Web Apps through Windows Live is not supported
- OneNote document support is limited to only notebooks created to be stored on a local computer and then published on SharePoint 2010.
- Office documents residing on SharePoint server cannot be opened with Microsoft office when the server is accessed through Secure Access Service.



**NOTE:** In the current release, we support sending contact information from Sharepoint to your Outlook client through the Content Intermediation Engine (Web rewriting feature). Transferring the contact information to the backend Exchange server requires WSAM, JSAM, or VPN Tunneling. To import contact information into the Sharepoint server from your Outlook client, first export your contacts and then upload them to the Sharepoint server.

---

To create a resource profile using the Microsoft Sharepoint template:

1. Select **Users > Resource Profiles > Web** in the admin console.
2. Click **New Profile**.
3. Select **Microsoft Sharepoint** from the Type list.

4. Enter a unique name and optionally a description for the Sharepoint resource profile.
5. Enter the URL of the Sharepoint resource to which you want to control access in the Base URL field. Use the format: [protocol://]host[:port][/path]. Secure Access uses the specified URL to define the default bookmark for the Sharepoint resource profile. You may enter a directory URL or a file URL.
6. Under Sharepoint Settings, select **Allow in-line editing of documents within explorer view** to allow users to modify files displayed in the explorer view.



**NOTE:** This option is supported only if you enable persistent session (User > User Roles > RoleName > General > Session Options.)

- a. Enter the URL to the Explorer View page, and then click Add. Do not enter a value that resolves to non-Explorer View URLs (such as http://\*:\*). Doing so might cause Explorer View to not launch.
- b. Order the resources in your list, if appropriate, by selecting the check box next to an item and then using the up and down arrows to move it to the correct place in the list.
- c. Enter the number of minutes a persistent cookie resides on a user's computer before it expires in the Persistent cookie timeout box.



**NOTE:** Do not confuse this timeout option with Max. Session Length, which determines the number of minutes an active nonadministrative user session may remain open before ending.

7. Under Autopolicy: Web Access Control, create a policy that allows or denies users access to the Web resource (and all of its subdirectories) listed in the Resource box.
  - a. Specify the Web server or HTML page to which you want to control access in the Resource box. Use the format: [protocol://]host[:port][/path].
  - b. Select **Allow** to enable access to the specified resource or Deny to block access to the specified resource from the Action list.
  - c. Click **Add**.
8. (Optional.) Click **Show ALL autopolicy types** to create additional autopolicies that fine-tune access to the resource. Then, create the autopolicies.
9. Click **Save and Continue**.
10. Select the roles to which the resource profile applies in the Roles tab, and click **Add**.

The selected roles inherit the autopolicies and bookmarks created by the Microsoft Sharepoint resource profile. If it is not already enabled, Secure Access also automatically enables the Web option in the Users > User Roles > Select Role > General > Overview page of the admin console.

11. Click **Save Changes**.
12. (Optional.) Modify the default bookmark created by Secure Access in the Bookmarks tab or create new ones.

**Related  
Documentation**

- [About Hosted Java Applet Templates on page 453](#)
- [Creating WSAM Client Application Resource Profiles on page 587](#)
- [Creating a JSAM Application Resource Profile on page 618](#)
- [Creating Resource Profiles Using Citrix Web Applications on page 471](#)



## CHAPTER 21

# Web Rewriting

- [Web Rewriting on page 490](#)
- [Silverlight Support on page 491](#)
- [Task Summary: Configuring the Web Rewriting Feature on page 492](#)
- [Remote SSO Overview on page 494](#)
- [Passthrough Proxy Overview on page 495](#)
- [Creating a Custom Web Application Resource Profile on page 496](#)
- [Defining a Web Access Control Autopolicy on page 499](#)
- [Defining a Single Sign-On Autopolicy on page 500](#)
- [Defining a Caching Autopolicy on page 503](#)
- [Defining a Java Access Control Autopolicy on page 505](#)
- [Defining a Rewriting Autopolicy on page 506](#)
- [Defining a Web Compression Autopolicy on page 510](#)
- [Defining Web Resource Profile Bookmarks on page 511](#)
- [Specifying Web Browsing Options on page 515](#)
- [Resource Policy Overview on page 519](#)
- [Writing a Web Access Resource Policy on page 521](#)
- [Defining Single Sign-On Policies on page 522](#)
- [About Basic, NTLM and Kerberos Resources on page 522](#)
- [Writing the Basic, NTLM and Kerberos Resources on page 523](#)
- [Writing a Basic Authentication, NTLM or Kerberos Intermediation Resource Policy on page 527](#)
- [Writing a Remote SSO Form POST Resource Policy on page 529](#)
- [Writing a Remote SSO Headers/Cookies Resource Policy on page 531](#)
- [Writing a Web Caching Resource Policy on page 533](#)
- [About OWA and Lotus Notes Caching Resource Policies on page 535](#)
- [Specifying General Caching Options on page 536](#)
- [Writing a Java Access Control Resource Policy on page 537](#)
- [Writing a Java Code Signing Resource Policy on page 538](#)

- [Creating a Selective Rewriting Resource Policy on page 540](#)
- [Creating a Passthrough Proxy Resource Policy on page 542](#)
- [Creating a Custom Header Resource Policy on page 544](#)
- [Creating an ActiveX Parameter Resource Policy on page 546](#)
- [Restoring the Default Secure Access Service ActiveX Resource Policies on page 548](#)
- [Writing a Web Compression Resource Policy on page 552](#)
- [Defining an OWA Compression Resource Policy on page 553](#)
- [Writing a Web Proxy Resource Policy on page 554](#)
- [Specifying Web Proxy Servers on page 555](#)
- [Writing An HTTP 1.1 Protocol Resource Policy on page 555](#)
- [Creating a Cross Domain Access Policy on page 557](#)
- [Defining Resource Policies: General Options on page 558](#)
- [Managing Resource Policies: Customizing UI Views on page 559](#)

## Web Rewriting

---

The Secure Access Service Web rewriting feature enables you to intermediate Web URLs through the Content Intermediation Engine. You can intermediate URLs on the World Wide Web or on your corporate Intranet.

When you intermediate standard Web content through the Secure Access Service, you can create supplemental policies that “fine-tune” the access requirements and processing instructions for the intermediated content. You can create these supplemental policies through resource profiles (recommended) or resource policies.

Standard Web rewriting policy types include:

- **Web access control**—Web access policies control which Web resources users can access in order to connect to the Internet, intranet, or extranet.
- **Single sign-on**—Single sign-on policies enable you to automatically pass user credentials to a Web application. You can configure single sign-on policies to intercept basic authentication and NTLM challenges or post the credentials and headers that you specify to the Web application.
- **Caching**—Caching policies control which Web content the Secure Access Service caches on a user’s machine.
- **Java**—Java policies control to which servers and ports Java applets can connect. These policies also specify trusted servers for which the Secure Access Service resigns content.
- **Rewriting**—Rewriting policies specify resources that the Secure Access Service should not intermediate, minimally intermediation, or only intermediate selectively.
- **Web compression**—Web compression policies specify which types of Web data the Secure Access Service should and should not compress.
- **Web proxy**—(Resource policies only) Web proxy resource policies specify Web proxy servers for which the Secure Access Service should intermediate content. Note that

the Secure Access Service intermediates both forward and backwards proxies, but only enables single sign-on to trusted proxies.

- **Launch JSAM—(Resource policies only)** Launch JSAM policies specify URLs for which the Secure Access Service automatically launches J-SAM on the client. This feature is useful if you enable applications that require J-SAM but do not want to require users to run J-SAM unnecessarily.
- **Protocol—(Resource policies only)** Protocol resource policies enable or disable HTTP 1.1 protocol support on the Secure Access Service. .
- **Options— (Resource policies only)** You can enable IP based matching for hostnames as well as case-sensitive matching for path and query strings in Web resources through resource policy options.

Web rewriting is a standard feature on all Secure Access appliances except the SA700 Series Appliance. If you are using an SA700 Series Appliance, you must install a Core Clientless Access upgrade license in order to access baseline Web rewriting features. Note, however, that the following advanced Web rewriting features are not available on the SA700 Series Appliance, even if you have the Core Clientless Access upgrade license:

- Remote SSO
- WSAM & JSAM rewriting policies (available through Web application resource profiles)
- Non-Java ICA rewriting options (available through Citrix templates)

#### Related Documentation

- [Task Summary: Configuring the Web Rewriting Feature on page 492](#)
- [Writing a Web Access Resource Policy on page 521](#)
- [Defining a Single Sign-On Autopolicy on page 500](#)
- [Defining a Caching Autopolicy on page 503](#)
- [Writing a Java Access Control Resource Policy on page 537](#)
- [Defining a Rewriting Autopolicy on page 506](#)
- [Defining a Web Compression Autopolicy on page 510](#)
- [Writing a Web Proxy Resource Policy on page 554](#)
- [Automatically Launching JSAM on page 625](#)
- [Writing An HTTP 1.1 Protocol Resource Policy on page 555](#)
- [Defining Resource Policies: General Options on page 558](#)

## Silverlight Support

---

Secure Access Service supports Silverlight for rewriting for:

- Sharepoint 2010 – only the default Silverlight pages on Sharepoint 2010
- OWA 2010 - including file attachments in emails

Secure Access Service does not support custom XAP packages (custom Silverlight applications that a user can upload to a Sharepoint site).

No configuration steps are required for Silverlight support.

To support Silverlight on Sharepoint 2010, a system-generated rewriting resource policy is added for ActiveX with the following details:

```
Classid= DFEAF541-F3E1-4C24-ACAC-99C30715084A
Parameter= initParams:mediaSource,previewImageSource
Action= Rewrite URL and response (Static HTML only)
```

This policy is loaded during both upgrades and new installations. Do not remove this resource policy.

The colon (:) in the above Parameter field means the object tag contains the **initParams** parameter followed by comma separated name-value pairs.

For example, the above policy works for the following tag:

```
<param name="initParams"
value="mediaSource=/silverlight/media/Wildlife.wmv,previewImageSource=/silverlight/image/VideoPreview.png"
/>
```

## Task Summary: Configuring the Web Rewriting Feature



**NOTE:** When intermediating content through the content intermediation engine, we recommend that the GMT time on both the Secure Access Service and the backend web application server be the same. This prevents any premature expiration of cookies if the Secure Access Service time is later than the web application server time.

To configure the Web rewriting feature:

1. Create resource profiles that enable access to Web sites, create supporting autopolicies (such as single sign-on and Java access control policies) as necessary, include bookmarks that link to the Web sites, and assign the policies and bookmarks to user roles using settings in the Web Applications Resource Profiles page (Users > Resource Profiles > Web) of the admin console.

We recommend that you use resource profiles to configure Web rewriting (as described above). However, if you do not want to use resource profiles, you can configure Web rewriting using role and resource policy settings in the following pages of the admin console instead:

- a. Create resource policies that enable access to Web sites using settings in the Users > Resource Policies > Web > Web ACL page of the admin console.
- b. As necessary, create supporting resource policies (such as single sign-on and Java access control policies) using settings in the Users > Resource Policies > Select Policy Type pages of the admin console.



- c. Determine which user roles may access the Web sites that you want to intermedate, and then enable Web access for those roles through the Users > User Roles > Select Role > General > Overview page of the admin console.
  - d. Create bookmarks to your Web sites using settings in the Users > User Roles > Select Role > Web > Bookmarks page of the admin console.
  - e. As necessary, enable Web general options that correspond to the types of Web content you are intermediating (such as Java) using settings in the Users > User Roles > Select Role > Web > Options page of the admin console.
2. After enabling access to Web applications or sites using Web rewriting resource profiles or roles and resource policies, you can modify general role and resource options in the following pages of the admin console:
    - a. (Optional) Set additional Web browsing options (such as allowing users to create their own bookmarks or enabling hostname masking) Users > User Roles > Select Role > Web > Options page of the admin console.



**NOTE:** Even if you enable hostname masking, links corresponding to protocols not rewritten by the Secure Access Service are not obfuscated. For example, `ftp://xyz.juniper.net` and `file://fileshare.juniper.net/filename` are not obfuscated. By not obfuscating the hostname, users can still access these resources.

- b. (Optional) Set additional Web options for individual resources (such as enabling the Secure Access Service to match IP addresses to host names) using settings in the Users > Resource Policies > Web > Options page of the admin console.



**NOTE:** Certain Web rewriting features (such as passthrough proxy and SSO to NTLM resources) require additional configuration. For more information, see the appropriate configuration instructions.

#### Related Documentation

- [Writing a Web Access Resource Policy on page 521](#)
- [Defining a Single Sign-On Autopolicy on page 500](#)
- [Defining a Caching Autopolicy on page 503](#)
- [Writing a Java Access Control Resource Policy on page 537](#)
- [Defining a Rewriting Autopolicy on page 506](#)
- [Defining a Web Compression Autopolicy on page 510](#)
- [Writing a Web Proxy Resource Policy on page 554](#)
- [Automatically Launching JSAM on page 625](#)
- [Writing An HTTP 1.1 Protocol Resource Policy on page 555](#)

- [Defining Resource Policies: General Options on page 558](#)

## Remote SSO Overview

---

The Remote Single Sign-On (SSO) feature enables you to specify the URL sign-in page of an application to which you want the Secure Access Service to post a user's credentials, minimizing the need for users to re-enter their credentials when accessing multiple back-end applications. You may also specify additional forms values and custom headers (including cookies) to post to an application's sign-in form.

Remote SSO configuration consists of specifying Web resource policies:

- **Form POST policy**—This type of Remote SSO policy specifies the sign-in page URL of an application to which you want to post Secure Access Service data and the data to post. This data can include the user's primary or secondary Secure Access Service username and password as well as system data stored by system variables. You can also specify whether or not users can modify this information.
- **Headers/Cookies policy**—This type of Remote SSO policy specifies resources, such as customized applications, to which you can send custom headers and cookies.

If a user's Secure Access Service credentials differ from those required by the back-end application, the user can alternatively access the application:

- **By signing in manually**—The user can quickly access the back-end application by entering his credentials manually into the application's sign-in page. The user may also permanently store his credentials and other required information in the Secure Access Service through the Preferences page as described below, but is not required to enter information in this page.
- **Specifying the required credentials on the Secure Access Service**—The user must provide the Secure Access Service with his correct application credentials by setting them through the Preferences page. Once set, the user must sign out and sign back in to save his credentials on the Secure Access Service. Then, the next time the user clicks the Remote SSO bookmark to sign in to the application, the Secure Access Service sends the updated credentials.



**NOTE:** Use the Remote SSO feature to pass data to applications with static POST actions in their HTML forms. It is not practical to use Remote SSO with applications that employ frequently changing URL POST actions, time-based expirations, or POST actions that are generated at the time the form is generated.

### Related Documentation

- [System Variables and Examples on page 1186](#)
- [Multiple Sign-In Credentials Execution on page 339](#)
- [Writing a Remote SSO Form POST Resource Policy on page 529](#)
- [Writing a Remote SSO Headers/Cookies Resource Policy on page 531](#)

## Passthrough Proxy Overview

---

The passthrough proxy feature enables you to specify Web applications for which the Secure Access Service performs minimal intermediation. Unlike traditional reverse proxy functionality, which also rewrites only selective parts of a server response but requires network changes as well as complex configuration, this feature only requires that you specify application servers and the way in which the Secure Access Service receives client requests to those application servers:

- Via a Secure Access Service port—When specifying an application for the passthrough proxy to intermediate, you specify a port on which the Secure Access Service listens for client requests to the application server. When the Secure Access Service receives a client request for the application server, it forwards the request to the specified application server port. When you choose this option, you must open traffic to the specified Secure Access Service port on your corporate firewall.
- Via virtual host name—When specifying an application for the passthrough proxy to intermediate, you specify an alias for the application server host name. You need to add an entry for this alias in your external DNS server that resolves to the Secure Access Service. When the Secure Access Service receives a client request for the alias, it forwards the request to the port you specify for the application server.

This option is useful if your company has restrictive policies about opening firewall ports to either internal servers or servers in the DMZ. When using this option, we recommend that each host name alias contains the same domain substring as your Secure Access Service host name and that you upload a wild card server certificate to the Secure Access Service in the format: \*.domain.com.

For example, if your Secure Access Service is iveserver.yourcompany.com, then a host name alias should be in the format appserver.yourcompany.com and the wild card certificate format would be \*.yourcompany.com. If you do not use a wild card certificate, then a client's browser issues a certificate name check warning when a user browses to an application server, because the application server host name alias does not match the certificate domain name. This behavior does not prevent a user from accessing the application server, however.



**NOTE:** When you configure passthrough proxy to work in virtual host name mode, users must use the Secure Access Service host name that you specify through the System > Network > Overview page of the admin console when signing into the Secure Access Service. They cannot access use passthrough proxy if they sign into the Secure Access Service using its IP address.

---

Just as with the Content Intermediation Engine, the passthrough proxy option offers increased security relative to the Secure Application Manager, because when enabled for an application, the Secure Access Service allows the client to send only layer-7 traffic directed to fixed application ports to the enterprise network. Use this option to enable the Secure Access Service to support applications with components that are incompatible

with the Content Intermediation Engine, such as Java applets in Oracle e-business suite applications or applets that run in an unsupported Java Virtual Machine (JVM).

Note the following:

- Passthrough proxy URLs must be host names. Paths of host names are not supported.
- Juniper Networks strongly recommends that you not mix passthrough proxy Port mode and passthrough proxy Host mode.
- The passthrough proxy option works only for applications that listen on fixed ports and where the client does not make direct socket connections.
- To use passthrough proxy with Oracle E-Business applications, you must install a real certificate on the Secure Access Service and you must configure Oracle Forms to use the Forms Listener Servlet mode.
- The following advanced features of the Secure Access Service framed toolbar are not available in passthrough proxy: bookmark current page, display the original URL, display the favorite bookmarks.

**Related  
Documentation**

- Task Summary: Configuring Passthrough Proxy
- Examples of Using Passthrough Proxy
- [Creating a Passthrough Proxy Resource Policy on page 542](#)

---

## Creating a Custom Web Application Resource Profile

---

A custom Web application resource profile is a resource profile that controls access to a Web application, Web server, or HTML page.

To create a custom Web application resource profile:

1. In the admin console, select **Users > Resource Profiles > Web**.
2. Click **New Profile**.
3. From the Type list, choose **Custom**.
4. Enter a unique name and optionally a description for the resource profile.
5. In the Base URL field, enter the URL of the Web application or page for which you want to control access using the format: [protocol://]host[:port][/path]. (The Secure Access Service uses the specified URL to define the default bookmark for the resource profile.)
6. In the Autopolicy: Web Access Control section, create a policy that allows or denies users access to the resource specified in the Base URL field. (By default, the Secure Access Service automatically creates a policy for you that enables access to the Web resource and all of its sub-directories.)
7. (Optional) Click **Show ALL autopolicy types** to create additional autopolicies that fine-tune access to the resource. Then, create the autopolicies using instructions in the following sections:

8. Click **Save and Continue**.
9. In the Roles tab, select the roles to which the resource profile applies and click **Add**.  
 The selected roles inherit the autopolicies and bookmarks created by the resource profile. If it is not already enabled, the Secure Access Service also automatically enables the Web option in the Users > User Roles > Select Role > General > Overview page of the admin console for all of the roles you select.
10. Click **Save Changes**.
11. (Optional) In the Bookmarks tab, modify the default bookmark created by the Secure Access Service and/or create new ones. (By default, the Secure Access Service creates a bookmark to the base URL defined in the Base URL field and displays it to all users assigned to the role specified in the Roles tab.)

### Defining Base URLs

When creating a Web resource profile, you must use the following format when defining base URLs:

[protocol://]host[:port][/path]

Within this format, the components are:

- Protocol (required)—Possible values: http:// and https://. Note that you cannot use special characters within the protocol.
- Host (required)—Possible values:
  - DNS Hostname—For example: www.juniper.com
  - IP address—You must enter the IP address in the format: a.b.c.d. For example: 10.11.149.2. You cannot use special characters in the IP address.
- Ports (optional)—You must use the delimiter “:” when specifying a port. For example: 10.11.149.2/255.255.255.0:\*
- Path (optional)—When specifying a path for a base URL, the Secure Access Service does not allow special characters. If you specify a path, you must use the “/” delimiter. For example, http://www.juniper.net/sales.

### Defining Web Resources

When creating a Web resource profile, you must use the following format when defining resources for autopolicies:

[protocol://]host[:ports][/path]

Within this format, the four components are:

- Protocol (required)—Possible values: http:// and https://. Note that you cannot use special characters within the protocol.
- Host (required)—Possible values:
  - DNS Hostname—For example: www.juniper.com

You may use the following special characters allowed in the hostname:

**Table 38: DNS hostname special characters**

*	Matches ALL characters.
%	Matches any character except dot (.)
?	Matches exactly one character

- IP address/Netmask—You must enter the IP address in the format: a.b.c.d

You may use one of two formats for the netmask:

- Prefix: High order bits
- IP: a.b.c.d

For example: 10.11.149.2/24 or 10.11.149.2/255.255.255.0

You cannot use special characters in the IP address or netmask.

- Ports (optional)—You must use the delimiter “:” when specifying a port. For example: 10.11.149.2/255.255.255.0:\*

**Table 39: Port possible values**

*	Matches ALL ports; you cannot use any other special characters
port[,port]*	A comma-delimited list of single ports. Valid port numbers are [1-65535].
[port1]-[port2]	A range of ports, from port1 to port2, inclusive.



**NOTE:** You can mix port lists and port ranges, such as: 80,443,8080-8090

If the port is missing, then the default port 80 is assigned for http, 443 for https.

- Path (optional)—When specifying a path for a Web access control autopolicy, you may use a \* character, meaning ALL paths match. (The Secure Access Service does not support any other special characters.) If you specify a path, you must use the “/” delimiter. For example:
  - http://www.juniper.net/sales
  - http://www.juniper.net:80/\*
  - https://www.juniper.net:443/intranet/\*

**Related Documentation**

- [Resource Profiles on page 127](#)
- [About Hosted Java Applet Templates on page 453](#)
- [About Citrix Templates on page 467](#)

- [Creating Resource Profiles Using the Lotus iNotes Template on page 477](#)
- [Creating Resource Profiles Using the Microsoft OWA Template on page 481](#)
- [Creating Resource Profiles Using the Microsoft Sharepoint Template on page 485](#)
- [Defining a Web Access Control Autopolicy on page 499](#)
- [Defining a Single Sign-On Autopolicy on page 500](#)
- [Defining a Rewriting Autopolicy on page 506](#)
- [Defining a Web Compression Autopolicy on page 510](#)
- [Defining a Java Access Control Autopolicy on page 505](#)
- [Defining a Caching Autopolicy on page 503](#)

## Defining a Web Access Control Autopolicy

---

Web access policies control which Web resources users can access in order to connect to the Internet, intranet, or extranet. When defining a custom Web resource profile, you must enable a corresponding Web access control autopolicy that enables access to the profile's primary resource. The Secure Access Service simplifies the process for you by automatically creating an autopolicy that allows access to the Web resource and all of its sub-directories.

If necessary, you may choose to modify this default autopolicy or create supplementary Web access control autopolicies that control access to additional resources. For instance, your IT department may use one server to store Web pages for your company intranet (<http://intranetserver.com>) and another server to store the images that the Web pages reference (<http://imagesserver.com>). In this case, you can create two Web access control autopolicies that enable access to both servers so that your users can access both your Web pages and the corresponding images.

To create a new Web access control autopolicy:

1. Create a custom Web application resource profile.
2. If available, click the **Show ALL autopolicy types** button to display the autopolicy configuration options.
3. If it is not already enabled, select the **Autopolicy: Web Access Control** checkbox.
4. In the Resource field, specify the Web server or HTML page to which you want to control access using the format: `[protocol://]host[:ports][/path]`.
5. From the Action list, choose **Allow** to enable access to the specified resource or **Deny** to block access to the specified resource.
6. Click **Add**.
7. Click **Save Changes**.

### Related Documentation

- [Creating a Custom Web Application Resource Profile on page 496](#)

- [Configuring General Role Options on page 109](#)

## Defining a Single Sign-On Autopolicy

---

Single sign-on policies enable you to automatically pass user credentials to the Web application specified in your policy. Single sign-on autopolicies also intermedate the data that you pass.

To create a single sign-on (SSO) autopolicy:

1. Create a Web resource profile.
2. If available, click the **Show ALL autopolicy types** button to display the autopolicy configuration options.
3. Select the **Autopolicy: Single Sign-On** checkbox.
4. Select a single sign-on method and configure the corresponding SSO options:



**NOTE:** SSO options require you to select credentials. If you have not already done so, define the credentials using the Resource Policies > Web > General page prior to defining your SSO autopolicy.

- **Disable SSO**—Disables single sign-on.
- **Basic Auth**—Enables the Secure Access Service to intermedate the challenge/response sequence during basic authentication and use the credentials it collects to sign into a protected resource within the same Intranet zone. This option does not apply to Citrix resource profiles.
- **NTLM**—Enables the Secure Access Service to intermedate the challenge/response sequence during NTLM authentication and use the credentials it collects to sign into a protected resource within the same Intranet zone. This option does not apply to Citrix resource profiles.



**NOTE:** Web rewriting and file browsing both support NTLM v1 and NTLM v2.

- **Kerberos**—Enables the Secure Access Service to intermedate the challenge/response sequence during Kerberos authentication and use the credentials it collects to sign into a protected resource within the same Intranet zone.
- **Constrained Delegation**—Enables authentication of users by Kerberos after their identity has been verified using a non-Kerberos authentication method. For example, suppose a user authenticates with RADIUS and enters their passcode (typically PIN and token code). When accessing a service, the user may be challenged again because the PIN is not recognized. With constrained delegation, the administrator sets up passwords for constrained delegation users. The users do not need to know



this password. When accessing the same HTTP service, the Secure Access Service now fetches the ticket on behalf of the user without challenging the user.

- **Remote SSO**—Enables the Secure Access Service to post the data that you specify (including Secure Access Service usernames, passwords, and system data stored by variables) to Web applications. This option also enables you specify custom headers and cookies to post to Web applications.

5. Click **Save Changes**.

### Specifying Basic Authentication, NTLM or Kerberos SSO Autopolicy Options

To configure basic authentication, NTLM or Kerberos SSO autopolicy options:

1. Create an SSO autopolicy and choose Basic Auth, NTLM or Kerberos.
2. In the Resource field, specify the resources to which this policy applies.

When entering a resource in this field, note that:

- If you want the Secure Access Service to automatically post values to a specific URL when an end-user clicks on a Secure Access Service bookmark, the resource that you enter here must exactly match the URL that you specify in the Base URL field of the resource profile.
  - If you want the Secure Access Service to automatically submit user credentials to other Web sites within the same Intranet zone, the host name that you enter here must end in the DNS suffix configured in the System > Network > Overview page of the admin console.
3. Select the credentials to use. If this pull-down menu is blank, no credentials are defined in the SSO General tab.
  4. (NTLM only) Select the **Fallback to NTLM V1** option to fallback to NTLM V1 if NTLM V2 fails. If you do not select this option, the Secure Access Service falls back only to NTLM V2. An intermediation page appears if SSO fails.
  5. (Kerberos only) Select the **Fallback to NTLM V2 only** option to fallback only to NTLM V2 if kerberos fails. If you do not select this option, a Kerberos intermediation page appears if Kerberos SSO fails.
  6. (Constrained delegation only) Select the **Fallback to Kerberos** option fallback to Kerberos if constrained delegation fails. If you do not select this option, an error page appears if SSO fails.

### Specifying Remote SSO Autopolicy Options

To configure remote SSO autopolicy options:

1. Create an SSO autopolicy through a custom Web resource profile and choose **Remote SSO**.
2. If you want to perform a form POST when a user makes a request to the resource specified in the Resource field, select the POST the following data checkbox. Then:
  - a. In the Resource field, specify the application's sign-in page, such as: `http://my.domain.com/public/login.cgi`. The Secure Access Service does not accept wildcard characters in this field.

If you want the Secure Access Service to automatically post values to a specific URL when an end-user clicks on Secure Access Service bookmark, the resource that you enter here must exactly match the URL that you specify in the Base URL or Web Interface (NFuse) URL field of the resource profile.

- - b. In the Post URL field, specify the absolute URL where the application posts the user's credentials, such as: `http://yourcompany.com/login.cgi`. You can determine the appropriate URL using a TCP dump or by viewing the application's sign-in page source and searching for the POST parameter in the FORM tag.
    - c. Optionally specify the user data you want to post and user modification permissions.

To specify user data to post, enter data in the following fields and click **Add**:

- **Name**—The name to identify the data of the Value field. (The back-end application should expect this name.)
  - **Value**—The value to post to the form for the specified Name. You can enter static data, a system variable, or Secure Access Service session variables containing username and password values.
  - **User modifiable? setting**—Set to **Not modifiable** if you do not want the user to be able to change the information in the Value field. Set to **User CAN change value** if you want the user to have the option of specifying data for a back-end application. Set to **User MUST change value** if users must enter additional data in order to access a back-end application. If you choose either of the latter settings, a field for data entry appears on the user's Advanced Preferences page in the Secure Access Service. This field is labeled using the data you enter in the User label field. If you enter a value in the Value field, this data appears in the field but is editable.
- - 
      - 
      - d. Select the **Deny direct login for this resource** checkbox if you do not want allow users to manually enter their credentials in a sign-in page. (Users may see a sign-in page if the form POST fails.)
      - e. Select the **Allow multiple POSTs to this resource** checkbox if you want the Secure Access Service to send POST and cookie values to the resource multiple times if required. If you do not select this option, the Secure Access Service does not attempt

single sign-on when a user requests the same resource more than once during the same session.

3. If you want to post header data to the specified URL when a user makes a request to a resource specified in the Resource field, select the **Send the following data as request headers** checkbox. Then:
  - a. In the Resource section, specify the resources to which this policy applies.
  - b. Optionally specify the header data to post by entering data in the following fields and clicking **Add**:
    - **Header name**—The text for the Secure Access Service to send as header data.
    - **Value**—The value for the specified header.
4. Click **Save Changes**.

**Related Documentation**

- [Creating a Custom Web Application Resource Profile on page 496](#)
- [Remote SSO Overview on page 494](#)

## Defining a Caching Autopolicy

Caching policies control which Web content the Secure Access Service caches on a user's machine.

To create a Web caching autopolicy:

1. Create a custom Web application resource profile.
2. If available, click the **Show ALL autopolicy types** to display the autopolicy configuration options.
3. Select the **Autopolicy: Caching** checkbox.
4. In the Resource field, specify the resources to which this policy applies.
5. In the Action field, select one of the following options:
  - **Smart**—Select this option to allow the Secure Access Service to send a cache-control:no-store header or a cache-control:no-cache header based on the user's Web browser and content type.

When you select this option, the Secure Access Service makes media files and zip files work properly by removing their origin server's cache-control headers. For example, the following logic searches for "msie" or "windows-media-player" in user-agent headers in order to remove cache or cache-control:no-store response headers and make the files cacheable:

```
(if content type has "audio/x-pn-realaudio" OR
 if content type begins with "video/" OR
 if content type begins with "audio/" OR
 if content type is "application/octet-stream" and the file extension begins
 with ".rm" or ".ram"
)
```

If the Secure Access Service finds “msie” or “windows-media-player” in the user-agent header and any of the following apply:

- Request is for Flash, .xls, .pps, .ppt files
- Content-type is application/, text/rtf, text/xml, model/
- Origin server sends a content-disposition header

then Secure Access Service sends the cache-control:no-store header and removes the origin server's cache-control header.

In all other cases, the Secure Access Service adds the pragma:no-cache or cache-control:no-store response headers.



**NOTE:** Citrix .ica and QuickPlace files get some special treatment. Citrix .ica files get cache-control:private only when smart caching is enabled. QuickPlace files that do not match a specified rule files (which takes precedence) get CCNS and cache-control:private.

Also note that if you select this option, enable GZIP compression, and try to access a text file attachment using Domino Web Access 6.5 through Internet Explorer, you cannot open the attachment. To enable text attachments, you must either install the Internet Explorer 323308 patch or enable the No Store option.

- **No-Store**—Select this option to deliver attachments to Internet Explorer without saving them to the disk. (The browser temporarily writes files to the disk, but immediately removes them once it has opened the file in the browser.) When you select this option, the Secure Access Service removes the origin server's cache-control header and adds a cache-control:no-store response header if the user-agent string sent by the browser contains “msie” or “windows-media-player.”

This option might slow browsing by causing repeated content fetches, which can cause performance issues on very slow connections.

- **No-Cache**—Select this option to prevent the user's browser from caching files to the disk. When you select this option, the Secure Access Service adds the standard HTTP pragma:no-cache header and cache-control:no-cache (CCNC) header (HTTP 1.1) to response files. Also, the Secure Access Service does not forward the origin server's caching headers, such as age, date, etag, last-modified, expires.

When no-cache headers are present on certain types of attachments (PDF, PPT, streaming files), Internet Explorer does not properly render the documents because the rendering process requires the browser to temporarily writes these files to cache.

- **Unchanged**—The Secure Access Service forwards the origin server's caching headers as is.

When using Citrix published applications through the Web interface, the Web interface server may send a Cache-Control:no-cache in the response header of the .ica file. Because the caching header is not removed when using the Unchanged

setting, .ica files are not downloaded to the client PC. To resolve this, use the Smart caching option.

6. Click **Add**.
7. Click **Save Changes**.

**Related Documentation**

- [Creating a Custom Web Application Resource Profile on page 496](#)

## Defining a Java Access Control Autopolicy

A Java access control autopolicy defines the list of servers and ports to which Java applets can connect. This autopolicy also specifies which resources the Secure Access Service signs using the code-signing certificate that you upload to the Secure Access Service.

When you enable Java access control using this autopolicy, the Secure Access Service automatically enables the Allow Java applets option on the Users > User Roles > Select Role > Web > Options page of the admin console.

To create a Java access control autopolicy:

1. Create a custom Web application resource profile.
2. Click **Show ALL autopolicy types**.
3. Select the **Autopolicy: Java Access Control** checkbox.
4. In the Resource field, specify the server resources to which this policy applies using the format: host:[ports]. (By default, the Secure Access Service populates this field with the server specified in your resource profile's base URL.)
5. Select one of the following options from the Action list:
  - **Allow socket access**—To enable Java applets to connect to the servers (and optionally ports) in the Resource list.
  - **Deny socket access**—To prevent Java applets from connecting to the servers (and optionally ports) in the Resource list.
6. Click **Add**.
7. Select the **Sign applets with code-signing certificate** checkbox to resign the specified resources using the certificate uploaded through the System > Configuration > Certificates > Code-signing Certificates page of the admin console. (The Secure Access Service uses the imported certificate to sign the server resources that you specify in the Resources field.)
8. Click **Save Changes**.

### Defining a Server to Which Java Applets Can Connect

When defining servers to which Java applets can connect, you must use the following format:

host[:ports]

Within this format, the two components are:

- Host (required)—Possible values:
  - DNS Hostname—For example: www.juniper.com

You may use the following special characters allowed in the hostname:

*	Matches ALL characters.
%	Matches any character except dot (.)
?	Matches exactly one character

- IP address/Netmask—You must enter the IP address in the format: a.b.c.d.

You may use one of two formats for the netmask:

Prefix: High order bits

IP: a.b.c.d

For example: 10.11.149.2/24 or 10.11.149.2/255.255.255.0 You cannot use special characters in the IP address or netmask.

- Ports—You must use the delimiter “:” when specifying a port. For example: 10.11.149.2/255.255.255.0:\*

**Table 40: Port Possible Values**

*	Matches ALL ports; you cannot use any other special characters
port[,port]*	A comma-delimited list of single ports. Valid port numbers are [1-65535].
[port1]-[port2]	A range of ports, from port1 to port2, inclusive.



**NOTE:** You can mix port lists and port ranges, such as: 80,443,8080-8090.

**Related Documentation**

- [About Hosted Java Applet Templates on page 453](#)
- [Creating a Custom Web Application Resource Profile on page 496](#)

## Defining a Rewriting Autopolicy

By default, the Secure Access Service intermediates all user requests to Web hosts—unless you have configured the Secure Access Service to serve requests to certain hosts using a different mechanism, such as the Secure Application Manager. Rewriting autopolicies enable you to “fine-tune” the default options by changing which mechanisms the Secure Access Service should use to rewrite Web data and defining resources that you want to minimally rewrite or not rewrite at all.

To create a rewriting autopolicy:

1. Create a custom Web application resource profile.
2. Click **Show ALL autopolicy types**.
3. Select the **Autopolicy: Rewriting Options** checkbox.
4. Select one of the following options:
  - **Passthrough Proxy**—Select this option to specify Web applications for which the Content Intermediation Engine performs minimal intermediation..
  - **No rewriting (use WSAM)**—Select this option to intermediate content using WSAM instead of the Content Intermediation Engine. Then, specify the application server for which you want to intermediate content. (At minimum, you need to click **Add** in order to intermediate content to and from the server that the Secure Access Service extracts from the Web access control policy.) .
  - **No rewriting (use JSAM)**—Select this option to intermediate content using JSAM instead of the Content Intermediation Engine. Then, specify the application server for which you want to intermediate content.(At minimum, you need to click **Add** in order to intermediate content to and from the server that the Secure Access Service extracts from the Web access control policy.)
  - **No rewriting**—Select this option to automatically create a selective rewriting policy for the autopolicy's URL, thereby configuring the Secure Access Service not intermediate any content to and from the resource. For example, you may choose this option if you do not want the Secure Access Service to intermediate traffic from Web sites that reside outside of the corporate network, such as yahoo.com. If you select this option, you do not have to configure any additional rewriting settings.

### Specifying Passthrough Proxy Autopolicy Options

To configure passthrough proxy autopolicy options:

1. Create an rewriting autopolicy and select **Passthrough Proxy**.
2. Choose the way in which you want to enable the passthrough proxy feature:
  - **Use virtual hostname**—If you choose this option, specify a host name alias for the application server. When the Secure Access Service receives a client request for the application server host name alias, it forwards the request to the specified application server port in the Base URL field.
  - **Use Secure Gateway port**—If you choose this option, specify a unique Secure Access Service port in the range 11000-11099. The Secure Access Service listens for client requests to the application server on the specified Secure Access Service port and forwards any requests to the application server port specified in the Base URL field.

The corresponding URL for the resource profile must specify the application server host name and the port used to access the application internally. You cannot enter a path for the base URL.

In order to make Sharepoint work successfully through the Secure Access Service, you must select the Override automatic cookie handling checkbox in Internet Explorer

under Tools Internet options > Privacy > Advanced Privacy Settings if the following conditions true:

- You select the **Use virtual hostname** option during Pass Through Proxy configuration.
  - The virtual hostname that you specify in your Sharepoint configuration is different from the hostname that you configure through Secure Access Service setup (that is, if the domains are different).
  - You enable persistent cookies through the Users > User Roles > Select Role > General > Session Options page of the admin console.
3. Select the **Rewrite XML** checkbox if you want the Secure Access Service to rewrite URLs contained within XML content. If this option is disabled, the Secure Access Service passes the XML content “as is” to the server.
  4. Select the **Rewrite external links** checkbox if you want the Secure Access Service to rewrite all the URLs presented to the proxy. If this option is disabled, the Secure Access Service rewrites only those URLs where the hostname is configured as part of the passthrough proxy policy.
  5. Select the **Block cookies from being sent to the browser** checkbox if you want the Secure Access Service to block cookies destined for the client’s browser. The Secure Access Service stores the cookies locally and sends them to applications whenever they are requested.
  6. Select the **Host-Header forwarding** checkbox if you want the Secure Access Service to pass the hostname as part of the host header instead of the actual host identifier.  
  
The Host-Header forwarding option is only valid in passthrough proxy Virtual hostname mode.
  7. Click **Save Changes**.
  8. If you select:
    - Use virtual hostname, you must also:
      - Add an entry for each application server host name alias in your external DNS that resolves to the Secure Access Service.
      - Upload a wildcard server certificate to the Secure Access Service (recommended).
      - Define the Secure Access Service name and host name in the Network Identity section of the System > Network > Internal Port tab.
    - To use the Secure Access Service port, you must also open traffic to the Secure Access Service port you specified for the application server in your corporate firewall.  
  
If your application listens on multiple ports, configure each application port as a separate passthrough proxy entry with a separate Secure Access Service port. If you intend to access the server using different host names or IP addresses, configure each of those options separately; in this case, you can use the same port.

### Specifying WSAM Rewriting Autopolicy Options



To configure WSAM rewriting autopolicy options:

1. Create an rewriting autopolicy and select **No rewriting (use WSAM)**.
2. In the Destination field, specify resources for which WSAM secures client/server traffic between the client and the Secure Access Service. By default, the Secure Access Service extracts the correct server from the Web access control policy. You may choose to use this server as-is, modify it, and/or add new servers to the list.

When specifying a server, specify the host name (the wild cards '\*' or '?' are accepted) or an IP/netmask pair. Specify multiple ports for a host as separate entries.

3. Click **Add**.
4. Click **Save Changes**.

When you intermeditation through WSAM using this autopolicy, the Secure Access Service automatically enables the Secure Application Manager option on the Users > User Roles > Select Role > General > Overview page of the admin console.

### Specifying JSAM Rewriting Autopolicy Options

To configure JSAM rewriting autopolicy options:

1. Create an rewriting autopolicy and select **No rewriting (use JSAM)**.
2. In the Server Name field, enter the DNS name of the application server or the server IP address.
3. In the Server Port field, enter the port on which the remote server listens for client connections.

For example, to forward Telnet traffic from a remote machine, specify port 23 for both the client port (on which JSAM listens) and the server port (on which the Telnet server listens).



**NOTE:** To enable drive mapping to this resource, enter 139 as the server port.

4. In the Client Loopback IP field, provide a static loopback address. If you do not provide a static IP loopback address, the Secure Access Service assigns an IP loopback address dynamically.
5. In the Client Port field, enter the port on which JSAM should listen for client application connections.

Typically, the local port value is the same value as the server port; the local port value usually only differs for Linux or Macintosh users who want to add applications for port forwarding that use ports under 1024.



**NOTE:** To enable drive mapping to this resource, enter 139 as the server port.

You may configure more than one application on a single port, such as app1.mycompany.com, app2.mycompany.com, app3.mycompany.com. Either you assign a static loopback address or the Secure Access Service assigns a dynamic loopback address (127.0.1.10, 127.0.1.11, 127.0.1.12) to each application. JSAM then listens on these multiple loopback addresses on the specified port. For example, when there is traffic on 127.0.1.12 on the specified port, the Secure Access Service forwards the traffic to the app3.mycompany.com destination host.

6. Select **Launch JSAM** to automatically start JSAM when the Secure Access Service encounters the Base URL.
7. Click **Add**.
8. Click **Save Application** or **Save + New**.

#### Related Documentation

- [Web Rewriting on page 490](#)
- [Passthrough Proxy Overview on page 495](#)
- [Task Summary: Configuring WSAM on page 584](#)
- [Task Summary: Configuring JSAM on page 601](#)

## Defining a Web Compression Autopolicy

Web compression autopolicies specify which types of Web data the Secure Access Service should and should not compress. For example, since javascript does not work when compressed, you might use this feature to specify that the Secure Access Service should not compress javascript data going to and from an email server by entering the following resource: http://owa.juniper.net/\*.js.



**NOTE:** In order to properly compress data, you must enable compression at the system level as well as creating compression autopolicies. To enable compression, use settings in the Maintenance > System > Options page of the admin console.

To create a Web compression autopolicy:

1. Create a custom Web application resource profile.
2. If available, click the **Show ALL autopolicy types** button to display the autopolicy configuration options.
3. Select the **Autopolicy: Web compression** checkbox.
4. In the Resource field, specify the resources to which this policy applies.
5. Select one of the following options from the Action list:
  - **Compress**—The Secure Access Service compresses the supported content types from the specified resource.

- **Do not compress**—The Secure Access Service does not compress the supported content types from the specified resource.
6. Click **Add**.
  7. Click **Save Changes**.

**Related  
Documentation**

- [About Compression on page 1157](#)
- [Creating a Custom Web Application Resource Profile on page 496](#)

## Defining Web Resource Profile Bookmarks

When you create a Web resource profile, the Secure Access Service automatically creates a bookmark that links to the primary URL or domain that you specified in the resource profile. The Secure Access Service enables you to modify this bookmark as well as create additional bookmarks within the same domain.

For example, you may create a resource profile that controls access to your company intranet. Within the profile, you may specify:

- Resource profile name: Your Intranet
- Primary resource: <http://intranet.com>
- Web access control autopolicy: Allow access to [http://intranet.com:80/\\*](http://intranet.com:80/*)
- Roles: Sales, Engineering

When you create this policy, the Secure Access Service automatically creates a bookmark called “Your Intranet” enabling access to <http://intranet.com> and displays the bookmark to members of the Sales and Engineering roles.

You may then choose to create the following additional bookmarks to associate with the resource profile:

- “Sales Intranet” bookmark: Creates a link to the <http://intranet.com/sales> page and displays the link to members of the Sales role.
- “Engineering Intranet” bookmark: Creates a link to the <http://intranet.com/engineering> page and displays the link to members of the Engineering role.

When configuring bookmarks, note that:

- You can only assign bookmarks to roles that you have already associated with the resource profile—not all of the roles defined on the Secure Access Service. To change the list of roles associated with the resource profile, use settings in its Roles tab.
- Bookmarks simply control which links the Secure Access Service displays to users—not which resources the users can access. For instance, in the example used above, a member of the Sales role would not see a link to the Engineering Intranet page, but he could access it by entering <http://intranet.com/engineering> his Web browser’s address bar.

- You cannot create bookmarks that link to additional URLs and domains defined through Web access control autopolicies.

You can use two different methods to create Web bookmarks:

- Create bookmarks through existing resource profiles (recommended)—When you select this method, the Secure Access Service automatically populates the bookmark with key parameters (such as the Web interface (NFuse) URL) using settings from the resource profile. Additionally, while you are creating the associated resource profile, the Secure Access Service guides you through the process of creating any required policies to enable access to the bookmark.
- Create standard bookmarks—When you select this option, you must manually enter all bookmark parameters during configuration. Additionally, you must enable access to the Web feature and create resource policies that enable access to the Web sites defined in the bookmark.

### Creating Bookmarks Through Existing Resource Profiles

To configure Web resource profile bookmarks:

1. If you want to create a resource profile bookmark through the standard resource profiles page:
  - a. In the admin console, select **Users > Resource Profiles > Web > Resource Profile Name > Bookmarks**.
  - b. Click the appropriate link in the Bookmark column if you want to modify an existing bookmark. Or, click **New Bookmark** to create an additional bookmark.

Alternatively, if you want to create a resource profile bookmark through the user roles page:

- a. In the admin console, select **Users > User Roles > Role Name > Web > Bookmarks**.
- b. Click **New Bookmark**.
- c. From the Type list, choose **Pick a Web Resource Profile**. (The Secure Access Service does not display this option if you have not already created a Web resource profile.)
- d. Select an existing resource profile.
- e. Click **OK**. (If you have not already associated the selected role with the resource profile, the Secure Access Service automatically makes the association for you. The Secure Access Service also enables any access control policies for the role that are required by the resource profile.)
- f. If this role is not already associated with the selected resource profile, the Secure Access Service displays an informational message. If you see this message, click **Save Changes** to add this role to the resource profile's list of roles and to update the profile's autopolicies as required. Then, repeat the previous steps to create the bookmark.

When you create a resource profile bookmark through the user roles page (instead of the standard resource profiles page), the Secure Access Service only associates the generated bookmark with the selected role. The Secure Access Service does not assign the bookmark to all of the roles associated with the selected resource profile.

2. Optionally change the name and description of the bookmark. (By default, the Secure Access Service populates names the bookmark using the resource profile name.)
3. In the URL field, add a suffix to the URL if you want to create links to sub-sections of the domain defined in the primary resource profile.

Make sure to enter a unique URL in this field. If you create two bookmarks with the same URL, the Secure Access Service deletes one of the bookmarks from the end-user view. You will still be able to see both bookmarks, however, in the administrator console.

4. Under Options, select the **Bookmark opens in new window** checkbox if want to enable the Secure Access Service to automatically open the Web resource in a new browser window. Next, select:
  - **Do not display browser address bar**—Select this option to remove the address bar from the browser window. This feature forces all Web traffic through the Secure Access Service by precluding users in the specified role from typing a new URL in the address bar, which circumvents the Secure Access Service.
  - **Do not display browser toolbar**—Select this option to remove the menu and toolbar from the browser. This feature removes all menus, browsing buttons, and bookmarks from the browser window so that the user browses only through the Secure Access Service.
5. If you are configuring the bookmark through the resource profile pages, under Roles, specify the roles to which you want to display the bookmark:
  - **ALL selected roles**—Select this option to display the bookmark to all of the roles associated with the resource profile.
  - **Subset of selected roles**—Select this option to display the bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL Selected Roles list and click **Add** to move them to the Subset of selected roles list.
6. Click **Save Changes**.

### Creating Standard Web Bookmarks

Information in this section is provided for backwards compatibility. We recommend that you configure access to Web URLs and servers through resource profiles instead, since they provide a simpler, more unified configuration method.

Use the Bookmarks tab to create bookmarks that appear on the welcome page for users mapped to this role. You can create two types of bookmarks through this page:

- **Web URL bookmarks**—These bookmarks link the user to Web URLs on the World Wide Web or on your corporate Intranet. When you create Web bookmarks, you can insert the user's Secure Access Service username in the URL path to provide single sign-on

access to back-end Web applications. For Web bookmark configuration instructions, see the instructions that follow.

- Java applet bookmarks—These bookmarks link the user to a Java applets that you upload to the Secure Access Service through the Users > Resource Profiles > Web > Hosted Java Applets page of the admin console.

When you create either of these bookmark types, the corresponding links appear on the welcome page for users mapped to this role.

To create a bookmark to a Web resource:

1. In the admin console, choose **Users > User Roles > Role > Web > Bookmarks**.
2. Click **New Bookmark**.
3. Select **Standard**.
4. Enter a name and description for the bookmark (optional). This information displays on the Secure Access Service home page instead of the URL.
5. Enter the URL to bookmark. If you want to insert the user's username, enter <username> at the appropriate place in the URL.

Make sure to enter a unique URL in this field. If you create two bookmarks with the same URL, the Secure Access Service deletes one of the bookmarks from the end-user view. You will still be able to see both bookmarks, however, in the administrator console.

6. Under Auto-allow, click **Auto-allow Bookmark** to enable the Secure Access Service to automatically create a corresponding Web access resource policy. Note that this functionality applies only to role bookmarks and not bookmarks created by users. Next, select:

- **Only this URL** to allow users to access only the URL.
- **Everything under this URL** to allow the user to access any path under the URL.

You may not see the Auto-allow option if you are using a new installation or if an administrator hides the option.

7. Under Display options, click **Open bookmark in a new window**

to enable the Secure Access Service to automatically open the Web resource in a new browser window. Note that this functionality applies only to role bookmarks and not bookmarks created by users. Next, select:

- **Do not display the URL address bar** if you want to remove the address bar from the browser window. This feature forces all Web traffic through the Secure Access Service by precluding users in the specified role from typing a new URL in the address bar, which circumvents the Secure Access Service.
- **Do not display the menu and the toolbar** to remove the menu and toolbar from the browser. This feature removes all menus, browsing buttons, and bookmarks

from the browser window so that the user browses only through the Secure Access Service.

8. Click **Save Changes** or **Save + New** to add another.

- Related Documentation**
- [Defining Resource Profile Bookmarks on page 134](#)
  - [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)

## Specifying Web Browsing Options

The Secure Access Service enables you to configure a wide-variety of Web browsing options for a user role.

### Configuring Basic Web Browsing Options

To configure basic Web browsing options for a role:

1. In the admin console, choose **Users > User Roles > RoleName > Web > Options**.
2. Select **User can type URLs in the Secure Access Service browse bar** if you want to enable users to enter URLs on the welcome page and browse to Internet sites.
3. Select **User can add bookmarks** if you want to enable users to create personal Web bookmarks on the Secure Access Service welcome page.
4. Select **Mask hostnames while browsing** if you want the Secure Access Service to obscure the target resources in the URLs to which users browse. When you select this option, the Secure Access Service masks IP addresses and host names in the user's:
  - Web browser address bar (when the user navigates to a page)
  - Web browser status bar (when a user hovers over a hyperlink)
  - HTML source files (when the user chooses to View Source)

The host name encoding feature (also called host name obfuscation or URL obfuscation) prevents casual observers from noting the URL of an internal resource by obscuring the target server within the URL without masking the full path name, target file, or port number. For example, if a user navigates to `www.msn.com` without selective rewriting or host name encoding enabled, the Secure Access Service displays an un-obscured URL in his Web browser's address bar:

```
http://www.msn.com/
```

If you then enable selective rewriting, the Secure Access Service might display the following URL:

```
https://mycompanyserver.com/,DanaInfo=www.msn.com,SSO=U+
```

If you then enable host name encoding, and the same user navigates to the same site, he sees a URL in which the host name (`www.msn.com`) is obscured:

```
https://i5.asglab.juniper.net/,DanaInfo=.awxyCqxtGkxw,SSO=U+
```

Host name encoding uses a lightweight reversible algorithm so that users can bookmark encoded URLs. (The Secure Access Service can translate the encoded URL and resolve it back to the original URL.) For compatibility, previously created bookmarks to unmasked URLs continue to work when host name encoding is enabled.

Note the following:

- If you enable selective rewriting and host name encoding, the Secure Access Service only obscures the host names and IP addresses of those servers that you have chosen to rewrite using the selective rewrite feature.
- Links not rewritten by the Secure Access Service are not obscured. For example, the rewriter does not intermediate ftp, rtsp, mms and mailto links and therefore the host names in these links are not masked. This is required to pass security audits.
- If you enable the framed toolbar and host name encoding, the Secure Access Service does not obscure host names that the user enters in the framed toolbar's browse field.
- The Secure Access Service does not obscure host names and IP addresses in log entries, including host name encoding log entries.

5. Click **Save Changes**.

### Configuring Advanced Web Browsing Options

To configure advanced Web browsing options for a role:

1. In the admin console, choose **Users > User Roles > RoleName > Web > Options**.
2. Select the **View advanced options** checkbox.
3. Select **Allow Java applets** if you want to enable users to browse to Web pages containing client-side Java applets. The Secure Access Service server appears to the application server as a browser over SSL. The Secure Access Service transparently handles any HTTP requests and TCP connections initiated by a Java applet and handles signed Java applets.

If you enable this feature, users can launch Java applets and run applications that are implemented as client-side Java applets, such as the Virtual Computing (VNC) Java client, Citrix NFuse Java client, WRQ Reflections Web client, and Lotus WebMail.

4. Select **Allow Flash content** to enable the Secure Access Service to intermediate Flash content through its Content Intermediation Engine. Note that Secure Access Service provides limited support for ActionScript 2.0 and Flash Remoting, and does not support XMLSocket connections.

The Content Intermediation Engine supports Flash versions 5, 6, 7 and 8, including dynamic rewriting of internal Web links during an access request. We support the rewriting of Actionscript in Flash. The calls in Actionscript that are supported are: load, send, sendAndLoad, loadVariables, loadMovie, loadVariablesNum, loadMovieNum, loadClip, loadSound, apply, connect on classes of XML, Sound, MovieClip, NetConnection, and MovieClipLoader. The eval equivalent of Actionscript is not supported. Therefore we recommend that the above function calls not be embedded in an Actionscript string object. Note, however, that Secure Access does not support



Flash applications that use the XMLSocket object or Flash remoting. For more information, see the *Content Intermediation Engine Best Practices Guide*.

5. Select **Persistent cookies** to enable users to customize their browsing experiences by enabling them to keep persistent cookies. By default, the Secure Access Service flushes Web cookies that are stored during a user session. A user can delete cookies through the Advanced Preferences page if you enable this option.
6. Select **Unrewritten pages open in new window** to configure the Secure Access Service to open content in a new browser window when a user access a un-rewritten Web page. Opening content in a new windows can help remind users that they still have a secure session. When a user request is made to a resource to which this option applies, the Secure Access Service displays a page that contains a link to the requested resource and directs the users to click on the link. This link opens the resource in a new browser window and the page from which the request originates continues to display in the Secure Access Service.

If you un-check this box, users might not realize that their Secure Access Service session is still active and that to return to the Secure Access Service, they need to use the browser's Back button. Users must return to the Secure Access Service to sign out. If they simply close the browser window, their sessions remain active until the session time limit expires.

7. Select **Allow browsing untrusted SSL Web servers** to enable users to access untrusted Web sites through the Secure Access Service. Untrusted Web sites are those whose server certificates are not installed through the System > Configuration > Certificates > Trusted Servers CAs tab of the admin console.



**NOTE:** If a web page has internal references to files within a SCRIPT tag and these files are hosted on different HTTPS servers that have SSL certificates not trusted by the Secure Access Service, the web page does not render correctly. In these cases, the Warn users about the certificate problems option must be disabled.

If you enable this option, you can specify what choices the Secure Access Service gives users when they navigate to an untrusted Web site:

- **Warn users about the certificate problems**—If enabled, the Secure Access Service displays a warning to the user when he first accesses an untrusted Web site telling him why the site's certificate is untrusted and allowing him to either continue or cancel. If the user chooses to continue after the Secure Access Service displays a warning, the Secure Access Service does not display any more warnings for that site during the current Secure Access Service session.

If you select the Warn users about the certificate problems option and the user accesses non-HTML content (such as images, js, and css) served from a different SSL server than the HTML page, the page containing the links may not display correctly. You can avoid this problem either by deselecting this option or by uploading a valid production SSL certificate on the servers that serve the non-HTML content.

- **Allow users to bypass warnings on a server-by-server basis**—If enabled, the Secure Access Service allows the user to suppress all further warnings for an untrusted Web site. If a user chooses this option, he never sees a warning for this site again, provided that he accesses it from the current Secure Access Service or cluster.

If you choose to allow users to access untrusted Web sites without seeing a warning, the Secure Access Service still logs a message to the user access log whenever a user navigates to an untrusted site. Also note that if a user chooses to suppress warnings, he can clear the persistent settings of the untrusted Web sites using the Delete Passwords option in the System > Preferences > Advanced tab in the end user console.

8. Select **Rewrite file:// URLs** to configure the Secure Access Service to rewrite file:// URLs so that they are routed through the Secure Access Service's file browsing CGI.
9. Select **Rewrite links in PDF files** to configure the Secure Access Service to rewrite hyperlinks in PDFs.
10. Under HTTP Connection Timeout, accept the default value or set the duration to tell the Secure Access Service how long to wait for a response from an HTTP server before timing out and closing the connection. Use values from 30 to 1800 seconds.

Higher timeout values might exhaust Secure Access Service resources if applications do not close connections properly or take too long to close the connections. Unless an application requires a higher timeout value, we recommend accepting the default value.

11. Under WebSocket Connection Timeout, accept the default value or set the duration to tell the Secure Access Service how long to wait for data transfer between the client and server. Use values from 30 to 1800 seconds.

WebSocket is a web technology that provides bi-directional, full-duplex communication channels over a single TCP connection. This provides a mechanism for browser-based applications that need two-way communication with servers that do not rely on opening multiple HTTP connections. Communication is done over the regular TCP port numbers 80 or 443.

Currently, only the following web resource policies support WebSocket:

- Web ACL Access
- Passthrough Proxy
- Options

The WebSocket URL that starts with **ws://** or **wss://** is not allowed in any of the web resource profile pages, web resource policies or web bookmark pages.

The following Web options under Roles accept WebSocket requests:

- Mask hostnames while browsing
- Persistent cookies
- Allow browsing untrusted SSL websites

12. Click **Save Changes**.

- Related Documentation**
- [Web Rewriting on page 490](#)
  - [Defining Resource Profile Bookmarks on page 134](#)
  - [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)
  - [Creating a Hosted Java Applet Resource Profile on page 457](#)

## Resource Policy Overview

---

When you enable the Web access feature for a role, you need to create resource policies that specify which resources a user can access, whether or not the Secure Access Service needs to rewrite the content requested by the user, and caching, applet, or single sign-on requirements. For every Web request, the Secure Access Service first evaluates the rewriting policies you configure. If the user's request is to a resource specified as "don't rewrite" due to either a selective rewriting or passthrough proxy resource policy, then the Secure Access Service forwards the user's request to the appropriate back-end resource. Otherwise, the Secure Access Service continues to evaluate those resource policies corresponding to the request, such as Java resource policies for a request to fetch a Java applet. After matching a user's request to a resource listed in a relevant policy, the Secure Access Service performs the action specified for the resource.

You can create resource policies through the standard interface (as described in this section) or through resource profiles (recommended method).

When writing a Web resource policy, you need to supply key information:

- **Resources**—A resource policy must specify one or more resources to which the policy applies. When writing a Web policy, you need to specify Web servers or specific URLs, as explained in the section that follows.
- **Roles**—A resource policy must specify the roles to which it applies. When a user makes a request, the Secure Access Service determines what policies apply to the role and then evaluates those policies that correspond to the request.
- **Actions**—Each type of resource policy performs a certain action, which is either to allow or deny a resource or to perform or not perform some function, such as rewrite content, re-sign an applet, or post Web data. You can also write detailed rules that apply more conditions to a user request.

The Secure Access Service platform's engine that evaluates resource policies requires that the resources listed in a policy's Resources list follow a canonical format.

### Canonical Format

This section outlines special considerations you must consider when specifying a Web resource using the canonical format.

[protocol://]host[:ports][/path]

The four components are:

- Protocol (optional)—Possible values: http and https (case-insensitive)  
If the protocol is missing, then both http and https are assumed. If a protocol is specified, then the delimiter “://” is required. No special characters are allowed.
- Host (required)—Possible values:
  - DNS Hostname—For example: www.juniper.com
 Special characters allowed are described in the following table.

*	Matches ALL characters
%	Matches any character except dot (.)
?	Matches exactly one character

- IP address/Netmask—The IP address needs to be in the format: a.b.c.d  
The netmask can be in one of two formats:
  - Prefix: High order bits
  - IP: a.b.c.d
 For example: 10.11.149.2/24 or 10.11.149.2/255.255.255.0  
No special characters are allowed.
- Ports—You must specify a port when specifying IP/netmask as a resource. The port is optional when specifying a DNS host name. If a port is specified, then the delimiter “:” is required. For example: 10.11.149.2/255.255.255.0:\*

**Table 41: Port Possible Values**

*	Matches ALL ports; no other special characters are allowed
port[,port]*	A comma-delimited list of single ports. Valid port numbers are [1-65535].
[port1]-[port2]	A range of ports, from port1 to port2, inclusive.



**NOTE:** You can mix port lists and port ranges, such as: 80,443,8080-8090

- If the port is missing, then the default port 80 is assigned for http, 443 for https.
- Path (optional)—If the path is missing, then star (\*) is assumed, meaning ALL paths match. If a path is specified, then the delimiter “/” is required. No other special characters are supported. For example:
    - http://www.juniper.com:80/\*
    - https://www.juniper.com:443/intranet/\*

- `*yahoo.com:80,443/*`
- `%danastreet.net:80/share/users/<username>/*`

## Writing a Web Access Resource Policy

---

Web access resource policies control which Web resources users can access in order to connect to the Internet, intranet, or extranet. You can deny or allow access to Web resources by URL or IP range. For URLs, you can use the “\*” and “?” wildcards to efficiently specify multiple host names and paths. For resources that you specify by host name, you can also choose either HTTP, HTTPS, or both protocols.

To write a Web Access resource policy:

1. In the admin console, choose **Users > Resource Policies > Web > Web ACL**.
2. On the Web Access Policies page, click **New Policy**.
3. On the New Policy page, enter a name to label this policy and optionally a description.
4. In the Resources section, specify the resources to which this policy applies.
5. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below** —To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. In the Action section, specify:
  - **Allow access**—To grant access to the resources specified in the Resources list.
  - **Deny access**—To deny access to the resources specified in the Resources list.
  - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
7. Click **Save Changes**.
8. On the Web Access Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy’s (or a detailed rule’s) Resource list, it performs the specified action and stops processing policies.

### Related Documentation

- [Defining a Resource Profile on page 6](#)
- [Creating Detailed Rules for Resource Policies on page 149](#)

## Defining Single Sign-On Policies

---

Single sign-on policies enable you to automatically pass user credentials to the Web application specified in your policy. You can configure single sign-on policies to intercept basic authentication, Kerberos and NTLM challenges and display an intermediate sign-in page to collect credentials for the Web resource. Or, you can post the credentials and headers that you specify to the Web application.

### Related Documentation

- [About Basic, NTLM and Kerberos Resources on page 522](#)
- [Writing the Basic, NTLM and Kerberos Resources on page 523](#)
- [Writing a Basic Authentication, NTLM or Kerberos Intermediation Resource Policy on page 527](#)
- [Writing a Remote SSO Form POST Resource Policy on page 529](#)
- [Writing a Remote SSO Headers/Cookies Resource Policy on page 531](#)

## About Basic, NTLM and Kerberos Resources

---

Use the SSO > General tab to set up the basic, NTLM and Kerberos credentials. The credentials you define here are used when defining Web resource profiles with SSO autopolicies and Web resource policies.

The following outlines the basic ideas behind the handling of SSO:

- The Secure Access Service will do Kerberos if challenged with Negotiate header, NTLM if challenged with NTLM header and Basic Auth if challenged with Basic.
- If the Secure Access Service receives multiple challenges, the order of preference is:
  - Kerberos
  - NTLM
  - Basic
- The Secure Access Service will first try constrained delegation if the service is configured in a service list.
- Policy configurations override any settings in the SSO > General tab.
- Disabling SSO or disabling all sections in the General tab prevents single sign-on. However, the Secure Access Service will continue to intermediate and display an intermediation page to the end-user.
- Basic authentication intermediation can be explicitly turned off in a policy. For kerberos and NTLM, the Secure Access Service will always intermediate.
- Depending on the SSO used, the intermediation page will show different fields for the end-user to complete:
  - Basic authentication intermediation page displays username and password fields
  - NTLM intermediation page displays username, password and domain fields

- Kerberos intermediation page displays username, password and realm fields
- For constrained delegation, you must defined a policy and specify roles. Entering data in the General tab only is not sufficient.
- If no policies are configured for single sign-on, the Secure Access Service uses the default system credentials.
- If credentials are defined, the order of preference is:
  - System credentials
  - Variable credentials
  - Fixed or static credentials
- For fixed or static credentials, you must defined a policy and specify roles. Entering data in the General tab only is not sufficient.
- If there is a policy match, the credential and protocol of the policy is used. If the policy fails to authenticate, the fallback mechanism defined in the policy is used. If the policy protocol does not match the protocol of the challenge, the logic defined in the General tab is used.
- When upgrading a Secure Access Service or performing a new install, the default SSO policy of BasicAuthNoSSO is preserved. Even if all sections of the General tab are enabled, SSO will not be enabled until the BasicAuthNoSSO policy is deleted.

**Related  
Documentation**

- [Writing the Basic, NTLM and Kerberos Resources on page 523](#)
- [Defining Single Sign-On Policies on page 522](#)

## Writing the Basic, NTLM and Kerberos Resources

---

To set up the basic, NTLM and Kerberos resources:

1. In the admin console, select **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show SSO policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **SSO** checkbox.
  - c. Select the **General** checkbox below the SSO checkbox.
  - d. Click **OK**.
3. Select the **SSO > General** tab.
4. Select **Enable kerberos** to enable Kerberos SSO. You can then define the type of intermediation: constrained delegation or Secure Access Service. If you do not define any intermediation types, the Secure Access Service attempts to figure out the realm from the hostname and performs SSO using the system credentials.

For realm intermediation, enter the following and click **Add**:

- **Realm**—Enter the Kerberos realm name. For example, KERBER.NET. The Secure Access Service will use KERBER.NET to obtain the list of Key Distribution Centers (KDCs).
- **Site Name**—(optional) Enter the Active Directory site names. Use this field to have the Secure Access Service contact the KDC at a specific site. For example, if site name is Sunnyvale and realm is KERBER.NET, then the Secure Access Service uses Sunnyvale.KERBER.NET to get a list of KDCs. Note that the Active Directory must have the sites defined and DNS should be configured to return the KDCs in the site.
- **Pattern List**—Enter the hostnames mapped to the Kerberos realm. You can enter wildcard characters, such as \*.y.com, \*.kerber.net, or \*. Note the following:
  - Make sure that realms to not have hostnames matching a subset of the patterns defined for another realm.
  - You do not need to define a pattern if all servers follow the mirrored DNS namespace convention. The Secure Access Service will determine the realm from the hostname.
  - All disjointed hostname patterns must be defined.
  - You can use \* as the default realm. Do not list more than one \* when defining multiple realms.
- **KDC**—Enter the hostname or IP address of the Key Distribution Centers if DNS is unavailable or if you want the Secure Access Service to contact a specific KDC for tickets. If you enter a KDC, the Secure Access Service will not use DNS to obtain the list of KDCs based on the values entered in the Site Name and Realm fields.

For constrained delegation intermediation, enter the following and click **Add**:

- **Label**—Enter a name to uniquely identify this row. No external mapping is made to the label value.
- **Realm**—Select the realm to use. The drop-down list is populated by values in the Realm Definition table.
- **Principal Account**—Enter the constrained delegation account the Secure Access Service uses to get constrained delegation tickets on behalf of the user.
- **Password**—Enter the constrained delegation account password.
- **Service List**—Select the service list to use. Click Edit to define and upload service lists. The list should be an exact match with the service list in Active Directory if you want the Secure Access Service to perform constrained delegation for all the services. Hostnames must be an exact match.

For more information about constrained delegation, see <http://msdn.microsoft.com/en-us/library/aa480585.aspx>.

For Secure Access Service intermediation, enter the following and click **Add**:



- **Label**—Enter a name to uniquely identify this row. No external mapping is made to the label value.
  - **Realm**—Select the realm to use. The drop-down list is populated by values in the Realm Definition table.
  - **Credential Type**—Select one of the following credential types:
    - **System credentials**—Use the set of user credentials, such as primary and secondary authorization credentials, stored on the Secure Access Service. If you select this option, you do not need to enter values in the Username and Password fields.
    - **Variable**—Allow tokens such as <username> and <password> to be used in the username and Variable Password fields.
    - **Static**—Use the username and password exactly as they are entered in the username and password fields.
  - **Username and Password**—Enter the account username and password. If you select Variable as the credential type, you can enter the username token here. For example, <username>.
  - **Variable Password**—If you select Variable as the credential type, enter the password token here. For example, <password>.
  - **Fallback to NTLM V2**—Select this option to fallback to NTLM V2 if Kerberos fails. If you do not select this option and Kerberos SSO fails, an intermediation page appears.
5. Select **Enable NTLM** to enable NTLM SSO. If you do not enter any configuration information, the Secure Access Service attempts to figure out the domain from the hostname and performs SSO using the system credentials.



**NOTE:** Do not edit or delete the default system credential.

- **Label**—Enter a name to uniquely identify this row. No external mapping is made to the label value.
- **Domain**—Enter the Active Directory domain name here.
- **Credential Type**—Select one of the following credential types:
  - **System credentials**—Use the set of user credentials, such as primary and secondary authorization credentials, stored on the Secure Access Service. If you select this option, you do not need to enter values in the Username and Password fields.
  - **Variable**—Allow tokens such as <username> and <password> to be used in the Username and Variable Password fields.
  - **Static**—Use the username and password exactly as they are entered in the username and password fields.
- **Username and Password**—Enter the account username and password. If you select Variable as the credential type, you can enter the username token here. For example, <username>.

- **Variable Password**—If you select Variable as the credential type, enter the password token here. For example, <password>.
  - **Fallback to NTLM V1**—Select this option to fallback to NTLM V1 if SSO fails. If you do not select this option and SSO fails, only NTLM V2 is attempted. An intermediation page appears if NTLM V2 fails.
6. Select **Enable Basic Authentication** to enable basic authentication SSO. If you select this option but do not set up any configuration data, the Secure Access Service will attempt SSO using system credentials.



**NOTE:** Do not edit or delete the default system credential.

- **Label**—Enter a name to uniquely identify this row. No external mapping is made to the label value.
- **Credential Type**—Select one of the following credential types:
  - **System credentials**—Use the set of user credentials, such as primary and secondary authorization credentials, stored on the Secure Access Service. If you select this option, you do not need to enter values in the Username and Password fields.
  - **Variable**—Allow tokens such as <username> and <password> to be used in the Username and Variable Password fields.
  - **Static**—Use the username and password exactly as they are entered in the username and password fields.
- **Username and Password**—Enter the account username and password. If you select Variable as the credential type, you can enter the username token here. For example, <username>.
- **Variable Password**—If you select Variable as the credential type, enter the password token here. For example, <password>.
- **Pattern List**—Enter the hostnames mapped to the Kerberos realm. You can enter wildcard characters, such as \*.y.com, \*.kerber.net, or \*.\*. Note the following:
  - Make sure that realms do not have hostnames matching a subset of the patterns defined for another realm.
  - You do not need to define a pattern if all servers follow the mirrored DNS namespace convention. The Secure Access Service will determine the realm from the hostname.
  - All disjointed hostname patterns must be defined.
  - You can use \* as the default realm. Do not list more than one \* when defining multiple realms.
  - You can use \* as the default domain. Do not list more than one \* when defining multiple domains.

- Related Documentation**
- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)
  - [About Single Sign-On on page 335](#)

## Writing a Basic Authentication, NTLM or Kerberos Intermediation Resource Policy

Basic Authentication, NTLM or Kerberos Intermediation resource policies enable you to control NTLM and Kerberos intermediation on the Secure Access Service. If a user accesses a Web resource that sends a basic authentication challenge, the Secure Access Service can intercept the challenge, display an intermediate sign-in page to collect credentials for the Web resource, and then rewrite the credentials along with the entire challenge/response sequence.

The initial HTTP request generated for an NTLM protected server should be for a request that results in HTML content. If SSO is not enabled or if the SSO credentials fail, the Secure Access Service responds with an HTML page to gather user credentials. If the browser is expecting non-HTML content, the browser rejects the response and the navigation to the resource fails.

With the Kerberos Intermediation resource policy, backend web applications protected by Kerberos are accessible to end users. For example, a user logs in to the Secure Access Service using Active Directory as the authentication server and the authentication protocol is Kerberos. When the user browses to a Kerberos-protected server, the user is single-signed on to the backend server and is not prompted for credentials. Or, if a user logs in to the Secure Access Service using an authentication protocol other than Kerberos and then browses to a Kerberos-protected server. Depending on the settings in Kerberos Intermediation resource policy and the configured Kerberos authentication server, the user will either be authenticated by the rewriter or the user will be prompted to enter a username and password.

To write a Basic Authentication, NTLM or Kerberos Intermediation resource policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show SSO policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **SSO** checkbox.
  - c. Select the **Kerberos/Basic Auth/NTLM** checkbox below the SSO checkbox.
  - d. Click **OK**.
3. Select the **SSO > Kerberos/NTLM/BasicAuth** tab.
4. Click **New Policy**.
5. Enter a name to label this policy (required) and a description of the policy (optional).
6. In the Resources section, specify the resources to which this policy applies.

If you want the Secure Access Service to automatically post values to a specific URL when an end-user clicks on a bookmark, the resource that you enter here must exactly match the URL that you specify in the Users > User Roles > Role > Web > Bookmarks page of the admin console.

7. In the Roles section, specify:

- **Policy applies to ALL roles**—To apply this policy to all users.
- **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
- **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.

8. In the Action section, specify:

- **Disable SSO**—The Secure Access Service disables automatic SSO authentication for this user role and, instead, prompts the user for sign-in credentials.
- **Basic**—This option specifies that the Secure Access Service use the Basic Authentication Intermediation method to control SSO behavior.
  - **Enable Intermediation**—Select the credentials to use. If this pull-down menu is blank, no basic authentication SSO settings are defined in the SSO General tab.
  - **Disable Intermediation**—When you select this option, The Secure Access Service does not intermediate the challenge/response sequence.

The Secure Access Service always intermediates requests to Web proxies that require basic authentication, even if you select Disable Intermediation.

Although you are given an option to disable basic authentication intermediation, we do not recommend this option, as it is a very insecure authentication method and, in some cases, can transmit user credentials over the network in clear (unencrypted) text.

- **NTLM**—This option specifies that the Secure Access Service use the Microsoft NTLM Intermediation method to control SSO behavior.
  - Select the credentials to use. If this pull-down menu is blank, no NTLM SSO settings are defined in the SSO General tab.
  - Select the **Fallback to NTLM V1** option to try both NTLM V1 and NTLM V2. If you do not select this option, the Secure Access Service falls back only to NTLM V2. An intermediation page appear if SSO fails.
- **Kerberos**—This option specifies that the Secure Access Service use the Kerberos Intermediation method to control SSO behavior.
  - Select the credentials to use. If this pull-down menu is blank, no kerberos SSO settings are defined in the SSO General tab

- Select the **Fallback to NTLM V2** option to fallback only to NTLM V2 if Kerberos fails. If you do not select this option, a Kerberos intermediation page appears if Kerberos SSO fails.
  - **Constrained Delegation**—This option specifies that the Secure Access Service use the constrained delegation intermediation method to control SSO behavior.
    - Select the credentials to use. If this pull-down menu is blank, no constrained delegation SSO settings are defined in the SSO General tab.
    - Select the **Fallback to Kerberos** option to fallback to Kerberos if constrained delegation fails. If you select this option, an intermediation page appears if constrained delegation fails. If you do not select this option and constrained delegation fails, an error page appears.
  - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. Click **Save Changes**.
  10. On the Basic Auth, NTLM and Kerberos policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

Check the activity events listed in the user log if you encounter any problems.

**Related  
Documentation**

- [Specifying Resources for a Resource Policy on page 145](#)
- [Resource Policy Components on page 144](#)
- [Writing the Basic, NTLM and Kerberos Resources on page 523](#)

## Writing a Remote SSO Form POST Resource Policy

Remote SSO Form POST resource policies specify Web applications to which the Secure Access Service posts data. This data can include a user's Secure Access Service username and password, as well as system data stored by system variables.

To write a remote SSO Form POST resource policy:

1. In the admin console, navigate to **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show SSO policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **SSO** checkbox.
  - c. Select the **Form Post** checkbox below the SSO checkbox.
  - d. Click **OK**.
3. Select the **SSO > Form Post** tab.

4. On the Form POST Policies page, click **New Policy**.
5. Enter a name to label this policy (required) and a description of the policy (optional).
6. In the Resources section, specify the application's sign-in page, such as:  
`http://yourcompany.com`.

If you want the Secure Access Service to automatically post values to a specific URL when an end-user clicks on a bookmark, the resource that you enter here must exactly match the URL that you specify in the Users > User Roles > Role > Web > Bookmarks page of the admin console.

7. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
  - **Perform the POST defined below**—The Secure Access Service performs a form POST with the user data specified in the POST details section to the specified URL when a user makes a request to a resource specified in the Resources list.
  - **Do NOT perform the POST defined below**—The Secure Access Service does not perform a form POST with the user data specified in the POST details section.
  - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. In the POST details section:
  - In the POST to URL field, specify the absolute URL where the application posts the user's credentials, such as: `http://yourcompany.com/login.cgi`. You can determine the appropriate URL using a TCP dump or by viewing the application's sign-in page source and searching for the POST parameter in the FORM tag. (The Secure Access Service does not accept wildcard characters in this field.)
  - Check **Deny direct login** for this resource if you do not want users to be able to access the URL directly.
  - Select the **Allow multiple POSTs to this resource** checkbox if you want the Secure Access Service to send POST and cookie values to the resource multiple times if required. If you do not select this option, the Secure Access Service does not attempt single sign-on when a user requests the same resource more than once during the same session.
  - Specify the user data to post and user modification permission:

- **User label**—The label that appears on a user’s Preferences page in the Secure Access Service. This field is required if you either enable or require users to modify data to post to back-end applications.
  - **Name**—The name to identify the data of the Value field. (The back-end application should expect this name.)
  - **Value**—The value to post to the form for the specified Name. You can enter static data, a system variable, or Secure Access Service session variables containing username and password values.
  - **User modifiable?** setting—Set to Not modifiable if you do not want the user to be able to change the information in the Value field. Set to User CAN change value if you want the user to have the option of specifying data for a back-end application. Set to User MUST change value if users must enter additional data in order to access a back-end application. If you choose either of the latter settings, a field for data entry appears on the user’s Advanced Preferences page in the Secure Access Service. This field is labeled using the data you enter in the User label field. If you enter a value in the Value field, this data appears in the field but is editable.
10. Click **Save Changes**.
  11. On the Form POST Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy’s (or a detailed rule’s) Resource list, it performs the specified action and stops processing policies.

**Related  
Documentation**

- [Remote SSO Overview on page 494](#)
- [Specifying Resources for a Resource Policy on page 145](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)
- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)
- [Multiple Sign-In Credentials Execution on page 339](#)

## Writing a Remote SSO Headers/Cookies Resource Policy

---

Remote SSO Headers/Cookies resource policies specify customized Web applications to which the Secure Access Service posts custom headers and cookies.

When creating a Headers/Cookies policy, note that the Secure Access Service does not parse or “understand” the headers that you enter in this section. For instance, if you add an Accept-Encoding: gzip or Accept-Encoding:deflate header, it does not mean that the Secure Access Service can handle gzip content or deflated content.

To write a remote SSO Headers/Cookies resource policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show SSO policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **SSO** checkbox.
  - c. Select the **Headers/Cookies** checkbox below the SSO checkbox.
  - d. Click **OK**.
3. Select the **SSO > Headers/Cookies** tab.
4. On the Headers/Cookies Policies page, click **New Policy**.
5. Enter a name to label this policy (required) and a description of the policy (optional).
6. In the Resources section, specify the resources to which this policy applies.
7. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
  - **Append headers as defined below**—The Secure Access Service posts the user data specified in the POST details section to the specified URL when a user makes a request to a resource specified in the Resources list.
  - **Do NOT append headers as defined below**—The Secure Access Service does not post the user data specified in the POST details section to the specified URL when a user makes a request to a resource specified in the Resources list.
  - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. In the Headers and values section, specify the:
  - **Header name**—The text for the Secure Access Service to send as header data.
  - **Value**—The value for the specified header.



**NOTE:** If you need to forward a cookie to a backend server, you must set the Header Name field to "Cookie" and the Value field to "CookieName=CookieValue".

---



10. Click **Save Changes**.
11. On the Headers/Cookies Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

**Related  
Documentation**

- [Remote SSO Overview on page 494](#)
- [Specifying Resources for a Resource Policy on page 145](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)
- [Resource Policies on page 143](#)

## Writing a Web Caching Resource Policy

---

To write a Web Caching resource policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show caching policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Caching** checkbox.
  - c. Select the **Policies** checkbox below the Caching checkbox.
  - d. Click **OK**.
3. Select the **Caching > Policies** tab.
4. On the Web Caching Policies page, click **New Policy**.
5. Enter a name to label this policy (required) and a description of the policy (optional).
6. In the Resources section, specify the resources to which this policy applies.
7. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, select one of the following options:
  - **Smart Caching (send headers appropriate for content and browser)** —Select this option to allow the Secure Access Service to send a cache-control:no-store header

or a cache-control:no-cache header based on the user's Web browser and content type.

When you select this option, the Secure Access Service makes media files and zip files work properly by removing their origin server's cache-control headers. For example, the following logic searches for "msie" or "windows-media-player" in user-agent headers in order to remove cache or cache-control:no-store response headers and make the files cacheable:

```
(if content type has "audio/x-pn-realaudio" OR
 if content type begins with "video/" OR
 if content type begins with "audio/" OR
 if content type is "application/octet-stream" and the file extension begins
 with "rm" or "ram"
)
```

If the Secure Access Service finds "msie" or "windows-media-player" in the user-agent header and any of the following apply:

- Request is for Flash, .xls, .pps, .ppt files
- Content-type is application/, text/rtf, text/xml, model/
- Origin server sends a content-disposition header

then Secure Access Service sends the cache-control:no-store header and removes the origin server's cache-control header.

In all other cases, the Secure Access Service adds the pragma:no-cache or cache-control:no-store response headers.

Citrix .ica and QuickPlace files get some special treatment. Citrix .ica files are always cacheable and get cache-control:private as well. QuickPlace files that do not match a specified rule files (which takes precedence) get CCNS and cache-control:private.

Also note that if you select this option, enable GZIP compression, and try to access a text file attachment using Domino Web Access 6.5 through Internet Explorer, you cannot open the attachment. To enable text attachments, you must either install the Internet Explorer 323308 patch or enable the Don't Cache (send "Cache Control: No Store") option.

- **Don't Cache (send "Cache Control: No Store")**—Select this option to deliver attachments to Internet Explorer without saving them to the disk. (The browser temporarily writes files to the disk, but immediately removes them once it has opened the file in the browser.) When you select this option, the Secure Access Service removes the origin server's cache-control header and adds a cache-control:no-store response header if the user-agent string sent by the browser contains "msie" or "windows-media-player."

This option might slow browsing by causing repeated content fetches, which can cause performance issues on very slow connections. Alternatively, you can specify a policy that allows certain kinds of content to be cached, such as images that do not exceed a specified size limit.

- **Don't Cache (send "Pragma: No Cache")**—Select this option to prevent the user's browser from caching files to the disk. When you select this option, the Secure

Access Service adds the standard HTTP pragma:no-cache header and cache-control:no-cache (CCNC) header (HTTP 1.1) to response files. Also, the Secure Access Service does not forward the origin server's caching headers, such as age, date, etag, last-modified, expires.

When no-cache headers are present on certain types of attachments (PDF, PPT, streaming files), Internet Explorer does not properly render the documents because the rendering process requires the browser to temporarily writes these files to cache.

- **Unchanged (do not add/modify caching headers)**—The Secure Access Service does not add the pragma:no-cache or cache-control:no-store response headers and forwards the origin server's caching headers.
- **Remove Cache-Control: No-Cache|No-Store**—Select this option to help “cache” files sent by web applications in an HTTPS environment. This option removes the Cache Control:No Cache and Pragma:no-cache headers. Removing these headers is necessary to allow the successful download of certain file types. These headers work fine in an HTTP environment, but fail in an HTTPS environment where the associated pages become uncachable, preventing the user’s web browser from downloading the pages.

Use this option when you want the end-user to have the ability to download and open a file that will be opened by another third party application. For example, zip files and wav files are stored on disk and opened by another application.

- **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. Click **Save Changes**.
  10. On the Web Caching Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy’s (or a detailed rule’s) Resource list, it performs the specified action and stops processing policies.

- Related Documentation**
- [Writing a Detailed Rule for Resource Policies on page 150](#)
  - [Defining Resource Policies: General Options on page 558](#)

## About OWA and Lotus Notes Caching Resource Policies

The following tables include examples of some of the content types that the Secure Access Service supports with the Outlook Web Access (OWA) and Lotus iNotes applications. Additionally, it specifies the cache control directives that you must implement in Microsoft Internet Explorer in order to support opening and saving the specified content types.

Note that for performance reasons, we recommend creating caching policies for everything in the iNotes directory.

**Table 42: OWA Caching Resource Policies**

Attachment type	To open the attachment, use:	To save the attachment, use:
-----------------	------------------------------	------------------------------

Table 42: OWA Caching Resource Policies (*continued*)

zip	Cache	Smart caching
ppt	Smart caching	Smart caching
doc	Smart caching	Smart caching
xls	Smart caching	Smart caching
pdf	Smart caching	Smart caching
txt	Cache	Cache control: No store
html	Smart caching	Cache control: No store

Table 43: iNotes Caching Resource Policies

Attachment type	To open the attachment, use:	To save the attachment, use:
zip	Cache control: No store	Cache control: No store
ppt	Cache control: No store	Cache control: No store
doc	Smart caching	Smart caching
xls	Cache control: No store	Cache control: No store
pdf	Cache control: No store	Cache control: No store
txt	Cache control: No store	Cache control: No store
html	Cache control: No store	Cache control: No store
other file types	Cache control: No store	Cache control: No store

- Related Documentation**
- [Standard Application Support: MS Outlook on page 610](#)
  - [Standard Application Support: Lotus Notes on page 612](#)

## Specifying General Caching Options

You can use caching options to specify the maximum image file size that is cached on a client. If the content-type header from the origin server begins with "image/" and the content-length header specifies a size less than the maximum size configured for this option, then the Secure Access Service passes along the origin server's caching headers. Otherwise, the Secure Access Service treats the request as though caching is disabled.

To specify caching options:

1. In the admin console, choose **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show caching policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Caching** checkbox.
  - c. Select the **Options** checkbox below the Caching checkbox.
  - d. Click **OK**.
3. Select the **Caching > Options** tab.
4. On the Caching Options page, specify a maximum allowable image size in the Clients should cache all images less than field.
5. On the Caching Options page, specify a maximum allowable image size in the Clients should cache all images less than field.

## Writing a Java Access Control Resource Policy

---

Java access control resource policies control to which servers and ports Java applets can connect.

To write a Java access control resource policy:

1. In the admin console, select **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show Java policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Java** checkbox.
  - c. Select the **Access Control** checkbox below the Java checkbox.
  - d. Click **OK**.
3. Select the **Java > Access Control** tab.
4. On the Java Access Policies page, click **New Policy**.
5. Enter a name to label this policy (required) and a description of the policy (optional).
6. In the Resources section, specify the resources to which this policy applies.
7. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.

- **Policy applies to all roles OTHER THAN those selected below** —To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
    - **Allow socket access**—To enable Java applets to connect to the servers (and optionally ports) in the Resources list.
    - **Deny socket access**—To prevent Java applets from connecting to the servers (and optionally ports) in the Resources list.
    - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
  9. Click **Save Changes**.
  10. On the Java Access Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.
  11. (Optional) To improve the performance of your Java applications:
    - a. Select **Enable Java instrumentation caching** on the Maintenance > System > Options page of the admin console. This option can improve the performance of downloading Java applications.
    - b. After you finish configuring the Secure Access Service, cache your Java applet and access it as end-user. This action eliminates the performance hit that occurs through the intermediation engine when the first end-user accesses the applet.

**Related Documentation**

- [About Hosted Java Applet Templates on page 453](#)
- [Specifying Resources for a Resource Policy on page 145](#)
- [Defining Resource Policies: General Options on page 558](#)

## Writing a Java Code Signing Resource Policy

---

Java code signing resource policies specify how the Secure Access Service rewrites Java applets. By default, when the Secure Access Service intermediates a signed Java applet, it re-signs the applet with its own certificate, which is not chained to a standard root certificate. When a user requests an applet that performs potentially high-risk tasks, such as accessing network servers, the user's browser displays a security warning that the root is not a trusted root. To forestall this warning, you can import a code-signing certificate that the Secure Access Service uses to re-sign applets that it intermediates.

When configuring Java code signing resource policies, enter the servers from which you trust applets. You can enter a server IP address or domain name. The Secure Access Service only re-signs applets served by a trusted server. If a user requests an applet from server not on the list, the Secure Access Service does not use the imported production certificates to sign the applet, which means the user is prompted by the browser with a

security warning. For Sun JVM users, the Secure Access Service additionally checks that the root CA of the original applet certificate is on its list of trusted root certificate authorities.

To write a Java code signing resource policy:

1. In the admin console, choose **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show java policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Java** checkbox.
  - c. Select the **Code-Signing** checkbox below the Java checkbox.
  - d. Click **OK**.
3. Select the **Java > Code-Signing** tab.
4. On the Java Signing Policies page, click **New Policy**.
5. Enter a name to label this policy (required) and description of the policy (optional).
6. In the Resources section, specify the resources to which this policy applies.
7. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
  - **Resign applets using applet certificate**—The uploaded code-signing certificate will be used to sign the Java applets intermediated by the Secure Access Service.
  - **Resign applets using default certificate**—The Secure Access Service re-signs the applet with its own self-signed code signing certificate that is not chained to a standard root certificate.
  - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. Click **Save Changes**.
10. On the Java Signing Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

- Related Documentation**
- [Using Code-signing Certificates on page 868](#)
  - [Specifying Resources for a Resource Policy on page 145](#)
  - [Defining Resource Policies: General Options on page 558](#)
  - [Writing a Detailed Rule for Resource Policies on page 150](#)

## Creating a Selective Rewriting Resource Policy

---

Selective rewriting resource policies enable you to define a list of hosts for which you want the Secure Access Service to intermediate content as well as exceptions to this list. By default, the Secure Access Service intermediates all user requests to Web hosts—unless you have configured the Secure Access Service to serve requests to certain hosts using a different mechanism, such as the Secure Application Manager.

Create a selective rewriting policy if you do not want the Secure Access Service to intermediate traffic from Web sites that reside outside of the corporate network, such as yahoo.com, or if you do not want the Secure Access Service to intermediate traffic for client/server applications you have deployed as Web resources, such as Microsoft OWA (Outlook Web Access).

To write a selective rewriting resource policy:

1. In the admin console, choose **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show rewriting policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Rewriting** checkbox.
  - c. Select the **Selective Rewriting** checkbox below the Rewriting checkbox.
  - d. Click **OK**.
3. Select the **Rewriting > Selective Rewriting** tab.
4. On the Web Rewriting Policies page, click **New Policy**.
5. Enter a name to label this policy (required) and a description of the policy (optional).
6. In the Resources section, specify the resources to which this policy applies.
7. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.



8. In the Action section, specify:

- **Rewrite content**—The Secure Access Service intermediates all Web content from the resources specified in the Resources list.
- **Rewrite content as...**—The Secure Access Service intermediates all Web content from the resources specified in the Resources list and rewrites the content as if it were the file type specified in the drop-down list. The available options are:
  - **HTML**—Rewrite content as Hypertext Markup Language (HTML)
  - **XML**—Rewrite content as Extensible Markup Language (XML)
  - **Javascript**—Rewrite content as Java scripting language
  - **VBScript**—Rewrite content as Virtual Basic scripting language
  - **CSS**—Rewrite content as Cascading Style Sheets
  - **XSLT**—Rewrite content as XML Style Sheets
  - **Flash**—Rewrite content as Shockwave Flash
  - **DTD**—Rewrite content as Document Type Definitions (DTD)
  - **HTC**—Rewrite content as HTML component
- **Don't rewrite content: Redirect to target Web server**—The Secure Access Service does not intermediate Web content from the resources specified in the Resources list and automatically redirects the request to the target Web server. This is the default option for all rewrite resource policies that you create. If you select this option, you might want to specify that the Secure Access Service open the unrewritten pages in a new window.



**NOTE:** Do not select this option if the specified content needs to access resources inside your corporate network. For instance, if you specify that the Secure Access Service should not rewrite a particular file, and that file calls another file within your network, the user will see an error.

- **Don't rewrite content: Do not redirect to target Web server**—The Secure Access Service retrieves the content from the original Web server, but does not modify it. This is useful in cases where users may not be able to reach the original server, thus disabling redirection. (For example, if the Web server is not accessible from the public internet because it resides behind a firewall.)

The Don't rewrite content: Do not redirect to target Web server option allows users to download data from network resources via the Secure Access Service, but bypasses the Secure Access Service rewriting engine in the process. We recommend you use this feature only when rewriting signed Java applets—not other content types. For other content types such as HTML and Javascript, use the Don't rewrite content: Redirect to target Web server option to download an applet via the Secure Access Service, thus enabling direct connections to network resources.

- **Use Detailed Rules**—To specify one or more detailed rules for this policy.

9. Click **Save Changes**.
10. On the Web Rewriting Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

**Related Documentation**

- [Specifying Resources for a Resource Policy on page 145](#)
- [Defining Resource Policies: General Options on page 558](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)

---

## Creating a Passthrough Proxy Resource Policy

---

Passthrough proxy resource policies specify Web applications for which the Secure Access Service performs minimal intermediation. To create a passthrough proxy resource policy, you need to specify two things:

- Which Web application to intermediate with the passthrough proxy
- How the Secure Access Service listens for client requests to the application server

To write a passthrough proxy resource policy:

1. In the admin console, choose **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show rewriting policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Rewriting** checkbox.
  - c. Select the **Passthrough Proxy** checkbox below the Rewriting checkbox.
  - d. Click **OK**.
3. Select the **Rewriting > Passthrough Proxy** tab.
4. On the Passthrough Proxy Policies page, click **New Application**.
5. Enter a name to label this policy (required) and a description of the policy (optional).
6. In the URL field, specify the application server host name and the port used to access the application internally. Note that you cannot enter a path in this field.
7. Choose the way in which you want to enable the passthrough proxy feature:
  - **Use virtual hostname**—If you choose this option, specify a host name alias for the application server. When the Secure Access Service receives a client request for the application server host name alias, it forwards the request to the specified application server port in the URL field.

If you choose this option, you must also define the Secure Access Service name and host name in the Network Identity section of the System > Network > Internal Port tab. In order to make Sharepoint work successfully through the Secure Access Service, you must select the Override automatic cookie handling checkbox in Internet Explorer under Tools Internet options > Privacy > Advanced Privacy Settings if the following conditions true:

- You select the **Use virtual hostname** option during Pass Through Proxy configuration.
  - The virtual hostname that you specify in your Sharepoint configuration is different from the hostname that you configure through Secure Access Service setup (that is, if the domains are different).
  - You enable persistent cookies through the Users > User Roles > Select Role > General > Session Options page of the admin console.
  - **Use SA port**—If you choose this option, specify a unique Secure Access Service port in the range 11000-11099. The Secure Access Service listens for client requests to the application server on the specified Secure Access Service port and forwards any requests to the application server port specified in the URL field.
8. In the Action section, specify the method for the Secure Access Service to use to intermediate traffic:
- **Rewrite XML**—If you select this option, the Secure Access Service rewrites URLs contained within XML content. If you disable this option, the Secure Access Service passes the XML content “as is” to the server.
  - **Rewrite external links**—If you select this option, the Secure Access Service rewrites all URLs. If you disable this option, the Secure Access Service rewrites only those URLs that contain a hostname specified in the passthrough proxy policy.
  - **Block cookies from being sent to the browser**—If you select this option, the Secure Access Service blocks cookies destined for the client’s browser. The Secure Access Service stores the cookies locally and sends them to applications whenever they are requested.
  - **Host-Header forwarding**—If you select this option, the Secure Access Service passes the hostname as part of the host header instead of the actual host identifier.  
  
The Host-Header forwarding option is only valid in passthrough proxy Virtual Host mode.
9. Click **Save Changes**.
10. On the Pass-through Proxy Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the application requested by the user to an application specified in a policy’s (or a detailed rule’s) Resource list, it performs the specified action and stops processing policies.
11. If you select:
- **Use virtual hostname**, you must also:

- a. Add an entry for each application server host name alias in your external DNS that resolves to the Secure Access Service.
  - b. Upload a wildcard server certificate to the Secure Access Service (recommended).
- **Use SA port**, open traffic to the Secure Access Service port you specified for the application server in your corporate firewall.

If your application listens on multiple ports, configure each application port as a separate passthrough proxy entry with a separate Secure Access Service port. If you intend to access the server using different host names or IP addresses, configure each of those options separately; in this case, you can use the same Secure Access Service port.

External passthrough proxy links that are embedded in a passthrough proxy page may not work. For example, if the bar.company.com page contains a link to foo.company.com and foo.company.com is configured as a host-mode passthrough proxy application, the link to foo.company.com fails. To avoid this, use port-mode passthrough proxy for passthrough proxy links embedded in passthrough proxy applications.

- Related Documentation**
- [Passthrough Proxy Overview on page 495](#)
  - [Using Virtual Ports on page 802](#)

---

## Creating a Custom Header Resource Policy

---

By default, the Secure Access Service rewriting engine only sends selected custom headers to browsers (clients) and backend servers. You can use custom header resource policies, however, to allow or deny custom headers for specific resources.

Note that custom header resource policies do not control standard HTTP headers such as Content-Type.

To write a custom header resource policy:

1. In the admin console, choose **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show rewriting policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Rewriting** checkbox.
  - c. Select the **Custom Headers** checkbox below the Rewriting checkbox.
  - d. Click **OK**.
3. Select the **Rewriting > Custom Headers** tab.
4. On the Custom Header Policies page, click **New Policy**.
5. Enter a name to label this policy (required) and a description of the policy (optional).

6. In the Resources section, specify the resources to which this policy applies.
7. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
  - **Allow Custom Headers**—Select this option to prevent the Secure Access Service from blocking the headers to browsers (clients) and backend servers.
  - **Deny Custom Headers**—Select this option to use the default custom header behavior on the Secure Access Service. When you select this option, the Secure Access Service blocks custom headers for added security.
  - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. Click **Save Changes**.
10. On the Web Rewriting Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

**Related  
Documentation**

- [Defining Resource Policies: General Options on page 558](#)
- [Specifying Resources for a Resource Policy on page 145](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)

## Creating an ActiveX Parameter Resource Policy

When the Secure Access Service rewrites a Web page, it does not rewrite the ActiveX controls that are embedded in the Web page. However, you can create resource policies specifying that the Secure Access Service should rewrite the URL and host name parameters that are passed by the Web page to the Active X controls. To configure these resource policies, you must obtain the following information:

- **Class ID**—Web pages generally use a class ID to embed an ActiveX control. A class ID is a unique, constant string that uniquely identifies an ActiveX control.

You can determine what an ActiveX object's class ID is using Internet Explorer 6: Select **Tools > Internet Options**, click **Settings**, and then click **View Objects**. Select the ActiveX object, right-click, and select **Properties**. The ActiveX object's ID is highlighted.

- **Language**—Web pages can use either static or dynamic HTML (that is, by using JavaScript) to embed an Active X control. When a Web page uses static HTML, the Secure Access Service can rewrite the specified ActiveX parameters on the Secure Access Service itself while it intermediates traffic, since all of the required information passes between the user's browser and the application's Web server. When a Web page uses dynamic HTML to embed an ActiveX control, however, the page frequently pulls information from the client and then generates HTML to embed the ActiveX control. Therefore, the Secure Access Service needs to run script in the user's browser in order to obtain the information it needs to rewrite the specified ActiveX parameters.
- **Parameter type**—When configuring the Secure Access Service to rewrite a parameter, you must determine whether the parameter is a URL or host name. The Secure Access Service does not support any other parameter types.
- **Parameter name**—You must specify the name of the parameter that you want the Secure Access Service to rewrite. You can find the parameters by searching for the param tag within an object tag. For example, you might find a flash movie embedded in a page using the following code:

```
<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000" > <param
name="movie" value="mymovie.swf" />
<param name="quality" value="high" />
</object>
```

When configuring the corresponding resource policy, you should enter movie in the Parameter name field because movie refers to the URL requires rewriting. Frequently, pages contain multiple param tags, but not all of them require rewriting. In this example, the quality parameter does not require rewriting.

To write an ActiveX parameter rewriting resource policy:

1. In the admin console, choose **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show rewriting policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Rewriting** checkbox.

- c. Select the **ActiveX Parameter Rewriting** checkbox below the Rewriting checkbox.
  - d. Click **OK**.
3. Select the **Rewriting > ActiveX Parameter Rewriting** tab.
  4. On the ActiveX Parameter Rewriting Policies page, click **New Policy**.
  5. Enter class ID of the ActiveX control that you want to control with the policy (required) and description of the policy (optional).
  6. In the Parameters section, specify the ActiveX parameters that you want to control with the policy and the corresponding actions. Possible actions include:
    - **Rewrite URL and response (Static HTML only)**—The Secure Access Service rewrites the specified URL parameter on the Secure Access Service. The Secure Access Service also rewrites any response from the Web server requesting the URL. Note that you should select this option if the Web page embeds the ActiveX control using only static HTML.
    - **Rewrite URL and response (Static and dynamic HTML)**—The Secure Access Service rewrites the specified URL on the client in addition to rewriting on the Secure Access Service. The Secure Access Service also rewrites any response from the Web server requesting the URL. Note that you should select this option if the Web page embeds the ActiveX control using dynamic HTML.
    - **Rewrite URL (Static HTML only)**—The Secure Access Service rewrites the specified URL parameter on the Secure Access Service. Note that you should select this option if the Web page embeds the ActiveX control using only static HTML.
    - **Rewrite URL (Static and dynamic HTML)**—The Secure Access Service rewrites the specified URL on the client in addition to rewriting on the Secure Access Service. Note that you should select this option if the Web page embeds the ActiveX control using dynamic HTML.
    - **Rewrite hostname (Static HTML only)**—The Secure Access Service rewrites the specified host name parameter on the Secure Access Service. Note that you should select this option if the Web page embeds the ActiveX control using only static HTML.
    - **Rewrite hostname (Static and dynamic HTML)**—The Secure Access Service rewrites the specified host name on the client in addition to rewriting on the Secure Access Service. Note that you should select this option if the Web page embeds the ActiveX control using dynamic HTML.
    - **Do not rewrite**—The Secure Access Service does not rewrite any of the ActiveX component's parameters.
  7. Click **Save Changes**.

**Related  
Documentation**

- [Resource Policies on page 143](#)

## Restoring the Default Secure Access Service ActiveX Resource Policies

The Secure Access Service comes with several predefined resource policies for rewriting the parameters of commonly used ActiveX objects. If you choose to delete any of these policies and then want to restore them later, you can recreate them using the following table as a guideline.

**Table 44: Predefined Resource Policies**

Description	Class ID	Parameter	Action
Citrix NFuse xginen_EmbeddedApp object	238f6f83-b8b4-11cf-8771-00a024541ee3	ICAFile	Rewrite URL and response (Static HTML only)
OrgPlus OrgViewer	DCB98BE9-88EE-4AD0-9790-2B169E8D5BBB	URL	Rewrite URL and response (Static HTML only)
Quickplace	05D96F71-87C6-11D3-9BE4-00902742D6E0	GeneralURL General_ServerName	Rewrite URL and response (Static and dynamic HTML)  Rewrite host name (Static and dynamic HTML)
iNotes Discussion	5BDBA960-6534-11D3-97C7-00500422B550	FullURL	Rewrite URL and response (Static and dynamic HTML)



Table 44: Predefined Resource Policies (*continued*)

B20D9D6A-0DEC-4d76-9BEF-175896006B4A	B20D9D6A-0DEC-4d76-9BEF-175896006B4A	ServerURL Error URL	Rewrite URL and response (Static and dynamic HTML)  Rewrite host name (Static and dynamic HTML)
Citrix NFuse Elite	2E687AA8-B276-4910-BBFB-4E412F685379	ServerURL	Rewrite URL and response (Static HTML only)
WebPhotos LEAD	00120000-B1BA-11CE-ABC6-F5B2E79D9E3F	BitmapDataPath	Rewrite URL and response (Static and dynamic HTML)
Shockwave Flash	D27CDB6E-AE6D-11cf-96B8-444553540000	Src Movie	Rewrite URL and response (Static and dynamic HTML)  Rewrite URL and response (Static and dynamic HTML)

Table 44: Predefined Resource Policies (*continued*)

iNotes Blue	3BFFE033-BF43-11d5-A271-00A024A51325	General_URL General_ServerName	Rewrite URL and response (Static and dynamic HTML)  Rewrite host name (Static and dynamic HTML)
Tabular Data Control	333C7BC4-460F-11D0-BC04-0080C7055A83	DataURL	Rewrite URL (Static HTML only)
Windows Media Player	6BF52A52-394A-11D3-B153-00C04F79FAA6	URL	Rewrite URL and response (Static HTML only)
FlowPartPlace	4A266B8B-2BB9-47db-9B0E-6226AF6E46FC	URL	Rewrite URL and response (Static HTML only)
HTML Help	adb880a6-d8ff-11cf-9377-00aa003b7a11	Item1	Rewrite URL and response (Static and dynamic HTML)
MS Media Player	22d6f312-b0f6-11d0-94ab-0080c74c7e95	FileName	Rewrite URL and response (Static HTML only)
CSV Files Handler	333c7bc4-460f-11d0-bc04-0080c7055a83	DataURL	Rewrite URL and response (Static HTML only)

Table 44: Predefined Resource Policies (*continued*)

Special ActiveX control for Microsoft OWA	D801B381-B81D-47a7-8EC4-EFC111666AC0	mailboxUrl	Rewrite URL and response (Static HTML only)
FlowPartPlace1	639325C9-76C7-4d6c-9B4A-523BAA5B30A8	Url	Rewrite URL and response (Static HTML only)
scriptx print control	5445be81-b796-11d2-b931-002018654e2e	Path	Rewrite URL and response (Static HTML only)
94F40343-2CFD-42A1-A774-4E7E48217AD4	94F40343-2CFD-42A1-A774-4E7E48217AD4	HomeViewURL	Rewrite URL and response (Static HTML only)
Microsoft License Manager	5220cb21-c88d-11cf-b347-00aa00a28331	LPKPath	Rewrite URL and response (Static HTML only)
Domino 7 beta 2 UploadControl	E008A543-CEFB-4559-912F-C27C2B89F13B	General_URL General_ServerName	Rewrite URL and response (Static and dynamic HTML)  Rewrite host name (Static and dynamic HTML)

Table 44: Predefined Resource Policies (*continued*)

iNotes	1E2941E3-8E63-11D4-9D5A-00902742D6E0	General_URL General_ServerName	Rewrite URL and response (Static and dynamic HTML)  Rewrite host name (Static and dynamic HTML)
ActiveCGM	F5D98C43-DB16-11CF-8ECA-0000C0FD59C7	FileName	Rewrite URL and response (Static HTML only)
00130000-B1BA-11CE-ABC6-F5B2E79D9E3F	00130000-B1BA-11CE-ABC6-F5B2E79D9E3F	BitmapDataPath	Rewrite URL and response (Static and dynamic HTML)

## Creating Rewriting Filters

Only use the Rewriting Filters tab when instructed to do so by the Juniper Networks Support team.

## Writing a Web Compression Resource Policy

The Secure Access Service comes pre-equipped with one Web compression policy (\*.\*/\*) which compresses all applicable Web data. You can enable this policy through the Users > Resource Policies > Web > Compression pages of the admin console.

To write a Web compression resource policy:

1. In the admin console, choose **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show compression policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Compression** checkbox.

- c. Click **OK**.
3. Select the **Compression** tab.
4. On the Web Compression Policies page, click **New Policy**.
5. Enter a name to label this policy (required) and a description of the policy (optional).
6. In the Resources section, specify the URLs to which this policy applies.
7. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
  - **Compress**—The Secure Access Service compresses the supported content types from the specified resource.
  - **Do not compress**—The Click Save Changes. does not compress the supported content types from the specified resource.
  - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. Click **Save Changes**.

**Related  
Documentation**

- [Specifying Resources for a Resource Policy on page 145](#)
- [Defining Resource Policies: General Options on page 558](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)

## Defining an OWA Compression Resource Policy

Due to caching issues with OWA, the Secure Access Service comes with the following built-in resource policies specifying that the Secure Access Service should not compress Javascript or CSS files that are routed through OWA:

1. Do Not Compress \*/\*/exchWeb/controls/\*.css (all roles)
2. Do Not Compress \*/\*/exchWeb/controls/\*.js (all roles)
3. Do Not Compress \*/\*/exchWeb/\*/controls/\*.css (all roles)
4. Do Not Compress \*/\*/exchWeb/\*/controls/\*.js (all roles)

In the last two policies, a wildcard (\*) is included in the path to account for different OWA build versions.

Juniper Networks recommends that you do not change the compression resource policies for OWA unless absolutely necessary.

**Related Documentation**

- [About OWA and Lotus Notes Caching Resource Policies on page 535](#)

---

## Writing a Web Proxy Resource Policy

---

Web proxy resource policies specify Web proxy servers for which the Secure Access Service should intermediate content. Note that the Secure Access Service intermediates both forward and backwards proxies, but only enables single sign-on to a proxy when you use these tabs to configure the proxy and thereby specify that you trust it.

To write a Web proxy resource policy:

1. In the admin console, choose **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show Web proxy policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Web Proxy** checkbox.
  - c. Select the **Policies** checkbox below the Web Proxy checkbox.
  - d. Click **OK**.
3. Select the **Web Proxy > Policies** tab.
4. On the Web Proxy Policies page, click **New Policy**.
5. Enter a name to label this policy (required) and a description of the policy (optional).
6. In the Resources section, specify the resources to which this policy applies.
7. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
  - **Access Web resources directly**—The Secure Access Service intermediates the user's request to a back-end server and the server's response to the user for requests made to a resource specified in the Resources list.
  - **Access Web resources through a Web proxy**—Specify a Web proxy server in the drop-down list that you have defined in the Users > Resource Policies > Web > Web Proxy > Servers tab.

- **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. Click **Save Changes**.
  10. On the Web Proxy Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

**Related Documentation**

- [Defining Resource Policies: General Options on page 558](#)
- [Specifying Resources for a Resource Policy on page 145](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)

## Specifying Web Proxy Servers

---

You can direct all Web requests made through the Secure Access Service to a Web proxy rather than using the Secure Access Service to connect directly to Web servers. This feature can be useful if your network security policy requires this configuration or if you want to use a caching Web proxy to improve performance.

To specify servers for Web proxy resource policies:

1. In the admin console, choose **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show Web proxy policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Web Proxy** checkbox.
  - c. Select the **Servers** checkbox below the Web Proxy checkbox.
  - d. Click **OK**.
3. Select the **Web Proxy > Servers** tab.
4. Under Web Proxy Servers, enter the name or IP address of the Web proxy server and the port number at which the proxy server listens, and then click **Add**.
5. Repeat this step to specify additional Web proxy servers.

**Related Documentation**

- [Writing a Web Proxy Resource Policy on page 554](#)

## Writing An HTTP 1.1 Protocol Resource Policy

---

Protocol resource policies enable or disable HTTP 1.1 protocol support between the Secure Access Service and backend servers. The Secure Access Service supports chunked Transfer-Encoding, gzip and deflate Content-Encoding, connection persistence, and

caching headers such as If-Modified-Since, If-None-Match, If-Unmodified-Since and If-Match. The Secure Access Service supports range requests with partial content when you select the Don't rewrite content: Do not redirect to target web server selective rewrite option.

For a detailed description of the HTTP 1.1 protocol, refer to the Hypertext Transfer Protocol -- HTTP 1.1 specification from the World Wide Web Consortium.

The Secure Access Service only communicates with network servers using HTTP 1.1 if the client also communicates using HTTP 1.1. If the client uses HTTP 1.0, the Secure Access Service communicates with backend servers using HTTP 1.0, regardless of whether or not HTTP 1.1 is enabled.

If you want to use HTTP 1.1 for a specific resource, enable HTTP 1.1 for that policy and ensure that the new policy appears above the default in the list of configured policies. You should add the HTTP 1.1 policy to the top of the policy list because the policy evaluation engine evaluates policies from top to bottom, stopping when it encounters a match.

The Secure Access Service comes with a default policy that disables HTTP 1.1 for all resources. If you want to use HTTP 1.1 for all resources, either redefine the “\*:\*/\*” policy or create a new policy enabling HTTP 1.1 and move it to the top of your policy list. If you delete this default policy (and any other policies that disable HTTP 1.1), the Secure Access Service uses HTTP 1.0 for all resources

To write an HTTP 1.1 protocol resource policy:

1. In the admin console, choose **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show protocol policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Protocol** checkbox.
  - c. Click **OK**.
3. Select the **Protocol** tab.
4. On the Web Protocol Policies page, click **New Policy**.
5. Enter a name to label this policy (required) and a description of the policy (optional).
6. In the Resources section, specify the URLs to which this policy applies.
7. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.



- **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
    - **Disable HTTP 1.1**—The Secure Access Service automatically communicates with backend servers via the HTTP 1.0 protocol.
    - **Enable HTTP 1.1**—The Secure Access Service automatically communicates with backend servers using the HTTP 1.1 protocol as long as the client also communicates using the HTTP 1.1 protocol.
    - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
  9. Click **Save Changes**.

**Related Documentation**

- [Resource Policy Evaluation on page 147](#)
- [Defining Resource Policies: General Options on page 558](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)

## Creating a Cross Domain Access Policy

The XMLHttpRequest object allows scripts to perform HTTP client functionality, such as submitting form data or loading data from a server. Today's web browsers impose a security restriction on the use of XMLHttpRequest. You are not allowed to make XMLHttpRequests to any server except the server where your web page came from. For example, if both your web application and the data required for that application come from the same web server, then there is no restriction. But, if your web application is on one server and you make a request to a different server, the browser prevents the connection from opening. It is possible to bypass this security, however.

The Secure Access Service lets you create a resource profile that determines whether or not to impose this restriction and to what level. By default, this restriction is bypassed and cross domain access is allowed.

To create a cross domain access policy:

1. In the admin console, choose **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show cross-domain policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Rewriting** checkbox.
  - c. Select the **Cross Domain Access** checkbox below the Rewriting checkbox.
  - d. Click **OK**.
3. Select the **Rewriting > Cross Domain Access** tab.

4. On the Cross Domain Access page, click **New Policy**.
5. Enter a name to label this policy (required) and a description of the policy (optional).
6. In the Resources section, specify the URLs to which this policy applies.
7. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
  - **Allow Cross Domain Access**—To not impose any restriction and allow cross domain access.
  - **Deny XMLHttpRequest Cross Domain Access only**—To deny cross domain access if the XMLHttpRequest object is used in the call.
  - **Deny all Cross Domain Access**—To deny cross domain access regardless of whether or not the XMLHttpRequest object is used in the call.
  - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
9. Click **Save Changes**.

**Related  
Documentation**

- [Defining Resource Policies: General Options on page 558](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)

---

## Defining Resource Policies: General Options

---

When you enable the Web resource policy options described in this section, the Secure Access Service compiles a list of host names specified in the Resources field of each Web resource policy. The Secure Access Service then applies the enabled options to this comprehensive list of host names.

To specify Web resource options:

1. In the admin console, navigate to **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show Web options, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Options** checkbox.

- c. Click **OK**.
3. Select the **Options** tab.
4. Select **IP based matching for Hostname based policy resources** if you want the Secure Access Service to look up IP address corresponding to each host name specified in a Web resource policy. When a user tries to access a server by specifying an IP address rather than the host name, the Secure Access Service compares the IP to its cached list of IP addresses to determine if a host name matches an IP. If there is a match, then the Secure Access Service accepts the match as a policy match and applies the action specified for the resource policy.



**NOTE:** This option does not apply to host names that include wildcards and parameters.

5. Select **Case sensitive matching for the Path and Query string components in Web resources** if you want to require users to enter a case-sensitive URL to a resource. For example, use this option when passing username or password data in a URL.
6. Click **Save Changes**.

**Related  
Documentation**

- [Resource Policies on page 143](#)
- [Resource Policy Components on page 144](#)

## Managing Resource Policies: Customizing UI Views

You can control which Web resource policy configuration pages the Secure Access Service displays so that you only have to view those pages that you actually use. Or, if you have a new Secure Access Service installation, you can use these settings to display additional pages (since the Secure Access Service only displays the most commonly used resource policy pages to new users).

To control which Web resource policy configuration pages the Secure Access Service displays:

1. In the admin guide, choose **Users > Resource Policies > Web > Policy Type**.
2. Click the **Customize View** button in the upper right corner of the console.
3. In the Customize View dialog box, specify which Web resource policies you want to display in the admin console. You may manually select individual checkboxes, click **All Pages** to display all Web resource policy configuration pages, or click **Common Pages** to display the most commonly used Web resource policy configuration pages. (Note that the Secure Access Service does not allow you to hide the Web Access Policies page.)
4. Click **OK**.

**Related  
Documentation**

## CHAPTER 22

# File Rewriting

- File Rewriting Overview on page 561
- Creating a File Rewriting Resource Profile on page 563
- Creating a File Access Control Autopolicy on page 564
- Creating a File Compression Autopolicy on page 564
- Creating a Single Sign-On Autopolicy (Windows Only) on page 565
- Configuring File Resource Profile Bookmarks on page 566
- Creating Windows File Bookmarks on page 568
- Creating Advanced Bookmarks to Windows Resources on page 569
- Creating Windows Bookmarks that Map to LDAP Servers on page 570
- Defining General Windows File Browsing Options on page 570
- Writing a File Resource Policy on page 570
- Writing a Windows Access Resource Policy on page 572
- Writing a Windows SSO Resource Policy on page 573
- Writing a Windows Compression Resource Policy on page 574
- Defining General File Writing Options on page 575
- Creating UNIX File Bookmarks on page 576
- Creating Advanced Bookmarks to UNIX Resources on page 576
- Defining General UNIX File Browsing Options on page 577
- Defining UNIX/NFS File Resource Policies on page 578
- Writing UNIX/NFS Resource Policies on page 579
- Writing a UNIX/NFS Compression Resource Policy on page 580
- Defining General UNIX/NFS File Writing Options on page 581

### File Rewriting Overview

---

A file resource profile controls access to resources on Windows server shares or UNIX servers.

File rewriting is a standard feature on all Secure Access appliances except the SA 700. If you are using an SA-700 appliance, you must install a Core Clientless Access upgrade license in order to access file rewriting features.

When creating a file resource profile, you must use the following formats when defining a resource policy's primary resource as well as its autopolicy resources.

Windows resources:

```
\\server[\share[\path]]
```

UNIX resources:

```
server[/path]
```

Within these formats, the three components are:

- Server (required)—Possible values:
  - Hostname—You may use the system variable <username> when defining the hostname.
  - IP address—The IP address needs to be in the format: a.b.c.d

The leading two back slashes are required for Windows, non-Nfs resources.

- Share (required, Windows only)—The system variable <username> is allowed. Note that when the Secure Access Service tries to connect to a Windows file share, it connects to ports 445 and 139.
- Path (optional)—Special characters allowed include:

*	Matches any character. Note that you cannot use the * wildcard character when defining a resource profile's primary resource (that is, the Server/share field for Windows resources or the Server field for UNIX resources).
%	Matches any character except slash (/)
?	Matches exactly one character

Valid Windows resources include:

```
\\juniper.com\dana
\\10.11.0.10\share\web
\\10.11.254.227\public\test.doc
```

Valid UNIX resources include:

```
juniper.com/dana
10.11.0.10/share/web
10.11.254.227/public/test.doc
```

**Related  
Documentation**

- [System Variables and Examples on page 1186](#)
- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)

---

## Creating a File Rewriting Resource Profile

---

To create a file rewriting resource profile:

1. In the admin console, choose **Users > Resource Profiles > Files**.
2. Click **New Profile**.
3. From the Type list, select **Windows** or **Unix**.
4. Enter a unique name and optionally a description for the resource profile. (This name becomes the default bookmark's name.)
5. Enter the resource to which you want to control access. Note that the format of the resource varies depending on which type of resource profile you are creating:
  - **Windows**—Enter the server name or IP address, share name, and optionally the path that you want to control access to in the Server/share field. When entering the resource, use the format: `\\server[\share[\path]]`.
  - **Unix**—Enter the server name or IP address and optionally the path that you want to control access to in the Server field. When entering the resource, use the format: `server[/path]`
6. In the Autopolicy: Windows File Access Control section or the Autopolicy: UNIX Access Control section, create a policy that allows or denies users access to the resource specified the previous step. (At minimum, you need to click Add in order to use the access control policy that the Secure Access Service automatically creates for you. This policy allows access to the specified directory and all of its sub-directories.)
7. (Optional) Click **Show ALL autopolicy types** to create additional autopolicies that fine-tune access to the resource. Then, create the autopolicies.
8. Click **Save and Continue**.
9. In the Roles tab, select the roles to which the resource profile applies and click Add.

The selected roles inherit the autopolicies and bookmarks created by the resource profile. If it is not already enabled, the Secure Access Service also automatically enables the Files, Windows option or the Files, UNIX/NFS option in the Users > User Roles > Select Role > General > Overview page of the admin console for all of the roles you select.
10. Click **Save Changes**.
11. (Optional) In the Bookmarks tab, modify the default bookmark created by the Secure Access Service and/or create new ones. (By default, the Secure Access Service creates a bookmark to the resource defined in the Windows or UNIX field and displays it to all users assigned to the role specified in the Roles tab.)

### Related Documentation

- [Defining a Resource Profile on page 6](#)
- [Creating a File Access Control Autopolicy on page 564](#)
- [Defining a Single Sign-On Autopolicy on page 500](#)

## Creating a File Access Control Autopolicy

---

File access control policies specify resources on your file servers that users may access. When defining a file resource profile, you must create a corresponding access control autopolicy that enables access to the profile's primary resource. The Secure Access Service simplifies the process for you by automatically creating an autopolicy that allows access to the directory specified in the Server/share field (Windows) or the Server field (UNIX) and all of its sub-directories. To enable this autopolicy, you simply need to select it and click Add.

If necessary, you may choose to modify this default autopolicy or create supplementary file access control autopolicies that allow or deny access to additional resources.

To create a new file access control autopolicy:

1. Create a file resource profile.
2. If it is not already enabled, select the **Autopolicy: Windows File Access Control** checkbox or the **Autopolicy: Unix Access Control** checkbox.
3. In the Resource field, specify the resource to which this policy applies using the format: \\server[\share[\path]] for Windows resources and \\server[\path] for UNIX resources.
4. From the Action list, select one of the following options:
  - **Allow**—Select this option to enable access to the specified resource.
  - **Read-only**—Select this option to allow users to view but not edit the specified resource.
  - **Deny**—Select this option to block access to the specified resource.
5. Click **Add**.
6. Click **Save Changes**.

### Related Documentation

- [Creating a File Rewriting Resource Profile on page 563](#)

## Creating a File Compression Autopolicy

---

Compression autopolicies specify which types of file data the Secure Access Service should compress when you enable GZIP compression through the Maintenance > System > Options page of the admin console.



**NOTE:** Gzip compression is not supported on the MAG Series Junos Pulse Gateways.



To create a file compression autopolicy:

1. Create a file resource profile.
2. Click **Show ALL autopolicy types**.
3. Select the **Autopolicy: Windows File Compression** checkbox or the **Autopolicy: Unix File Compression** checkbox.
4. In the Resource field, specify the resource to which this policy applies using the format: \\server[\share[\path]] for Windows resources and \\server[\path] for UNIX resources.
5. In the Action field, select one of the following options:
  - **Compress**—Select this option to compress data from the specified resource.
  - **Do not compress**—Select this option to disable compression for the specified resource.
6. Click **Add**.

**Related Documentation**

- [About Compression on page 1157](#)

## Creating a Single Sign-On Autopolicy (Windows Only)

---

Single sign-on (SSO) autopolicies configure the Secure Access Service to automatically submit credentials to a Windows share or directory so that the user does not have to reenter his credentials.

To create a Windows SSO autopolicy:

1. Create a Windows file resource profile.
2. Click **Show ALL autopolicy types**.
3. Select the **Autopolicy: Windows Server Single Sign-On** checkbox.
4. In the Resource field, specify the resource to which this policy applies using the format: \\server[\share[\path]].
5. Select one of the following options:
  - **Use predefined credentials**—Select this option if you want to specify credentials to pass to the Windows share or directory. Then:
    - In the Username field, enter variable (such as <username> or a static username (such as administrator) to submit to the Windows share or directory. When entering a variable, you may also include a domain. For example, yourcompany.net\<username>.
    - Enter a variable (such as <password> in the Variable Password field or enter a static password in the Variable field. Note that the Secure Access Service masks the password you enter here with asterisks.

When entering static credentials, note that the Secure Access Service file browsing server maintains the connections open to a server share, however, so connecting

to a different folder on the same share using a different account may not work reliably.

If the specified credentials fail, the Secure Access Service may submit alternative credentials.

- **Disable SSO**—Select this option if you do not want the Secure Access Service to automatically submit credentials to the specified Windows share or directory.

6. Click **Save Changes**.

#### Related Documentation

- [About Single Sign-On on page 335](#)
- [File Rewriting Overview on page 561](#)
- [Multiple Sign-In Credentials Execution on page 339](#)

---

## Configuring File Resource Profile Bookmarks

---

When you create a file resource profile, the Secure Access Service automatically creates a bookmark that links to the primary resource that you specified in the resource profile. The Secure Access Service enables you to modify this bookmark as well as create additional bookmarks within the same domain.

When configuring bookmarks, note that:

- You can only assign bookmarks to roles that you have already associated with the resource profile—not all of the roles defined on the Secure Access Service. To change the list of roles associated with the resource profile, use settings in its Roles tab.
- Bookmarks simply control which links the Secure Access Service displays to users—not which resources the users can access. For instance, if you enable access to a Windows directory but do not create a bookmark to that directory, users can access the directory through Windows Explorer.
- You cannot create bookmarks that link to additional servers defined through file access control autopolicies.
- If you use a bookmark to reference a file shortcut, note that the Secure Access Service only displays bookmarks with shortcuts to files or folders on a network share such as \\server5\share\users\jdoe\file.txt. However, the Secure Access Service does not display bookmarks with shortcuts to local directories such as C:\users\jdoe\file.txt.

To configure file resource profile bookmarks:

1. If you want to create a resource profile bookmark through the standard resource profiles page:
  - a. Navigate to the **Users > Resource Profiles > Files > Resource Profile Name > Bookmarks** page in the admin console.
  - b. Click the appropriate link in the Bookmark column if you want to modify an existing bookmark. Or, click **New Bookmark** to create an additional bookmark.

Alternatively, if you want to create a resource profile bookmark through the user roles page:

- a. Navigate to the **Users > User Roles > Role Name > Files > Windows Bookmarks|Unix Bookmarks** page in the admin console.
- b. Click **New Bookmark**.
- c. From the Type list, choose **File Resource Profile**. (The Secure Access Service does not display this option if have not already created a file resource profile.)
- d. Select an existing resource profile.
- e. Click **OK**. (If you have not already associated the selected role with the resource profile, the Secure Access Service automatically makes the association for you. The Secure Access Service also enables any access control policies for the role that are required by the resource profile.)
- f. If this role is not already associated with the selected resource profile, the Secure Access Service displays an informational message. If you see this message, click **Save Changes** to add this role to the resource profile's list of roles and to update the profile's autopolicies as required. Then, repeat the previous steps to create the bookmark.



**NOTE:** When you create a resource profile bookmark through the user roles page (instead of the standard resource profiles page), the Secure Access Service only associates the generated bookmark with the selected role. The Secure Access Service does not assign the bookmark to all of the roles associated with the selected resource profile.

2. Optionally change the name and description of the bookmark. (By default, the Secure Access Service populates names the bookmark using the resource profile name.)
3. In the File Browsing Path field, add a suffix to the resource if you want to create links to sub-directories of the resource defined in the primary resource profile.  
  
Make sure to enter a unique server and path in this field. If you create two bookmarks that contain the same concatenated server and path string, the Secure Access Service deletes one of the bookmarks from the end-user view. You will still be able to see both bookmarks, however, in the administrator console.
4. In the Appearance section, choose one of the following options:
  - **Appear as bookmark on homepage and in file browsing**—Select this option if you want the bookmark to appear both on a user's welcome page and when browsing network files.
  - **Appear in file browsing only**—Select this option if you want the bookmark to appear only when users are browsing network files.

5. If you are configuring the bookmark through the resource profile pages, under Roles, specify the roles to which you want to display the bookmark:
  - **ALL selected roles**—Select this option to display the bookmark to all of the roles associated with the resource profile.
  - **Subset of selected roles**—Select this option to display the bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL Selected Roles list and click **Add** to move them to the Subset of selected roles list.
6. Click **Save Changes**.

**Related Documentation**

- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)
- [Creating Windows File Bookmarks on page 568](#)

---

## Creating Windows File Bookmarks

---

You can use two different methods to create Windows file bookmarks:

- **Create bookmarks through existing resource profiles (recommended)**—When you select this method, the Secure Access Service automatically populates the bookmark with key parameters (such as the primary server and share) using settings from the resource profile. Additionally, while you are creating the associated resource profile, the Secure Access Service guides you through the process of creating any required policies to enable access to the bookmark.
- **Create standard bookmarks**—When you select this option, you must manually enter all bookmark parameters during configuration. Additionally, you must enable access to the file browsing at the role level and create resource policies that enable access to the servers defined in the bookmark.

You can create Windows bookmarks that appear on the welcome page for users mapped to this role. You can insert the user's Secure Access Service username in the URL path to provide quick access to the user's network directories.

When Secure Access Service users are browsing files on a Dfs server, the Dfs server uses the site configuration data stored in Active Directory to return Dfs referrals to the Secure Access Service in the right order. Referrals to closer servers are put higher in the list than referrals to servers that are farther away. Clients try referrals in the order in which they are received. If a request comes from a client which resides in a subnet which is not in this list, the server will not know where the client is coming from and will return the list of referrals to the customer in an arbitrary order. This could potentially cause the Dfs requests from the Secure Access Service (acting as the client in this case) to access a server much farther away. In turn, this could cause serious delays, especially if the Secure Access Service attempts to access a server which is unreachable from the subnet which the Secure Access Service resides in. If the Secure Access Service is installed on a subnet which is not in the Dfs server's list, the Dfs administrator may use the "Active Directory Sites and Services" tool on the domain controller to add the Secure Access Service's subnet to the appropriate site.

- Related Documentation**
- [Configuring File Resource Profile Bookmarks on page 566](#)

## Creating Advanced Bookmarks to Windows Resources

---

Information in this topic is provided for backwards compatibility. We recommend that you configure access to Windows shares and directories through resource profiles instead, since they provide a simpler, more unified configuration method.

To create a bookmark to a Windows resource:

1. In the admin console, choose **Users > User Roles > Role Name > Files > Windows Bookmarks**.
2. Click **New Bookmark** and then browse to or enter the server and share name. Specify a path to further restrict access. If you want to insert the user's username, enter <username> at the appropriate place in the path. For information about additional system variables and attributes that you can include in the bookmark. If you specify a name and description for the bookmark, this information displays on the Secure Access Service home page instead of the server/share.

You may not bookmark a Windows server. You must specify both the server and share name.

Make sure to enter a unique server and path in this field. If you create two bookmarks that contain the same concatenated server and path string, the Secure Access Service deletes one of the bookmarks from the end-user view. You will still be able to see both bookmarks, however, in the administrator console.

3. For Appearance, choose either:
  - **Appear as bookmark on homepage and in file browsing** if you want the bookmark to appear both on a user's welcome page and when browsing network files.
  - **Appear in file browsing only** if you want the bookmark to appear only when browsing network files.
4. For Access, click **Enable auto-allow access to this bookmark** if you want the Secure Access Service to automatically create a corresponding Windows Access resource policy. Note that this functionality applies only to role bookmarks and not bookmarks created by users. Next, select:
  - **Read-write access** to enable users to save files on the server. Note that users cannot upload files greater than 500 MB to the server.
  - **Include sub-folders** to enable users to view files in directories below the specified bookmark path.



**NOTE:** You may not see the Auto-allow option if you are using a new installation or if an administrator hides the option.

---

5. Click **Save Changes** or **Save + New** to add another.

- Related Documentation**
- [Creating a File Rewriting Resource Profile on page 563](#)
  - [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)

## Creating Windows Bookmarks that Map to LDAP Servers

---

To create a bookmark that automatically maps to a user's LDAP home directory:

1. Create an LDAP server instance.
2. Add the LDAP attribute homeDirectory to the Server Catalog.
3. Configure a realm and bind LDAP as the authentication server.
4. Configure role-mapping rules, as needed.
5. Create a Windows bookmark. During configuration, specify <userAttr.homeDirectory> in the bookmark.
6. Click **Save Changes**.

- Related Documentation**
- [Using an LDAP Server on page 175](#)
  - [Defining an LDAP Server Instance on page 176](#)
  - [Creating Windows File Bookmarks on page 568](#)

## Defining General Windows File Browsing Options

---

To specify general Windows file browsing options:

1. In the admin console, choose **Users > User Roles > Role Name > Files > Options**.
2. Under Windows Network Files, specify which options to enable for users:
  - **User can browse network file shares**—If enabled, users can view and create bookmarks to resources on available Windows file shares.
  - **User can add bookmarks**—If enabled, users can view and create bookmarks to resources on available Windows file shares.
3. Click **Save Changes**.

**Related Documentation**

## Writing a File Resource Policy

---

When you enable the File access feature for a role, you need to create resource policies that specify which Windows and UNIX/NFS resources a user may access, as well as the encoding to use when communicating with Windows and NFS file shares. When a user makes a file request, the Secure Access Service evaluates the resource policies corresponding to the request, such as Windows access resource policies for a request

to fetch an MS Word document (.doc file). After matching a user's request to a resource listed in a relevant policy, the Secure Access Service performs the action specified for the resource.

You can create resource policies through the standard interface (as described in this section) or through resource profiles (recommended method).

When writing a File resource policy, you need to supply key information:

- **Resources**—A resource policy must specify one or more resources to which the policy applies. When writing a File policy, you need to specify File servers or specific shares.
- **Roles**—A resource policy must specify the roles to which it applies. When a user makes a request, the Secure Access Service determines what policies apply to the role and then evaluates those policies that correspond to the request.
- **Actions**—Each type of resource policy performs a certain action, which is either to allow or deny a resource or to perform or not perform some function, such as allow a user to write to a directory. You can also write detailed rules that apply more conditions to a user request.

The Secure Access Service engine that evaluates resource policies requires that the resources listed in a policy's Resources list follow a canonical format.

## Windows File Resources Canonical Format

Information in this section is provided for backwards compatibility. We recommend that you configure access to Windows file servers through resource profiles instead, since they provide a simpler, more unified configuration method.

When writing a resource policy for a Windows file resource, you need to understand the following canonical format.

```
\\server[\share[\path]]
```

The three components are:

- **Server (required)**—Possible values:
  - **Hostname**—The system variable <username> may be used.
  - **IP address**—The IP address needs to be in the format: a.b.c.d
  -
- **Share (optional)**—If the share is missing, then star (\*) is assumed, meaning ALL paths match. The system variable <username> is allowed.
- **Path (optional)**—Special characters allowed include:

*	Matches any character
%	Matches any character except slash (/)
?	Matches exactly one character

If the path is missing, then slash (/) is assumed, meaning only top-level folders are matched. For example:

```
\\%.danastreet.net\share*
.juniper.com\dana
\\10.11.0.10\share\web*
\\10.11.254.227\public\%.doc
```

**Related  
Documentation**

- [Writing a Detailed Rule for Resource Policies on page 150](#)
- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)

---

## Writing a Windows Access Resource Policy

Information in this topic is provided for backwards compatibility. We recommend that you configure access to Windows file servers through resource profiles instead, since they provide a simpler, more unified configuration method.

To write a Windows access resource policy:

1. In the admin console, choose **Users > Resource Policies > Files > Access > Windows**.
2. On the Windows File Access Policies page, click **New Policy**.
3. Enter a name to label this policy (required) and a description of the policy. (optional)
4. In the Resources section, specify the resources to which this policy applies.
5. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. In the Action section, specify:
  - **Allow access**—To grant access to the resources specified in the Resources list. Check **Read-only** to prevent users from saving files on the server.
  - **Deny access**—To deny access to the resources specified in the Resources list.
  - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
7. Click **Save Changes**.
8. On the Windows File Access Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.



If you want to write a File resource policy that enables you to specify credentials for the Secure Access Service to submit to a file server when a user request matches a resource in the Resource list, you can use the following procedure to do so. You can also configure the Secure Access Service to prompt users for credentials.

- Related Documentation**
- [Creating a File Rewriting Resource Profile on page 563](#)
  - [Writing a Detailed Rule for Resource Policies on page 150](#)

## Writing a Windows SSO Resource Policy

---

Information in this topic is provided for backwards compatibility. We recommend that you configure access to Windows file servers through resource profiles instead, since they provide a simpler, more unified configuration method.

To write a Windows credentials resource policy:

1. In the admin console, choose **Users > Resource Policies > Files > SSO > Windows**.
2. On the Windows Credentials Policies page, click **New Policy**.
3. Enter a name to label this policy (required) and a description of the policy. (optional)
4. In the Resources section, specify the resources to which this policy applies.
5. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. In the Action section, specify the action to take when a resource requires credentials:
  - **Use System Credentials**—If the Secure Access Service has stored credentials for the specified user and resource in its cache, it submits the stored credentials. If the stored credentials fail or if no stored credentials exist for that user, the Secure Access Service prompts for new credentials and stores the new credentials.
  - **Use Specific Credentials**—You specify static credentials that the Secure Access Service submits to resources. The Secure Access Service file browsing server maintains the connections open to a server\share so connecting to a different folder on the same share using a different account may not work reliably. If the specified credentials fail, the Secure Access Service may submit alternative credentials. Note that the Secure Access Service masks the password you enter here with asterisks.
  - **Prompt for user credentials**—The Secure Access Service intermediates the share challenge by presenting an authentication challenge in the Secure Access Service the first time a user attempts to access the share. The user enters the credentials

and the credentials are stored in the Secure Access Service. If the credentials later fail, the Secure Access Service again prompts the user for their credentials.

- **Use Detailed Rules**—To specify one or more detailed rules for this policy.
7. Click **Save Changes**.
  8. On the Windows File Access Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

#### Related Documentation

- [Creating a File Rewriting Resource Profile on page 563](#)
- [About Single Sign-On on page 335](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)

## Writing a Windows Compression Resource Policy

Information in this section is provided for backwards compatibility. We recommend that you configure compression through resource profiles instead, since they provide a simpler, more unified configuration method.

Compression policies specify which types of file data the Secure Access Service should compress when you enable GZIP compression through the Maintenance > System > Options page of the admin console.



**NOTE:** Gzip compression is not supported on the MAG Series Junos Pulse Gateways.

The Secure Access Service comes pre-equipped with two file compression policies (\*.\*/\*) which compress all applicable file data. You may enable these policies through the Resource Policies > Files > Compression pages of the admin console.

To write a Windows file compression resource policy:

1. In the admin console, choose **Resource Policies > Files > Compression**.
2. Select the **Windows** tab.
3. Click **New Policy**.
4. Enter a name to label this policy (required) and a description of the policy. (optional)
5. In the Resources section, specify the resources to which this policy applies.
6. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.

- **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
7. In the Action section, specify:
    - **Compress**—The Secure Access Service compresses the supported content types from the specified resource.
    - **Do not compress**—The Secure Access Service does not compress the supported content types from the specified resource.
    - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
  8. Click **Save Changes**.

**Related  
Documentation**

- [About Compression on page 1157](#)
- [Creating a File Compression Autopolicy on page 564](#)
- [Specifying Resources for a Resource Policy on page 145](#)
- 

## Defining General File Writing Options

You can specify File resource options that apply to your File resource policies. When you enable a File resource policy option, the Secure Access Service compiles a list of host names specified in the Resources field of each File resource policy. The Secure Access Service then applies the enabled options to this comprehensive list of host names.

To specify resource options for Windows file servers:

1. In the admin console, choose **Users > Resource Policies > Files > Options**.
2. Select:
  - **IP based matching for Hostname based policy resources**—The Secure Access Service looks up the IP address corresponding to each host name specified in a File resource policy. When a user tries to access a server by specifying an IP address rather than the host name, the Secure Access Service compares the IP to its cached list of IP addresses to determine if a host name matches an IP. If there is a match, then the Secure Access Service accepts the match as a policy match and applies the action specified for the resource policy.

This option does not apply to host names that include wildcards and parameters.

- **Case sensitive matching for the Path component in File resources**—Require users to enter a case-sensitive path component.
- **Encoding**—Select the encoding to use when communicating with Windows and NFS file shares.

- **Use NTLM v1, NTLM v1 will be used for all NTLM negotiations**—Select this option to use only NTLM V1 for file share authentication.
  - **Use NTLM v2, NTLM v2 will be used for all NTLM negotiations**—Select this option to use only NTLM V2 for file share authentication.
  - **Number of NTLM authentication protocol variant attempts**—Controls the number of login attempts while doing SSO, Select “Low” if you are seeing account lockout issues.
3. Click **Save Changes**.

**Related  
Documentation**

- [About Basic, NTLM and Kerberos Resources on page 522](#)
- [About Single Sign-On on page 335](#)

---

## Creating UNIX File Bookmarks

---

You can use two different methods to create UNIX file bookmarks:

- Create bookmarks through existing resource profiles (recommended)—When you select this method, the Secure Access Service automatically populates the bookmark with key parameters (such as the server) using settings from the resource profile. Additionally, while you are creating the associated resource profile, the Secure Access Service guides you through the process of creating any required policies to enable access to the bookmark.
- Create standard bookmarks—When you select this option, you must manually enter all bookmark parameters during configuration. Additionally, you must enable access to the file browsing at the role level and create resource policies that enable access to the servers defined in the bookmark.

You can create UNIX bookmarks that appear on the welcome page for users mapped to this role. You can insert the user’s Secure Access Service username in the URL path to provide quick access to the user’s network directories.

**Related  
Documentation**

- [Creating Windows File Bookmarks on page 568](#)
- [Creating Advanced Bookmarks to UNIX Resources on page 576](#)

---

## Creating Advanced Bookmarks to UNIX Resources

---

Information in this topic is provided for backwards compatibility. We recommend that you configure access to UNIX servers through resource profiles instead, since they provide a simpler, more unified configuration method.

You can create UNIX/NFS bookmarks that appear on the Secure Access Service home page. You can insert the user’s Secure Access Service username in the URL path to provide quick access to the user’s network directories.

To create a bookmark to a UNIX/NFS resource:

1. In the admin console, choose **Users > User Roles > Role Name > Files > UNIX Bookmarks**.
2. Click **New Bookmark** and then enter the server host name or IP address and the path to the share. If you want to insert the user's username, enter <username> at the appropriate place in the path. If you specify a name and description for the bookmark, this information displays on the Secure Access Service home page instead of the server/path.

Make sure to enter a unique server and path in this field. If you create two bookmarks that contain the same concatenated server and path string, the Secure Access Service deletes one of the bookmarks from the end-user view. You will still be able to see both bookmarks, however, in the administrator console.

3. For Appearance, choose either:
  - **Appear as bookmark on homepage and in file browsing** if you want the bookmark to appear both on a user's welcome page and when browsing network files.
  - **Appear in file browsing only** if you want the bookmark to appear only when browsing network files.
4. For Access, click **Enable auto-allow access to this bookmark** if you want the Secure Access Service to automatically create a corresponding UNIX/NFS resource policy. Note that this functionality applies only to role bookmarks and not bookmarks created by users. Next, select:
  - **Read-write access** to enable users to save files on the server. Note that users cannot upload files greater than 500 MB to the server.
  - **Include sub-folders** to enable users to view files in directories below the specified bookmark path.



**NOTE:** You may not see the Auto-allow option if you are using a new installation or if an administrator hides the option.

5. Click **Save Changes** or **Save + New** to add another.

**Related Documentation**

- [Creating a File Rewriting Resource Profile on page 563](#)

## Defining General UNIX File Browsing Options

For NFS file browsing to work properly, you must configure an NIS server on the Secure Access Service before enabling NFS file browsing.

To specify general file browsing options:

1. In the admin console, choose **Users > User Roles > Role Name > Files > Options**.
2. Under UNIX Network Files, specify which options to enable for users:

- **User can browse network file shares**—If enabled, users can view and create bookmarks to resources on available UNIX file shares.
  - **User can add bookmarks**—If enabled, users can view and create bookmarks to resources on available UNIX file shares.
  - **Allow automount shares**—If enabled, users access to automount shares specified on a NIS server.
3. Click **Save Changes**.

**Related  
Documentation**

- [Defining General Windows File Browsing Options on page 570](#)

---

## Defining UNIX/NFS File Resource Policies

---

When you enable the File access feature for a role, you need to create resource policies that specify which Windows and UNIX/NFS resources a user may access, as well as the encoding to use when communicating with Windows and NFS file shares. When a user makes a file request, the Secure Access Service evaluates the resource policies corresponding to the request, such as Windows access resource policies for a request to fetch an MS Word document (.doc file). After matching a user's request to a resource listed in a relevant policy, the Secure Access Service performs the action specified for the resource.

You can create resource policies through the standard interface (as described in this section) or through resource profiles (recommended method).

When writing a File resource policy, you need to supply key information:

- **Resources**—A resource policy must specify one or more resources to which the policy applies. When writing a File policy, you need to specify File servers or specific shares.
- **Roles**—A resource policy must specify the roles to which it applies. When a user makes a request, the Secure Access Service determines what policies apply to the role and then evaluates those policies that correspond to the request.
- **Actions**—Each type of resource policy performs a certain action, which is either to allow or deny a resource or to perform or not perform some function, such as allow a user to write to a directory. You can also write detailed rules that apply more conditions to a user request.

The Secure Access Service engine that evaluates resource policies requires that the resources listed in a policy's Resources list follow a canonical format.

### Canonical Format: UNIX/NFS File Resources

When writing a resource policy for a UNIX/NFS file resource, you need to understand the following canonical format.

server[/path]

The two components are:

- Server (required)—Possible values:
  - Hostname—The system variable <username> may be used.
  - IP address—The IP address needs to be in the format: a.b.c.d
- Path (optional)—Special characters allowed include:

*	Matches any character
%	Matches any character except back slash (\)
?	Matches exactly one character

If the path is missing, then back slash (\) is assumed, meaning only top-level folders are matched. For example:

```
% .danastreet.net/share/users/<username>
* .juniper.com/dana/*
10.11.0.10/web/*
10.11.254.227/public/%.txt
```

**Related Documentation** • [Defining General File Writing Options on page 575](#)

## Writing UNIX/NFS Resource Policies

Information in this section is provided for backwards compatibility. We recommend that you configure access to UNIX file servers through resource profiles instead, since they provide a simpler, more unified configuration method.

To write a UNIX/NFS resource policy:

1. In the admin console, choose **Users > Resource Policies > Files > Access > Unix/NFS**.
2. On the UNIX/NFS File Access Policies page, click **New Policy**.
3. Enter a name to label this policy (required) and a description of the policy. (optional)
4. In the Resources section, specify the resources to which this policy applies.
5. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. In the Action section, specify:

- **Allow access**—To grant access to the resources specified in the Resources list. Check Read-only to prevent users from saving files on the server.
  - **Deny access**—To deny access to the resources specified in the Resources list.
  - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
7. Click **Save Changes**.
  8. On the UNIX/NFS File Access Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

**Related Documentation**

- [Creating a File Rewriting Resource Profile on page 563](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)

## Writing a UNIX/NFS Compression Resource Policy

Information in this section is provided for backwards compatibility. We recommend that you configure access to UNIX file servers through resource profiles instead, since they provide a simpler, more unified configuration method.

Compression policies specify which types of file data the Secure Access Service should compress when you enable GZIP compression through the Maintenance > System > Options page of the admin console.



**NOTE:** Gzip compression is not supported on the MAG Series Junos Pulse Gateways.

The Secure Access Service comes pre-equipped with two file compression policies (\*:\*/\*) which compress all applicable file data. You may enable these policies through the Resource Policies > Files > Compression pages of the admin console.

To write a UNIX/NFS file compression resource policy:

1. In the admin console, choose **Resource Policies > Files > Compression**.
2. Select the **Unix/NFS** tab.
3. Click **New Policy**.
4. Enter a name to label this policy (required) and a description of the policy. (optional)
5. In the Resources section, specify the resources to which this policy applies.
6. In the Roles section, specify:
  - **Allow access**—To grant access to the resources specified in the Resources list. Check Read-only to prevent users from saving files on the server.



- **Deny access**—To deny access to the resources specified in the Resources list.
  - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
7. In the Action section, specify:
    - **Compress**—The Secure Access Service compresses the supported content types from the specified resource.
    - **Do not compress**—The Secure Access Service does not compress the supported content types from the specified resource.
    - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
  8. Click **Save Changes**.

#### Related Documentation

- [Creating a File Rewriting Resource Profile on page 563](#)
- [Specifying Resources for a Resource Policy on page 145](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)

## Defining General UNIX/NFS File Writing Options

You can specify File resource options that apply to your File resource policies. When you enable a File resource policy option, the Secure Access Service compiles a list of host names specified in the Resources field of each File resource policy. The Secure Access Service then applies the enabled options to this comprehensive list of host names.

To specify options for UNIX/NFS resources:

1. In the admin console, choose **Users > Resource Policies > Files > Options**.
2. Select:
  - **IP based matching for Hostname based policy resources**—The Secure Access Service looks up the IP address corresponding to each host name specified in a File resource policy. When a user tries to access a server by specifying an IP address rather than the host name, the Secure Access Service compares the IP to its cached list of IP addresses to determine if a host name matches an IP. If there is a match, then the Secure Access Service accepts the match as a policy match and applies the action specified for the resource policy.  
This option does not apply to host names that include wildcards and parameters.
  - **Case sensitive matching for the Path component in File resources**—Select this option to require users to enter a case-sensitive URL to an NFS resource. Use this option when passing username or password data in a URL.



**NOTE:** This option does not apply to Windows servers.

- **Encoding**—Select the encoding to use for communicating with the Windows and NFS file shares.

- **NTLM Version**—Select whether to fall back to NTLM version 1 or version 2 authentication if Kerberos authentication of administrator credentials fails.
- **Number of NTLM authentication protocol**—Select **High** to allow a large number of authentication attempt to be made to the backend server. This applies only to NTLM, not basic authentication. If your server locks users out for too many failed attempts, select **Low**.



.....

**NOTE:** Many servers do not support the different NTLM protocol variant attempts when you select High. If you find that authentication is failing even though the username and password are correct, set this option to Low.

.....

3. Click **Save Changes**.

**Related  
Documentation**

- [About Basic, NTLM and Kerberos Resources on page 522](#)

## CHAPTER 23

# Secure Application Manager

- [Secure Application Manager Overview on page 584](#)
- [Task Summary: Configuring WSAM on page 584](#)
- [Launching VPN Tunneling During a WSAM Session on page 585](#)
- [Debugging WSAM Issues on page 586](#)
- [About WSAM Resource Profiles on page 586](#)
- [Creating WSAM Client Application Resource Profiles on page 587](#)
- [Creating WSAM Destination Network Resource Profiles on page 588](#)
- [Specifying Applications and Servers for WSAM to Secure on page 589](#)
- [Specifying Applications that Need to Bypass WSAM on page 591](#)
- [Specifying Role-Level WSAM Options on page 593](#)
- [Specifying Application Servers that Users Can Access on page 594](#)
- [Specifying Resource Level WSAM Options on page 596](#)
- [Using the WSAM Launcher on page 596](#)
- [JSAM Overview on page 600](#)
- [Task Summary: Configuring JSAM on page 601](#)
- [Using JSAM for Client/Server Communications on page 602](#)
- [Configuring a PC that Connects to the Secure Access Service Through a Proxy Web Server on page 607](#)
- [Determining the Secure Access Service-Assigned Loopback Address on page 607](#)
- [Configuring External DNS Servers and User Machines on page 608](#)
- [JSAM Linux and Macintosh Support on page 609](#)
- [Standard Application Support: MS Outlook on page 610](#)
- [Standard Application Support: Lotus Notes on page 612](#)
- [Configuring the Lotus Notes Client on page 613](#)
- [Standard Application Support: Citrix Web Interface for MetaFrame \(NFuse Classic\) on page 614](#)
- [Enabling Citrix Published Applications on the Citrix Native Client on page 614](#)
- [Enabling Citrix Secure Gateways on page 617](#)

- [Creating a JSAM Application Resource Profile on page 618](#)
- [Specifying Applications for JSAM to Secure on page 622](#)
- [Specifying Role Level JSAM Options on page 624](#)
- [Automatically Launching JSAM on page 625](#)
- [Specifying Application Servers that Users Can Access on page 627](#)
- [Specifying Resource Level JSAM Options on page 628](#)

## Secure Application Manager Overview

---

The Secure Application Manager option provides secure, application-level remote access to enterprise servers from client applications. You may deploy two versions of the Secure Application Manager:

- Windows version (WSAM)—The Windows version of the Secure Application Manager is a Windows-based solution that enables you to secure traffic to individual client/server applications and application servers.
- Java version (JSAM)—The Java version of the Secure Application Manager provides support for static TCP port client/server applications, including enhanced support for Microsoft MAPI, Lotus Notes, and Citrix NFuse. JSAM also provides NetBIOS support, which enables users to map drives to specified protected resources.

The Secure Application Manager features (WSAM and JSAM) are not available on the SA 700 appliance.

### Related Documentation

- [Task Summary: Configuring WSAM on page 584](#)
- [Task Summary: Configuring JSAM on page 601](#)

## Task Summary: Configuring WSAM

---

This section provides high-level WSAM configuration steps. These steps do not account for preliminary Secure Access Service configuration steps such as specifying the Secure Access Service's network identity or adding user IDs to the Secure Access Service.

To configure WSAM:

1. Create resource profiles that enable access to client/server applications or destination networks, create supporting autopolicies as necessary, and assign the policies to user roles using settings in the Users > Resource Profiles > SAM pages of the admin console.

We recommend that you use resource profiles to configure WSAM (as described above). However, if you do not want to use resource profiles, you can configure WSAM using role and resource policy settings in the following pages of the admin console instead:

- a. Enable access to WSAM at the role-level using settings in the Users > User Roles > Role > General > Overview page of the admin console.

- b. Specify which client/server applications and servers WSAM should intermediate using settings in the Users > User Roles > SAM > Applications page of the admin console.
  - c. Specify which application servers users can access through WSAM using settings in the Users > Resource Policies > SAM > Access page of the admin console.
2. After enabling access to client/server applications and/or destination networks using WSAM resource profiles or roles and resource policies, you can modify general role and resource options in the following pages of the admin console:
  - a. (Optional) Configure role-level options such as whether the Secure Access Service should automatically launch and upgrade WSAM using settings in the Users > User Roles > SAM > Options page of the admin console.
  - b. (Optional) Control IP based hostname matching at the resource level using settings in the Users > Resource Policies > SAM > Options page of the admin console.
3. Ensure that an appropriate version of WSAM is available to remote clients using settings in the Maintenance > System > Installers page of the admin console.
4. If you want to enable or disable client-side logging for WSAM, configure the appropriate options through the System > Configuration > Security > Client-side Logs tab of the admin console.

**Related Documentation**

- [About WSAM Resource Profiles on page 586](#)
- [Specifying Resource Level WSAM Options on page 596](#)
- [User Roles Overview on page 105](#)
- [Specifying Applications and Servers for WSAM to Secure on page 589](#)
- [Downloading Application Installers on page 813](#)
- [About Client-Side Logs on page 948](#)

## Launching VPN Tunneling During a WSAM Session

Users can launch VPN Tunneling while signed in to the Secure Access Service via WSAM. If they do, however, the VPN Tunneling installer automatically terminates the WSAM session prior to launching VPN Tunneling. During the process, the Secure Access Service prompts users with a warning message informing them that they are about to terminate their WSAM session in favor of launching VPN Tunneling.

To deal with situation, we recommend that you give users as much access to network resources through VPN Tunneling as through WSAM. If you do, when the users choose to launch VPN Tunneling (simultaneously terminating WSAM), they will still be able to access the same network resources.

**Related Documentation**

- [Launching VPN Tunneling During a Windows Secure Application Manager Session on page 749](#)

## Debugging WSAM Issues

---

You can use the Secure Application Manager dialog box on the an end-user's system to view the WSAM status and a variety of details about the user's session. For instance, the Secure Application Manager dialog box displays the applications and servers that WSAM is configured to secure, event logs and Winsock data for the user's session, and various system diagnostics and performance data. This information can help you or a Juniper Networks Support representative debug any problems your users may encounter.

To access the Secure Application Manager dialog box, users simply need to double-click the WSAM icon on their Windows task bars:



For more information about viewing information in the Secure Application Manager dialog box, see the end-user help system available from the Help link in the Secure Access Service end-user console.

### Related Documentation

- [Task Summary: Configuring WSAM on page 584](#)

## About WSAM Resource Profiles

---

You can create two types of WSAM resource profiles:

- WSAM application resource profiles—These resource profiles configure WSAM to secure traffic to a client/server application. When you create a WSAM application resource profile, the WSAM client intercepts requests from the specified client applications to servers in your internal network.
- WSAM destination network resource profiles—These resource profiles configure WSAM to secure traffic to a server. When you create a WSAM destination network resource profile, the WSAM client intercepts requests from processes running on the client that are connecting to the specified internal hosts.

When creating WSAM resource profiles, note that the resource profiles do not contain bookmarks. To access the applications and servers that WSAM intermediates, users must first launch WSAM and then launch the specified application or server using standard methods (such as the Windows Start menu or a desktop icon).

When you enable JSAM or WSAM through Web rewriting autopolicies in the Users > Resource Profiles > Web Applications/Pages page of the admin console, the Secure Access Service automatically creates JSAM or WSAM autopolicies for you. You can only view these SAM policies through the appropriate Web resource profile—not through the SAM resource profile pages of the admin console.

### Related Documentation

- [Resource Profiles on page 127](#)
- [Task Summary: Configuring WSAM on page 584](#)
- [Defining a Rewriting Autopolicy on page 506](#)

- [Enabling WSAM on PDAs on page 1169](#)

## Creating WSAM Client Application Resource Profiles

---

When you create a WSAM application resource profile, the WSAM client intercepts requests from the specified client applications to servers in your internal network.

To create a WSAM application resource profile:

1. In the admin console, choose **Users > Resource Profiles > SAM > Client Applications**.
2. Click **New Profile**.
3. From the Type list, choose **WSAM**.
4. From the Application list, select one of the following options:
  - **Custom**—When you select this option, you must manually enter your custom application's executable file name (such as telnet.exe). Additionally, you may specify this file's path and MD5 hash of the executable file (although it is not required that you specify the exact path to the executable). If you enter an MD5 hash value, WSAM verifies that the checksum value of the executable matches this value. If the values do not match, WSAM notifies the user that the identity of the application could not be verified and does not forward connections from the application to the Secure Access Service.
  - **Lotus Notes**—When you select this option, WSAM intermediates traffic from the Lotus Notes fat client application.
  - **Microsoft Outlook**—When you select this option, WSAM intermediates traffic from the Microsoft Outlook application.
  - **NetBIOS file browsing**—When you select this option, WSAM intercepts NetBIOS name lookups in the TDI drivers on port 137.
  - **Citrix**—When you select this option, WSAM intermediates traffic from Citrix applications.

You can only use WSAM to configure access to a standard application once per user role. For example, you can enable one configuration of Microsoft Outlook and one configuration of Lotus Notes for the "Users" role.

The Secure Access Service supports several mechanisms for intermediating traffic to the Lotus Notes, Microsoft Outlook, and Citrix applications.

- **Domain Authentication**—Select this option to allow integrated Windows applications, such as file sharing, Outlook, and so forth to authenticate to the domain controller when the client machine is part of a domain. Before using this option, you must:
  - Specify domain controllers that are reachable through the Secure Access Service in the WSAM Destination list so that LDAP and Kerberos traffic can be proxied and sent to the Secure Access Service.
  - Configure a WSAM Access Control Policy (ACL) to allow access to all domain controllers.

5. Enter a unique name and optionally a description for the resource profile. The Secure Access Service displays this information in the Client Application Sessions section of the Secure Access Service end-user home page.
6. In the Autopolicy: SAM Access Control section, create a policy that allows or denies users access to the server that hosts the specified application:
  - a. If it is not already enabled, select the **Autopolicy: SAM Access Control** checkbox.
  - b. In the Resource field, specify the application server to which this policy applies. You can specify the server as a host name or an IP/netmask pair. You may also include a port.  
  
If you select Domain Authentication from the Application list, enter your domain controller server addresses into the Resource field. You can add multiple domain controller servers if more than one is available.  
  
When enabling auto-policy for any client application for WSAM, avoid entering \*\* in the resource list since the access control policies are not restricted to that particular application. This may result in other resources being accessed through client applications for which the access control policies are not defined.
  - c. From the Action list, select **Allow** to enable access to the specified server or **Deny** to block access to the specified server.
  - d. Click **Add**.
7. Click **Save and Continue**.
8. In the Roles tab, select the roles to which the resource profile applies and click Add.  
  
The selected roles inherit the autopolicy created by the resource profile. If it is not already enabled, the Secure Access Service also automatically enables the SAM option in the Users > User Roles > Select Role > General > Overview page of the admin console for all of the roles you select.
9. Click **Save Changes**.

#### Related Documentation

- [Creating Resource Profiles Using the Lotus iNotes Template on page 477](#)
- [Creating Resource Profiles Using the Microsoft OWA Template on page 481](#)
- [Comparing Secure Access Access Mechanisms for Configuring Citrix on page 468](#)

## Creating WSAM Destination Network Resource Profiles

When you create a WSAM destination network resource profile, the WSAM client intercepts requests from processes running on the client to internal hosts.



**NOTE:** When destinations (using either IP address or hostnames) are configured on the Secure Access Service, all DNS and NetBIOS names are resolved through the Secure Access Service.



To create a WSAM destination network resource profile:

1. In the admin console, choose **Users > Resource Profiles > SAM > WSAM Destinations**.
2. Click **New Profile**.
3. Enter a unique name and optionally a description for the resource profile.
4. In the WSAM Destinations section, specify which servers you want to secure using WSAM and click **Add**. You can specify the servers as hostname or IP/netmask pairs. You may also include a port.
5. Select the Create an access control policy allowing SAM access to this server checkbox to enable access to the server specified in the previous step (enabled by default).
6. Click **Save and Continue**.
7. In the Roles tab, select the roles to which the resource profile applies and click Add.

The selected roles inherit the autopolicy created by the resource profile. If it is not already enabled, the Secure Access Service also automatically enables the SAM option in the Users > User Roles > *Role Name* > General > Overview page of the admin console for all of the roles you select.

#### Related Documentation

- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)

## Specifying Applications and Servers for WSAM to Secure

Information in this section is provided for backwards compatibility. We recommend that you secure traffic using WSAM resource profiles instead, since they provide a simpler, more unified configuration method.

Use the Applications tab to specify applications and servers for which WSAM secures traffic. When WSAM downloads to a client PC, it contains the information you configure on the Applications tab for the role. After a user launches the Secure Application Manager, WSAM intercepts requests from client applications to servers in your internal network and requests from processes running on the client to internal hosts. You define these resources on the Applications tab by configuring two lists:

- WSAM supported applications list—This list contains applications for which you want WSAM to secure client/server traffic between the client and the Secure Access Service.
- WSAM allowed servers list—This list contains hosts for which you want WSAM to secure client/server traffic between the client and the Secure Access Service.

To specify applications for which WSAM secures client/server traffic between the client and the Secure Access Service:

1. In the admin console, choose **Users > User Roles > Select Role > SAM > Applications**.
2. Click **Add Application**.

3. Enter the name of the application and, optionally, a description. This information displays in the Client Application Sessions section of the Secure Access Service end-user home page.
4. From the Type list, choose one of the following options:
  - **Standard**—If you select this option, choose one the following applications from the Application Parameters section:
    - **Citrix**—When you select this option, WSAM intermediates traffic from Citrix applications.
    - **Lotus Notes**—When you select this option, WSAM intermediates traffic from the Lotus Notes fat client application.
    - **Microsoft Outlook/Exchange**—When you select this option, WSAM intermediates traffic from the Microsoft Outlook application.

- **NetBIOS file browsing**—When you select this option, WSAM intercepts NetBIOS name lookups in the TDI drivers on port 137.

Note that in order to access a share using WSAM with NetBIOS, you need to explicitly specify the server's NetBIOS name (alphanumeric string up to 15 characters) in two places: on the Add Server page and in a SAM resource policy. (Wildcards are currently not supported.) Alternatively, you can enable the Auto-allow application servers option on the SAM > Options tab, and then the Secure Access Service automatically creates a SAM resource policy that allows access to this server.

- **Custom**—Select this option to specify a custom client/server application. Then:
    - a. In the Filename field, specify the name of the file's executable file.
    - b. Optionally specify the file's path and MD5 hash of the executable file. If you enter an MD5 hash value, WSAM verifies that the checksum value of the executable matches this value. If the values do not match, WSAM notifies the user that the identity of the application could not be verified and does not forward connections from the application to the Secure Access Service.
5. Click **Save Changes** or **Save + New**.
  6. Configure a WSAM resource policy to specify to which enterprise resources (based on IP address/port combination) the Secure Access Service may send the application.

### Specifying Servers for WSAM to Secure

To specify servers for which WSAM secures client/server traffic between the client and the Secure Access Service:

1. In the admin console, choose **Users > User Roles > Select Role > SAM > Applications**.
2. Click **Add Server**.
3. Enter the name of the server and, optionally, a description.
4. Specify the server's host name (the wild cards '\*' or '?' are accepted) or an IP/netmask pair. Specify multiple ports for a host as separate entries.

5. Click **Save Changes** or **Save + New**.
6. Configure a WSAM resource policy to specify to which enterprise resources (based on IP address/port combination) the Secure Access Service may send a server request.

Alternatively, you can enable the Auto-allow application servers option on the SAM > Options tab, and then the Secure Access Service automatically creates a SAM resource policy that allows access to the specified server. Note that you need to enable this option before specifying the application or server; otherwise, you need to create a SAM resource policy.

#### Related Documentation

- [Creating Resource Profiles Using the Lotus iNotes Template on page 477](#)
- [Creating Resource Profiles Using the Microsoft OWA Template on page 481](#)
- [Comparing Secure Access Access Mechanisms for Configuring Citrix on page 468](#)
- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)

## Specifying Applications that Need to Bypass WSAM

The WSAM client comes pre-configured with a list of “passthrough” applications bypass WSAM. The WSAM client does not secure traffic for these applications. In addition to bypassing these pre-defined applications, you may also specify additional applications on the Secure Access Service that should bypass WSAM.



**NOTE:** WSAM does not bypass applications on Pocket PCs and other handheld devices.

To specify applications for WSAM to secure:

1. In the admin console, choose **Users > User Roles > Select Role > SAM > Applications**.
2. Click **Add Bypass Application**. The New Bypass Application page displays.
3. Name the application and provide a description (optional).
4. Provide the file name (required).
5. Enter the absolute path to the application (optional).
6. Select **Save Changes** to add the bypass application to the list or **Save + New** to save the bypass application and create another bypass application.

#### Default Bypass Applications

The WSAM client is pre-configured to bypass WSAM processing for the following applications:

- apache.exe
- apache\*
- licadmin.exe

- vni.exe
- lmgrd.exe
- TNSLSD.EXE
- ORACLE.EXE
- Agntsvc.exe
- ONRSD.EXE
- Pagntsv.exe
- ENCSVC.EXE
- Agntsvc.exe
- sqlplus.exe
- sqlplusw.exe
- EiSQLW.exe
- Sqlservr.exe
- Sqlmangr.exe
- inetinfo.EXE
- svchost.exe
- LSASS.EXE
- CSRSS.EXE
- WINLOGON.EXE
- SERVICES.EXE
- spoolsv.exe
- hostex32.exe
- xstart.exe
- idsd.exe
- dsTermServ.exe
- dsCitrixProxy.exe
- dsNcService.exe
- dsNetworkConnect.exe

**Related  
Documentation**

- [Specifying Applications and Servers for WSAM to Secure on page 589](#)

## Specifying Role-Level WSAM Options

To specify WSAM options at the role level:

1. In the admin console, choose **Users > User Roles > Select Role > SAM > Options**.
2. If it is not already enabled, select the Windows SAM option at the top of the page.
3. Under Secure Application Manager options, configure the following options:
  - **Auto-launch Secure Application Manager**—If you enable this option, the Secure Access Service automatically launches the Secure Application Manager when a user signs in. If you do not select this option, users must manually start the Secure Application Manager from the Client Applications Sessions section of the Secure Access Service end-user home page.

Although you configure the Secure Application Manager to automatically launch when users sign into the Secure Access Service, users can override this setting through the Preferences > Applications page of the Secure Access Service end-user console. If you or the end-user disables WSAM from automatically launching, users need to manually start the Secure Application Manager by clicking its link on the Secure Access Service home page.

- **Auto-allow application servers**—If you enable this option, the Secure Access Service automatically creates a SAM resource policy that allows access to the server specified in the WSAM application and server lists.

You may not see the Auto-allow option if you are using a new installation or if an administrator hides the option.

4. Under Windows SAM Options, configure the following options:
  - **Auto-uninstall Secure Application Manager**—If you enable this option, the Secure Access Service automatically un-installs the Secure Application Manager after users sign off.
  - **Prompt for username and password for intranet sites**—If you enable this option, the Secure Access Service requires users to enter their sign-in credentials before connecting to sites on your internal network. This option changes Internet Explorer's intranet zone setting so that Internet Explorer prompts the user for network sign-in credentials whenever the user wants to access an intranet site.
  - **Auto-upgrade Secure Application Manager**—If you enable this option, the Secure Access Service automatically downloads the Secure Application Manager to a client machine when the version of Secure Application Manager on the Secure Access Service is newer than the version installed on the client. If you select this option, note the following:
    - The user must have Administrator privileges in order for the Secure Access Service to automatically install Secure Application Manager on the client.
    - If a user un-installs Secure Application Manager and then signs in to the Secure Access Service for which the Auto-upgrade Secure Application Manager option is not enabled, the user no longer has access to Secure Application Manager.

- **Resolve only host names with domain suffixes in the device DNS domains**—If this option is configured, WSAM filters DNS requests (FQDNs) and sends to Secure Access Service only those DNS requests that have a domain suffix in the list of DNS Domains configured on the Network Overview page. This option is limited to resolution of FQDNs only. No filtering is applied to short names and NetBIOS requests.
- **Session start script and Session end script**—If you want to run a batch, application, or Win32 service file when the WSAM session starts or ends, enter the name and path for the file. For example, if you want to terminate an application and then restart it, you may use PSKILL.exe (an third-party utility that terminates processes on local or remote systems).

If you enable the Session start script option or Session end script option, note the following:

- You must either install the specified file on your end-user's computers or specify a path on an accessible network directory.
- To ensure that the Secure Access Service can locate a file on different platforms, you can use Windows variables, such as in a path such as %WINDIR%\system32\log.
- The file must invoke the WSAM launcher using the appropriate command-line options.

5. Click **Save Changes**.

**Related Documentation**

- [Using the WSAM Launcher on page 596](#)

---

## Specifying Application Servers that Users Can Access

---

Information in this section is provided for backwards compatibility. We recommend that you secure traffic using WSAM resource profiles instead, since they provide a simpler, more unified configuration method.

When you enable the Secure Application Manager access feature for a role, you need to create resource policies that specify which application servers a user may access. These policies apply to both the Java version and Windows version of the Secure Application Manager (JSAM and WSAM, respectively). When a user makes a request to an application server, the Secure Access Service evaluates the SAM resource policies. If the Secure Access Service matches a user's request to a resource listed in a SAM policy, the Secure Access Service performs the action specified for the resource.

When writing a SAM resource policy, you need to supply key information:

- **Resources**—A resource policy must specify one or more resources to which the policy applies. When writing a SAM policy, you need to specify application servers to which a user may connect.
- **Roles**—A resource policy must specify the roles to which it applies. When a user makes a request, the Secure Access Service determines what policies apply to the role and

then evaluates those policies that correspond to the request. SAM resource policies apply to users requests made through either version, JSAM or WSAM.

- **Actions**—A Secure Application Manager resource policy either allows or denies access to an application server.

You can create resource policies through the standard interface (as described in this section) or through resource profiles (recommended method).

The Secure Access Service's engine that evaluates resource policies requires that the resources listed in a policy's Resources list follow a canonical format.

To write a Secure Application Manager resource policy:

1. In the admin console, choose **Users > Resource Policies > SAM > Access**.
2. On the Secure Application Manager Policies page, click **New Policy**.
3. Enter a name to label this policy (required) and a description of the policy (optional).
4. In the Resources section, specify the application servers to which this policy applies.
5. In the Roles section, specify:
  - **Policy applies to ALL roles**—Choose this option to apply this policy to all users.
  - **Policy applies to SELECTED roles**—Choose this option to apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—Choose this option to apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. In the Action section, specify:
  - **Allow socket access**—Choose this option to grant access to the application servers specified in the Resources list.
  - **Deny socket access**—Choose this option to deny access to the application servers specified in the Resources list.
  - **Use Detailed Rules**—Choose this option to specify one or more detailed rules for this policy.
7. Click **Save Changes**.
8. On the Secure Application Manager Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

**Related  
Documentation**

- [About WSAM Resource Profiles on page 586](#)
- [Specifying Resources for a Resource Policy on page 145](#)

## Specifying Resource Level WSAM Options

Use the Options tab to specify the SAM resource option to match IP addresses to host names specified as resources in your SAM resource policies. When you enable this option, the Secure Access Service looks up IP addresses corresponding to each host name specified in a SAM resource policy. When a user tries to access a server by specifying an IP address rather than the host name, the Secure Access Service compares the IP to its cached list of IP addresses to determine if a host name matches an IP. If there is a match, then the Secure Access Service accepts the match as a policy match and applies the action specified for the resource policy.

When you enable this option, the Secure Access Service compiles a list of host names specified in the Resources field of each SAM resource policy. The Secure Access Service then applies the option to this comprehensive list of host names.



**NOTE:** This option does not apply to host names that include wildcards and parameters.

To specify the SAM resource option:

1. In the admin console, choose **Users > Resource Policies > SAM > Options**.
2. Select **IP based matching for Hostname based policy resources**. When you select this option, the Secure Access Service looks up the IP address corresponding to each host name specified in a Secure Application Manager resource policy. When a user tries to access a server by specifying an IP address rather than the host name, the Secure Access Service compares the IP to its cached list of IP addresses to determine if a host name matches an IP. If there is a match, then the Secure Access Service accepts the match as a policy match and applies the action specified for the resource policy.
3. Click **Save Changes**.

**Related Documentation**

- [Task Summary: Configuring WSAM on page 584](#)

## Using the WSAM Launcher

The WSAM launcher (samlauncher.exe) is a tool that signs a user into the Secure Access Service and then downloads and launches WSAM. The launcher provides a command-line interface that a script or application can call. For example, you can write an application that calls the WSAM executable when needed.

To use the WSAM launcher, you need to:

1. Write a script, batch file, service, or application that calls the WSAM launcher using command line arguments. You need to distribute this file to each client PC that requires it.



2. Download the WSAM launcher from Maintenance > System > Installers page of the admin console and then distribute it to your users.

Use the command-line arguments in the following table to invoke the WSAM launcher.

**Table 45: WSAM Command Line Arguments**

Argument	Action
-start	Initiates the WSAM connection.
-stop	Terminates the WSAM connection.
-signout	Terminates the WSAM connection and Secure Access Service user session.
-version	Displays WSAM version information and then exits.
-help	Displays available arguments.
-noupgrade	Cancels automatic upgrade of WSAM software.
-reboot	Automatically reboots if prompted by an upgrade. If reboot flag is not set, WSAM exits and does not reboot during an upgrade. Be sure to set the reboot flag if WSAM is operating automatically on a remote PC.
-u <i>username</i>	Specifies the user name.
-p <i>password</i>	Specifies the password for authentication.
-loginscript file	Specifies the location and name of the script file to run when WSAM launches. This command takes precedence over a script file specified on the Users > User Roles > <i>Role Name</i> > SAM > Options page.
-postsript file	Specifies the location and name of the script file to run when WSAM exits. This command takes precedence over a script file specified on the Users > User Roles > <i>Role Name</i> > SAM > Options page.
-c <i>certificateName</i>	Specifies the certificate submitted by the user for authentication. Note that the user can only use this option if a valid SSL certificate is installed on the Secure Access Service. If the Secure Access Service uses a self-signed certificate, the user must import that certificate into his browser.
-u <i>URL</i>	Specifies the sign-in URL for the Secure Access Service.
-r <i>realm</i>	Specifies the realm to which the Secure Access Service submits the user's credentials.
-verbose	Prompts users for input through dialog boxes.



**NOTE:** samlauncher does not support secondary authentication.

The following table lists the possible codes the WSAM launcher returns when it exits.

Code	Description
0	Success
1	Invalid argument
2	Could Not Connect.
3	Invalid Credentials
4	Role Not Specified (credentials map to multiple roles)
5	Pre-authentication Error (Host Checker or Cache Cleaner did not load)
6	Installation Failed
7	Reboot Required (if '-reboot' not specified)
8	Unable to perform a required software upgrade
10	Feature not supported
12	Failed to authenticate the client certificate
100	Unable to stop the Secure Application Manager
101	Unable to start the Secure Application Manager due to a software conflict caused by another Layered Service Provider

### Running Scripts Manually

Users may manually specify scripts to run when a WSAM session begins or ends using the following command-line arguments.

If you specify scripts to run through the Users > User Roles > *Role Name* > SAM > Options page of the admin console, the configured script does not run if a user manually invokes WSAM using the launcher and specifies a different script.

To manually launch a script after a WSAM session begins:

- At a command prompt, enter `-loginscript file` followed by a system variable or script file name and location.

To manually launch a script after a WSAM session ends:

- At a command prompt, enter `-postscript file` followed by a system variable and the script file name and location.

Place system variables, file paths, and file names in quotes. Precede and append system variables with a percent sign (%)

For example:

```
-loginscript file "%program files%\Internet Explorer\IEXPLORER.EXE"
```

### Running Scripts Automatically

You may automatically run a script when WSAM starts or stops by entering the script path and name in the Session start script field or Session end script field on the Users > User Roles > *Role Name* > SAM > Options page of the admin console. This section includes an example batch file that you can automatically launch.

The following example shows how to use the WSAM launcher to invoke WSAM. This sample batch file generates error messages when WSAM launches:

```
SamLauncher -start -url %1 -user %2 -password %3 -realm %4
if errorlevel 1 goto error_invalid_args
if errorlevel 2 goto error_connect
if errorlevel 3 goto error_credentials
if errorlevel 4 goto error_role
if errorlevel 5 goto error_preauth
if errorlevel 6 goto error_install
if errorlevel 7 goto error_reboot
```

```
:error_invalid_args
@echo invalid arguments
goto done
```

```
:error_connect
@echo could not connect
goto done
```

```
:error_credentials
@echo invalid credentials
goto done
```

```
:error_role
@echo invalid role
goto done
```

```
:error_preauth
@echo pre auth version checking
goto done
```

```
:error_install
@echo install failed
goto done
```

```
:error_reboot
@echo reboot required
```

```

goto done

:error_success
@echo Secure Application Manager has started
goto done

:done

```

Win32 API example

```

CHAR szCmd = "SamLauncher.exe -stop";
DWORD dwExitCode = 0;
STARTUPINFO si;
PROCESS_INFORMATION pi;
ZeroMemory(&si, sizeof(si));
si.cb = sizeof(si);
ZeroMemory(&pi, sizeof(pi));
if (!CreateProcess(NULL, szCmd, NULL, NULL, FALSE,
0, NULL, NULL, &si, &pi)) {
 printf("CreateProcess(%s) failed %d", szCmd, GetLastError());
 return -1;
}
WaitForSingleObject(pi.hProcess, 20000);
GetExitCodeProcess(&pi.hProcess, &dwExitCode);
CloseHandle(pi.hProcess);
CloseHandle(pi.hThread);
printf("SamLauncher return %d\n", dwExitCode);
return 0;

```

If you are using Windows Vista, open the command window as an administrator user. Standard output from the SamLauncher.exe does not display if the command window is opened by a user without administrator privileges.

#### Related Documentation

- [Task Summary: Configuring WSAM on page 584](#)

## JSAM Overview

The Java version of the Secure Application Manager provides support for static TCP port client/server applications, including enhanced support for Microsoft MAPI, Lotus Notes, and Citrix NFuse. JSAM also provides NetBIOS support, which enables users to map drives to specified protected resources.

JSAM works well in many network configurations but does not support dynamic port TCP-based client/server applications, server-initiated connections, or UDP traffic.



**NOTE:** regedit.exe is required for some JSAM functionality. If regedit.exe is disabled, automatic host mapping and the NetBIOS and Outlook/Exchange applications will not work properly.

For information about the operating systems, Web browsers, and JVMs on which Juniper Networks supports JSAM, see the *Supported Platforms Guide* on the Juniper Networks Customer Support Center.

- Related Documentation**
- [Task Summary: Configuring JSAM on page 601](#)
  - [JSAM Linux and Macintosh Support on page 609](#)

## Task Summary: Configuring JSAM

---

This topic provides high-level JSAM configuration steps. These steps do not account for preliminary Secure Access Service configuration steps such as specifying the Secure Access Service's network identity or adding user IDs to the Secure Access Service.

To configure JSAM:

1. Create resource profiles that enable access to client/server applications, create supporting autopolicies as necessary, and assign the policies to user roles using settings in the Users > Resource Profiles > SAM pages of the admin console.

We recommend that you use resource profiles to configure JSAM (as described above). However, if you do not want to use resource profiles, you can configure JSAM using role and resource policy settings in the following pages of the admin console:

- a. Enable access to JSAM at the role-level using settings in the Users > User Roles > Select Role > General > Overview page of the admin console.
  - b. Specify which client/server applications JSAM should intermediate using settings in the Users > User Roles > SAM > Applications page of the admin console.
  - c. Specify which application servers users can access through JSAM using settings in the Users > Resource Policies > SAM > Access page of the admin console.
2. After enabling access to client/server applications using JSAM resource profiles or roles and resource policies, you can modify general role and resource options in the following pages of the admin console:
    - a. (Optional) Configure role-level options such as whether the Secure Access Service should automatically launch JSAM using settings in the Users > User Roles > SAM > Options page of the admin console.
    - b. (Optional) Control IP based hostname matching at the resource level using settings in the Users > Resource Policies > SAM > Access page of the admin console.
  3. If you want to enable or disable client-side logging for JSAM, configure the appropriate options through the System > Configuration > Security > Client-side Logs tab of the admin console.
  4. If you have multiple internal domains, such as company-a.com and company-b.com, add DNS domains to the Secure Access Service using settings in the System > Network > Overview page of the admin console so that names such as app1.company-a.com and app2.company-b.com resolve correctly.

5. If a remote user's PC is set up to use a Web proxy in Internet Explorer, configure the client machine to bypass the proxy server when the user launches applications that need to connect to the Secure Application Manager.
6. Enable JSAM to associate IP loopback addresses with application servers on specific ports either by enabling JSAM to edit the hosts file on your users' systems or by creating an external DNS to route client application traffic to the JSAM applet.

**Related  
Documentation**

- [Using JSAM for Client/Server Communications on page 602](#)
- [JSAM Linux and Macintosh Support on page 609](#)
- [Creating a JSAM Application Resource Profile on page 618](#)
- [Specifying Applications for JSAM to Secure on page 622](#)
- [Specifying Role Level JSAM Options on page 624](#)
- [Automatically Launching JSAM on page 625](#)
- [Specifying Resource Level JSAM Options on page 628](#)
- [User Roles Overview on page 105](#)
- [Specifying Application Servers that Users Can Access on page 627](#)
- [Configuring a PC that Connects to the Secure Access Service Through a Proxy Web Server on page 607](#)
- [Configuring External DNS Servers and User Machines on page 608](#)

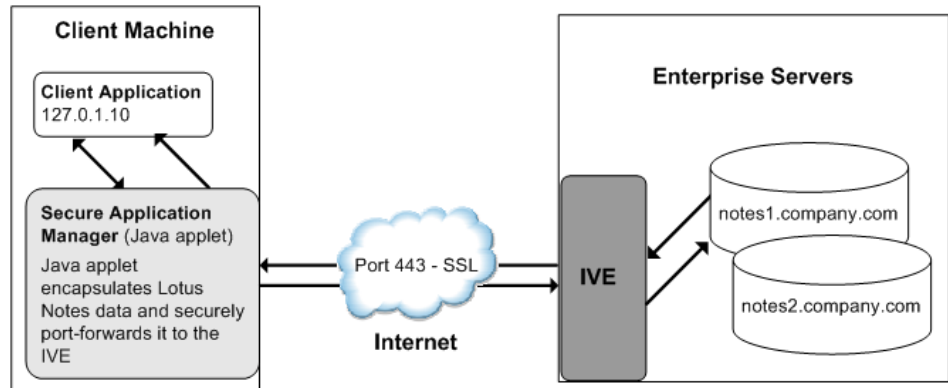
## Using JSAM for Client/Server Communications

---

JSAM provides secure port forwarding by directing client application traffic to the JSAM applet running on a client machine. To the client application running on the local machine, JSAM appears as the application server. To the application server in your network, the Secure Access Service appears as the client application.

The following diagram illustrates the interaction between a client application and its server via the Secure Access Service. (This figure assumes that the user specified a localhost IP address as the server in the client application.)

Figure 40: Java Secure Application Manager



1. The user starts a client application listed in the Client Application Sessions section of the Secure Access Service end-user home page. The application resolves the remote server to localhost.
2. The client application connects to JSAM running on the user's machine and starts sending requests.
3. JSAM encapsulates and forwards all client requests to the Secure Access Service over SSL.
4. The Secure Access Service un-encapsulates the client data and forwards it to the specified application server.
5. The application server responds with data to the Secure Access Service.
6. The Secure Access Service encapsulates and forwards the response from the application server to JSAM over SSL.
7. JSAM un-encapsulates the application server data and forwards it to the client application.

A status indicator on the JSAM window shows the current state of JSAM. If green, JSAM is working correctly. If red, JSAM is unable to send/receive requests to/from the Secure Access Service.

The JSAM window updates the status indicator only when traffic is passed through JSAM. If no traffic is passed through JSAM, the status indicator remains in its current state. For example, if there is a network outage or if the user's session times out, the status indicator remains green even though it cannot send/receive requests to/from the Secure Access Service.

Note the following:

- If a remote user's PC is set up to use a Web proxy in Internet Explorer, you must configure the client machine to bypass the proxy server when the user launches applications that need to connect to the Secure Application Manager.
- JSAM allocates 20-30 MB of RAM when running (the exact amount of memory depends on the Java Virtual Machine (JVM) used) and, if caching is enabled, may leave a .jar file

on the client machine. For more information about files left by JSAM on client machines, see the Client-side Changes Guide on the Juniper Networks Customer Support Center.

- Users may experience problems waiting for the Secure Application Manager to fully load if they enable pop-up blockers through their Web browsers. This problem occurs because a pop-up window alerting users to accept the Secure Application Manager plug-in may appear in the background (behind the Web browser window) where users cannot see it.
- When launching applications through JSAM, Juniper Networks supports configuration of 1200 unique IP/port combinations on Windows and Mac and 800 unique IP/port combinations on Linux. Note that this limit is based on IP/port combinations, not applications (which may listen on more than one IP address and port). Juniper Networks determined these numbers by testing on Windows XP and Windows 2000 machines using default JRE memory settings.

## Assigning IP Loopback Addresses to Servers

For JSAM to function, it must listen on loopback addresses for client requests to network application servers. The Secure Access Service assigns these unique IP loopback address to each application server that you specify for a given port. For example, if you specify:

app1.mycompany.com, app2.mycompany.com, app3.mycompany.com,...

for a single port, the Secure Access Service assigns a unique IP loopback address to each application:

127.0.1.10, 127.0.1.11, 127.0.1.12,...

When the Secure Access Service installs JSAM on a user's machine, JSAM listens on the loopback addresses (on the corresponding client port specified for the application server) for client requests to network application servers. You can configure the Secure Access Service to dynamically assign these loopback addresses, or you can configure static loopback addresses yourself through the admin console.

You must enable these associations between IP loopback addresses and applications servers on a specific port in one of two ways:

- Allow the Secure Access Service to edit the hosts file on the client system with IP loopback assignments. The Secure Access Service makes a copy of the current hosts file and then creates a new hosts file with the IP loopback assignments. When the user ends the session, the Secure Access Service deletes the new hosts file and restores the original hosts file.

If the client system shuts down unexpectedly, the hosts file still points the client to loopback addresses for outside connections. Settings in the hosts file are returned to their original state when the client system reboots.

Users must have the proper privileges on their machines in order for the Secure Access Service to edit the hosts file.

- Create an external DNS to route client application traffic to the JSAM applet.



## Using Static Loopback Addresses

Using an external DNS server with dynamic loopback addresses requires an administrator to update the DNS settings each time the JSAM application configuration changes. On the other hand, configuring an external DNS server using static loopback addresses provides administrators with the highest degree of configuration control. For example, consider the following IP loopback assignments:

```
app1.mycompany.com - 127.0.1.10
app2.mycompany.com - 127.0.1.11
app3.mycompany.com - 127.0.1.12
```

If you configure an external DNS server using dynamic loopback address assignments and you delete the first application server, the address assignments change:

```
app2.mycompany.com - 127.0.1.10
app3.mycompany.com - 127.0.1.11
```

With static IP loopback addresses in an external DNS, deleting the first application server does not affect the IP loopback assignments for the remaining application servers:

```
app2.mycompany.com - 127.0.1.11
app3.mycompany.com - 127.0.1.12
```

You can assign static IP loopback addresses when creating a JSAM custom resource profile through the Users > Resource Profiles > SAM > Client Applications page of the admin console or when enabling JSAM applications through the Users > User Roles > Select Role > SAM > Applications page of the admin console.

If you assign a static IP loopback address while creating a new application, the Secure Access Service checks the address for conflicts against other configured applications in the same role. If another application uses the same address, the Secure Access Service displays an error message prompting you to enter a different IP address.



**NOTE:** Static IP loopback addresses apply only to application servers configured by an administrator. The Secure Access Service assigns dynamic IP loopback addresses for user-defined application servers. If the administrator does not assign an IP loopback address to an application server, the Secure Access Service assigns a dynamic address.

## IP Loopback Address Considerations When Merging Roles

### IP Loopback Address Considerations When Merging Roles

- If two or more roles map to the same application and each mapping contains a different static IP loopback address, all of the static IP loopback addresses remain unchanged.
- If two or more roles map to the same application and only one role uses a static IP loopback address, JSAM uses only the static IP loopback address and binds to only one statically defined socket on the client.

- If two or more roles map to the same application using dynamic IP loopback addresses, only one dynamic IP loopback address is used. The application listener binds to only one dynamically assigned socket on the client.
- If you use the same host name in multiple roles, either use the same static IP loopback address, or dynamic addresses for all the applications.
- If you use different host names associated with the same loopback address and port combination, JSAM cannot distinguish between the two different hosts at the back-end and, hence, cannot accurately direct IP traffic bound for those hosts.

## Resolving Host Names to Localhost

For JSAM to successfully intermediate traffic, a client application on the user's machine needs to resolve the application server to the client localhost. This process enables JSAM to capture and securely port forward the data intended for the application server via the Secure Access Service. JSAM can perform automatic host-mapping, in which it edits the client's hosts file, to map application servers to localhost. (You can enable automatic host-mapping through the Users > User Roles > Select Role > SAM > Options page of the admin console.)

In order for JSAM to edit a user's hosts file, the user must have the appropriate authority on the client machine:

- Windows users using the FAT file system may belong to any user group. For Exchange MAPI support, however, users must have at least Power User privileges on their machines.
- Windows users using the NTFS file system must have Administrator privileges on their machines.
- Linux (RedHat) users must launch the browser that will launch JSAM as root.
- Macintosh users must supply the Administrator password when prompted by JSAM.

If users do not have the appropriate privileges on their machines, JSAM cannot automatically edit the hosts file, preventing host name resolution to localhost.

Alternatives for users who do not have the appropriate privileges are:

- You configure your external DNS server to resolve application servers to localhost. If you configure your external DNS server to use a localhost address instead of the application server host name, remote users need to configure the order in which their machine searches DNS servers to start with the corporate DNS.
- You relax the permissions on the etc directory and the etc\hosts file to enable JSAM to make the necessary modifications.
- Users configure a client application to use the localhost address assigned by the Secure Access Service where they typically specify the application server host name in the client application.

### Related Documentation

- [Task Summary: Configuring JSAM on page 601](#)

## Configuring a PC that Connects to the Secure Access Service Through a Proxy Web Server

If a remote user's PC is set up to use a Web proxy in Internet Explorer, you must configure the client machine to bypass the proxy server and contact the Secure Application Manager instead.

To configure a PC that connects to the Secure Access Service through a Web proxy in Internet Explorer:

1. From the Internet Explorer Tools menu, choose **Internet Options**.
2. On the Connections tab, click the **LAN Settings** button.
3. Under Proxy server, click the **Advanced** button.
4. Under Exceptions, enter the addresses for which you do not want to use a proxy server. Enter all addresses (host names and localhost) that the client application uses when connecting through the Secure Application Manager. For example:

If your application server is `app1.company.com`, enter the following exceptions:

`app1;app1.company.com;127.0.0.1`

If your Exchange Server is `exchange.company.com`, enter the following exceptions:

`exchange;exchange.company.com;127.0.0.1`



**NOTE:** Secure Access Service clients parse Internet Explorer's static proxy exception list. We support most exceptions that Internet Explorer supports with the following limitations:

- For IP address exception, we support `n.*.*`, `n.n.*`, `n.n.n.*`. For example, `10.*.*`, `10.10.*`, `10.10.10.*`, or `10.10.10.10`. We do not support `10*` or `10.*10.*` even though Internet Explorer may support them.
- For string expression, we support specific strings such as `my.company.net`, or a wild card at front of the string, for example, `*.my.company.net` or `*.company.net`. We do not support `*.company.*`, `*.company*`, `*.company.*.com`, `*.net`, `*.com` and so forth.

## Determining the Secure Access Service-Assigned Loopback Address

Users cannot modify the corporate DNS server for applications they add for port forwarding. If you allow users to specify applications for JSAM to proxy, users need to configure a client application to use the localhost address assigned by the Secure Access Service where they typically enter the server host name.

The Details pane of the JSAM browser window displays the loopback IP address assigned by the Secure Access Service along with the port specified by the user. To determine what IP address the Secure Access Service assigns to an application specified through

the Client Applications page, a user must restart the Secure Application Manager after adding the application. The loopback address assigned to the application appears on the Details pane of the Secure Application Manager browser window.

In the client application, the user needs to enter the Secure Access Service-assigned loopback address as the application server. For example, if a user wants to access a telnet server behind your corporate firewall, the user needs to follow these steps:

1. In the Client Application Sessions section of the Secure Access Service end-user home page, click the **Item Properties** icon, then click **Add Application**
2. On the Add Application page, specify:
  - The server's fully qualified domain name or IP address in the Remote Server field, such as terminalserver.juniper.com.
  - The port on which JSAM should listen for client traffic to the server in the Client Port field, such as 3389.
  - The port on which the remote server should listen for traffic from the client application (JSAM) in the Server Port field, such as 3389.
3. Click **Add** to save the information.
4. Close the Secure Application Manager browser window.
5. In the Client Application Sessions section of the Secure Access Service end-user home page, click **Start** to restart the Secure Application Manager.
6. In the Secure Application Manager browser window, click Details.
7. On the Details tab, look at which loopback address the Secure Access Service assigned to the remote server, such as 127.0.1.18.
8. In the client application, such as Remote Desktop Connection, specify the loopback address in the configuration field for the server. This field appears in different places for different applications. Users may enter this information through a setup wizard or other configuration dialog.

**Related Documentation** • [Task Summary: Configuring JSAM on page 601](#)

---

## Configuring External DNS Servers and User Machines

---

Client applications must resolve server host names to JSAM, which proxies data between a client and a server. On Windows PCs, server host names are stored in the hosts file. To intercept data using JSAM, the server names in the hosts file need to resolve to the local machine (localhost) so that the Secure Access Service can intermediate the traffic. The recommended process for mapping application servers to a user's local PC is to enable the automatic host-mapping option, which enables the Secure Access Service to automatically modify the PC hosts file to point application servers to the localhost for secure port forwarding.

For the Secure Access Service to perform automatic host-mapping, however, PC users must have the proper privileges on their machines. If your PC users do not have these

privileges, you must ensure that your internal application server names resolve externally to a PC's localhost by adding entries to your external Internet-facing DNS server such as:

```
127.0.0.1 app1.company-a.com
127.0.0.1 app2.company-b.com
127.0.0.1 exchange1.company-a.com
127.0.0.1 exchange1.company-b.com
```

If the client application uses an unqualified name for the application server, users need to specify DNS suffixes so that the PC can attach the suffix and contact your external DNS server for name resolution. For example, an MS Outlook client typically has an unqualified name for an MS Exchange server. In order for the qualified name to resolve to 127.0.0.1, users need to specify the appropriate DNS suffixes on their PCs. Adding domain names does not affect other operations on the PC, including use of the client application from within the enterprise.

To configure a user PC with DNS suffixes (Windows 2000):

1. From the Windows Start menu, choose **Settings > Network and Dial-up Connections > Local Area Connection** and then choose **Properties**.
2. Select **Internet Protocol (TCP/IP)** and then click **Properties**.
3. Click **Advanced** and then click the **DNS** tab.
4. Click **Append these DNS suffixes** and then click **Add**.
5. Add your enterprise's internal domains as additional DNS suffixes.

**Related Documentation**

- [JSAM Overview on page 600](#)

## JSAM Linux and Macintosh Support

Linux users do not have access to ports below 1024 unless they are signed into their machines as root. Macintosh users do not have access to ports below 1024 unless they supply the Administrator password when prompted by JSAM. To support applications that run on privileged ports (ports below 1024), such as a telnet application:

- Users may launch the browser that will launch JSAM as root.
- You or the user may specify a client port number equal to or greater than port 1024 when enabling client applications.

For example, if you specify 2041 for the client port and 23 for the server port for a telnet application, the command to run the application is:

```
telnet loopbackIP 2041
```

where loopbackIP is the loopback IP address assigned to the application server by the Secure Access Service. JSAM listens on port 2041 for traffic from the telnet application and forwards it to the Secure Access Service. The Secure Access Service then forwards the traffic to port 23 on the destination server.



**NOTE:** Due to the design of the Sun JVM code, Macintosh users cannot relaunch JSAM within the same Safari user session. In order to re-launch JSAM, the user must exit Safari and then launch JSAM again.

---

**Related Documentation**

- [Task Summary: Configuring JSAM on page 601](#)

## Standard Application Support: MS Outlook

---

Remote users can use the Microsoft Outlook client on their PCs to access email, their calendars, and other Outlook features through the Secure Access Service. Versions of MS Outlook currently supported are MS Outlook 2000 and MS Outlook 2002. This ability does not require changes to the Outlook client and does not require a network layer connection, such as VPN.

Refer to the Supported Platforms Document on the Juniper Networks Customer Support Center for details on operating system support and dependencies. See Client-Side Changes for details about registry changes made by JSAM.

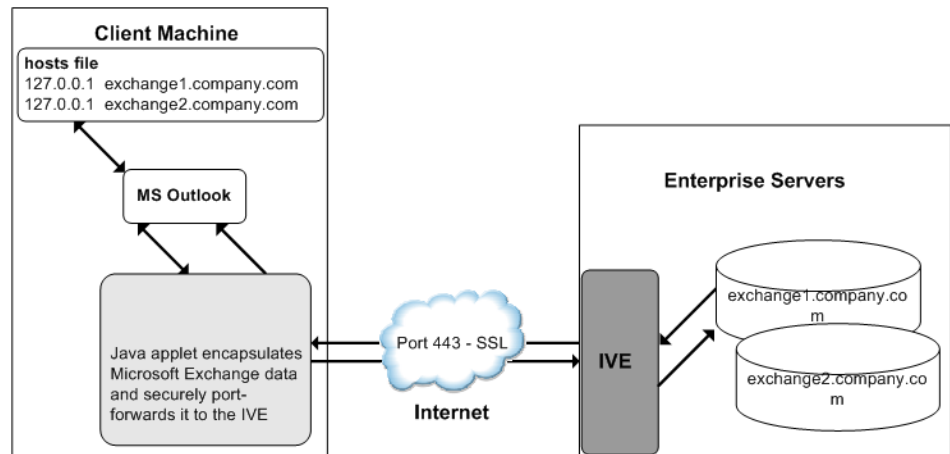
Also, note that the Secure Access Service does not support Outlook through SVW, since Outlook applications require HKLM registry key changes.

In order for this feature to work for remote users, the network settings of the user's PC must resolve the name of the Exchange Servers embedded in the Outlook client to the local PC (127.0.0.1, the default localhost IP address). We recommend that you configure the Secure Access Service to automatically resolve Exchange server host names to the localhost by temporarily updating the hosts file on a client computer through the automatic host-mapping option.

### Client/Server Communication Using JSAM

The following diagram describes the interactions between the Outlook client and an Exchange Server via the Secure Access Service. This figure assumes that the Secure Access Service is configured to perform automatic host-mapping.

**Figure 41: Java Secure Application Manager and Enhanced MS Exchange Support**



The above figure shows the Secure Access Service configured to use automatic host-mapping for the MS Outlook client.

1. The user starts the MS Outlook client. Outlook tries to contact the Exchange Server `exchange1.yourcompany.com`. The Secure Access Service resolves the Exchange Server host name to `127.0.0.1` (localhost) through temporary changes to the hosts file.
2. Outlook connects to the Secure Application Manager running on the user's PC and then starts sending requests for email.
3. The Secure Application Manager encapsulates and forwards all the requests from the Outlook client to the Secure Access Service over SSL.
4. Secure Access Service un-encapsulates the client data and looks in the MAPI request to find the target Exchange Server. The request is then forwarded to the target server.
5. Each request in the MAPI protocol encodes the target server for the request. When MAPI requests arrive from the Secure Application Manager, the Secure Access Service looks in each of them and dispatches them to the appropriate target server. This process works transparently even if there are multiple Exchange Servers.
6. The Exchange Server responds to the Secure Access Service with email data.
7. The Secure Access Service encapsulates and forwards the response from the Exchange Server to the Secure Application Manager over SSL.
8. The Secure Application Manager un-encapsulates the information sent from the Secure Access Service and forwards the normal MAPI response from the Exchange Server to the Outlook client.

**Related Documentation**

- [Enabling the Secure Virtual Workspace on page 437](#)

## Standard Application Support: Lotus Notes

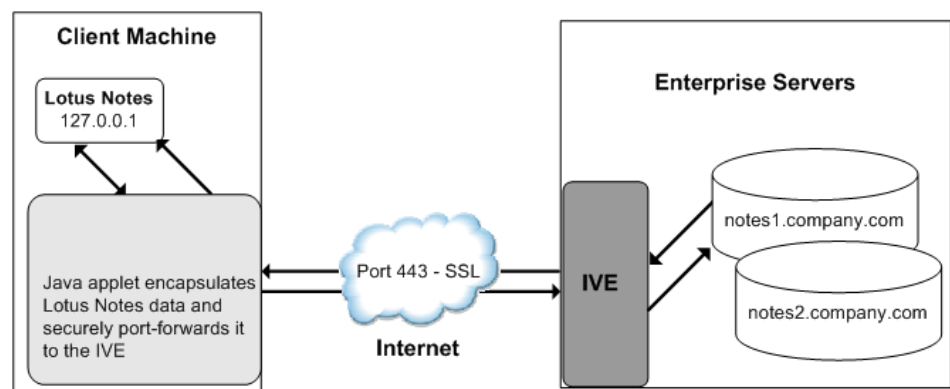
Remote users can use the Lotus Notes client on their PCs to access e-mail, their calendars, and other features through the Secure Access Service. This ability does not require a network layer connection, such as a VPN.

See the *Supported Platforms Document* at Junos Pulse Secure Access Service for details on operating system support and dependencies.

### Client/Server Communication Using JSAM

In order for this feature to work for remote users, they need to configure the Lotus Notes client to use “localhost” as their location setting (that is, their Home Location, Remote Location, or Travel Location setting). The Secure Application Manager then picks up connections requested by the Lotus Notes client. The following diagram describes the interactions between the Lotus Notes client and a Lotus Notes Server via the Secure Access Service.

**Figure 42: Java Secure Application Manager and Enhanced Lotus Notes Support**



The above figure shows the Lotus Notes client location value to be configured to the localhost.

1. The user starts the Lotus Notes client with the location setting. The client uses the HTTP Tunnel proxy setting for its location setting. Note that you must set the HTTP Tunnel proxy setting to use localhost (or 127.0.0.1) as the proxy address and 1352 as the proxy port.
2. The Lotus Notes client connects to the Secure Application Manager and starts sending requests for email.
3. The Secure Application Manager encapsulates and forwards requests from the Lotus Notes client to Secure Access Service over SSL.
4. The Secure Access Service un-encapsulates the client data and looks in the Lotus Notes request to find the target Lotus Notes Server. The request is then forwarded to the target server.



Each request in the Lotus Notes protocol encodes the target server for the request. When Lotus Notes requests arrive from the application proxy, the Secure Access Service obtains the target server information from the requests and dispatches the requests to the appropriate target server. Thus, this feature works transparently even if there are multiple Lotus Notes Servers accessed by a single user. Note that you must create JSAM ACLs on the Secure Access Service that enable access to these target servers.

5. The Lotus Notes Server responds with email data to the Secure Access Service.
6. The Secure Access Service encapsulates and forwards the response from the Lotus Notes Server to the Secure Application Manager over SSL.
7. The Secure Application Manager un-encapsulates the information sent from the Secure Access Service and forwards the normal response from the Lotus Notes Server to the Lotus Notes client.

**Related Documentation** • [Task Summary: Configuring JSAM on page 601](#)

## Configuring the Lotus Notes Client

Before a remote user can connect from Lotus Notes to a Lotus Notes Server through the Secure Access Service, the user must edit the Lotus Notes client to set a Location document Proxy field to the PC's localhost port. The Location document edited should be the one used for remote access, such as the Remote Location or Travel Location setting. Setting the Proxy field to the PC's localhost port enables the Secure Access Service to connect to multiple Lotus Notes Servers, including those set up as pass-through servers.

You should use the following configuration in these cases:

- JSAM is configured to use Lotus Notes as a standard application.
- The Lotus Notes client can connect to multiple Lotus Notes servers.

To configure a Lotus Notes client for use with the Secure Access Service:

1. From the Lotus Notes client, choose **File > Mobile > Locations**.
2. Select the Location used for remote access and then click **Edit Location**.
3. In the Basics tab, click the **Proxy** icon.
4. In the Proxy Server Configuration box, enter **127.0.0.1:1352** in the HTTP Tunnel field.
5. Click **OK**.

**Related Documentation** • [Standard Application Support: Lotus Notes on page 612](#)

## Standard Application Support: Citrix Web Interface for MetaFrame (NFuse Classic)

---

Remote users can use the Citrix Web Interface for MetaFrame server to access a variety of applications via the Secure Access Service. This process does not require any alterations to the user permissions on the client.

After a user browses to a Citrix Web Interface for MetaFrame server and selects an application, the server sends an ICA file to the client. When the Secure Access Service rewrites the ICA file, it replaces host names and IP addresses with pre-provisioned loopback IP addresses. The ICA client then sends application requests to one of the loopback IP addresses. The Secure Application Manager encapsulates the data and sends it to the Secure Access Service. The Secure Access Service un-encapsulates the data and sends it to the appropriate MetaFrame server using port 1494 or 2598 (depending on the client)

Note the following:

- The Secure Access Service supports several mechanisms for intermediating traffic between a Citrix server and client, including the Terminal Services, JSAM, WSAM, VPN Tunneling, and hosted Java applets features.
- JSAM does not automatically launch when Embedded Applications are set to "Auto" in the Citrix Web Interface for MetaFrame console. In these cases, we recommend that you configure JSAM to automatically launch after the user signs into the Secure Access Service. Otherwise, end-users must manually launch JSAM before using Citrix Web Interface for MetaFrame.
- If a user attempts to use the server discovery feature and then attempts to use application discovery, the application discovery process fails. To resolve this particular situation, shut down and restart Citrix Program neighborhood.
- The Secure Access Service serves as an alternative to deploying the Citrix Secure Gateway (CSG).
- To use the applet-mode of the Java client, make sure to enable Java applet support on the Users > User Roles > *Role Name* > Web > Options page of the admin console.
- If you set the Network Protocol setting in the Citrix Program Neighborhood client to TCP/IP, the Secure Access Service does not support the application through JSAM since the TCP/IP setting produces UDP traffic.

### Related Documentation

- [Comparing Secure Access Access Mechanisms for Configuring Citrix on page 468](#)
- [Enabling Citrix Published Applications on the Citrix Native Client on page 614](#)

## Enabling Citrix Published Applications on the Citrix Native Client

---

When enabling Citrix published applications on the Citrix native client through the Secure Access Service, you must complete the following steps:

1. Specify custom application on JSAM to port forward.

2. Configure the Citrix metaframe server for published applications.
3. Configure the Citrix client for published applications.

Note the following:

- These instructions assume that you are not using the Citrix Web Interface for Citrix Presentation Server (formerly known as Nfuse server).
- These instructions do not cover how to configure the standard Citrix application option. (For standard Citrix application instructions, use settings in the Users > Resource Profiles > Web > Web Applications/Pages page of the admin console.) You can enable both the standard Citrix application and the custom Citrix application—these settings do not impact each other.
- The Secure Access Service supports several mechanisms for intermediating traffic between a Citrix server and client, including the Terminal Services, JSAM, WSAM, VPN Tunneling, and hosted Java applets features.

### Specifying Custom Applications on JSAM to Port Forward

When configuring JSAM to work with published applications, you must open 2 ports—ports 80 and 1494. Each opened port creates a connection through JSAM to the Citrix Metaframe server.

To specify published applications for JSAM to port forward:

1. Add a custom application through JSAM. When adding the custom application, keep the following settings in mind:
  - Server name—For published applications, you must enter the Metaframe server's fully qualified DNS name, not its IP address.
  - Server port—For published applications, enter 80 and 1494. (Create one entry for port 80 and another for port 1494.) If you have multiple Metaframe servers, you must configure all of them on the same ports.
  - Client port—For published applications, enter 80 and 1494. (Create one entry for port 80 and another for port 1494.)
2. If you have multiple internal domains, such as company-a.com and company-b.com, add DNS domains to the Secure Access Service using settings in the System > Network > Overview page of the admin console so that names such as app1.company-a.com and app2.company-b.com resolve correctly.
3. If a remote user's PC is set up to use a Web proxy in Internet Explorer, configure the client machine to bypass the proxy server when the user launches applications that need to connect to the Secure Application Manager.
4. Enable JSAM to associate IP loopback addresses with application servers on specific ports either by enabling JSAM to edit the hosts file on your users' systems or by creating an external DNS to route client application traffic to the JSAM applet.
- 5.

### Configuring the Citrix Metaframe Server for Published Applications

When enabling Citrix published applications through the Secure Access Service, you must enable the XML service DNS address resolution on the metaframe server. The following instructions describe how to do this on Metaframe XP.

To configure the Citrix metaframe server to work with the Secure Access Service:

1. Open the Citrix Management Console.
2. Right-click on the name of your server farm and click **Properties**.
3. Select the **MetaFrame Settings** tab.
4. Select the **Enable XML Service DNS address resolution** checkbox.
5. Click **OK**.

### Configuring the Citrix Client for Published Applications

When enabling Citrix published applications through the Secure Access Service, you must create an ICA connection on each Citrix client using the instructions that follow.

To configure the Citrix client to work with the Secure Access Service:

1. Open the Citrix Program Neighborhood and choose the **Add ICA Connection** option.
2. In the Add New ICA Connection wizard, select the connection type that your computer uses to communicate.
3. In the next screen:
  - a. Enter a description of the new ICA Connection.
  - b. Select **TCP/IP + HTTP** as the network protocol.
  - c. Select **Published Application**.
  - d. Click **Server Location**, and then:
    - i. Deselect the **Use Default** checkbox.
    - ii. Click **Add** in the Locate Server or Published Application dialog box.
    - iii. Confirm that HTTP/HTTPS is selected from the Network Protocol list.
    - iv. Enter the metaframe server DNS in the Add Server Location Address dialog box.
    - v. Enter **80** in the port field.
    - vi. Click **OK** in the Add Server Location Address dialog box and the Locate Server or Published Application dialog box.
  - e. Select an application from the Published Application list.
4. Enter information in the remaining wizard screens as prompted.

#### Related Documentation

- [Configuring a PC that Connects to the Secure Access Service Through a Proxy Web Server on page 607](#)

## Enabling Citrix Secure Gateways

When enabling Citrix secure gateways (CSGs) through the Secure Access Service, you must:

1. Disable Citrix NFuse as a standard application through the Users > Resource Profiles > Web > Web Applications/Pages page of the admin console.



**NOTE:** You cannot enable the Citrix NFuse standard application and Citrix Secure Gateways (CSGs) custom applications through JSAM on the same Secure Access Service.

The Secure Access Service supports several mechanisms for intermediating traffic between a Citrix server and client, including the Terminal Services, JSAM, WSAM, VPN Tunneling, and hosted Java applets features.

2. Specify applications for JSAM to port forward by adding a custom application through JSAM. When adding the custom application, keep the following settings in mind:
  - Server name—For CSGs, you must enter the Citrix secure gateway server's fully qualified DNS name, not its IP address.
  - Server port—For CSGs, enter 443. If you have multiple Citrix secure gateway servers, you must configure all of them on the same port.
  - Client port—For CSGs, enter 443. (Create one entry for port 80 and another for port 443.)
3. If you have multiple internal domains, such as company-a.com and company-b.com, add DNS domains to the Secure Access Service using settings in the System > Network > Overview page of the admin console so that names such as app1.company-a.com and app2.company-b.com resolve correctly.
4. If a remote user's PC is set up to use a Web proxy in Internet Explorer, configure the client machine to bypass the proxy server when the user launches applications that need to connect to the Secure Application Manager.
5. Enable JSAM to associate IP loopback addresses with application servers on specific ports either by enabling JSAM to edit the hosts file on your users' systems or by creating an external DNS to route client application traffic to the JSAM applet.
6. Setup your Citrix Secure Gateway and confirm that it works on your desktop.
7. Add a bookmark to the end-users' home page that points to the list of Citrix secure gateway servers and use the Secure Access Service's Selective Rewrite feature to turn off rewriting for the URL.

Or, if you do not want to create a bookmark through the Secure Access Service, simply instruct users to access the URL using their Web browser's address bar instead of the Secure Access Service address bar.

- Related Documentation**
- [Configuring a PC that Connects to the Secure Access Service Through a Proxy Web Server on page 607](#)

## Creating a JSAM Application Resource Profile

---

JSAM resource profiles configure JSAM to secure traffic to a client/server application. When you create a JSAM application resource profile, the JSAM client tunnels network traffic generated by the specified client applications to servers in your internal network.

When creating JSAM resource profiles, note that the resource profiles do not contain bookmarks. Therefore, end-users will not see a link for the configured application in the end-user interface. To access the applications and servers that JSAM intermediates, users must first launch JSAM and then launch the specified application using standard methods (such as the Windows Start menu or a desktop icon).

Also note that when you enable JSAM or WSAM through rewriting autopolicies for Web resource profiles, the Secure Access Service automatically creates JSAM or WSAM autopolicies for you. You can only view these SAM policies through the appropriate Web resource profile—not through the SAM resource profile pages of the admin console.

To create a JSAM application resource profile:

1. In the admin console, choose **Users > Resource Profiles > SAM > Client Applications**.
2. Click **New Profile**.
3. From the Type list, choose **JSAM**.
4. From the Application list, select one of the following options.

- **Custom**—Select this option to intermediate traffic to a custom application. Then:
  - a. In the Server name field, enter the name or IP address of the remote server. If you are using automatic host mapping, enter the server as it is known to the application. If you enter an IP address, note that end-users must connect to JSAM using that IP address in order to connect to the specified server.
  - b. In the Server Port field, enter the port on which the remote server listens for client connections. For example, to forward Telnet traffic from a remote machine, specify port 23 for both the client port (on which JSAM listens) and the server port (on which the Telnet server listens).

To disable the registry change made by JSAM and restore the original copy of the etc/hosts file, users must uninstall the JSAM client using settings in the Preferences > Applications page of the end-user console. To re-enable the change, they need to reboot.

You can also use the restore system settings script. However, the restore system settings script cannot restore the hosts file successfully if you log in as a different user from the one that originally launched JSAM.

- c. In the Client Loopback IP field, provide a static loopback address. If you do not provide a static IP loopback address, the Secure Access Service assigns an IP loopback address dynamically.

When configuring an external DNS, do not use IP loopback addresses in the 127.0.2.x range because the Secure Access Service reserves IP loopback addresses in that range for use with Citrix NFuse.

If you want to modify a static loopback address for a JSAM application server configured on multiple ports, you must delete all applications referring to this application server and re-enter these applications with the new static loopback address.

- d. In the Client Port field, enter the port on which JSAM should listen for client application connections. Typically, the local port value is the same value as the server port; the local port value usually only differs for Linux or Macintosh non-root users who want to add applications for port forwarding that use ports under 1024.

You may configure more than one application on a single port, such as app1.mycompany.com, app2.mycompany.com, app3.mycompany.com. Either you assign a static loopback address or the Secure Access Service assigns a dynamic loopback address (127.0.1.10, 127.0.1.11, 127.0.1.12) to each application. JSAM then listens on these multiple loopback addresses on the specified port. For example, when there is traffic on 127.0.1.12 on the specified port, the Secure Access Service forwards the traffic to the app3.mycompany.com destination host.

- e. Click **Add**.
- f. Select the **Allow JSAM to dynamically select an available port if the specified client port is in use** checkbox if JSAM is listening for multiple hosts on the same port

and you want JSAM to select an available port when the client port you specify is taken. The client application must allow you to specify the port number for the connection in order to use this option.

- g. Select the **Create an access control policy allowing SAM access to these servers** checkbox to enable access to the list of servers specified in the Server column (enabled by default).
- **Lotus Notes**—Select this option to intermediate traffic from the Lotus Notes fat client application. Then, in the Autopolicy: SAM Access Control section, create a policy that allows or denies users access to the Lotus Notes server:
  - a. If it is not already enabled, select the **Autopolicy: SAM Access Control** checkbox.
  - b. In the Resource field, specify the application server to which this policy applies. You can specify the server as a fully-qualified host name or an IP/netmask pair. For example, if the fully-qualified hostname is notes1.yourcompany.com, add notes1.yourcompany.com and notes1 to the Resource field.
  - c. From the Action list, select **Allow** to enable access to the specified server or **Deny** to block access to the specified server.
  - d. Click **Add**.



**NOTE:** If you select the Lotus Notes option, or you configure the Lotus Notes client to connect to multiple Lotus Notes servers, you should configure the Lotus Notes client appropriately to work with the Secure Access Service.

You can only use JSAM to configure access to one Lotus Notes application per user role.

- **Microsoft Outlook**—Select this option to intermediate traffic from the Microsoft Outlook application. Then:
  - a. Enter the hostname for each MS Exchange server in the Servers field. For example, if the fully-qualified hostname is exchange1.yourcompany.com, add exchange1.yourcompany.com to the Servers field. For information about system variables and attributes you can use in this field, see “Using System Variables in Realms, Roles, and Resource Policies” on page 1069.

You must enter the full name of the servers in this field since the Secure Access Service creates direct one-to-one mappings between the servers you enter here and IP addresses in the etc/hosts file. For more information about registry changes made by JSAM, see the *Client-side Changes Guide* on the Juniper Networks Customer Support Center.

The Secure Access Service does not support Outlook through SVW, since Outlook applications require HKLM registry key changes.



- b. Select the **Create an access control policy allowing SAM access to this server** checkbox to enable access to the server specified in the previous step (enabled by default).



**NOTE:** You can only use JSAM to configure access to one Microsoft Outlook application per user role.

- **NetBIOS file browsing**—Select this option to tunnel NetBIOS traffic through JSAM. Then:

- a. Enter the fully-qualified host name for your application servers in the Servers field.

You must enter the full name of the servers in this field since the Secure Access Service creates direct one-to-one mappings between the servers you enter here and IP addresses in the etc/hosts file. For more information about registry changes made by JSAM, see the *Client-side Changes Guide* on the Juniper Networks Customer Support Center.

If you want to enable drive mapping on a Windows client machine, use the standard NetBIOS file browsing option. When you do, JSAM automatically modifies the registry to disable port 445 on Windows XP machines, which forces Windows XP to use port 137, 138, or 139 for drive-mapping. Windows XP users need to reboot one time to enable the registry change to take effect.

- b. Select the **Create an access control policy allowing SAM access to this server** checkbox to enable access to the server specified in the previous step (enabled by default).



**NOTE:** You can only use JSAM to configure NetBIOS file browsing once per user role.

The Secure Access Service does not support NetBIOS file browsing through SVW, since NetBIOS requires HKLM registry key changes.

- 5. Enter a unique name and optionally a description for the resource profile. The Secure Access Service displays this information in the Client Application Sessions section of the Secure Access Service end-user home page.

- 6. Click **Save and Continue**.

- 7. In the Roles tab, select the roles to which the resource profile applies and click Add.

The selected roles inherit the autopolicy created by the resource profile. If it is not already enabled, the Secure Access Service also automatically enables the SAM option in the Users > User Roles > *Role Name* > General > Overview page of the admin console for all of the roles you select.

- 8. Click **Save Changes**.

- Related Documentation**
- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)
  - [Configuring the Lotus Notes Client on page 613](#)
  - [Enabling the Secure Virtual Workspace on page 437](#)

## Specifying Applications for JSAM to Secure

---

Information in this section is provided for backwards compatibility. We recommend that you secure traffic using JSAM resource profiles instead, since they provide a simpler, more unified configuration method.

To specify applications for JSAM to secure:

1. In the admin console, choose **Users > User Roles > Select Role > SAM > Applications**.
2. Select **Add Application**.
3. Enter the name of the application and, optionally, a description. This information displays in the Client Application Sessions section of the Secure Access Service end-user home page.
4. Choose either:
  - **Standard application**—Select Citrix NFuse, Lotus Notes, or Microsoft Outlook/Exchange.

The Secure Access Service does not support the standard JSAM applications Outlook and Netbios file browsing through SVW, since these applications require registry key changes. However, the Secure Access Service does support the Citrix and Lotus Notes JSAM standard applications through SVW.

If you select the Lotus Notes option, or you configure the Lotus Notes client to connect to multiple Lotus Notes servers, you should configure the Lotus Notes client appropriately to work with the Secure Access Service.

The Secure Access Service supports several mechanisms for intermediating traffic to the Lotus Notes, Microsoft Outlook, and Citrix applications.

- **Custom application**
  - a. In the Server name field, enter the DNS name of the server or the server IP address. If entering the DNS name, enter name of the remote server as it is known to the application if you are using automatic host mapping.
  - b. Enter the server name.
  - c. In the Server Port field, enter the port on which the remote server listens for client connections.

For example, to forward Telnet traffic from a remote machine, specify port 23 for both the client port (on which JSAM listens) and the server port (on which the Telnet server listens).

To disable the registry change made by JSAM and restore the original copy of the etc/hosts file, users must uninstall the JSAM client using settings in the

Preferences > Applications page of the end-user console. To re-enable the change, they need to reboot.

You can also use the restore system settings script. However, the restore system settings script cannot restore the hosts file successfully if you log in as a different user from the one that originally launched JSAM.

- d. In the Client Loopback IP field, provide a static loopback address. If you do not provide a static IP loopback address, the Secure Access Service assigns an IP loopback address dynamically.

When configuring an external DNS, do not use IP loopback addresses in the 127.0.2.x range because the Secure Access Service reserves IP loopback addresses in that range for use with Citrix NFuse.

If you want to modify a static loopback address for a JSAM application server configured on multiple ports, you must delete all applications referring to this application server and re-enter these applications with the new static loopback address.

- e. In the Client Port field, enter the port on which JSAM should listen for client application connections.

Typically, the local port value is the same value as the server port; the local port value usually only differs for Linux or Macintosh non-root users who want to add applications for port forwarding that use ports under 1024.

You may configure more than one application on a single port, such as app1.mycompany.com, app2.mycompany.com, app3.mycompany.com. Either you assign a static loopback address or the Secure Access Service assigns a dynamic loopback address (127.0.1.10, 127.0.1.11, 127.0.1.12) to each application. JSAM then listens on these multiple loopback addresses on the specified port. For example, when there is traffic on 127.0.1.12 on the specified port, the Secure Access Service forwards the traffic to the app3.mycompany.com destination host.

- f. Select the **Allow Secure Application Manager to dynamically select an available port ...** checkbox if JSAM is listening for multiple hosts on the same port and you want JSAM to select an available port when the client port you specify is taken. The client application must allow you to specify the port number for the connection in order to use this option.
- g. Click **Add**.

5. If a remote user's PC is set up to use a Web proxy in Internet Explorer, configure the client machine to bypass the proxy server when the user launches applications that need to connect to the Secure Application Manager.
6. Add DNS domains to the Secure Access Service if you have multiple internal domains, such as company-a.com and company-b.com, so that names such as app1.company-a.com and app2.company-b.com resolve correctly:
  - a. In the admin console, choose **System > Network > Overview** .

- b. Under DNS Name Resolution, add a comma-separated list of domains in the to DNS Domains field.
- c. Click **Save Changes**.

**Related Documentation**

- [Creating a JSAM Application Resource Profile on page 618](#)
- [Enabling the Secure Virtual Workspace on page 437](#)
- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)
- [Configuring a PC that Connects to the Secure Access Service Through a Proxy Web Server on page 607](#)

## Specifying Role Level JSAM Options

---

To specify JSAM options at the role level:

1. In the admin console, choose **Users > User Roles > Select Role > SAM > Options**.
2. Under Secure Application Manager options, select the options to enable for users:
  - **Auto-launch Secure Application Manager**—If enabled, the Secure Access Service automatically launches the Secure Application Manager when a user signs in. If you do not select this option, users must manually start the Secure Application Manager from the Client Applications Sessions section of the Secure Access Service end-user home page.

Although you configure the Secure Application Manager to automatically launch when users sign into the Secure Access Service, users can override this setting through the Preferences > Applications page of the Secure Access Service end-user console. If disabled from automatically launching, users need to manually start the Secure Application Manager by clicking its link on the Secure Access Service home page.

- **Auto-uninstall Secure Application Manager**—If enabled, the Secure Access Service automatically un-installs the Secure Application Manager after users sign off.
- **Auto-allow application servers**—If enabled, the Secure Access Service automatically creates a SAM resource policy that allows access to the server specified in the WSAM application and server lists and the JSAM application list.

You may not see the Auto-allow option if you are using a new installation or if an administrator hides the option.

3. Under Java SAM Options, select the options to enable for users:

- **User can add applications**—If enabled, users can add applications. For users to add applications, they need to know the application server DNS name and client/server ports.

When you enable this option, users can set up port forwarding to any host or port in your enterprise. Before providing users with the ability to add applications, please verify that this feature is consistent with your security practices. If a user adds an application, the application remains available to the user even if you later change disable the feature.

- **Automatic host-mapping**—If enabled, the Secure Application Manager edits the Windows PC hosts file and replaces entries of Windows application servers with localhost. These entries are changed back to the original data when a user closes the Secure Application Manager.

For the Java version of the Secure Application Manager to work, the client application needs to connect to the local PC on which the Secure Application Manager is running as the application server. The recommended process for mapping application servers to a user's local PC is to enable automatic host-mapping, which enables the Secure Access Service to automatically modify the PC's hosts file to point application servers to the PC's localhost for secure port forwarding. Alternatively, you can configure your external DNS server.

- **Skip web-proxy registry check**—If enabled, JSAM does not check a user's registry for a Web proxy. Some users do not have permissions to look at their registries, so if JSAM tries to look at their registries, then users see an error that they do not have permission. This option ensures that users do not see this message.
- **Auto-close JSAM window on sign-out**—If enabled, JS-AM automatically closes when a user signs out of the Secure Access Service by clicking Sign Out in the Secure Access Service browser window. JSAM continues to run if the user simply closes the browser window.

4. Click **Save Changes**.

#### Related Documentation

- [Task Summary: Configuring JSAM on page 601](#)

## Automatically Launching JSAM

Use the Launch JSAM tab to write a Web resource policy that specifies a URL for which the Secure Access Service automatically launches JSAM on the client. The Secure Access Service launches JSAM in two scenarios:

- When a user enters the URL in the Address field of the Secure Access Service home page.
- When a user clicks a Web bookmark (configured by an administrator) on the Secure Access Service home page to the URL.

This feature is useful if you enable applications that require JSAM but don't want to require users to run JSAM unnecessarily. This feature requires, however, that users access

the URL through the Secure Access Service home page. If users enter the URL in a browser Address field, the Secure Access Service does not serve the request.

The Secure Access Service provides tight integration with Citrix. If you specify Citrix as a standard JSAM application, the Secure Access Service automatically launches JSAM when a user selects an ICA file even if the URL is not configured as a resource policy.

To write a Launch JSAM resource policy:

1. In the admin console, choose **Users > Resource Policies > Web**.
2. If your administrator view is not already configured to show Launch JSAM policies, make the following modifications:
  - a. Click the **Customize** button in the upper right corner of the page.
  - b. Select the **Launch JSAM** checkbox.
  - c. Click **OK**.
3. Select the **Launch JSAM** tab.
4. On the JSAM Autolaunch Policies page, click **New Policy**.
5. Enter a name to label this policy (required) and a description of the policy (optional).
6. In the Resources section, specify the URLs to which this policy applies.



**NOTE:** The resource policies configured for the JSAM auto launch policy must be a specific URL and not include wildcards. The URL should specify the entry point of the web application for which JSAM tunneling is needed.

7. In the Roles section, specify:
  - **Policy applies to ALL roles**—Choose this option to apply this policy to all users.
  - **Policy applies to SELECTED roles**—Choose this option to apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—Choose this option to apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
8. In the Action section, specify:
  - **Launch JSAM for this URL**—The Secure Access Service downloads the Java Secure Application Manager to the client and then serves the requested URL.  
  
JSAM launches automatically for the specified URL only if a user enters the URL or selects a bookmark to the URL on the Secure Access Service home page (Browsing > Bookmarks). The bookmark does not launch the application that is configured through JSAM, but launches JSAM itself.
  - **Don't Launch JSAM for this URL**—The Secure Access Service does not download the Java Secure Application Manager to the client for the requested URL. This option

is useful if you want to temporarily disable JSAM auto-launching for the specified URLs.

- **Use Detailed Rules**—To specify one or more detailed rules for this policy.

9. Click **Save Changes**.

**Related  
Documentation**

- [Task Summary: Configuring JSAM on page 601](#)

## Specifying Application Servers that Users Can Access

Information in this topic is provided for backwards compatibility. We recommend that you secure traffic using JSAM resource profiles instead, since they provide a simpler, more unified configuration method.

When you enable the Secure Application Manager access feature for a role, you need to create resource policies that specify which application servers a user may access. These policies apply to both the Java version and Windows version of the Secure Application Manager (JSAM and WSAM, respectively). When a user makes a request to an application server, the Secure Access Service evaluates the SAM resource policies. If the Secure Access Service matches a user's request to a resource listed in a SAM policy, the Secure Access Service performs the action specified for the resource.

When writing a SAM resource policy, you need to supply key information:

- **Resources**—A resource policy must specify one or more resources to which the policy applies. When writing a SAM policy, you need to specify application servers to which a user may connect.
- **Roles**—A resource policy must specify the roles to which it applies. When a user makes a request, the Secure Access Service determines what policies apply to the role and then evaluates those policies that correspond to the request. SAM resource policies apply to users requests made through either version, JSAM or WSAM.
- **Actions**—A Secure Application Manager resource policy either allows or denies access to an application server.

You can create resource policies through the standard interface (as described in this section) or through resource profiles (recommended method).

The Secure Access Service's engine that evaluates resource policies requires that the resources listed in a policy's Resources list follow a canonical format.

To write a Secure Application Manager resource policy:

1. In the admin console, choose **Users > Resource Policies > SAM > Access**.
2. On the Secure Application Manager Policies page, click **New Policy**.
3. Enter a name to label this policy (required) and a description of the policy (optional).
4. In the Resources section, specify the application servers to which this policy applies.
5. In the Roles section, specify:

- **Policy applies to ALL roles**—Choose this option to apply this policy to all users.
  - **Policy applies to SELECTED roles**—Choose this option to apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—Choose this option to apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. In the Action section, specify:
    - **Allow socket access**—Choose this option to grant access to the application servers specified in the Resources list.
    - **Deny socket access**—Choose this option to deny access to the application servers specified in the Resources list.
    - **Use Detailed Rules**—Choose this option to specify one or more detailed rules for this policy.
  7. Click **Save Changes**.
  8. On the Secure Application Manager Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

**Related  
Documentation**

- [Task Summary: Configuring JSAM on page 601](#)

## Specifying Resource Level JSAM Options

Use the Options tab to specify the SAM resource option to match IP addresses to host names specified as resources in your SAM resource policies. When you enable this option, the Secure Access Service looks up IP addresses corresponding to each host name specified in a SAM resource policy. When a user tries to access a server by specifying an IP address rather than the host name, the Secure Access Service compares the IP to its cached list of IP addresses to determine if a host name matches an IP. If there is a match, then the Secure Access Service accepts the match as a policy match and applies the action specified for the resource policy.

When you enable this option, the Secure Access Service compiles a list of host names specified in the Resources field of each SAM resource policy. The Secure Access Service then applies the option to this comprehensive list of host names.



**NOTE:** This option does not apply to host names that include wildcards and parameters.



To specify the SAM resource option:

1. In the admin console, choose **Users > Resource Policies > SAM > Options**.
2. Select IP based matching for Hostname based policy resources. When you select this option, the Secure Access Service looks up the IP address corresponding to each host name specified in a Secure Application Manager resource policy. When a user tries to access a server by specifying an IP address rather than the host name, the Secure Access Service compares the IP to its cached list of IP addresses to determine if a host name matches an IP. If there is a match, then the Secure Access Service accepts the match as a policy match and applies the action specified for the resource policy.
3. Click **Save Changes**.

**Related  
Documentation**

- [Task Summary: Configuring JSAM on page 601](#)



# Telnet/SSH

- [About Telnet/SSH on page 631](#)
- [Task Summary: Configuring the Telnet/SSH Feature on page 632](#)
- [Creating a Telnet/SSH Resource Profile on page 633](#)
- [Associating Bookmarks with Telnet/SSH Resource Profiles on page 634](#)
- [Configuring General Telnet/SSH Options on page 637](#)
- [Writing a Telnet/SSH Resource Policy on page 638](#)

## About Telnet/SSH

---

The Telnet/SSH option enables users to connect to internal server hosts in the clear using Telnet protocols or to communicate over an encrypted Secure Shell (SSH) session through a Web-based terminal session emulation. This feature supports the following applications and protocols:

- **Network Protocols**—Supported network protocols include Telnet and SSH.
- **Terminal Settings**—Supported terminal settings include VT100, VT320, and derivatives and screen buffers.
- **Security**—Supported security mechanisms include Web/client security using SSL and host security (such as SSH if desired).

You can create secure terminal session bookmarks that appear on the welcome page for users mapped to a specific role. A terminal session bookmark defines Terminal Session information for Telnet or SSH sessions that users may launch. These sessions give users access to a variety of networked devices, including UNIX servers, networking devices, and other legacy applications, that utilize terminal sessions. The Secure Access Service supports SSH versions V1 and V2 and uses the following SSH versions: OpenSSH\_2.9.9p1, SSH protocols 1.5/2.0, and OpenSSL 0x0090607f.

When communicating over an encrypted Secure Shell (SSH) session, note that the Telnet/SSH feature does not support using the ^J character combination. (Some applications use this character combination to justify text). If you want to use this character combination, we recommend that you find a java applet that supports it and upload that applet through the Secure Access Service using the hosted Java applets feature.

If you are using an SA700 Series Appliance, you must install a Core Clientless Access upgrade license in order to access the Telnet/SSH feature.

**Related  
Documentation**

- [Task Summary: Configuring the Telnet/SSH Feature on page 632](#)

---

## Task Summary: Configuring the Telnet/SSH Feature

---

To configure the Telnet/SSH feature:

1. Create resource profiles that enable access to Telnet and SSH servers, include bookmarks that link to those servers, and assign the bookmarks to user roles using settings in the Users > Resource Profiles > Telnet/SSH page of the admin console.

We recommend that you use resource profiles to configure Telnet/SSH (as described above). However, if you do not want to use resource profiles, you can configure Telnet/SSH using role and resource policy settings in the following pages of the admin console instead:

- Create resource policies that enable access to Telnet and SSH servers using settings in the Users > Resource Policies > Telnet/SSH > Sessions page of the admin console.
  - Determine which user roles may access the Telnet and SSH servers that you want to intermediate, and then enable Telnet/SSH access for those roles through the Users > User Roles > Select Role > General > Overview page of the admin console.
  - Create bookmarks to your Telnet and SSH servers using settings in the Users > User Roles > Select Role > Telnet/SSH > Access page of the admin console.
2. After configuring Telnet/SSH using resource profiles or roles and resource policies, you can modify general role and resource options in the following pages of the admin console:
    - (Optional) Enable users to create their own connections to Telnet and SSH sessions using settings in the Users > User Roles > Select Role > Telnet/SSH > Options page of the admin console.
    - (Optional) Enable the Secure Access Service to match IP addresses to host names and disable the auto-allow bookmarks option using settings in the Users > Resource Policies > Telnet/SSH > Options page of the admin console.

**Related  
Documentation**

- [About Telnet/SSH on page 631](#)
- [Creating a Telnet/SSH Resource Profile on page 633](#)
- [Associating Bookmarks with Telnet/SSH Resource Profiles on page 634](#)
- [Configuring General Telnet/SSH Options on page 637](#)
- [Writing a Telnet/SSH Resource Policy on page 638](#)

---

## Creating a Telnet/SSH Resource Profile

---

A Telnet/SSH resource profile is a resource profile that enables users to connect to internal server hosts in the clear using Telnet protocols or to communicate over an encrypted Secure Shell (SSH) session through a Web-based terminal session emulation.

To create a Telnet/SSH resource profile:

1. In the admin console, choose **Users > Resource Profiles > Telnet/SSH**.
2. Click **New Profile**.
3. From the Type list, specify the session type (Telnet or SSH) for this resource profile.
4. Enter a unique name and optionally a description for the resource profile. (This name becomes the default bookmark's name.)
5. In the Host field, enter the name or IP address of the server to which this resource profile should connect.
6. Select the **Create an access control policy allowing Telnet/SSH access to this server** checkbox to enable access to the server specified in the previous step (enabled by default).
7. In the Port field, enter the port on which the Secure Access Service should connect to the server. (By default, the Secure Access Service populates this field with port number 23 if you select Telnet and port number 22 if you select SSH.)
8. If you want to pass the user's credentials to the server, enter a static username, the <username> variable, or another Secure Access Service-appropriate session variable in the Username field. (Required for SSH sessions.)
9. Click **Save and Continue**.
10. In the Roles tab, select the roles to which the resource profile applies and click **Add**.  

The selected roles inherit the autopolicy and bookmarks created by the resource profile. If it is not already enabled, the Secure Access Service also automatically enables the Telnet/SSH option in the Users > User Roles > Select Role > General > Overview page of the admin console for all of the roles you select.
11. Click **Save Changes**.
12. (Optional) In the Bookmarks tab, modify the default bookmark created by the Secure Access Service and/or create new ones. (By default, the Secure Access Service creates a bookmark to the server defined in the Host field and displays it to all users assigned to the role specified in the Roles tab.)

### Related Documentation

- [Task Summary: Configuring the Telnet/SSH Feature on page 632](#)
- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)

## Associating Bookmarks with Telnet/SSH Resource Profiles

---

When you create a Telnet/SSH resource profile, the Secure Access Service automatically creates a bookmark that links to the host that you specified in the resource profile. The Secure Access Service enables you to modify this bookmark as well as create additional bookmarks to the same host.

You can use two different methods to create Telnet/SSH session bookmarks:

- Create bookmarks through existing resource profiles (recommended)—When you select this method, the Secure Access Service automatically populates the bookmark with key parameters (such as the host, port, username, and session type) using settings from the resource profile. Additionally, while you are creating the associated resource profile, the Secure Access Service guides you through the process of creating any required policies to enable access to the bookmark.
- Create standard bookmarks—When you select this option, you must manually enter all bookmark parameters during configuration. Additionally, you must enable access to the Telnet/SSH feature and create resource policies that enable access to the servers defined in the bookmark.

### Creating Bookmarks Through Existing Resource Profiles

When configuring bookmarks, note that:

- To change the host, port, or username for a Telnet/SSH bookmark created through a resource profile, you must edit the values through the resource profile's Resource tab (not its Bookmark tab).
- You can only assign bookmarks to roles that you have already associated with the resource profile—not all of the roles defined on the Secure Access Service. To change the list of roles associated with the resource profile, use settings in its Roles tab.
- Bookmarks simply control which links the Secure Access Service displays to users—not which resources the users can access. For example, if you enable access to a Telnet server through a resource profile but do not create a corresponding bookmark to that server, the user can still access the server by entering it into the Address field of the Secure Access Service home page.
- Make sure to enter a unique set of parameters when defining a Telnet/SSH bookmark. If you create two bookmarks that contain the same set of parameters, the Secure Access Service deletes one of the bookmarks from the end-user view. You will still be able to see both bookmarks, however, in the administrator console.

To associate bookmarks with Telnet/SSH resource profiles:

1. If you want to create a resource profile bookmark through the standard resource profiles page:
  - Choose **Users > Resource Profiles > Telnet/SSH > Select Resource Profile > Bookmarks**.
  - Click the appropriate link in the Bookmark column if you want to modify an existing bookmark. Or, click **New Bookmark** to create an additional bookmark.

Alternatively, if you want to create a resource profile bookmark through the user roles page:

- a. Choose **Users > User Roles > Select Role > Telnet/SSH > Sessions**.
- b. Click **Add Session**.
- c. From the Type list, choose **Telnet/SSH Resource Profile**. (The Secure Access Service does not display this option if have not already created a Telnet/SSH resource profile.)
- d. Select an existing resource profile. (The Secure Access Service automatically populates the Host and Port fields using settings from the selected resource profile.)
- e. Click **OK**. (If you have not already associated the selected role with the resource profile, the Secure Access Service automatically makes the association for you. The Secure Access Service also enables any access control policies for the role that are required by the resource profile.)
- f. If this role is not already associated with the selected resource profile, the Secure Access Service displays an informational message. If you see this message, click **Save Changes** to add this role to the resource profile's list of roles and to update the profile's autopolicies as required. Then, repeat the previous step to create the bookmark.



**NOTE:** When you create a resource profile bookmark through the user roles page (instead of the standard resource profiles page), the Secure Access Service only associates the generated bookmark with the selected role. The Secure Access Service does not assign the bookmark to all of the roles associated with the selected resource profile.

2. Optionally change the name and description of the bookmark. (By default, the Secure Access Service populates names the bookmark using the resource profile name.)
3. If you want to change the font size in the server display window, choose one of the following options in the Font Size section:
  - **Fixed size of \_pixels**—Enter a size from 8 to 36 pixels. (By default, the Secure Access Service sets the font size to 12.)
  - **Resize to fit window**—Dynamically changes the font size as you resize the window. This option requires Internet Explorer. (Enabled by default.)
4. If you want to change the size of the server display window, select an option from the Screen Size drop-down list. (By default, the Secure Access Service sets the window size at 80 characters by 24 rows.)
5. If you want to change the number of rows that the server window retains to display during scrolling, change the value in the Screen Buffer field (By default, the Secure Access Service sets the buffer at 100 rows.)
6. If you are configuring the bookmark through the resource profile pages, under Roles, specify the roles to which you want to display the bookmark:

- **ALL selected roles**—Select this option to display the bookmark to all of the roles associated with the resource profile.
- **Subset of selected roles**—Select this option to display the bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL Selected Roles list and click Add to move them to the Subset of selected roles list.

7. Click **Save Changes**.

### Creating Standard Bookmarks

Information in this topic is provided for backwards compatibility. We recommend that you configure access to Telnet and SSH servers through resource profiles instead, since they provide a simpler, more unified configuration method.

To create a bookmark for secure terminal sessions:

1. In the admin console, choose **Users > User Roles > Select Role > Telnet/SSH > Sessions**.
2. Click **Add Session**. The New Telnet/SSH Session page loads.
3. From the Type list, choose **Standard**. (The Secure Access Service only displays the Type list if you have already created a Telnet/SSH resource profile.)
4. Enter a bookmark name and description for the new Telnet/SSH session (optional). If you specify a bookmark name and description, this information appears on the Terminal Sessions page.
5. Enter the name or IP address of the remote host for this session in the Host field.
6. Select the Session Type, either **Telnet** or **SSH Secure Shell**, and specify the port if different from the pre-populated port assignment.
7. Provide a username or use the <username> or other Secure Access Service appropriate session variable.
8. Specify the Font Size by selecting one of the following:
  - **Fixed size of \_ pixels**—enter a size from 8 to 36 pixels.
  - **Resize to fit window**—dynamically changes the font size as you resize the window. This option requires Internet Explorer.
9. Select the Screen Size using the drop-down list.
10. Specify the Screen Buffer size.
11. Click **Save Changes** or **Save + New**.

In addition to creating bookmarks for secure terminal sessions, you must create a resource policy allowing Telnet/SSH sessions for the role, or enable Auto-allow role Telnet/SSH sessions on the Telnet/SSH > Options tab to automatically allow access to the resources defined in the session bookmark.

Make sure to enter a unique set of parameters when defining a Telnet/SSH bookmark. If you create two bookmarks that contain the same set of parameters, the Secure Access Service deletes one of the bookmarks from the end-user view. You will still be able to see both bookmarks, however, in the administrator console.



- Related Documentation**
- [Task Summary: Configuring the Telnet/SSH Feature on page 632](#)

## Configuring General Telnet/SSH Options

You can enable users to create their own Telnet/SSH bookmarks, browse to a terminal session, and to configure the Secure Access Service to create Telnet/SSH resource policies that allow access to the servers specified in the session bookmarks.

When you allow users to browse to a terminal session, note that they can use two different methods:

- Use the Secure Access Service homepage—Users can enter the server and port that they want to access into the Address field of the Secure Access Service home page. Valid formats for the URL include:

- Telnet://host:port
- SSH://host:port

For example: Telnet://terminalserver.yourcompany.com:3389

- Use the Web browser's address bar—Users can enter the server and port that they want to access (as well as session parameters such as font and window size) into the address bars of their Web browsers using standard Web protocol. For example:

`https://terminalserver.yourcompany.com:3389/terminalsession?font=12&width=800&height=600`

To specify general Telnet/SSH options:

1. In the admin console, choose **Users > User Roles > Select Role > Telnet/SSH > Options**.
2. Enable **User can add sessions** to allow users to define their own session bookmarks and to allow users to browse to a terminal session using telnet:// and ssh:// syntax as well as the /dana/term/newlaunchterm.cgi syntax. When you enable this option, the Add Terminal Session button appears on the Terminal Sessions page the next time a user refreshes the Secure Access Service welcome page.
3. Enable **Auto-allow role Telnet/SSH sessions** to enable the Secure Access Service to automatically allow access to the resources defined in the session bookmark (rather than having to create resource policies). Note that this only applies to role bookmarks, not user bookmarks.

You may not see the Auto-allow option if you are using a new installation or if an administrator hides the option.

4. Click **Save Changes**.

- Related Documentation**
- [Task Summary: Configuring the Telnet/SSH Feature on page 632](#)

## Writing a Telnet/SSH Resource Policy

---

When you enable the Telnet/SSH access feature for a role, you need to create resource policies that specify which remote servers a user may access. If the Secure Access Service matches a user's request to a resource listed in a Telnet/SSH policy, the Secure Access Service performs the action specified for the resource.

You can create resource policies through the standard interface (as described in this topic) or through resource profiles (recommended method).

When writing a Telnet/SSH resource policy, you need to supply key information:

- **Resources**—A resource policy must specify one or more resources to which the policy applies. When writing a Telnet/SSH policy, you need to specify remote servers to which a user may connect.
- **Roles**—A resource policy must specify the roles to which it applies. When a user makes a request, the Secure Access Service determines what policies apply to the role and then evaluates those policies that correspond to the request.
- **Actions**—A Telnet/SSH resource policy either allows or denies access to a server.

The Secure Access Service engine that evaluates resource policies requires that the resources listed in a policy's Resources list follow a canonical format.

### Writing Telnet/SSH Resource Policies

Information in this section is provided for backwards compatibility. We recommend that you configure access to Telnet and SSH servers through resource profiles instead, since they provide a simpler, more unified configuration method.

To write a Telnet/SSH resource policy:

1. In the admin console, choose **Users > Resource Policies > Telnet/SSH > Access**.
2. On the Telnet/SSH Policies page, click **New Policy**.
3. On the New Policy page, enter a name to label this policy and optionally a description.
4. In the Resources section, specify the servers to which this policy applies.
5. In the Roles section, specify:
  - **Policy applies to ALL roles**—Use this field to apply this policy to all users.
  - **Policy applies to SELECTED roles**—Use this field to apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—Use this field to apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. In the Action section, specify:

- **Allow access**—Use this field to grant access to the servers specified in the Resources list.
  - **Deny access**—Use this field to deny access to the servers specified in the Resources list.
  - **Use Detailed Rules**—Use this field to specify one or more detailed rules for this policy.
7. Click **Save Changes**.
  8. On the Telnet/SSH Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

### Matching IP Addresses to Host Names

You can configure Telnet/SSH to match IP addresses to host names specified as resources in your Telnet/SSH resource policies. When you enable this option, the Secure Access Service looks up IP address corresponding to each host name specified in a Telnet/SSH resource policy. When a user tries to access a server by specifying an IP address rather than the host name, the Secure Access Service compares the IP to its cached list of IP addresses to determine if a host name matches an IP. If there is a match, then the Secure Access Service accepts the match as a policy match and applies the action specified for the resource policy.

When you enable this option, the Secure Access Service compiles a list of host names specified in the Resources field of each Telnet/SSH resource policy. The Secure Access Service then applies the option to this comprehensive list of host names.

This option does not apply to host names that include wildcards and parameters.

To specify the Telnet/SSH resource option:

1. In the admin console, choose **Users > Resource Policies > Telnet/SSH > Options**.
2. Select **IP based matching for Hostname based policy resources**.

The Secure Access Service looks up the IP address corresponding to each host name specified in a Telnet/SSH resource policy. When a user tries to access a server by specifying an IP address rather than the host name, the Secure Access Service compares the IP to its cached list of IP addresses to determine if a host name matches an IP. If there is a match, then the Secure Access Service accepts the match as a policy match and applies the action specified for the resource policy.

3. Click **Save Changes**.

### Related Documentation

- [Task Summary: Configuring the Telnet/SSH Feature on page 632](#)



# Terminal Services

- [About Terminal Services on page 642](#)
- [Task Summary: Configuring the Terminal Services Feature on page 643](#)
- [Terminal Services Execution on page 645](#)
- [Configuring Citrix to Support ICA Load Balancing on page 646](#)
- [About Terminal Services Resource Profiles on page 648](#)
- [Configuring a Windows Terminal Services Resource Profile on page 649](#)
- [Defining a Hosted Java Applet Autopolicy on page 650](#)
- [Defining a Bookmark for a Windows Terminal Services Profile on page 653](#)
- [Creating a Windows Terminal Services Bookmark Through the User Roles Page on page 654](#)
- [Defining Display Options for the Windows Terminal Services Session on page 655](#)
- [Defining SSO Options for the Windows Terminal Services Session on page 656](#)
- [Defining Application Settings for the Windows Terminal Services Session on page 656](#)
- [Defining Device Connections for the Windows Terminal Services Session on page 657](#)
- [Defining Desktop Settings for the Windows Terminal Services Session on page 659](#)
- [Creating a Citrix Terminal Services Resource Profile Using Default ICA Settings on page 659](#)
- [Defining a Bookmark for a Citrix Profile Using Default ICA Settings on page 660](#)
- [Defining Display Options for the Citrix Terminal Services Session on page 663](#)
- [Defining SSO Options for the Citrix Terminal Services Session on page 663](#)
- [Defining Application, Auto-Launch, and Session Reliability Settings for the Citrix Terminal Services Session on page 664](#)
- [Defining Device Connections for the Citrix Terminal Services Session on page 665](#)
- [Creating a Citrix Resource Profile That Uses a Custom ICA File on page 666](#)
- [Defining a Bookmark for a Citrix Profile Using a Custom ICA File on page 668](#)
- [Creating a Citrix Profile That Lists Published Applications on page 669](#)
- [Defining a Bookmark for a Citrix Profile Listing Applications on page 670](#)
- [Creating Session Bookmarks to Your Terminal Server on page 672](#)
- [Creating Advanced Terminal Services Session Bookmarks on page 673](#)

- [Creating Links from an External Site to a Terminal Services Session Bookmark on page 679](#)
- [Specifying General Terminal Services Options on page 685](#)
- [Configuring Terminal Services Resource Policies on page 688](#)
- [Specifying the Terminal Services Resource Option on page 689](#)
- [Using the Remote Desktop Launcher on page 689](#)

## About Terminal Services

---

Use the Terminal Services feature to enable a terminal emulation session on a Windows terminal server, Citrix NFuse server, or Citrix Metaframe server. You can also use this feature to deliver the terminal services through the Secure Access Service, eliminating the need to use another Web server to host the clients.

The Secure Access Service supports several mechanisms for intermediating traffic between a Citrix server and client, including the Terminal Services, JSAM, WSAM, VPN Tunneling, and hosted Java applets features.

The Terminal Services features (Windows Terminal Services and Citrix) are not available on the SA700 Series Appliance.

## Terminal Services User Experience

From an end-user perspective, accessing secured terminal services resources through the Secure Access Service is simple. When you enable the Terminal Services feature for a user role, the end user simply needs to do the following tasks:

1. Specify the resource that the user wants to access—The user can specify the resource he wants to access by clicking a link or entering the resource in the Secure Access Service browse bar. Or, if you enable auto-launch for a bookmark, the Secure Access Service automatically launches the resource for the user when he signs into the Secure Access Service.
2. Enter credentials for the resource—When the user accesses a resource, the Secure Access Service prompts him to enter his username and password (if required by the resource). Or if you enable SSO, the Secure Access Service automatically sends this information to the resource without prompting the user. Once the resource verifies the credentials, the Secure Access Service launches the resource.

Users can access terminal services resources using the following methods:

- Session bookmarks—A session bookmark defines various information, including the server to which the user can connect, the terminal session's window parameters, and the username and password that the Secure Access Service sends to the Windows terminal server or Metaframe server. You can create any number of session bookmarks for a role, enabling the user to access multiple servers using different session bookmarks for each. (Users can simultaneously open multiple sessions to the same terminal server or to different servers.)
- URLs from other Web sites—In most cases, users access session bookmarks directly from the Secure Access Service end-user console. If you do not want to require users

to sign into the Secure Access Service end-user console to find and access terminal services links, you can create URLs on other Web sites that point to session bookmarks that you have already created on the Secure Access Service. Or, you can create URLs that include all of the parameters that you want to pass to the Terminal Services program, such as the host, ports, and terminal window parameters.



**NOTE:** If you create links on external servers to terminal services bookmarks on the Secure Access Service and you are using multiple customized sign-in URLs, some restrictions occur.

- **Secure Access Service browse bar**—In addition to enabling users to link to terminal services links through bookmarks and URLs, you can also enable them to access these resources through the Secure Access Service browse bar on Windows systems. Users can access Citrix Metaframe or Nfuse servers by entering `ica://hostname` in the browse box. Or, users can access Microsoft terminal services or remote desktop sessions by entering `rdp://hostname` in the browse box.
- **Server address**—By entering a terminal server IP address or hostname, users can launch a remote desktop connection to any accessible server.

**Related Documentation**

- [Task Summary: Configuring the Terminal Services Feature on page 643](#)

## Task Summary: Configuring the Terminal Services Feature

To configure the Terminal Services feature:

1. Create resource profiles that enable access to Windows terminal servers or Citrix servers, include session bookmarks that link to those servers, and assign the session bookmarks to user roles using settings in the Users > Resource Profiles > Terminal Services page of the admin console.

We recommend that you use resource profiles to configure terminal services (as described here). However, if you do not want to use resource profiles, you can configure the Terminal Services feature using role and resource policy settings in the following pages of the admin console instead:

- Create resource policies that enable access to Windows terminal servers and Citrix servers using settings in the Users > Resource Policies > Terminal Services > Access page of the admin console.
- Determine which user roles may access the Windows terminal servers and Citrix servers that you want to intermediate, and then enable Terminal Services access for those roles through the Users > User Roles > Select\_Role > General > Overview page of the admin console.
- Create session bookmarks to your Windows terminal servers and Citrix servers using settings in the Users > User Roles > Select\_Role > Terminal Services > Sessions page of the admin console.

2. (Optional.) Modify general role and resource options after configuring terminal services using resource profiles or roles and resource policies. Use the following pages of the admin console:
  - (Optional.) Enable users to define their own terminal services sessions, specify the local devices to which users can connect, and set display and performance options using settings in the Users > User Roles > Select\_Role > Terminal Services > Options page of the admin console. If you choose to enable users to define their own terminal services sessions, you must also create corresponding resource policies or resource profiles that enable access the specified resources, as explained in earlier in this topic.
  - (Optional.) Create links to a terminal services session on the Secure Access Service that users can access from an external Web site.
  - (Optional.) Enable the Secure Access Service to match IP addresses to host names using settings in the Users > Resource Policies > Terminal Services > Options page of the admin console.
3. (Citrix only) Specify where the Secure Access Service should obtain the Citrix client to upload to the users' systems through settings in the Users > User Roles > Select\_Role > Terminal Services > Options page of the admin console.

Additionally, if you specify that the Secure Access Service should obtain a Citrix client from an external Web site, you must:

- Create a Web access resource policy that enables access to the Web site where the Citrix client resides through settings in the Users > Resource Policies > Web > Access > Web ACL page of the admin console.
- Create a Web caching resource policy through settings in the Users > Resource Policies > Web > Caching page of the admin console so the user's browser can deliver the Citrix client. (Note that you must select the Unchanged (do not add/modify caching headers) option.)

**Related Documentation**

- [About Terminal Services on page 642](#)
- [Terminal Services Execution on page 645](#)
- [About Terminal Services Resource Profiles on page 648](#)
- [Specifying General Terminal Services Options on page 685](#)
- [Configuring Terminal Services Resource Policies on page 688](#)
- [Specifying the Terminal Services Resource Option on page 689](#)



---

## Terminal Services Execution

---

When a user tries to access a terminal services resource, the Secure Access Service completes the following steps to initiate and intermediate the terminal services session:

1. The Secure Access Service checks for a Java client.

To enable a terminal services session, the user either needs an RDP client on his system (to access a Windows terminal server) or an ICA client (to access a Citrix Metaframe server or server farm). These clients come in both Windows and Java versions and enable the user to run an application on the server while only transmitting keyboard, mouse, and display information over the network.

The Secure Access Service enables you to upload a Java version of the RDP or ICA client through a terminal services resource profile (but not role). If you have uploaded a client to the Secure Access Service and specified that the Secure Access Service always use it to run your users' terminal sessions, the Secure Access Service launches the specified Java client.

2. (Citrix only.) If necessary, the Secure Access Service checks for a Windows client.

If you have not uploaded a Java client to the Secure Access Service, the Secure Access Service checks for a Windows version of the ICA client. If the Secure Access Service cannot find a Windows ICA client, it installs the version you specified in the Users > User Roles > Role > Terminal Services > Options page of the Secure Access Service admin console.

3. The Secure Access Service checks for the terminal services proxy.

To intermediate a Windows or Citrix session, the user either needs a Juniper Windows Terminal Services proxy on his system or a Juniper Networks Citrix Terminal Services proxy. The Secure Access Service checks for the appropriate proxy on the user's computer, and if it cannot find it, installs a new one. Depending on the user's rights, the Secure Access Service either uses an ActiveX component or Java component to install the proxy.

4. The proxy tries to invoke the Windows client.

Once the Secure Access Service has confirmed that a proxy is installed on the user's computer, the proxy attempts to invoke the Windows RDP or ICA client. If successful, the client initiates the user's terminal services session and the proxy intermediates the session traffic.

5. The proxy tries to invoke the Java client.

If a Windows client is not present on the user's machine (for instance, because it was deleted or because the user does not have the proper privileges to install it), but you have uploaded one to the Secure Access Service through the terminal services resource profile, the Secure Access Service uses the uploaded Java applet to launch the session.

As part of the installation, the Secure Access Service asks the user if he wants to always use the Java client or only for this session. The Secure Access Service then stores the user's preference as a persistent cookie. Once the Java client is installed,

the client initiates the user's terminal services session and the proxy intermediates the session traffic.

For information about the specific files installed by the Secure Access Service when you enable the Terminal Services feature, as well as the rights required to install and run the associated clients, see the *Client-side Changes Guide* on the Juniper Networks Customer Support Center.

**Related  
Documentation**

- [Task Summary: Configuring the Terminal Services Feature on page 643](#)

---

## Configuring Citrix to Support ICA Load Balancing

---

The Secure Access Service Terminal Services feature supports connecting to Citrix server farms in which published applications are preconfigured (as described later in this topic). The Secure Access Service does not support load balancing configurations in which Nfuse servers dynamically retrieve a list of Citrix published applications within a server farm.

### Citrix Load Balancing Overview

The Secure Access Service supports the following Citrix load balancing scenario:

1. The Citrix administrator makes a published application available to multiple Citrix servers in a farm by generating a custom ICA file. The generated ICA file contains a parameter called HTTPBrowserAddress that points to the IP address and port number of the master browser (that is, the server that performs the load balancing).
2. When the ICA client attempts to launch a published application on the user's computer, it uses the HTTPBrowserAddress parameter to connect to the master browser.
3. The master browser pings servers in the farm to determine their respective loads and returns the IP address of the least busy server to the ICA client.
4. The ICA client uses the IP address returned by the master browser to connect to the appropriate terminal server.

### Configuring Citrix Load Balancing

For the Secure Access Service to work properly with a Citrix farm, you must configure the Citrix farm and Secure Access Service as described in the following steps. Note that these instructions are based on using a Citrix Metaframe Presentation Server 3.0.

1. On the Citrix server, enable a server (or multiple servers) in your farm as a master browser:
  - a. Right-click a server in the Metaframe Farm and select **Properties**.
  - b. Select **Metaframe Settings**.

- c. Enter the TCP/IP port for the Citrix XML service.
2. On the Citrix server, publish the applications that are hosted on MetaFrame XP servers in the farm:
  - a. Right-click the Applications link and select **Publish applications**.
  - b. Specify which desktop or application to publish.
  - c. Follow the prompts in the wizard.
  - d. Specify the list of servers that host the application you are publishing and click **Finish**.

The specified published application appears in the server farm.

3. On the Citrix server, generate a corresponding Citrix ICA file for the published application:
  - a. Select the application you published in Step 2 and select **Create ICA file**.
  - b. Follow the prompts in the wizard.
  - c. On the TCP/IP + HTTP Server page, enter the name of the HTTPBrowser server and the port number. (The port should match the Citrix XML Service port that you set up in Step 1).
  - d. Save the ICA file.
4. On the Secure Access Service, upload the ICA file using settings in either of the following admin console pages:
  - Users > User Roles > *Role* > Terminal Services > Sessions
  - Users > Resource Profiles > *Profile*
5. On the Secure Access Service, create a resource policy for the HTTPBrowser server and port entered in Step 3.
6. On the Secure Access Service, test the configuration by launching the bookmark as an end user.



**NOTE:** One of the Citrix servers in the farm performs the load balancing, not the Secure Access Service. If the ICA client is already installed on the user's desktop then administrator rights are not required.

For more information about the rights required to use the Terminal Services feature, see [Client-Side Changes](#).

If the XML response from the master browser contains the hostname, it will not work through the Secure Access Service. To ensure that the response is in dot-port format (an IP address), clear the Enable XML service DNS address resolution check box during the browser server configuration. This option controls whether the destination Citrix server is represented as a hostname or as an IP address.

**Related Documentation** • [Comparing Secure Access Access Mechanisms for Configuring Citrix on page 468](#)

## About Terminal Services Resource Profiles

Terminal Services resource profile configuration instructions vary depending on whether you want to configure access to a Windows terminal server (which requires a RDP client) or Citrix terminal server (which requires an ICA client). Furthermore, if you choose to configure access to a Citrix server using a custom ICA file, you include many of your configuration settings in the ICA file itself and therefore do not need to configure them through the Secure Access Service. If you configure access to a Citrix server using the default ICA file on the Secure Access Service, however, you must configure additional settings through the Secure Access Service.

You may want to create multiple bookmarks for the same terminal services resource in order to provide easy access to multiple applications. For instance, the server defined in your resource profile may provide access to multiple applications (such as Siebel and Outlook). To easily provide access to each of these applications, you can create resource profile bookmarks to each. Or, you may want to use multiple bookmarks to configure single sign-on to one application, but not another.

When configuring session bookmarks, note that:

- To change the host or ports for a terminal services session bookmark created through a resource profile, you must edit the values through the resource profile's Resource tab (not its Bookmark tab).
- You can only assign session bookmarks to roles that you have already associated with the resource profile—not all of the roles defined on the Secure Access Service. To change the list of roles associated with the resource profile, use settings in its Roles tab.
- Session bookmarks simply control which links the Secure Access Service displays to users—not which resources the users can access. For example, if you enable access to a terminal server through a resource profile but do not create a corresponding session

bookmark to that server, the user can still access the server by entering it into the Address box of the Secure Access Service home page.

- Make sure to enter a unique set of parameters when defining a terminal services bookmark. If you create two bookmarks that contain the same set of parameters, the Secure Access Service deletes one of the bookmarks from the end-user view. You can still see both bookmarks, however, in the administrator console.

**Related  
Documentation**

- [Task Summary: Configuring the Terminal Services Feature on page 643](#)
- [Defining Resource Profile Bookmarks on page 134](#)

## Configuring a Windows Terminal Services Resource Profile

This topic describes how to configure a terminal services resource profile that enables access to a Windows terminal server using an RDP client.

Users can use RDP7 features through the Juniper Networks terminal services if an RDP7 client is present. However, the true multi-monitor and bidirectional audio features of RDP7 are not supported with this release.

To create a Windows terminal services resource profile:

1. In the admin console, select **Users > Resource Profiles > Terminal Services**.
2. Click **New Profile**. Or select an existing profile from the list.
3. Select **Windows Terminal Services** from the Type list.
4. Enter a unique name and optionally a description for the resource profile. (This name becomes the default session bookmark's name.)
5. Specify the server and port to which this resource profile should connect in the Host field. When entering the server, you may enter a hostname or IP address.
6. Enter the port on which the terminal server listens in the Server port box. (By default, the Secure Access Service populates this box with port number 3389.)
7. Select the **Create an access control policy allowing Terminal Service access to this server** check box to enable access to the server specified in the Server Port box (enabled by default).
8. If you want to enable intermediation using a Java client, select **Enable Java support** and then specify which Java client the Secure Access Service should use.
9. Click **Save and Continue**.
10. Select the roles to which the resource profile applies in the Roles tab and click Add.

The selected roles inherit the autopolicy and session bookmarks created by the resource profile. If it is not already enabled, the Secure Access Service also automatically enables the Terminal Services option in the Users > User Roles > Select\_Role > General > Overview page of the admin console for all of the roles you select.

11. Click **Save Changes**.
12. (Optional.) Modify the default session bookmark created by the Secure Access Service in the Bookmarks tab and/or create new ones. By default, the Secure Access Service creates a session bookmark to the server defined in the Host box and displays it to all users assigned to the role specified in the Roles tab.)

**Related  
Documentation**

- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)

## Defining a Hosted Java Applet Autopolicy

Hosted Java applet autopolicies enable you to store terminal services Java clients directly on the Secure Access Service without employing a separate Web server to host them. You can then associate these Java applets with the resource profile and specify that the Secure Access Service always use them to intermediate traffic, or that the Secure Access Service fall back to the applets when other terminal services clients are not available on the user's system.

Although you can use a Java applet to intermediate traffic to an SSO-enabled resource, we do not recommend it because the applet may require the user's password to be presented as plain text.

A default HOB-Juniper RDP Java applet is shipped with each Secure Access device and can not be deleted. The HOB applet is available through the New Terminal Services Resource Profile window and the Users > User Roles > Users > Terminal Services > Options window. To use the Juniper-supplied HOB applet, you must contact Juniper Customer Care to purchase a license including the number of concurrent users you want to support.

The HOB applet is similar to any other Java applet accessed through the Secure Access System or uploaded to the Secure Access System. You must install a code-signing certificate to avoid seeing the warning "This applet was signed by "Secure Access Gateway", but Java cannot verify the authenticity of the signature's certificate. Do you trust this certificate?" Install a valid Applet signing certificate (JavaSoft) in the **Configuration > Certificates > Code-signing Certificates** window.



**NOTE:** The HOB applet is for RDP connections and appears only for Windows Terminal Services. It is not applicable for Citrix Terminal Services profiles.

You can purchase HOB applets directly from HOB; however, Juniper Networks will support them only to the extent of uploading them. If you have any problems configuring or running the applet, you must contact HOB support.

To create a hosted Java applet autopolicy:

1. Create a terminal services resource profile.
2. Select **Enable Java support** within the resource profile.

3. Select the Java applet that you want to associate with the resource profile from the Applet to use list. Or, if the applet that you want to use is not currently available in the list, click Edit Applet. Then:
  - a. Click **New Applet** to add an applet to this list. Or, select an existing applet and click **Replace** (to replace an existing applet with a new applet) or **Delete** (to remove an applet from the Secure Access Service).



**NOTE:** If you replace an existing archive, make sure that the new applet archive contains all of the necessary files for the applet to successfully launch and run. If the associated HTML for the applet refers to files that do not exist in the new archive, then the applet will not function correctly.

The Secure Access Service only allows you to delete applets that are not currently in use by a Web or terminal services resource profile.

If you select the Enable Java support option and have a custom ICA file that you uploaded to the Secure Access Service, your HTML file is auto-populated with references to your custom ICA file. No additional HTML code needs to be added.

- b. Enter a name to identify the applet in the Name box. (This applies to new and replaced applets only.)
- c. Browse to the applet that you want to upload to the Secure Access Service. You can upload applets (.jar or .cab files) or archives (.zip, .jar, and .tar files) that contain applets and all of the resources that the applets need. (This applies to new and replaced applets only.)
- d. If the file that you selected is an archive that contains the applet, select the Uncompress jar/cab file check box. (This applies to new and replaced applets only.)
- e. Click **OK** and **Close Window**.



**NOTE:** When you select an applet in the Java Applets dialog box, you are loading third-party software onto the Juniper Networks product. By clicking OK, you are agreeing to the following terms on behalf of yourself (as purchaser of the equipment) or the organization that purchased the Juniper product, as applicable:

By loading third party software onto the Juniper Networks product, you are responsible for obtaining all rights necessary for using, copying, and/or distributing such software in or with the Juniper Networks product. Juniper Networks is not responsible for any liability arising from use of such third party software and will not provide support for such software. The use of third party software may interfere with the proper operation of the Juniper Networks product and/or Juniper Networks software, and may void any warranty for the Juniper Networks product and/or Juniper software.

4. Create an HTML page definition in the HTML box that includes references to your Java applets. The maximum size of the HTML that can be specified is 25k. Then, fill in any required attributes and parameters.

If you are using HTML generated by the Secure Access Service, make sure to search the HTML code for “\_\_PLEASE\_SPECIFY\_” and update the code as necessary.



**NOTE:** If you select Hob-Juniper RDP Applet from the Applet to Use menu, you must select the Configure HTML for the default applet checkbox in order to edit the HTML. Otherwise, the default HTML is used. By default, the proxy mode is disabled in the Hob-Juniper RDP Applet.

To enable the proxy mode, add the following:

```
<parameter name="proxymode" value="http">
```

If your proxy requires authentication, add the following to the Hob-Juniper RDP Applet:

```
<parameter name="proxyuser" value="<username>">
<parameter name="proxypassword" value="<password>">
```

You can also add any additional HTML or JavaScript that you choose to this Web page definition. The Secure Access Service rewrites all of the code that you enter in this box.

Make sure to enter unique HTML in this box. If you create two bookmarks with the same HTML code, the Secure Access Service deletes one of the bookmarks in the end-user view. You can still see both bookmarks, however, in the administrator console.

For dynamic drive mapping to work with HOB Applet 3.3.0692, you must enable both the **AUTOLDM** and **TWAutomAPDRIVE** parameters. See the *Premier Java Applet Configuration Options* document located on the Juniper Networks support site for more details on these two parameters.



5. Select **Use this Java applet as a fallback mechanism** to use this applet only when the Windows client fails to launch. Or select **Always use this Java applet** to use this applet regardless of whether or not the Windows client launches.
6. Click **Save Changes**.

**Related  
Documentation**

- [About Hosted Java Applet Templates on page 453](#)
- [Task Summary: Configuring the Terminal Services Feature on page 643](#)
- [Required Attributes for Uploaded Java Applets on page 461](#)
- [Required Parameters for Uploaded Java Applets on page 462](#)

## Defining a Bookmark for a Windows Terminal Services Profile

When you create a terminal services resource profile, the Secure Access Service automatically creates a bookmark that links to the terminal server that you specified in the resource profile. The Secure Access Service allows you to modify this bookmark as well as create additional bookmarks to the same terminal server.

To configure resource profile bookmarks for Windows terminal services:

1. In the admin console, select **Users > Resource Profiles > Terminal Services > Resource Profile Name > Bookmarks**.
2. Click the appropriate link in the Bookmark column if you want to modify an existing session bookmark. Or, click **New Bookmark** to create an additional session bookmark.  
  
Although it is generally easiest to create a resource profile session bookmark through the resource profile configuration page, you can choose to create one through the user roles page as well.
3. (Optional.) Change the name and description of the session bookmark. (By default, the Secure Access Service populates and names the session bookmark using the resource profile name.)
4. Specify how the terminal emulation window should appear to the user during a terminal session by configuring options in the Settings area of the bookmark configuration page.
5. Pass user credentials from the Secure Access Service to the terminal server so that users can sign onto the terminal server without having to manually enter their credentials. You can do this by configuring options in the Session area of the bookmark configuration page.
6. Allow users to access specific applications on the terminal server by configuring options in the Start Application area of the bookmark configuration page. In addition, you can use settings in this area to define auto-launch and session reliability options.
7. Allow users to access local resources such as printers and drives through the terminal session by configuring options in the Connect Devices area of the bookmark configuration page.

8. Specify how the terminal emulation window should appear to the user during a terminal session by configuring options in the Desktop Settings area.
9. Specify the roles to which you want to display the session bookmarks if you are configuring the session bookmark through the resource profile pages, under Roles:
  - **ALL selected roles**—Displays the session bookmark to all of the roles associated with the resource profile.
  - **Subset of selected roles**—Displays the session bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL Selected Roles list and click **Add** to move them to the Subset of selected roles list.
10. Click **Save Changes**.

**Related Documentation**

- [Task Summary: Configuring the Terminal Services Feature on page 643](#)
- [Defining SSO Options for the Windows Terminal Services Session on page 656](#)
- [Defining Application Settings for the Windows Terminal Services Session on page 656](#)
- [Defining Desktop Settings for the Windows Terminal Services Session on page 659](#)

---

## Creating a Windows Terminal Services Bookmark Through the User Roles Page

---

It is generally easiest to create a terminal services bookmark through the resource profile configuration pages. However, you can choose to create a resource profile session bookmark through the user roles page using the following instructions:

1. In the admin console, select **Users > User Roles > Select Role > Terminal Services > Sessions**.
2. Click **Add Session**.
3. Select **Terminal Services Resource Profile** from the Type list. (The Secure Access Service does not display this option if you have not already created a terminal services resource profile.)
4. Select an existing resource profile that connects to a Windows terminal server on the Secure Access Service. (The Secure Access Service automatically populates the Host and Server Port boxes using settings from the selected resource profile.)
5. Click **OK**. (If you have not already associated the selected role with the resource profile, the Secure Access Service automatically makes the association for you. The Secure Access Service also enables any access control policies for the role that are required by the resource profile.)
6. If this role is not already associated with the selected resource profile, the Secure Access Service displays an informational message. If you see this message, click **Save Changes** to add this role to the resource profile's list of roles and to update the profile's autopolicies as required. Then, repeat the previous steps to create the session bookmark.

When you create a resource profile session bookmark through the user roles page (instead of the standard resource profiles page), the Secure Access Service only

associates the generated session bookmark with the selected role. The Secure Access Service does not assign the session bookmark to all of the roles associated with the selected resource profile.

7. (Optional.) Change the name and description of the session bookmark. (By default, the Secure Access Service populates names the session bookmark using the resource profile name.)
8. Configure the bookmark's settings.

**Related Documentation**

- [Task Summary: Configuring the Terminal Services Feature on page 643](#)

## Defining Display Options for the Windows Terminal Services Session

When configuring a terminal services bookmark, you can specify how the terminal emulation window should appear to users during their terminal sessions.

To define display and auto-launch options:

1. Create a terminal services bookmark or edit an existing bookmark.
2. Scroll to the Settings area of the bookmark configuration page.
3. Select an option from the Screen Size drop-down list if you want to change the size of the terminal services window on the user's workstation. (By default, the Secure Access Service sets the window size to full screen.)



**NOTE:** If you select the Full Screen option and are connecting to a Windows terminal server, the Secure Access Service needs to modify the user's hosts file to display the correct hostname in the terminal services window. If the user does not have the proper rights to modify the hosts file, the Secure Access Service displays the loopback address instead.

Also note that to restore the hosts file to its original state after running the terminal services window, the user must properly close his application. Otherwise, other applications that use the hosts file (such as JSAM and Host Checker) might not run properly. The user can also restore his hosts file to its original state by rebooting his system or by renaming the backup hosts file (hosts\_ive.bak).

4. Select **8-bit**, **15-bit**, **16-bit**, **24-bit**, or **32-bit** color from the Color Depth list if you want to change the color-depth of the terminal session data. (By default, the Secure Access Service sets the color depth to 8-bit.)
5. Click **Save Changes**.

**Related Documentation**

- [Defining a Bookmark for a Windows Terminal Services Profile on page 653](#)

## Defining SSO Options for the Windows Terminal Services Session

---

When configuring a terminal services bookmark, you can configure the Secure Access Service to pass user credentials from the Secure Access Service to the terminal server so that the user does not have to manually enter his username and password. The Secure Access Service passes the specified credentials when a user clicks the session bookmark. If the credentials fail, the server prompts the user to manually enter his username and password.

To define single sign-on options:

1. Create a terminal services bookmark or edit an existing bookmark.
2. Scroll to the Authentication area of the bookmark configuration page.
3. Specify the username that the Secure Access Service should pass to the terminal server. You can enter a static username or a variable. Enter the <username> variable to pass the username stored in the Secure Access Service's primary authentication server. Or use the following syntax to submit the username for the secondary authentication server: <username@SecondaryServerName> or <username[2]>.
4. Select Password if you want to specify a static password or select Variable Password if you want use the password stored in the Secure Access Service's primary or secondary authentication server. To use the password from the primary authentication server, enter the <password> variable. Or use the following syntax to submit the password for the secondary authentication server: <Password@SecondaryServerName> or <Password[2]>.
5. Click **Save Changes**.

### Related Documentation

- [Defining a Bookmark for a Windows Terminal Services Profile on page 653](#)
- [Task Summary: Configuring the Terminal Services Feature on page 643](#)

## Defining Application Settings for the Windows Terminal Services Session

---

When configuring a terminal services bookmark, you can specify that users can only access specific applications on the terminal server.

To define applications that users can access:

1. Create a terminal services bookmark or edit an existing bookmark.
2. Scroll to the Start Application area of the bookmark configuration page.
3. Select the **Launch seamless window** check box to have the Windows application server manage the display of the application. This allows an application's windows to behave in the same way as an application running on a Windows application server, regardless of the user's desktop environment.



**NOTE:** If SSO is not configured, seamless window is supported only on Remote Desktop Protocol (RDP) 6.0 and later.

The Launch seamless window check box is applicable only for servers running Windows 2008 and later.

Enter the server alias name (applicable only for servers running Windows 2008 and later) in the Alias name box.

- Specify where the application's executable file resides on the terminal server in the Path to application box (visible only when you clear Launch seamless window). For example, you might enter the following directory for the Microsoft Word application:

C:\Program Files\Microsoft Office\Office10\WinWord.exe

- Specify where the terminal server should place working files for the application in the Working directory box. For example, you might specify that Microsoft Word should save files to the following directory by default:

C:\Documents and Settings\username\My Documents



**NOTE:** You can use session variables such as <username> and <password> in the Path to application and Working directory boxes. For example, when specifying an application path, you might want to include the <username> variable to personalize the location. For example:  
C:\Documents and Settings\<username>\My Documents.

- Select the **Auto-launch** check box if you want to automatically launch this Terminal Service session bookmark when users sign into the Secure Access Service. When you select this option, the Secure Access Service launches the terminal services application in a separate window when the user signs into the Secure Access Service.
- Click **Save Changes**.

#### Related Documentation

- [Defining a Bookmark for a Windows Terminal Services Profile on page 653](#)
- [System Variables and Examples on page 1186](#)

## Defining Device Connections for the Windows Terminal Services Session

When configuring a terminal services bookmark, you can specify local resources that users can access through the terminal session.



**NOTE:** The Secure Access Service does not support providing users access to local resources when intermediating traffic using Java applets. Therefore, if you select the Enable Java Applets option when creating a Windows Terminal Services resource profile, note that the Connect Devices options described below might not work.

When you enable local resources through the terminal server, each user can only access his own local resources. For instance, user 1 cannot see user 2's local directories.

To define local resources that users can access:

1. Create a terminal services bookmark or edit an existing bookmark.
2. Scroll to the Connect Devices area of the bookmark configuration page.
3. Select **Connect local drives** to connect the user's local drive to the terminal server, enabling the user to copy information from the terminal server to his local client directories.
4. Select **Connect local printers** to connect the user's local printers to the terminal server, enabling the user to print information from the terminal server to his local printer.
5. Select **Connect COM Ports** to connect the user's COM ports to the terminal server, allowing communication between the terminal server and the devices on his serial ports.
6. Select **Allow Clipboard Sharing** to allow the contents of the clipboard to be shared between the user's host computer and the terminal server. Because of limitations in RDP client earlier than version 6.0, clearing the Allow Clipboard Sharing option will automatically disable the Connect local drives, Connect local printers, and Connect COM Ports options.
7. Select **Connect smart cards** to allow users to use smart cards to authenticate their remote desktop sessions.



**NOTE:** Smart cards are supported by Microsoft Remote Desktop Protocol versions 5.1 and later.

8. Select **Sound Options** to enable sound during the remote session. Select **Bring to this computer** to redirect audio to the local computer. Select **Leave at remote computer** to play the audio only at the server.



**NOTE:** Sound options are supported by Microsoft Remote Desktop Protocol versions 5.1 and later.

9. Click **Save Changes**.

- Related Documentation**
- [Defining a Bookmark for a Windows Terminal Services Profile on page 653](#)

## Defining Desktop Settings for the Windows Terminal Services Session

---

When configuring a terminal services bookmark, you can specify how the terminal emulation window should appear to the user during a terminal session.



**NOTE:** The options in this topic only apply to Windows Terminal Services bookmarks.

To define display settings for the users' sessions:

1. Create a terminal services bookmark or edit an existing bookmark
2. Scroll to the Display Settings area of the bookmark configuration page.
3. Select **Desktop background** to display a wallpaper background to users. If you do not select this option, the background is blank.
4. Select **Show contents of window while dragging** to show the contents of the Windows Explorer window while users move the windows on their desktops.
5. Select **Menu and window animation** to animate the movement of windows, menus, and lists.
6. Select **Themes** to allow users to set Windows themes in their terminal server windows.
7. Select **Bitmap Caching** to improve performance by minimizing the amount of display information that is passed over a connection.
8. Select **Font Smoothing (RDP 6.0 onwards)** to make text smoother and easier to read. This option only works on Windows Vista computers running RDP clients that are version 6.0 or later.
9. Select **Desktop Composition (RDP 6.0 onwards)** to allow desktop composition. With desktop composition, individual windows no longer draw directly to the screen. Instead, their drawing is redirected to video memory, which is then rendered into a desktop image and presented on the display.
10. Click **Save Changes**.

- Related Documentation**
- [Defining a Bookmark for a Windows Terminal Services Profile on page 653](#)

## Creating a Citrix Terminal Services Resource Profile Using Default ICA Settings

---

This topic describes how to configure access to a Citrix Metaframe server using a default ICA configuration file.

To create a Citrix Terminal Services resource profile that uses default ICA settings:

1. In the admin console, select **Users > Resource Profiles > Terminal Services**.
2. Click **New Profile**. Or select an existing profile from the list.
3. Select **Citrix using default ICA** from the Type list.
4. (Existing resource profiles only) If you want to customize the default ICA file that comes with the Secure Access Service, click the **Open** link, customize the file, and upload it to the Secure Access Service.
5. Enter a unique name and optionally a description for the resource profile. (This name becomes the default session bookmark's name.)
6. Specify the server and port to which this resource profile should connect in the Host box. When entering the server, you may enter a host name or IP address.
7. Enter the port on which the terminal server listens in the Server Port field. (By default, the Secure Access Service populates this field with port number 1494 for Citrix.)
8. Select the **Create an access control policy allowing Terminal Service access to this server** check box to enable access to the server specified in the Server Port box (enabled by default).
9. Enable intermediation using a Java client by selecting **Enable Java support** and then specifying which Java client the Secure Access Service should use.
10. Click **Save and Continue**.
11. Select the roles to which the resource profile applies in the Roles tab and click Add.  

The selected roles inherit the autopolicy and session bookmarks created by the resource profile. If it is not already enabled, the Secure Access Service also automatically enables the Terminal Services option in the Users > User Roles > Select\_Role > General > Overview page of the admin console for all of the roles you select.
12. Click **Save Changes**.
13. (Optional.) Modify the default session bookmark created by the Secure Access Service in the Bookmarks tab and/or create new ones. (By default, the Secure Access Service creates a session bookmark to the server defined in the Host box and displays it to all users assigned to the role specified in the Roles tab.)

**Related Documentation**

- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)
- [Creating a Citrix Resource Profile That Uses a Custom ICA File on page 666](#)
- [Defining a Hosted Java Applet Autopolicy on page 650](#)

---

## Defining a Bookmark for a Citrix Profile Using Default ICA Settings

When you create a Terminal Services resource profile, the Secure Access Service automatically creates a bookmark that links to the terminal server that you specified in



the resource profile. The Secure Access Service enables you to modify this bookmark as well as create additional bookmarks to the same terminal server.

To configure resource profile bookmarks for Citrix Terminal Services using default ICA settings:

1. In the admin console, select **Users > Resource Profiles > Terminal Services > Select Resource Profile > Bookmarks**.
2. Click the appropriate link in the Bookmark column if you want to modify an existing session bookmark. Or, click **New Bookmark** to create an additional session bookmark.



**NOTE:** Although it is generally easiest to create a resource profile session bookmark through the resource profile configuration page, you can choose to create one through the user roles page as well.

3. (Optional.) Change the name and description of the session bookmark. (By default, the Secure Access Service populates and names the session bookmark using the resource profile name.)
4. Specify how the terminal emulation window should appear to the user during a terminal session use configuration options in the Settings area of the bookmark configuration page.
5. Pass user credentials from the Secure Access Service to the terminal server so users can sign onto the terminal server without having to manually enter their credentials. You can do this by using the configuration options in the Session area of the bookmark configuration page.
6. Allow users to access specific applications on the terminal server by using configuration options in the Start Application area of the bookmark configuration page. In addition, you can use settings in this section to define auto-launch and session reliability options.
7. Allow users to access local resources such as printers and drives through the terminal session by using the configuration options in the Connect Devices section of the bookmark configuration page.
8. Specify the roles to which you want to display the session bookmark if you are configuring the session bookmark through the resource profile pages, under Roles:
  - **ALL selected roles**—Displays the session bookmark to all of the roles associated with the resource profile.
  - **Subset of selected roles**—Displays the session bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL selected roles list and click Add to move them to the Subset of selected roles list.
9. Click **Save Changes**.

#### Creating a Citrix Terminal Services Bookmark Through the User Roles Page

It is generally easiest to create a terminal services bookmark through the resource profile configuration pages, as explained in the previous topic. However, you can choose to create a resource profile session bookmark through the user roles page using the following instructions:

1. In the admin console, select **Users > User Roles > Select\_Role > Terminal Services > Sessions**.
2. Click **Add Session**.
3. Choose **Terminal Services Resource Profile** from the Type list. (The Secure Access Service does not display this option if you have not already created a terminal services resource profile.)
4. Select an existing resource profile that connects to a Citrix server using the default ICA file on the Secure Access Service. (The Secure Access Service automatically populates the Host and Server Port fields using settings from the selected resource profile.)
5. Click **OK**. (If you have not already associated the selected role with the resource profile, the Secure Access Service automatically makes the association for you. The Secure Access Service also enables any access control policies for the role that are required by the resource profile.)
6. If this role is not already associated with the selected resource profile, the Secure Access Service displays an informational message. If you see this message, click **Save Changes** to add this role to the resource profile's list of roles and to update the profile's autopolicies as required. Then, repeat the previous steps to create the session bookmark.



**NOTE:** When you create a resource profile session bookmark through the user roles page (instead of the standard resource profiles page), the Secure Access Service only associates the generated session bookmark with the selected role. The Secure Access Service does not assign the session bookmark to all of the roles associated with the selected resource profile.

7. (Optional.) Change the name and description of the session bookmark. (By default, the Secure Access Service populates and names the session bookmark using the resource profile name.)
8. Configure the bookmark's settings.

#### Related Documentation

- [About Terminal Services Resource Profiles on page 648](#)
- [Defining Display Options for the Citrix Terminal Services Session on page 663](#)
- [Defining SSO Options for the Citrix Terminal Services Session on page 663](#)
- [Defining Application, Auto-Launch, and Session Reliability Settings for the Citrix Terminal Services Session on page 664](#)
- [Defining Device Connections for the Citrix Terminal Services Session on page 665](#)

## Defining Display Options for the Citrix Terminal Services Session

When configuring a terminal services bookmark, you can specify how the terminal emulation window should appear to users during their terminal sessions.

To define display, auto-launch, and session reliability options:

1. Create a terminal services bookmark or edit an existing bookmark.
2. Scroll to the Settings area of the bookmark configuration page.
3. Select an option from the Screen Size drop-down list if you want to change the size of the terminal services window on the user's workstation. (By default, the Secure Access Service sets the window size to full screen.)
4. Select **8-bit**, **15-bit**, **16-bit**, **24-bit**, or **32-bit** color from the Color Depth list if you want to change the color-depth of the terminal session data. (By default, the **8-bit** sets the color depth to 8-bit.)



**NOTE:** When configuring a Citrix session bookmark, note that the setting you choose here and the user's local desktop setting both affect the client's color-depth display. If these settings do not match, the user sees the lower of the two color-depths during his session. For example, if you select 16-bit color during Secure Access Service configuration, but the user's local desktop is set to 8-bit, the user sees 8-bit color depth during his session.

5. Click **Save Changes**.

### Related Documentation

- [Defining a Bookmark for a Citrix Profile Using Default ICA Settings on page 660](#)

## Defining SSO Options for the Citrix Terminal Services Session

When configuring a terminal services bookmark, you can configure the Secure Access Service to pass user credentials from the Secure Access Service to the terminal server so that the user does not have to manually enter his username and password. The Secure Access Service passes the specified credentials when a user clicks the session bookmark. If the credentials fail, the server prompts the user to manually enter his username and password.

To define single sign-on options:

1. Create a terminal services bookmark or edit an existing bookmark.
2. Scroll to the Authentication area of the bookmark configuration page.
3. Specify the username that the Secure Access Service should pass to the terminal server in the Username field. You can enter a static username or a variable. Enter the `<username>` variable to pass the username stored in the Secure Access Service's primary authentication server. Or use the following syntax to submit the username

for the secondary authentication server: <username@SecondaryServerName> or <username[2]>.

4. Select **Password** if you want to specify a static password or select **Variable Password** if you want to use the password stored in the Secure Access Service's primary or secondary authentication server. To use the password from the primary authentication server, enter the <password> variable. Or use the following syntax to submit the password for the secondary authentication server:  
<Password@SecondaryServerName> or <Password[2]>.
5. (Default ICA file and listed applications only.) Select **Use domain credentials** to pass the user's cached domain credentials to the Citrix Metaframe server (also called pass-through authentication). When you select this option, the Secure Access Service uses the Citrix Program Neighborhood client to intermediate the Citrix terminal session.



**NOTE:** If you want to download the Program Neighborhood client, select **Users > User Roles > Select\_Role > Terminal Services > Options** in the admin console and enter the URL in the **Download from URL** box. See the Citrix Web site for the location of the latest Program Neighborhood client cab file.

When you select the **Use domain credentials** option, you must also enable SSO through the user's settings file (appsrv.ini). If the user has already successfully signed into the Metaframe server using cached domain credentials, this setting should already be enabled. Otherwise, you or the user must:

- **Set EnableSSOnThruICAFile=On** in appsrv.ini. You can locate appsrv.ini in the %HOMEPATH%\Application Data\ICAClient directory.
- **Set UseLocalUserAndPassword=On** in the ICA file.

If you have not enabled SSO through the INI file, the user is prompted to manually enter his credentials when he tries to access the Metaframe server through the Secure Access Service.

6. Click **Save Changes**.

#### Related Documentation

- [Defining a Bookmark for a Citrix Profile Using a Custom ICA File on page 668](#)

## Defining Application, Auto-Launch, and Session Reliability Settings for the Citrix Terminal Services Session

When configuring a terminal services bookmark, you can specify that users can only access specific applications on the terminal server.

To define applications that users can access:

1. Create a terminal services bookmark or edit an existing bookmark.
2. Scroll to the **Start Application** area of the bookmark configuration page.

3. Select the **Launch seamless window** check box to have the Windows application server manage the display of the application. This allows an application's windows to behave in the same way as an application running on a Windows application server, regardless of the user's desktop environment.



**NOTE:** If SSO is not configured, seamless window is supported only on Remote Desktop Protocol (RDP) 6.0 and later.

Enter the server alias name in the Alias Name field (applicable only for servers running Windows 2008 and later).

4. Specify where the application's executable file resides on the terminal server in the Path to application box (visible only when you clear Launch seamless window). For example, you might enter the following directory for the Microsoft Word application:

C:\Program Files\Microsoft Office\Office10\WinWord.exe

5. Specify where the terminal server should place working files for the application in the Working directory field. For example, you might specify that Microsoft Word should save files to the following directory by default:

C:\Documents and Settings\\My Documents



**NOTE:** You can use Secure Access Service session variables such as <username> and <password> in the Path to application and Working directory boxes. For example, when specifying an application path, you might want to include the <username> variable to personalize the location. For example, C:\Documents and Settings\\My Documents.

6. Select the **Auto-launch** check box if you want to automatically launch this terminal service session bookmark when users sign into the Secure Access Service. When you select this option, the Secure Access Service launches the terminal services application in a separate window when the user signs into the Secure Access Service.
7. Select **Session Reliability and Auto-client reconnect** to keep ICA sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application they are using until the network connectivity resumes or the session reliability time-out has expired (the time-out value is defined by the Citrix product). Enter the port to use in the Port to be enabled box.
8. Click **Save Changes**.

#### Related Documentation

- [System Variables and Examples on page 1186](#)

## Defining Device Connections for the Citrix Terminal Services Session

When configuring a terminal services bookmark, you can specify local resources that users can access through the terminal session.

For the Connect Devices settings to take effect, they must also be enabled on the Metaframe server. For example, if you enable Connect Drives on the Secure Access Service, but disable it on the Metaframe server, then the Metaframe server will block access to local drives. Note that if you clear the Configure access to local resources check box, the settings on the Metaframe server take effect.

To define local resources that users can access:

1. Create a terminal services bookmark or edit an existing bookmark.
2. Scroll to the Connect Devices area of the bookmark configuration page.
3. Select **Connect local drives** to connect the user's local drive to the terminal server, enabling the user to copy information from the terminal server to his local client directories.
4. Select **Connect local printers** to connect the user's local printers to the terminal server, enabling the user to print information from the terminal server to his local printer.
5. Select **Connect COM Ports** to connect the user's COM ports to the terminal server, allowing communication between the terminal server and the devices on his serial ports.

When you enable local resources through the terminal server, each user can only access his own local resources. For instance, user 1 cannot see user 2's local directories.

6. Click **Save Changes**.

**Related  
Documentation**

- [Defining a Bookmark for a Citrix Profile Using Default ICA Settings on page 660](#)
- [Defining a Bookmark for a Windows Terminal Services Profile on page 653](#)

---

## Creating a Citrix Resource Profile That Uses a Custom ICA File

---

Use this type of resource profile to enable a terminal session to a Citrix Metaframe server using settings that you specify in a customized ICA file. Use custom ICA files to enable terminal sessions to Citrix Metaframe servers or NFuse servers governing Citrix server farms (in other words, to load balance). You may also use custom ICA files to link to single servers, if necessary. When you select this option, the Secure Access Service uses the session parameters defined in the specified custom ICA file.

To enable the connection between the Secure Access Service and the Citrix server farm, you must use the TCP/IP+HTTP protocol for browsing and specify the Citrix Metaframe or NFuse server port and IP address. The Secure Access Service does not support UDP port-forwarding.

To create a Citrix resource profile that uses a custom ICA file:

1. In the admin console, select **Users > Resource Profiles > Terminal Services**.
2. Click **New Profile**. Or select an existing profile from the list.
3. Select **Citrix using custom ICA file** from the Type list.

4. Specify the ICA file that contains the session parameters that you want use in the Custom ICA File box. Note that you may download and customize the following ICA files from the Secure Access Service:
  - ICA file that comes with the Secure Access Service—To customize this file, click the **Open** link, save the file to your local machine, customize the file as required, and upload it back to the Secure Access Service using the Browse option. If you customize this file, you must replace the following parameters in the default.ica file: <CITRIX\_CLIENT\_NAME>, <APPDATA> and <TARGET\_SERVER>.
  - ICA file that you have already associated with the resource profile—To customize this file, click the **Current ICA File** link, save the file to your local machine, and customize the file as required. Once you make changes, you must upload the revised version to the Secure Access Service using the Browse option.

Before uploading the ICA file, you should test it to make sure it initiates the Citrix session correctly. To test, create an ICA file and access it directly. If the file displays the Citrix session correctly then it should work through the Secure Access Service.

If SSO is configured in the custom ICA bookmark, seamless mode is ignored and the application is launched in non-seamless mode.

When using the Java rewriting technology to tunnel Citrix JICA applets through the Secure Access Service, you must set the proxyType parameter in the ICA file to None (even if a client-side proxy is configured in the browser).

5. Enter a unique name and optionally a description for the resource profile. (This name becomes the default session bookmark's name.)
6. Enable access to the servers specified in the custom ICA file:
  - a. Select the **Autopolicy: Terminal Services Access Control** check box.
  - b. Specify the Metaframe servers to which you want to enable access in the Resource field.
  - c. Choose **Allow** to enable access to the specified resource or **Deny** to block access to the specified resource from the Action list.
  - d. Click **Add**.
7. Enable intermediation using a Java client by selecting Enable Java support.
 

If you select the **Enable Java support** option and have a custom ICA file that you uploaded to the Secure Access Service, your HTML file is auto-populated with references to your custom ICA file. No additional HTML code needs to be added.
8. Click **Save and Continue**.
9. Select the roles to which the resource profile applies in the Roles box and click **Add**.

The selected roles inherit the autopolicy and session bookmarks created by the resource profile. If it is not already enabled, the Secure Access Service also automatically enables the Terminal Services option in the Users > User Roles > Select\_Role > General > Overview page of the admin console for all of the roles you select.

10. Click **Save Changes**.
11. (Optional) Modify the default session bookmark created by the Secure Access Service in the Bookmarks tab and/or create new ones. (By default, the Secure Access Service creates a session bookmark to the server defined in your custom ICA file and displays it to all users assigned to the role specified in the Roles tab.)

**Related  
Documentation**

- [Defining a Hosted Java Applet Autopolicy on page 650](#)
- [Defining a Bookmark for a Citrix Profile Using a Custom ICA File on page 668](#)

---

## Defining a Bookmark for a Citrix Profile Using a Custom ICA File

---

When you create a terminal services resource profile, the Secure Access Service automatically creates a bookmark that links to the terminal server that you specified in the resource profile. The Secure Access Service enables you to modify this bookmark as well as create additional bookmarks to the same terminal server.

To configure resource profile bookmarks for Citrix Terminal Services using custom ICA settings:

1. In the admin console, select **Users > Resource Profiles > Terminal Services > Select\_Resource\_Profile > Bookmarks**.  
  
Click the appropriate link in the Bookmark column if you want to modify an existing session bookmark. Or, click **New Bookmark** to create an additional session bookmark.  
  
Although it is generally easiest to create a resource profile session bookmark through the resource profile configuration page, you can choose to create one through the user roles page as well.
2. (Optional.) Change the name and description of the session bookmark. (By default, the Secure Access Service populates and names the session bookmark using the resource profile name.)
3. Pass user credentials from the Secure Access Service to the terminal server so that users can sign onto the terminal server without having to manually enter their credentials. You can do this by configuring options in the Session area of the bookmark configuration page.
4. Automatically launch this terminal service session bookmark when a user signs in to the Secure Access Service by selecting the **Auto-launch** check box. When you select this option, the Secure Access Service launches the terminal services application in a separate window when the user signs into the Secure Access Service.
5. Under Roles, specify the roles to which you want to display the session bookmark:
  - **ALL selected roles**—Displays the session bookmark to all of the roles associated with the resource profile.



- **Subset of selected roles**—Displays the session bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL selected roles list and click **Add** to move them to the Subset of selected roles list.
6. Click **Save Changes**.

**Related  
Documentation**

- [About Terminal Services Resource Profiles on page 648](#)
- [Defining SSO Options for the Citrix Terminal Services Session on page 663](#)

## Creating a Citrix Profile That Lists Published Applications

Citrix created published applications to satisfy the need for security. It is dangerous to allow any executable to be run on the server. With published applications, only applications that are allowed to be run are published.

With the Secure Access Service, these published applications are displayed on the Secure Access Service index page as terminal services bookmarks.

To create a Citrix profile that lists published applications:

1. In the admin console, select **Users > Resource Profiles > Terminal Services**.
2. Click **New Profile**.
3. Select **Citrix Listed Applications** from the Type list.
4. Enter a unique name and optionally a description for the resource profile. This name becomes the default session bookmark's name.
5. Enter the IP address and port of the Citrix MetaFrame server where the XML service is running.

You do not need to enter the port number if you are using the default value. The default port is 80 (if SSL is selected, the default port is 443).

You can enter more than one server. If the connection fails on one server, the next server in the list is used.

6. Click the **Use SSL for connecting to Citrix XML Service** check box to send the password through SSL instead of cleartext.



**NOTE:** Although cleartext is supported, we recommend you always use SSL to avoid any security issues.

7. Enter the username, password, and domain name for connecting to the Citrix Metaframe server where the XML service is running.

You can enter variable credentials such as <USERNAME> and <PASSWORD>. If you use variable credentials, the Subset of selected Applications option is disabled in the Bookmarks window.

When the user accesses the application list, their credentials are submitted to the Citrix XML service, substituting the session context variables <USERNAME> and <PASSWORD>. Only the user's specific applications (as determined by the Citrix administrator) are returned.

8. Enable access to the servers specified in the custom ICA file:
  - a. Select the **Autopolicy: Terminal Services Access Control** check box.
  - b. Specify the Metaframe servers to which you want to enable access in the Resource field.
  - c. Choose **Allow** to enable access to the specified resource or **Deny** to block access to the specified resource from the Action list.
  - d. Click **Add**.
9. Enable intermediation using a Java client by selecting **Enable Java support** and then specifying which Java client the Secure Access Service should use.
10. Click **Save and Continue**.
11. Select the roles to which the resource profile applies in the Roles tab and click Add.

The selected roles inherit the autopolicy and session bookmarks created by the resource profile. If it is not already enabled, the Secure Access Service also automatically enables the Terminal Services option in the Users > User Roles > Select\_Role > General > Overview page of the admin console for all of the roles you select.
12. Click **Save Changes**.
13. (Optional.) Modify the default session bookmark created by the Secure Access Service in the Bookmarks box and/or create new ones.

**Related  
Documentation**

- [Defining a Bookmark for a Citrix Profile Listing Applications on page 670](#)
- [System Variables and Examples on page 1186](#)

---

## Defining a Bookmark for a Citrix Profile Listing Applications

---

When you create a terminal services resource profile, the Secure Access Service automatically creates a bookmark that links to the terminal server that you specified in the resource profile. The Secure Access Service enables you to modify this bookmark as well as create additional bookmarks to the same terminal server.

To configure resource profile bookmarks for Citrix terminal services list applications:

1. In the admin console, select **Users > Resource Profiles > Terminal Services > Resource\_Profile > Bookmarks**.

Click the appropriate link in the Bookmark column if you want to modify an existing session bookmark. Or, click **New Bookmark** to create an additional session bookmark.

Although it is generally easiest to create a resource profile session bookmark through the resource profile configuration page, you can choose to create one through the user roles page as well.

2. (Optional.) Change the name and description of the session bookmark. (By default, the Secure Access Service populates and names the session bookmark using the resource profile name.)
3. Under Applications, select the applications you want available to the end user.
  - **ALL Applications**—Allow all executables on the server to be available to the end user.
  - **Subset of selected applications**—Select the executables from the Available list and click **Add** to allow only those applications to be run. The Available list is automatically populated from the Metaframe server.

This option is disabled when you enter variable credentials, such as <USERNAME> and <PASSWORD> while defining the resource profile.
4. Under Settings, specify how the terminal emulation window should appear to users during their terminal sessions.



**NOTE:** You cannot change the IP address or XML Service running port for connecting to the XML Service or the Java client to use for intermediation.

5. Under Session, you can configure the Secure Access Service to pass user credentials from the Secure Access Service to the terminal server so that the user does not have to manually enter his username and password.
    - Select an option from the Screen Size drop-down list if you want to change the size of the terminal services window on the user's workstation.
    - (Optional.) Select **8-bit**, **15-bit**, **16-bit**, **24-bit**, or **32-bit** color from the Color Depth list if you want to change the color-depth of the terminal session data.
5. Under Session, you can configure the Secure Access Service to pass user credentials from the Secure Access Service to the terminal server so that the user does not have to manually enter his username and password.
    - Specify the username that the Secure Access Service should pass to the terminal server in the Username box. You can enter a static username or a variable.
    - Select **Password** if you want to specify a static password or select **Variable Password** if you want to use the password stored in the Secure Access Service's primary or secondary authentication server.
    - Select **Use domain credentials** to pass the user's cached domain credentials to the Citrix Metaframe server (also called pass-through authentication). When you select this option, the Secure Access Service uses the Citrix Program Neighborhood client to intermediate the Citrix terminal session.



**NOTE:** If you want to download the Citrix Program Neighborhood client, select **Users > User Roles > Role Name > Terminal Services > Options** of the admin console and enter the following URL in the Download from URL box:

<http://download2.citrix.com/FILES/en/products/client/ica/client9230/wficat.cab>

When you select the Use domain credentials option, you must also enable SSO through the user's settings file (appsrv.ini).

6. Under Connect Devices, specify which user devices to connect to the terminal server.
  - **Connect local drives**—Connect the user's local drive to the terminal server, enabling the user to copy information from the terminal server to his local client directories.
  - **Select Connect local printers**—Connect the user's local printers to the terminal server, enabling the user to print information from the terminal server to his local printer.
  - **Select Connect COM Ports**—Connect the user's COM ports to the terminal server, allowing communication between the terminal server and the devices on his serial ports.
7. Under Roles, specify the roles to which you want to display the session bookmark:
8. Click **Save Changes**.

**Related Documentation**

- [Creating Resource Profiles Using Citrix Web Applications on page 471](#)
- [Defining SSO Options for the Citrix Terminal Services Session on page 663](#)

## Creating Session Bookmarks to Your Terminal Server

When you enable the Terminal Services option through the admin console, you can create session bookmarks to your terminal server. A terminal services session bookmark defines information about the terminal server to which users can connect and (optionally) applications that they can use on the terminal server. The session bookmarks that you define appear on the Terminal Services panel in the end-user console for users who map to the appropriate role.

You can use two different methods to create terminal services session bookmarks:

- **Create session bookmarks through existing resource profiles (recommended)**—When you select this method, the Secure Access Service automatically populates the session bookmark with key parameters (such as the session type) using settings from the resource profile. Additionally, while you are creating the associated resource profile, the Secure Access Service guides you through the process of creating any required policies to enable access to the session bookmark.
- **Create standard session bookmarks**—With this option, you must manually enter all session bookmark parameters during configuration. Additionally, you must enable access to the Terminal Services feature and create resource policies that enable access to the servers defined in the session bookmark.



**NOTE:** If you enable the Terminal Services option but do not give users the ability to create their own session bookmarks, make sure that you configure session bookmarks for them. Otherwise, users cannot use this feature.

You can also enable users to create their own session bookmarks on the Secure Access Service homepage and browse to the terminal servers using the Secure Access Service browse bar. Or, you can create links from external sites to a terminal services bookmarks.

#### Related Documentation

- [Defining a Bookmark for a Windows Terminal Services Profile on page 653](#)
- [Defining a Bookmark for a Citrix Profile Using a Custom ICA File on page 668](#)
- [Creating Advanced Terminal Services Session Bookmarks on page 673](#)
- [Creating Links from an External Site to a Terminal Services Session Bookmark on page 679](#)
- [Specifying General Terminal Services Options on page 685](#)

## Creating Advanced Terminal Services Session Bookmarks

The information in this topic is provided for backwards compatibility. We recommend that you configure access to Windows terminal servers and Citrix servers through resource profiles instead, because they provide a simpler, more unified configuration method. Resource profile also contain features (such as the ability to use Java RDP clients to support Macintosh and Linux users) which are not available through roles.

Make sure to enter a unique set of parameters when defining a terminal services bookmark. If you create two bookmarks that contain the same set of parameters, the Secure Access Service deletes one of the bookmarks from the end user view. You can still see both bookmarks in the administrator console.

To create a session bookmark for terminal sessions:

1. In the admin console, select **Users > User Roles > Role > Terminal Services > Sessions**.
2. Click **Add Session**.
3. Select **Standard** in the Type drop-down list.
4. Specify the type of user session you want to create from the Session Type list:
  - **Windows Terminal Services**—Enables a terminal session to a Windows terminal server.
  - **Citrix using default ICA**—Enables a terminal services session to a Citrix Metaframe server. When you select this option, the Secure Access Service uses default Citrix session parameters stored on the Secure Access Service.

(Existing sessions only.) You can also use the Open link to open the Secure Access Service's default ICA file, which you can then save to your local machine and customize as required. If you customize this file, you must replace the following

parameters in the default.ica file: <CITRIX\_CLIENT\_NAME>, <APPDATA>, and <TARGET\_SERVER>.

- **Citrix using custom ICA file**—Enables a terminal services session to a Citrix Metaframe or NFuse server governing a Citrix server farm. When you select this option, the Secure Access Service uses the session parameters defined in the specified custom ICA file, thus removing the Session Reliability, Start Application, and Connect Devices configuration items from the current page.



**NOTE:** Because the Secure Access Service does not support UDP port-forwarding, you must use the TCP/IP+HTTP protocol for browsing and specify the Citrix Metaframe or NFuse server port and IP address to enable the connection between the Secure Access Service and the Citrix server farm.

5. Enter a name and (optionally) a description for the session bookmark.
6. In the Host field, specify the host name or IP address of the Windows terminal server or Metaframe terminal server.
7. In the Client Port and Server Port fields, enter the ports on which the user client communicates and terminal server listens.

If you specify a client port and the Juniper terminal services client is unable to bind to this port, then the terminal services client will fail. However, if you leave the Client Port field blank, the Juniper terminal services client dynamically selects an available port.

8. (Windows Terminal Services and Citrix using default ICA only) If you want to specify the screen size and color depth options for the terminal emulation window, use configuration options in the Settings section.
9. If you want to pass user credentials from the Secure Access Service to the terminal server, enabling users to sign onto the terminal server without having to manually enter their credentials, use configuration options in the Session section.
10. If you only want to allow users to access specific applications on the terminal server, use configuration options in the Start Application section of the bookmark configuration page. In addition, you can use settings in this section to define auto-launch and session reliability options.
11. (Windows Terminal Services and Citrix using default ICA only) If you want to allow users to access local resources such as printers and drives through the terminal session, use configuration options in the Connect Devices section of the bookmark configuration page.
12. (Windows Terminal Services only) If you want to specify how the terminal emulation window should appear to the user during a terminal session, use configuration options in the Desktop Settings section.
13. Click **Save Changes** or **Save + New**.

### Defining Screen Size and Color Depth Options for the Terminal Services Session

When configuring a terminal services bookmark, you can specify how the terminal emulation window should appear to users during their terminal sessions.

The options in this section only apply to Windows Terminal Services bookmarks, Citrix using default ICA bookmarks and Citrix listed applications bookmarks.

To define display, auto-launch, and session reliability options:

1. Create a terminal services session bookmark or edit an existing session bookmark.
2. Scroll to the Settings section of the bookmark configuration page.
3. Select an option from the Screen Size drop-down list if you want to change the size of the terminal services window on the user's workstation. (By default, the Secure Access Service sets the window size to full screen.)

If you select the Full Screen option and are connecting to a Windows terminal server, the Secure Access Service needs to modify the user's hosts file in order to display the correct host name in the terminal services window. If the user does not have the proper rights to modify the hosts file, the Secure Access Service displays the loopback address instead.

Also note that in order to restore the hosts file to its original state after running the terminal services window, the user must properly close his application. Otherwise, other applications that use the hosts file (such as JSAM and Host Checker) might not run properly. The user can also restore his hosts file to its original state by rebooting his system or by renaming the backup hosts file (hosts\_ive.bak).

4. Select a value from the Color Depth list if you want to change the color-depth of the terminal session data. (By default, the Secure Access Service sets the color depth to 8-bit.)

When configuring a Citrix session bookmark, note that the setting you choose here and the user's local desktop setting both affect the client's color-depth display. If these settings do not match, the user sees the lower of the two color-depths during his session. For example, if you choose 16-bit color during Secure Access Service configuration, but the user's local desktop is set to 8-bit, the user sees 8-bit color depth during his session.

5. Click **Save Changes** or **Save + New**.

### Defining SSO Options for the Terminal Services Session

When configuring a terminal services bookmark, you can configure the Secure Access Service to pass user credentials from the Secure Access Service to the terminal server so that the user does not have to manually enter his username and password. The Secure Access Service passes the specified credentials when a user clicks the session bookmark. If the credentials fail, the server prompts the user to manually enter his username and password.

To define single sign-on options:

1. Create a terminal services session bookmark or edit an existing session bookmark.
2. Scroll to the Authentication section of the bookmark configuration page.

3. In the Username field, specify the username that the Secure Access Service should pass to the terminal server. You can enter a static username or a variable. Enter the <username> variable to pass the username stored in the Secure Access Service's primary authentication server. Or use the following syntax to submit the username for the secondary authentication server: <username@SecondaryServerName> or <username[2]>.
4. Select **Password** if you want to specify a static password or select **Variable Password** if you want use the password stored in the Secure Access Service's primary or secondary authentication server. To use the password from the primary authentication server, enter the <password> variable. Or use the following syntax to submit the password for the secondary authentication server: <Password@SecondaryServerName> or <Password[2]>.
5. (Citrix using default ICA or listed applications) Select **Use domain credentials** to pass the user's cached domain credentials to the Citrix Metaframe server (also called pass-through authentication). When you select this option, the Secure Access Service uses the Citrix Program Neighborhood client to intermediate the Citrix terminal session.



**NOTE:** If you want to download the Program Neighborhood client, go to the **Users > User Roles > Select Role > Terminal Services > Options** page of the admin console and enter the following URL in the Download from URL field:

<http://download2.citrix.com/FILES/en/products/client/ica/client9230/wficat.cab>

When you select the Use domain credentials option, you must also enable SSO through the user's settings file (appsrv.ini). If the user has already successfully signed into the Metaframe server using cached domain credentials, this setting should already be enabled. Otherwise, you or the user must:

- Set EnableSSOnThruICAFile=On in appsrv.ini. You can locate appsrv.ini in the %HOMEPATH%\Application Data\ICAClient directory.

Set UseLocalUserAndPassword=On in the ICA file.

If you have not enabled SSO through the INI file, the user is prompted to manually enter his credentials when he tries to access the Metaframe server through the Secure Access Service.

6. Click **Save Changes** or **Save + New**.

### Defining Application Settings for the Terminal Services Session

When configuring a terminal services bookmark, you can specify that users can only access specific applications on the terminal server. Additionally, you can define auto-launch and session reliability options for the session.

To define applications that users can access:

1. Create a terminal services session bookmark or edit an existing session bookmark.
2. Scroll to the Start Application section of the bookmark configuration page.



If you specify Citrix using custom ICA file in the Session Type configuration section, the Start Application configuration item is not available.

3. (Windows Terminal Services and Citrix using default ICA only) In the Path to application field, specify where the application's executable file resides on the terminal server. For example, you might enter the following directory for the Microsoft Word application:

C:\Program Files\Microsoft Office\Office10\WinWord.exe

4. (Windows Terminal Services and Citrix using default ICA only) In the Working directory field, specify where the terminal server should place working files for the application. For example, you might specify that Microsoft Word should save files to the following directory by default:

C:\Documents and Settings\\My Documents

You can use session variables such as <username> and <password> in the Path to application and Working directory fields. For example, when specifying an application path, you might want to include the <username> variable to personalize the location. For example: C:\Documents and Settings\\My Documents.

5. (Citrix using default ICA only) Select **Session Reliability and Auto-client reconnect** to keep ICA sessions active and on the user's screen when network connectivity is interrupted. Users continue to see the application they are using until the network connectivity resumes or the session reliability time-out has expired (the time-out value is defined by the Citrix product). Enter the port to use in Port to be enabled.
6. Select the **Auto-launch** checkbox if you want to automatically launch this Terminal Service session bookmark when users sign into the Secure Access Service. When you select this option, the Secure Access Service launches the terminal services application in a separate window when the user signs into the Secure Access Service.
7. Click **Save Changes** or **Save + New**.

### Defining Device Connections for the Terminal Services Session

When configuring a terminal services bookmark, you can specify local resources that users can access through the terminal session.

The options in this section only apply to Windows Terminal Services bookmarks and Citrix using default ICA bookmarks.

The Connect Devices options that you specify at the role-level control whether end-users can enable or disable access to local resources when they configure their own bookmarks. These role-level options do not control whether users can access local resources through a bookmark created by the Secure Access Service administrator.

To define local resources that users can access:

1. Create a terminal services session bookmark or edit an existing session bookmark.
2. Scroll to the Connect Devices section of the bookmark configuration page.

If you specify Citrix using custom ICA file in the Session Type configuration section, the Connect Devices configuration item is not available.

3. Select **Connect local drives** to connect the user's local drive to the terminal server, enabling the user to copy information from the terminal server to his local client directories.
4. Select **Connect local printers** to connect the user's local printers to the terminal server, enabling the user to print information from the terminal server to his local printer.
5. Select **Connect COM Ports** to connect the user's COM ports to the terminal server, allowing communication between the terminal server and the devices on his serial ports.
6. (Windows Terminal Services only) Select **Allow Clipboard Sharing** if you want to allow the contents of the clipboard to be shared between the user's host computer and the terminal server. Due to the limitations in the pre-6.0 versions of the RDP client, disabling the Allow Clipboard Sharing option will automatically disable the Connect local drives, Connect local printers, and Connect COM Ports options.

When you enable local resources through the terminal server, each user can only access his own local resources. For instance, user 1 cannot see user 2's local directories.

7. (Windows Terminal Services only) Select **Connect smart cards** to allow users to use smart cards to authenticate their remote desktop sessions.
8. (Windows Terminal Services only) Select **Sound Options** to enable sound during the remote session. Choose Bring to this computer to redirect audio to the local computer. Choose Leave at remote computer to play the audio only at the server.



**NOTE:** Smart cards and sound options are supported by Microsoft Remote Desktop Protocol versions 5.1 and later.

9. Click **Save Changes** or **Save + New**.

### Defining Desktop Settings for the Terminal Services Session

When configuring a terminal services bookmark, you can specify how the terminal emulation window should appear to the user during a terminal session.

The options in this section only apply to Windows Terminal Services bookmarks.

To define display settings for the users' sessions:

1. Create a terminal services session bookmark or edit an existing session bookmark.
2. Scroll to the Display Settings section of the bookmark configuration page.
3. Select **Desktop background** if you want to display a wallpaper background to users. If you do not select this option, the background is blank.
4. Select **Show contents of window while dragging** if you want to show the contents of the Windows Explorer window while users move the windows on their desktops.
5. Select **Menu and window animation** if you want to animate the movement of windows, menus, and lists.

6. Select **Themes** if you want to allow users to set Windows themes in their terminal server windows.
7. Select **Bitmap Caching** if you want to improve performance by minimizing the amount of display information that is passed over a connection.
8. Select **Font Smoothing (RDP 6.0 onwards)** to make text smoother and easier to read. This option only works on Windows Vista computers running RDP clients that are version 6.0 or later.
9. Select **Desktop Composition (RDP 6.0 onwards)** to allow desktop composition. With desktop composition, individual windows no longer draw directly to the screen. Instead, their drawing is redirected to video memory, which is then rendered into a desktop image and presented on the display.
10. Click **Save Changes** or **Save + New**.

#### Related Documentation

- [About Terminal Services Resource Profiles on page 648](#)
- [System Variables and Examples on page 1186](#)
- [Specifying the Terminal Services Resource Option on page 689](#)
- [Defining SSO Options for the Citrix Terminal Services Session on page 663](#)
- [Defining Application Settings for the Windows Terminal Services Session on page 656](#)
- [Defining Device Connections for the Windows Terminal Services Session on page 657](#)
- [Defining Desktop Settings for the Windows Terminal Services Session on page 659](#)
- [Multiple Sign-In Credentials Execution on page 339](#)

## Creating Links from an External Site to a Terminal Services Session Bookmark

When creating a link to a terminal services session bookmark from another site, you can construct either of the following types of URLs:

- URL that includes all necessary parameters—Create a URL that includes all of the parameters that you want to pass to the terminal services program, such as the host, ports, and terminal window parameters. When constructing the URL, use the following syntax:

```
https://<SASeriesAppliance>/dana/term/winlaunchterm.cgi?<param1>=<value1>&<param2>=<value2>
```

When constructing your URL, you can use the case-insensitive parameter names described in Table 38. If you want to include more than one parameter in the session bookmark, string them together using ampersand characters (&). For example:

```
https://<SASeriesAppliance>/dana/term/winlaunchterm.cgi?Host=<Host>&Port=<Port>&WinId=<WinId>&Session=<Session>
```

- URL to terminal services bookmark—Create a URL that simply points to a session bookmark that you have already created on the Secure Access Service. When constructing the URL, use the following syntax:

```
https://<SASeriesAppliance>/dana/term/winlaunchterm.cgi?bmname=<bookmarkName>
```

Within the URL, only define the bmName parameter.

When using the Secure Access Service to host Terminal Services session bookmarks, you must:

- Enable the User can add sessions option in the Users > User Roles > Select Role > Terminal Services > Options page. If you do not select this option, users cannot link to the Terminal Services session bookmarks from external sites.
- Create a policy that prevents the Secure Access Service from rewriting the link and the page that contains the link using settings in the Users > Resource Policies > Web > Rewriting > Selective Rewriting page of the admin console.

Additionally, we recommend that you use https protocol instead of http. Otherwise, when users launch the session bookmark, they see an insecure site warning.



**NOTE:** If you create links on external servers to Terminal Services bookmarks on the Secure Access Service and you are using multiple customized sign-in URLs, some restrictions occur.

**Table 46: Case-Insensitive Terminal Services Session Bookmark Parameter Names**

Parameter Name	Description and Possible Values	Example
host	Required. Host name or IP address of the Windows terminal server or Metaframe terminal server.	<code>https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer</code>
type	Type of terminal server. Possible values include Windows or Citrix.	<code>https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;type=Wind</code>
clientPort	Port on which the user client communicates.	<code>https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;clientPort=</code>
serverPort	Port on which the terminal server listens. Default values are 3389 for Windows and 1494 for Citrix.	<code>https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;serverPort=</code>

Table 46: Case-Insensitive Terminal Services Session Bookmark Parameter Names (*continued*)

user	Username to pass to the terminal server. You can enter a static username, such as JDoe, or a variable username such as <user> or <username>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;user=jDoe">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;user=jDoe</a>
password	Password to pass the terminal server.	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;user=jDoe&amp;password=Password">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;user=jDoe&amp;password=Password</a>
bmname	Specifies the session bookmark name	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?bmname=&lt;bookmarkname&gt;">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?bmname=&lt;bookmarkname&gt;</a>
screenSize	Terminal services window's size. Possible values: <ul style="list-style-type: none"> <li>• fullScreen</li> <li>• 800x600</li> <li>• 1024x768</li> <li>• 1280x1024</li> </ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;screenSize=fullScreen">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;screenSize=fullScreen</a>
colorDepth	Terminal services window's color depth, in bits. Possible values: <ul style="list-style-type: none"> <li>• 8</li> <li>• 15</li> <li>• 16</li> <li>• 24</li> <li>• 32</li> </ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;colorDepth=32">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;colorDepth=32</a>
startApp	Specifies the path of an application executable to start.	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;startApp=C:\Office\Office10\WinWord.exe">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;startApp=C:\Office\Office10\WinWord.exe</a>
startDir	Specifies where the terminal server should place working files for the application.	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;startapp=C:\temp">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;startapp=C:\temp</a>

Table 46: Case-Insensitive Terminal Services Session Bookmark Parameter Names (*continued*)

connectDrives	Specifies whether the user can connect his local drive to the terminal server. Possible values: <ul style="list-style-type: none"><li>• Yes</li><li>• No</li></ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;connectDrives">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;connectDrives</a>
connectPrinters	Specifies whether the user can connect his local printer to the terminal server. Possible values: <ul style="list-style-type: none"><li>• Yes</li><li>• No</li></ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;connectPrinters">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;connectPrinters</a>
connectComPorts	Specifies whether the user can connect his COM ports to the terminal server. Possible values: <ul style="list-style-type: none"><li>• Yes</li><li>• No</li></ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;connectComPorts">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;connectComPorts</a>
allowclipboard	Specifies whether the user can share the contents of the clipboard between the user's host computer and the terminal server. Possible values: <ul style="list-style-type: none"><li>• Yes</li><li>• No</li></ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;allowclipboard">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;allowclipboard</a>

Table 46: Case-Insensitive Terminal Services Session Bookmark Parameter Names (*continued*)

desktopbackground	Specifies whether to display your current wallpaper setting. Possible values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;desktopbackground=YourValue">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;desktopbackground=YourValue</a>
showDragContents	Specifies whether to show the contents of the Windows Explorer window while moving the window around your desktop. Possible values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;showDragContents=YourValue">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;showDragContents=YourValue</a>
showMenuAnimation	Specifies whether to animate the movement of windows, menus, and lists. Possible values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;showMenuAnimation=YourValue">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;showMenuAnimation=YourValue</a>
themes	Specifies whether to allow users to set Windows themes in their terminal server windows. Possible values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;themes=YourValue">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;themes=YourValue</a>

Table 46: Case-Insensitive Terminal Services Session Bookmark Parameter Names (*continued*)

bitmapcaching	Specifies whether to improve performance by minimizing the amount of display information that must be passed over a connection. Possible values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;bitmapcaching">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;bitmapcaching</a>
fontsmoothing	Specifies whether to make text smoother and easier to read. This option only works on Windows Vista computers running RDP clients that are version 6.0 or later. Possible values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;fontsmoothing">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;fontsmoothing</a>
desktopcomposition	Specifies whether to enable desktop composition. Possible values: <ul style="list-style-type: none"> <li>• Yes</li> <li>• No</li> </ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;desktopcomposition">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;desktopcomposition</a>
soundoptions	Specifies whether to enable sound. Possible values: <ul style="list-style-type: none"> <li>• 0—disable sound</li> <li>• 1—bring sound to this computer</li> <li>• 2—leave sound at remote computer</li> </ul>	<a href="https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;soundoptions">https://YourSASeriesAppliance.com/dana/term/winlaunchterm.cgi?host=YourTermServer&amp;soundoptions</a>



- Related Documentation**
- [Creating Advanced Terminal Services Session Bookmarks on page 673](#)
  - [Defining a Sign-In Policy on page 10](#)

## Specifying General Terminal Services Options

---

Users can create their own terminal services session bookmarks and can configure the Secure Access Service to create Terminal Services resource policies that enable access to the servers specified in the terminal services session bookmarks.

To specify general Terminal Services options:

1. In the admin console, choose **Users > User Roles > Role > Terminal Services > Options**.
2. If you are enabling Citrix sessions, under Citrix client delivery method, specify where the Secure Access Service should obtain the ICA client to download to users' systems:
  - **Download from the Citrix web site**—The Secure Access Service installs the latest version of the ICA client from the Citrix web site. You can edit the URL to point to a new location if the one listed is no longer valid.
  - **Download from the IVE**—Use the Browse button to browse to the ICA client on your local network. You can upload a CAB, MSI or EXE file. Once you upload the client, the Secure Access Service uses it as the default and downloads it to your users' systems when necessary. You must also specify the exact version number of the ICA client.

If you upload an MSI or EXE file, an open/save dialog box appears to download and install the client. If Java fallback is configured, you are given the option to bypass this download and use Java instead.

- **Download from a URL**—The Secure Access Service installs the ICA client of your choice from the specified Web site. You must also specify the exact version number of the ICA client. If Java fallback is configured, you are given the option to bypass this download and use Java instead.



**NOTE:** We recommend that you test the Citrix client that you expect the Secure Access Service to download with the custom ICA file that you have uploaded to the Secure Access Service. Perform this testing without the Secure Access Service to determine if the Citrix client supports the features in the custom ICA file. If the features do not work without the Secure Access Service, they will not work through the Secure Access Service either.

If you choose to download an ICA client from the Citrix web site or a URL, the Secure Access Service secures the download transaction by processing the URL through the Secure Access Service Content Intermediation Engine. Therefore, you must choose a site that is accessible by the Secure Access Service and enabled for users within this role.

To determine if the ICA web client is already installed on a machine, check for the following entry in your Windows registry:  
`HKEY_CLASSES_ROOT\CLSID\{238F6F83-B8B4-11CF-8771-00A024541EE3}`

You can determine the version number of an ICA client by extracting the cab file (for example, wficat.cab), looking for an inf file in the archive (for example, wficat.inf), and then locating the information about each ocx in the inf file. For example, wficat.inf (in wficat.cab) might contain the following information:

```
[wfica.ocx]
file-win32-x86=thiscab
clsid={238F6F83-B8B4-11CF-8771-00A024541EE3}
FileVersion=8,00,24737,0
[wfica32.exe]
file-win32-x86=thiscab
FileVersion=8,00,24737,0
```

In this case, "8,00,23737,0" is the file version. (Note that the version includes commas instead of periods.)

3. Enable the **User can add sessions** option to enable users to define their own terminal session bookmarks and to enable users to access terminal servers through the Secure Access Service browse bar on the home page. When you enable this option, the **Add Terminal Services Session** button appears on the Terminal Services page the next time a user refreshes the Secure Access Service user console.
4. Select the **Deny single sign-on for sessions added by user** option if you do not want the user Add Terminal Service Session page to include the Authentication section used for single sign-on. This setting is disabled by default. When enabled, it disallows SSO for all user-added terminal services sessions, even if the user had previously configured SSO authentication credentials when that was permitted. This option adds a security measure to protect against exploitation of a security breach. If SSO is allowed, an attacker who gains access to a user's home page could gain access to the terminal services added by the user.

5. Enable the **Auto-allow role Terminal Services sessions** option to enable the Secure Access Service to automatically enable access to the resources defined in the terminal session bookmark (rather than having to create resource policies). Note that this only applies to role bookmarks, not user bookmarks.

You may not see the Auto-allow option if you are using a new installation or if an administrator hides the option.

6. If you want to allow users to enable access to local devices through the bookmarks they create, select from the following options in the Allow users to enable local resources defined below section:
  - **Users can connect drives**—Enables the user to create bookmarks that connect the his local drives to the terminal server, enabling the user to copy information from the terminal server to his local client directories.
  - **User can connect printers**—Enables the user to create bookmarks that connect his local printers to the terminal server, enabling the user to print information from the terminal server to his local printer.
  - **User can connect COM ports**—Enables the user to create bookmarks that connects his COM ports to the terminal server, allowing communication between the terminal server and the devices on his serial ports.
  - **Allow Clipboard Sharing**—Enables the user to create bookmarks that shares the contents of the clipboard between the user's host computer and the terminal server. Due to the limitations in the pre-6.0 versions of the RDP client, disabling the Allow Clipboard Sharing option will automatically disable the Connect local drives, Connect local printers, and Connect COM Ports options.

When you enable local resources through the terminal server, each user can only access his own local resources. For instance, user 1 cannot see user 2's local directories.

The Connect Devices options that you specify at the role-level override any Connect Devices options that you set at the bookmark level.

- **User can connect smart cards**—Allow users to use smart card readers connected to their system for authenticating their remote desktop session.
- **User can connect sound devices**—Allow users to redirect audio from the remote desktop session to their local system.



**NOTE:** Smart cards redirecting audio are supported by Microsoft Remote Desktop Protocol versions 5.1 and later.

7. In the Allow users to modify Display settings below section:
  - Select **Desktop background** to display your current wallpaper setting. If you do not select this option, your background is blank.
  - Select **Show contents of window while dragging** to show the contents of the Windows Explorer window while moving the window around your desktop.

- Select **Menu and window animation** to animate the movement of windows, menus, and lists.
  - Select **Themes** to allow Windows themes to be set in the terminal server window.
  - Select **Bitmap Caching** to improve performance by minimizing the amount of display information that must be passed over a connection.
  - Select **Font Smoothing (RDP 6.0 onwards)** to make text smoother and easier to read. This option only works on Windows Vista computers running RDP clients that are version 6.0 or later.
8. Click **Save Changes**.

**Related Documentation**

- [Task Summary: Configuring the Terminal Services Feature on page 643](#)

---

## Configuring Terminal Services Resource Policies

---

When you enable the Terminal Services feature for a role, you need to create resource policies that specify which remote servers a user can access. You can create resource policies through the standard interface (as described in this section) or through resource profiles (recommended method).

The information in this section is provided for backwards compatibility. We recommend that you configure access to Windows terminal servers and Citrix servers through resource profiles instead, since they provide a simpler, more unified configuration method.

When writing a Terminal Services resource policy, you need to supply key information:

- **Resources**—A resource policy must specify one or more resources to which the policy applies. When writing a Terminal Services policy, you need to specify the terminal server to which users can connect.
- **Roles**—A resource policy must specify the roles to which it applies. When a user makes a request, the Secure Access Service determines what policies apply to the role and then evaluates those policies that correspond to the request.
- **Actions**—A Terminal Services resource policy either allows or denies access to a terminal server.

The Secure Access Service's engine that evaluates resource policies requires that the resources listed in a policy's Resources list follow a canonical format.

To write a Terminal Services resource policy:

1. In the admin console, choose **Users > Resource Policies > Terminal Services > Access**.
2. On the Terminal Services Policies page, click **New Policy**.
3. On the New Policy page, enter a name to label this policy and optionally description.
4. In the Resources section, specify the servers to which this policy applies.
5. In the Roles section, specify which roles to which this policy applies.

6. In the Action section, specify:
  - **Allow access**—To grant access to the servers specified in the Resources list.
  - **Deny access**—To deny access to the servers specified in the Resources list.
  - **Use Detailed Rules**—To specify one or more detailed rules for this policy.
7. Click **Save Changes**.
8. On the Terminal Services Policies page, order the policies according to how you want the Secure Access Service to evaluate them. Keep in mind that once the Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

**Related  
Documentation**

- [About Terminal Services Resource Profiles on page 648](#)
- [Specifying Resources for a Resource Policy on page 145](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)

## Specifying the Terminal Services Resource Option

Use the Options tab to match IP addresses to host names specified as resources in your terminal services resource policies. When you enable this option, the Secure Access Service looks up IP address corresponding to each host name specified in a Terminal Services resource policy. When a user tries to access a server by specifying an IP address rather than the host name, the Secure Access Service compares the IP to its cached list of IP addresses to determine if a host name matches an IP. If there is a match, then the Secure Access Service accepts the match as a policy match and applies the action specified for the resource policy.

When you enable this option, the Secure Access Service compiles a list of host names specified in the Resources field of each Terminal Services resource policy. The Secure Access Service then applies the option to this comprehensive list of host names.

This option does not apply to host names that include wildcards and parameters.

To specify the Terminal Services resource option:

1. In the admin console, choose **Users > Resource Policies > Terminal Services > Options**.
2. Select **IP based matching for Hostname based policy resources**.
3. Click **Save Changes**.

**Related  
Documentation**

- [Configuring Terminal Services Resource Policies on page 688](#)

## Using the Remote Desktop Launcher

End-user can connect to a terminal server by:

- Entering `rdp://hostname` in the Secure Access browser bar
- Creating a terminal services bookmark
- Using the remote desktop launcher (RDPLauncher)

RDPLauncher uses the Terminal Services section in the end-user home page and allows the end-user to enter a terminal service IP address or hostname. The default server port is 3389.

RDPLauncher provides only the screen. User experience options are not available through RDPLauncher. For example, the following options in the New Terminal Services Sessions window do not apply to terminal services launched through RDPLauncher:

- Client port
- Authentication settings
- Start application settings
- Connect Devices settings
- Display Settings
- Remote Audio

To allow end-users to use RDPLauncher,

1. Select the **Terminal Services** option in Users > User Roles > *Role Name* > General > Overview.
2. Select **Enable Remote Desktop Launcher** in Users > User Roles > *Role Name* > Terminal Services > Options.
3. (optional) If your end-users are on non-Windows systems, such as a Macintosh or Linux system, select **Enable Java for Remote Desktop Launcher** and select the applet to use.



**NOTE:** If you select **Hob-Juniper RDP Applet** from the Applet to Use menu, you must select the **Configure HTML for the default applet** checkbox in order to edit the HTML. Otherwise, the default HTML is used.

---

Screen size and color depth parameters for the RDPLauncher terminal services session are defined through Preferences > General on the end-users home page.

**Related  
Documentation**

- [Creating Advanced Terminal Services Session Bookmarks on page 673](#)
- [Defining a Hosted Java Applet Autopolicy on page 650](#)

# Junos Pulse Collaboration

- [Junos Pulse Collaboration Overview on page 691](#)
- [Task Summary: Configuring Junos Pulse Collaboration on page 693](#)
- [Scheduling Meetings Through the Secure Access Service End-User Console on page 694](#)
- [Scheduling Meetings Through Microsoft Outlook on page 695](#)
- [Sending Notification Emails on page 697](#)
- [Junos Pulse Collaboration Bridge Profile on page 698](#)
- [Joining Meetings on page 703](#)
- [Attending Meetings on page 705](#)
- [Conducting Meetings on page 706](#)
- [Presenting Meetings on page 707](#)
- [About Instant Meetings and Support Meetings on page 707](#)
- [About MyMeeting Meetings on page 709](#)
- [Enabling and Configuring Junos Pulse Collaboration on page 710](#)
- [Permissive Merge Guidelines for Junos Pulse Collaboration on page 714](#)
- [Specifying Authentication Servers that Meeting Creators Can Access on page 714](#)
- [Configuring System-Level Meeting Settings on page 716](#)
- [Configuring a Junos Pulse Collaboration Meeting Server on page 718](#)
- [Junos Pulse Collaboration Meeting Server Use Cases on page 720](#)
- [Troubleshooting Junos Pulse Collaboration on page 721](#)
- [Monitoring Junos Pulse Collaboration on page 723](#)

## Junos Pulse Collaboration Overview

---

Junos Pulse Collaboration (formerly Secure Meeting) allows users to securely schedule and hold online meetings between both Secure Access Service users and non-Secure Access Service users. In meetings, users can share their desktops and applications with one another over a secure connection, allowing everyone in the meeting to instantaneously share electronic data on-screen. Meeting attendees can also securely collaborate online by remote-controlling one another's desktops and through text chatting using a separate application window that does not interfere with the presentation.

The Junos Pulse Collaboration feature is not available on the SA 700 appliance. On SA 4000 appliances and up, Junos Pulse Collaboration is available as an individual upgrade.

The number of meetings and users doubles in a cluster configuration compared to a single unit. For example, if you have  $x$  meeting/ $y$  users in a single unit, then you have  $2x$  meeting/ $2y$  users in a two-plus cluster unit.



**NOTE:** During installation, if the Juniper Installer Service is not present Junos Pulse Collaboration prompts for the administrator credentials. If you do not know the administrator credentials, Junos Pulse Collaboration will install but the remote controlling of higher privilege processes feature will not be enabled. If you enter the administrator credentials correctly, this feature is enabled.

All Junos Pulse Collaboration online meetings must be scheduled by a Secure Access Service user. The meeting creator specifies meeting details such as the meeting name, description, start time, start date, recurrence pattern, duration, password, and a list of invitees.

Meeting creators can use either of the following applications to schedule meetings:

- Secure Access Service end-user console—When the meeting creator uses the Secure Access Service end-user console to schedule a meeting, Junos Pulse Collaboration displays it in the Meetings page of meeting-enabled Secure Access Service invitees. If you choose to enable a Simple Mail Transfer Protocol (SMTP) email server, Junos Pulse Collaboration also sends a notification email to each invitee with a known email address.
- Microsoft Outlook—When the meeting creator uses Microsoft Outlook to schedule a meeting, Outlook displays it in the Calendar page of other Outlook-enabled invitees and sends a notification email to each invitee through the Outlook email server. Junos Pulse Collaboration also displays the meeting in the Meetings page of the Secure Access Service end-user console for the meeting creator (but does not send email notifications through the SMTP server).

Meeting creators can bypass these scheduling mechanisms if they choose to create instant meetings or support meetings instead of standard meetings.

You can create meetings with static URLs for a particular type of meeting (for example, weekly status meetings). You do not need to schedule these types of meetings. The host starts the meeting and the invitees enter the URL to attend the meeting.

**Related Documentation**

- [Enabling and Configuring Junos Pulse Collaboration on page 710](#)
- [Troubleshooting Junos Pulse Collaboration on page 721](#)
- [Task Summary: Configuring Junos Pulse Collaboration on page 693](#)



---

## Task Summary: Configuring Junos Pulse Collaboration

---

To configure Junos Pulse Collaboration:

1. Specify a network identity for the Secure Access Service through the System > Network > Overview page of the admin console. Junos Pulse Collaboration uses this host name when constructing meeting URLs for email notifications.
2. Configure role-level settings using settings in the following pages of the admin console:
  - Use settings in the Users > User Roles > *Role Name* > General page to enable Junos Pulse Collaboration at the role level.
  - Use settings in the Users > User Roles > *Role Name* > Meetings > Options page to configure role-level meeting restrictions.
3. Specify which authentication servers meeting creators can access and search using settings in the following pages of the admin console:
  - Use settings in the Users > User Roles > Select Role > Meetings > Auth Servers page to specify which authentication servers meeting creators can access and search.
  - If you want to allow meeting creators to invite users from an LDAP server, use settings in Authentication > Auth. Servers > Select LDAP Server > Meetings page to enable the server.
4. If you want to change the default sign-in page or URL that meeting attendees use to sign into meetings, use settings in the following pages of the admin console to configure meeting sign-in policies:
  - Use settings in the Authentication > Signing In > Sign-in Pages page to customize the pages that meeting attendees see when they sign into a meeting.
  - Use settings in the Authentication > Signing In > Sign-in Policies > *Meeting Policy* page to define the URL that meeting invitees must use in order to access a meeting. You can also use this page to associate a meeting page with the URL.
  - Use settings in the Authentication > Signing In > Sign-in Policies > *User Policy* page to associate your meeting sign-in policy with a user sign-in policy. The Secure Access Service applies the specified meeting URL to any meeting created by a user who signs into the associated user URL.
5. Configure system-level meeting settings, include session timeouts, SMTP server information, time zone settings, and color-depth settings using options in the System > Configuration > Junos Pulse Collaboration page of the admin console.
6. If you want to enable client-side logging, use settings in the following pages of the admin console:
  - Use settings in the System > Log/Monitoring > Client Logs > Settings page of the admin console to enable client-side logging. You must enable this option in order to generate logs for Secure Access Service end-users and for meeting attendees.
  - Use settings in the System > Log/Monitoring > Uploaded Logs page of the admin console to view the logs that users push to the Secure Access Service.



**NOTE:** Junos Pulse Collaboration installs client files in different directories depending on your operating system and privileges. For more information, see [Client-Side Changes](#).

---

**Related Documentation**

- [General Network Settings on page 790](#)
- [Specifying Authentication Servers that Meeting Creators Can Access on page 714](#)
- [Configuring LDAP Search Attributes for Meeting Creators on page 178](#)
- [Configuring System-Level Meeting Settings on page 716](#)
- [About Client-Side Logs on page 948](#)

---

## Scheduling Meetings Through the Secure Access Service End-User Console

---

If you enable meeting creation abilities at the role level, Secure Access Service users can create meetings through the Meetings page of the Secure Access Service end user console. When they do, they must specify all of the standard meeting details such as the meeting name, description, start time, start date, recurrence pattern, duration, password, and a list of invitees. Additionally, they must categorize all invitees into one of two categories:

- **Secure Access Service invitees**—A Secure Access Service invitee (also called an in-network invitee) is a Secure Access Service user who signs into the same Secure Access Service or cluster as the meeting creator. When inviting a Secure Access Service user to a meeting, the meeting creator must specify the user's username and authentication server.
- **Non-Secure Access Service invitees**—A non-Secure Access Service invitee (also called an out-of-network invitee) is a non-Secure Access Service user or a Secure Access Service user who signs into a different Secure Access Service or cluster than the meeting creator. When inviting a non-Secure Access Service user to a meeting, the meeting creator must specify the user's email address.



**NOTE:** If a Secure Access Service invitee uses the meeting URL instead of the Meetings page in the Secure Access Service end user console to join a meeting, Junos Pulse Collaboration classifies the user as a non-Secure Access Service invitee.

---

**Related Documentation**

- [Specifying Authentication Servers that Meeting Creators Can Access on page 714](#)
- [Joining Meetings on page 703](#)

## Scheduling Meetings Through Microsoft Outlook

If you enable meeting creation abilities at the role level, Secure Access Service users can create meetings through the Microsoft Outlook calendar using the Junos Pulse Collaboration Outlook plug-in.

You must use the same Outlook profile to remove the Junos Pulse Collaboration plug-in for Outlook as the one used to install the plug-in. Switching profiles between the installation and removal of the Plug-In is not supported.

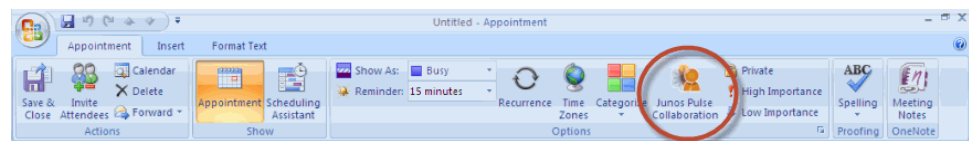


**NOTE:** The Junos Pulse Collaboration Outlook plug-in is only supported on Windows machines with Outlook 2007 or later.

To use this plug-in, the user must:

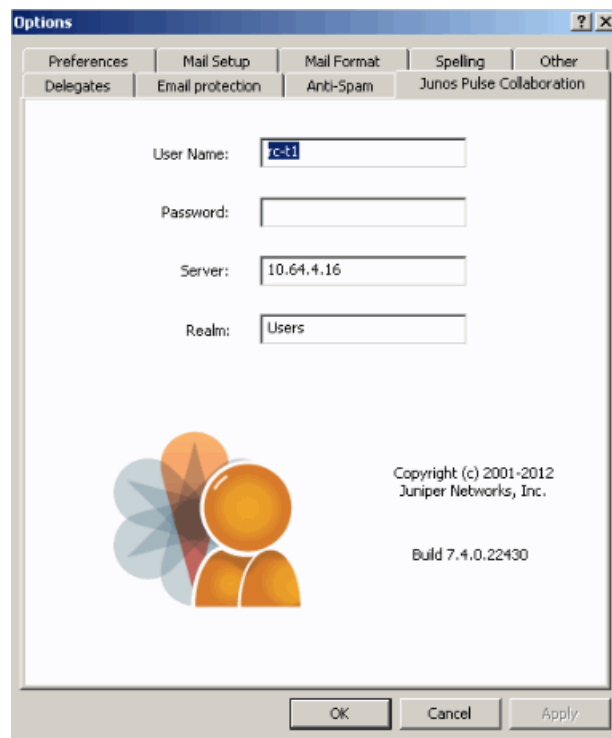
1. Install the plug-in from the Meetings page in the Secure Access Service end user console.
2. Open the Junos Pulse Collaboration scheduling form in Outlook by clicking the Collaboration button located on the Outlook ribbon.

**Figure 43: Using the Junos Pulse Collaboration**



3. Use the Options window to enter details about the server on which the meeting should be scheduled as well as the user's sign-in credentials, realm, and a meeting password. To open the Options window:
  - (Outlook 2010) Select **File > Help > Options > Add-Ins** and then click **Add-in Options**.
  - (Outlook 2007) Select **Tools > Options** and then click the **Junos Pulse Collaboration** tab.

Figure 44: Using the Junos Pulse Collaboration Tab in the Options Window



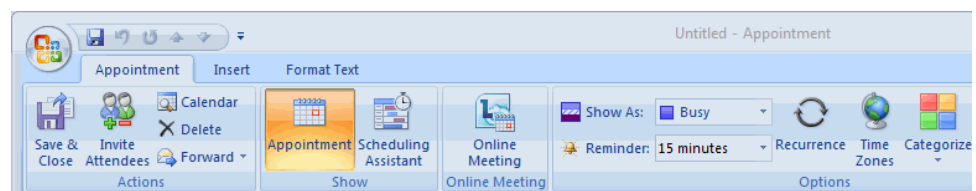
Due to limitations with Microsoft Outlook, not all meeting details cross-populate between Microsoft Outlook and the Secure Access Service. For example, if the user schedules a meeting through the Secure Access Service, Microsoft Outlook does not display the meeting in its calendar. For a complete list of restrictions, see the Junos Pulse Collaboration for Outlook document available from the Secure Access Service end user help system as well as the Junos Pulse Collaboration for Outlook plug-in installer.

4. Use the Outlook Scheduling and Appointment tabs to schedule the meeting and add invitees using standard Outlook functionality. Note that Junos Pulse Collaboration supports creating standard or recurring meetings through Outlook.



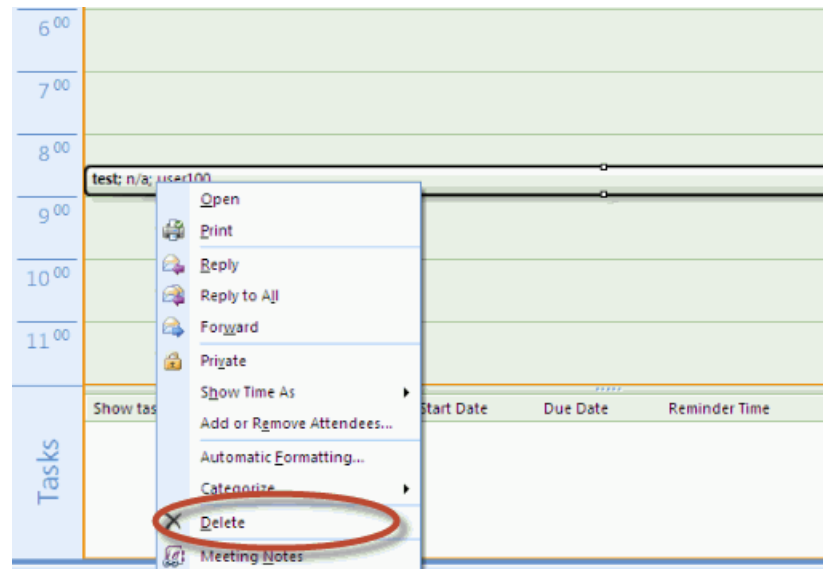
**NOTE:** Depending on your Outlook version, the Appointment tab may have an Online Meeting button. This button is not related to the Meeting Server or the Junos Pulse Collaboration Outlook Plug-in and cannot be used by a third-party plug-in.

Figure 45: Online Meeting Button is Not Used



5. Save the calendar entry to send the information to the Junos Pulse Collaboration server. Note that when saving a meeting, the user might see a certificate warning because the plug-in is communicating with a secure server.
6. Outlook sends invitation emails to the invitees using the text and meeting URL link constructed by the Junos Pulse Collaboration Outlook plug-in. Outlook also adds the meeting to the Outlook calendars of meeting invitees. This calendar item includes all of the standard information recorded by Outlook as well as an additional Junos Pulse Collaboration tab containing the information specified by the meeting creator in the Junos Pulse Collaboration tab. Note that the Secure Access Service does not send an additional email using the SMTP server.
7. To delete a meeting, right-click the meeting in the Outlook window and select Delete.

**Figure 46: Deleting the Meeting**



The Junos Pulse Collaboration Outlook plug-in authentication does not work if the realm enables Host Checker policies or requires users to select a role.

**Related Documentation**

- [Sending Notification Emails on page 697](#)

## Sending Notification Emails

You can configure Junos Pulse Collaboration or Outlook to send notification emails to invitees when the meeting creator saves a new or modified meeting. The email contains meeting details, a link that the invitee can use to join the meeting, and another link that the invitee can use to check whether his system is compatible with Junos Pulse Collaboration.



**NOTE:** You cannot send email notifications for meetings.

If your users are scheduling meetings through the Secure Access Service end user console, you must enable an SMTP server in the Users > Resource Policies > Meetings page of the admin console in order to send email notifications to invitees.

If your users are scheduling a meeting through Microsoft Outlook, the Junos Pulse Collaboration Outlook plug-in uses the email addresses that are stored on the Outlook email server.

If the person creating a Junos Pulse Collaboration is using email invitations and accesses the Secure Access Service using a URL that is not the fully-qualified domain name (for example, <https://sa>, not <https://sa.company.com>), the email invitation may display <https://sa> in the invitation information and not the true hostname. As a result, email recipients may not be able to access the link from the email. We recommend you configure the Secure Access Service's network identity. If configured, Junos Pulse Collaboration invitations use that hostname.

**Related Documentation**

- [Monitoring Junos Pulse Collaboration on page 723](#)
- [About MyMeeting Meetings on page 709](#)
- [Specifying Authentication Servers that Meeting Creators Can Access on page 714](#)

---

## Junos Pulse Collaboration Bridge Profile

---

- [Junos Pulse Collaboration Bridge Profile Overview on page 698](#)
- [Creating a Junos Pulse Collaboration Bridge Profile on page 699](#)
- [Viewing, Editing and Deleting Your Junos Pulse Collaboration Bridge Profile on page 701](#)
- [Entering the Junos Pulse Collaboration Bridge Profile Conference and PIN IDs on page 702](#)

### Junos Pulse Collaboration Bridge Profile Overview

You can embed the phone bridge number, or a list of phone numbers, and the conference access PIN into your email so that mobile phone users can just click the link to join a Junos Pulse Collaboration meeting. The Junos Pulse Collaboration meeting bridge profile lets you enter “structured” data for audio bridges. This data can then be passed from the meeting server to a meeting client and used for dialing the audio bridge.

For example, a Secure Access Service administrator creates a meeting bridge profile. A meeting invite is sent out using the bridge profile and looks similar to this.

[Example email will be provided in the next draft of this topic]

An end-user opens the meeting invite email through their mobile phone and selects a local phone number from the list. The mobile phone dials the selected phone number. After the call connects, the access code is automatically entered and the user connects to the Junos Pulse Collaboration meeting.

Depending on how the bridge profile is configured, mobile phone users can use their location services feature or IP address to display the local phone number at the top of the list. For example, if the administrator creates a profile with “US”, “China” and “India”

numbers and includes the correct country codes, mobile phone users joining from the US will see the US number displayed at the top of the list.



**NOTE:** With Secure Access Service Release 7.3, the meeting bridge profile applies only to mobile phones. Joining audio conference bridges from a desktop client is not supported.

## Creating a Junos Pulse Collaboration Bridge Profile

Secure Access Service ships with a sample Junos Pulse Collaboration bridge profile template. You can download and edit the sample bridge profile template, shown below, to create your own custom version. For example, you may want to create a meeting bridge profile for each audio bridge provider your company uses.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
dialing-number: You can configure 1-500 dialing numbers in one profile.
display-name: Please use UTF-8 encoding.
country-code: Country code of the phone number.
phone-number: Please enter digits only, without '!', '(', '-' or ')'.
 You can enter 3-15 digits in each phone number.
```

### moderator:

Please enter the extra dialing steps for the moderator (host).  
In this example, after the moderator dials one of the phone numbers, she needs to enter a "Meeting Code" and a "PIN" to start the bridge.  
You only need to specify the names of the extra steps here, the moderator will configure their own pin codes.

### participant:

Please enter the extra dialing steps for other participants.  
In this example, after a participant dials one of the phone numbers, she needs to enter a "Meeting Code" to connect to the bridge.  
You only need to specify the names of the extra steps here, the moderator will configure their own pin codes.

```
-->
<jnpr:configuration xmlns:jnpr="http://xml.juniper.net/">
<dialing-numbers>
<dialing-number>
<display-name>US Local</display-name>
<country-code>1</country-code>
<phone-number>8001112222</phone-number>
</dialing-number>
<dialing-number>
<display-name>China Southern</display-name>
<country-code>86</country-code>
<phone-number>108001234567</phone-number>
</dialing-number>
<dialing-number>
<display-name>Germany</display-name>
<country-code>49</country-code>
<phone-number>01801003825</phone-number>
</dialing-number>
```

```
<dialing-number>
 <display-name>India, Mumbai</display-name>
 <country-code>91</country-code>
 <phone-number>2261501727</phone-number>
</dialing-number>
</dialing-numbers>
<moderator>
 <display-name>Meeting Code</display-name>
 <display-name>PIN Code</display-name>
</moderator>
<participant>
 <display-name>Meeting Code</display-name>
</participant>
</jnpr:configuration>
```

The moderator and participant sections contain <display-name> parameters. These strings are the text included in the collaboration emails and in the end-user Preference page that identify the meeting conference code and the host's PIN number. For example, if you change the participant <display-name> from "Meeting Code" to "Participant Passcode":

```
<participant>
 <display-name>Participant Passcode</display-name>
</participant>
```

The collaboration email invite will look similar to this:

```
Teleconference Info

Participant Passcode: 1234567

Local Access Numbers:
US Local: 12 123456789012345
China Southern: 86 108001234567
Germany: 49 01801003825
India, Mumbai: 91 0008001007678
```

Any bridge profile configured by the Secure Access Service administrator is available to all user roles.

To download and edit the sample bridge profile template:

1. Select **System > Configuration > Junos Pulse Collaboration > Teleconference Bridge Profiles**.
2. Click **Download Template**.
3. Select **Save** to save the template to your hard drive, or click **Open** to open the template in your default editor.
4. Edit the template according to the instructions located at the top of the template and save it to your local hard drive. See the above example for the template format.



To upload your modified bridge profile:

1. Select **System > Configuration > Junos Pulse Collaboration > Teleconference Bridge Profiles**.
2. Click **Upload New Profile**.
3. Enter a unique name to identify your new bridge profile template.
4. Click **Browse** to locate your bridge profile and click **Open**.
5. Click **Create New Profile** and then click **Close Window**.

Secure Access Service parses the profile for syntax errors. If no errors are found, the new bridge profile appears in the Available Bridge Profiles section.

## Viewing, Editing and Deleting Your Junos Pulse Collaboration Bridge Profile

Once your Junos Pulse Collaboration bridge profile is created, you can perform the following operations:

- [Viewing the Contents of the Junos Pulse Collaboration Bridge Profile on page 701](#)
- [Editing a Junos Pulse Collaboration Bridge Profile on page 701](#)
- [Deleting a Junos Pulse Collaboration Bridge Profile on page 702](#)

### Viewing the Contents of the Junos Pulse Collaboration Bridge Profile

You can view a bridge profile's content at any time. The content includes the:

- Name of each country listed in the profile
- Country code
- Phone number
- Moderator information
- Participant information

To view the contents of a Junos Pulse Collaboration bridge profile:

1. Select **System > Configuration > Junos Pulse Collaboration > Teleconference Bridge Profiles**.
2. Click the **View** button next to the profile name that you want to display.  
A new window appears displaying the contents of the bridge profile.
3. When you're done, click the **Close** icon located in the lower right corner of the window.

### Editing a Junos Pulse Collaboration Bridge Profile

You can edit a Junos Pulse Collaboration bridge profile at any time. However, you must download the bridge profile to your local system before you can edit it. Updated information will be present the next time a meeting invite email is sent.

To download and edit a Junos Pulse Collaboration bridge profile:

1. Select **System > Configuration > Junos Pulse Collaboration > Teleconference Bridge Profiles**.
2. Click the **Edit/Modify** button next to the profile name you just updated.
  - a. Click **Download Profile**.
  - b. Click **Open** to open the profile in your default text editor or click **Save** to save the profile to your local drive.
  - c. Edit your bridge profile.
3. Click **Next**.
4. Click **Browse** to locate the bridge profile you just edited and then click **Open**.
5. Click **Update Profile**.

Secure Access Service parses the profile for syntax errors. If no errors are found, an upload successful message appears and the bridge profile is saved to the Secure Access Service.

6. Click **Close Window**.

### Deleting a Junos Pulse Collaboration Bridge Profile

When you no longer need a Junos Pulse Collaboration bridge profile you can remove it from Secure Access Service. Once you delete a bridge profile, you cannot retrieve it later.

To delete a Junos Pulse Collaboration bridge profile:

1. Select **System > Configuration > Junos Pulse Collaboration > Teleconference Bridge Profiles**.
2. Click the **Delete** button next to the name of the bridge profile you want to remove.
3. Click **Delete Profile** to delete the bridge profile or click **Cancel** to close the dialog box without deleting the bridge profile.

### Entering the Junos Pulse Collaboration Bridge Profile Conference and PIN IDs

End-users can select the default bridge profile and assign their conference ID and host PIN ID through the Preference window of their Secure Access Service home page.

When creating a meeting through the web interface, the meeting host can choose whether to include the bridge profile details (phone number, conference code, and PIN number) in the collaboration email.

If you are using the Junos Pulse Collaboration Outlook plug-in, you are given the option to include the bridge profile information in your email.



**NOTE:** If the option to include the bridge profile information is disabled, verify that you selected a default bridge profile.

End-users must log in to their Secure Access Service home page. To set up the conference ID and PIN numbers:

1. Click **Preferences** and then click **Pulse Collaboration**.
2. Under Meeting Bridge Profile, do the following:
  - a. Select the bridge profile to use from the Default Meeting Bridge Profile pull-down menu.
  - b. Enter the moderator meeting code and PIN number.
  - c. Enter the participant PIN number.

Typically, there is a slight delay after entering a PIN number and the meeting operator confirming your PIN number. To reduce this delay, append a pound sign (#) to the end of the PIN. For example, **1234#**.

3. Click **Save Changes**.

## Joining Meetings

Invitees are allowed to join up to 15 minutes before the meeting is scheduled to start. Junos Pulse Collaboration holds its online meetings on the Secure Access Service, allowing both Secure Access Service users and non-Secure Access Service users to attend meetings. (However, non-Secure Access Service meeting attendees cannot access anything on the Secure Access Service except the meeting to which they were invited.)

To join a meeting, Junos Pulse Collaboration invitees must navigate to the meeting site on the Junos Pulse Collaboration server (Secure Access Service) using one of the following methods:

- Use the link provided in the Meetings page (Secure Access Service invitees only).
- Use the link provided in the notification email.
- Enter the meeting URL in a Web browser.



**NOTE:** MyMeeting support only entering the meeting URL in a Web browser.

To obtain the URL for a meeting, the meeting creator can look on the Join Meeting page. Or, if you choose to use the default meeting URL, any meeting invitee can determine the appropriate URL by entering the applicable values into the following URL:

`https://<YourSA>/meeting/<MeetingID>`

Where:

- *<YourSA>* is the name and domain of the Secure Access Service hosting the meeting, such as *SAserver.yourcompany.com*. Junos Pulse Collaboration pulls this name from the Hostname field in the System > Network > Overview tab, if defined. Otherwise, Junos Pulse Collaboration pulls the Secure Access Service name from the meeting creator's browser.
- *meeting* is a literal string. (This string is always the same.) Note that *meeting* must start with a lower-case "m." For s, the default is *meeting*, but it can be defined by your system administrator.
- *<MeetingID>* is the unique 8-digit identification number that Junos Pulse Collaboration generates for the meeting. If the user does not include the meeting ID in the URL, Junos Pulse Collaboration prompts him for it when he signs into the meeting. For example:

```
https://connect.acmegizmo.com/meeting/86329712
```

For s, *<MeetingID>* is the meeting name token for this meeting. It is static for a particular meeting, and can be reused indefinitely until it is deleted. For example:

```
https://connect.acmegizmo.com/meetings/chris/weeklyStatus
```



**NOTE:** You can choose to customize the meeting URL using the customized sign-in pages feature. If you do, users cannot access a meeting using the URL described here.

---

Once they have navigated to the meeting site, authenticated Secure Access Service users can directly join the meeting—they do not need to enter a username or password to access the meeting site on the Secure Access Service since they are already authenticated through the Secure Access Service.

Non-Secure Access Service users must enter a name and password in the meeting sign-in page, however, since they are not yet authenticated. Junos Pulse Collaboration authenticates the non-Secure Access Service users based on the meeting IDs and passwords that they enter in the sign-in page. (Note that the Secure Access Service does not use the invitees' names for authentication—it only uses the names for display purposes during the meeting.)

When an invitee chooses to join a meeting, Junos Pulse Collaboration downloads and launches either a Windows client or a Java applet on to the invitee's system. This client-side component contains a meeting viewer, presentation tools, and a text messaging application. Once Junos Pulse Collaboration launches the Windows client or Java applet on the user's desktop, the user becomes a meeting attendee and can begin participating in the meeting.



**NOTE:** When configuring Junos Pulse Collaboration, note that:

- Junos Pulse Collaboration does not work with PAC files on Macintosh or Linux systems.
- Junos Pulse Collaboration allows Windows users to join meetings through an NTLM proxy with or without authentication, provided that their browsers properly support proxies. Junos Pulse Collaboration does not support NTLM proxies on Macintosh or Linux clients.
- 

A few things to note about joining a meeting from an Apple iOS device using the Junos Pulse Client:

- If the Junos Pulse client is not installed on the Apple iOS device, nothing happens when a user clicks the mobile meeting invitation link.
- The Junos Pulse client on an Apple iOS device supports only meetings from a Secure Access Service 7.2 or later meeting host. If you try to access a meeting from a meeting host that has pre-7.2 software, the client will receive an “Invalid username, password or URL” error.
- If a user joins a meeting from an Apple iOS device, the user is removed from the attendee list if the iOS device goes to sleep or is locked. The user is added back to the attendee list after the device is awakened or unlocked.

**Related Documentation**

- [About MyMeeting Meetings on page 709](#)
- [About Sign-In Policies on page 321](#)

## Attending Meetings

By default, as soon as an attendee joins a meeting, he can see the names of other users who are attending the meeting and can start sending text messages to them using the Junos Pulse Collaboration Chat window. However, you can choose to disable these capabilities in order to make meetings more secure or productive.

For instance, if your company's CFO chooses to hold a meeting with your company's analyst community, you can choose to hide attendee names in order to keep the identities of the analysts confidential. Additionally, you can choose to disable text chatting so that the meeting attendees cannot disrupt the CFO's presentation.

You can disable text chatting and enable hidden names for individual user roles. Or, you can specify that meeting creators within the role can decide themselves whether or not Junos Pulse Collaboration hides attendee names. If you do, meeting creators can make this choice in the following situations:

- When scheduling or modifying a meeting from the Meetings page of the standard Secure Access Service interface. (The meeting creator cannot choose to hide attendee names from the Microsoft Outlook scheduling interface.)
- When joining a standard meeting or instant meeting. (Note, however, that the meeting creator can only choose to hide attendee names if he is the first person to join the meeting. If another attendee joins the meeting before the creator, Junos Pulse Collaboration automatically displays the names of the meeting attendees and does not allow the meeting creator to change the display setting.)

If you or the meeting creator chooses to hide attendee names, Junos Pulse Collaboration users can only see their own names and the names of the meeting host and presenter.

The Junos Pulse Collaboration Chat functionality only supports users using the same language encoding (based on the Web browser settings) in a single meeting. Using a different encoding results in garbled text. Meeting invitations are sent based on the language setting in the creator's Web browser when meetings are created or saved.

- Related Documentation**
- [Conducting Meetings on page 706](#)
  - [Presenting Meetings on page 707](#)

---

## Conducting Meetings

---

The meeting host is a Secure Access Service user who is responsible for starting the meeting. Junos Pulse Collaboration grants the host the following responsibilities and capabilities in order to help him effectively run his meeting:

- Starting the meeting presentation—Before the host joins, the other attendees can only chat. They cannot view or make a presentation because the host is also the default meeting presenter. The meeting presenter starts the meeting presentation by sharing his desktop or applications with other attendees.
- Passing host and presenter rights—The meeting host can choose to pass some or all of his responsibilities to another meeting attendee. For instance, after joining the meeting, the host can specify that another attendee should start the meeting presentation by passing that attendee presenter rights. The host can pass his host rights to any other Secure Access Service user and pass his presenter rights to any other Secure Access Service user or non-Secure Access Service user.
- Monitoring the meeting— The meeting host is responsible for expelling meeting attendees if necessary. The meeting host can also see the names of all meeting attendees so that he can determine who is attending.
- Ending the meeting—The meeting host is responsible for extending the meeting if it runs over the scheduled duration and closing the meeting when it is done.

- Related Documentation**
- [Presenting Meetings on page 707](#)
  - [Attending Meetings on page 705](#)

## Presenting Meetings

---

Once the presenter begins sharing, a meeting viewer automatically opens on all of the meeting attendees' desktops and displays the presenter's shared applications. Junos Pulse Collaboration grants the presenter the following capabilities in order to help him effectively present to other users:

- **Sharing multiple applications**—The presenter can share a single application, multiple applications, or his entire desktop with other meeting attendees. (Note that Macintosh users cannot share individual applications. They can only share their desktops.)
- **Annotating presentations**—The presenter can use annotations in the Junos Pulse Collaboration toolbar to illustrate key concepts or to point to important features in a shared application. In addition, he can enable annotation rights for other meeting attendees.
- **Passing controller rights**—The meeting presenter can designate a controller. A *meeting controller* uses his own mouse and keyboard to remote control the presenter's shared desktop or applications. The presenter can pass remote control rights to any other attendee. When the presenter wants to regain control of his remote-controlled applications, he simply needs to click and Junos Pulse Collaboration returns control to the presenter.

Like the meeting host, the meeting presenter can also see the names of all meeting attendees. Junos Pulse Collaboration allows him to view all attendee names so that he knows to whom he is passing controller rights.



**NOTE:** Meeting presenters cannot enable annotations and remote control at the same time.

Junos Pulse Collaboration cannot display the content of meeting presenter's desktop if it is locked.

Viewers on Linux and Macintosh clients may take a while to load the presentation if the presenter's desktop screen area is larger than 1856 x 1392.

### Related Documentation

- [Conducting Meetings on page 706](#)
- [Attending Meetings on page 705](#)

## About Instant Meetings and Support Meetings

---

Instant meetings and support meetings are meetings that users can quickly create without going through the Secure Access Service or Microsoft Outlook scheduling pages. Instead, a Secure Access Service user simply needs to click the Instant Meeting button or Support Meeting button in the Secure Access Service end-user console and click Start Meeting. The Secure Access Service then starts the meeting.

When creating instant meetings and support meetings, the Secure Access Service expedites the process by skipping certain scheduling steps. For instance, the Secure Access Service does not prompt the meeting creator to add the email addresses of other invitees. Instead, the Secure Access Service makes the meeting creator the only meeting invitee. The meeting creator can then provide other invitees with the information they need to join the meeting, such as the meeting URL, ID, and password.

The Secure Access Service also expedites the scheduling process by making certain assumptions about what the meeting attendees want to do. For instance, in addition to making the meeting creator the only meeting invitee, the Secure Access Service also assumes that he wants to run the meeting and therefore makes him the meeting host. (In fact, since other attendees are probably joining the meeting through the meeting URL instead of the Secure Access Service end-user console, the meeting creator is the only user who can conduct the meeting. Additionally, the Secure Access Service automatically assigns a meeting name (“Junos Pulse Collaboration (MeetingID)” for instant meetings and “Support Meeting (MeetingID)” for support meetings), a meeting start time and date (immediately), a meeting duration (one hour), and a meeting recurrence (one-time meeting).

The Secure Access Service also uses default settings that correspond to the meeting type:

- Instant meeting—An instant meeting is basically a standard meeting that users can create more quickly. Therefore, when a user chooses to create an instant meeting, the Secure Access Service applies all of the user’s role-level settings, such as authentication requirements, remote control, and secure chatting.
- Support meeting—A support meeting is a two-person meeting that is primarily intended to allow a Secure Access Service user to quickly troubleshoot another user’s problem. Therefore, the Secure Access Service does not enable all of the user’s role-level settings. Instead, the Secure Access Service automatically enables those options that facilitate quick troubleshooting and disables other settings, as described below:
  - Desktop sharing enabled—When the second user joins the meeting, the Secure Access Service automatically shares his desktop with the meeting host, enabling the host to immediately view the user’s problem without having to explain what a meeting presenter is or how to share a desktop.
  - Remote control initiated—When the second user joins the meeting, the Secure Access Service automatically asks him whether the host can remote control his desktop. Assuming the user clicks Yes, the meeting creator can immediately start navigating through the user’s computer in order to find and fix the problem. If the user clicks No, the host can gain remote control later using the standard request mechanisms.
  - Annotations disabled—The Secure Access Service does not expose the annotations feature during a support meeting, since the meeting only contains two users. If the users need to demonstrate a problem to each other, they can use the remote control feature to directly control the troubled applications.
  - Secure chatting disabled—The Secure Access Service does not expose the secure chatting feature during a support meeting, since users should not need to send text



messages to each other. Instead, the users should talk to each directly over the phone.

- Related Documentation**
- [Joining Meetings on page 703](#)
  - [Conducting Meetings on page 706](#)

## About MyMeeting Meetings

MyMeetings, or personal meetings, are meetings that users can quickly create without going through the Secure Access Service or Microsoft Outlook scheduling pages. Instead, a Secure Access Service user simply needs to click the Meeting button in the Secure Access Service end-user console, enter the meeting subject and click Start Meeting. The Secure Access Service then starts the meeting.

MyMeeting meetings are different from instant meetings in that MyMeeting meetings have a fixed meeting URL for a specific meeting. You can bookmark this URL since it doesn't change. Meetings name must be unique within your personal meeting list and can be reused indefinitely until it is deleted by either the owner or the administrator. The meeting URL uses the format:

`https://YourSA/MyMeetingRoot/userToken/MeetingID`

where:

- *YourSA* is the name and domain of the Secure Access Service hosting the meeting, such as `SAServer.yourcompany.com`. Junos Pulse Collaboration pulls this name from the Hostname field in the System > Network > Overview tab, if defined. Otherwise, Junos Pulse Collaboration pulls the Secure Access Service name from the meeting creator's browser.
- *MyMeetingRoot* is the root string of your personal URL. By default, the root is `meeting`.
- *userToken* is a string that uniquely identifies this URL. It can be the user's username, a string (with a number automatically appended for uniqueness), or an expression. For example:
  - `https://my.company.com/meetings/chris/`
  - `https://my.company.com/meetings/room1`
  - `https://my.company.com/meetings/chris.andrew`
- *MeetingID* is the meeting name token for this meeting. It is static for a particular meeting, and can be reused indefinitely until it is deleted. For example:

`https://my.company.com/meetings/chris/weeklystaff`

The user's Meetings page displays their personal meeting address(es). Users can send this URL to the invitees to join whenever the meeting starts.

All past meetings are listed on the user's Meetings page, making it easy to locate a specific meeting and retrieve the meeting details.

## Joining MyMeeting Meetings

Attendees can join the MyMeeting meeting by entering the meeting URL in a browser.

Once they have navigated to the meeting site, authenticated Secure Access Service users can directly join the meeting—they do not need to enter a username or password to access the meeting site on the Secure Access Service since they are already authenticated through the Secure Access Service.

Non-Secure Access Service users must enter a name and password in the meeting sign-in page, however, since they are not yet authenticated. MyMeetings authenticates the non-Secure Access Service users based on the meeting IDs and passwords that they enter in the sign-in page. (Note that the Secure Access Service does not use the invitees' names for authentication—it only uses the names for display purposes during the meeting.)

**Related Documentation**

- [Configuring System-Level Meeting Settings on page 716](#)

## Enabling and Configuring Junos Pulse Collaboration

---

To enable and configure meetings:

1. In the admin console, choose **Users > User Roles**.
2. Select a role.
3. If you have not already enabled Junos Pulse Collaboration, in the **General > Overview** tab, select the **Meetings** checkbox and click **Save Changes**.



**NOTE:** If you do not select the **Meetings** checkbox, users cannot create meetings, schedule meetings, or view the **Meetings** page. Note, however, that they can still attend the meetings to which they are invited by using the link provided in their invitation emails or by directly entering the meeting URL in to their web browsers.

4. Choose the **Meetings > Options** tab.
5. Under Meeting Types section, specify the type of meeting you want to provide users:
  - **Users cannot create meetings**—Select this option to disable meeting creation and scheduling, but still provide users access to the **Meetings** page in order to join the meetings to which they are invited.
  - **MyMeetings**—Select this option to allow users to create personal meetings without having to schedule them ahead of time.
    - **Users can create additional meeting URLs under their personal URL**—Select this checkbox if you want to enable users to create additional <meetingID> tokens.
    - **Users can create Support meetings**—Select this checkbox if you want to enable users to create two-person support meetings.
  - **Standard Meetings**—Select this option to allow users to create scheduled meetings through the **Meetings** page.
    - **Users can create Scheduled meetings**—Select this checkbox to allow users to create scheduled meetings.

- **Users can create Instant meetings**—Select this checkbox to allow users to create instant meetings.
  - **Users can create Support meetings**—Select this checkbox if you want to enable users to create two-person support meetings.
6. Under Authentication Requirements, specify the authentication restrictions that you want users to apply to the meetings that they create:
- **Meeting password optional** (more accessible)—Select this option to allow the meeting creator to decide whether or not the meeting requires a password to join. When you choose this option, anyone who knows the meeting URL, ID number, and password (if applicable) can join the meeting, including non-Secure Access Service users.
  - **Require meeting password** (more secure)—Select this option to require the meeting creator to either create a meeting password or use the one generated by Junos Pulse Collaboration. When you choose this option, anyone who knows the meeting URL, ID number, and password can join the meeting, including non-Secure Access Service users.
  - **Require server-generated password** (even more secure)—Select this option to require the meeting creator to use the password generated by Junos Pulse Collaboration. When you choose this option, anyone who knows the meeting URL, ID number, and password can join the meeting, including non-Secure Access Service users.
  - **Require secure gateway authentication** (most secure)—Select this option to only allow invited users authenticated against the Secure Access Service secure gateway to attend meetings. When you choose this option, the meeting creator does not need to create a meeting password, since all users must authentication through the Secure Access Service secure gateway.
7. (MyMeeting only) Under Password Options, specify password requirements.
- **Minimum length**—Set the minimum character length for passwords.
  - **Maximum length**—Set the maximum character length for passwords (optional). The maximum length cannot be less than the minimum length. There is no maximum limit to the length.
  - **Password must have one or more digits**—Select this option to require passwords to have at least one digit.
  - **Password must have one or more letters**—Select this option to require passwords to have at least one letter.
  - **Password must have mix of UPPERCASE and lowercase letters**—Select this option if you want all passwords to contain a mixture of upper- and lowercase letters.
  - **Password must be different from username**—Select this option if the password cannot equal the username.
8. (MyMeeting only) Under Password Management, specify when passwords should be changed.

- **Allow meeting creator to decide**—Select this option to let the meeting creator decide when to change the password
  - **Every\_meetings**—Select this option to specify the number of meetings after which a password expires.
9. (Standard Meetings only) Under Password Distribution, specify the distribution method that you want meeting creators to employ:
- **Do not display the password in the notification email (more secure)**—Select this option to require that meeting creators manually distribute the meeting password to invitees. When you select this option, Junos Pulse Collaboration does not distribute the password in the automatic email notifications it sends to invitees and Microsoft Outlook does not display the Junos Pulse Collaboration tab (which contains the meeting password) to invitees. Omitting the password from the meeting email and Microsoft Outlook calendar entry helps increase meeting security.
  - **Display the password in the notification email (more accessible)**—Select this option to automatically distribute the meeting password in the email notification sent by Junos Pulse Collaboration and to display the Junos Pulse Collaboration tab in Microsoft Outlook calendar entries.
  - **Allow the meeting creator to decide**—Select this option to allow the meeting creator to determine whether or not Junos Pulse Collaboration and Microsoft Outlook should automatically distribute the meeting password to meeting invitees.



**NOTE:** You must enable an email server in order to send meeting notification emails.

---

10. (Instant or Scheduled meetings only) Under Attendee Names, specify whether you want Junos Pulse Collaboration to display the names of attendees during a meeting:
- **Do not allow hiding of attendee names**—Select this option to always display the names of meeting attendees.
  - **Allow meeting creator to hide attendee names**—Select this option to allow the meeting creator to decide whether or not to display the names of meeting attendees.
  - **Hide attendee names**—Select this option to always hide the names of meeting attendees. Note that when you select this option, Junos Pulse Collaboration still exposes the names of the meeting host and presenter to other meeting attendees.
11. (Instant or Scheduled meetings only) Under Remote Control, specify whether you want to allow meeting presenters to share control of their desktops and applications with other meeting attendees:
- **Allow remote control of shared windows (more functional)**—Select this option to allow the meeting presenter or host to pass control of the presenter's desktop and desktop applications to any of the meeting attendees, including non-Secure Access Service users.
  - **Disable remote control (more secure)**—Select this option to limit control of the meeting presenter's desktop and desktop applications exclusively to the presenter.

12. Under Secure Chat, indicate whether or not you want to allow users to chat during their meetings:

- **Allow secure chat** (more functional)—Select this option to enable chatting in the meetings that are created by users who map to this role.
- **Disable secure chat** (more secure)—Select this option to disable chatting in the meetings that are created by users who map to this role.



**NOTE:** If you change this setting while a meeting is in progress (that is, after any user has joined the meeting), Junos Pulse Collaboration does not apply the modified setting to the in-progress meeting.

13. (Standard Meetings only) Under Junos Pulse Collaboration for Outlook, select the **Allow users to download Junos Pulse Collaboration for Outlook Plugin** checkbox if you want to allow users to schedule secure meetings through Microsoft Outlook.

14. Under Meeting Policy Settings, indicate whether or not you want to restrict the resources that are used by Junos Pulse Collaboration users:

- **Limit number of simultaneous meetings**—Select this checkbox and enter a corresponding value to specify the maximum number of meetings that may be held by at any given time by members of the role.
- **Limit number of simultaneous meeting attendees**—Select this checkbox and enter a corresponding value to specify the maximum number of people that may simultaneously attend meetings scheduled by members of the role.
- **Limit duration of meetings (minutes)**—Select this checkbox and enter a corresponding value to specify a maximum duration (in minutes) that a meeting may run.



**NOTE:** The Secure Access Service also limits the number of meetings users can attend. An individual user can only attend one meeting at a time per computer and cannot attend more than 10 consecutive meetings within a 3 minute period. These limits are in addition to the meeting and user limits defined by your Junos Pulse Collaboration license.

15. Click **Save Changes**. The Secure Access Service adds a Meeting link to the secure gateway home pages of the users in the specified role.

#### Related Documentation

- [About Instant Meetings and Support Meetings on page 707](#)
- [Sending Notification Emails on page 697](#)
- [Attending Meetings on page 705](#)
- [Conducting Meetings on page 706](#)
- [Scheduling Meetings Through Microsoft Outlook on page 695](#)

## Permissive Merge Guidelines for Junos Pulse Collaboration

---

If you choose to merge roles, the Secure Access Service merges all options on the Users > User Roles > Select Role > Meetings > Options page to favor more accessible settings rather than more secure, except policy settings. When applying the policy settings that control the number of meetings and attendees allowed per role, Junos Pulse Collaboration runs through the various roles trying to find one whose limit is not yet reached.

For example, you might specify that the following roles can schedule the following number of meetings:

- Engineering: 25 meetings
- Management: 50 meetings
- Sales: 200 meetings

If Joe maps to all of these roles (in the order listed), and tries to schedule a meeting, Junos Pulse Collaboration first checks whether the scheduled meeting limit for Engineering has been met. If it has, Junos Pulse Collaboration then checks the Management meeting quota. If that limit has been met, Junos Pulse Collaboration checks the limit for the Sales role. Only when the limit for all of these roles has been reached does display a message to Joe telling him that the scheduled meeting limit has been reached and he cannot create a meeting. You cannot limit the number of meetings or meeting users at the realm level.

### Related Documentation

- [User Roles Overview on page 105](#)

## Specifying Authentication Servers that Meeting Creators Can Access

---

You can specify which authentication servers meeting creators may access and search when inviting other Secure Access Service users to meetings. When specifying servers, you can select any authentication server that you have enabled through the Authentication > Auth. Servers page of the admin console.

When you enable servers for meeting creators, Junos Pulse Collaboration displays the following tabs to them in the Add Invitees dialog box:

- **Local**—Using the Local tab, the meeting creator may access and search for users from any enabled authentication server (including LDAP servers). The meeting creator may access and search all users that are managed through a local Secure Access Service authentication server in addition to all users that are managed by other types of authentication servers and cached in the Secure Access Service's memory. The meeting creator cannot view or search for users who are included in a non-Secure Access Service server's database but have not yet signed in to the Secure Access Service and created persistent data (such user bookmarks or password modifications).
- **LDAP**—If you enable an LDAP server, Junos Pulse Collaboration displays the LDAP tab in the Add Invitees dialog box. The meeting creator may use this tab to access and search for all users in the enabled LDAP server(s)—not just those users who are cached

in the Secure Access Service's memory. When a meeting creator adds a user through the LDAP tab, Junos Pulse Collaboration also uses the email attribute defined in the LDAP server to populate the invitee's email address in his notification email.

When adding local and LDAP users, the meeting creator's ability to access and search the servers is dependent on options you specify in the Auth Servers tab of the admin console. This tab contains two options that you may use to control access to each authentication server:

- **Access**—Select this option to allow the meeting creator to add and validate users from the corresponding authentication server. If you enable this option, Junos Pulse Collaboration validates any users that the meeting creator tries to add from this server. If the meeting creator enters the name of a user that does not exist, Junos Pulse Collaboration displays a warning to the creator when he finishes configuring the meeting and removes the invalid user from the list of invitees. If you disable this option, the meeting creator must use email addresses instead of Secure Access Service usernames to invite any users from this server to a meeting. Junos Pulse Collaboration then treats the specified users as non-Secure Access Service invitees.
- **Search**—Select this option to allow the meeting creator to search user entries in the corresponding authentication server. If you enable this option, Junos Pulse Collaboration displays information about all available users who match the search criteria entered by the meeting creator. If you disable this option, the meeting creator must know the exact username and authentication server of the Secure Access Service users that he wants to invite to the meeting.



**NOTE:** If you enable an LDAP server, note that it must be searchable. Also note that you may use options in the Authentication > Auth. Servers > Select LDAP Server > Meetings tab to specify individual LDAP attributes that Junos Pulse Collaboration should display to meeting creators when they search an LDAP database.

To specify which authentication servers users may access and search when scheduling a meeting:

1. In the admin console, choose **Users > User Roles**.
2. Select a role.
3. If you have not already enabled Junos Pulse Collaboration, in the General > Overview tab, select the **Meetings** checkbox and click **Save Changes**.
4. Choose the **Meetings > Auth Servers** tab.
5. In the User's Authentication Server section, indicate whether the members of this role may access and search the authentication servers that they are currently authenticated against.
6. In the Authentication Servers section, indicate additional authentication servers that members of this role may access and search.
7. Click **Save Changes**.

- Related Documentation**
- [Configuring System-Level Meeting Settings on page 716](#)

## Configuring System-Level Meeting Settings

---

Unlike other access features, Junos Pulse Collaboration does not have a resource policy. Instead, you configure system-level settings that apply to all roles for which this feature is enabled. You can:

- Specify session lifetime limits for meetings
- Enable daylight savings adjustments to scheduled meetings
- Specify the maximum color depth of meeting presentations
- Enable automatic email notifications for users who are invited to meetings scheduled through the Secure Access Service end user console
- Define the MyMeeting URL

To configure Junos Pulse Collaboration:

1. In the admin console, choose **System > Configuration > Junos Pulse Collaboration**.
2. In the Session lifetime section, specify values for:
  - **Idle Timeout**—Use this field to specify the number of minutes a meeting session may remain idle before ending.
  - **Max. Session Length**—Use this field to specify the number of minutes a meeting session may remain open before ending.



**NOTE:** The values entered here apply to the meeting session, not the Secure Access Service session. For example, you may enter lower session lifetime values in the **Users > User Roles > Select Role > General > Session Options** page of the admin console. If the user reaches one of the role-level values before joining a meeting, he must sign back in to the Secure Access Service in order to access the meeting through the Secure Access Service end user console. If the user reaches these role-level values after joining a meeting, however, they are not applied to the meeting. He may continue attending the meeting uninterrupted until he reaches the resource policy-level limits specified here.

3. In the Upload logs section, select **Enable Upload Logs** to allow non-Secure Access Service users to upload meeting logs.



**NOTE:** If you select the Upload Logs option, you must also use settings in the **System > Log/Monitoring > Client Logs > Settings** page of the admin console to enable client-side logging.

4. In the MyMeeting section, specify values for:



- **Root meeting URL**—Select the meeting URL you want associated with MyMeeting meetings. Meeting URLs are created in the Authentication > Signing In > Sign-In Policies page.
- **Meeting name**—Specify the token to append to the meeting URL to uniquely identify this URL. You can use:
  - **Username**—Append the user's Secure Access Service username to the meeting URL.
  - **Sequential room number with prefix**—Specify a string to append to the meeting URL, such as a "meeting". Numbers will be appended to the string to ensure uniqueness. For example, meeting\_room1, meeting\_room2, etc.
  - **Expression**—Append an expression, such as <userAttr.lname>, to the meeting URL. If the attribute is not valid, username is appended to the meeting URL instead.



**NOTE:** Changing this token affects only users who have not created meetings. Users who have already created MyMeetings retain their existing token setting.

To view a list of MyMeeting URLs users have already created, see System > Status > Meeting Schedule. Choose MyMeeting URLs from the View drop-down menu.

5. In the Email meeting notifications section, select **Enabled** to enable an SMTP email server. Then:
  - In the SMTP Server field, enter the IP address or host name of an SMTP server that can route email traffic from the appliance to the meeting invitees.
  - In the SMTP Login and SMTP Password fields, enter a valid login name and password for the specified SMTP email server (if required by the SMTP server).
  - In the SMTP Email field, enter your email address or the address of another administrator. Junos Pulse Collaboration uses the specified address as the sender's email if the email creator does not configure his own email address on the Secure Access Service.



**NOTE:** If you enable an SMTP server for use with Junos Pulse Collaboration, you should also define a virtual host name for your Secure Access Service in the Hostname field of the System > Network > Overview tab. Junos Pulse Collaboration uses the name you specify when populating notification emails with meeting URLs and when making SMTP calls. If your Secure Access Service maps to multiple names and you do not define a virtual host name, you may need to restrict which name Secure Access Service users sign in to before creating a meeting. For example, if your Secure Access Service maps to an internal name (such as sales.acmegizmo.com) that is only accessible from inside your company's firewall and another name (such as partners.acmegizmo.com) that is accessible from anywhere, Secure Access Service users should sign in to partners.acmegizmo.com before creating meetings. Otherwise, non-Secure Access Service invitees will receive email notifications containing links to the Secure Access Service to which they cannot connect.

6. In the Options section, configure daylight savings and color-depth options:
  - From the Observe DST rules of this country list, specify the country whose daylight savings time rules the Secure Access Service should observe. The client uses this setting as a baseline and then adjusts meeting times for individual users as necessary based on browser settings and Secure Access Service client-side DST preference settings.



**NOTE:** When a user signs into the Secure Access Service, Junos Pulse Collaboration determines his time zone by running an ActiveX component called "Timezone Grabber" on his machine.

- Select **Enable 32-bit (True Color) Presentations** to allow users to present in true color. By default, Junos Pulse Collaboration presents applications to users using the same color-depth as the presenter's desktop (up to 32-bit color). If you do not select this option and a user presents an application in 32-bit color, however, Junos Pulse Collaboration changes the image to 16-bit to improve performance.
7. Click **Save Changes**.
  8. Configure Junos Pulse Collaboration settings for individual roles.

**Related Documentation**

- [Enabling and Configuring Junos Pulse Collaboration on page 710](#)

## Configuring a Junos Pulse Collaboration Meeting Server

If your environment includes Junos Pulse clients, you can set up your secure access service as a meeting server so that your end-users can start meetings from Junos Pulse instead of having to log in to their secure gateway web interface.

Pulse clients can list more than one Junos Pulse Collaboration server.

To set up your secure access service as a meeting server for Pulse clients:

1. From the admin console, select **Junos Pulse > Connections**.
2. Click the connection set containing the server you want to define as a meeting server.
3. Under Connections, click the connection server.
4. Under Options, select:
  - **Support Junos Pulse Collaboration integration on this connection**—Define this server as a meeting server and make it available in your end-user’s Junos Pulse.
  - **Support Remote Access on this connection**—Allow users to log in to this server using the web interface. If you want this server to be only a meeting server (users cannot log in to this server through the web interface), uncheck this option. However, make sure the **Support Junos Pulse Collaboration integration on this connection** is selected.
5. Click **Save Changes**.

End-users can start meetings when the Pulse client is not connected to a server. With this scenario, the Pulse client attempts to log in to the meeting server using saved credentials, if available. If saved credentials do not exist, or the server login fails, the end-user is prompted to enter their credentials.

If the Pulse client is connected to a Pulse server when the user starts a meeting, the client first checks to see if the meeting server is the same server that Pulse is currently connected to. If they are the same server, then the meeting starts immediately. If they are different servers, the client then checks if the end-user is in the same authentication group on both servers. If it is the same authentication group, the client can use the existing user session to single sign-on (SSO) into the meeting server. This SSO to a meeting server feature is configurable through the admin console.

To configure Junos Pulse Collaboration SSO:

1. From the admin console, select **Users > User Realms >**.
2. Select an existing realm, or create a new Realm.
3. On the General page, select the **Session Migration and Sharing** check box. Additional options appear.
4. Choose one of the following options:
  - **Enable Session Migration**—Copy the user session from the currently connected Pulse server to the Junos Pulse Collaboration meeting server and then terminate the user session on the Pulse server.
  - **Enable Session Sharing**—Create a new user session on the Junos Pulse Collaboration meeting server and retain the user’s current session on the Pulse server.
5. Click **Save Changes**.

For more information on session migration, see the *Junos Pulse Administration Guide* located on the Juniper Networks support site.

## Junos Pulse Collaboration Meeting Server Use Cases

This topic describes several scenarios of starting a meeting where the Pulse server and Junos Pulse Collaboration meeting server may or may not be the same. For these use cases, assume the following server configurations:

Server Name	Server Type	Additional Configuration
Server 1	Junos Pulse Collaboration meeting server and allows active VPN sessions	Server 1 is configured for session sharing with Server 2, and the user authentication realms are the same between Server 1 and Server 2.
Server 2	Junos Pulse Collaboration meeting server only	Server 1 is configured for session sharing with Server 2, and the user authentication realms are the same between Server 1 and Server 2.  Server 2 is configured for session sharing with Server 3 using IF-MAP, and the authentication realms for the user are same between Server 2 and Server 3.
Server 3	Allows only active VPN sessions (is not a Junos Pulse Collaboration meeting server)	Server 2 is configured for session sharing with Server 3 using IF-MAP, and the authentication realms for the user are same between Server 2 and Server 3.
Server 4	Junos Pulse Collaboration meeting server and allows active VPN sessions	No session sharing with any other server.

### Use Case: User has an active VPN Session on Server 1 and starts a meeting on Server 1

Pulse uses the user's existing VPN session credentials to SSO the user in to the Junos Pulse Collaboration meeting server. The Meeting web page appears (same as clicking the Meeting button on the end-user's secure gateway home page) and the user starts a meeting. The user is not logged out of the Junos Pulse Collaboration meeting server when they end the meeting since this is a shared server. The meeting server sign out option on the Pulse tray menu is disabled. If the user attempts to disconnect from Pulse while the meeting is active, a warning message alerts the user that disconnecting from the Pulse server will end their meeting.

### Use Case: User has an active VPN Session on Server 1 and starts a meeting on Server 2

When the user starts the meeting on Server 2, Pulse uses the user's credentials on Server 1 to SSO in to Server 2. The Meeting web page appears (same as clicking the Meeting button on the end-user's secure gateway home page) and the user starts a meeting. The user can also sign out of Server 1 while their meeting is still active and the meeting will not disconnect. The user is not logged out of Server 2 when they end the meeting. The user can manually disconnect Server 1 or from Server 2 through the Pulse tray menu. Signing out on one server has no effect on the other server.

**Use Case: User has an active VPN Session on Server 3 and starts a meeting on Server 1**

Since Server 3 has session sharing only with Server 2, the option to start a meeting on Server 1 is disabled. In this case, the user can start a meeting only on Server 2.

**Use Case: User has an active VPN Session on Server 3 and starts a meeting on Server 2**

When the user starts the meeting on Server 2, Pulse uses the user's credentials on Server 3 to SSO in to Server 2. The Meeting web page appears (same as clicking the Meeting button on the end-user's secure gateway home page) and the user starts a meeting. The user can also sign out of Server 3 while their meeting is still active and the meeting will not disconnect. The user is not logged out of Server 2 when they end the meeting. The user can manually disconnect Server 3 or from Server 2 through the Pulse tray menu. Signing out on one server has no effect on the other server.

**Use Case: User has no active VPN session and starts a meeting on Server 1**

When the user starts the meeting on Server 1, they are prompted to log in. The Meeting web page appears (same as clicking the Meeting button on the end-user's secure gateway home page) and the user starts a meeting. The user is not logged out of the Junos Pulse Collaboration meeting server when they end the meeting since this is a shared server. The meeting server sign out option on the Pulse tray menu is disabled. If the user attempts to disconnect from Pulse while the meeting is active, a warning message alerts the user that disconnecting from the Pulse server will end their meeting.

**Use Case: User has no active VPN session and starts a meeting on Server 2**

When the user starts the meeting on Server 2, they are prompted to log in. The Meeting web page appears (same as clicking the Meeting button on the end-user's secure gateway home page) and the user starts a meeting. The user have to re-enter their credentials if they try to log in to Sever 1, Server 3 or Server 4. The user is not logged out of the Server 2 when they end the meeting. They can, however, manually disconnect from Server 2 through the Pulse tray menu.

## Troubleshooting Junos Pulse Collaboration

---

If you or your end-users encounter problems with Junos Pulse Collaboration and the admin console pages described above do not help you solve the problem, we recommend that you following the guidelines below.

Troubleshooting methods include:

- Uninstall the Junos Pulse Collaboration client from your system—If you are having a problem launching Junos Pulse Collaboration, click the Joining a Meeting: Troubleshooting link on the Join Meeting page, and then click Uninstall. Click Return to Join Meeting and try to launch the meeting again. The next time you try to join a meeting, Junos Pulse Collaboration updates your client with the latest version. For information about where Junos Pulse Collaboration installs files and which files it leaves behind after uninstallation, see the *Client-side Changes Guide* on the Juniper Customer Support Center.
- Check your system's compatibility—You might encounter problems joining or presenting at a meeting if your system configuration is not compatible with Junos Pulse Collaboration. To determine if your system is compatible, navigate to the meeting sign-in page at any time or accept the meeting invitation email and click Check Meeting Compatibility. Junos Pulse Collaboration determines your compatibility level to achieve full compatibility if required. Note, however, that the Junos Pulse Collaboration compatibility checker does not check all factors that can affect your meeting experience.

For a comprehensive list of about the operating systems and browsers that are supported, as well as system requirements such as CPU, memory, monitor resolutions, and screen depths, see the *Supported Platforms Document* posted on the Juniper Networks Customer Support Center.

- Determine if you are using unsupported functionality—Junos Pulse Collaboration does not support the sharing of streaming media applications. Junos Pulse Collaboration also does not support graphic intensive applications that dynamically change the screen resolution or screen depth.
- Install a production-level certificate on your Secure Access Service—We recommend that you install a production-level certificate on the Junos Pulse Collaboration server (i.e., the Secure Access Service) when using Junos Pulse Collaboration in conjunction with an SSL certificate. If you install a self-signed SSL certificate, Junos Pulse Collaboration users might encounter difficulties signing in to meetings. If you choose to use a self-signed certificate, instruct meeting attendees to install the certificate before joining the meeting. (Through Internet Explorer, users should click View Certificate and then Install Certificate when they see the error message.)
- Refer to the *Junos Pulse Collaboration Error Messages PDF*—The *Junos Pulse Collaboration Error Messages PDF* on the Juniper Networks Customer Support Center lists errors that you might encounter when configuring or using Junos Pulse Collaboration and explains how to handle them.
- Contact Juniper Networks Support—If you encounter an error and cannot solve it using the solutions described above, send a clear description of the problem to Juniper Support with detailed steps explaining how to reproduce the problem, the error message text, your Secure Access Service operating system and build number, and your Secure Access Service administrator log files, installation log files, and client-side log files.

## Known Issues with Junos Pulse Collaboration

### Launching Junos Pulse Collaboration Using the Java Client

When using the Java client to launch a Junos Pulse Collaboration, if the user clicks No on the certificate warning presented by the JVM, the meeting client does not launch, but it appears to the user as though the applet is still loading.

### Toolbars on Macintosh and Linux Platforms

Even if the viewers are set to full screen, the toolbar is still visible on the Macintosh and Linux platforms.

### Joining Meetings From a Cluster

When using two Secure Access Service devices in a Junos Pulse Collaboration cluster, users should always connect to the VIP (Virtual IP) address to join the Junos Pulse Collaboration, not the IP address of the physical machine.

### Clock Synchronization in Clusters

Junos Pulse Collaboration may function erratically if the time clocks on Secure Access Services in a cluster are not synchronized. We recommend you use the same NTP server for each node within a cluster to keep the Secure Access Service times synchronized.

### Number Attendee Limitation with Safari

When creating a Junos Pulse Collaboration using the Safari Web browser, you can not add more than 250 attendees.

### Dial-Up Bandwidth

When presenting, the presenter should consider which access methods are being used by attendees. Dial-up attendees may have bandwidth issues for presentations that redraw the screen or update the screen too frequently. If the presentation saturates the dial-up attendees' bandwidth, remote control and chat functions may not work, as they require sending data back to the Secure Access Service over the same, saturated, dial-up link over which they are receiving data.

### Creating Clusters

In progress Junos Pulse Collaboration meetings are stopped if a cluster is created during the meeting.

#### Related Documentation

- [Using Multiple Secure Access Service Certificates on page 845](#)
- [Monitoring Junos Pulse Collaboration on page 723](#)

## Monitoring Junos Pulse Collaboration

---

You can use the following pages in the admin console to monitor Junos Pulse Collaboration performance and users:

- System > Status > Overview—Use this page to view system capacity utilization on the Secure Access Service.

- System > Status > Meeting Schedule—Use this page to view which users are currently signed in to a meeting and expel them from meetings if required.

**Related  
Documentation**

- [Troubleshooting Junos Pulse Collaboration on page 721](#)



# Email Client

- [About the E-Mail Client on page 725](#)
- [Choosing an E-Mail Client on page 726](#)
- [Working with a Standards-Based Mail Server on page 727](#)
- [Working with the Microsoft Exchange Server on page 728](#)
- [About Lotus Notes and the Lotus Notes Mail Server on page 730](#)
- [Enabling the E-Mail Client at the Role Level on page 730](#)
- [Writing the E-Mail Client Resource Policy on page 731](#)

## About the E-Mail Client

---

The email support provided by your Secure Access Service depends on the optional features licensed for your Secure Access Service:

- **Secure Email Client option**—If you have the Secure Email Client option, the Secure Access Service supports the Internet Mail Application Protocol (IMAP4), the Post Office Protocol (POP3), and the Simple Mail Transfer Protocol (SMTP).



**NOTE:** Secure Email Client does not support the roaming session options you can select in Users > User Roles > Role > General > Session Options.

- **Secure Application Manager option**—If you have the Secure Application Manager option, the Secure Access Service supports the native Microsoft Exchange MAPI protocol and the native Lotus Notes protocol.



**NOTE:** If your Secure Access Service is licensed with the Secure Application Manager option, which supports the native Microsoft Exchange MAPI protocol and the native Lotus Notes protocol, this section does not apply.

The Secure Email Client option enables users to use standards-based email clients to access corporate email securely from remote locations without the need for any additional software, such as a VPN client. The Secure Access Service works with any mail server that supports Internet Mail Application Protocol (IMAP4), Post Office Protocol (POP3),

and Simple Mail Transfer Protocol (SMTP), including the Microsoft Exchange Server and Lotus Notes Mail server, which provide IMAP4/POP3/SMTP interfaces.

The Secure Access Service sits between the remote client and your mail server, serving as a secure email proxy. The remote client uses Secure Access as a (virtual) mail server and sends mail using the SSL protocol. The Secure Access Service terminates SSL connections from the client and forwards the decrypted mail traffic within your LAN to your mail server. The Secure Access Service then converts unencrypted traffic from the mail server into S-IMAP (Secure IMAP), S-POP (Secure POP), and S-SMTP (Secure SMTP) traffic, respectively, and transports it over SSL to the email client.



**NOTE:** If you have configured multiple sessions per user, note the following regarding email sessions. If a user has concurrent sessions and starts the email client from all sessions, the email client from the last session is the only one that can access the backend email server through The Secure Access Service. For example, if a user has two concurrent sessions and starts the email client from both sessions, only the second session can access the email server.

#### Related Documentation

- [Choosing an E-Mail Client on page 726](#)
- [Working with a Standards-Based Mail Server on page 727](#)
- [Working with the Microsoft Exchange Server on page 728](#)
- [About Lotus Notes and the Lotus Notes Mail Server on page 730](#)
- [Enabling the E-Mail Client at the Role Level on page 730](#)
- [Writing the E-Mail Client Resource Policy on page 731](#)

---

## Choosing an E-Mail Client

The Secure Access Service supports the following email clients:

- Outlook 2000 and 2002
- Outlook Express 5.5 and 6.x
- Netscape Messenger 4.7x and Netscape Mail 6.2

Users who need remote access to email typically fall into one of two categories:

- Corporate laptop users—These users use the same laptop when in the office and traveling.
- Home machine users—These users use a different machine at home than their office machine.

Before recommending an email client to your users, read the following sections about how the supported clients interact with:

- Standards-based mail servers, including the Lotus Notes Mail Server
- Microsoft Exchange Server



**NOTE:** You can find instructions for configuring each of the supported email clients on the Integration Guides and How-Tos page of the Juniper Networks Customer Support Center.

**Related Documentation**

- [About the E-Mail Client on page 725](#)
- [Working with a Standards-Based Mail Server on page 727](#)
- [Working with the Microsoft Exchange Server on page 728](#)
- [About Lotus Notes and the Lotus Notes Mail Server on page 730](#)
- [Enabling the E-Mail Client at the Role Level on page 730](#)
- [Writing the E-Mail Client Resource Policy on page 731](#)

## Working with a Standards-Based Mail Server

The Secure Access Service works with mail servers that support IMAP4, POP3, and SMTP.

- IMAP Mail Servers
  - Corporate laptop users—May use any of the six supported email clients. We recommend that users use the same client—configured to point to the Secure Access Service—both while in the office and while traveling to ensure a seamless experience.
  - Home machine users—May use any of the six supported email clients for remote access to the IMAP server via the Secure Access Service.
- POP Mail Servers
  - Corporate laptop users—May use any of the four Outlook email clients\*. We recommend that users use the same client—configured to point to the Secure Access Service—both while in the office and while traveling to ensure a seamless experience.
  - Home machine users—May use any of the four Outlook email clients\* for remote access to the POP server via the Secure Access Service.

\*The Netscape email clients cannot be used in POP mode for remote access, because they do not support S-POP, which is required by the Secure Access Service for secure data transmission.

**Related Documentation**

- [About the E-Mail Client on page 725](#)
- [Choosing an E-Mail Client on page 726](#)
- [Working with the Microsoft Exchange Server on page 728](#)
- [About Lotus Notes and the Lotus Notes Mail Server on page 730](#)

- [Enabling the E-Mail Client at the Role Level on page 730](#)
- [Writing the E-Mail Client Resource Policy on page 731](#)

## Working with the Microsoft Exchange Server

---

The Microsoft Exchange Server supports:

- Native MAPI (Messaging Application Programming Interface) clients
- IMAP clients
- POP clients
- Outlook Web Access (OWA)

The Secure Access Service provides access to the Microsoft Exchange Server through IMAP and POP clients using the Secure Email Client option and through OWA using the secure Web browsing feature.

### Exchange Server and IMAP Clients

If your corporate mail server is an Exchange Server, then we presume that an employee's office machine is configured to use the Outlook 2000 or 2002 email client in native MAPI mode.

- Corporate laptop users: May use either of the Outlook Express or Netscape clients for remote access to the Exchange Server via the Secure Access Service.



**NOTE:** The Outlook 2000 client only supports one mail server configuration, which in this case would be the native MAPI mode, thus preventing users from using the same client for remote access. The Outlook 2002 client provides support for simultaneous MAPI and IMAP server configurations but does not support IMAP access when the MAPI account is off-line, preventing remote users from retrieving email.

- Home machine users: May use any of the six supported email clients for remote access to the Exchange Server via the Secure Access Service, assuming no MAPI account is configured on the remote machine.

When users run the Outlook Express or Netscape clients in IMAP mode, please note the following folder management behavior:

- When using Outlook Express mail clients—Deleted emails appear in the Outlook Express Inbox with a strike through them; they are not moved to the Deleted Items folder on the Exchange Server, which is the behavior when using the Outlook 2000 or 2002 client. When a user purges deleted emails in an Outlook Express client, the emails are gone forever. We recommend that Outlook Express users either:
  - Manually drag emails they wish to delete to the Deleted Items folder that appears under Local Folders (these are default folders that appear). This folder syncs with

the Deleted Items folder on the Exchange Server, enabling users to retrieve deleted emails later.

- Leave deleted emails in the Outlook Express Inbox, and then the next time they log in to their Outlook 2000 or 2002 program, move the deleted emails to the Deleted Items folder.
- When using Netscape mail clients—Deleted emails are moved to the Netscape Trash folder and no longer appear in the Netscape Inbox, but they do not disappear from the Outlook 2000 or 2002 Inbox unless users:
  - Configure the Netscape program to move deleted messages to the Trash folder and check the option to expunge the Inbox upon exiting.
  - Run only one program at a time and exit when finished so that the other program's Inbox synchronizes with the server and displays the same messages.

Also, sent emails are moved to the Netscape Sent folder (or other user-defined folder). If users wants sent messages to appear in the Microsoft Exchange Server Sent Items folder, then they need to manually drag them from the Netscape Sent folder to the Sent Items folder.

## Exchange Server and POP Clients

If your corporate mail server is an Exchange Server, then we presume that an employee's office machine is configured to use the Outlook 2000 or 2002 email client in native MAPI mode.

- Corporate laptop users: May use either of the supported Outlook Express clients for remote access to the Exchange Server via the Secure Access Service.
- Home machine users: May use any of the four Outlook clients for remote access to the Exchange Server via the Secure Access Service, assuming no MAPI account is configured on the remote machine.



**NOTE:** The Netscape email clients cannot be used in POP mode for remote access, because they do not support S-POP, which is required by the Secure Access Service for secure data transmission.

## Exchange Server and Outlook Web Access

To provide OWA access to your Exchange Server and enable users to access the Exchange Server through the Secure Access Service Web browsing feature, simply deploy OWA as a Web-based application on your intranet. You do not need to perform any additional setup to deploy an OWA implementation outside of your network.



**NOTE:** Using the Secure Access Service to access Outlook Web Access protects the Outlook Web Access IIS Web Server from standard attacks, such as Nimda, and thus is much more secure than putting Outlook Web Access directly on the Internet.

---

**Related Documentation**

- [About the E-Mail Client on page 725](#)
- [Choosing an E-Mail Client on page 726](#)
- [Working with a Standards-Based Mail Server on page 727](#)
- [About Lotus Notes and the Lotus Notes Mail Server on page 730](#)
- [Enabling the E-Mail Client at the Role Level on page 730](#)
- [Writing the E-Mail Client Resource Policy on page 731](#)

---

## About Lotus Notes and the Lotus Notes Mail Server

---

The Lotus Notes Mail Server provides POP3 and IMAP4 interfaces, enabling users to retrieve email from a Lotus Notes mail configuration through the Secure Access Service.

To enable access to:

- Corporate IMAP/POP/SMTP mail servers—Specify mail server, email session, and authentication information in the **Users > Resource Policies > Email Settings** page of the admin console.
- Microsoft Exchange Servers and Lotus Notes Servers—Use settings in the **Users > User Roles > SAM > Applications** page of the admin console.

**Related Documentation**

- [About the E-Mail Client on page 725](#)
- [Choosing an E-Mail Client on page 726](#)
- [Working with a Standards-Based Mail Server on page 727](#)
- [Working with the Microsoft Exchange Server on page 728](#)
- [Enabling the E-Mail Client at the Role Level on page 730](#)
- [Writing the E-Mail Client Resource Policy on page 731](#)

---

## Enabling the E-Mail Client at the Role Level

---

To use the Email Client feature, you must first enable it at the role level and then create a resource policy that specifies mail server settings.

To enable the Email Client feature at the role level:

1. In the admin console, choose **Users > User Roles > RoleName > General > Overview**.
2. In the Access features section, select the **Email Client** checkbox.

3. Click **Save Changes**.
4. Create a resource policy that specifies mail server settings.

**Related  
Documentation**

- [About the E-Mail Client on page 725](#)
- [Choosing an E-Mail Client on page 726](#)
- [Working with a Standards-Based Mail Server on page 727](#)
- [Working with the Microsoft Exchange Server on page 728](#)
- [About Lotus Notes and the Lotus Notes Mail Server on page 730](#)
- [Writing the E-Mail Client Resource Policy on page 731](#)

## Writing the E-Mail Client Resource Policy

When you enable the Email Client access feature for a role, you need to create a resource policy that specifies mail server settings. Unlike other access features, Secure Email Client has only one resource policy that applies to all roles for which this feature is enabled. If you choose to enable the email client service for users, you must specify IMAP/POP/SMTP mail server information and user authentication settings. The Secure Access Service serves as the email proxy for the specified server(s).

The Secure Access Service supports multiple mail servers. You can require all users to use a default mail server or you can enable users to specify a custom SMTP and IMAP or POP mail server. If you allow users to specify a custom mail server, the user must specify the server settings through the Secure Access Service. The Secure Access Service manages email usernames to avoid name conflicts.



**NOTE:** SMTP email proxy is not supported on the MAG Series Junos Pulse Gateways.

To write an Email Client mail server resource policy:

1. Enable the Email Client feature at the role-level.
2. In the admin console, choose **Users > Resource Policies > Email Client**.
3. Under Email Client Support, click **Enabled**.
4. Under Email Authentication Mode, select an option:
  - Web-based email session—Users must complete a one-time email setup for the Secure Access Service. Then, users configure their email client to use the username and password that are generated by the Secure Access Service email setup. It is recommended that users sign into the Secure Access Service to start an email session. (default)
  - Combined Secure Access Service and mail server authentication—Users configure their email client to use the following credentials:

- **Username**—The user's normal mail server username or a username that is generated by the Secure Access Service email setup if one of the following are true: (a) the user has multiple mail server usernames, or (b) the username on the Secure Access Service and mail server are different
- **Password**—The user's Secure Access Service password followed by a customizable credential separator character followed by the user's mail server password.

Users do not have to sign in to the Secure Access Service to use email.

- **Mail server authentication only**—Users configure their email client to use their normal mail server username and password. Users do not have to sign in to the Secure Access Service to configure or use email.



**NOTE:** Your users can easily determine their username and password for email by going to the Email Setup page.

5. Under Default Server Information, specify your mail server information. The Secure Access Service serves as the email proxy for this server.



**NOTE:** You can specify only one default mail server. If users need to retrieve email from more than one SMTP and POP or IMAP server, then allow users to define additional mail servers by clicking the appropriate checkbox. If you allow users to specify custom servers, they need to enter that server information one time in their Secure Access Service Email Setup page.

6. Under Email Session Information, specify the:
  - **Idle Timeout** value, which controls how long a user's email session may remain idle before the Secure Access Service ends the email client session.
  - **Max. Session Length** value, which controls how long a user's email session may remain active before the Secure Access Service ends the email client session.
7. Click **Save Changes**.

#### Related Documentation

- [About the E-Mail Client on page 725](#)
- [Choosing an E-Mail Client on page 726](#)
- [Working with a Standards-Based Mail Server on page 727](#)
- [Working with the Microsoft Exchange Server on page 728](#)
- [About Lotus Notes and the Lotus Notes Mail Server on page 730](#)
- [Enabling the E-Mail Client at the Role Level on page 730](#)



## CHAPTER 28

# VPN Tunneling

- [About VPN Tunneling on page 734](#)
- [VPN Tunneling on 64-Bit Linux Platforms on page 736](#)
- [Task Summary: Configuring VPN Tunneling on page 737](#)
- [VPN Tunneling Execution on page 739](#)
- [Automatically Signing into VPN Tunneling using GINA on page 740](#)
- [Using GINA Chaining on page 742](#)
- [Credential Provider for Windows Vista and Later on page 742](#)
- [Smart Card Credential Provider on page 744](#)
- [Credential Provider Authentication for Pulse Secure Access Service on page 745](#)
- [Launching VPN Tunneling During a Windows Secure Application Manager Session on page 749](#)
- [Logging In To Windows Through a Secure Tunnel on page 750](#)
- [VPN Tunneling Connection Profiles with Support for Multiple DNS Settings on page 751](#)
- [VPN Tunneling Incompatibility with Other VPN Client Applications on page 752](#)
- [Linux Client Requirements on page 752](#)
- [Client Side Logging on page 752](#)
- [VPN Tunneling Proxy Support on page 753](#)
- [VPN Tunneling Quality of Service on page 754](#)
- [VPN Tunneling Multicast Support on page 755](#)
- [Defining VPN Tunneling Role Settings on page 755](#)
- [About VPN Tunneling Resource Policies on page 759](#)
- [Defining VPN Tunneling Access Control Policies on page 760](#)
- [Creating VPN Tunneling Connection Profiles on page 761](#)
- [Defining Split Tunneling Network Policies on page 768](#)
- [VPN Tunneling Resource Policy Configuration Use Case on page 770](#)
- [About VPN Tunneling Bandwidth Management Policies on page 772](#)
- [Writing a VPN Tunneling Bandwidth Management Resource Policy on page 775](#)
- [Configuring the VPN Tunnel Server on page 776](#)

- [VPN Tunneling Installer Overview on page 777](#)
- [Network Connect Launcher \(NC Launcher\) Overview on page 780](#)
- [Launching Network Connect On Other Platforms on page 782](#)
- [Troubleshooting Network Connect Errors on page 784](#)

## About VPN Tunneling

---

The VPN tunneling access option (formerly called Network Connect) provides a VPN user experience, serving as an additional remote access mechanism to corporate resources using the Secure Access Service. This feature supports all Internet-access modes, including dial-up, broadband, and LAN scenarios, from the client machine and works through client-side proxies and firewalls that allow SSL traffic.

When a user launches VPN tunneling, Secure Access Services transmits all traffic to and from the client over the secure VPN tunnel. The only exception is for traffic initiated by other Secure Access Service-enabled features, such as Web browsing, file browsing, and telnet/SSH. If you do not want to enable other Secure Access Service features for certain users, create a user role for which only the VPN tunneling option is enabled and make sure that users mapped to this role are not also mapped to other roles that enable other Secure Access Service features.

With VPN tunneling, the client's machine effectively becomes a node on the remote (corporate) LAN and becomes invisible on the user's local LAN; the Secure Access Service serves as the Domain Name Service (DNS) gateway for the client and knows nothing about the user's local LAN. Users may define static routes on their PCs, however, to continue to access the local LAN while simultaneously connecting to the remote LAN. Since PC traffic goes through the VPN tunnel to your internal corporate resources, make sure that other hosts within a user's local network cannot connect to the PC through the VPN tunnel.

In the event of broken network connectivity, only the Windows and Macintosh versions of VPN tunneling try (indefinitely) to reconnect.

You can ensure that other hosts in a remote user's LAN cannot reach internal corporate resources by denying the user access to the local subnet (configured on the Users > User Roles > Select Role > VPN Tunneling tab). If you do not allow access to a local subnet, then Secure Access Service terminates VPN tunneling sessions initiated by clients on which static routes are defined. You may also require clients to run endpoint security solutions, such as a personal firewall, before launching a network-level remote access session. Host Checker, which performs endpoint security checks on hosts that connect to a Secure Access Service, can verify that clients use endpoint security software.



**NOTE:** A Hosts file entry is added by VPN tunneling to support the following case:

- If, when VPN Tunneling connects, split tunneling is disabled and the original externally resolved hostname (the hostname the user initially connected to prior to the VPN tunnel launch) resolves to another IP address against the internal DNS, the browser will redirect to a “Server not found” page, because no route is defined within the client system.
- At a graceful termination (sign-out or timeout) of the VPN tunnel client connection, the Hosts file is restored. If the Hosts file was not restored in a prior case due to an ungraceful termination, the Hosts file will be restored the next time the user launches VPN tunneling.

For VPN tunneling to communicate, the following ports must be open:

- UDP port 4242 on loopback address
- TCP port 443
- If using ESP mode, the UDP port configured on the Secure Access Service ( default is UDP 4500).

The VPN tunneling option provides secure, SSL-based network-level remote access to all enterprise application resources using Secure Access Service over port 443. Port 4242 is used for IPC communication between the VPN tunneling service and the VPN tunnel executable on the client PC. Typically endpoint products do not block this type of IPC communication. However, if you have an endpoint product that does block this communication, you must allow it for VPN tunneling to work properly.



**NOTE:** If you enable the multiple sessions per user feature, VPN tunnel clients may not be assigned the same IP address. For example, VPN tunnel client may be assigned a different VIP address each time they connect to a Secure Access Service when the Secure Access Service is obtaining the DHCP addresses from a DHCP server.

#### Related Documentation

- [Task Summary: Configuring VPN Tunneling on page 737](#)
- [Defining VPN Tunneling Role Settings on page 755](#)
- [About VPN Tunneling Resource Policies on page 759](#)
- [Network Connect Launcher \(NC Launcher\) Overview on page 780](#)
- [Troubleshooting Network Connect Errors on page 784](#)

## VPN Tunneling on 64-Bit Linux Platforms

A native 64-bit VPN Tunneling client is not yet available. Instead, changes in the existing 32-bit client were made so that it can be run on 64-bit platforms. Because of this, VPN Tunneling has dependencies with 32-bit Java and 32-bit standard libraries even when running on a 64-bit platform.

See the *Secure Access Service Supported Platforms Guide* for a list of supported browsers, platforms and plug-ins for VPN Tunneling.

To run VPN Tunneling on a 64-bit Linux platform, you must perform the following tasks on your Linux system:

- Install a 64-bit web browser and configure the Java plug-in.
- Download and install the 32-bit Java for Linux.
- Update the Java alternatives links. If you install the 32-bit Java using package managers like “apt-get” and “yum” and so forth, the Java alternatives links are updated automatically and you can skip this step.
  - **sudo update-alternatives --install /usr/bin/java java 32-bit-Java-path priority.**
  - Check that 64-bit Java is the default. To see which is the default Java, use the **update-alternatives --display java** command.
  - If necessary, use the **sudo update-alternatives ---config java** command to change the default Java.
- Install the standard 32-bit libraries and components. For example:

**Table 47: Installing Standard 32-Bit Libraries and Components**

Linux Distribution Method	Command
Ubuntu	<b>apt-get install ia32-libs</b>
Fedora	<b>yum -y install xterm</b> <b>yum -y ld-linux.so.2</b> <b>yum -y libstdc++-so.6</b> <b>yum -y libz.so.1</b> <b>yum -y libXext.so.6</b> <b>yum -y libXrender.so.1</b> <b>yum -y libXtst.so.6</b>
OpenSUSE	<b>zypper install libXi.so.6</b>

The syntax for launching VPN Tunneling from the command line is:

```
32-bit_Java_path -cp NC.jar -h ivehostname -u username -p password [-r realm] -f sa_certificate_in_der_format [-l gui_log_level [-L ncsvc_log_level] [-y proxy-z proxy_port [-s proxy_username -a proxy_password [-d proxy_domain]]]
```

There are no changes in the Secure Access Service admin GUI or in the VPN Tunneling client user interface to run on a 64-bit Linux platform, however you should note the following:

- The 32-bit Java path must be used when launching VPN Tunneling from the command line.
- If the VPN Tunneling launcher cannot find the 32-bit Java path in the alternatives links, the “Setup Failed. Please install 32-bit Java and update alternatives links using update-alternatives command. For more details, please refer KB article KB25230.” error appears.
- Agentless host checker is supported when VPN Tunneling is launched from a browser but is not supported when VPN Tunneling is launched from command line.

**Related  
Documentation**

- [About VPN Tunneling on page 734](#)

## Task Summary: Configuring VPN Tunneling

The following steps do not account for preliminary configuration steps such as specifying the Secure Access Service's network identity or adding user IDs.

To configure the Secure Access Service for VPN tunneling:

1. Enable access to VPN tunneling at the role-level using settings in the Users > User Roles > Role > General > Overview page of the admin console.
2. Create VPN tunneling resource policies using the settings in the Users > Resource Policies > VPN Tunneling tabs:
  - a. Specify general access settings and detailed access rules for VPN tunneling in the Access Control tab of the admin console.
  - b. Specify Connection Profiles to assign to remote users in the Connection Profiles tab of the admin console.
  - c. (Optional) Specify split tunneling behavior for VPN tunneling in the Split Tunneling tab of the admin console.
3. Specify whether or not to enable GINA/Credential Provider installation, employ split tunneling, and/or auto-launch behavior in the Users > User Roles > Role > VPN Tunneling page of the admin console.



**NOTE:** If you choose to activate split tunneling behavior in this page, you must first create at least one split-tunneling resource profile, as described above.

You must enable VPN tunneling for a given role if you want a user mapped to that role to be able to use GINA/Credential Provider during Windows logon.

4. Specify an IP address for the VPN tunneling server-side process to use for all VPN tunneling user sessions on the System > Network > VPN Tunneling page in the admin console.
5. Ensure that an appropriate version of VPN tunneling is available to remote clients.
6. If you want to enable or disable client-side logging for VPN tunneling, configure the appropriate options in the System > Log/Monitoring > Client Logs > Settings page of the admin console.

To install VPN tunneling, users must have appropriate privileges, as described in Client-Side Changes. If the user does not have these privileges, use the Juniper Installer Service available from the Maintenance > System > Installers page of the admin console to bypass this requirement.

VPN tunneling requires signed ActiveX or signed Java applets to be enabled within the browser to download, install, and launch the client applications.

By default, Vista Advanced firewall blocks all inbound traffic and allow all outbound traffic. For VPN tunneling to work in conjunction with Vista Advanced firewall, configure the following settings:

- Change the Vista Advance firewall default settings to block all inbound and outbound traffic
- Create the following outbound rules in the appropriate firewall profile:
  - Create a port rule to allow any to any IP and TCP any port to 443
  - Create a custom rule to allow 127.0.0.1 to 127.0.0.1 TCP any to any
- Allow iExplorer.exe

In prior releases you could specify whether Secure Access Service compiles packet logs for specific VPN tunneling users. This option is no longer available as it impacts performance.

**Related  
Documentation**

- [Defining Default Options for User Roles on page 122](#)
- [Defining VPN Tunneling Access Control Policies on page 760](#)
- [Creating VPN Tunneling Connection Profiles on page 761](#)
- [Defining Split Tunneling Network Policies on page 768](#)
- [Downloading Application Installers on page 813](#)
- [About Client-Side Logs on page 948](#)

## VPN Tunneling Execution

The VPN tunneling agent executes as follows:

1. If Graphical Identification and Authorization (GINA) is installed and registered on the remote client, the client automatically initiates a VPN tunnel to the Secure Access Service when the user signs into Windows; otherwise, the user needs to sign into Secure Access Service and click on the VPN Tunneling link on the end-user home page (if you have not configured VPN tunneling to launch automatically).



**NOTE:** SSO is supported only when VPN tunneling GINA is the only GINA installed on the client's system.

2. If the user does not have the latest version of the VPN tunneling installer, the Secure Access Service attempts to download an ActiveX control (Windows) or a Java applet (Macintosh and Linux) to the client machine that then downloads the VPN tunneling software and performs installation functions. If the Secure Access Service fails to download or upgrade the ActiveX control to a Windows client due to restricted access privileges or browser restrictions, the Secure Access Service uses a Java applet to deliver the VPN tunneling software to the client.



**NOTE:** If Microsoft Vista is running on the user's system, the user must click the setup link that appears during the installation process to continue installing the setup client and VPN tunneling. On all other Microsoft operating systems, the setup client and VPN tunneling install automatically.

Whether the Secure Access Service downloads an ActiveX control or a Java applet, both components attempt to identify the presence and version of existing VPN tunneling software on the client before determining which of the following installation functions to perform:

- If the client machine has no VPN tunneling software, install the latest version.
- If the client machine has an earlier version of VPN tunneling software, upgrade the shared VPN tunneling components to the newer version and install the most current UI version from Secure Access Service.



**NOTE:** For information about valid Java applets, installation files and logs, and the operating system directories in which delivery mechanisms run, see Client-Side Changes.

3. Once installed, the VPN tunneling agent sends a request to the Secure Access Service to initialize the connection with an IP address from the pre-provisioned IP pool (as

defined by the VPN Tunneling Connection Profiles resource policies applicable to the user's role).

4. The VPN tunneling system tray icon starts running in the taskbar on a Windows client or in the Dock on a Mac client.
5. Secure Access Service allocates an IP address (from a VPN Tunneling Connection Profiles resource policy) and assigns a unique IP to the VPN tunneling service running on the client.
6. The client-side VPN tunneling service uses the assigned IP address to communicate with the VPN tunneling process running on the Secure Access Service.
7. After the Secure Access Service allocates an IP address to the client, the Secure Access Service opens a direct channel of communication between the client and all enterprise resources to which the user's resource policy allows access. The internal application server sees the source IP as the client's IP address.

The client-side VPN tunneling agent communicates with the Secure Access Service, which, in turn, forwards client requests to enterprise resources.



**NOTE:** If you use Host Checker to validate the presence of client-side security components based on policies you define on the Secure Access Service and the client cannot conform to the security policies at any point during a VPN tunneling session, Host Checker terminates the session.

**Related Documentation**

- [Task Summary: Configuring VPN Tunneling on page 737](#)

## Automatically Signing into VPN Tunneling using GINA

The Graphical Identification and Authorization (GINA) sign-in function is an automated sign-in method you can install and enable on Windows clients signing in to a Windows NT domain. You can require VPN tunneling to install GINA on the client machine, or you can allow users to decide whether or not to install GINA when they launch VPN tunneling.



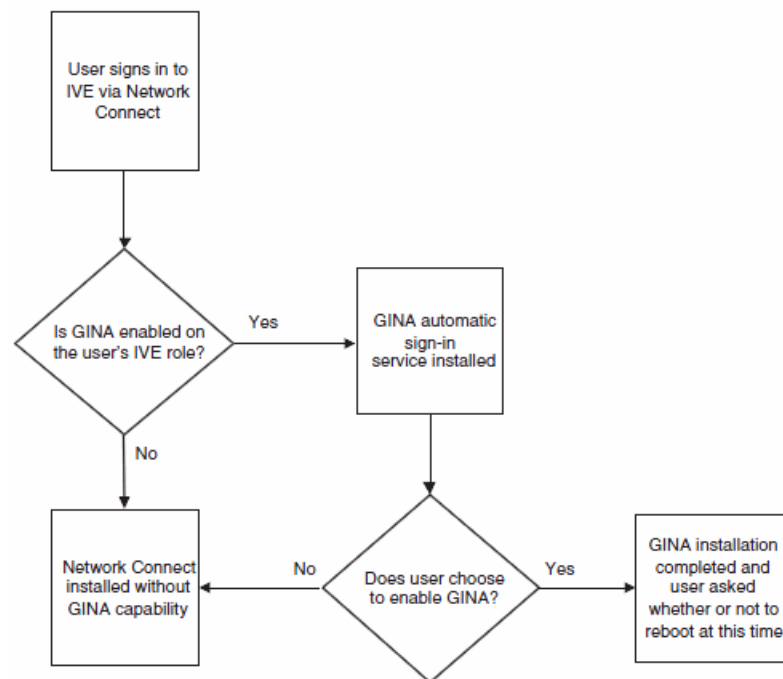
**NOTE:** You cannot install more than one GINA automatic sign-in function on a client's system. If another application on the client's system uses a GINA function, VPN tunneling cannot install and activate the GINA component.

If GINA is installed on the client, it automatically prompts the user to choose whether or not to launch VPN tunneling each time he/she signs in to Windows. If you choose to make GINA installation optional, the user can activate GINA using the Auto connect when login to Windows option in the VPN tunneling window. This option is only available during an open VPN tunneling session.

The option to enable GINA installation on client systems is available when you define role attributes in the Users > User Roles > Role > VPN Tunneling page.



Figure 47: GINA Installation Process



The GINA installation process takes place one time and requires the user to perform a system reboot in order to enable GINA sign-in capability. From that session forward, GINA prompts the user to decide whether or not to launch VPN tunneling at each Windows sign-in. When the user signs in, unless otherwise specified, GINA passes the user's Windows sign-in credentials to Secure Access Service for authentication before establishing the VPN tunneling tunnel.



**NOTE:** End-users can not modify their Windows user password through VPN tunneling GINA.

When a user logs in to the Secure Access Service through the Juniper GINA, if the version of the VPN tunneling client on the user's computer matches that on the Secure Access Service, the Juniper GINA establishes a VPN tunneling connection to the Secure Access Service. If the VPN tunneling versions do not match, the Juniper GINA does not establish a VPN tunneling connection to the Secure Access Service. Prior to release 5.4, the Juniper GINA displays a version mismatch warning and allows users to log in to the Windows desktop using their cached credentials. With release 5.4 and later, the Juniper GINA allows the users to log in to the Windows desktop using their cached credentials and then launches a standalone VPN tunneling. Users log in to the Secure Access Service and the appropriate VPN tunneling client automatically downloads to the user's computer and launches.

If you use Host Checker to validate the presence of client-side security components (pre-authorization), Host Checker starts after VPN tunneling is launched. This is

sometimes called a system-mode check. Host Checker exists after successful validation and is later restarted once the user is logs in to their desktop (called user-mode).

## Using GINA Chaining

---

VPN tunneling supports GINA chaining. GINA chaining means that one GinaDLL calls another GinaDLL. By default, enabling VPN tunneling GINA also enables VPN tunneling GINA chaining. The VPN tunneling client detects any currently installed GINA component on top of the existing GINA chain. If the GINA component is compatible, VPN tunneling GINA is placed in front of the current GINA components. Currently, VPN tunneling supports the following GINA components:

- Cisco VPN client (CSGina.dll)
- Microsoft GINA (msgina.dll)
- Nortel Networks VPN client (nngina.dll)
- RSA SecurID (AceGina.dll)
- Novell GINA (NWGINA.dll)

If an installed GINA component is not supported (that is, not in the above list), a warning message appears and the VPN tunneling GINA is not installed.

If you uninstall a GINA component after VPN tunneling adds its information to the GINA chain, the VPN tunneling GINA removes the saved GINA information and does not call the removed GINA component the next time it goes through GINA chaining.



**NOTE:** If the VPN tunneling GINA is installed at the top of the GINA chain (meaning, it is the last one installed), the VPN tunneling GINA is uninstalled when you uninstall the VPN tunneling client. However, if the VPN tunneling GINA is in the middle of the chain, you must remove all GINAs higher in the chain than the VPN tunneling GINA prior to removing the VPN tunneling GINA.

---

## Credential Provider for Windows Vista and Later

---

In releases prior to Windows Vista, the customization of interactive user logon was done by creating a custom GINA. Users entered their authentication credentials in the logon UI and GINA passed this information to Winlogon for authentication. However, because GINAs do more than pass authentication information, they are typically difficult to implement.

Windows Vista introduces a new authentication model where the logon UI and Winlogon talk directly with each other. A credential provider is a module that plugs into the logon UI and describes the credential information required for the login UI to render and to communicate with an external authentication provider. After the credential provider gathers the credential information, it passes the final credentials to Winlogon.

There are two basic types of credential providers: standard authentication and Pre-Logon Access Providers (PLAP). Standard authentication includes password-based or

certificate-based credentials. A PLAP is a special type of credential provider that allows users to make a network connection before logging in to their system. Another difference between these two types of providers is timeout. PLAP credentials have no timeout where standard credentials typically have a 120 second timeout.

The VPN tunneling credential provider is a PLAP provider. This provider is visible only if the system is configured as part of a domain. The VPN tunneling provider creates a network connection. If the user's credentials are the same as the domain credential (SSO) then the credential information is entered only once. If the user's credentials are not the same as the domain credentials, the users selects another credential provider for domain authentication.

After a user logs in to the Secure Access Service through VPN Tunneling Credential Providers, the user has 5 minutes to log in to Vista either through single sign-on or through another Credential Provider. After the user logs into Vista, VPN tunneling attaches to the tunnel. If the user does not log in to Vista within 5 minutes, the VPN tunneling tunnel is disconnected.

To install the VPN tunneling credential provider,

1. Make sure your client user is part of a Windows domain.
2. In the Admin console, go to User Roles > VPN tunneling and select the Require VPN tunneling to start when logging into Windows option.
3. When installing VPN tunneling on the client system (running Windows Vista), you are prompted by the GINA/Credential Provider window to configure the GINA/Credential Provider authentication. Click OK.
4. Once the VPN tunnel is established on the client system, open the VPN tunneling window. Go to the Advanced View and select the Information tab. In the Results section, ensure that the GINA/Credential Provider plug-in is configured. You should see something similar to GINA Plug-In: Configured.

To use credential provider:

1. Log out of Windows and press Ctrl+Alt+Delete.  
You should see the Network logon icon. If you see only the Windows user standard tiles, click the Switch user option under the standard Windows credential tiles to see the Network logon icon.
2. Click the Network login icon and then click the Secure Access Service logon icon.
3. Enter your Windows domain credential and click the right arrow button. For your username, use the format domain\username or user@domain.

VPN tunneling signs the user in to the default URL and proxy server in config.ini.



**NOTE:** If your Secure Access Service credential is not the same as your Windows domain credential, an alert box appears. Click OK and enter your Secure Access Service credentials in the login window that appears. The window also contains an option button to launch another window to enter a URL, proxy server, and so forth.

There are a few things to note about the VPN tunneling credential provider on Vista:

- On Windows XP, GINA appears prior to the Windows logon window. On Windows Vista, you enter the Windows domain credential on the Secure Access Service logon icon. The VPN tunneling window appears and establishes the PLAP connection while logging in to the Windows desktop.
- VPN tunneling credential provider supports the following authentication provider: local authentication, LDAP, RADIUS (UN/PWD only), NIS, ADS and Dial-up connection. In addition, smart card credential provider supports certificate login.

## Smart Card Credential Provider

Windows Vista also supports smart card credential provider—passing user credentials upon a smart card being inserted. If there is smart card present, a VPN tunneling Smart Card Credential Provider DLL tile shows on the PLAP layer. Click the tile and enter your smart card PIN to login.

To install the smart card VPN tunneling credential provider,

1. Make sure your client user is part of a Windows domain.
2. In the Admin console, select **User Roles > Role > VPN Tunneling** and select the **Require client to start when logging into Windows** option.
3. When installing VPN tunneling on the client system (running Windows Vista), you are prompted by the GINA window to configure the GINA authentication. Click **OK**.

Use the smart card to log in to the Secure Access Service from a browser so the config.ini file will contain the smart card login URL which can then be used by the smart card DLL.

4. Once the VPN tunnel is established on the client system, open the VPN tunneling window. Go to the Advanced View and select the Information tab. In the Results section, ensure that the GINA plug-in is configured. You should see something similar to GINA Plug-In: Configured.

To use the smart card credential provider:

1. Log out of Windows and press Ctrl+Alt+Delete.

You should see the Network logon icon located in the lower right corner of your screen. If you see only the Windows user standard tiles, click the Switch user option under the standard Windows credential tiles to see the Network logon icon.

2. Click the Network login icon and then click the smart card icon.
3. Enter your PIN number or password and click the right arrow button.

VPN tunneling uses the PIN to retrieve the stored certificate and to log in to the Secure Access Service. After a successful login, the PIN is passed to Winlogon to log in to Vista.



**NOTE:** If your Secure Access Service credential is not the same as your Windows domain credential, an alert box appears. Click OK. If a connection icon appears in the lower right corner of your screen, switch to the standard credential login tiles and log in to Vista. Otherwise, enter your Windows credential in the login box.

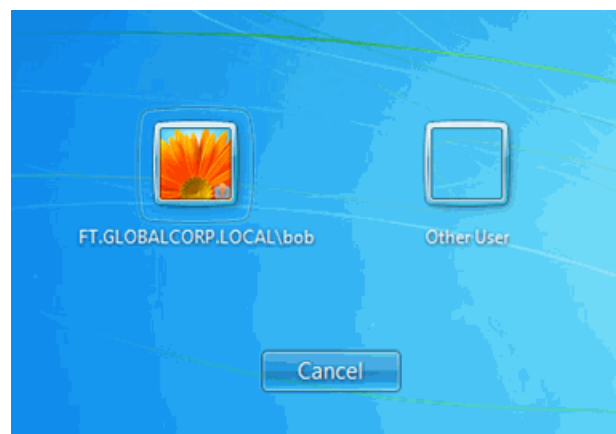
VPN tunneling retrieves the user principal name (UPN) from the smart card and compares them with the login user and domain names. If they do not match, the tunnel is disabled. The UPN typically has the format user@domain.

- Related Documentation**
- [Task Summary: Configuring VPN Tunneling on page 737](#)

## Credential Provider Authentication for Pulse Secure Access Service

The Junos Pulse credential provider integration enables connectivity to a network that is required for the user to logon to the Windows domain. For example, the domain controller might reside behind a firewall and the endpoint uses credential provider login to connect to Pulse Access Control Service prior to domain login. Junos Pulse integrates with Microsoft credential providers to enable password based login and smart card login. A credential provider interface appears as a tile on a Windows Vista or Windows 7 login screen.

**Figure 48: Pulse Logon Tile**



You enable Pulse credential provider support on a Pulse connection. After the connection has been downloaded to the endpoint through the normal Pulse distribution methods,

a Pulse logon tile appears on the endpoint's desktop. When the user initiates the logon process, Pulse establishes the connection.

Pulse supports the following credential provider types:

- **user-at-credprov**—The connection is established before the user login using credentials collected at the selected credential tile, which provides single-sign-on functionality. The connection is maintained as an active connection on the user's desktop.
- **machine-then-user-at-credprov**—The connection is established using machine credentials when no user is logged in. When a user clicks a logon tile and provides user credentials, the machine connection is disconnected and a new connection is established. When the user logs off, the user connection is disconnected and the machine connection is reestablished. In one typical machine-then-user-at-cred prov implementation, the machine connection and the user connection are mapped to different VLANs.

Pulse credential provider support usage notes:

- If the endpoint includes more than one Pulse Layer 2 connection, Windows determines which connection to use:
  1. If a network cable is attached to the endpoint, Layer 2 wired connections are attempted, and then wireless connections. If there are more than one wireless network available, the order is determined by the scan list specified as a Pulse connection option.
  2. After all Layer 2 options are attempted, Pulse runs location awareness rules to find one or more eligible Layer 3 connections that are configured for credential provider login. If more than one Layer 3 connection is found, Pulse prompts the user to select a connection. A user can cancel the network connection attempt by clicking the cancel button.
  3. After Pulse evaluates all configured connection options, Pulse returns control to Windows, which enables the user login operation.
- For connections that use user credentials, the Pulse connection may be configured so that prompts are presented during the login process, for example, prompts for realm or role selection or a server certificate trust prompt. For connections that use machine credentials, Pulse prompts cause the connection to fail because there is no interface to allow a response to the prompts. You can suppress any potential realm and role choice by specifying a preferred realm and role for the connection.
- Pulse upgrade notifications and actions are disabled during credential provider login and postponed until the user connection is established. Host Checker remediation notifications are displayed.

To enable user-at-credprov credential provider support for a Pulse connection:

1. Create a Pulse connection set for the role (**Users > Junos Pulse > Connections**), and then create a new Pulse connection. You can select either a Layer 3 connection type, **SSL VPN or UAC (L3)**, or a Layer 3 connection type, **UAC (802.1X)**.
2. In the Connection is established section, select one of the following options:
  - **Automatically at user login**—The user credentials are used to establish the authenticated Pulse connection to the network, login to the endpoint, and login to the domain server. The Pulse connection may be configured so that prompts are presented during the login process, for example, prompts for realm or role selection or a server certificate trust prompt.



**NOTE:** This label changed at Pulse Secure Access Service R7.3. If you had selected the old label for a Pulse connection, “Automatically during desktop authentication. User is presented with the Junos Pulse credential tile at the logon screen,” it is automatically converted to the new label, “Automatically at user login” when you perform the upgrade from R7.2.

- **Automatically when the machine starts. Connection is authenticated again at user login**—Machine credentials are used to establish the authenticated Pulse connection to the network when the endpoint is started. When a user clicks the login tile and provides user credentials, the connection is authenticated again and the original connection is dropped. When the user logs off, the user connection is ended and the machine connection is established again. In one typical use case, the machine credentials provide access to one VLAN and the user credentials provide access to a different VLAN. Be sure that the Pulse connection does not result in Pulse prompts, for example, prompts for realm or role selection or a server certificate trust prompt, because the machine credential login does not present an interface to respond to the prompts.
3. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type **Any** as the Server certificate DN. To allow only one server certificate, specify the server certificate’s full DN for example, C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=username@mycompany.com.
  4. Specify **Realm and Role Preferences** to suppress realm or role selection dialogs during the logon process:
    - **Preferred User Realm**—Specify the realm that for this connection. The connection ignores any other realm available for the specific logon credentials
    - **Preferred User Role Set**—Specify the preferred role or the name of rule for the role set to be used for user authentication. The role or rule name used must be a member of the preferred user realm.

To enable machine-then-user-at-credprov credential provider support for a Pulse connection:

1. Create a Pulse connection set for the role (**Users > Junos Pulse > Connections**), and then create a new Pulse connection. You can select either a Layer 3 connection type, **SSL VPN or UAC (L3)**, or a Layer 3 connection type, **UAC (802.1X)**.
2. In the Connection is established section, select one of the following options:
  - **Automatically at user login**—The user credentials are used to establish the authenticated Pulse connection to the network, login to the endpoint, and login to the domain server. The Pulse connection may be configured so that prompts are presented during the login process, for example, prompts for realm or role selection or a server certificate trust prompt.



**NOTE:** This label changed at Pulse Secure Access Service R7.3. If you had selected the old label for a Pulse connection, “Automatically during desktop authentication. User is presented with the Junos Pulse credential tile at the logon screen,” it is automatically converted to the new label, “Automatically at user login” when you perform the upgrade from R7.2.

- **Automatically when the machine starts. Connection is authenticated again at user login**—Machine credentials are used to establish the authenticated Pulse connection to the network when the endpoint is started. When a user clicks the login tile and provides user credentials, the connection is authenticated again and the original connection is dropped. When the user logs off, the user connection is ended and the machine connection is established again. In one typical use case, the machine credentials provide access to one VLAN and the user credentials provide access to a different VLAN. Be sure that the Pulse connection does not result in Pulse prompts, for example, prompts for realm or role selection or a server certificate trust prompt, because the machine credential login does not present an interface to respond to the prompts.
3. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type **Any** as the Server certificate DN. To allow only one server certificate, specify the server certificate's full DN for example, C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=username@mycompany.com.
  4. Specify **Realm and Role Preferences** to suppress realm or role selection dialogs during the logon process for both machine logon and user logon:
    - **Preferred Machine Realm**—Specify the realm that this connection uses when establishing the machine connection. The connection ignores any other realm available for the specific logon credentials
    - **Preferred Machine Role Set**—Specify the role or the name of rule for the role set that this connection uses when establishing the machine connection. The role or rule name used must be a member of the preferred machine realm.



- **Preferred User Realm**—Specify the realm that for this connection that is used when a user logs onto the endpoint. The connection ignores any other realm available for the user’s logon credentials
  - **Preferred User Role Set**—Specify the preferred role or the name of rule for the role set to be used for user authentication. The role or rule name used must be a member of the preferred user realm.
5. Optionally specify pre-login preferences:
- **Pre-login maximum delay**—The time period (seconds) that a Windows client waits for an 802.1x connection to succeed during the login attempt. The range 1 to 120 seconds.
  - **Pre-login user based virtual LAN**—If you are using VLANs for the machine login and the user login, you can enable this check box to allow the system to make the VLAN change.
6. Click **Save Changes** and then distribute the Pulse connection to Pulse client endpoints.

The Junos Pulse tile appears on the login page the next time the end-users log in.



**NOTE:** The user account must exist on both the Windows PC and on the Secure Access Service with the same login name.

Check the user logs for credential provider log-in information.

Figure 49: Credential Provider Log Information

Severity	ID	Message
Info	NWC30477	2012-07-19 16:29:38 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - VPN Tunneling: User with IP 192.168.247.100 connected with ESP transport mode.
Info	NWC23508	2012-07-19 16:29:38 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - Key Exchange number 1 occurred for user with NCIP 192.168.247.100
Info	NWC30477	2012-07-19 16:29:32 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - VPN Tunneling: User with IP 192.168.247.100 connected with SSL transport mode.
Info	NWC23464	2012-07-19 16:29:32 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - VPN Tunneling: Session started for user with IP 192.168.247.100, hostname W7-001
Info	ERR24670	2012-07-19 16:29:32 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - VPN Tunneling: ACL count = 1.
Info	AUT24414	2012-07-19 16:29:32 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - Agent login succeeded for FT.GLOBALCORP.LOCAL\bob/Users from 192.168.1.12.
Info	AUT24326	2012-07-19 16:29:32 - ive - [192.168.1.12] Root::FT.GLOBALCORP.LOCAL\bob(Users)[Enterprise, Remediation] - Primary authentication successful for FT.GLOBALCORP.LOCAL\bob/AD from 192.168.1.12

Related  
Documentation

## Launching VPN Tunneling During a Windows Secure Application Manager Session

Users can launch VPN tunneling while signed in to the Secure Access Service via Windows Secure Application Manager (WSAM). When a user launches VPN tunneling in this scenario, however, the VPN tunneling installer automatically terminates the WSAM session prior to launching VPN Tunneling.

During the process, the user is prompted with a warning message informing them that they are about to terminate their WSAM session in favor of launching VPN tunneling. We recommend that you configure users' VPN tunneling resource policies to feature as much access to network resources as they would have in their WSAM sessions. This way, when users choose to launch VPN tunneling (simultaneously terminating WSAM) they will still be able to access the same network resources.



**NOTE:** If users choose not to launch VPN tunneling, the VPN tunneling installer still automatically installs the client application on their computer, but does not launch VPN tunneling. After the client application has been installed, users can choose to uninstall it manually via their secure gateway home page or the folder options available in the Windows Start menu.

**Related Documentation**

- [Task Summary: Configuring VPN Tunneling on page 737](#)

---

## Logging In To Windows Through a Secure Tunnel

---

Use the Logoff On Connect feature for users to log in to their Windows environment through an existing VPN tunnel. This feature lets them authenticate against a Windows Domain server in real time, as opposed to authenticating with the locally cached credentials. When this feature is enabled, they are automatically logged off Windows after the VPN tunneling session starts. The standard Windows login screen re-appears and they log in using their Windows credentials. Their Windows environment is now established through the VPN tunnel.



**NOTE:** Users must log in to Windows within 5 minutes of the login screen re-appearing or before the Host Checker policy evaluate period ends, whichever is shorter. If they do not, their VPN tunnel connection may time out and they will not be logged in to Windows through a secure tunnel. An error appears if the VPN tunnel connection times out.

The Logoff On Connect feature is not supported within SVW.

To use the Logoff On Connect feature:

1. Users log on to their local machine using their domain cached credentials. Their machine must be part of a Windows domain.
2. Users launch VPN tunneling and click **Tools** from the login page.
3. Select the **Logoff on Connect** option and click **OK**.
4. Users enter their username and password credentials in the login page.

A tunnel is established and logs them off of their local machine. The Windows login page appears.

5. Users enter their username and password credentials to sign-in to their Windows Domain using the VPN tunnel.

**Related Documentation**

- [Task Summary: Configuring VPN Tunneling on page 737](#)

## VPN Tunneling Connection Profiles with Support for Multiple DNS Settings

To ensure remote users are able to perform DNS searches as efficiently or as securely as possible, you can configure the Secure Access Service to allow multiple DNS settings during VPN tunneling sessions, based on a user's role membership.

When Secure Access Service launches a user's VPN tunneling session, the Secure Access Service uses a matching profile based on the user's role membership containing IP address, DNS, and WINS settings.

If you enable split-tunneling, the DNS search order setting allows you to define which DNS setting takes precedence—for example, search for a DNS server on the client's LAN before the Secure Access Service's DNS server, or vice-versa. VPN tunneling makes a backup of the client's DNS settings/search order preference before establishing a connection. After the session terminates, VPN tunneling restores the client to the original DNS settings. If you disable split-tunneling, all DNS requests go to the Secure Access Service's DNS server and your setting for the DNS search order preference does not apply.



**NOTE:** After stopping and restarting a DNS client, the client may not pick up the search order of multiple DNS addresses in a timely manner, resulting in an incorrect lookup order when launching VPN tunneling. The rules governing DNS name resolution and failover are complex and often specific to the particular client operating system. You or the end-user can attempt to run the `ipconfig /registerdns` commands from a command window on the client machine. This may reset the search order to the correct order. To understand the search resolution order for DNS servers, refer to the appropriate Microsoft DNS documentation for your operating system platform.

When employing a multi-site cluster of Secure Access Service devices, the IP pool and DNS settings may be unique to each Secure Access Service residing at a different site. For this reason, Secure Access Service allows the VPN Tunneling Connection Profile policy to be node-specific. That is, the resource policy enables the client to connect to the same Secure Access Service in the cluster each time a new session is established.

**Related Documentation**

- [Deploying an IVS on page 1014](#)
- [Configuring VPN Tunneling for Use on a Virtualized Secure Access Service on page 1043](#)

## VPN Tunneling Incompatibility with Other VPN Client Applications

Third-party vendor VPN client applications may be incompatible with VPN tunneling. The following table lists known VPN client vendors and VPN tunneling's relative compatibility with those vendors' VPN client applications.

**Table 48: VPN tunneling Compatibility with Third-Party VPN Clients**

Vendor	Compatible?
Cisco	Yes
Nortel	Yes
NS Remote	Yes
Intel	Yes
Checkpoint	Yes

If you want to install VPN tunneling on a client featuring an incompatible VPN client application, you must uninstall the incompatible application before you install or launch VPN tunneling on the client.

**Related Documentation**

- [Task Summary: Configuring VPN Tunneling on page 737](#)

## Linux Client Requirements

Linux clients signing in to VPN tunneling via Mozilla Firefox must ensure that the OpenSSL libraries are installed on the client. Most Linux versions come pre-packaged with OpenSSL. If you encounter a Linux user that does not have the required OpenSSL libraries, you can direct them to the following resource where they can be obtained and installed for free:

See <http://www.openssl.org/related/binaries.html> for details. (You can also advise users to compile their own version by directing them to the source at <http://www.openssl.org/source/>.) The required version is libssl.so.0.9.6b.

**Related Documentation**

- [Task Summary: Configuring VPN Tunneling on page 737](#)

## Client Side Logging

VPN tunneling client-side logs are files that reside on the remote client containing sign-in, debug, and other statistical information you can use to troubleshoot potential issues with VPN tunneling. When you enable client-side logging for VPN tunneling users, the client records VPN tunneling events in a series of log files, continually appending entries each time a feature is invoked during subsequent user sessions. The resulting log files are useful when working with the support team to debug problems with VPN tunneling.

If VPN tunneling users turn client-side logging off, (even if logging is enabled on the Secure Access Service) the client does not record any new client-side log information. If the user turns on the logging function and the Secure Access Service is then configured to disable client-side logging, the client does not record any new client-side log information.

- Related Documentation**
- [Task Summary: Configuring VPN Tunneling on page 737](#)
  - [About Client-Side Logs on page 948](#)

## VPN Tunneling Proxy Support

VPN tunneling provides support for remote clients using a proxy server to access the Internet (and the Secure Access Service via the Internet), as well as clients who do not need a proxy to access the Internet, but who access resources on an internal network through a proxy. VPN tunneling also provides support for clients accessing a Proxy Automatic Configuration (PAC) file that specifies client and Secure Access Service proxy settings enabling access to Web applications.



**NOTE:** The VPN tunneling client does not support the use of the MS Winsock proxy client. Please disable the MS Winsock proxy client before running the VPN tunneling client. For more information, see <http://www.microsoft.com/windowsxp/using/mobility/expert/vpns.msp>.

To address these varying methods of proxy implementation, VPN tunneling temporarily changes the proxy settings of the browser so that only traffic intended for the VPN tunneling session uses the temporary proxy settings. All traffic not intended for the VPN tunneling session uses the existing proxy settings.



**NOTE:** The VPN tunneling client does not support the option to automatically detect proxy settings. You must choose to use either an automatic configuration script (PAC) or specify a proxy server. You cannot use both a proxy server and an automatic configuration script, together. You can define one or the other under the Proxy section in Users > Resource Policies > VPN Tunneling > Connection Profiles > *Profile*.

Whether split-tunneling is enabled or disabled, the Secure Access Service supports the following proxy scenarios:

- Using an explicit proxy to access the Secure Access Service
- Using an explicit proxy to access internal Web applications
- Using a PAC file to access the Secure Access Service
- Using a PAC file to access internal Web applications

Please note the following exceptions:

- Secure Access Service does not support redirect downloads and therefore does not support the redirecting of the internal PAC file download.
- The Secure Access Service's dsinet client does not support SSL; you can not obtain the internal PAC file from the SSL server.
- Secure Access Service does not support "auto detect proxy". If both static proxy and "auto proxy script (pac)" are defined, Secure Access Service uses the static proxy configuration.
- The VPN tunneling profile does not have a static proxy exception field for internal proxy. If you require proxy exceptions, you can use a PAC file with proxy exception logic.
- The VPN tunneling client supports "auto proxy script (pac)" only when the configuration is the PAC file URL. If the URL is a redirect URL or IE proxy configuration script it is not supported.

When split-tunneling is enabled on the Secure Access Service, VPN tunneling manages proxy settings in one of the following ways, depending on the method with which the proxy is implemented:

- For remote clients using a proxy server to access the Internet, all HTTP requests generated by the browser and intended for the Secure Access Service go through either an explicit proxy or a PAC file accessed by the remote client. Because the presence of an explicit proxy or access to a PAC file is already provisioned on the client-side, the client sets up the local, temporary proxy before attempting to establish a VPN tunnel.
- For remote clients using a proxy server to access the Internet, all HTTP requests generated by the browser and intended for the Secure Access Service go through either an explicit proxy or a PAC file accessed by the remote client. Because the presence of an explicit proxy or access to a PAC file is already provisioned on the client-side, the client sets up the local, temporary proxy before attempting to establish a VPN tunnel.
- When a remote client accesses a pre-configured HTTP-based PAC file, the client cannot access the PAC file until after a VPN tunnel is established. After a connection is established, the client accesses the PAC file, includes the PAC file contents in the local temporary proxy, and then refreshes the browser proxy setting.

**Related  
Documentation**

- [Task Summary: Configuring VPN Tunneling on page 737](#)

---

## VPN Tunneling Quality of Service

---

To support Quality of Service (QoS) on your internal network via VPN tunneling, Secure Access Service translates the "inner" IP packet header (for Application-layer packet encapsulation, for example) to the "outer" packet header, thus enabling Network layer-level packet prioritization. Routers in the network are then able to identify, prioritize, and appropriately forward VPN tunneling IPsec packets across the network. This feature helps ensure that you are able to support time-sensitive IP packet transmission and reception like IP video streams, for example.



**NOTE:** VPN tunneling QoS applies to UDP (IPsec) packets only. SSL packet encapsulation and forwarding behavior remains unchanged when you employ the QoS feature.

**Related Documentation**

- [Task Summary: Configuring VPN Tunneling on page 737](#)

## VPN Tunneling Multicast Support

To enable streaming IP video broadcasts over the internal network, VPN tunneling features Internet Group Management Protocol (IGMP) gateway multicast proxy support.



**NOTE:** If you are using VPN tunneling multicast support, and you are using L2 switches, make sure the switches support IGMP v3.

When users initiate a request to join a multicast group, Secure Access Service initiates an IGMP join message to the local multicast router or switch on the client's behalf. In addition, Secure Access Service stores the IGMP group request queries in its cache so that whenever a multicast router in the network polls Secure Access Service for IGMP group information, Secure Access Service responds with its current collection of multicast user and group requests. If a router or switch does not receive a response from Secure Access Service, the multicast group information for Secure Access Service is removed from the router or switch's forwarding table.



**NOTE:** VPN tunneling supports streaming media at up to 2 mbps on a single tunnel (megabits per second).

**Related Documentation**

- [Task Summary: Configuring VPN Tunneling on page 737](#)

## Defining VPN Tunneling Role Settings

Use role-level settings to specify split-tunneling, auto-launch, auto-uninstall, and Graphical Identification and Authentication (GINA) options.

To specify VPN tunneling split-tunneling, auto-launch, auto-uninstall, and GINA installation options:

1. In the admin console, choose **Users > User Roles > Role Name > VPN Tunneling**.
2. Under General VPN Options, select one of the following options:
  - **Enable Split Tunneling**—This option activates split-tunneling and requires you to specify the network IP address/netmask combinations for which Secure Access Service handles traffic passed between the remote client and the corporate intranet. With split tunneling enabled, traffic meant for the corporate intranet uses the virtual

adapter created by the tunnel and all other traffic goes through the local physical adapter.

- **Disable Split Tunneling**—All network traffic from the client goes through the VPN tunnel. When the session is established, predefined local subnet and host-to-host routes that might cause split-tunneling behavior are removed, and all network traffic from the client goes through the VPN tunnel. With split tunneling disabled, users cannot access local LAN resources during an active VPN session.

3. Under **Juniper client options**, select:

- **Route precedence** – You can define which routing table takes precedence
  - **Tunnel Routes**—The route table associated with the Pulse virtual adapter take precedence. Pulse overwrites the physical interface routes if there is conflict between the Pulse virtual adapter and the physical adapters. Pulse restores the original routes when the connection is ended.
  - **Endpoint Routes**—The route table associated with the endpoint's physical adapter take precedence.
- **Route Monitor** – Specify whether you want route monitoring enabled.
  - **Yes** – VPN tunneling ends the connection only if the route change affects the VPN tunnel traffic. For example, if the route metric is changed higher, it should not disconnect VPN tunneling.
  - **No** – Route tables are allowed to change on the client endpoint.
- **Enable TOS Bits Copy**—Select this option to control the client behavior in networks that employ Quality of Service (QoS) protocols. When you enable this check box, the Juniper client copies IP Type of Service (TOS) bits from the inner IP header to outer the IP Header. Note that enabling this option might require a reboot of the client endpoint when the client software is installed for the first time on Windows endpoints. Juniper clients support TOS bit copy only for IPsec transport and not for SSL transport.
- **Multitask**—Select this option if you want VPN tunneling to operate in multicast mode.
- **Auto-launch**—Select this option to activate VPN tunneling automatically when the endpoint is started.

4. Under **Options for Juniper client on Windows**, select:

- **Launch client during Windows Interactive User Logon**—When this option is enabled, the Juniper client starts when the user logs into Windows. Note that this setting is not the same as the Pulse connection settings that control machine authentication and credential provider authentication. Choose one of the following options:

**Require client to start when logging into Windows**

**Allow user to decide whether to start client when logging into Windows**

5. For Session Scripts, specify the following:



- **Windows: Session start script**—Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Junos Pulse connects with Pulse Secure Access Service. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources.
- **Windows: Session end script**—Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Junos Pulse disconnects from Pulse Secure Access Service. For example, you can specify a script that disconnects mapped network drives. If there is no start script defined, or the start script has not been run, the end script does not run.

**Options for Juniper client on Mac** apply only to Junos Pulse and Network Connect on Apple OS X endpoints:

- **Mac: Session start script**—Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Junos Pulse connects with Pulse Secure Access Service. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources.
- **Mac: Session end script**—Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Junos Pulse disconnects from Pulse Secure Access Service. For example, you can specify a script that disconnects mapped network drives. If there is no start script defined, or the start script has not been run, the end script does not run.

When VPN tunneling launches, start and end scripts are copied to the client and, upon session termination, are removed from the client. Scripts can be accessed locally or remotely via file share or other permanently-available local network resource. Macintosh clients only support running start and end script located on the local machine.



**NOTE:** The client should be a member of the same domain as the remote server to allow VPN tunneling to copy start and end scripts. If the client credentials are unknown to the server, the script copy fails, and VPN tunneling does not prompt the user to enter username and password.

Windows only supports scripts with the .bat or .cmd extension (referring to batch files, not the .cmd applications within MSDOS). To run a .vbs script, the user must have a batch file to call the .vbs script. Similarly, to run an .exe application (like C:\WINDOWS\system32\mstsc.exe), the user must have a batch file to call the .exe application.

The client makes a copy of the end script after the tunnel has been set up and stores the script in a temporary directory to ensure that, if the network connection were to fail, the end script can still be used to terminate the VPN tunnel session.

- Select the **Skip if Windows Interactive User Logon Enabled** option to bypass the specified Windows session start script.

If the client signs in to their Windows Domain via the GINA/Credential Provider automatic sign-in function, a script is executed by the Windows client. In this case, the sign-in script may be identical to the specified VPN Tunneling start script. You can use this option, therefore, as a way to avoid executing the same script twice.

6. Under Advanced Options for Network Connect, select options for legacy VPN Tunneling clients. This section is not applicable for Junos Pulse.
  - **NC Client Check** – Select this option to check the integrity of your VPN Tunneling client components prior to starting a VPN Tunneling tunnel. Selecting this option requires you to have either administrator rights on the client or Juniper Installer Service (JIS) running on the client. If the integrity check fails, error 23787 “Cannot start the VPN Tunneling service. Please re-install VPN Tunneling.” appears. This option is applicable only when you use a VPN Tunneling client. If you are using a Junos Pulse client, this option is ignored.
  - **Do not allow client proxy** – Select this option to prevent a VPN Tunneling tunnel from being created when a client proxy is present. Error 30572, “VPN Tunneling unable to connect because a client proxy is not allowed”, appears if the user tries to start a VPN Tunneling tunnel. This option is applicable only when you use a VPN Tunneling client. If you are using a Junos Pulse client, this option is ignored.
  - **Auto-Uninstall Network Connect** – Select this option to automatically remove Network Connect from the client when the user logs out of their session.
  - **Enable FIPS compliant Network Connect** – Applicable only to Network Connect on FIPS devices, this option allows administrators to control NC-FIPS-compliance on FIPS Secure Access Service devices. Deselect this option to allow VPN Tunneling to connect from unmanaged endpoints to Secure Access Service (running software version 7.2 or later) with a private CA issued certificate as the device certificate. This option is applicable to both SSL and ESP modes.



**NOTE:** This option is available only on FIPS devices.

Tunnel Type	Enable FIPS compliant Network Connect	
	Enabled	Disabled
SSL	SSL default	SSL default
	Unmanaged endpoints are not supported	Unmanaged endpoints are supported
ESP	Dishonors ESP, always ` gives SSL tunnel	ESP default, fallback to SSL
	Unmanaged endpoints are not supported	Unmanaged endpoints are supported

This option affects the following clients:

- Network Connect launched from a browser window
- Network Connect launched from a mini-browser window

- nclauncher
- GINA/credential provider

7. Click **Save Changes**.

**Related  
Documentation**

- [Task Summary: Configuring VPN Tunneling on page 737](#)
- [Defining Split Tunneling Network Policies on page 768](#)
- [Creating VPN Tunneling Connection Profiles on page 761](#)

## About VPN Tunneling Resource Policies

VPN tunneling resource policies specify a variety of session parameters you can use to determine the method of access for remote clients. You can configure the following types of resource policies on Secure Access Service and apply them to one or more user roles:

- **Access resource policies**—This policy type specifies which resources users may access when using VPN tunneling, such as Web, file, and server machines on the corporate intranet.
- **Packet logging resource policies**—This policy type allows you to compile client-side VPN tunneling packet logs on the Secure Access Service to help diagnose and resolve connection issues.
- **Connection profiles resource policies**—This policy type specifies which option (DHCP or Secure Access Service-managed IP address pool) Secure Access Service uses to assign an IP address to the client-side VPN tunneling agent. You can also use this feature to specify the transport protocol and encryption method for the VPN tunneling session.
- **Split Tunneling resource policies**—This policy type enables you to specify one or more network IP address/netmask combinations for which Secure Access Service handles traffic passed between the remote client and the corporate intranet.

A few notes about specifying resources for a VPN tunneling resource policy:

- You cannot specify a host name for a VPN tunneling resource policy. You can only specify an IP address.
- You can specify protocols (such as tcp, udp, icmp) for VPN tunneling. For all other access feature resource policies, specifying protocols is not supported.
- If the protocol is missing, all protocols are assumed. If a protocol is specified, then the delimiter “://” is required. No special characters are allowed.
- You cannot mix port lists and port ranges, such as 80, 443, 8080-8090 for VPN tunneling resource policies.
- If you specify a port, you must specify a protocol.
- If the port number is missing, the default port \* is assigned for http.

**Related  
Documentation**

- [Defining VPN Tunneling Access Control Policies on page 760](#)

- [Creating VPN Tunneling Connection Profiles on page 761](#)
- [Defining Split Tunneling Network Policies on page 768](#)
- [Specifying Resources for a Resource Policy on page 145](#)

## Defining VPN Tunneling Access Control Policies

Use the VPN Tunneling Access Control tab to write a resource policy that controls resources users can connect to when using VPN tunneling.

To write a VPN tunneling access resource policy:

1. In the admin console, choose **Users > Resource Policies > VPN Tunneling > Access Control**.
2. On the Access Control page, click **New Policy**.
3. On the New Policy page, enter:
  - A name to label this policy.
  - A description of the policy. (optional)
4. In the Resources section, specify the resources to which this policy applies.



**NOTE:** When a packet is fragmented, fragment #1 contains more information than all subsequent fragments. Fragment #1 contains the IP address, protocol, and port information. All subsequent fragmented packets contain just the IP address and protocol information. Therefore the VPN Tunneling ACL evaluates the first packet fragment different from the subsequent packet fragments. For the subsequent packet fragments, Secure Access Service applies the VPN Tunneling ACL based on just the IP address and protocol since the port number is not available.

5. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. In the Action section, specify:
  - **Allow access**—Select this option to grant access to the resources specified in the Resources list.
  - **Deny access**—Select this option to deny access to the resources specified in the Resources list.

- **Use Detailed Rules**—Select this option to define resource policy rules that put additional restrictions on the specified resources.
7. Click **Save Changes**.
  8. On the Access Policies page, order the policies according to how you want Secure Access Service to evaluate them. Keep in mind that once Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

**Related Documentation**

- [Writing a Detailed Rule for Resource Policies on page 150](#)
- [Task Summary: Configuring VPN Tunneling on page 737](#)

## Creating VPN Tunneling Connection Profiles

Use the **Users > Resource Policies > VPN Tunneling > Connection Profiles** page to create VPN tunneling connection profiles. When Secure Access Service receives a client request to start a VPN tunneling session, Secure Access Service assigns an IP address to the client-side agent. Secure Access Service assigns this IP address based on the DHCP Server or IP Address Pool policies that apply to a user's role. In addition, this feature allows you to specify the transport protocol, encryption method, and whether or not to employ data compression for the VPN tunneling session.

Nodes in a multi-site cluster share configuration information, which means that Secure Access Service devices in different networks share an IP address pool. Since any Secure Access Service node may receive the client request to start the VPN tunneling session, you need to specify an IP filter for that node that filters out only those network addresses available to that node. When the cluster node receives a request to create a VPN tunnel, it assigns the IP address for the session from the filtered IP address pool.



**NOTE:** Release 7.3 and Release 7.4 do not support IP filters for IPv6 addresses.

To write a VPN tunneling connection profile:

1. In the admin console, choose **Users > Resource Policies > VPN Tunneling > Connection Profiles**.
2. On the Connection Profiles page, click **New Profile** and configure the settings described in [Table 49 on page 762](#).
3. Save the configuration.
4. On the Connection Profiles page, order the profiles according to how you want Secure Access Service to evaluate them. Keep in mind that once Secure Access Service matches the resource requested by the user to a resource in a profile's (or a detailed rule's) Resource list, it performs the specified action and stops processing profiles.

Table 49: VPN Tunneling Connection Profile Settings

Setting	Guidelines
Name	A name to label this policy.
Description	A description of the policy (optional).
<b>IPv4 address assignment</b>	
DHCP servers	<p>Specify the host name or IP address of a network Dynamic Host Configuration Protocol (DHCP) server responsible for handling client-side IP address assignment.</p> <p>You can specify up to three DHCP servers by listing each one on a separate line. When multiple DHCP servers are listed, Secure Access Service sends a DHCP Discover message to all listed DHCP servers and then waits five seconds for a response. If multiple DHCP servers respond, Secure Access Service chooses the one with the longest lease period.</p> <p>Secure Access Service sends a DHCP release packet to the DHCP server when the VPN tunneling session ends.</p> <p>DHCP provides a framework for passing configuration information to hosts. Configuration parameters and other control information are carried in tagged data items that are stored in the options field of the DHCP message. You can specify the DHCP options to forward by entering the option number, its value and type and then clicking Add. For a complete list of DHCP options, see the "RFC2132 - DHCP Options and BOOTP Vendor Extensions" article available on the Internet. To delete an option, select the checkbox next to the option number then click the <b>Delete</b> button.</p>
DHCP options	<p>By default, the client's hostname is sent by Secure Access Service to the DHCP server in the DHCP host name option (option12.) Passing the userid in the DHCP hostname option is no longer supported. As an alternative, you can configure the following entry in the DHCP options table. For example:</p> <p style="padding-left: 40px;"><b>option number=12, option value=&lt;username&gt;&lt;authMethod&gt;, option type=String</b></p> <p>Or you can pass a value by adding an entry in the DHCP options table for hostname with whatever value you want. For example:</p> <p style="padding-left: 40px;"><b>option number=12, option value=foo, option type=String</b></p>

Table 49: VPN Tunneling Connection Profile Settings (*continued*)

Setting	Guidelines
IPv4 address pool	<p>Specify IP addresses or a range of IP addresses for Secure Access Service to assign to clients that run the VPN tunneling service. Use the canonical format: <code>ip_range</code>.</p> <p>The last component of the IP address is a range delimited by a hyphen (-). No special characters are allowed. The <code>ip_range</code> can be specified as shown in the following list:</p> <ul style="list-style-type: none"> <li>• <code>a.b.c.d</code> — Specifies a single IP address.</li> <li>• <code>a.b.c.d-e.f.g.h</code> — Specifies all IP addresses from the first address to the last address, inclusive.</li> <li>• <code>a.b.c.d-f.g.h</code> — An abbreviated form that specifies the range <code>a.b.c.d</code> through <code>a.f.g.h</code></li> <li>• <code>a.b.c.d-g.h</code> — An abbreviated form that specifies the range <code>a.b.c.d</code> through <code>a.b.g.h</code>.</li> <li>• <code>a.b.c.d-h</code> — An abbreviated form that specifies the range <code>a.b.c.d</code> through <code>a.b.c.h</code>.</li> <li>• <code>a.b.c.d/mask</code> — Specifies all addresses in a network.</li> </ul> <p>For example, to allocate all addresses in the range <code>172.20.0.0</code> through <code>172.20.3.255</code>, specify <code>172.20.0.0-3.255</code>. Or, to allocate all addresses in a class C network, specify <code>10.20.30.0/24</code>.</p> <p><b>NOTE:</b> Be sure to specify a sufficient number of addresses in the IP address pool for all of the endpoints in your deployment. When all of the addresses in the pool have been assigned to endpoints, additional endpoints are unable to obtain a virtual IP address and are blocked from accessing protected resources. Secure Access Service logs a message in the Event log when an IP address cannot be assigned to an endpoint.</p> <p>We recommend that you set up your network so that the client-side IP address pool, or the DHCP server specified in the VPN tunneling connection profile, resides on the same subnet as Secure Access Service.</p> <p>If your network topology dictates that Secure Access Service internal IP interface and the IP address pool or DHCP server reside on different subnets, you need to add static routes to your intranet's gateway router(s) to ensure that your Enterprise resources and Secure Access Service can see each other on the internal network.</p> <p>If you are running a multi-unit cluster across a LAN, make sure that the IP address pool contains addresses that are valid for each node in the cluster. Then, configure an IP filter for each node to apply to this IP address pool.</p> <p>Secure Access Service does not support a common IP address pool for VPN tunneling for an Active/Active cluster. In A/A VPN tunneling deployments, we recommend that you split the IP pool into node-specific subpools. Furthermore, you are advised to perform static route configuration on the backend router infrastructure in a coordinated fashion, with static routes to each subpool pointing to the internal IP address of the hosting cluster node as the next-hop gateway.</p> <p>IP address pool also supports attribute substitution. For example, you can enter a RADIUS role mapping attribute in this field, such as <code>&lt;userAttr.Framed-IP-Address&gt;</code>.</p>
<b>IPv6 address assignment</b>	
Enable IPv6 address assignment to clients	<p>Select this option to enable IPv6 connections. Release 7.4 does not support assignment by a DHCPv6 server. You must configure a static IPv6 address pool.</p> <p><b>NOTE:</b> IPv6 must be enabled on internal interface for IPv6 addresses to be allocated to clients.</p>
IPv6 address pool	<p>Specify IPv6 address ranges for this profile, one per line. Like the IPv4 address pool, the configuration supports entering <code>ip_range</code> values. We recommend using the IPv6 network prefix / netmask style (such as <code>2001:DB8::6:0/112</code>).</p>

Table 49: VPN Tunneling Connection Profile Settings (*continued*)

Setting	Guidelines
<b>Connection settings</b>	
Transport	<p>Select one of the following options for transport, encryption, and compression settings:</p> <ul style="list-style-type: none"><li>• <b>ESP</b>—Use a UDP encapsulated ESP transfer method to securely transfer data between the client and Secure Access Service. ESP uses an LZO compression algorithm. You can use the default settings or configure data transfer parameters by defining the UDP port, ESP-to-SSL fallback time-out value, and ESP encryption key lifetime values.</li><li>• <b>SSL</b>—Use the standard SSL transport method. SSL uses a deflate compression method. In SSL mode, compression is controlled by the Enable GZIP compression option on the System Maintenance Options page. Gzip compression is not supported on the MAG Series Junos Pulse Gateways.</li></ul> <p><b>NOTE:</b> To support IPv6 connections, be sure to set MTU greater than 1380. We recommend 1500. If the MTU value on the external interface is lower than 1380 and IPv6 address assignment is enabled, the transport setting for the connection profile is ignored. To avoid IP fragmentation, the session falls back to SSL mode for both IPv6 and IPv4 traffic.</p>



Table 49: VPN Tunneling Connection Profile Settings (*continued*)

Setting	Guidelines
	<p>If you select ESP mode, configure the following transport and compression settings:</p> <ul style="list-style-type: none"> <li>• <b>UDP port</b>—Port through which you intend to direct UDP connection traffic. The default port number is 4500.</li> </ul> <p><b>NOTE:</b> Whether you specify a custom port number or choose to use the default port number (4500), you must also ensure that other devices along the encrypted tunnel allow UDP traffic to pass between Secure Access Service and the clients. For example, if you employ an edge router and a firewall between the Internet and your corporate intranet, you must ensure that port 4500 is enabled on both the router and the firewall and that port 4500 is configured to pass UDP traffic.</p> <p>IKEv2 uses port 500 exclusively. Do not configure port 500 in your VPN Tunneling profiles.</p> <ul style="list-style-type: none"> <li>• <b>ESP to SSL fallback timeout</b>—Period of time (in seconds) to fall back to the SSL connection already established following UDP connection failure. The default is 15 seconds.</li> </ul> <p><b>NOTE:</b> A nonconfigurable idle timeout of 60 seconds also affects when fallback occurs. After the tunnel is established through ESP, the client sends keep alives after 60 seconds of inactivity on the ESP channel (the idle timeout). The total time to fallback is therefore the idle timeout (60 seconds) plus the fallback timeout. For example, if ESP to SSL fallback timeout is set to 25 seconds, it takes approximately 60+25 or 85 seconds for the VPN tunneling client to switch.</p> <ul style="list-style-type: none"> <li>• <b>Key lifetime (time based)</b>—Period of time (in minutes) the system continues to employ the same ESP encryption key for this connection profile. Both the local and remote sides of the encrypted transmission tunnel use the same encryption key only for a limited period of time to help prevent unauthorized access. The default is 20 minutes.</li> <li>• <b>Key lifetime (bytes transferred)</b>—Maximum amount of data that is transferred on the tunnel for an ESP encryption key. The default is 0 bytes, meaning no limit.</li> </ul> <p><b>NOTE:</b> When either of the key lifetime limits is reached, a new key is exchanged between Secure Access Service and the client. The reason for changing keys is to help prevent unauthorized access, however, changing the encryption key too frequently can increase CPU overhead on Secure Access Service.</p> <ul style="list-style-type: none"> <li>• <b>Replay Protection</b>—Activates replay protection. When enabled, this option protects against hostile “repeat attacks” from the network. When packets arrive from the client, Secure Access Service checks the IP header information to verify that a packet featuring the same IP header information has not already been received. If one has been received, the packet is rejected. This option is enabled by default.</li> </ul> <p>If you activate the Enable TOS Bits Copy option, IP packets with different TOS bits may be reordered when passing through gateway routers on your network. To ensure that any packets received out of order are not automatically dropped when they reach Secure Access Service, you can disable the Replay Protection option.</p> <p><b>NOTE:</b> We recommend that you leave replay protection enabled if you are not expecting more than one source of packets from the client (for example, if only one application is transmitting and receiving traffic over the VPN tunnel).</p> <ul style="list-style-type: none"> <li>• <b>Compression</b>—Use compression for the secure connection. Compression is useful for a slow link but may cause issues in extremely large deployments since extra cycles are spent compressing the data.</li> </ul>

Table 49: VPN Tunneling Connection Profile Settings (*continued*)

Setting	Guidelines
	<p>If you have selected ESP, select one the following encryption settings:</p> <ul style="list-style-type: none"> <li>• <b>AES128/MD5 (maximize performance)</b>—Uses Advanced Encryption Standard (AES) 128-bit encryption on the data channel and the MD5 authentication method for VPN tunneling sessions.</li> <li>• <b>AES128/SHA1</b>—Uses AES 128-bit encryption on the data channel and the SHA1 authentication method during VPN tunneling sessions.</li> <li>• <b>AES256/MD5</b>—Uses AES 256-bit encryption on the data channel and the MD5 authentication method for VPN tunneling sessions.</li> <li>• <b>AES256/SHA1 (maximize security)</b>—Uses AES 256-bit encryption on the data channel and the SHA1 authentication method during VPN tunneling sessions.</li> </ul> <p><b>NOTE:</b> The MD5 authentication algorithm creates digital signatures. The MD5 authentication method translates an input string (like a user's ID or sign-in password, for example) into a fixed, 128-bit fingerprint (also called a "message digest") before it is transmitted to or from Secure Access Service. The SHA1 authentication method is easy to use and efficient when encoding user ID and password information.</p> <p>The SHA1 algorithm translates the characters comprising a user ID or password string into unreadable text before it is transmitted to or from Secure Access Service. The same algorithm is then used to reverse the translation before it is presented to the authentication server.</p>
<b>DNS settings</b>	
IVE DNS Settings	<p>In the DNS Settings section, select an option that determines the settings sent to the client:</p> <ul style="list-style-type: none"> <li>• <b>IVE DNS Settings</b>—Send the Secure Access Service DNS settings.</li> <li>• <b>Manual DNS Settings</b>—Override standard DNS settings with the settings you provide: <ul style="list-style-type: none"> <li>• <b>Primary DNS</b>—Enter the IP address for the primary DNS.</li> <li>• <b>Secondary DNS</b>—Enter the IP address for the secondary DNS.</li> <li>• <b>DNS Domain(s)</b>—Enter the DNS domain(s), such as "yourcompany.com, yourcompany.net".</li> <li>• <b>WINS</b>—Enter the WINS resolution name or IP address.</li> </ul> </li> <li>• <b>DHCP DNS Settings</b>—Send the values the DHCP server sends to Secure Access Service. There is no fallback to the DNS settings if the DHCP Server does not send any values.</li> </ul>
Auto-allow	<p>Select <b>Auto-allow IP's in DNS/WINS settings (only for split-tunnel enabled mode)</b> if you want to create an allow rule for the DNS server, For example, if you have defined policies to allow requests from IP address 10.0.0.0 but your DNS server has an address of 172.125.125.125 the DNS server requests will be dropped. If you select this option, Secure Access Service creates a rule to allow the DNS requests.</p>

Table 49: VPN Tunneling Connection Profile Settings (*continued*)

Setting	Guidelines
DNS search order	<p>Select the DNS server search order. Applicable only if split tunneling is enabled:</p> <ul style="list-style-type: none"> <li>• Search client DNS first, then the device</li> <li>• Search the device's DNS servers first, then the client</li> <li>• Search device DNS only.</li> </ul> <p><b>NOTE:</b> Junos Pulse clients do not support the <b>Search device DNS only</b> option.</p> <p>For the <b>Search client DNS first, then the device</b> and <b>Search the device's DNS servers first, then the client</b> options, DNS configured on the Secure Access Service are added to the end user's system along with the existing DNS already available on the end user's system. So either the device (Secure Access Service) DNS servers or client DNS servers get precedence at the end user's systems.</p> <p>When the <b>Search device DNS only</b> option is selected, DNS on the end user's system are replaced with device DNS. This option is recommended to avoid ISP's DNS hijacking. Note that this option is applicable only for Windows platforms; non-Windows clients will use the <b>Search the device's DNS servers first, then the client</b> search order if this option is selected. When using this option, you must ensure that packets to the Secure Access Service DNS are going through the tunnel. To do this, add the required routes to the split tunnel networks policy (Users &gt; Resource Policies &gt; VPN Tunneling &gt; Split-Tunneling Networks), or select the <b>Auto-allow IPs in DNS/WINS settings</b> option.</p> <p>For the <b>Search device DNS only</b> option, Network Connect removes the DNS information of the available adapters on the client system after the tunnel is created. Once the tunnel is created, Network Connect does not monitor the presence of new adapters and does not monitor if changes are made to the DNS of existing adapters. Because of this, the <b>Search device DNS only</b> option may not work properly if any of the following occurs after the tunnel is created:</p> <ul style="list-style-type: none"> <li>• A new interface appears with a DNS server that does DNS hijacking.</li> <li>• A third-party application adds DNS to the adapters whose DNS was removed by Network Connect as part of the tunnel set up process.</li> <li>• Third-party applications change the TCP/IP option from "Use the following DNS servers" to "Obtain DNS servers automatically" for those adapters whose DNS was removed by Network Connect as part of the tunnel set up process.</li> <li>• End users enable the interfaces that are in the disabled state during the tunnel set up process.</li> </ul>
<b>Proxy Server Settings</b>	

Table 49: VPN Tunneling Connection Profile Settings (*continued*)

Setting	Guidelines
Proxy server settings	<p>Select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>No proxy server</b>—Specifies that the new profile requires no proxy server.</li> <li>• <b>Automatic (URL for PAC file on another server)</b>—Specify the URL of the server on which the PAC file resides, and the frequency (in minutes) with which the client polls the server for an updated version of the PAC file. You can configure VPN tunneling to check for an updated PAC files as often as every 10 minutes. The default (and minimum) update period is 10 minutes. The PAC file should reside on a Web server, not on the local PC. The PAC file update method runs on a 10 minute interval. Specifying a frequency update period that is a multiple of 10 will get an exact result. If you specify the update frequency at a value that is not a multiple of 10, it is rounded up to the next interval. For example, if you specify the update frequency at 15 minutes, the Secure Access Service updates a PAC file every 20 minutes. <b>NOTE:</b> VPN tunneling limits the size of internal (server side) PAC files. The logical maximum size is 256 KB. The actual maximum size that can be used in your deployment might be smaller, reduced according to the size of other VPN tunneling settings in use, such as the number of split tunnel networks and DNS suffix entries.</li> <li>• <b>Manual configuration</b>—Specify the IP address or the hostname of the server and provide the port assignment.</li> <li>• <b>Preserve client-side proxy settings</b>—By default, VPN tunneling may change proxy settings when needed. For example, VPN tunneling may temporarily change the proxy settings of the browser so that traffic intended for the VPN session uses the temporary proxy settings. Select the Preserve client-side proxy settings option to prevent the client-side proxy settings from being overridden by VPN tunneling. If you select this option, HTTP and FTP traffic path can change after VPN tunneling establishing the connection. Please analyze the proxy logic and split-tunnel option, and make sure it directs the traffic as intended.</li> </ul>
Roles	<p>Specify one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Policy applies to ALL roles</b>—To apply this policy to all users.</li> <li>• <b>Policy applies to SELECTED roles</b>—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.</li> <li>• <b>Policy applies to all roles OTHER THAN those selected below</b>—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.</li> </ul>
<p><b>Related Documentation</b></p>	<ul style="list-style-type: none"> <li>• <a href="#">Configuring VPN Tunneling for Use on a Virtualized Secure Access Service on page 1043</a></li> <li>• <a href="#">Task Summary: Configuring VPN Tunneling on page 737</a></li> </ul>

## Defining Split Tunneling Network Policies

Use the Split Tunneling Network tab to write a VPN tunneling resource policy that specifies one or more network IP address/netmask combinations for which Secure Access Service handles traffic passed between the remote client and the corporate intranet. You can also specify traffic that should not pass through the VPN tunnel.

When split-tunneling is used, VPN tunneling modifies routes on clients so that traffic meant for the corporate intranet networks flow through the tunnel and all other traffic

goes through the local physical adapter. Secure Access Service tries to resolve all DNS requests through the physical adapter first and then routes those that fail to the VPN tunneling adapter.

For example:

- If split tunnel is disabled, all split tunnel configuration is ignored, including the exclude route.
- Split tunneling is enabled and the included route contains 10.204.64.0/18 and the exclude traffic contains 10.204.68.0/24. In this scenario, networks from 10.204.64.0/18 to 10.204.127.0/18 will pass through the VPN tunnel with the exception of the 10.204.68.0/24 network, which will not pass through the VPN tunnel.
- If split tunneling is enabled and the include route contains 10.204.64.0/24 (subnet of the excluded route) and the exclude route contains 10.204.64.0/18 (super set of the included route) then the included network's traffic will still be routed through the VPN tunnel.



**NOTE:** If split tunneling is enabled and there are no include routes configured to be sent to the client, VPN tunneling adds a default route to send traffic through the tunnel.

To write a split-tunneling networks resource policy:

1. In the admin console, choose **Users > Resource Policies > VPN Tunneling > Split-tunneling Networks**.
2. On the Connect Split Tunneling page, click **New Policy**.
3. On the New Policy page, enter:
  - A name to label this policy.
  - A description of the policy (optional).
4. In the Resources section, specify one or more network IP address/netmask combinations for which Secure Access Service handles traffic passed between the remote client and the corporate intranet. You may also use the '/' (slash) notation to specify these networks.
5. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. In the Action section:

- **Allow access**—Network IP address/netmask combinations specified in the Resources list pass through the VPN tunnel.
- **Exclude access**—Network IP address/netmask combinations specified in the Resources list do not pass through the VPN tunnel.
- **Use Detailed Rules** (available after you click ‘Save Changes’)—Select this option to define resource policy rules that put additional restrictions on the specified resources.



NOTE: Junos Pulse 1.0 does not support the Exclude access option.

7. Click **Save Changes**.
8. On the Split Tunneling Policies page, order the policies according to how you want Secure Access Service to evaluate them. Keep in mind that once Secure Access Service matches the resource requested by the user to a resource in a policy's (or a detailed rule's) Resource list, it performs the specified action and stops processing policies.

**Related  
Documentation**

- [Task Summary: Configuring VPN Tunneling on page 737](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)

## VPN Tunneling Resource Policy Configuration Use Case

This topic describes a real-world VPN tunneling application and the steps necessary to configure the appropriate resource policy providing access to remote users on the network.

Large financial institutions (also called “Fortune Companies”) require a robust client sign-in application like VPN tunneling to help provide remote employees seamless network connection to a large range of enterprise resources at the corporate headquarters. Often, remote users need to be able to access multiple applications on their laptops/client machines beyond simple Email or meeting scheduling applications. These remote “super users” or “power users” require secure, encrypted access to powerful server applications like Microsoft Outlook™, Oracle™ databases, and the Remedy™ case management system.

For this scenario, let's assume the following:

- There is a small collection of remote users who will all access their financial institution's enterprise resources via the same Secure Access Service.
- All the users have the same “user\_role\_remote” role assigned to their user ID
- Host Checker and Cache Cleaner are configured and verifying the users' machines upon logging into Secure Access Service and launching their VPN tunneling sessions
- All users require access to three large servers at the corporate headquarters with the following attributes:
  - “outlook.acme.com” at IP address 10.2.3.201

- “oracle.financial.acme.com” at IP address 10.2.3.202
- “case.remedy.acme.com” at IP address 10.2.3.99
- Because the Company wants to manage their IP address pool very strictly, each Secure Access Service provides IP addresses to remote users (our particular Secure Access Service controls the IP addresses between 10.2.3.128 and 10.2.3.192)
- The company is interested in the most secure access possible, simultaneously accepting only the least possible amount of client down-time

To configure a VPN tunneling resource policy providing appropriate access to the Fortune Company remote users:

1. Create a new VPN tunneling resource policy where you specify the three servers to which you want to grant remote users access:
  - a. In the Resources section, specify the IP address ranges necessary to allow access to the three servers (“outlook.acme.com,” “oracle.financial.acme.com,” and “case.remedy.acme.com”) separated by carriage returns.

```
udp://10.2.3.64-127:80,443
udp://10.2.3.192-255:80,443
```



**NOTE:** Configuring your resource as 10.1.1.1-128:\* is not supported. Doing so will result in an error.

- b. In the Roles section, select the **Policy applies to SELECTED roles** option and ensure that only the “user\_role\_remote” role appears in the Selected roles list.
  - c. In the Action section, select the **Allow access** option.
2. Create a new VPN tunneling connection profile where you define the transport and encryption method for the data tunnel between the client(s) and Secure Access Service:
    - a. In the IP address assignment section, select the **IP address pool** option and enter 10.2.3.128-192 in the associated text field.
    - b. In the Connection Settings section, select the **ESP transport** option and the AES/SHA1 encryption option.
    - c. In the Roles section, select the **Policy applies to SELECTED roles** option and ensure that only the “user\_role\_remote” role appears in the Selected roles list.

**Related Documentation**

- [Task Summary: Configuring VPN Tunneling on page 737](#)
- [VPN Tunneling Execution on page 739](#)

## About VPN Tunneling Bandwidth Management Policies

Bandwidth management controls the rate of traffic sent or received on a network interface. Bandwidth management discards excess packets and ensures that a user is allocated a specified amount of bandwidth. Traffic less than or equal to the specified rate is guaranteed to be sent. Traffic exceeding the rate is either dropped or delayed.

The total guaranteed bandwidth and spare bandwidth amounts are tracked and updated as users log in and out. Spare bandwidth is defined as the administrator-configured maximum minus the total guaranteed bandwidth for logged-in users.

Guaranteed bandwidth and maximum bandwidths are defined at the role level. This limit applies to each user in the role and ensures that each user receives at least the guaranteed amount of bandwidth but no more than the configured maximum amount. When users are mapped to multiple roles, the higher limit is used. If you do not define a guaranteed bandwidth to a role, users in that role can still log in, but they are not guaranteed any bandwidth. That is, their guaranteed bandwidth is set to zero.

Bandwidth management also applies to IVS. The administrator configures the total guaranteed bandwidth for each IVS and configures the limits for roles within each IVS. The sum of the total guaranteed bandwidths for every IVS must be less than or equal to the maximum bandwidth of the appliance. The sum of all VPN tunneling maximum bandwidths of all IVSs must be less than or equal to the VPN tunneling maximum bandwidth. Be sure to set the bandwidth for both Secure Access Service (System > Network > Overview) and the IVS (System > Virtual Systems > root).



**NOTE:** If you use the same VLAN across multiple IVS systems, Bandwidth Management is not supported.

To ensure Secure Access Service does not allow more bandwidth than the total available, the ability to start VPN tunnels is restricted. Users can start a VPN tunnel only if the guaranteed bandwidth for their role is available. Once users start a session, they are never dropped due to bandwidth restrictions. A privilege level controls this restriction as shown in the following table.

**Table 50: Privilege Levels and Percent of Maximum Bandwidth**

Privilege Level	Percent of Maximum Bandwidth
Low	Limited to 50%
Medium	Limited to 75%
High	Limited to 90%
Maximum	Limited to 100%



For example, users assigned to a low privilege level are able to launch a VPN tunnel if the total current bandwidth usage is less than 50% of the configured Maximum Bandwidth. Users assigned to the maximum privilege level are able to launch a VPN tunnel at any time as long as there is any Secure Access Service bandwidth available.

When a user attempts to launch a VPN connection, the sum of the Guaranteed Minimum Bandwidth of all open VPN connections is divided by the configured Total Bandwidth. If the resulting value is less than the configured privilege level of this user, then the user's VPN connection is established. Otherwise, the connection request is denied. For example, if the user's privilege is 75% and the calculated current consumption is 70%, the user's VPN connection is established. If the calculated current consumption is 80%, the user's connection request is denied and the user receives a 23791 error code.



**NOTE:** We recommend that average employees be given Low or Medium privilege levels. Higher privilege employees can be assigned the Maximum privilege level to ensure intranet access as long as there is bandwidth available.

If a user does not have the bandwidth to set up any VPN tunnels, the user can still log in but is restricted in what they can do. For example, they may only be able to access web e-mail, etc.

A guaranteed minimum bandwidth is the bandwidth a user gets once a VPN connection is established. If the remaining VPN bandwidth is smaller than the guaranteed minimum bandwidth, the user's VPN connection request is denied and the user receives an 23791 error code. The Guaranteed Minimum Bandwidth must be smaller than the Maximum Bandwidth.

Maximum bandwidth is the bandwidth a user can use through the VPN connection. This is a limit on how much the user can use if there is bandwidth available. For example, if the user's maximum bandwidth is 100 kbps, the user can not use more than 100 kbps regardless how much available bandwidth.

Statistics for bandwidth management are recorded in the system snapshots.



**NOTE:** Before using VPN tunneling bandwidth management policies, you must specify the maximum bandwidth and VPN maximum bandwidth values for the appliance.

## User is Mapped to Multiple Roles

The following decision process is made when a user is mapped to multiple roles:

- Calculate the Bandwidth management policies based on the privilege level defined.
  - The current used bandwidth percentage is calculated and compared with the privilege levels of the Bandwidth management policy of the mapped roles.

- All bandwidth management policies with the privilege levels that disallow the user to set up VPN tunnels are discarded.
- Compare the matched bandwidth management policies and choose the one with the highest guaranteed minimum bandwidth. If more than one policy with the highest guaranteed minimum bandwidth exists, the policy with the highest maximum bandwidth wins.

For example, a user is mapped to 3 roles and the bandwidth management policy for each role is as follows:

	Role 1	Role 2	Role 3
Minimum guaranteed bandwidth	100 mbps	200 mbps	100 mbps
Maximum guaranteed bandwidth	500 mbps	400 mbps	400 mbps
Privilege level	Medium	High	Maximum

If the current total used bandwidth is at 80%:

- Since role 1's privilege is not enough to allow this user to set up a VPN tunnel, role1's bandwidth management policy is ignored.
- Role 2's policy has higher minimum guaranteed bandwidth than role 3 so role 2 wins. The user receives a 200mbps minimum guaranteed bandwidth and 400mbps maximum guaranteed bandwidth.

However, if the current total used bandwidth is 92%, only role3's privilege allows the user to set up NC tunnel, so role3's bandwidth management policy is used. Thus the user has a 100mbps minimum guaranteed bandwidth and 400mbps maximum guaranteed bandwidth.

## Limitations

Bandwidth management may not operate correctly under the following conditions:

- More than one IVS uses the same Secure Access Service internal port.
- More than one IVS has the same VLAN IP.
- Overlapping VPN tunneling IPs across IVSs.

### Related Documentation

- [Task Summary: Configuring VPN Tunneling on page 737](#)
- [VPN Tunneling Execution on page 739](#)
- [General Network Settings on page 790](#)

## Writing a VPN Tunneling Bandwidth Management Resource Policy

To write a VPN tunneling bandwidth management resource policy:

1. In the admin console, choose **Users > Resource Policies > VPN Tunneling > Bandwidth Management**.
2. On the Bandwidth Management page, click **New Policy**.
3. On the New Policy page, enter:
  - A name to label this policy.
  - A description of the policy (optional).
4. In the Bandwidth Management Settings section, specify:
  - **Admission Privilege Level**—Select the percentage of the maximum bandwidth that allows users to start a VPN session. Only when the bandwidth is below this percentage can users log in.
  - **Guaranteed Minimum Bandwidth**—Specify the user's minimum bandwidth once they start a VPN session.
  - **Maximum Bandwidth**—Specify the user's maximum bandwidth once they start a VPN session.



**NOTE:** The maximum bandwidth must be less than or equal to the maximum rated value for the appliance.

5. In the Roles section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
6. Click **Save Changes**.

### Related Documentation

- [Task Summary: Configuring VPN Tunneling on page 737](#)
- [VPN Tunneling Execution on page 739](#)
- [General Network Settings on page 790](#)

## Configuring the VPN Tunnel Server

You use the **System > Network > VPN tunneling** page to configure VPN tunnel server options. This topic includes the following information:

- [Specifying IP Filters on page 776](#)
- [Specifying the VPN Tunneling Server Base IP Address on page 776](#)

### Specifying IP Filters

The VPN Tunneling Server uses the filter list to assign IP addresses to clients requesting a VPN client session. A filter is an IP address/netmask combination. For example: 10.11.0.0/255.255.0.0 or 10.11.0.0/16.

To add an IP address to the VPN tunneling filter list:

1. In the admin console, choose **System > Network > VPN tunneling**.
2. Specify an IP address/netmask combination and then click **Add**.

### Specifying the VPN Tunneling Server Base IP Address



**NOTE:** Only change the VPN tunneling server base IP address when instructed to do so by the Juniper Networks Support team.

To change the VPN tunneling server base IP address:

1. In the admin console, choose **System > Network > VPN tunneling**.
2. In the **VPN Tunnel Server IP Address** text box, specify the base IP address used by the VPN tunneling server to assign IP addresses to the IVE tunnel interfaces created for VPN Tunneling sessions. If your service is deployed in a cluster, the base IP address you specify will be common to all cluster nodes. Be sure to configure a base IP address that does not encroach on the IP address pool for VPN Tunneling Connection Profiles or for the IP addresses for the IVE external or internal interface. Take DHCP servers into consideration.

For IPv6 addresses, no additional configuration is required. The base IPv6 address used by the VPN tunneling server will be generated by prepending the network prefix "fd00::" to IPv4 address configured for this.

3. Save the configuration.

#### Related Documentation

- [About VPN Tunneling on page 734](#)
- [VPN Tunneling Connection Profiles with Support for Multiple DNS Settings on page 751](#)

---

## VPN Tunneling Installer Overview

---

To download the VPN tunneling application as a Windows executable file, go to Maintenance > System > Installers.

### VPN tunneling Installation Process Dependencies

During installation, VPN tunneling interacts with a number of system components, performing checks and validations along the way. The following list provides the order of execution during installation, which may be helpful if you need to debug a VPN tunneling installation process.

1. Start Pre-Installation Process:
  - a. Parse command line arguments.
  - b. Set appropriate variables via command line.
  - c. Process commands, as necessary.
  - d. If the command line entry responds with help or version information, the VPN tunneling installation program quits, following the command line processing. Typically occurs when you run the VPN tunneling installer as a standalone installer.
2. Validate System:
  - a. Check OS. VPN tunneling support for Windows 98, Windows 2K, and Windows XP only. If OS is 95, ME or NT 4.0, display error and abort validation process.
  - b. Check Administrator privileges.
  - c. 3rd-party GINA component – if GINA is to be registered, check whether there is any existing registered GINA component. If yes, abort installation.
3. If there is an existing VPN tunneling installation, trigger the uninstall in upgrade mode of the existing VPN tunneling.
4. Wait until the existing VPN tunneling un-installation process completes (in upgrade mode).
5. If the un-installation process times-out, display error message and abort the VPN tunneling installation, otherwise, continue the VPN tunneling installation.
6. Write logging registry keys for VPN tunneling components.
7. Start VPN tunneling installation.
8. Shared component installation:
  - a. Check sharedDll registry value of the shared components to see if this is the first instance of shared component installation.
  - b. Check if Neo\_CleanInst flag is set.
  - c. If steps a or b are true, ensure the sharedDll registry value is clean.

- d. Stop service if still running.
  - e. Check installation and driver
    - If driver is installed and it is a clean installation, uninstall the driver.
    - If driver is installed and it is not a clean installation, compare driver versions.
    - If it is an upgrade, set the driver install flag, otherwise, do not install the driver (keep the current higher version driver).
9. VPN tunneling component installation:
- a. If the driver install flag is set or if it is a clean install, install the driver.
  - b. Call the shared component installation macro for the VPN tunneling service and GINA component. This macro performs a version comparison, ensures a proper upgrade, and increments the sharedDll registry key value.
  - c. Copy other VPN tunneling binary files.
  - d. Call the NCCopyFile macro for the files that might be locked by msGINA. This macro takes care of renaming old files and mark them delete on reboot.
  - e. Register GINA if GINA flag is set.
10. Save locale and GINA settings in user's config.ini file.
11. Start the NCSERVICE.
12. Create program shortcut.
13. Create Uninstall registry keys.
14. Start VPN tunneling user interface.
15. End VPN tunneling installation process.
16. Start Post-Installation Process:
- a. Print product version and append the install log to admin log file
  - b. Reboot, if the reboot flag was set.

## VPN Tunneling Un-installation Process Dependencies

During un-installation, VPN tunneling interacts with a number of system components, performing checks and validations along the way. The following list provides the order of execution during un-installation, which may be helpful if you need to debug a VPN tunneling un-installation process.

1. Start Pre-Uninstall Process:
  - a. Parse command line inputs, including:
    - Locale
    - Clean uninstall flag
    - Upgrade flag
2. Start uninstall operation.
3. Check Administrator privileges.
4. Un-register GINA if already registered.
5. If un-installing in upgrade mode, stop the VPN tunneling service.
6. If the un-installation is not in upgrade mode, check the current sharedDll registry key value. If the value is 1, this is the only instance using the shared components, so:
  - a. Uninstall the driver.
  - b. Delete the driver file.
  - c. Stop and un-register the VPN tunneling service.
7. Call the shared components macro to uninstall shared components. This macro decrements the SharedDLL registry key value and removes the source file.



**NOTE:** If the uninstall process is in upgrade mode, this step is not executed because the uninstall is triggered from a VPN tunneling installation process and the shared component macro in the installation process will handle the shared component upgrade operations.

8. Delete other VPN tunneling files, including:
  - dsNcAdmin.dll
  - dsNcDiag.dll
  - versioninfo.ini
9. Call the NCDeleteFile macro to delete the files that may be locked by msGINA.
10. Delete VPN tunneling registry keys.
11. Remove VPN tunneling program file directories.
12. End the uninstall process.
13. Print the product version and append the VPN tunneling installation log to the Admin log.
14. Reboot, if the reboot flag was set.

**Related  
Documentation**

- [Downloading Application Installers on page 813](#)

## Network Connect Launcher (NC Launcher) Overview

The Network Connect Launcher is a client-side command-line utility that maintains a very small footprint. You can bundle NC Launcher with other applications that need an operational Network Connect client. Bundling the NC Launcher with other applications allows you to be confident that the end-user can access these applications without difficulty. The NC Launcher allows you to initiate an NC session with a script, batch file, or a call from an application, without using a graphical user interface.



**NOTE:** The NC Launcher does not support the role mapping option Users must select from assigned Roles when more than one role is assigned to a user. If you use NC Launcher and more than one role can be assigned to a user, you must choose to either Merge settings for all assigned roles or you must choose the option that forces the User to select the sets of merged roles assigned by each rule.

To use the NC Launcher:

1. Write a script, batch file or application to call the NC Launcher.
2. Include a call to the NC Launcher executable.

The NC Launcher command syntax is:

```
nclauncher.exe [-version|-help|-stop|-signout] -u user -p password -url url -r realm -ir [true | false] -t seconds -c certificate-name -d DSID
```

Argument	Action
-version	Displays the NC Launcher version information, then exits.
-help	Displays available arguments information.
-u <i>user</i>	Specifies the username.
-p <i>password</i>	Specifies the password for authentication.
-url <i>url</i>	Specifies the Secure Access Service URL information.
-r <i>realm</i>	Specifies the realm to which Secure Access Service submits the user's credentials.
-ir [true   false]	Specifies whether to avoid client-side certificate revocation list on the client.
-t <i>seconds</i>	How long to wait for the NC tunnel to establish (in seconds).



<code>-c certificate-name</code>	<p>Specifies the certificate to use for user authentication instead of a user name and password. For <i>certificate-name</i> use the string specified in the Issued To field of the certificate.</p> <p>To use certificate authentication with NC Launcher, you must first configure Secure Access Service to allow the user to sign in via user certificate authentication. You must also configure a trusted client CA on Secure Access Service and install the corresponding client-side certificate in the Web browsers of your end-users before running NC Launcher.</p> <p>When using the <code>-c</code> argument, also specify the <code>-url</code> and <code>-r</code> arguments.</p> <p>If the certificate is invalid, NC Launcher displays an error message on the command line and logs a message in the <code>nclauncher.log</code> file.</p>
<code>-d DSID</code>	Passes a cookie to NC Launcher from another authentication mechanism when NC Launcher starts
<code>-signout</code>	Terminates NC tunnel and signs out current user.
<code>-stop</code>	Terminates NC tunnel.



**NOTE:** `nclauncher` does not support secondary authentication.

For example, you might distribute a simple login application to your end-users. The application might capture the end-user's username and password, the Secure Access Service resource they are trying to reach, and the realm to which they are assigned.

In this example, you need to write a script or add logic to your application to capture the credentials the end-user enters, and pass the credentials as the arguments to the `nclauncher.exe`, as follows:

```
nclauncher.exe -u JDoe -p my$Pass84 -url https://int-company.portal.com/user -r User
```

The following table lists the possible return codes `nclauncher` returns when it exits.

Code	Description
-1	(-Stop/-Signout) Network Connect is not running. System error occurred.
0	Network Connect started.
1	Invalid arguments.
2	Network Connect is unable to connect to the Secure Gateway.
3	Network Connect is unable to authenticate with the server.
4	The specified role is invalid or does not exist
5	Network Connect can not run because a required pre-authentication application could not be started.
6	Network Connect installation failed.

8	Network Connect was unable to perform a required software upgrade.
10	The server to which you are trying to connection does not support this feature.
12	Network Connect failed to authenticate the client certificate.
15	Network Connect failed to authenticate the client certificate because the certificate is invalid.
16	Network Connect failed to authenticate the client certificate because the certificate has expired.
17	Network Connect failed to authenticate the client certificate because the certificate has been revoked.
18	Host Checker policy failed.

If Network Connect is launched through a browser, certificate verification is taken care of by the browser. Similarly, if Network Connect is launched through the stand-alone application on Windows, certificate verification is handled by the application. However, if Network Connect is launched through nclauncher on Windows, nclauncher handles the expired or revoked client certificates.

**Related Documentation**

- [About VPN Tunneling on page 734](#)

## Launching Network Connect On Other Platforms

To launch a Network Connect command-line session on a non-Windows platform:

```
cd ~/.juniper_networks/network_connect/
./ncsvc -h host -u user -p passwd -f cert_file [-r realm] [-L log_level] [-g]
[-U sign_in_url] [-y proxy] [-z proxy_port] [-s proxy_user] [-a proxy_password]
[-d proxy_domain] [-v] [-K]
```

To launch a stand-alone Network Connect graphical user interface session on a non-Windows platform:

```
cd /user/local/nc/
#<javapath> -cp NC.jar NC -h host -u user -p passwd -f cert_file [-r realm] [-L
log_level] [-L log_level] [-U sign_in_url] [-y proxy] [-z proxy_port] [-s
proxy_user] [-a proxy_password] [-d proxy_domain] [-n start_script] [-t end_script]
ncsvc parameters are as follows:
```

Parameter	Description
Sign-in Options	
-h <i>host</i>	Secure Access Service hostname or IP address
-u <i>user</i>	Username
-p <i>passwd</i>	Password
-r <i>realm</i>	Secure Access Service sign-in realm

<code>-P port</code>	Service port number
<code>-f cert_file</code>	Secure Access Service certificate
<code>-m md5hash</code>	Secure Access Service certificate MD5 hash
<code>-U url</code>	Secure Access Service realm sign-in URL
Proxy options	
<code>-y proxy</code>	Proxy server hostname or IP address
<code>-z proxy_port</code>	Proxy server port number
<code>-s proxy_user</code>	Proxy server username
<code>-a proxy_pass</code>	Proxy server password
<code>-d proxy_domain</code>	Proxy server domain name
Logging options	
<code>-L log-level</code>	Log message level. Options are: 0—Log critical messages only 1—Log critical and error message 2—Log critical, error and warning message 3—Log critical, error, warning and info message (default) 4—Log verbose messages 5—Log all messages
Miscellaneous options	
<code>-v</code>	Print version number
<code>-g</code>	Zip and upload log file to host
<code>-K</code>	Kill all running ncsvc services
Script options	
<code>-n start_script</code>	Network Connect start script
<code>-t end_script</code>	Network Connect disconnect script

**Related Documentation** • [Network Connect Launcher \(NC Launcher\) Overview on page 780](#)

## Troubleshooting Network Connect Errors

---

Your end-users may be unable to resolve some of the errors they might encounter, without your intervention. The following topics may correspond to errors listed in the end-user help.

### nc.windows.app.23792

If your end-user encounters this error (or nc.windows.app.1023), they have been unable to connect to Secure Access Service.

Check items on both the client machine and on Secure Access Service.

On the client

- The error may indicate a faulty Java installation on the client. Have the client uninstall and reinstall the JRE.
- One or more of the 3rd-party clients on your end-user's computer may be faulty or interrupting the connection. You will need to check or have your user check clients such as VPN clients, Anti-Virus, Personal Firewalls, Spyware, and other types of endpoint security clients.
- The \Documents and Settings folder on the end-user's computer might be encrypted. Network Connect cannot install itself to an encrypted directory.

On Secure Access Service:

- Ensure that the DNS name lookup for Secure Access Service does not resolve to its public/private IP address.
- If the NC profile is configured to use an external DHCP server, ensure that the DHCP server is responding to Secure Access Service.
- Select System > Network > Overview and make sure that you have configured DNS for Secure Access Service.

### Version Conflict on Downgrade

When you downgrade to a prior release, your end-users might receive a version conflict error when Network Connect initiates. The problem may occur because the client contains a newer version of certain files which the older version cannot use properly.

To resolve this problem, delete the following files:

- <user\_home>/.juniper\_networks/ncLinuxApp.jar
- <user\_home>/.juniper\_networks/network\_connect/\*.\*

If this solution does not solve the version conflict problem, contact your system administrator.

## Error When Connecting to a FIPS Appliance

The error “Could not connect to Secure Gateway because the certificate is invalid or not trusted by the client system. Click OK to exit NC and Sign in to Secure Gateway again. If problem persists, please contact administrator.” occurs when the Network Connect client has received a server certificate from the FIPS appliance and:

- Secure Access Service is configured with self-signed certificate then either the server certificate is not valid or is not trusted by the client system.
- Secure Access Service is configured with complete certificate chain then either the server certificate is not valid or the root CA of the certificate chain is not trusted by the client.
- Secure Access Service is configured with complete certificate chain, but Secure Access Service has sent only a leaf certificate (this may happen if Secure Access Service is missing some of its sub-CAs) then either the server certificate is not valid or the complete certificate chain is not available on the client.

### Related Documentation

- [Task Summary: Configuring VPN Tunneling on page 737](#)
- [VPN Tunneling Execution on page 739](#)



## PART 5

# System Management

- [General System Management on page 789](#)
- [Certificates on page 837](#)
- [Elliptic Curve Cryptography on page 875](#)
- [System Archiving on page 889](#)
- [Logging and Monitoring on page 931](#)
- [Troubleshooting on page 959](#)
- [Clustering on page 977](#)
- [Delegating Administrator Roles on page 1005](#)
- [Instant Virtual System on page 1011](#)
- [IPv6 Support on page 1065](#)
- [Secure Access Service and IDP Interoperability on page 1081](#)
- [Routing AAA Over the Management Port for Virtual Appliances on page 1091](#)





## CHAPTER 29

# General System Management

- [General Network Settings on page 790](#)
- [Internal and External Ports on page 791](#)
- [Configuring the Internal and External Ports on page 792](#)
- [Configuring SFP Ports on the SA Series 6000 SSL VPN Appliance on page 797](#)
- [Configuring the Management Port on the SA Series 6000 SSL VPN Appliance on page 798](#)
- [Using VLANs with Secure Access Service on page 799](#)
- [Creating a New VLAN Port on page 802](#)
- [Using Virtual Ports on page 802](#)
- [Configuring Static Routes for Network Traffic on page 805](#)
- [Creating ARP Caches on page 806](#)
- [Specifying Host Names for Secure Access Service to Resolve Locally on page 807](#)
- [Configuring System Utilities on page 807](#)
- [Downloading Application Installers on page 813](#)
- [Obtaining, Entering and Upgrading Your License Keys on page 815](#)
- [Configuring License Options on page 818](#)
- [Upgrading License Keys on page 819](#)
- [About Subscription Licenses on page 821](#)
- [Activating and Deactivating Emergency Mode on page 822](#)
- [Setting Security Options on page 823](#)
- [Configuring NCP and JCP on page 827](#)
- [Installing a Juniper Software Service Package on page 828](#)
- [Configuring Your Management Port Network Settings From the Serial Console on page 829](#)
- [Configuring Management Port Network Settings on page 830](#)
- [Adding Static Routes to the Management Route Table on page 832](#)
- [Assigning Certificate to Management Port on page 833](#)
- [Controlling Administrator Sign-In Access on page 833](#)

- [Signing in Over the Management Port on page 834](#)
- [Setting Role-Mapping Rules Using Custom Expressions on page 834](#)
- [Troubleshooting the Management Port on page 835](#)
- [Using the Management Port on a Cluster on page 836](#)
- [Importing Configurations to a System with the Management Port Enabled on page 836](#)

## General Network Settings

---

Secure Access Service enables you to modify the network settings that you enter through the serial console during your initial configuration as well as configure additional network settings such as IP filters in order to enable other Secure Access Service features. This section provides the following overviews of network settings that you can set through the admin console:

You can view the status of the system ports, to specify a host name for Secure Access Service, and to configure DNS name resolution, Windows Internet Naming Service (WINS) server, and master browser settings for Secure Access Service through settings in the System > Network > Overview page in the admin console. You can also use settings in this page to view the DNS and WINS settings that you entered through the serial console during initial configuration.

When you remove a Windows workgroup, it might continue to appear in the Secure Access Service workgroup list for several hours before finally being removed from the list. This situation occurs because Secure Access Service collects workgroup information from all of the systems it can contact. The workgroup name might be cached on one or more Windows systems for several hours and when Secure Access Service interrogates the systems, it still finds the workgroup names. This is a common occurrence on systems other than Secure Access Service as well, and poses no integrity problems.

Use settings in this tab to configure general network settings. The Status area displays read-only status of the following items:

- **Node Name**—Name of the current node, if running a cluster.
- **Failover Message**—Indicates whether or not the failover functionality is enabled (only on an SA 6000 appliance).
- **Internal Port**—The status and speed of the internal port.
- **Port 1**—The status and speed of the external port, if used.
- **Management Port**—The status of the Management Port, if used.

System management features are an integral part of all Secure Access Service products—you do not need a special license to manage your Secure Access Service. However, note that the following advanced management features are not available on the SA 700:

- Bonding ports
- SFP ports

- Management ports
- VLANs
- Clustering features
- SSL acceleration
- WSAM installers

**Related  
Documentation**

- [Internal and External Ports on page 791](#)
- [Using VLANs with Secure Access Service on page 799](#)
- [Using Virtual Ports on page 802](#)
- [Configuring Static Routes for Network Traffic on page 805](#)

## Internal and External Ports

The internal port, also known as the internal interface, handles all LAN requests to resources, listening for Web browsing, file browsing, authentication, and outbound mail requests. You configure the internal port by providing IP address, gateway, DNS server and domain, and MTU settings during the initial setup of Secure Access Service. You can also change them on the System > Network > Internal Port > Settings tab. Alternatively, you can deploy the appliance in dual-port mode to listen for incoming Web and mail proxy SSL connections on an external port.

The external port, also known as the external interface, handles all requests from users signed into Secure Access Service from outside the customer LAN, for example, from the Internet. Before sending a packet, Secure Access Service determines if the packet is associated with a TCP connection that was initiated by a user through the external interface. If that is the case, Secure Access Service sends the packet to the external interface. All other packets go to the internal interface.

The routes that you specify for each interface apply after Secure Access Service has determined whether to use the internal or external interface. No requests are initiated by Secure Access Service from the external interface, and this interface does not accept any other connections (except ping and traceroute connections). All requests to any resource are issued from the internal interface.



**NOTE:** If you enable the external port, then, by default, administrators may no longer sign in from an external location. You can open the external port for administrators on the Administrators > Admin Realms > RealmName > Authentication Policy > Source IP tab.

## Bonding Ports on the SA 6000 SSL VPN Appliance

By default, on the SA6000 only, Secure Access Service uses bonding of the multiple ports to provide failover protection. Bonding two ports on Secure Access Service automatically shifts traffic to the secondary port when the primary port fails.

The SA6000 SSL VPN Appliance bonds ports as follows:

- Internal port = Port 0+Port 2
- External port = Port 1+Port 3

A message on the System > Network > Overview page indicates whether or not the failover functionality is enabled.

## Bonding Ports on the SA 6500 SSL VPN Appliance

By default, on the SA6500 only, if Secure Access Service uses bonding of the multiple ports to provide failover protection. Bonding describes a technology for aggregating two physical ports into one logical group. Bonding two ports on the SA6500 increases the failover capabilities by automatically shifting traffic to the secondary port when the primary port fails.

The SA6500 Series SSL VPN Appliance bonds ports as follows:

- Internal port = Port 0 + Port 1
- External port = Port 2 + Port 3

A message on the System > Network > Overview page of the administrator admin console whether or not the functionality is enabled. Bonding ports cannot span separate networks (multi-homed).

### Related Documentation

- [Configuring the Internal and External Ports on page 792](#)
- [Using VLANs with Secure Access Service on page 799](#)

---

## Configuring the Internal and External Ports

The internal interface settings are configured when you run the setup wizard from the serial console as part of the installation procedure. You can use the admin GUI System > Network pages to make changes to the internal interface or to enable and configure the external interface. This topic includes the following information:

- [Configuring the Internal Port on page 792](#)
- [Configuring the External Port on page 794](#)

### Configuring the Internal Port

The internal port connects to the local area network (LAN).

To modify network settings for the internal port:

1. In the admin GUI, choose **System > Network > Internal Port > Settings**.
2. As necessary, modify the settings described in [Table 51 on page 793](#).
3. Click **Save Changes**.

Table 51: Internal Port Settings

Setting		Guideline
IPv4 Settings	IP Address	<p>You must assign an IPv4 address to the internal interface.</p> <p>An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination.</p> <p>The format of an IPv4 address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.</p>
	Netmask	<p>A netmask indicates which part of an IP address indicates network identification and which part indicates the host identification. For example, the IP address and netmask 10.20.30.1 255.255.255.0 (or 10.20.30.1/24) refers to all the hosts in the 10.20.30.0 subnet. The IP address and netmask 10.20.30.1 255.255.255.255 (or 10.20.30.1/32) refers to a single host.</p>
	Default Gateway	<p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p> <p>Specify the IPv4 address for the default gateway for the routing domain to which the device belongs.</p>
IPv6 Settings	Enable IPv6 / Disable IPv6	<p>Disabled by default. Enable to support access from IPv6 endpoints.</p> <p>When you enable IPv6, the system acquires a link local address.</p> <p>If you switch from enabled to disabled, the system clears the link local address.</p>
	Link Local Address	<p>Displays the auto-configured link local address (after you have enabled and saved the IPv6 configuration).</p>
	IPv6 Address	<p>Specify a routable IPv6 address, such as a global unicast address that your network plan has provisioned for this host and interface. Automatic configuration methods are not supported. You must specify the appropriate address manually.</p>
	Prefix Length	<p>Specify how many of the higher-order contiguous bits of the IPv6 address comprise the prefix (the network portion of the IPv6 address). The default is 64.</p>
	Gateway	<p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p> <p>Specify the IPv6 address for the default gateway for the routing domain to which the device belongs.</p>

Table 51: Internal Port Settings (*continued*)

Setting	Guideline
Advanced Settings	
MAC Address	Displays the MAC Address for the interface.
Link Speed	Specify the speed and duplex combination for the interface.  If you run SNMP_GET and then change the Link Speed value, you must wait at least 5 minutes after submitting the change before running SNMP_GET again.
ARP Ping Timeout	(IPv4 only.) Specify how long Secure Access Service should wait for responses to Address Resolution Protocol (ARP) requests before timing out. Clustered Secure Access Service devices send ARP requests to the gateways of other Secure Access Service devices to determine if they are properly communicating with one another.  If you are not running Secure Access Service in a clustered environment, Secure Access Service does not use this setting. If your Secure Access Service devices are clustered, the timeout interval that you specify is synchronized across the cluster. In multisite clusters, you can override this setting for the individual nodes in the cluster using options in the System > Clustering page. Use caution when changing this setting in active/passive clusters, however, because Secure Access Service also uses the ARP Ping Timeout setting on the Internal tab as a failover timer for the VIP.
MTU	Specify the maximum transmission unit.  If IPv6 is enabled, the valid range is 1280 to 1500. If IPv6 is not enabled, the valid range is 576 to 1500.  We recommend you retain the default MTU setting (1500) unless you must change the setting for troubleshooting purposes.

## Configuring the External Port

The external port connects to the Internet. Remote users connect to the Secure Access Service external port.

To modify network settings for the external port:

1. In the admin GUI, choose **System > Network > External Port > Settings**.
2. As necessary, modify the settings described in [Table 52 on page 795](#).
3. Click **Save Changes**.

Table 52: External Port Settings

Setting	Guideline
IPv4 Settings      Enable IPv4 / Disable IPv4	<p>Disabled by default. If the external port was enabled prior to upgrading to Release 7.3 or Release 7.4, this option is enabled after upgrading, and the previous settings are preserved.</p> <p>Enable IPv4 if you want remote users to be able to access the device from IPv4 clients.</p> <p>If you enable IPv4, you must complete the IPv4 configuration.</p> <p>If you switch from enabled to disabled, the system retains your configured settings.</p>
IP Address	<p>An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination.</p> <p>The format of an IPv4 address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.</p>
Netmask	<p>A netmask indicates which part of an IP address indicates network identification and which part indicates the host identification. For example, the IP address and netmask 10.20.30.1 255.255.255.0 (or 10.20.30.1/24) refers to all the hosts in the 10.20.30.0 subnet. The IP address and netmask 10.20.30.1 255.255.255.255 (or 10.20.30.1/32) refers to a single host.</p>
Default Gateway	<p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p> <p>Specify the IPv4 address for the default gateway for the routing domain to which the device belongs.</p>

Table 52: External Port Settings (*continued*)

Setting	Guideline
IPv6 Settings      Enable IPv6 / Disable IPv6	<p>Disabled by default. Enable to support access from IPv6 endpoints.</p> <p>If you enable IPv6, you must complete the IPv6 configuration.</p> <p>When you enable IPv6, the system acquires a link local address.</p> <p>If you switch from enabled to disabled, the system clears the link local address but retains configured settings.</p>
Link Local Address	<p>Displays the auto-configured link local address (after you have enabled and saved the IPv6 configuration).</p>
IPv6 Address	<p>Specify a routable IPv6 address, such as a global unicast address that your network plan has provisioned for this host and interface. Automatic configuration methods are not supported. You must specify the appropriate address manually.</p>
Prefix Length	<p>Specify how many of the higher-order contiguous bits of the IPv6 address comprise the prefix (the network portion of the IPv6 address). The default is 64.</p>
Gateway	<p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p> <p>Specify the IPv6 address for the default gateway for the routing domain to which the device belongs.</p>



Table 52: External Port Settings (*continued*)

Setting	Guideline
Advanced Settings	
MAC Address	Displays the MAC Address for the interface.
Link Speed	Specify the speed and duplex combination for the interface.  If you run SNMP_GET and then change the Link Speed value, you must wait at least 5 minutes after submitting the change before running SNMP_GET again.
ARP Ping Timeout	(IPv4 only.) Specify how long Secure Access Service should wait for responses to Address Resolution Protocol (ARP) requests before timing out. Clustered Secure Access Service devices send ARP requests to the gateways of other Secure Access Service devices to determine if they are properly communicating with one another.  If you are not running Secure Access Service in a clustered environment, Secure Access Service does not use this setting. If your Secure Access Service devices are clustered, the timeout interval that you specify is synchronized across the cluster. In multisite clusters, you can override this setting for the individual nodes in the cluster using options in the System > Clustering page. Use caution when changing this setting in active/passive clusters, however, because Secure Access Service also uses the ARP Ping Timeout setting on the Internal tab as a failover timer for the VIP.
MTU	Specify the maximum transmission unit.  If IPv6 is enabled, the valid range is 1280 to 1500. If IPv6 is not enabled, the valid range is 576 to 1500.  We recommend you retain the default MTU setting (1500) unless you must change the setting for troubleshooting purposes.

- Related Documentation**
- [Internal and External Ports on page 791](#)
  - [Using VLANs with Secure Access Service on page 799](#)
  - [Understanding IPv6 on page 1065](#)

## Configuring SFP Ports on the SA Series 6000 SSL VPN Appliance

The SA 6000 includes two Small Form-factor Pluggable (SFP) Gigabit Ethernet ports (designated ports 2 and 3 on the front of the SA 6000). These ports are used primarily for failover. There is no need to configure SFP ports; once you plug them in, they are immediately available for use.

Be sure to enable the external port:

1. Choose **System > Network > Port [#] (External Port)** and select the Settings tab.
2. Under Use Port? select **Enabled** to activate the external port.

**Related Documentation** • [Internal and External Ports on page 791](#)

## Configuring the Management Port on the SA Series 6000 SSL VPN Appliance

The SA 6000 provides a Management Port that enables seamless integration into a dedicated Management Network, provides continuously available management access to Secure Access Service, and enables you to perform management activities without impacting user traffic and vice versa.

The typical deployment scenario takes advantage of the internal port for access to company business systems, the external port for access to and from the Internet, and the Management Port for access to the management network, consisting of dedicated devices such as syslog servers and SNMP servers.

Once you enable the Management Port capabilities, specific types of management traffic are sent over the management port:

- Syslog traffic
- SNMP traps
- SNMP queries
- NTP traffic
- FTP/SCP archive traffic



**NOTE:** If you apply an IVS license, you cannot use the Management Port to capture IVS administrative and management traffic. Also, you cannot use the IVS path-based URL prefix to sign in on the Management Port.

You can configure the Management Port just as you configure the internal port. The admin console provides a separate configuration tab in System > Network > Management Port, where you can specify port settings and advanced settings, such as IP address, netmask, MTU, ARP cache, and others.

To modify network settings for the Management Port:

1. Select the **Management Port > Settings** tab.



**NOTE:** Most fields on this page are pre-populated with the settings specified during installation.

2. Under Use Port? select **Enabled** to activate the Management Port.
3. Choose **System > Network > Management Port > Settings**.
4. In the Port Information section, update the IP address, netmask, gateway, and link speed settings.

5. In the ARP Ping Timeout field, specify how long Secure Access Service should wait for responses to Address Resolution Protocol (ARP) requests before timing out. Clustered Secure Access Service devices send ARP requests to the gateways of other Secure Access Service devices in order to determine if they are properly communicating with one another.



**NOTE:** If you are not running Secure Access Service in a clustered environment, Secure Access Service does not use this setting. If your Secure Access Service devices are clustered, the timeout interval that you specify is synchronized across the cluster. In multi-site clusters, you can override this setting for the individual nodes in the cluster using options in the System > Clustering page. Use caution when changing this setting in active/passive clusters, however, because Secure Access Service also uses the ARP Ping Timeout setting on the Management Port tab as a failover timer for the VIP.

6. In the ARP Ping Timeout field, specify how long Secure Access Service should wait for responses to Address Resolution Protocol (ARP) requests before timing out.
7. In the MTU field, specify a maximum transmission unit for Secure Access Service's internal interface.



**NOTE:** Use the default MTU setting (1500) unless you must change the setting for troubleshooting purposes.

8. Click **Save Changes**.

#### Related Documentation

- [Internal and External Ports on page 791](#)

## Using VLANs with Secure Access Service

Secure Access Service enable you to create VLANs for your enterprise. VLANs are used extensively in the virtual systems. You can also create a VLAN for use in an environment in which you have deployed a Secure Access Service device for use by all of your enterprise end-users.

The Secure Access Service VLAN feature is based on VLAN tagging, by which Secure Access Service tags traffic with 802.1Q VLAN IDs before transmitting the traffic over the backend. The infrastructure uses the VLAN tag to direct the packets to your appropriate VLANs/subnets.

Traffic coming in over the front-end—that is, inbound traffic—does not have VLAN tags. Secure Access Service adds the tag to a message upon its arrival over one of the Secure Access Service ports.

Each VLAN is assigned a VLAN ID which is part of an IEEE 802.1Q-compliant tag that is added to each outgoing Ethernet frame. The VLAN ID uniquely identifies all inbound

traffic. This tagging allows the system to direct all traffic to the appropriate VLAN and to apply respective policies to that traffic.

The VLAN termination point is any device on which VLAN-tagged traffic is identified, stripped of the VLAN tag, and forwarded to the appropriate tunnel to the backend.

You must define a VLAN port for each VLAN. You assign the specific VLAN ID when defining the VLAN port.

For each VLAN you configure, the Secure Access Service provisions a unique, logical VLAN interface, or port, on the internal interface. There is no relationship between the internal port IP address and any VLAN port IP address. Each VLAN port has its own route table.

The Internal Port must be assigned to the root system and marked as the default VLAN. Additionally, VLAN interfaces can be assigned to the root system. All authentication servers configured for the root system, however, must have routes in the Internal Port's route table, even if the servers are reachable via VLAN interfaces. Routes to servers reachable via VLAN interfaces must have the next-hop gateway set to the configured gateway for the VLAN interface, and the output port defined as the VLAN port.

For an Active/Passive clustered deployment, the root admin of an MSP network should configure all VLAN ports with at least one virtual port (System > Network > VLANs > Virtual Ports). The router administrator must configure routes for the IVS Network Connect IP ranges that point to the VLAN virtual port's IP address as the next-hop gateway. This is required for Network Connect session failover from an IVS in the Active Node to the corresponding IVS in the Passive Node.



**NOTE:** Suppose your Secure Access Service has a VLAN license but no IVS license. When you create VLANs, they are available for the entire system. However, when an IVS license is applied to the Secure Access Service, the VLANs are not applied to the Root IVS. They must manually be assigned to the Root IVS or other IVSes that you create.

---

Each VLAN port definition consists of:

- **Port Name**—Must be unique across all VLAN ports that you define on the system or cluster.
- **VLAN ID**—An integer in the range from 1 to 4094 that uniquely identifies the VLAN.
- **IP Address/Netmask**—Must be an IP address or netmask from the same network as the VLAN termination point, because Secure Access Service connects to the VLAN termination point on a Layer 2 network connection. VLAN IP addresses must be unique. You cannot configure a VLAN to have the same network as the internal port. For example, if the internal port is 10.64.4.30/16 and you configure a VLAN as 10.64.3.30/16, you may get unpredictable results and errors.

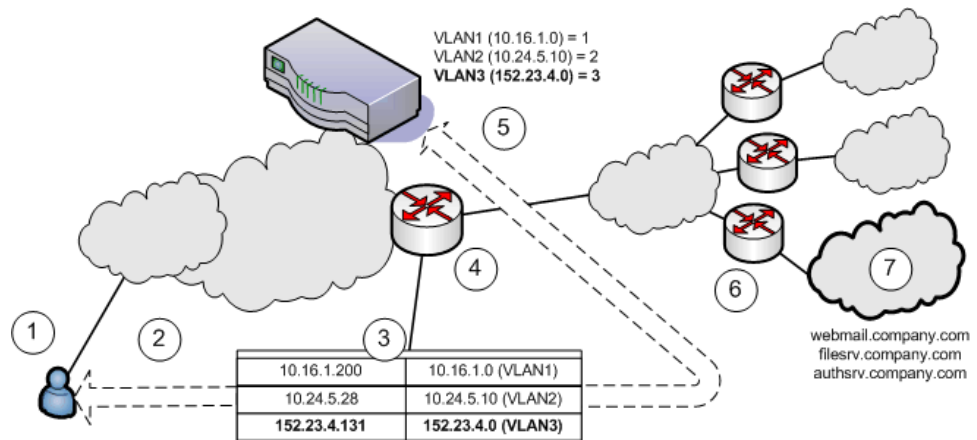
- **Default gateway**—The IP address of the default router, typically the CE or CPE router. The default gateway could act as the VLAN termination point, or could reside behind the VLAN termination point.
- **Other network settings**—Inherited from the internal port.

When you create a new VLAN port, the system creates two static routes, by default:

- The default route for the VLAN, pointing to the default gateway.
- The interface route to the directly connected network.

Figure 50 on page 801 shows an example of using VLANs. In this example, we are configuring a static route in the CE router to point to the end-user's IP address, with the next-hop gateway set to the IP address of the subscriber's VLAN port.

Figure 50: Example VLAN Use



The following briefly describes the steps shown in Figure 50 on page 801.

1. End-users sign in over an Internet connection using an IP address agreed upon by the MSP and the subscriber company.
2. Specify a static route in the MSP's VLAN termination point (in this example, a CE router) route table to point to the end-user sign-in IP addresses for each subscriber company.
3. You must also specify the next-hop gateway in the CE router's route table.
4. In the CE route table, specify all end-user sign-in IP addresses as static routes, and all corresponding VLAN port IP addresses as defined in the virtualized Secure Access Service.
5. Define at least one unique VLAN ID for each subscriber company. Use the IP addresses of each VLAN as the next-hop gateway addresses in the CE router's route table.
6. The subscribers' CPE routers perform the proper traffic routing to the subscriber company intranets.
7. Each subscriber company must provide sign-in pages for the IP addresses defined as static routes for end-user sign-in.

**Related Documentation**

## Creating a New VLAN Port

---

To create a VLAN port, perform the following steps:

1. Select **System > Network > VLANs** to open the VLAN Network Settings tab.
2. Click **New Port**. If you are running a cluster, you must create the VLAN for the entire cluster, not just for a single node.
3. Under VLAN settings, enter a name for the VLAN port.
4. Enter a VLAN ID.



**NOTE:** The VLAN ID must be between 1 and 4094 and must be unique on the system.

5. Enter the IP address for the VLAN.
6. Enter a netmask for the VLAN.
7. Enter a default gateway for the VLAN.
8. Click **Save Changes**.

**Related Documentation**

- [Using Virtual Ports on page 802](#)

## Using Virtual Ports

---

This topic provides the following information about using virtual ports:

- [About Virtual Ports on page 802](#)
- [Creating Virtual Ports on page 803](#)
- [Associating a Device Certificate with a Virtual Port on page 803](#)
- [Associating a Virtual Port with a Role on page 803](#)
- [Using Virtual Ports with Client Certificate Authentication on page 804](#)
- [Creating Virtual Ports for a Cluster on page 804](#)

### About Virtual Ports

A virtual port is an IP alias bound to a physical port. It shares all of the network settings, except IP address, with the associated physical port.

You can use virtual ports for different purposes, depending on the physical port or the VLAN on which you base the virtual port. You can:

- Configure virtual ports on the external port to support clustering and external sign-ins.

- Configure virtual ports on the internal port or the VLAN ports to support subnetting in the backend network with role-based source IP aliases.
- Use virtual ports to direct traffic to different virtual systems (requires an IVS license).

## Creating Virtual Ports

To create a virtual port:

1. In the admin GUI, choose **System > Network > PortName > Virtual Ports**. *PortName* is Internal Port or External Port, for example.
2. Click **New Port**.
3. Create alias name-address pairs. The names and IP addresses must be unique in your network. An alias may include IPv4 addresses, IPv6 addresses, or both. However, the corresponding IP protocol must be enabled on the physical port for the address(es) to take effect.



**NOTE:** Release 7.3 and Release 7.4 support IPv6 addresses for virtual ports on the external or internal ports, but not on VLAN ports.

4. Save the configuration.

## Associating a Device Certificate with a Virtual Port

You can associate device certificates with virtual ports. When you associate device certificates with ports, the Secure Access Service challenges the client for a valid client certificate (one that corresponds with the device certificate bound to the virtual port). Client certificate authentication is supported on the external port, as well as the internal and external virtual ports.

To associate a device certificate with a virtual port:

1. Use settings in the **System > Configuration > Certificates > Device Certificates** page to import the server certificates.
2. On the **System > Configuration > Certificates > Device Certificates** page, click the link to the imported certificate to display its details and settings page.
3. Under **Present certificate on these ports**, select the virtual port(s) that the Secure Access Service should associate with the certificate. You cannot select a port that is already associated with another certificate.
4. Click **Save Changes**.

## Associating a Virtual Port with a Role

You can also specify virtual ports as role-based source IP aliases. These aliases can correspond to source IP addresses that you specify on a backend network device as valid addresses originating from the Secure Access Service internal interface. For example, you might want to use a firewall behind the Secure Access Service to direct end-user

traffic to particular departments based on source IP addresses. You can define a role-based source IP alias for each departmental site. Each end user is then directed to a specific location based on their role through the use of the source IP alias.



**NOTE:** Role-based source IP aliasing is supported for virtual port aliases configured with IPv4 addresses only.

To associate subnet destinations and roles:

1. Use settings in the System > Network > Internal Port tab to create virtual ports.
2. Modify one or more roles to point to the virtual ports in the Users > Roles > *RoleName* > General > Source IP page.
3. Map your users to specific roles based on the subnet indicated by the source IP of the role in the Authentication > *RealmName* > Role Mapping page.

## Using Virtual Ports with Client Certificate Authentication

Any mobile device capable of supporting ActiveSync (push e-mail) along with client side certificates can be challenged by the Secure Access Service for a valid client certificate before being allowed access to the ActiveSync server. This provides greater assurance that only properly authenticated mobile devices are reaching the corporate e-mail services. Client certificate validation on the external and virtual ports does not support OCSP checking. If a client fails to provide a valid certificate, then SSL termination occurs. The end user will not see any other message or error from the Secure Access Service. It is up to the client devices to handle the failure gracefully.

To enable client certificate authentication on a virtual port:

1. Use settings in the System > Configuration > Certificates > Trusted Client CAs page to import the CA certificates used for client certificate authentication.



**NOTE:** If there is no Trusted Client CA configured or imported in the Secure Access Service, users cannot access the external or virtual ports.

2. On the System > Configuration > Security > SSL Options page, use the controls in the “ActiveSync Client Certificate Configuration” section to select the virtual ports that you want to enforce the client certificate requirement.
3. Save the configuration.

## Creating Virtual Ports for a Cluster

Special instructions apply when you create virtual ports for a cluster.



To create a virtual port on a cluster node:

1. In the admin GUI, choose **System > Network > PortName > Virtual Ports**. *PortName* is Internal or External, for example.
2. From the Settings list, select **Entire cluster** and then click **Update**.
3. Click **New Port**.
4. Enter a unique name for the virtual port and then click **Save Changes**. Secure Access Service adds the virtual port name to the Virtual Ports list and provides access to each node in the cluster.
5. Click the link to a node to access the IP address configuration page.
6. Create alias name-address pairs. The names and IP addresses must be unique in your network. An alias may include IPv4 addresses, IPv6 addresses, or both. However, the corresponding IP protocol must be enabled on the physical port for the address(es) to take effect.



**NOTE:** Release 7.3 and Release 7.4 support IPv6 addresses for virtual ports on the external or internet ports, but not on VLAN ports.

7. Save the Configuration.

The Virtual Ports page returns to the virtual port tab. If necessary, reselect **Entire cluster** from the Settings list and then repeat the last two steps of this procedure.

#### Related Documentation

- [Specifying Role-Based Source IP Aliases on page 111](#)
- [Specifying Role Mapping Rules for an Authentication Realm on page 309](#)
- [Using Device Certificates on page 839](#)
- [Internal and External Ports on page 791](#)
- [Using VLANs with Secure Access Service on page 799](#)

## Configuring Static Routes for Network Traffic

Secure Access Service enables you to add routing table entries using settings in the System > Network > Routes tab. All connection requests to internal resources come from the Secure Access Service internal port regardless of route settings. The route settings on the external port are used only to route packets associated with connections that are initiated by a remote client.

You can add static routes if you want to indicate a specific route that Secure Access Service should use when routing requests. You need to specify a valid IP address, gateway, and DNS address. The metric is a way of comparing multiple routes to establish precedence. A lower metric number, from 0 to 15, is a higher precedence. So, a route with a metric of 2 would be chosen over a route with a metric of 14.

To view or manage static route tables:

1. In the admin GUI, choose **System > Network > Routes**.
2. To display a route table, select properties from the “View route table for:” list boxes.

The list boxes allow you to select route tables per interface port and IP protocol (IPv4 or IPv6).



**NOTE:** In Secure Access Service Release 7.3 and Release 7.4, you can view discovered IPv6 routes, but you cannot add or delete them from the route table.

3. To add a route, click **New Route**, complete the required fields, and click **Add**.



**NOTE:** For SA6000, the “View route table for:” list boxes include tables for Port 2 and Port 3. Although ports 2 and 3 appear to be equivalent to the Internal port, they are not, and by default, Secure Access Service directs traffic to the Internal port when establishing an outbound connection. Therefore, if one of these two ports is connected to a network that the Internal port cannot reach, you need a static route for rewrites to access the unreachable network. Otherwise, the rewrites might fail.

#### Related Documentation

- [Internal and External Ports on page 791](#)

## Creating ARP Caches

You can use ARP caching to determine the physical (MAC) address of a network device such as a router or backend application server that connects to Secure Access Service. Use the **System > Network > Internal Port > ARP Cache** tab to manage the following types of ARP (address resolution protocol) entries:

- **Static entries**—You can add a static ARP entry to the cache associated with the IP and MAC address. Secure Access Service stores static entries during reboots and re-activates them after re-booting. Static entries are always present on Secure Access Service.
- **Dynamic entries**—The network “learns” dynamic ARP entries during normal use and interaction with other network devices. Secure Access Service caches dynamic entries for up to 20 minutes and deletes them during a reboot or when you manually delete them.

You can view and delete static and dynamic entries from the ARP cache as well as add static entries. If you have a cluster of Secure Access Service devices, note that ARP cache information is node-specific. Secure Access Service only synchronizes ARP cache information across non-multi-site clusters.

To add a static entry to the ARP Cache:

1. In the admin console, choose **System > Network > Port Tab > ARP Cache**. The Port Tab could be for any one of ports 1, 2, 3, 4, the internal or external ports, or the Management Port.
2. Enter the **IP Address** and the **Physical Address** in their respective fields at the top of the table. If you add an entry containing an existing IP address, Secure Access Service overwrites the existing entry with your new entry. Also note that Secure Access Service does not verify the validity of MAC addresses.
3. Click **Add**.

## Specifying Host Names for Secure Access Service to Resolve Locally

Specify host names that Secure Access Service can resolve to IP addresses locally by using the Hosts tab. This feature is useful when:

- Your DNS server is not accessible to Secure Access Service.
- You use WINS to access servers within the LAN.
- Your corporate security policy does not allow internal servers to be listed on an external DNS or requires that internal host names are masked.

To specify host names for Secure Access Service to resolve locally:

1. In the admin console, choose the **System > Network > Hosts** tab.
2. Enter an IP address, a comma delimited list of host names that resolve to the IP address, a comment of 200 words or less (optional), and then click **Add**.

## Configuring System Utilities

Secure Access Service utilities enable you to manage your server, upgrade or downgrade system software, enable version monitoring, and to download client applications and services.

## Reviewing System Data

The Maintenance > System > Platform page in the admin console lists system data and contains controls for restarting, rebooting, or shutting down a Secure Access Service device. It also contains a control to test server connectivity. When the Secure Access Service device is a member of a cluster, this page lists additional, cluster-specific, system data and the controls operate on a cluster-wide basis.

### Restarting, Rebooting, Shutting Down, or Testing Server Connectivity

The Maintenance > System > Platform page lists the following system data for Secure Access Service:

- **Model**—Displays the model of the Secure Access Service device.
- **Version**—Displays the Secure Access Service's software version.

- **Rollback**—Displays the software version to which Secure Access Service reverts when you roll back the installed image.
- **Last Reboot**—Displays amount of time since Secure Access Service's last reboot.

When the Secure Access Service device is a member of a cluster, the Platform page lists the following additional system data:

- **Cluster**—Displays the name of the cluster to which Secure Access Service belongs.
- **Member**—Displays the Secure Access Service's cluster member name.

The Platform page contains the following controls:

- **Restart Services/Cluster**—Kills all processes and restarts Secure Access Service. When the Secure Access Service device is a member of a cluster, this control kills all processes and restarts all members of a cluster.
- **Reboot**—Power cycles and reboots the Secure Access Service device. When the Secure Access Service device is a member of a cluster, this control power cycles and reboots all members of the cluster.
- **Shut down**—Shuts down the Secure Access Service device, requiring you to press the reset button on the appliance to restart the server. When the Secure Access Service device is a member of a cluster, this control shuts down all members of a cluster, requiring you to press the reset button on all clustered appliances to restart the cluster. Note that the machine power remains on after a server shutdown.



**NOTE:** If you want to restart, reboot, or shut down, or upgrade one Secure Access Service device in a cluster, you first disable the Secure Access Service using the controls on the System > Clustering > Status page, and then return to the Platform page to employ the control of your choice.

- **Rollback**—Rolls back the software image and reboots the Secure Access Service device. After Secure Access Service reboots, the image on Secure Access Service is automatically rolled back to the image displayed in the Rollback field, above.
- **Test Connectivity**—Sends an ICMP ping from Secure Access Service to all the servers the Secure Access Service device is configured to use and report their connectivity. Each server's status is reported under Server Connectivity Results.

### Hardware Status

Depending on your device, the Platform page also displays hard drive status, fan status and temperature.

The following table lists the RAID status and hard drive status for the SA6000 and SA6500 devices. Depending on your system, you may or may not see all these possible statuses.

Table 53: RAID and Hard Drive Status for the SA6000 and SA6500

RAID Status	Drive 1	Drive 2
Hard Disk RAID is operational	Active	Active
Hard Disk RAID is in Single Drive Mode	Missing	Active
Hard Disk RAID is in Single Drive Mode	Active	Missing
Hard Disk RAID has failed	Failed	Active
Hard Disk RAID has failed	Active	Failed
Hard Disk RAID is in the process of recovering	Active	Reconstructing
Hard Disk RAID is in the process of recovering	Reconstructing	Active
Hard Disk RAID is in the process of recovering	Active	Verifying
Hard Disk RAID is in the process of recovering	Verifying	Active
Hard Disk RAID status is unknown	Unknown	Active
Hard Disk RAID status is unknown	Active	Unknown
Hard Disk RAID status is unknown	Unknown	Unknown
Not available	n/a	n/a

The following table lists all the possible RAID status and hard drive status for the MAG-SM360. You can also view the RAID and hard drive status in log messages and in SNMP.

Table 54: RAID and Hard Drive Status for the MAG-SM360

RAID Status	Drive 1	Drive 2
Optimal	Optimal	Optimal
Degraded	Rebuilding	Optimal
Degraded	Optimal	Rebuilding
Degraded	Offline	Optimal
Degraded	Optimal	Offline

## Upgrading or Downgrading the Secure Access Service Device

You can install a different service package by first obtaining the software from the Juniper Support Web site and then uploading it through the admin console. Package files are encrypted and signed so that the Secure Access Service server accepts only valid packages issued by Juniper Networks. This measure prevents the Secure Access Service server from accepting Trojan horse programs.

This feature is typically used to upgrade to newer versions of the system software, but you can also use this process to downgrade to a previous version or to delete all your current configuration settings and start from a “clean slate.” You may also roll back to a previous system state through the serial console.

You can upgrade or downgrade Secure Access Service from the Maintenance > System > Upgrade/Downgrade page of the admin console.



**NOTE:** Installing a service package can take several minutes and requires Secure Access Service to reboot. Because existing system data is backed up during this process, you can decrease installation time by clearing your system log before trying to install a service package.

---

## Upgrading Virtual Appliances

You can upgrade or downgrade virtual appliances the same way you upgrade or downgrade Secure Access Service devices. Note that the Upload Status window or the Service Package Installation Status sometimes appears to not update its progress status or appears to be not responding. Check the VA-SPE console from the vSphere Client to view the current status.

## Changing Personalities

The Change Personality tab is applicable only for MAG Series Junos Pulse Gateways and lets you to change the service module from, for example, an Access Control Service to a Secure Access Service.

To change the personality from the service module administrator Web console:

1. In the admin console, choose **Maintenance > System > Change Personality**.
2. Click **Browse** to select the service package to install.
3. Click **Change Now**.

Changing a service module's personality deletes all configuration files and system and user data. You must perform the basic setup again to reestablish network connectivity. The installation process may take up to 20 minutes.

For more information, see the *MAG Series Junos Pulse Gateway Hardware Guide* located on the Juniper Networks support site.

## Setting System Options

You can set a number of system options, such as:

- **Enable Automatic Version monitoring**—Keep your system current and secure by having Secure Access Service notify you about critical software patches and updates. To do this, it reports to Juniper Networks the following data: your company name, an MD5 hash of your license settings, and information describing the current software version.
- **Enable gzip compression**—Reduce download speeds when using HTTP compression-enabled browsers.



**NOTE:** Gzip compression is not supported on the MAG Series Junos Pulse Gateways.

- **Enable Kernel Watchdog**—Enables the kernel watchdog that automatically restarts the system under kernel deadlock or when the kernel runs low on some key resources.



**NOTE:** Enable the kernel watchdog only when instructed by Juniper Networks Technical Support.

- **Enable File System Auto-clean Feature**—Enables the system to automatically clean up the file system when disk utilization reaches 90%. **IMPORTANT:** when enabled, this feature may result in loss of data that may be relevant in debugging system problems that occurred a week or earlier in the past. (i.e. old debuglogs, core files, and snapshots may be removed.)
- **Enable web installation and automatic upgrade of Junos Pulse Clients**—Select the behavior of Pulse client upgrades.

If you select this option, after you deploy Junos Pulse client software to endpoints, software updates occur automatically. A Pulse client can receive updates from the server. If you upgrade the Pulse software on your Pulse server, updated software components are pushed to a client the next time it connects.



**NOTE:** A bound endpoint receives connection set options and connections from its binding server, but it can have its Pulse client software upgraded from any Pulse server that has the automatic upgrade option enabled. During a client software upgrade the client loses connectivity temporarily.

- **Enable Java instrumentation caching**—Improve the performance of downloading Java applications.
- **End-user localization**—End-user localization—Set the language version for the end-user browser, or accept the default.

- **Show auto-allow**—Copy bookmarks for roles to corresponding access control policies when using resource policies.
- **External user records management**—Remove old user records from the system. Use with caution.

Set the following system options from Maintenance > System > Options:

1. Select the **Automatic Version Monitoring** check box to automatically receive notifications of critical software patches and updates. For your protection, we strongly recommend that you enable this automatic service. If necessary, you can disable the service later.
2. Select the **Enable gzip compression** check box to reduce the amount of data sent to browsers that support HTTP compression.



**NOTE:** Gzip compression is not supported on the MAG Series Junos Pulse Gateways.

3. Select **Enable Kernel Watchdog** to allow Secure Access Service to automatically shut down in the event of an issue with the kernel.
4. Select **Enable File System Auto-clean Feature** to allow the system to automatically clean up the file system when disk utilization reaches 90%.
5. Select the **Enable Java instrumentation caching** checkbox to improve the performance of downloading Java applications. With Java instrumentation caching enabled, Secure Access Service caches Java applets accessed by end users and serves the cached applets to subsequent requests for the same applets.
6. Select the **Enable SSL acceleration** checkbox to off-load the encryption and decryption of SSL handshakes from the appliance to the accelerator card.



**NOTE:** This option appears only if you have purchased a Secure Access Service device equipped with the corresponding accelerator card.

7. If the **Show Auto-allow** checkbox is checked, deselect the checkbox if you want to hide the auto-allow option from yourself or other administrators who create new bookmarks for roles.

The auto-allow option provides the means to automatically add bookmarks for a given role to an access control policy, for example, Web bookmarks with auto-allow set are added to the Web access control policy. You only use this feature if you also use Resource Policies. We recommend that you use Resource Profiles instead.

8. Under the Show Auto-allow option, choose either:
  - **Only this URL**—This option restricts the bookmarks to be added to the access control policy to the primary URL. For example, the URL `http://www.company.com` would be added to the access control policy.



- **Everything under this URL**—This option enables bookmarks to other paths under the primary URL to be added to the access control policy. If you define additional Web sites by role, you might want to include these in the access control policy. For example, the following URLs are both added when you select this option:
    - <http://www.company.com/sales>
    - <http://www.company.com/engineering>
9. Use the options under **External User Records Management** to remove old user records from Secure Access Service. This feature is useful when system performance is affected due to a large number of user records. We highly recommend you consult Juniper Networks Technical Support prior to using this feature.
- Deleting a user record removes all persistent cookies, SSO information, and other resources for that user on Secure Access Service. It does not remove the user record from the external or internal authentication server. If you delete a user record and that user logs back in to the authentication server, new user records are created. Records are not removed if that user is currently logged in.
- **Persistent user records limit**—Enter the maximum number of allowable user records on Secure Access Service.
  - **Number of user records to delete when the limit is exceeded**—Enter how many records to delete when the limit is exceeded. Older records are removed first. A user record is not deleted if that user is currently logged in.
  - **Delete Records Now**—Click this button to check whether the persistent user records limit has been exceeded. If it is, delete the number of user records specified in the option above.
  - **Enable automatic deletion of user records during new user logins**—Check whether the persistent user records limit will be exceeded whenever a new user record is about to be created. If true, delete the records prior to creating the user new record.
10. Select the language for the end-user browser from the End-user Localization drop down menu.
11. Click **Save Changes**.

**Related Documentation**

- [Setting Security Options on page 823](#)

## Downloading Application Installers

You can download an application or service as a Windows executable file, which enables you to:

- Distribute the file to client machines using software distribution tools. This option enables you to install an application or service on client machines whose users do not have Administrator privileges, which are required to install the application or service.
- Post the executable in a secure repository so that users with the proper administrator right may download and install the appropriate version.

- Download and execute a script that automatically retrieves the proper version of the installer from an FTP server.

These options allow you to control which version of an application or service runs on client machines.

- **Juniper Installer Service**—The Juniper Installer Service allows users to download, install, upgrade, and run client-side applications without administrator privileges. In order to perform these tasks (which require administrator privileges), the Juniper Installer Service runs under the client's Local System account (a powerful account with full access to the system) and registers itself with Windows' Service Control Manager (SCM). An Active-X control or a Java applet running inside the user's Web browser communicates the details of the installation processes to be performed through a secure channel between Secure Access Service and the client system.

When installing the Juniper Installer Service on client systems, note that:

- You need administrator privileges to install the Juniper Installer Service. For additional information, see Client-Side Changes.
- You should ensure that the Microsoft Windows Installer exists on the client system prior to installing the Juniper Installer Service.
- Your end-users' client systems must contain either a valid and enabled Java Runtime Engine (JRE) or a current Secure Access Service ActiveX control. If the client systems do not contain either of these software components, the endusers will be unable to connect to the gateway.
  - You should ensure that a valid JRE is enabled on your end-users' client systems.
  - If there is no JRE on your end-users' client systems, you should download an appropriate installer package from Maintenance > System > Installers.
- The service appears in the Windows Services (Local) list as Neoteris Setup Service.
- The service starts automatically on install and during client system start up.
- **Host Checker**—This installer (HCInst.exe) installs Host Checker on users' systems. Host Checker is a client-side agent that performs endpoint security checks on hosts that connect to Secure Access Service.

If you decide to distribute Host Checker, make sure to uncheck the Autoupgrade Host Checker option on the Authentication > Endpoint Security > Host Checker page. Otherwise Secure Access Service downloads the Host Checker application to a user's machine, which may not be the same version as the distributed version.

- **Third-party Integrity Measurement Verifier (IMV) Server**—This installer (RemoteIMVServerInstall.exe) installs IMVs on users' systems. IMVs are software modules running on Secure Access Service that are responsible for verifying a particular aspect of an endpoint's integrity.
- **Windows Secure Application Manager**—This installer (WSAMInstNt.exe) includes the NetBIOS version of W-SAM, which enables users to map drives to Windows resources.

- **Junos Pulse for Windows Mobile 5.0 PocketPC/6.0 Classic/6.0 Professional**—This installer includes the PDA version of WSAM, now called Junos Pulse. Use this version to install Junos Pulse on Pocket PC systems.
- **Junos Pulse for Windows Mobile 5.0 Smartphone/6.0 Standard**—This installer includes the PDA version of WSAM, now called Junos Pulse. Use this version to install Junos Pulse on Smartphone systems.
- **Network Connect for Windows**—This installer (NcInst.exe) installs Network Connect on Windows systems. Network Connect is a remote access mechanism that provides a VPN user experience.
- **Network Connect for 64-bit Windows**—This installer (NcInst64.exe) installs Network Connect on 64-bit Windows systems.
- **Network Connect for Mac OS X**—This installer (NetworkConnect.dmg) installs Network Connect on Macintosh OS X systems. Network Connect is a remote access mechanism that provides a VPN user experience.
- **Network Connect for Linux**—This installer (ncui-1.2-1.i386.rpm) installs Network Connect on Linux systems. Network Connect is a remote access mechanism that provides a VPN user experience.
- **Junos Pulse Installer (32-bit)**—This installer installs all the Junos Pulse components on a 32-bit Windows endpoint.
- **Junos Pulse Installer (64-bit)**—This installer installs all the Junos Pulse components on a 64-bit Windows endpoint.
- **Junos Pulse Installer (Macintosh)**—This setup application installs all Junos Pulse components. Use this installer for all Macintosh platforms version 10.6 and greater.

Download all installers from Maintenance > System > Installers.

#### Related Documentation

- [Obtaining, Entering and Upgrading Your License Keys on page 815](#)
- [Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 59](#)
- [Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 63](#)

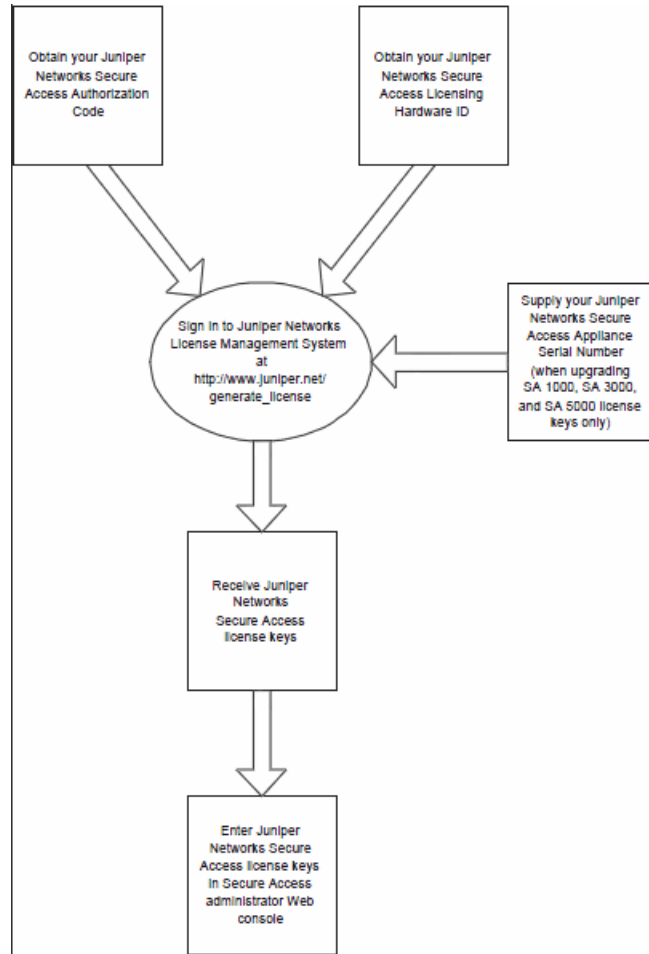
## Obtaining, Entering and Upgrading Your License Keys

Secure Access Service ships with a license that allows you basic access. To take full advantage of your appliance, however, you must access the Juniper Networks License Management System, provide your Licensing Hardware ID and Authorization Code(s) to obtain your license keys, and sign in to the admin console to enter the license keys you receive from Juniper Networks.

A Licensing Hardware ID is a unique 16-character code Juniper Networks uses to identify your particular Secure Access Service when generating license keys. You can find the Secure Access Service's Licensing Hardware ID above the menu options in the serial console and at the bottom of the admin console.

An Authorization Code is a pass key required to generate and activate license keys you or your company have purchased for your Secure Access Service. You receive your Authorization Code(s) after you purchase your Secure Access Service and associated product and feature licenses.

**Figure 51: License Key Generation and Activation**



The package you download from the Juniper Networks License Management System or the email message you receive from Juniper Networks may contain different types of licenses:

- **User license keys**—The user license key enables you to host as many users as are specified in the license key code. Secure Access Service user license keys are additive, meaning that you can expand the number of users that can access Secure Access Service by simply acquiring an additional user license key and adding it to your configuration. For example, if you initially purchase a 100 user license and then purchase another 100 user license in the future, your Secure Access Service could accommodate up to 200 users.



**NOTE:** When the user license limit is reached, any new user logging in will experience a slowdown in the sign-in process. Existing user sessions are not affected.

- **Access feature license keys**— access feature license keys allow you to enable access methods on Secure Access Service. Access feature license keys are available for a variety of access methods including Network Connect and Secure Application Manager, Junos Pulse Collaboration, and Advanced access feature licenses.
- **Cluster Licensing**—Secure Access Service software version 7.0 introduces several cluster license changes, including:
  - A license is no longer required to create a cluster.
  - CL licenses are no longer necessary but are still supported.
  - A 10 day *cluster grace period* provides license flexibility when a node crashes or loses connectivity with the rest of the cluster.
  - Juniper Networks recommends that you distribute your ADD licenses equally across the cluster to avoid losing a large number of licenses when a node disconnects from the cluster.

The maximum number of concurrent users allowed in a cluster is the sum of all user licenses of all connected nodes. If a node disconnects from the cluster (either A/A or A/P), up until the grace period ends the maximum license per each remaining node is their current license plus the minimum of their own license and the licenses of the other nodes.

- **In Case of Emergency (ICE) license keys**—In Case of Emergency (ICE) license keys allow you to activate the Secure Access Service emergency mode, and provides licenses for additional users on a Secure Access Service device and Junos Pulse Collaboration for up to eight weeks for periodic testing and transitioning to permanent licenses, if necessary. The ICE license does not include EES or other 3rd-party features.
- **Evaluation license keys**—Evaluation license keys allow you to enable and roll out the latest functionality for a limited time before deciding whether or not to purchase license keys and enable the new Secure Access Service functionality on a permanent basis. Evaluation license keys are valid for one, two, or four weeks.

Use the System > Configuration > Licensing tab to enter the license keys for your site, view their expiration dates, and delete them (if required).

Ensure that you read the license agreement, which is accessible from the Licensing tab, before submitting your license key. The license agreement available from the Licensing tab is the same text displayed in the serial console during the initial setup.

**Related Documentation**

- [Configuring License Options on page 818](#)
- [Activating and Deactivating Emergency Mode on page 822](#)

---

## Configuring License Options

---

To create and enter new license keys or transfer license keys to a replacement Secure Access Service device:

1. Ensure that you have your Licensing Hardware ID and Authorization Code(s) readily available.

You can find the Secure Access Service's Licensing Hardware ID above the menu options in the serial console and at the bottom of the admin console.

You receive your *Authorization Code(s)* separate from the Secure Access Service device after you purchase your Secure Access Service and associated product and feature licenses.

2. Navigate to the Juniper Networks License Management System at [https://www.juniper.net/generate\\_license](https://www.juniper.net/generate_license).



**NOTE:** The Juniper Networks License Management System offers you an access point where you can obtain detailed information about Juniper Networks licenses, including all licenses registered to you and your company, as well as licenses currently associated with specific Licensing Hardware IDs.

You must have a valid Juniper Networks Customer Support Center user ID and password to access the information at this location. To obtain a Juniper Networks Customer Support Center user ID and password, access the Customer Support Center.

---

3. Click the Secure Access SSL VPN link to generate new license keys or click Generate Replacement License for RMA Device to create a license key based on an existing license for the Secure Access Service device that you are replacing.



**NOTE:** The Generate Replacement License for RMA Device option is designed to accommodate RMA hardware-replacement scenarios only. It cannot be used to replace a license key that was created in error (for example, using an Authorization Code to create a license key for a Secure Access Service device other than the Secure Access Service device for which the license was originally purchased).

4. On the Generate Licenses page:
  - If you are creating a license key for only one Secure Access Service, enter the Licensing Hardware ID and one or more Authorization Codes in the appropriate fields.
  - If you want to create license keys for multiple Secure Access Service devices at the same time, click **Generate License Keys for Multiple SSL VPN Devices** and follow the on-screen procedure to create the Excel file necessary to generate your license keys.
5. Click Generate.
 

The Confirm License Information page appears, displaying a summary of the information you submitted to the License Management System.
6. Review the information to ensure everything is correct and then click **Generate License**.
 

The Generate License SSL VPN page appears, displaying a summary of your license keys, including a link that displays the details of your new license keys.
7. Click **Download/Email** and specify the file format and delivery method you want to use to obtain your new license keys.

After you download or receive your license keys by using email:

1. In the admin console, select **System > Configuration > Licensing**.
2. Click on the license agreement link. Read the license agreement and, if you agree to the terms, continue to the next step.
3. Enter your license key(s) and click **Add**.

**Related Documentation**

- [Obtaining, Entering and Upgrading Your License Keys on page 815](#)
- [Activating and Deactivating Emergency Mode on page 822](#)

## Upgrading License Keys

If you are using a SA700 or SA Series FIPS Appliance and you want to upgrade your license keys after upgrading the image on your Secure Access Service to 5.1 or later, you must go through the following procedure to create and enter your new license keys. Since Secure Access Service retains existing license information when upgrading, you are only required to validate and create new license keys for any license upgrades you purchase.

When you upgrade your license keys on an older Secure Access Service device, the Juniper Networks License Management System retains information about the new license keys you create as well as any future license keys you purchase and enter in your Secure Access Service device. Older license key details are not accessible. Juniper Networks cannot verify license key information for software versions older than 5.1. If you accidentally delete your license information, please contact Juniper Customer Care via the Customer Support Center Case Manager:

- 1-800-638-8296 (US and Canada)
- 1-408-745-9500 (International)

Juniper Customer Care will open a case on your behalf and provide you with a record of your lost license key(s).

To upgrade your license keys:

1. Ensure that you have your Licensing Hardware ID and Authorization Code(s) readily available.

You can find the Secure Access Service's Licensing Hardware ID above the menu options in the serial console and at the bottom of the admin console.

If you are upgrading your Secure Access Service's software and license keys, you receive your Authorization Code(s) for your additional feature licenses from the vendor from whom you originally purchased your Secure Access Service device.

2. Navigate to the Juniper Networks License Management System at [https://www.juniper.net/generate\\_license](https://www.juniper.net/generate_license).

The Juniper Networks License Management System offers you an access point where you can obtain detailed information about Juniper Networks licenses, including all licenses registered to you and your company, as well as licenses currently associated with specific Licensing Hardware IDs.

You must have a valid Juniper Networks Customer Support Center user ID and password to access the information at this location. To obtain a Juniper Networks Customer Support Center user ID and password, access the Customer Support Center.

3. Click the **Secure Access SSL VPN** link to generate new license keys or click **Generate Replacement License for RMA Device** to create a license based on an existing license for a Secure Access Service device that you are replacing.

The Generate Replacement License for RMA Device option is designed to accommodate RMA hardware-replacement scenarios only. It cannot be used to replace a license key that was created in error (for example, using an Authorization Code to create a license key for a Secure Access Service device other than the one for which the license was originally purchased).

4. On the Generate Licenses page:

- If you are creating a license key for only one Secure Access Service, enter the Licensing Hardware ID and one or more Authorization Codes in the appropriate fields.



- If you want to create license keys for multiple Secure Access Service devices at the same time, click **Generate License Keys for Multiple SSL VPN Devices** and follow the on-screen procedure to create the Excel file necessary to generate your license keys.
5. Click **Generate**.
  6. Enter the Secure Access Service device's serial number in the Serial Number field. If you do not enter the serial number when prompted, the license-generation portal automatically uses the Licensing Hardware ID you entered above.
  7. Click **Generate** again.  
The Confirm License Information page appears, displaying a summary of the information you submitted to the License Management System.
  8. Review the information to ensure everything is correct and then click Generate License.  
The Generate License SSL VPN page appears, displaying a summary of your license keys, including a link that displays the details of your new license keys.
  9. Click **Download/Email** and specify the file format and delivery method you want to use to obtain your new license keys.

After you download or receive your license key upgrades via email:

1. In the admin console, choose **System > Configuration > Licensing**.
2. Click on the license agreement link. Read the license agreement and, if you agree to the terms, continue to the next step.
3. Enter license keys and click **Save Changes**.

#### Related Documentation

- [Obtaining, Entering and Upgrading Your License Keys on page 815](#)

## About Subscription Licenses

---

Subscription licenses and renewal licenses (identified by a -R appended to the license name) have a start and end date embedded within them. Customers initially purchase a subscription license that is valid until a specified date. When the license expiration date nears, customers can renew their licenses.

When the license is installed, the start and end date are interpreted relative to the local time and time zone on the machine. The start date begins at 12:00 am; the end date ends at midnight of the end date (12:00 am of the following day). If the start date is in the future, the subscription or renewal license is not activated till the start date. A renewal license is automatically activated only if there is a corresponding expired subscription license.

A subscription license can only be renewed by a corresponding renewal license and a renewal can be activated only by the expiration of a corresponding subscription or renewal license.

## Available Subscription Licenses

The following subscription licenses are available (X and Z will be replaced by the appropriate number of user and/or year count):

- ACCESS-EES-XU-ZYR—Enhanced endpoint security
- ACCESS-RDP-XU-ZYR—Embedded RDP applet
- ACCESS-PRM-xU-zYR—Patch remediation management
- ACCESS-XU-ZYR—Concurrent user count subscription
- ACCESS-SUB-SVR-ZYR—Allows a device to be a license server



**NOTE:** With Secure Access Service 7.1 and later software, you can use either the ACCESS-LICENSE-SVR or the ACCESS-SUB-SVR-ZYR to identify a license server. With Secure Access Service 7.0 and earlier software, you must use the ACCESS-SUB-SVR-ZYR.

Both capacity-based licenses (such as ACCESS-EES) and time-base licenses (such as ACCESS-SUB) stack. For example:

- If you purchase two ACCESS-ES-10K-1YR licenses, they stack to 20K for 1 year.
- If you purchase both a one ACCESS-10K-1YR license and one ACCESS-ESS-10K-2YR license, they do not stack. They must be of the same *type*. For example, two ACCESS-10K-1YR licenses stack.
- If you purchase both an ACCESS-SUB-SVR-1YR and an ACCESS-SUB-SVR-2YR licenses, they stack to a three year license.

Note the following:

- ACCESS-SUB-SVR licenses have a maximum of 3 years. LMS will reject requests that stack ACCESS-SUB-SVR licenses to more than 3 years.
- Renewal licenses must match the license being renewed. For example, if your ACCESS-ESS-10K-1YR licenses is about to expire, you can only renew another ACCESS-ESS-10K-1YR-R license. You can not renew it with an ACCESS-ESS-10K-2YR-R license.

### Related Documentation

- About License Management

---

## Activating and Deactivating Emergency Mode

The emergency mode feature allows you to temporarily enable Secure Access Service for a large number of users.

To activate Secure Access Service in emergency mode, you must first install an In Case of Emergency (ICE) license using the standard Secure Access Service license installation

procedure. Then, when the emergency occurs, you can easily activate emergency mode through the Secure Access Service Web console. When your emergency has passed, you should then deactivate the emergency mode.



**NOTE:** The ICE license is permanent until you activate emergency mode. Activating emergency mode switches the ICE license to a temporary license and only enables you to operate in emergency mode for 8 weeks. Once the ICE license expires, all features disappear and your users can no longer access Secure Access Service using the emergency mode.

To activate or deactivate emergency mode:

1. In the Web console, select **System > Configuration > Licensing**.
2. Find the In Case of Emergency License entry in the license list. Sample ICE license names include:
  - SA4000-ICE
  - SA4000-ICE-CL
  - SA6000-ICE
  - SA6000-ICE-CL
3. Click the **Enable** link in the right side of the license column to activate emergency mode or click **Disable** to deactivate it.

When you enable and disable emergency mode, Secure Access Service decrements the corresponding license in 5 minute intervals.

**Related  
Documentation**

- [Obtaining, Entering and Upgrading Your License Keys on page 815](#)
- [Configuring License Options on page 818](#)

## Setting Security Options

Use the **System > Configuration > Security** page to change the default security settings for your Secure Access Service. We recommend that you use the default security settings, which provide maximum security, but you may need to modify these settings if your users cannot use certain browsers or access certain Web pages. You can also configure lockout options for protecting Secure Access Service and back-end systems from DOS/DDOS/Password Guessing attacks from the same IP address.

## Setting System-Wide Security Options

If any of your users experience browser problems when accessing certain Web pages, consider adjusting the following settings:

- **Allowed SSL and TLS Version**—Specify encryption requirements for Secure Access Service users. Secure Access Service honors this setting for all Web server traffic, including oNCP and Secure Email client, and all types of clients, including Pocket PC and iMode. (Secure Access Service requires SSL version 3 and TLS by default.) You can require users who have older browsers that use SSL version 2 to update their browsers or change Secure Access Service setting to allow SSL version 2, SSL version 3, and TLS.
- **Allowed Encryption Strength**—Secure Access Service requires 128-bit encryption by default, or you can specify that Secure Access Service requires 168-bit encryption. Older browsers, which pre-date the 2000 change in the U.S. export law that required 40-bit cipher encryption for international export, may still use 40-bit encryption. You can either require users to update to a browser with 128-bit cipher encryption or change the required encryption strength to also allow 40-bit ciphers.

If you select the Accept only 168-bit and greater option, Secure Access Service gives preference to 256-bit AES over 3DES.

If you select the Accept only 128-bit and greater option or the Accept 40-bit and greater option, Secure Access Service gives preference to RC4 ciphers.

To specify a combination of cipher suites for the incoming connection from the user's browser, choose the Custom SSL Cipher Selection option under Allowed Encryption Strength. If you select the AES/3DES option, Secure Access Service gives preference to 256-bit AES over 3DES. The same selected custom ciphers are also used for backend rewriter connections. Secure Access Service gives preference to 256-bit AES encryption for incoming SSL connections to the mail proxy.

When you use a custom cipher, the selected ciphers are enforced to the SSL connections from clients. Secure Access Service will always present "High" ciphers to back-end servers when making SSL connections.



**NOTE:** When using 168-bit encryption on Secure Access Service, some Web browsers may still show 128-bit encryption (the gold lock on the browser status bar) even though the connection is 168-bit. This is typically a limitation of the browser's capability.

If you are using the FIPS SA 6500 version, you can choose High, Medium or Low security cipher suites. AES/3DES High and AES Medium check boxes are recommended for FIPS deployment.

- **Encryption Strength option**— Normally, the allowed encryption strength is enforced after an SSL session is established, so that a user connecting with a disallowed encryption strength receives a Web page describing the problem. The **Do not allow connections from browsers that only accept weaker ciphers** option prevents a browser with a weak cipher from establishing a connection. This option is enabled by default.

- **SSL Handshake Timeout option**—Determines how many seconds before the SSL handshake times out. The default is 60 seconds.
- **SSL Legacy Renegotiation Support option** – SSL and Transport Layer Security (TLS) renegotiations can be subjected to man-in-the-middle (MITM) attacks that can lead to abuse. A new TLS extension (defined in RFC 5746) ties renegotiations to the TLS connections they are being performed over to prevent these kinds of attacks. The SSL Legacy Renegotiation Support option is enabled by default and allows renegotiation between clients and servers even if they do not support the new TLS extension. Disable this option to not allow renegotiations between clients and servers that do not support the new TLS extension. A web server restart is required when you change the value of this option.



**NOTE:** The SSL Legacy Renegotiation Support option is not available for IVS.

- **ActiveSync Client Certificate Configuration**—Use these controls to enforce client certificate requirement for active sync access on the selected ports, including virtual ports. When enabled, all ActiveSync clients must present a client authentication certificate to the Secure Access Service to be able to connect using ActiveSync. Non-ActiveSync access (like web browser based access to SA, NC, JSAM, WSAM, Pulse, WTS, IKEv2 and so forth) on the port/interface on which the ActiveSync client certificate is required might not work properly. We recommend you use a separate port or interface exclusively for ActiveSync access and then enable client certificate requirement for the port intended for ActiveSync access.
- **Delete all cookies at session termination**—For convenience, Secure Access Service sets persistent cookies on the user's machine to support functions such as multiple sign-in, last associated realm, and the last sign-in URL. If you desire additional security or privacy, you may choose to not set them.
- **Include session cookie in URL**—Mozilla 1.6 and Safari may not pass cookies to the Java Virtual Machine, preventing users from running JSAM and Java applets. To support these browsers, Secure Access Service can include the user session cookie in the URL that launches JSAM or a Java applet. By default, this option is enabled, but if you have concerns about exposing the cookie in the URL, you can disable this feature.
- **Last Login options**—Display the day and time and IP address the user last logged in to the system. For users, this information appears on their bookmark page. For administrators, this information appears on the System Status Overview page. These settings do not apply to the custom start page option on Role UI Options page.

## Configuring Lockout Options

You can configure the following Lockout options to protect Secure Access Service and other systems from Denial of Service (DoS), Distributed Denial of Service (DDoS), and password-guessing attacks from the same IP address:



**NOTE:** Lockout options are not available to IVS systems. All other security options are available to IVS systems.

- **Rate**—Specify the number of failed sign-in attempts to allow per minute.
- **Attempts**—Specify the maximum number of failed sign-in attempts to allow before triggering the initial lockout. Secure Access Service determines the maximum initial period of time (in minutes) to allow the failed sign-in attempts to occur by dividing the specified number of attempts by the rate. For example, 180 attempts divided by a rate of 3 results in a initial period of 60 minutes. If 180 or more failed sign-in attempts occur within 60 minutes or less, Secure Access Service locks out the IP address being used for the failed sign-in attempt.
- **Lockout period**—Specify the number of minutes you want Secure Access Service to lock out the IP address.

Secure Access Service reacts quickly to an attack that persists, and then gradually becomes less restrictive when the attack subsides. After a lockout occurs, Secure Access Service gradually recovers by maintaining the Rate. If the current failure rate since the last lockout exceeds the specified Rate, Secure Access Service locks out the IP address again. If the failure rate is less than the specified Rate for the period of Attempts/Rate, Secure Access Service returns to the initial monitoring state.

For example, if you use the following settings for the Lockout options, Secure Access Service locks out the IP address for the time periods in the following scenario.

- **Rate** = 3 failed sign-in attempts/minute
- **Attempts** = 180 maximum allowed in initial period of 60 minutes (180/3)
- **Lockout period** = 2 minutes
  1. During a period of three minutes, 180 failed sign-in attempts occur from the same IP address. Because the specified value for Attempts occurs in less than the allowed initial period of 60 minutes (180/3), Secure Access Service locks out the IP address for 2 minutes (4th and 5th minutes).
  2. In the 6th minute, Secure Access Service removes the lock on the IP address and begins maintaining the rate of 3 failed sign-in attempts/minute. In the 6th and 7th minutes, the number of failed sign-in attempts is 2 per minute, so Secure Access Service does not lock the IP address. However, when the number of failed sign-in attempts increases to 5 in the 8th minute, which is a total of 9 failed sign-in attempts within 3 minutes, Secure Access Service locks out the IP address for 2 minutes again (9th and 10th minutes).

3. In the 11th minute, Secure Access Service removes the lock on the IP address and begins maintaining the rate of 3 failed sign-in attempts/minute again. When the rate remains below an average of 3/minute for 60 minutes, Secure Access Service returns to its initial monitoring state.

In environments where two or more users share the same IP address (as seen by Secure Access Service), the lockout feature prevents all users from logging in from the shared IP address even when only one of them is the offending user. Sharing of the IP address as seen by Secure Access Service can happen when, for example, users are logging in from behind a NAT box.

**Related Documentation**

- [Configuring System Utilities on page 807](#)

## Configuring NCP and JCP

The following types of internal protocols are used to communicate between the Secure Access Service server and client applications:

- **Network Communications Protocol (NCP)**—Standard NCP has been replaced by oNCP. Windows client applications, including the Junos Pulse Collaboration Windows client, WSAM, and Terminal Services fallback to NCP if oNCP fails.
- **Optimized NCP (oNCP)**—Optimized NCP (oNCP) significantly improves the throughput performance of the client applications over NCP because it contains improvements to protocol efficiency, connection handling, and data compression. Windows client applications, including the Junos Pulse Collaboration Windows client, WSAM, Network Connect and Terminal Services use oNCP by default.
- **Java Communications Protocol (JCP)**—JCP is the Java implementation of standard NCP. Secure Access Service uses JCP to communicate with Java client applications, including the Junos Pulse Collaboration Java client, JSAM, and the Java Content Intermediation Engine.

To set NCP options:

1. In the admin console, choose **System > Configuration > NCP**.
2. (Windows clients) Under NCP Auto-Select, select:
  - **Auto-select Enabled** (recommended)—Use the oNCP by default. If you select this option, Secure Access Service uses oNCP for most client/server communications and then switches to standard NCP when necessary. Secure Access Service reverts to NCP if the user is running an unsupported operating system, browser type, or combination thereof, or if the client application fails to open a direct TCP connection to Secure Access Service for any reason (for instance, the presence of a proxy, timeout, disconnect).
  - **Auto-select Disabled**—Always use standard NCP. This option is primarily provided for backwards compatibility.



**NOTE:** If you are using Network Connect to provide client access, we recommend that you exercise caution when employing the Auto-select Disabled option, as Mac and Linux clients cannot connect using the traditional NCP protocol. If you disable the oNCP/NCP auto-selection feature and a UDP-to-oNCP/NCP fail-over occurs, Secure Access Service disconnects Macintosh and Linux clients because Secure Access Service fails over from UDP to NCP (instead of oNCP), which does not support these users.

3. (Java clients) Under Read Connection Timeout, set the timeout interval for Java clients (15-120 seconds). If client-side secure access methods do not receive data from Secure Access Service for the specified interval, they try to reestablish a connection to Secure Access Service. Note that this value does not apply to user inactivity in client applications.
4. (Windows clients) Under Idle Connection Timeout, set the idle connection interval. This timeout interval determines how long Secure Access Service maintains idle connections for client-side Windows secure access methods.
5. Click **Save Changes**.

---

## Installing a Juniper Software Service Package

---

The admin console lets you install a new service package immediately or stage the service package. Staging lets you to push the package to a directory on Secure Access Service before the planned maintenance time and then install the package during the maintenance window. Note that staging does not provide the ability to schedule the installation of the stored service package. It only pushes the service package to the device without installing it. You must still manually start the installation process.

For clusters, we recommend you stage the service package at each cluster node, especially for “slower” networks. This reduces the upgrade time by allowing each node to upgrade simultaneously instead of having one node push the upgrade process to each of the other cluster’s nodes. Note, however, that the service package revision at the node where you first start the installation process overwrites the service package revision at the other cluster’s nodes if they are different. For example, suppose you stage service packages at *clusterNode1*, *clusterNode2* and *clusterNode3*. Now start the upgrade process on *clusterNode3*. The service pack revision on *clusterNode1* is compared to *clusterNode3*. If it is different, then the service package on *clusterNode3* is pushed to *clusterNode1* before *clusterNode1* starts its upgrade. If the revisions are the same, then *clusterNode3* does not push its service package to *clusterNode1*. Similarly for *clusterNode2*.

Before installing a new service package, please export your current system configuration, local user accounts, customized user settings, and role and policy information.



To install a service package:

1. Browse to the Juniper Networks Customer Support Center and obtain the desired service package.
2. In the admin console, select **Maintenance > System > Upgrade/Downgrade**.
3. Click **Browse** to find the service package on your hard drive that you obtained from the Juniper Networks Customer Support Center. If you want to delete your current configuration settings but continue to use the same Secure Access Service version, choose the service package that is currently installed on your appliance.
4. Alternately, select the **Upload new package into staging area** option button and **Browse** for a locally stored file and select the option button for **From stated package**.
5. If you are rolling back to an older service package or deleting your configuration settings, select **Delete all system and user data**.



**NOTE:** If you choose to revert to delete all system and user data from the appliance using this option, you will have to reestablish network connectivity before reconfiguring the system. Also note that you cannot roll back to a version lower than 3.1.

6. Select the service package file and click **Install Now**.

**Related Documentation**

- [Configuring System Utilities on page 807](#)

## Configuring Your Management Port Network Settings From the Serial Console

To configure your Management Port network settings from the serial console

1. Start a serial console session.
2. Select item 1, **System Settings and Tools**.
3. Select item 10, **Configure Management port**. The text indicates if the option is enabled or disabled.
4. Enter the network settings for the Management Port, as prompted.



**NOTE:** If you enable the Management Port but neglect to configure the IP address and netmask, the port reverts to a disabled state. Also, you cannot clear Management Port settings from the serial console when the port is disabled, though you can clear them from within the admin console.

5. When prompted to accept the changes, if they are correct, enter y. Otherwise, repeat the process to correct the settings.
6. Close the serial console.

**Related Documentation** • [Configuring Management Port Network Settings on page 830](#)

## Configuring Management Port Network Settings

If your Secure Access Service device has a management port, enable it so that management traffic uses a dedicated port. When you enable the management port, the following traffic is directed out of the management port: syslog, SNMP traps, SNMP queries, NSM, NTP, FTP/SCP archiving, and Push Config. You might have configured the management port when you ran the setup wizard from the serial console as part of the installation procedure. You can use the admin GUI **System > Network** pages to make changes.

Before you begin:

1. Make sure your backend management network is already configured.
2. Connect the Secure Access Service management port to a network device, such as a switch, that can access the network gateway.

To modify network settings for the management port:

1. In the admin GUI, choose **System > Network > Management Port > Settings**.
2. As necessary, modify the settings described in [Table 55 on page 830](#).
3. Click **Save Changes**.

**Table 55: Management Port Settings**

Setting	Guideline
IPv4 Settings	<p><b>IP Address</b></p> <p>An IP address is an identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination.</p> <p>The format of an IPv4 address is a 32-bit numeric address written as four numbers separated by periods. Each number can be zero to 255.</p>
	<p><b>Netmask</b></p> <p>A netmask indicates which part of an IP address indicates network identification and which part indicates the host identification. For example, the IP address and netmask 10.20.30.1 255.255.255.0 (or 10.20.30.1/24) refers to all the hosts in the 10.20.30.0 subnet. The IP address and netmask 10.20.30.1 255.255.255.255 (or 10.20.30.1/32) refers to a single host.</p>
	<p><b>Default Gateway</b></p> <p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p> <p>Specify the IPv4 address for the default gateway for the routing domain to which the device belongs.</p>

Table 55: Management Port Settings (*continued*)

Setting	Guideline
IPv6 Settings      Enable IPv6 / Disable IPv6	<p>Disabled by default. Enable IPv6 to support management traffic over an IPv6 network.</p> <p>If you enable IPv6, you must complete the IPv6 configuration.</p> <p>When you enable IPv6, the system acquires a link local address.</p> <p>If you switch from enabled to disabled, the system clears the link local address but retains configured settings.</p>
Link Local Address	<p>Displays the auto-configured link local address (after you have enabled and saved the IPv6 configuration).</p>
IPv6 Address	<p>Specify a routable IPv6 address, such as a global unicast address that your network plan has provisioned for this host and interface. Automatic configuration methods are not supported. You must specify the appropriate address manually.</p>
Prefix Length	<p>Specify how many of the higher-order contiguous bits of the IPv6 address comprise the prefix (the network portion of the IPv6 address). The default is 64.</p>
Gateway	<p>A gateway is the router that resides at the point of entry to the current routing domain, often called the default gateway.</p> <p>Specify the IPv6 address for the default gateway for the routing domain to which the device belongs.</p>

Table 55: Management Port Settings (*continued*)

Setting	Guideline
Advanced Settings	MAC Address
	Displays the MAC Address for the interface.
	Link Speed
	Specify the speed and duplex combination for the interface.  If you run SNMP_GET and then change the Link Speed value, you must wait at least 5 minutes after submitting the change before running SNMP_GET again.
	ARP Ping Timeout
	(IPv4 only). Specify how long Secure Access Service should wait for responses to Address Resolution Protocol (ARP) requests before timing out. Clustered Secure Access Service devices send ARP requests to the gateways of other Secure Access Service devices to determine if they are properly communicating with one another.  If you are not running Secure Access Service in a clustered environment, Secure Access Service does not use this setting. If your Secure Access Service devices are clustered, the timeout interval that you specify is synchronized across the cluster. In multisite clusters, you can override this setting for the individual nodes in the cluster using options in the System > Clustering page. Use caution when changing this setting in active/passive clusters, however, because Secure Access Service also uses the ARP Ping Timeout setting on the Internal tab as a failover timer for the VIP.
	MTU
	Specify the maximum transmission unit.  If IPv6 is enabled, the valid range is 1280 to 1500. If IPv6 is not enabled, the valid range is 576 to 1500.  We recommend you retain the default MTU setting (1500) unless you must change the setting for troubleshooting purposes.

- Related Documentation**
- [Configuring Your Management Port Network Settings From the Serial Console on page 829](#)
  - [Understanding IPv6 on page 1065](#)

## Adding Static Routes to the Management Route Table

You can also add static routes to the management route table. This is easily accomplished by following the procedure for adding static routes to route tables. When you enable the Management Port, the New Route page includes a new interface selection for the management route table.

- Related Documentation**
- [Configuring Static Routes for Network Traffic on page 805](#)

---

## Assigning Certificate to Management Port

---

You can assign only one device certificate to the Management Port. If you assign a certificate other than the default device certificate to the Management Port, the default device certificate is automatically deselected as the default. If you do not select a device certificate for the Management Port, then Secure Access Service uses the default device certificate that is presented on the Internal port.



**NOTE:** You cannot assign certificates to Management Port VIPs.

### Related Documentation

- [Troubleshooting the Management Port on page 835](#)

---

## Controlling Administrator Sign-In Access

---

You can control administrator access to the ports on the Secure Access Service device. When you enable the Management Port, access to it is controllable through the configuration of your Administrator realms.

To control administrator access to the Management Port

1. Enable the Management Port.
2. Perform one of the following steps:
  - Choose **Administrators > Admin Realms > Admin Users** to modify the default admin users realm.
  - Choose **Administrators > Admin Realms**, then click **New**, to create a new administrator realm.
3. Click the Authentication Policy tab.
4. Scroll to the bottom of the Source IP tab. You should see a message stating that the Management Port is enabled, along with a link to the Network Settings page.
5. Select the available options to allow administrators to sign in to all available ports, to the management port or the internal port only, or to restrict them from signing in to any of the ports. In some cases you may inadvertently limit administrative access completely. If this occurs, you can reconfigure the ports by way of the serial console.



**NOTE:** If you limit administrative access to the Management Port, then export configuration and import the configuration to an SA2000/2500 Series Appliance or an SA4000/4500 Series Appliance, the import operation may fail or the Management Port configuration will be ignored, possibly stranding your administrator access. This could occur because only the SA6000/6500 Series Appliance supports the Management Port. The other appliance models do not recognize the Management Port configuration.

If you enable administrators to sign in to the Management Port or to the Internal Port but you neglect to enable the Management Port itself, Secure Access Service considers the option to be set to allow administrators to sign in to the Internal port only. If you then enable the Management Port, the setting for administrator access to the Management Port will be restored, assuming you have left the Management Port option selected on the Authentication Policy tab.

6. Click **Save Changes**.

- Related Documentation**
- [Configuring Management Port Network Settings on page 830](#)
  - [Creating an Authentication Realm on page 306](#)

## Signing in Over the Management Port

If you sign in to an appliance directly via the Management Port IP address, you will be unable to access the end-user sign-in page, as you normally can with the default configuration over the internal port. You are only allowed to sign in to the realm defined for the administrative access to the Management Port. If you want to access the end-user sign-in page, you need to sign in over either the internal port or the external port.

However, if you have restricted access within the realm, so that administrators must sign in over the Management Port, access to the other ports is effectively blocked when signing in to the Management Port IP address.

- Related Documentation**
- [Troubleshooting the Management Port on page 835](#)

## Setting Role-Mapping Rules Using Custom Expressions

When you have enabled the Management Port, you can use a new value for the network interface (networkIF) variable in custom expressions to assign roles to the port.

To use the new variable:

1. Set up the administrator sign-in access then click the Role Mapping tab.
2. Select **Custom Expressions** from the **Rule based on** pull-down menu.

3. Click **Update**.
4. Under the Rule section, click **Expressions**.
5. On the Expressions tab of the Server Catalog dialog, enter a name for your new rule.
6. Enter the expression as:
 

```
networkIF = "management"
```

Make sure you enclose the value in double quotes. Unlike the values for internal and external ports, you must delimit the Management Port value with double quotes.
7. Click **Save Changes**. Your named expression appears in the Available Expressions text box.
8. Select the expression and click **Add** to move the expression to the Selected Expressions text box.
9. Select the appropriate role, for example, .Administrators, then click **Add** to move the role to the Selected Roles text box.
10. Click **Save Changes**.

This procedure assigns the selected role or roles to the Management Port.

**Related  
Documentation**

- [Troubleshooting the Management Port on page 835](#)

## Troubleshooting the Management Port

Secure Access Service provides a number of troubleshooting features to help you identify and resolve problems, if necessary. Some potential problems can occur if you do not configure your management network and if you allow management devices, such as syslog servers to send traffic over Secure Access Service's internal port.

For example, if you configure management devices to send traffic over the internal port, you may be unable to retrieve that information. For example, if you configure an SNMP trap to send results over the internal port when the Management Port is enabled, Secure Access Service drops the data.



**NOTE:** Secure Access Service ignores SNMP queries that occur on any port other than the Management Port, when the Management Port is enabled.

Management Port traffic is captured in the admin log.

### Using TCPDump to Troubleshoot the Management Port

You can use the TCPDump utility to troubleshoot the Management Port.

1. Choose **Maintenance > Troubleshooting > Tools > TCP Dump**.
2. Select **Management Port**.

3. Configure the other available options as needed.
4. Click **Start Sniffing**.

#### Using Network Utilities to Test Connectivity

Secure Access Service provides a number of network utilities that you can use to test connectivity to the Management Port, including ARP, ping, traceroute, and NSlookup.

1. Choose **Maintenance > Troubleshooting > Tools > Commands**.
2. Select the command type from the Command drop down menu.
3. Configure the specific utility as needed.
4. Select **Management Port**.
5. Click **Ok**.

- Related Documentation**
- [Using the Management Port on a Cluster on page 836](#)

---

## Using the Management Port on a Cluster

The Management Port uses node-specific network settings, including the enable/disable settings. In effect, this means that you can combine different models of Secure Access Service devices in a cluster, but doing so may limit the use of the Management Port for the entire cluster.

The Management Port is not available on any appliance other than the SA6000 or SA6500 Series Appliance. If you enable the Management Port on a node that is an SA6000 or SA6500 Series Appliance, management traffic from that node travels over the Management Port. Traffic from non-SA6000 or SA6500 Series Appliance nodes, however, travels over the internal port.

- Related Documentation**
- [Troubleshooting the Management Port on page 835](#)

---

## Importing Configurations to a System with the Management Port Enabled

If you import a configuration from a system that does not support a management port into a system that has an enabled management port and you import everything, including licenses, the management port on the target system will appear to be removed. The management port actually continues to be operational and will reappear along with its original configuration when you reapply the management port license for the target system. If you import to the target but specify the Import everything except network settings and licenses option, the management port and its configuration persist on the target system and the port is operational.

- Related Documentation**
- [Troubleshooting the Management Port on page 835](#)



## CHAPTER 30

# Certificates

- [About Using Certificates on Secure Access Service on page 838](#)
- [Using Device Certificates on page 839](#)
- [Importing Certificates Into the Secure Access Service on page 840](#)
- [Downloading a Device Certificate From the Secure Access Service on page 842](#)
- [Creating a Certificate Signing Request \(CSR\) for a New Certificate on page 843](#)
- [Using Intermediate Server CA Certificates on page 844](#)
- [Importing Intermediate Server CA Certificates on page 845](#)
- [Using Multiple Secure Access Service Certificates on page 845](#)
- [Using a Trusted Client CA on page 846](#)
- [Automatically Importing an Intermediate Trusted Client CA Certificate on page 849](#)
- [Manually Uploading CA Certificates on page 851](#)
- [Specifying Attributes for the Trusted Client CA Certificate on page 853](#)
- [Specifying Client-side Certificate Restrictions on page 855](#)
- [Enabling Client CA Hierarchies on page 857](#)
- [Enabling CRLs on page 858](#)
- [Using a Proxy Server for CRL Downloads and OCSP Status Checks on page 860](#)
- [Specifying CDP Options on page 861](#)
- [Enabling OCSP on page 863](#)
- [Using Trusted Server CAs on page 864](#)
- [Uploading Trusted Server CA Certificates on page 865](#)
- [Renewing a Trusted Server CA Certificate on page 866](#)
- [Viewing Trusted Server CA Certificate Details on page 867](#)
- [Restoring the Prepopulated Group of Trusted Server CA Certificates on page 867](#)
- [Using Code-signing Certificates on page 868](#)
- [Task Summary: Configuring the Secure Access Service to Sign or Re-Sign Java Applets on page 869](#)
- [Importing a Code-Signing Certificate on page 870](#)
- [About Two-Way SSL Authentication on page 870](#)

- [Task Summary: Configuring the Secure Access Service for Two-Way SSL Authentication on page 871](#)
- [Importing the Certificates for Two-Way SSL Handshake on page 872](#)
- [Mapping Resource Policies to the Certificate on page 873](#)
- [Mapping an Client Authentication Auto-Policy on page 874](#)

## About Using Certificates on Secure Access Service

---

Secure Access Service uses *Public Key Infrastructure (PKI)* to secure the data that it sends to clients over the Internet. PKI is a security method that uses public and private keys to encrypt and decrypt information. These keys are enabled and stored through digital certificates. A digital certificate is an encrypted electronic file issued that establishes a Web server's or user's credentials for client-server transactions.

In public key cryptography, a public-private key pair is used to encrypt and decrypt data. Data encrypted with a public key, which the owner makes available to the public, can be decrypted with the corresponding private key only, which the owner keeps secret and protected.

For example, if Alice wants to send Bob an encrypted message, Alice can encrypt it with Bob's public key and send it to him. Bob then decrypts the message with his private key. The reverse process is also useful: encrypting data with a private key and decrypting it with the corresponding public key. This process is known as creating a digital signature. For example, if Alice wants to present her identity as the sender of a message, she can encrypt the message with her private key and send the message to Bob. Bob then decrypts the message with Alice's public key, thus verifying that Alice is indeed the sender.

Secure Access Service uses the following types of digital certificates to establish credentials and secure Secure Access Service session transactions:

- **Device certificates**—A device certificate helps to secure network traffic to and from Secure Access Service elements such as your company name, a copy of your company's public key, the digital signature of the certificate authority (CA) who issued the certificate, a serial number, and expiration date.
- **Trusted client CAs**—A trusted client CA is a client-side certificate issued by a certificate authority (CA) that allows you to control access to realms, roles, and resource policies based on certificates or certificate attributes. For example, you may specify that users must present a valid client-side certificate with the OU attribute set to "yourcompany.com" in order to sign into the "Users" authentication realm.
- **Trusted server CAs**—A trusted server CA is the certificate of a Web server that you trust. If you have a Web browsing license, you may install a trusted server CA on Secure Access Service in order to validate the credentials of the Web sites that users access through Secure Access Service.
- **Code-signing certificates**—A code-signing certificate (also called an applet certificate) is a type of server-side certificate that re-signs Java applets intermediated by Secure Access Service. You may use the self-signed code-signing certificate that comes pre-loaded on Secure Access Service, or you may install your own code-signing certificate.

In a basic setup, the only required certificates are a device certificate and a code-signing certificate. Secure Access Service can use a single code-signing certificate to resign all Java applets and a single device certificate to intermediate all other PKI-based interactions. If the basic certificates do not meet your needs, however, you may install multiple device and applet certificates on Secure Access Service or use trusted CA certificates to validate users.



NOTE:

- Secure Access Service can verify certificates that use SHA2 as the message digest.
- DSA certificates are currently not supported.

Certificate management features are an integral part of the Secure Access Service management framework—All Secure Access Service products include some certificate management features. If you are an SA700 Series administrator, however, note that trusted server CA and code-signing certificate administration features are only available if you have a Core Clientless Access upgrade license.

**Related Documentation**

- [Using Device Certificates on page 839](#)
- [Using a Trusted Client CA on page 846](#)
- [Using Trusted Server CAs on page 864](#)

## Using Device Certificates

A device certificate helps to secure network traffic to and from Secure Access Service using elements such as your company name, a copy of your company's public key, the digital signature of the certificate authority (CA) who issued the certificate, a serial number, and expiration date.

When receiving encrypted data from Secure Access Service, the client's browser first checks whether the Secure Access Service's certificate is valid and whether the user trusts the CA that issued the Secure Access Service's certificate. If the user has not already indicated that they trust the Secure Access Service's certificate issuer, the Web browser prompts the user to accept or install the Secure Access Service's certificate.

When you initialize Secure Access Service, it creates a temporary self-signed digital certificate locally that enables users to immediately begin using your Secure Access Service. Note that the encryption for the self-signed certificate created during initialization is perfectly safe, but users are prompted with a security alert each time they sign in to Secure Access Service because the certificate is not issued by a trusted certificate authority (CA). For production purposes, we recommend that you obtain a digital certificate from a trusted CA.

The Secure Access Service supports X.509 device certificates in DER and PEM encode formats (file extensions include .cer, .crt, .der, and .pem) as well as PKCS #12 (file

extensions include .pfx and .p12). The Secure Access Service also supports using the following additional features with device certificates:

- **Intermediate device CA certificates**—Within a certificate hierarchy, one or more intermediate certificates are branched off of a single root certificate.
- **Multiple device certificates**—When using multiple device certificates, each certificate handles validation for a separate host name or fully-qualified domain name (FQDN) and may be issued by a different CA.



**NOTE:** Beginning with Secure Access Service Release 7.2, you can assign device certificates to the Secure Access Service VLAN interfaces.

#### Related Documentation

- [About Using Certificates on Secure Access Service on page 838](#)
- [Importing Certificates Into the Secure Access Service on page 840](#)
- [Downloading a Device Certificate From the Secure Access Service on page 842](#)
- [Using Multiple Secure Access Service Certificates on page 845](#)

## Importing Certificates Into the Secure Access Service

### Importing an Existing Root Certificate and Private Key

You can create Web server certificates from servers such as Apache, IIS, Sun ONE (formerly iPlanet), or Netscape, and then import the certificate into the Secure Access Service. To export a digital server certificate and key, please follow your Web server's instructions for exporting certificates. Then, use the Device Certificates tab to import these files.



**NOTE:** When exporting a certificate from another Web server, note that it must be encrypted and you must export the password with the certificate.

You cannot import a Web server certificate's private key into a Secure Access Service FIPS device, since the key is created in a non-FIPS compliant environment. You may, however, import a certificate key from another Secure Access Service along with its security world.

To import an existing root server certificate and private key:

1. In the admin console, select **System > Configuration > Certificates > Device Certificates**.
2. Click **Import Certificate & Key**.



**NOTE:** This option is not available on FIPS platforms as importing private keys is not supported. On a FIPS system, you can only create a CSR and then import a signed certificate from the CSR. On the FIPS device, you must use the Configuration > Certificates > New CSR button to create a CSR. You pass the CSR request to an external CA, and then import the generated certificate file into the Pending Certificate Signing Request page.

The Configuration > Certificates > Device Certificate > Import Certificate and Key button is disabled on the FIPS device.

3. Select the appropriate form to import the certificate:
  - If the certificate and key are contained in one file, use the **If certificate file includes private key** form.
  - If the certificate and key are separate files, use the **If certificate and private key are separate files** form.
  - If the certificate and key are contained in a system configuration file, use the **Import via System Configuration file** form. When you choose this option, Secure Access Service imports all of the certificates specified in the configuration file into the Device Certificates page (including private keys and pending CSRs, but not the corresponding port mappings).
4. In the appropriate form, browse to the certificate and key file. If the file is encrypted, enter the password key.
5. Click **Import**.

#### Importing a Renewed Certificate That Uses the Existing Private Key

You can renew a device certificate in two ways:

- **Submit a new CSR to a CA**—This process of renewing a certificate is more secure, because the CA generates a new certificate and private key, retiring the older private key. To use this renewal method, you must first create a CSR through the admin console.



**NOTE:** You cannot import a Web server certificate's private key into an SA FIPS Series Appliance, since the key is created in a non-FIPS compliant environment.

- **Request renewal based on the CSR previously submitted to the CA**—This process of renewing a certificate is less secure, because the CA generates a certificate that uses the existing private key.

When ordering a renewed certificate, you must resubmit your original CSR or ensure that the CA has a record of the CSR that you submitted for your current certificate.

To import a renewed device certificate that uses the existing private key:

1. Follow your CA's instructions for renewing a certificate that you previously purchased through them.



**NOTE:** Ensure you specify the same information you used in the original CSR. Your CA uses this information to create a new certificate that corresponds to the existing key.

Even though you specify the same information used in the original CSR, your rootCA may have different serial numbers and keys from the original. You may need to support both new client and old client certificates during the transition period, which means that you will need to maintain two rootCA certificates (your existing cert and the renewed cert), at least temporarily

2. In the admin console, select **System > Configuration > Certificates > Device Certificates**.
3. If you want to renew an intermediate certificate, click the **Intermediate Device CAs** link at the top of the page.
4. Click the link that corresponds to the certificate that you want to renew.
5. Click **Renew Certificate**.
6. In the Renew the Certificate form, browse to the renewed certificate file, enter the password for the certificate key, and click **Import**.

#### Related Documentation

- [Using Multiple Secure Access Service Certificates on page 845](#)
- [Creating a Certificate Signing Request \(CSR\) for a New Certificate on page 843](#)
- [Downloading a Device Certificate From the Secure Access Service on page 842](#)
- [About Using Certificates on Secure Access Service on page 838](#)

## Downloading a Device Certificate From the Secure Access Service

If you create a SAML resource policy, for example, you must create a trust relationship between the Secure Access Service and your access management system. (Trust relationships ensure that SAML-enabled systems are only passing information to and from trusted sources.) If you choose to create a SAML SSO resource policy using a POST profile, part of creating a trust relationship involves installing the Secure Access Service's device certificate on the access management system. The Device Certificates page enables you to easily download the Secure Access Service's certificate so you can install it on your access management system.

To download a device certificate from the Secure Access Service:

1. In the admin console, choose **System > Configuration > Certificates > Device Certificates**.
2. Click the link that corresponds to the certificate that you want to save.

3. Click **Download**.
4. Browse to the location where you want to save the certificate and click **Save**.

**Related  
Documentation**

- [About Using Certificates on Secure Access Service on page 838](#)
- [Importing Certificates Into the Secure Access Service on page 840](#)
- [Creating a Certificate Signing Request \(CSR\) for a New Certificate on page 843](#)
- [Using Multiple Secure Access Service Certificates on page 845](#)

## Creating a Certificate Signing Request (CSR) for a New Certificate

If your company does not own a digital certificate for its Web servers, or if you are running a Secure Access Service FIPS device, you can create a CSR (certificate signing request) through the admin console and then send the request to a CA for processing. When you create a CSR through the admin console, a private key is created locally that corresponds to the CSR. If you delete the CSR at any point, this file is deleted, too, prohibiting you from installing a signed certificate generated from the CSR.



**NOTE:** Do not send more than one CSR to a CA at one time. Doing so may result in duplicate charges. You may view details of any pending requests that you previously submitted by clicking the Certificate Signing Request Details link in the Device Certificates tab.

To create a certificate signing request:

1. In the admin console, choose **System > Configuration > Certificates > Device Certificates**.
2. Click **New CSR**.
3. Enter the required information and click **Create CSR**.



**NOTE:** Generating a 2048-bit CSR on a FIPS hardware device (such as the SA6500 FIPS SSL VPN appliance) may take up to 10 minutes. Due to the nature of the FIPS hardware security module (HSM), access to the device is interrupted during the CSR generation. Juniper Networks recommends that CSR generation be performed during a maintenance window.

4. Follow the instructions on-screen, which explain what information to send to the CA and how to send it.
5. When you receive the signed certificate from the CA, import the certificate file using the instructions that follow.

When submitting a CSR to a CA authority, you may be asked to specify either the type of Web server on which the certificate was created or the type of Web server the certificate is for. Select **apache** (if more than one option with **apache** is available,

choose any). Also, if prompted for the certificate format to download, select the standard format.

### Importing a Signed Certificate Created From a CSR

To import a signed device certificate created from a CSR:

1. In the admin console, choose **System > Configuration > Certificates > Device Certificates**.
2. Under Certificate Signing Requests, click the **Pending CSR** link that corresponds to the signed certificate.
3. Under Import signed certificate, browse to the certificate file you received from the CA and then click **Import**.

#### Related Documentation

- [About Using Certificates on Secure Access Service on page 838](#)
- [Using Intermediate Server CA Certificates on page 844](#)

---

## Using Intermediate Server CA Certificates

Within a certificate hierarchy, one or more intermediate certificates are branched off of a single root certificate. The root certificate is issued by a root certificate authority (CA) and is self-signed. Each intermediate certificates is issued by the certificate above it in the chain.

If you are securing traffic using chained certificates, you must ensure that the Secure Access Service and Web browser together contain the entire certificate chain. For example, you may choose to secure traffic using a chain that stems from a Verisign root certificate. Assuming your users' browsers come pre-loaded with Verisign root certificates, you only need to install the lower-level certificates in the chain on the Secure Access Service. Then, when your users browse to Secure Access Service, Secure Access Service presents any required certificates within the chain to the browser in order to secure the transaction. (Secure Access Service creates the proper links in the chain using the root certificate's IssuerDN.) If the Secure Access Service and browser together do not contain the entire chain, the user's browser will not recognize or trust the Secure Access Service's device certificate since it is issued by another certificate instead of a trusted CA.

When installing certificates through Secure Access Service, you may install certificates in any order. Secure Access Service supports uploading one or more intermediate CAs in a PEM file.

#### Related Documentation

- [Importing Intermediate Server CA Certificates on page 845](#)
- [Enabling Client CA Hierarchies on page 857](#)



## Importing Intermediate Server CA Certificates

To import an intermediate device certificate and private key:

1. In the admin console, choose **System > Configuration > Certificates > Device Certificates**.
2. Click the **Intermediate Device CAs** link at the top of the page.
3. Click **Import CA certificate**.
4. Browse to the CA certificate that you want to upload to the Secure Access Service and click **Import Certificate**.

### Related Documentation

- [Enabling Client CA Hierarchies on page 857](#)
- [Using Intermediate Server CA Certificates on page 844](#)

## Using Multiple Secure Access Service Certificates

When using multiple Secure Access Service device certificates, each certificate handles validation for a separate host name or fully qualified domain name (FQDN) and may be issued by a different CA. You can use multiple root certificates in conjunction with multiple sign-in URLs. With the multiple sign-in URLs feature, you can provide access to the Secure Access Service from multiple host names by creating a different sign-in URL for each host name or FQDN. Then, you can create separate sign-in pages and authentication requirements for each sign-in URL. With the multiple device certificates feature, you can use different certificates to validate users signing into each of those host names or FQDNs. For example, you can associate one certificate with the `partners.yourcompany.com` site and another with the `employees.yourcompany.com` site.

### Task summary: Enabling Multiple Device Certificates

To enable multiple device certificates, you must:

1. Specify the IP addresses from which users may access the Infranet Controller and then create a virtual port for each. A virtual port activates an IP alias on a physical port. To create virtual ports for:
  - **Internal users**—Use settings in the **System > Network > Internal Port > Virtual Ports** tab to create virtual ports for users such as employees who are signing into the Secure Access Service from inside your internal network.
  - **External users**—Use settings in the **System > Network > Port 1 > Virtual Ports** tab to create virtual ports for users such as customers and partners who are signing into the Secure Access Service from outside of your internal network.
2. Upload your device certificates to the Secure Access Service. You can import certificates from the **System > Configuration > Certificates > Device Certificates** page of the admin console or the **Maintenance > Import/Export > System Configuration** page of the admin console. Upload one device certificate for each domain (host name) that you want to host on the Infranet Controller.

3. Specify which virtual ports the Secure Access Service should associate with the certificates using settings in the System > Configuration > Certificates > Device Certificates tab. When a user tries to sign into the Secure Access Service using the IP address defined in a virtual port, Secure Access Service uses the certificate associated with the virtual port to initiate the SSL transaction.

## Associating a Certificate With a Virtual Port

If you choose to associate multiple host names with a single Secure Access Service, you must specify which certificates the Secure Access Service should use to validate users signing in to the different host names. Options include:

- **Associate all host names with a single wildcard certificate**—With this method, you use a single wildcard certificate to validate all users, regardless of which host name they use to sign into the Secure Access Service. A wildcard certificate includes a variable element in the domain name, making it possible for users signing in from multiple hosts to map to the “same” domain. For example, if you create a wildcard certificate for `*yourcompany.com`, Secure Access Service uses the same certificate to authenticate users who sign into `employees.yourcompany.com` as it does to authenticate users who sign into `partners.yourcompany.com`.
- **Associate each host name with its own certificate**—With this method, you associate different host names with different certificates. Since Secure Access Service does not know the host name that the end-user uses to sign into the Secure Access Service, however, you must create a virtual port for each host name and then associate your certificates with the virtual ports. A virtual port activates an IP alias on a physical port. For example, you may choose to create two virtual ports on a single appliance, mapping the first virtual port to the IP address 10.10.10.1 (`sales.yourcompany.com`) and the second virtual port to the IP address 10.10.10.2 (`partners.yourcompany.com`). Then, you can associate each of these virtual ports with its own certificate, ensuring that the Secure Access Service authenticates different users through different certificates.

### Related Documentation

- [Importing Certificates Into the Secure Access Service on page 840](#)
- [Using Virtual Ports on page 802](#)

---

## Using a Trusted Client CA

This topic describes how to use a trusted client certificate authority with the Secure Access Service. It includes the following information:

- [About Trusted CAs on page 846](#)
- [Enabling Trusted Client CAs on page 848](#)
- [Limitations on page 849](#)

### About Trusted CAs

A *trusted client CA* is a certificate authority (CA) trusted by the Secure Access Service. The Secure Access Service trusts any certificate issued by that CA. To use client CA certificates, you must install and enable the proper certificates on the Secure Access

Service. Additionally, you must install the corresponding client-side certificates in the Web browsers of your end-users or use MMC Certificates snap in your users' computer accounts (machine certificate). When validating a client-side CA certificate, the Secure Access Service checks that the certificate is not expired or corrupt and that the certificate is signed by a CA that the Secure Access Service recognizes. If the CA certificate is chained (described below) the Secure Access Service also follows the chain of issuers until it reaches the root CA, checking the validity of each issuer as it goes. The Secure Access Service supports X.509 CA certificates in DER and PEM encode formats.

When installing a client-side certificate, you must determine whether you want to use the certificate to identify individual users or individual machines. To use the certificate to identify individual users, you must install the certificate in each user's individual certificate store. Then you must enable authentication through the Secure Access Service administration console using a certificate server or enable authorization using realm, role, and/or resource policy settings. To use the certificate to identify individual machines, you must install the certificate in each computer's certificate store. Then, you must configure a Host Checker policy that checks for the machine certificate and authorizes access to realms, roles, and/or resource policies based on the certificate's validity.



**NOTE:** If you have a user license, you can only install one root CA certificate on the Secure Access Service and validate users using one corresponding client-side CA certificate.

The Secure Access Service supports using the following additional features with CA certificates:

- **Certificate servers**—A certificate server is a type of local authentication server that allows you to authenticate Secure Access Service users based solely on their certificate attributes rather than authenticating them against a standard authentication server (such as LDAP or RADIUS), as well as requiring specific certificates or certificate attributes.
- **Certificate hierarchies**—Within a certificate hierarchy, one or more subordinate certificates (called intermediate certificates) are branched off of a root certificate creating a certificate chain. Each intermediate certificate (also called a chained certificate) handles requests for a part of the root CA's domain. For example, you may create a root certificate that handles all requests to the `yourcompany.com` domain and then branch off intermediate certificates that handle requests to `partners.yourcompany.com` and `employees.yourcompany.com`. When you install a chained certificate on the Secure Access Service, the appliance confirms that the chain is valid and allows users to authenticate using the leaf certificate (that is, the lowest certificate in the chain).
- **Certificate revocation lists**—Certificate revocation is a mechanism by which a CA invalidates a certificate before its expiration date. A certificate revocation list (CRL) is a list of revoked certificates published by a CA. Within CRLs, each entry contains the serial number of the revoked certificate, the date that the certificate was revoked, and the reason that the certificate was revoked. The CA may invalidate a certificate for various reasons such as the employee to whom the certificate is issued has left the

company, the certificate's private key is compromised, or the client-side certificate is lost or stolen. Once the CA revokes a certificate, the Secure Access Service can appropriately deny access to users who present a revoked certificate.

- OSCP (Online Certificate Status Protocol)—OCSP is an alternative to CRL. OSCP allows certificate status checking to be delegated to OSCP responders. When a user attempts to access a server, OSCP sends a request for certificate status information. The status is “current,” “expired,” or “unknown.”
- RFC 5280 Path Validation Settings—IETF RFC 5280 describes a sophisticated algorithm for path validation that permits CAs to be only partially trusted, as may be required in complex PKIs. When Advanced Certificate Processing Settings are configured, a new path validation library is employed that enforces RFC 5280 requirements.

## Enabling Trusted Client CAs

To require users to provide a client-side certificate to sign in to the Secure Access Service, upload the corresponding CA certificate into the Secure Access Service. You can upload CA certificates manually or configure the Secure Access Service to upload CA certificates automatically. If you have just a standard Secure Access Service user license, you can only import one CA certificate to the Secure Access Service.

When uploading a certificate chain to the Secure Access Service, you must either install the certificates one at a time in descending order starting with the root certificate (DER or PEM files), or you must upload a single file to the Secure Access Service that contains the entire certificate chain (PEM files only). By using one of these methods, you ensure that the Secure Access Service can link the certificates together in the correct order.

The Secure Access Service uses the uploaded certificate to verify that the browser-submitted certificate is valid. In addition, you can specify whether or not to automatically import CA certificates for validation and the CRL/OCSP retrieval method the Secure Access Service uses when automatically importing the CA certificates.

Uploading a CA certificate to the Secure Access Service does not enable client-side SSL authentication or authorization. To enable authentication and/or authorization, you must use a certificate server, or enable certificate restrictions at the realm, role, or resource policy level, or create a Host Checker policy that checks for a machine certificate.



**NOTE:** When using client-side certificates, we strongly recommend that you advise your users to close their Web browsers after signing out of the Secure Access Service. If they do not, other users may be able to use their open browser sessions to access certificate-protected resources on the Secure Access Service without re-authentication. After loading a client-side certificate, both Internet Explorer and Netscape cache the certificate's credentials and private key. The browsers keep this information cached until the user closes the browser (or in some cases, until the user reboots the workstation). For details, see <http://support.microsoft.com/?kbid=290345>. To remind users to close their browsers, modify the sign out message in the Authentication > Signing In > Sign-in Pages tab.

## Limitations

When using OCSP with an RSA Keon server, the device certificate used to sign the OCSP request must be issued by the RSA Keon server itself. Secure Access Service cannot use the CA certificate that signed the device certificate.

To use OCSP with an RSA Keon server:

1. From the Secure Access Service, generate a CSR for a server certificate. Use the New CSR button on the Configuration > Certificates > Device Certificates page.
2. Issue a CSR request to the RSA Keon certificate server and generate the server certificate.
3. Import the server certificate into the Secure Access Service Device Certificates store. Use the Configuration > Certificates > Device Certificates page.
4. Import the RSA Keon CA into the Secure Access Service Trusted Client CA store. Use the Configuration > Certificates > Trusted Client CAs page.
5. Configure the Trusted Client CA that you just imported:
  - a. Select **Use OCSP (Online Certification Status Protocol)** and click **Save Changes** to enable you to specify OCSP options.
  - b. Under OCSP Settings, click the **OCSP Options** button.
  - c. Under “Use,” select **Responder(s) specified in the CA certificate**.
  - d. Under “Device Certificate to sign the request,” select the server certificate you imported in Step 3. With this configuration, the client request is signed by the server certificate issued by the RSA Keon CA.

### Related Documentation

- [Configuring a Certificate Server Instance on page 174](#)
- [Task Summary: Configuring Sign In Pages on page 324](#)
- [Specifying Customized Requirements Using Custom Rules on page 394](#)
- [Enabling CRLs on page 858](#)
- [Enabling Client CA Hierarchies on page 857](#)
- [Specifying Client-side Certificate Restrictions on page 855](#)

## Automatically Importing an Intermediate Trusted Client CA Certificate

Secure Access Service must have access to the root CA certificate and the intermediate CA certificates in order to validate a client certificate during user authentication. You can manually import the intermediate CA certificates but this process becomes tedious if you have a large number intermediate CAs. In this case, you can use the auto-import feature which installs the CA certificates and configures the CDP/OCSP locations automatically from the client browser during user authentication.

To automatically import and specify options for an intermediate trusted client CA certificate on the Secure Access Service:

1. In the admin console, choose **System > Configuration > Certificates > Trusted Client CAs**.
2. Click **Auto-import options**. The Auto-import options page appears.
3. Click **Auto-import Trusted CAs**.
4. Under Client certificate status checking, specify the method the Secure Access Service uses to verify client certificate status:

- **None**—Specifies that the Secure Access Service should not validate this trusted client certificate.
- **Use OCSP**—Specifies that the Secure Access Service should use the OCSP method, validating the client certificate in real-time, as needed. After you select this option, you can specify options for OCSP.

If you select this option, you must manually configure the OCSP options and OCSP responders should it be necessary for the certificate to sign the OCSP request and the certificate to validate the OCSP response after the intermediate CA is imported and the OCSP responder is created for that CA.

- **Use CRLs**—Specifies that the Secure Access Service should use CRLs to validate the client certificate. After you select this option, you can specify options for OCSP.
- **Use OCSP with CRL fallback**—Specifies that the Secure Access Service should use the OCSP validation method when possible, but attempt to validate client certificates using CRLs should the OCSP method fail (for example, if the link to the OCSP Responder were to fail). After you select this option, you can specify options for OCSP.
- **Inherit from root CA**—Specifies that the certificate status check is inherited from the root CA. This allows you to use the same configuration in the root CA of the chain without having to configure the intermediate CAs for certificate status check.



**NOTE:** Changes to the root CA values after the intermediate CA client certificate has already inherited its configuration (from the root CA) are not pushed to the intermediate CA. Intermediate CAs must be reconfigured to obtain the new values.



**NOTE:** When you select **Inherit from root CA**, options under CDP(s)/OCSP responder are ignored.

5. Under CDP(s)/OCSP responder, specify the CRL/OCSP retrieval method from the associated drop-down list:
  - **None**—Specifies that the Secure Access Service does not to use a CRL/OCSP retrieval method.

- **From client certificate**—Specifies that the Secure Access Service use a CRL/OCSP retrieval method found in the client certificate.
  - **From trusted CA certificates**—Specifies that the Secure Access Service use a CRL/OCSP retrieval method found in the intermediate trusted client CA certificate.
6. Enable the **Verify imported CA certificates** option if you want the Secure Access Service to validate the CRL from which the certificate is issued.
  7. Click **Save**.
  8. Use one of the following methods to specify how the Secure Access Service should use the certificate to authenticate users and/or authorize access to resources:
    - Use a certificate server to authenticate individual users.
    - Use realm, role, and resource policy settings to authorize individual users access to resources.
    - Use a Host Checker policy to authorize individual machines to access resources.



**NOTE:** For intermediate trusted client CA certificates to be auto imported, the root CA certificate already needs to be available under trusted client CAs in Secure Access Service.

## Manually Uploading CA Certificates

To manually upload CA certificates to the Secure Access Service:

1. Install a client-side user certificate or machine certificate through the user's Web browser. For help, see the instructions provided with the browser.
2. In the admin console, choose **System > Configuration > Certificates > Trusted Client CAs**.
3. Click **Import CA Certificate**. The Import Trusted Client CA page appears.
4. Browse to the CA certificate that you want to upload to the Secure Access Service and click **Import Certificate**.
5. Under Client certificate status checking, specify the method the Secure Access Service uses to verify client certificate status:
  - **None**—Specifies that the Secure Access Service should not validate this trusted client certificate.
  - **Use OCSP**—Specifies that the Secure Access Service should use the OCSP method, validating the client certificate in real-time, as needed. After you select this option, you can specify options for OCSP.
  - **Use CRLs**—Specifies that the Secure Access Service should use CRLs to validate the client certificate. After you select this option, you can specify options for OCSP.
  - **Use OCSP with CRL fallback**—Specifies that the Secure Access Service should use the OCSP validation method when possible, but attempt to validate client

certificates using CRLs should the OCSP method fail (for example, if the link to the OCSP Responder were to fail). After you select this option, you can specify options for OCSP and for CDP.

6. Enable the **Verify Trusted Client CA** option if you want the Secure Access Service to validate the CRL from which the certificate is issued.
7. Enable the **Trusted for Client Authentication?** option if you want the Secure Access Service to trust this certificate when authenticating client certificates. If you added this certificate for non-authentication purposes (such as for SAML signature verification or machine certificate validation), disable this option, indicating that the Secure Access Service should not trust any client certificate issued by this CA. If this option is enabled, it must be enabled for all of the certificates that are part of the certificate chain of trust, or the client can not successfully log in.
8. Enable **Participate in Client Certificate Negotiation** to have the CA participate in client certificate selection for authentication. In client certificate authentication or restriction, the Secure Access Service sends a list of all trusted client CAs configured in the trusted client CA store with this flag enabled to the user's browser for user certificate selection. The browser prompts the client certificates whose issuer CA and/or root CA is in that list. This option allows you to control which client certificate(s) are prompted for selection. Deselecting this option for all certificates in a CA chain results in those certificates not being prompted. This flag is disabled if the CA certificate is not intended for client authentication (when Trusted for Client Authentication is de-selected). This flag is enabled by default.



**NOTE:** If the number of trusted client CAs is greater than zero and the CA list for negotiation is zero (empty), the browser sends all available client certificates for selection. To eliminate a particular CA from being used in client certificate negotiation, you need to either mark that CA as untrusted or have a non-empty CA list in the negotiation.

9. Select options under Advanced Certificate Processing Settings for complex PKI deployments with client certificate authentication.
  - **Initial Inhibit Policy Mapping**—Select this option to reject paths where policy mapping is required.
  - **Initial Policy Set**—Enter a sequence of certificate policy Object Identifiers, for example, 2.5.29.32.0, separated by newlines. Leave this field blank if you want all policies.
  - **Initial Require Explicit Policy**—Select this checkbox to require the path to be valid for at least one of the certificate policies listed in Initial Policy Set.





**NOTE:** Please note the following about the options under Advanced Certificate Processing Settings.

- These are options are global settings. If you enable these settings from any Root CA, the Secure Access Service uses RFC 5280 conforming certificate path validation checking for all the client certs from any imported Root CA.
- You must ensure sure the whole certificate chain (including all the intermediate CA certificates) is imported into the Secure Access Service before enabling these advanced settings. Otherwise, the client cert authentication will fail.
- The Auto Import of Intermediate CA Certificates option is ignored after you enable options under Advanced Certificate Processing Settings.

10. Click **Save Changes**.

After you have manually imported the CA certificate, you can specify CA certificate attributes.

11. Use one of the following methods to specify how the Secure Access Service should use the certificate to authenticate users and/or authorize access to resources:
- Use a certificate server to authenticate individual users.
  - Use realm, role, and resource policy settings to authorize individual users access to resources.
  - Use a Host Checker policy to authorize individual machines to access resources.

**Related Documentation**

- [Specifying Client-side Certificate Restrictions on page 855](#)
- [Specifying CDP Options on page 861](#)
- [Using a Trusted Client CA on page 846](#)
- [Specifying Attributes for the Trusted Client CA Certificate](#)

## Specifying Attributes for the Trusted Client CA Certificate

To specify attributes for the trusted client CA certificate:

1. In the admin console, choose **System > Configuration > Certificates > Trusted Client CAs**.
2. Click the certificate that you want to view. The Trusted Client CA page appears displaying all of the information about the certificate you selected.
3. Under Certificate, use the arrow next to the following field names to view certificate details:

- **Issued To**—Name and attributes of the entity to whom the certificate is issued.
  - **Issued By**—Name and attributes of the entity that issued the certificate. Note that the value of this field should either match the Issued To field (for root certificates) or the Issued To field of the next certificate up in the chain (for intermediate certificates).
  - **Valid Dates**—Time range that the certificate is valid.
  - **Details**—Includes various certificate details, including its version, serial number, signature algorithm, CRL distribution points, public key algorithm type, and the public key. Note that although the Secure Access Service may display a CRL distribution point in the Details field, it does not check the CDP unless you enable it.
4. If you want to renew the certificate:
    - a. Click **Renew Certificate**.
    - b. Browse to the renewed CA certificate that you want to upload to the Secure Access Service and click **Import Certificate**.
  5. Under CRL checking for client certificates, view details about the CRL(s) that are enabled for this certificate:
    - **Enable**—Displays a check mark if the Secure Access Service is configured to use the CRL from this CDP.
    - **CRL Distribution Points**—Location of the CRL distribution point against which the client certificates are validated. This field also indicates whether or not the last attempt to download the CRL from the CDP was successful or not.
    - **Status**—Indicates the status of the CRL (OK, No CRL, Expired, Download in progress), the CRL size, and the number of revocations contained in the CRL.
    - **Last Updated**—Indicates the last time the Secure Access Service downloaded a CRL from the specified CRL distribution point. Also contains a link that allows you to save the Secure Access Service's current version of the CRL.
    - **Next Update**—Indicates the next download time based on the interval specified in the CRL distribution point. Note that a download interval is specified both in the CRL and in the Secure Access Service CRL configuration page (as the CRL Download Frequency)—the actual download time is the shorter of the two intervals, regardless of what is displayed in the Next Update column.
  6. In the Client Certificate Status Checking section, specify the method the Secure Access Service uses to validate the client certificate:
    - **None**—Specifies that the Secure Access Service should not validate this trusted client certificate.
    - **Use OCSP**—Specifies that the Secure Access Service should use the OCSP method, validating the client certificate in real-time, as needed. After you select this option, you can specify options for OCSP.
    - **Use CRLs**—Specifies that the Secure Access Service should use CRLs to validate the client certificate. After you select this option, you can specify options for OCSP.

- **Use OCSP with CRL fallback**—Specifies that the Secure Access Service should use the OCSP validation method when possible, but attempt to validate client certificates using CRLs should the OCSP method fail (for example, if the link to the OCSP Responder were to fail). After you select this option, you can specify options for OCSP.
- **Inherit from root CA**—Specifies that the certificate status check is inherited from the root CA. This allows you to use the same configuration in the root CA of the chain without having to configure the intermediate CAs for certificate status check.



**NOTE:** This option is disabled in this window. To inherit certificate status checks from the root CA, you must select **Inherit from root CA** under **Auto-Import Options**.

7. Enable the **Verify Trusted Client CA** option to instruct the Secure Access Service to validate the trusted client CA.
8. Click **Save Changes**.

#### Related Documentation

### Specifying Client-side Certificate Restrictions

Use a certificate restriction to require client machines to possess a valid client-side certificate in order to access the Secure Access Service sign-in page, be mapped to a role, or access a resource. If you use this feature, make sure that you import a CA certificate to verify the client-side certificate. To maximize the security of this feature, make sure that a user's client settings are set to require the user to enter a password each time the user signs in. The default setting for some browser versions is to remember the certificate password, which means the user won't be prompted for this additional sign-in information after installing the certificate.

To specify certificate restrictions:

1. Navigate to: **System > Configuration > Certificates > Trusted Client CAs** and specify the root certificate authority that you want to use to validate the client-side certificate restrictions that you enable at the realm, role, and resource policy levels.
2. Select the level at which you want to implement certificate restrictions:
  - **Realm level**—Navigate to:
    - **Administrators > Admin Realms > Select Realm > Authentication Policy > Certificate**
    - **Users > User Realms > Select Realm > Authentication Policy > Certificate**
  - **Role level**—Navigate to:
    - **Administrators > Admin Roles > Select Role > General > Restrictions > Certificate**

- **Users > User Realms > *Select Realm* > Role Mapping > Select|Create Rule > Custom Expression**
  - **Users > User Roles > *Select Role* > General > Restrictions > Certificate**
  - **Resource policy level**—Navigate to: Users > Resource Policies > Select Resource > Select Policy > Detailed Rules > Select|Create Rule > Condition Field
3. Select one of the following options:
- **Allow all users (no client-side certificate required)**—Does not require a user's client to have a client-side certificate.
  - **Allow all users and remember certificate information while user is signed in**—Does not require a user's client to have a client-side certificate, but if the client does have a certificate, the Secure Access Service remembers the certificate information during the entire user session.
  - **Only allow users with a client-side certificate signed by Trusted Client CAs to sign in**—Requires a user's client to have a client-side certificate in order to satisfy the access management requirement. To restrict access even further, you can define unique certificate attribute-value pairs. Note that the user's certificate must have all the attributes you define.
4. Add a certificate field name and an expected value to optionally require specific values in the client certificate. You can specify variables in the Expected Value field. For example, you can add the value *uid* to the Certificate field and `<userAttr.uid>` to the Expected Value field.



**NOTE:** The user attribute can come from any authentication server that supports attributes. Any attribute name specified in a certificate restriction must be included in the server catalog so the values are collected during authentication and added to the session context data.

5. Click **Save Changes** to save your settings.



## NOTE:

- The Secure Access Service supports all X.509 Distinguished Name (DN) attributes (such as C, CN, L, O, OU).
- The attribute and value fields are not case-sensitive.
- Define only one value for each attribute. If you specify multiple values, the client-side certificate may not authenticate correctly against the CA certificate.
- The Secure Access Service currently recognizes an e-mail address in the subjectAltName attribute in a certificate.
- The Secure Access Service can extract the User Principal Name (UPN) from the subjectAltName attribute. The Secure Access Service locates a specific UPN Object Identifier (OID) in the certificate and decodes the value. To represent the UPN in the subjectAltName attribute, use the token <certAttr.altName.UPN>

**Related  
Documentation**

- [Role Restrictions on page 110](#)
- [Creating an Authentication Realm on page 306](#)

## Enabling Client CA Hierarchies

Within a certificate hierarchy, one or more intermediate certificates are branched off of a single root certificate. The root certificate is issued by a root certificate authority (CA) and is self-signed. Each intermediate certificate is issued by the certificate above it in the chain.

To enable authentication in a chained certificate environment, you must install the appropriate client-side certificates in each user's Web browser and then upload the corresponding CA certificates to the Secure Access Service.



**NOTE:** With a user license, you cannot install a chain whose certificates are issued by different CAs. The CA that signs the lowest-level certificate in the chain must also sign all other certificates in the chain.

You can install client CAs through the System > Configuration > Certificates > Trusted Client CAs page of the admin console. When uploading the certificate chain to the Secure Access Service, you must use one of the following methods:

- **Import the entire certificate chain at once**—When installing a chain of certificates contained in a single file, the Secure Access Service imports the root certificate and any sub-certificates whose parents are in the file or on the Secure Access Service. You can include certificates in any order in the import file.

- **Import the certificates one at a time in descending order**—When installing a chain of certificates contained in multiple files, the Secure Access Service requires that you install the root certificate first, and then install the remaining chained certificates in descending order.

When you install chained certificates using one of these methods, the Secure Access Service automatically chains the certificates together in the correct order and displays them hierarchically in the admin console.



**NOTE:** If you install multiple certificates in a user's Web browser, the browser prompts the user to choose which certificate to use whenever he signs into the Secure Access Service.

**Related  
Documentation**

- [Using Intermediate Server CA Certificates on page 844](#)

## Enabling CRLs

A *certificate revocation list (CRL)* is a mechanism for cancelling a client-side certificate. As the name implies, a CRL is a list of revoked certificates published by a CA or delegated CRL issuer. The Secure Access Service supports base CRLs, which include all of the company's revoked certificates in a single, unified list.

The Secure Access Service knows which CRL to use by checking the client's certificate. (When issuing a certificate, the CA includes CRL information for the certificate in the certificate itself.) To ensure that it receives the most up-to-date CRL information, the Secure Access Service periodically contacts a CRL distribution point to get an updated list of revoked certificates. A CRL distribution point (CDP) is a location on an LDAP directory server or Web server where a CA publishes CRLs. The Secure Access Service downloads CRL information from the CDP at the interval specified in the CRL, at the interval that you specify during CRL configuration, and when you choose to manually download the CRL. The Secure Access Service also supports CRL partitioning. CRL partitioning enables you to verify portions of very large CRLs without having to spend the time and bandwidth necessary to access and validate a very large CRL or collection of large CRLs. CRL partitioning is only enabled on the Secure Access Service when you employ the Specify the CDP(s) in the client certificates method (described below). In this case, the Secure Access Service validates the user by verifying only the CRL specified in the client certificate.

Although CAs include CRL information in client-side certificates, they do not always include CDP information, as well. A CA may use any of the following methods to notify the Secure Access Service of a certificate's CDP location:

- **Specify the CDP(s) in the CA certificate**—When the CA issues a CA certificate, it may include an attribute specifying the location of the CDP(s) that the Secure Access Service should contact. If more than one CDP is specified, the Secure Access Service chooses the first one listed in the certificate and then fails over to subsequent CDPs, if necessary.

- **Specify the CDP(s) in the client certificates**—When the CA issues client-side certificates, it may include an attribute specifying the location of the CDP(s) that the Secure Access Service should contact. If more than one CDP is specified, the Secure Access Service chooses the first one listed in the certificate and then fails over to subsequent CDPs, if necessary. When the Secure Access Service employs CRL partitioning and the client certificate specifies only one CRL, the Secure Access Service performs verification using only that CRL.



**NOTE:** If you choose this method, the user receives an error the first time he tries to sign into the Secure Access Service because no CRL information is available. Once the Secure Access Service recognizes the client's certificate and extracts the CRL location, it can start downloading the CRL and subsequently validate the user's certificate. In order to successfully sign into the Secure Access Service, the user must try to reconnect after a few seconds.

- **Require the administrator to manually enter the CDP location**—If the CA does not include the CDP location in the client or CA certificates, you must manually specify how to download the entire CRL object when configuring the Secure Access Service. You may specify a primary and backup CDP. (Manually entering the CDP location provides the greatest flexibility because you do not need to reissue certificates if you change your CDP location.)

The Secure Access Service checks the user's certificate against the appropriate CRL during authentication. If it determines that the user's certificate is valid, the Secure Access Service caches the certificate attributes and applies them if necessary during role and resource policy checks. If it determines that the user's certificate is invalid, if it cannot contact the appropriate CRL, or if the CRL is expired, the Secure Access Service denies the user access.

You can configure CRL checking through the **System > Configuration > Certificates > Trusted Client CAs** page of the admin console.



**NOTE:**

- The Secure Access Service only supports CRLs that are in a PEM or DER format and that are signed by the CA for which the revocations apply.
- The Secure Access Service only saves the first CRL in a PEM file.
- The Secure Access Service does not support the Issuing Distribution Point (IDP) CRL extension.

**Related Documentation**

- [Specifying CDP Options on page 861](#)

## Using a Proxy Server for CRL Downloads and OCSP Status Checks

You can configure the system to send CRL download requests and OCSP status checks to the proxy server and collect the response. You might want to do this if you deploy proxy server to control access to the Internet.

The following types of CRL downloads can use the proxy server:

- CDPs specified in the trusted client CAs
- CDPs specified in client certificates
- Manually configured CDPs



**NOTE:** Once you configure a proxy, any CRL download initiated from the system goes through the configured proxy server.

CRL download through proxy is only for web-based URLs, not LDAP URLs.

Similarly, the system can send OCSP requests to the OCSP responder through the proxy server. The OCSP responses are also received through the proxy server. This feature is useful when you deploy a large number of Pulse access systems and the OCSP responders are located outside the network.

Figure 52: Defining Proxy Settings

The screenshot shows the configuration page for Trusted Client CAs, specifically the Proxy Settings section. The breadcrumb navigation is Configuration > Trusted Client CAs > Proxy Settings. There are two checkboxes: 'Use Proxy Server for HTTP-based CRL download' (unchecked) and 'Use Proxy Server for HTTP-based OCSP status checking' (checked). Below this is a section titled 'Proxy Server' with the following fields: '\* Host Address:' (required), '\* Port:' (set to 80), and a note 'Address can be a fully qualified domain name (e.g. "proxy.net") or an IP.'. There are also fields for 'Username:' and 'Password:'. A legend at the bottom indicates '\* indicates required field'.

To use a proxy server:

1. In the admin console, choose **System > Configuration > Certificates > Trusted Client CAs**.
2. Click **Proxy Settings**.



3. Select the **Use Proxy Server for HTTP-based CRL download** or **Use Proxy Server for HTTP-based OCSP status checking** checkbox.
4. Enter the proxy server hostname. You can specify either an IP address or a fully qualified domain name.
5. Enter the proxy server port number if it is different from the default value of 80.
6. (optional) If your proxy server required authentication, enter a username and password to log in to the proxy server.

## Specifying CDP Options

If you selected either Use CRLs or Use OCSP with CRL fallback. You can enable and periodically download certificate revocation lists (CRL) from *CRL distribution points* (CDPs) to verify the ongoing validity of client-side certificates.

1. In the admin console, choose **System > Configuration > Certificates > Trusted Client CAs**.
2. Click the link that corresponds to the certificate for which you want to enable CRL checking.



**NOTE:** Since the Secure Access Service supports CRL partitioning, you may see multiple CRLs displayed under CRL distribution points. This is because the partitioned portions of a revocation list are not identified individually, but referred to as the CDP from which they are derived.

3. Click **CRL Checking Options**. The CRL Checking Options page appears.
4. Under CRL Distribution Points, specify where the Secure Access Service should find access information for the CDP. Options include:
  - **No CDP (no CRL Checking)**—When you select this option, the Secure Access Service does not check CRLs issued by the CA, so you do not need to enter any parameters to access the CDP that issued the CRL.
  - **CDP(s) specified in the Trusted Client CA**—When you select this option, the Secure Access Service checks the CRL distribution point attribute in the certificate and displays the URIs of the CDPs that it finds in the CRL Checking Options page. If the CA certificate does not include all of the information required to access the CDP, specify the additional required information:
    - **CDP Server: (LDAP only)**—Enter the location of the CDP server. When using LDAP protocol, enter the IP address or host name (for example, ldap.domain.com).
    - **CRL Attribute: (LDAP only)**—Enter the LDAP attribute on the object that contains the CRL (for example, CertificateRevocationList).
    - **Admin DN, Password: (LDAP only)**—If the CDP server does not allow anonymous searches of the CRL, enter the admin DN and password that are required to authenticate into the CDP server.

- **CDP(s) specified in client certificates**—If the client certificate does not include all of the information required to access the CDP, specify the additional required information:
  - **CDP Server: (LDAP only)**—Enter the location of the CDP server. When using LDAP protocol, enter the IP address or host name (for example, ldap.domain.com).
  - **CRL Attribute: (LDAP only)**—Enter the LDAP attribute on the object that contains the CRL (for example, CertificateRevocationList).
  - **Admin DN, Password: (LDAP only)**—If the CDP server does not allow anonymous searches of the CRL, enter the admin DN and password that are required to authenticate into the CDP server.
- **Manually configured CDP**—When you select this option, the Secure Access Service accesses the CDP that you specify. Enter the URL of the primary CDP and optionally of a backup CDP. For an LDAP server, use the syntax: ldap://Server/BaseDN?attribute?Scope?Filter. For a Web server, enter the complete path to the CRL object. For example:  
http://domain.com/CertEnroll/CompanyName%20CA%20Server.crl  
Additionally, if the CDP server does not allow anonymous searches of the CRL, enter the admin DN and password that are required to authenticate into the CDP server. (LDAP only)



**NOTE:** If you choose to download CDPs using one method and then select a different method, the Secure Access Service deletes any CDPs from disk that were downloaded using the previous method.

5. In the **CRL Download Frequency** field, specify how often the Secure Access Service should download the CRL from the CDP. The allowable range is from 1 to 9999 hours.
6. Click **Save Changes**.
7. If you want to check the validity of your CA certificate (in addition to client-side certificates) against the CRL specified in the previous steps, select **Verify Trusted Client CA on the Trusted Client CA** page.



**NOTE:**

- When you choose to verify an intermediate certificate, make sure that CRLs are available for all of the CA certificates that are above the intermediate certificate in the chain—when verifying a CA certificate, the Secure Access Service also verifies all issuing CAs above the certificate in the chain.
- If you select this option but do not enable CRL checking, the Secure Access Service checks the CA certificate against the CDP for the CA's issuer. If no CRL is enabled for the issuer, user authentication fails.

8. Click **Save Changes**. The Secure Access Service downloads the CRL using the method you specified (if applicable) and displays CRL checking details (described in the following section).
9. Click **Update Now** in the Trusted Client CA page to manually download the CRL from the CDP (optional).

**Related  
Documentation**

- [Specifying Attributes for the Trusted Client CA Certificate](#)
- [Enabling CRLs on page 858](#)

## Enabling OCSP

The *Online Certification Status Protocol (OCSP)* offers you the ability to verify client certificates in real-time. Using OCSP, the Secure Access Service becomes a client of an OCSP responder and forwards validation requests for users, based on client certificates. The OCSP responder maintains a store of CA-published CRLs and maintains an up-to-date list of valid and invalid client certificates. Once the OCSP responder receives a validation request from the Secure Access Service (which is commonly an HTTP or HTTPS transmission), the OCSP responder either validates the status of the certificate using its own authentication database or calls upon the OCSP responder that originally issued the certificate to validate the request. After formulating a response, the OCSP responder returns the signed response to the Secure Access Service and the original certificate is either approved or rejected, based on whether or not the OCSP responder validates the certificate.

### Specifying OCSP Options

If you selected either **Use OCSP** or **Use OCSP with CRL fallback**, the Secure Access Service displays a list of known OCSP responders and enables you to configure OCSP responder options:

1. Delete, enable, or disable OCSP Responder configuration using the **Delete**, **Enable**, or **Disable** buttons, respectively.
2. If you want to configure OCSP options, click **OCSP Options**. The OCSP Options page appears.
3. Specify the type of OCSP responder the Secure Access Service uses to validate trusted client CAs in the **Use** drop-down list:
  - **None**—The Secure Access Service does not use OCSP to verify the status of certificates issued by this CA.
  - **Responder(s) specified in the CA certificate**—The Secure Access Service uses OCSP responders specified in the imported client CA to perform verification. When you select this option, the Secure Access Service displays a list of OCSP responders specified in the imported CA (if any) and the last time they were used.
  - **Responder(s) specified in the client certificates**—The Secure Access Service uses responders specified during client authentication to perform verification. When you

select this option, the Secure Access Service displays a list of known OCSP responders (if any) and the last time they were used.

- **Manually configured responders**—The Secure Access Service uses primary and secondary OCSP responders at the addresses you specify.



**NOTE:** A *nonce* is random data the Secure Access Service includes in an OCSP request and the OCSP Responder returns in the OCSP response. The Secure Access Service compares the nonce in the request and response to ensure that the response is generated by the OCSP responder. If the two do not match, the Secure Access Service disregards the response and sends a new request. Nonces are a common way of prevent replay attacks.

4. Click **Save Changes**.

#### Specifying OCSP Responder Options

To specify OCSP Responder Signer Certificate options for one or more OCSP responders:

1. Click the name of the OCSP responder you want to configure in the OCSP responders list. The option specification page for the OCSP responder appears.
2. Browse to the network path or local directory location of a Responder Signer Certificate. This is the certificate the OCSP responder uses to sign the response. You must specify the Responder Signer Certificate if the signer certificate is not included in the response
3. If you want to allow an OCSP responder certificate that matches the responder signer certificate, activate the **Trust Responder Certificate** checkbox.
4. Enable the **Revocation Checking** option to ensure that the certificate the Secure Access Service and OCSP responder are using has not recently been revoked. This option only has any implications if you specified the Use OCSP with CRL fallback option.
5. Specify a clock discrepancy value in the **Allow clock discrepancy** field to account for possible mismatches in timestamps between the Secure Access Service and the OCSP responder. If the mismatch is significant enough, the Secure Access Service simply disregards the response from the OCSP responder as out-of-date or expired.
6. Click **Save Changes**.

#### Related Documentation

- [Specifying Attributes for the Trusted Client CA Certificate](#)

## Using Trusted Server CAs

If you have a Web browsing license, you may validate the credentials of the Web sites that users access through the Secure Access Service. You must simply install the CA certificate of the Web servers that you trust on the Secure Access Service.

Then, whenever a user visits an SSL-enabled Web site, the Secure Access Service verifies that:

- The Web site's certificate is issued by one of the trusted root CA chains installed on the Secure Access Service.
- The Web site's certificate is not expired.
- The Web site's certificate Subject CN value matches the actual host name of the accessed URL. (Note that the Secure Access Service allows the Subject CN value to contain wildcards in the format: \*company.com.)

If any of these conditions are not met, the Secure Access Service logs a major event to the user access log and allows or denies the user access to the Web site based on role-level settings that you have configured through the Users > User Roles > *Select Role* > Web > Options tab of the admin console. (If you do not configure these settings, the Secure Access Service warns the user that the Web site's certificate is invalid, but still allows him to access the site.)



**NOTE:** The Secure Access Service System > Configuration > Certificates > Trusted Server CAs page is prepopulated with all of the trusted root CAs for the Web certificates installed in Internet Explorer 7.0 and Windows XP service pack 2. When you upgrade to Secure Access Service Release 7.2, the previous group of prepopulated Trusted Server CAs are overwritten with the new group. Any Trusted Server CAs you had imported manually are unaffected. They remain available to you and included in the Trusted Servers CAs list.

#### Related Documentation

- [Uploading Trusted Server CA Certificates on page 865](#)
- [Renewing a Trusted Server CA Certificate on page 866](#)
- [Restoring the Prepopulated Group of Trusted Server CA Certificates on page 867](#)
- [Configuring Virus Signature Version Monitoring and Patch Assessment Data Monitoring on page 388](#)
- [Using Third-party Integrity Measurement Verifiers on page 405](#)

## Uploading Trusted Server CA Certificates

The Secure Access Service System > Configuration > Certificates > Trusted Server CAs page is prepopulated with all of the trusted root CAs for the Web certificates installed in Internet Explorer 7.0 and Windows XP service pack 2. You can use the import functionality on this page to import additional trusted server CA certificates.

The Secure Access Service supports X.509 CA certificates in PEM (Base 64) and DER (binary) encode formats. Note that you should also specify what the Secure Access Service should do in cases where a user tries to access an untrusted Web site.



---

**NOTE:**

- When uploading a certificate chain to the Secure Access Service, you must either install the certificates one at a time in descending order starting with the root certificate (DER or PEM files), or you must upload a single file to the Secure Access Service that contains the entire certificate chain (PEM files only). By using one of these methods, you ensure that the Secure Access Service can link the certificates together in the correct order.
  - The Secure Access Service does not support CRL revocation checks for trusted server CA certificates.
- 

To upload CA certificates to the Secure Access Service:

1. In the admin console, choose **System > Configuration > Certificates > Trusted Server CAs**.
2. Click **Import Trusted Server CA**.
3. Browse to the CA certificate that you want to upload to the Secure Access Service and click **Import Certificate**.

**Related Documentation**

- [Using Trusted Server CAs on page 864](#)
- [Renewing a Trusted Server CA Certificate on page 866](#)
- [Restoring the Prepopulated Group of Trusted Server CA Certificates on page 867](#)

---

## Renewing a Trusted Server CA Certificate

---

If one of your trusted Web sites renews its certificate, you must upload the renewed certificate to the Secure Access Service as well.

To import a renewed CA certificate into the Secure Access Service:

1. In the admin console, choose **System > Configuration > Certificates > Trusted Server CAs**.
2. Click the link that corresponds to the certificate that you want to renew.
3. Click **Renew Certificate**.
4. Browse to the renewed CA certificate that you want to upload to the Secure Access Service and click **Import Certificate**.

**Related Documentation**

- [Using Trusted Server CAs on page 864](#)
- [Uploading Trusted Server CA Certificates on page 865](#)
- [Restoring the Prepopulated Group of Trusted Server CA Certificates on page 867](#)

---

## Viewing Trusted Server CA Certificate Details

---

You can view a variety of details about each of the CA certificates installed on the Secure Access Service.

To view trusted server CA certificate details:

1. In the admin console, choose **System > Configuration > Certificates > Trusted Server CAs**.
2. Click the certificate that you want to view.
3. Under Certificate, use the arrow next to the following field names to view certificate details:
  - **Issued To**—Name and attributes of the entity to whom the certificate is issued.
  - **Issued By**—Name and attributes of the entity that issued the certificate. Note that the value of this field should either match the Issued To field (for root certificates) or the Issued To field of the next certificate up in the chain (for intermediate certificates).
  - **Valid Dates**—Time range that the certificate is valid.
  - **Details**—Includes various certificate details, including its version, serial number, signature algorithm, CRL distribution points, public key algorithm type, and the public key. (Note that the Secure Access Service does not support CRL checking for trusted server CA certificates.)

### Related Documentation

- [Using Trusted Server CAs on page 864](#)
- [Uploading Trusted Server CA Certificates on page 865](#)
- [Renewing a Trusted Server CA Certificate on page 866](#)
- [Restoring the Prepopulated Group of Trusted Server CA Certificates on page 867](#)

---

## Restoring the Prepopulated Group of Trusted Server CA Certificates

---

The Secure Access Service System > Configuration > Certificates > Trusted Server CAs page is prepopulated with all of the trusted root CAs for the Web certificates installed in Internet Explorer 7.0 and Windows XP service pack 2. You can use the delete functionality on this page to delete CAs and the reset functionality to restore the list to the set that was installed during the upgrade to Secure Access Service Release 7.2. The reset operation clears all manually imported certificates.

To restore the prepopulated group of trusted CA certificates:

1. In the admin console, choose **System > Configuration > Certificates > Trusted Server CAs**.
2. Click **Reset Trusted Server CAs**.

3. Confirm that you want to restore the set of trusted server CAs that was installed when you upgraded to Release 7.2.

The Secure Access Service restores the group of prepopulated trusted server CAs that were installed upon upgrade to Release 7.2. This operation clears all manually imported certificates.

**Related  
Documentation**

- [Using Trusted Server CAs on page 864](#)
- [Renewing a Trusted Server CA Certificate on page 866](#)
- [Uploading Trusted Server CA Certificates on page 865](#)

---

## Using Code-signing Certificates

---

When the Secure Access Service intermediates a signed Java applet, the Secure Access Service re-signs the applet with a self-signed certificate by default. This certificate is issued by a non-standard trusted root CA. As a result, if a user requests a potentially high-risk applet (such as an applet that accesses network servers), the user's Web browser alerts him that the root is untrusted.

If you import a code-signing certificate to the Secure Access Service, the Secure Access Service uses the imported certificate to re-sign applets instead of the default self-signed certificate. As a result, if a user requests a potentially high-risk applet, the user's Web browser displays an informational message instead of a warning. The message informs the user that the applet is signed by a trusted authority.

The Secure Access Service supports the following types of code-signing certificates:

- **Microsoft Authenticode Certificate**—The Secure Access Service uses this certificate to sign applets that run on either MS JVM or SUN JVM. Note that we only support Microsoft Authenticode Certificates issued by Verisign. You may purchase Microsoft Authenticode Certificates at the following location:

<http://www.verisign.com/products-services/security-services/code-signing/index.html>

- **JavaSoft Certificate**—The Secure Access Service uses this certificate to sign applets that run on SUN JVM. Note that we only support JavaSoft Certificates issued by Verisign and Thawte.

When deciding which code-signing certificate to import, consider the following browser dependencies:

- **Internet Explorer**—Internet Explorer running on new computers shipped with Windows XP pre-installed typically runs the SUN JVM, which means that the Secure Access Service needs to re-sign applets using the JavaSoft certificate.

Internet Explorer running on a Windows 98 or Windows 2000 PC, or a PC that has been upgraded to Windows XP, typically runs the MS JVM, which means that the Secure Access Service needs to re-sign applets using the Authenticode certificate.

- **Netscape, Firefox, and Safari**—These browsers only support the SUN JVM, which means that the Secure Access Service needs to re-sign applets using the JavaSoft certificate.





**NOTE:** If you create IVS systems, you can also import code-signing certificates for each IVS. You must navigate to each IVS system, using the IVS system drop down menu in the admin console header, then import the code-signing certificate for each IVS on the System > Configuration > Certificates > Code-signing Certificates page.

## Additional Considerations for SUN JVM Users

By default, the Java Plug-in caches an applet along with the code-signing certificate presented when a user accesses the applet. This behavior means that even after importing a code-signing certificate to the Secure Access Service, the browser continues to present applets with the original certificate. To ensure that SUN JVM users are not prompted with an untrusted certificate for applets accessed prior to importing a code-signing certificate, users need to flush the Java Plug-in cache. Alternatively, users can disable the cache, but this option may impact performance since the applet needs to be fetched each time the user accesses it.

The Java Plug-in maintains its own list of trusted Web server certificates that is different from the browser's list of trusted certificates. When a user accesses an applet, the SUN JVM makes its own connection (in addition to the browser) to the Web server on which the applet resides. The user is then presented with the option to accept the Web server certificate in addition to the code-signing certificate. In these cases, the user needs to select the "Always Trust" button for the Web server certificate. Due to a built-in timeout in the Java Plug-in, if the user waits too long to select this button for the Web server certificate, the applet does not load.

### Related Documentation

- [Task Summary: Configuring the Secure Access Service to Sign or Re-Sign Java Applets on page 869](#)
- [Importing a Code-Signing Certificate on page 870](#)

## Task Summary: Configuring the Secure Access Service to Sign or Re-Sign Java Applets

To configure the Secure Access Service to re-sign applets using code-signing certificates, you must:

1. Install the Java code-signing certificates through the System > Configuration > Certificates > Code-Signing Certificates page of the admin console.
2. Do one of the following:
  - Create code-signing policies specifying which applets the Secure Access Service should re-sign through the Users > Resource Policies > Web > Java > Code Signing page of the admin console or the Users > Resource Profiles > Web Application Resource Profiles > Profile page. The policies should specify the host names from which the applets originate.
  - Upload your own java applets to the Secure Access Service and configure the Secure Access Service to sign or re-sign them.

- Related Documentation**
- [About Hosted Java Applet Templates on page 453](#)
  - [Importing a Code-Signing Certificate on page 870](#)

## Importing a Code-Signing Certificate

---

To import a code-signing certificate:

1. In the admin console, choose **System > Configuration > Certificates > Code-Signing Certificates**.
2. Under Applet Signing Certificates, click **Import Certificates**.
3. On the Import Certificates page, browse to the appropriate code-signing certificate files, enter the password key information, and then click **Import**.
4. When you have successfully imported a certificate, a Sign Juniper Web Controls With dialog pane appears where you can specify the Secure Access Service's signing option:
  - **Default Juniper Certificate**—Select this option to specify that the Secure Access Service should sign all ActiveX and Java applets originating from the Secure Access Service using the default Juniper Networks certificate. If you have previously selected an imported code-signing certificate and are reverting back to this option, after you click Save, a process icon appears indicating that the Secure Access Service is processing the request and re-signing all of the relevant code. This process can take several minutes to complete.
  - **Imported Certificate**—Select this option to specify that the Secure Access Service signs all ActiveX and Java applets using the certificate or certificates imported in the previous step. When you click Save, a process icon appears indicating that the Secure Access Service is processing the request and signing all of the relevant code. This process can take several minutes to complete.
5. Use settings in the following tabs to specify which resources are signed or re-signed by the applet certificate:
  - Users > Resource Policies > Web > Java > Code Signing
  - Users > Resource Policies > Web > Java > Applets

- Related Documentation**
- [Task Summary: Configuring the Secure Access Service to Sign or Re-Sign Java Applets on page 869](#)

## About Two-Way SSL Authentication

---

In certain corporate environments, servers on the LAN are protected with two-way SSL authentication. These servers require the client to authenticate by presenting a valid certificate.

In the remote access scenario, the Secure Access Service is a client of these servers. You can configure the Secure Access Service to present client authentication certificates to

servers whenever it communicates over SSL. Note that Secure Access Service will present client certificates only when the SSL handshake requires it.



**NOTE:** This feature authenticates only the Secure Access Service (as a client) to back-end servers. It does not authenticate end-users or end-user machines to servers on the corporate LAN.

The SSL protocol provides for mutual authentication of server and client at the time of session initiation. The client part of the authentication is optional. For enhanced security, some deployments may require that the client also authenticate itself with a certificate. Normally, when setting up an SSL connection with a server on behalf of the end-user, the Secure Access Service does not present any certificate to the server. It needs to be explicitly configured to present such certificate. This section explains how such configuration may be performed.

The basic idea is to upload a certificate, private key pair to the Secure Access Service, and configure a mapping between this pair and a server resource. Subsequently, when a end-user attempts to establish an SSL connection with that server, the Secure Access Service presents the associated certificate to the server. If no certificate is associated with the server in the Secure Access Service's certificate store, then it is assumed that the server does not demand client certificate.

If, during the SSL handshake, the back-end server requests a client certificate but the Secure Access Service doesn't send a certificate, the end-user sees an "access denied" error message. Similarly, if the back-end server rejects the Secure Access Service certificate, the end-user sees an "access denied" error message. If a certificate is configured, is successfully retrieved and no error is encountered during handshake, the user is granted access to the server.



**NOTE:** The Secure Access Service allows client authentication certificates to be uploaded to the device in two ways: generate a CSR and upload the signed certificate returned by the CA, or directly import the certificate if one is available. The first option is not available on FIPS devices.

**Related Documentation**

- [Task Summary: Configuring the Secure Access Service for Two-Way SSL Authentication on page 871](#)
- [Importing the Certificates for Two-Way SSL Handshake on page 872](#)

## Task Summary: Configuring the Secure Access Service for Two-Way SSL Authentication

To configure the Secure Access Service for two-way SSL authentication, you must:

1. Import the certificates used for two-way SSL handshake in the System > Configuration > Certificates > Client Auth Certificates window.

2. Define the back-end resource and assign a certificate to be presented when accessing it using the Users > Resource Policies > Web > Client Authentication window.

**Related  
Documentation**

- [About Two-Way SSL Authentication on page 870](#)
- [Importing the Certificates for Two-Way SSL Handshake on page 872](#)

---

## Importing the Certificates for Two-Way SSL Handshake

---

The Secure Access Service allows for certificates that include the private key and for instances where the private key is in a separate file from the certificate. In addition, if your certificates have been exported into a system configuration file, you can import the system configuration file to upload the certificates.

To import the certificate files individually:

1. Select **System > Configuration > Certificates > Client Auth Certificates**.
2. Click **Import Certificate & Key**.
3. Click **Browse** and locate your certificate file.
4. If your private key is in a separate file from the certificate, click **Browse** and locate your private key file.
5. If your files are encrypted, enter the password.
6. Click **Import**.

To import the certificates from a system configuration file:

1. Select **System > Configuration > Certificates > Client Auth Certificates**.
2. Click **Import Certificate & Key**.
3. Click **Browse** and locate your system configuration file.
4. Enter the password used to encrypt the system configuration file.
5. Click **Import**.

Clicking the certificate link in the System > Configuration > Certificates > Client Auth Certificates window displays details about that particular certificate, such as issued to/by information, valid dates, and a button to renew the certificate.

**Related  
Documentation**

- [Task Summary: Configuring the Secure Access Service for Two-Way SSL Authentication on page 871](#)

---

## Mapping Resource Policies to the Certificate

---

Once the certificates have been uploaded, you can map resources to the certificates and the roles to which they apply.

1. Select **Users > Resource Policies > Web > Client Authentication**.
2. If you do not see the Client Authentication menu item, select **Users > Resource Policies > Web**.
  - a. Click the **Customize** button in the upper right corner of the console.
  - b. In the Customize View dialog box, select **Client Authentication**.
  - c. Click **OK**.
  - d. Click the **Client Authentication** tab.
3. Click **New Policy**.
4. On the New Policy page:
  - Enter a name to label this source interface policy.
  - Enter an optional description.
5. In the Resources section, specify the back-end servers to which this policy applies. Valid values/formats are: hostnames, IP addresses, IP Address:Port and Hostname:Port.

If you specify \* as the resource, one certificate is used for all resources requesting a back-end certificate authentication. This certificate becomes the default certificate. Defining a default certificate is not required.
6. In the Roles section, select one of the following options:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who map to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
7. In the Action section, select one of the following options:
  - **Use the Client Authentication Certificate Below**—Select this option to associate this policy with a client authentication certificate. Select the certificate to use from the Certificate menu.

If the Certificates menu is blank, no certificates have been uploaded to the System > Configuration > Certificates > Client Auth Certificates window.
  - **Do not use Client Authentication**—If this option is selected, the Secure Access Service does not perform client authentication for the configured resource.

- **Use Detailed Rules**—Select this option to specify one or more detailed rules for this policy.

8. Click **Save Changes**.

**Related  
Documentation**

- [Importing the Certificates for Two-Way SSL Handshake on page 872](#)
- [Writing a Detailed Rule for Resource Policies on page 150](#)

## Mapping an Client Authentication Auto-Policy

---

A client authentication auto-policy option is available on the Users > Resource Profiles > Web page. If the back-end server requires two-way SSL authentication, this auto-policy lets you configure a certificate to be presented during the SSL handshake.

1. Select **Users > Resource Profiles > Web**.
2. Follow the process as a regular resource profile for defining the name and type.
3. Select the **Autopolicy: Client Authentication** checkbox.
4. In the Resource field, specify the back-end server. Valid formats/values are: host names, IP addresses, IP Address:Port, and HostName: Port.

If you specify \* as the resource, one certificate is used for all resources requesting a back-end certificate authentication. This certificate becomes the default certificate. Defining a default certificate is not required.

5. Click **Save Changes**.

**Related  
Documentation**

- [Resource Profiles on page 127](#)

# Elliptic Curve Cryptography

- [Understanding ECC Certificates on page 875](#)
- [Example: Assigning an ECC P-256 Certificate to an External Virtual Port and Giving Preference to Suite B Ciphers on page 877](#)
- [Verifying the Certificate on the Client on page 883](#)
- [Using TCP Dump to View Cipher Information on page 885](#)

## Understanding ECC Certificates

---

Public-key cryptography is a cryptographic system that requires a secret key and a public key that are mathematically linked with each other. One key encrypts the plain text while the other decrypts the cipher text. RSA is the most widely used public-key algorithm.

Elliptic Curve Cryptography (ECC) were introduced as an alternative to RSA in public key cryptography. One advantage of ECC over RSA is key size versus strength. For example, a security strength of 80 bits can be achieved through an ECC key size of 160 bits, whereas RSA requires a key size of 1024. With a 112-bit strength, the ECC key size is 224 bits and the RSA key size is 2048 bits.

The most popular signature scheme that uses elliptic curves is called the Elliptic Curve Digital Signature Algorithm (ECDSA). The most popular key agreement scheme is called Elliptic Curve Diffie-Hellman (ECDH). An ECDH exchange is a variant of the Diffie-Hellman (DH) protocol and is an integral part of the Suite B cryptography standards proposed by the National Security Agency (NSA) for protecting both classified and unclassified information.

## About Suite B

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. Because a single encryption algorithm cannot satisfy all of the needs of the national security community, NSA created a larger set of cryptographic algorithms, called Suite B, which can be used along with AES in systems used by national security users. In addition to AES, Suite B includes cryptographic algorithms for hashing, digital signatures, and key exchanges.

Per RFC 6460, to be Suite B TLS 1.2 compliant the server and client should negotiate with the following ciphers:

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

RFC 6460 also lists a transitional Suite B profile for TLS 1.0 and TLS 1.1. Clients and servers that do not yet support Suite B TLS 1.2 should negotiate with the following ciphers:

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA

There is no special configuration to ensure that Secure Access Service and Access Control Service negotiates Suite B ciphers. However, the following general steps should be performed to enable Suite B compliance:

- An ECC certificate signed by an ECC Root CA is associated with a network port.
  - A P-256 CSR is signed by either a P-256 or P-384 Root CA.
  - A P-384 CSR is signed by a P-384 Root CA.
- Manually enable only AES128 and/or AES256 custom ciphers.



**NOTE:** Secure Access Service and Access Control Service cannot be configured to allow only Suite B ciphers.

---

## Using ECC Certificates with Secure Access Service and Access Control Service

ECC certificates are currently supported only on the MAG and virtual appliance platforms. As with RSA certificates, ECC certificates are associated with a network port. You can create multiple virtual ports on the server with each port supporting a specific certificate. For example, external virtual port 1 can use a 1024-bit RSA while external virtual port 2 uses ECC P-256 and external virtual port 3 uses ECC P-384. Only clients that support ECC cipher suites can connect to the web server on that network port.

When an Elliptic Curve Cryptography (ECC) certificate is associated with a network port, only clients that support ECC cipher suites can connect to the Web server on that network port.

Except for the key and certificate generation process, the use of ECC certificates is basically the same as using RSA certificates.

### Related Documentation

- [Example: Assigning an ECC P-256 Certificate to an External Virtual Port and Giving Preference to Suite B Ciphers on page 877](#)



## Example: Assigning an ECC P-256 Certificate to an External Virtual Port and Giving Preference to Suite B Ciphers

This example outlines the general steps for creating an external port and assigning an ECC P-256 certificate. The steps are generally the same as assigning an RSA certificate to a port.

- [Configuring the External Port on page 877](#)
- (optional) [Configuring the Virtual Ports on page 878](#)
- [Creating the Certificate Signing Request for a New Certificate on page 878](#)
- [Importing the Signed Certificate Created from a CSR on page 880](#)
- [Presenting the Certificate on the Network on page 880](#)
- [Setting the Security Options on page 881](#)

### Configuring the External Port

The external port handles all requests from users signed into the server from outside the customer LAN, for example, from the Internet.

To configure the external port:

1. In the admin GUI, choose **System > Network > External Port > Settings**.
2. Modify the settings as needed. In this example, only IPv4 is enabled. See [Figure 53 on page 877](#).

**Figure 53: Configuring the External Port for IPv4**

Overview Internal Port External Port Management Port VLANs Routes Hosts VPN Tunneling

Settings Virtual Ports ARP Cache ND Cache

Enter the network settings and click the Save Changes button at the bottom of the page.

**Use Port?**

Enabled  Disabled

**IPv4 Settings**

Enable IPv4  Disable IPv4

Note: Changing above setting might restart some services. This restart might drop all the connections to the Junos Pulse Secure Access Service.

\* IP Address:

\* Netmask:

\* Default Gateway:

Note: If you need to specify static routes, you can do so on the [Static Routes](#) page.

**IPv6 Settings**

**Advanced Port Settings**

MAC Address:

Link Speed:

\* ARP Ping Timeout:  seconds 3 to 300 seconds

\* MTU:  bytes Maximum Transmission Unit. If IPv6 is enabled (1280 to 1500), else (576 to 1500).

**Save changes?**

3. Click **Save Changes**.

## (optional) Configuring the Virtual Ports

A virtual port is an IP alias bound to a physical port. It shares all of the network settings, except IP address, with the associated physical port. You can use virtual ports for different purposes, depending on the physical port or the VLAN on which you base the virtual port. In this example, we are configuring the virtual port on the external port to support external sign-ins. This is an optional step that shows one way of allowing multiple certificates on the device.

To configure the external virtual port:

1. In the admin GUI, choose **System > Network > External Port > Virtual Ports**.
2. Click **New Port**.

In this example, the port is named p\_ecdsa256 and accepts only IPv4 addresses. See [Figure 54 on page 878](#).

**Figure 54: Creating the Virtual Port on the External Port**

The screenshot shows the Junos Pulse Secure Admin GUI. The breadcrumb navigation is **Network Settings > External Port > Virtual Ports > Virtual Port p1**. The configuration form for the virtual port is as follows:

* Name:	<input type="text" value="p_ecdsa256"/>
Physical Port:	External Port <small>The physical port determines all characteristics of this virtual port other than IP address</small>
IPv4 Address:	<input type="text" value="10.64.80.11"/>
IPv6 Address:	<input type="text"/>

At the bottom of the form are two buttons: **Save Changes** and **Cancel**.

3. Click **Save Changes**.

## Creating the Certificate Signing Request for a New Certificate

A certificate signing request (CSR) is a message sent from an applicant to a certificate authority (CA) to apply for a digital identity certificate. You create a CSR through the admin console. When you create a CSR, a private key is created locally that corresponds to the CSR. If you delete the CSR at any point, the private key is deleted too, prohibiting you from installing a signed certificate generated from the CSR.

In this example, a CSR for an ECC P-256 certificate is requested.

To create a CSR for a new certificate:

1. In the admin console, choose **System > Configuration > Certificates > Device Certificates**.
2. Click **New CSR**.
3. Enter the required requestor information. In this example, the common name is ecc-p256.juniper.net.
4. Click **ECC** and select **P-256** from the ECC Curve menu. See [Figure 55 on page 879](#).

Figure 55: Creating an ECC P-256 Certificate Signing Request

Configuration >  
**New Certificate Signing Request**

Use this page to create a new Certificate Signing Request (CSR) to send to your Certificate Authority of choice.

Common Name:  
 (e.g., secure.company.com)

Organization Name:  
 (e.g., Company Inc.)

Org. Unit Name:  
 (e.g., IT Group)

Locality:  
 (e.g., SomeCity)

State (fully spelled out):  
 (e.g., California)

Country (2 letter code):  
 (i.e., US)

Email Address:

Key Type:  RSA  ECC

ECC Curve:

5. Click **Create CSR**. A CSR is successfully created, as shown in Figure 56 on page 879.

Figure 56: CSR Successfully Created

CSR created successfully

Your CSR was created successfully. See below for instructions on sending the CSR to a Certificate Authority.

The certificate approval process may take several days. When you receive the signed certificate from the Certificate Authority, you will need to import the certificate to complete this process.

Configuration >  
**Pending Certificate Signing Request**

**CSR Details**

Common Name: ecc-p256.juniper.net  
 Created: 1/22/2013 13:26:42  
 Org. Name: Security Business Group Locality: Sunnyvale  
 Org. Unit Name: iX Group State: California  
 Email Address: myemail@juniper.net Country: US  
 Key Size: 1024 bits

[Back to Device Certificates](#)

**Step 1. Send CSR to Certificate Authority for signing**

To send the CSR to a Certificate Authority (CA), you need to copy the encoded text below, including the BEGIN and END lines, and submit it to the CA in one of the following ways:

- Save the text as a .cert file and attach it to an email message to the CA
- Paste the text into an email message to the CA
- Paste the text into a Web form provided by the CA

Note: Manage the CSR process carefully. If you submit more than one CSR to a CA, you may be billed for each CSR.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBe3CCARECAQAg4kCzA2JgNBAYTA1VlNRNNEQYVQOIExpDYWp2m9ybm1h
NRlVeAVDVOQHEvITd9SueX2hbGUXETAFB9NVAaSTCG1YIEdyb3VvMSAvHgYVQOQR
ExdtZNN1cm10eSBcdXlpbmVzcyBBcm91cDEEdmB6G1UEAaKHU2WNjLXAyHTYuanYu
aXB1c15UZXQwIjAqB9kqphKtS9w0BQZWEZ15Zw1haWkaanYuaXB1c15UZXQwWTAT

```

**Step 2. Import signed certificate**

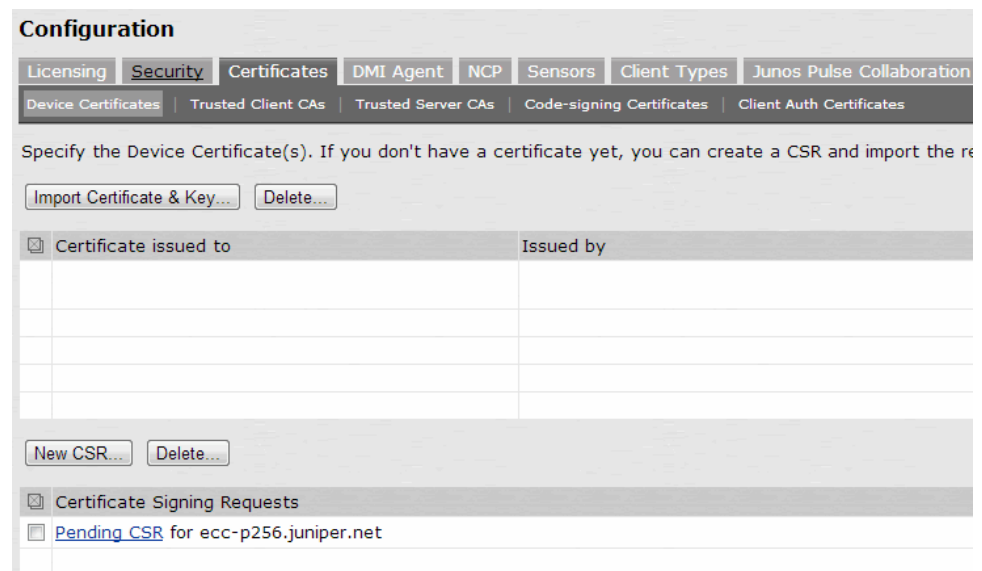
When you receive the signed certificate file from the CA, select it below and click Import. This will add the signed certificate and remove this pending CSR.

Signed certificate:  No file chosen

6. The CSR is encoded and can be copied or saved to a file. The ECC certificate should be signed by an ECC CA for Suite B compliance. Follow your CA's process for sending a CSR.

7. Click the **Back to Device Certificates** link. Until you import the signed certificate from your CA, your CSR is listed as Pending. See Figure 57 on page 880.

Figure 57: Pending CSR



## Importing the Signed Certificate Created from a CSR

Once your CA has sent your signed certificate, you must import that into the pending CSR.

To import a signed device certificate created from a CSR:

1. In the admin console, choose **System > Configuration > Certificates > Device Certificates**.
2. Under Certificate Signing Requests, click the **Pending CSR** link that corresponds to the signed certificate. See [Figure 57 on page 880](#).
3. Under Import signed certificate, browse to the certificate file you received from the CA and then click **Import**. See [Figure 56 on page 879](#).

## Presenting the Certificate on the Network

You can present a certificate many ways, depending on your configuration. For example, you can present the certificate to one or more virtual ports or on an internal or external port. In this example, the ECC P-256 certificate is presented on the external virtual port p1.

To present a certificate on an external virtual port:

1. In the admin console, select **System > Configuration > Certificates > Device Certificates**.
2. Click the certificate name you want to assign to a port. In this example, click **ecc-p256.juniper.net**.
3. Under External Ports, select **p\_ecdsa256** and click **Add**. See [Figure 58 on page 881](#).

Figure 58: Associating the ECC P-256 With The External Virtual Port p\_ecdsa256

Certificates >  
**Certificate Details**

**Certificate**

**Issued To:** ▶ ecc-p256.juniper.net  
**Issued By:** ▶  
**Valid:** Nov 9 03:17:18 2012 GMT to May 2 03:17:18 2018 GMT  
**Details:** ▶ Other Certificate Details  
[Download](#)

**Present certificate on these ports**

Select the internal and external virtual ports that will present this certificate:

**Internal Virtual Ports:**      **Selected Virtual Ports:**

↑      Add ->      <Internal Port> ↑  
 ↓      Remove      ↓

**External Virtual Ports:**      **Selected Virtual Ports:**

<External Port> ↑      Add ->      p\_ecdsa256 ↑  
 ↓      Remove      ↓

**Vlan Ports:**      **Selected Vlan Ports:**

↑      Add ->      ↑  
 ↓      Remove      ↓

Management Port

4. Click **Save Changes**.

## Setting the Security Options

To specify the cipher suites for the incoming connection to the web server, use the SSL Options page and select the **Custom SSL Cipher Selection** option. This step is required in our example to give Suite B cipher suites preference. If you do not want to give Suite B cipher suites preference, you do not have to perform this step.

To set the security options:

1. In the admin console, select **System > Configuration > Security > SSL Options**.
2. Under Allowed Encryption Strength choose **Custom SSL Cipher Selection**. See [Figure 59 on page 882](#).

Figure 59: Setting Custom SSL Cipher Selections

**Allowed Encryption Strength**  
 Strong ciphers (rated by the number of bits in the cipher) improve the security of SSL encryption, but some browsers may or Secure Access Service will give preference to the cipher with the fastest data transfer rate, regardless of its relative encrypt Please see the Setting Security Options section in the Admin guide for more details.

Accept only 168-bit and greater (maximize security)  
 Accept only 128-bit and greater (security and browser compatibility)  
 Accept 40-bit and greater (maximize browser compatibility)  
 Custom SSL Cipher Selection

**Note:** Custom cipher selection disables the **Encryption Strength option**.

Cipher Suites	High (>=168-bit)	Medium (>=128-bit and <168-bit)	Low (>=40-bit and <128-bit)	Description
AES/3DES	<input checked="" type="checkbox"/>			cipher suites using triple DES and AES (Maximizes security)
AES		<input checked="" type="checkbox"/>		cipher suites using AES (Maximizes performance)
DES			<input type="checkbox"/>	cipher suites using DES (not triple DES)
RC4		<input type="checkbox"/>		cipher suites using RC4

Recommended for FIPS deployment

**Encryption Strength option**  
 Normally, the allowed encryption strength is enforced after an SSL session is established, so that a user that connects using option below will prevent a browser with a weak cipher from establishing a connection. Changing this option will cause the w

Do not allow connections from browsers that only accept weaker ciphers

**SSL Handshake Timeout option**  
 By default, the SSL handshake has a timeout of 60 seconds. Use the text box below to set a different value.

Timeout:  seconds 10-600 seconds

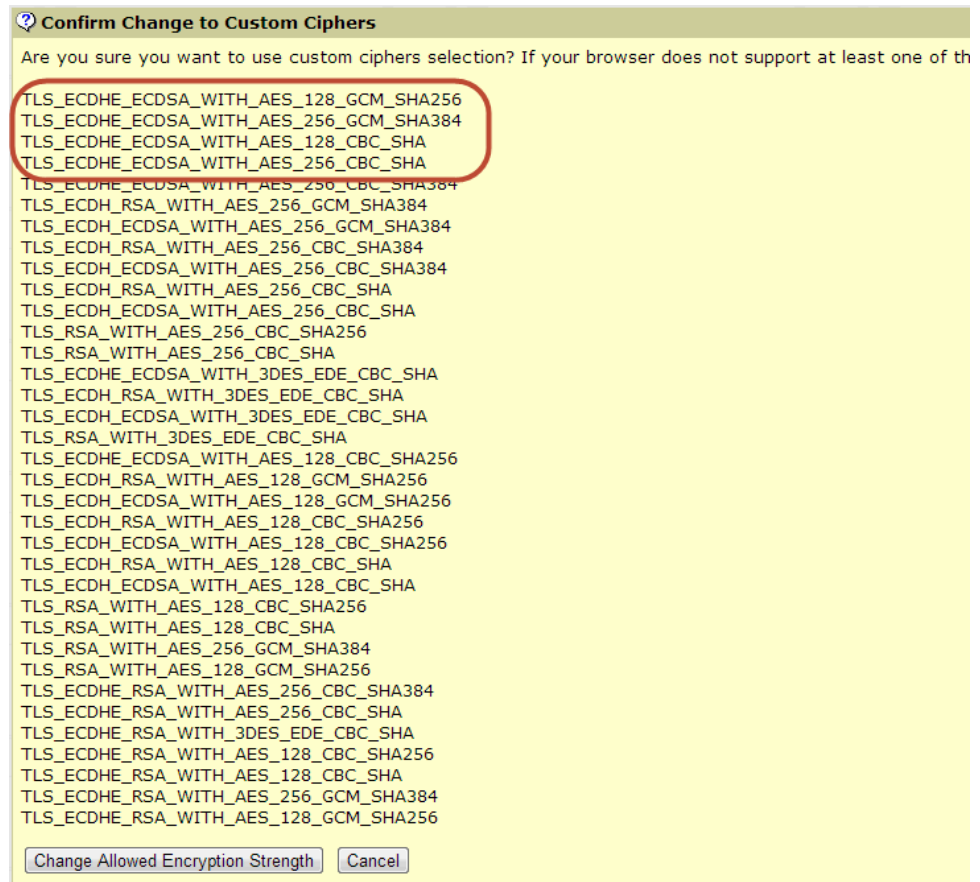
**SSL Legacy Renegotiation Support option**  
 When this option is enabled, renegotiation with clients and servers, which dont support the new TLS Renegotiation Info exte and servers will not be allowed. Changing this option will cause the web service to restart.

Enable support for SSL legacy renegotiation

3. Choose the recommended options (in green) if they are not already selected.
4. If you are using client certificate authentication (Secure Access Service only):
  - Select **Enable client certificate on the external port** under ActiveSync Client Certificate Configuration.
  - Move p\_ecdsa256 to the Selected Virtual Ports column.
5. Click **Save Changes**.

A list of the custom ciphers to be used on the device's port is displayed in the order the web server will select them. Note that Suite B ciphers are listed on top. See [Figure 60 on page 883](#). End users who now log in to external virtual port p\_ecdsa256 must have at least one of the listed ciphers installed on their browser or else they cannot log in to the server.

Figure 60: Confirming Custom Ciphers



6. Click **Change Allowed Encryption Strength**.

### Related Documentation

- [Verifying the Certificate on the Client on page 883](#)

## Verifying the Certificate on the Client

End users can check which certificate their browser is using to connect to the server. In the following example, the end user connects to server port p3, which uses an ECC curve P-256 certificate. See [Figure 61 on page 883](#).

Figure 61: Connecting to a Port Using an ECC Curve P-256 Certificate



To view the certificate from an Internet Explorer 8 browser:

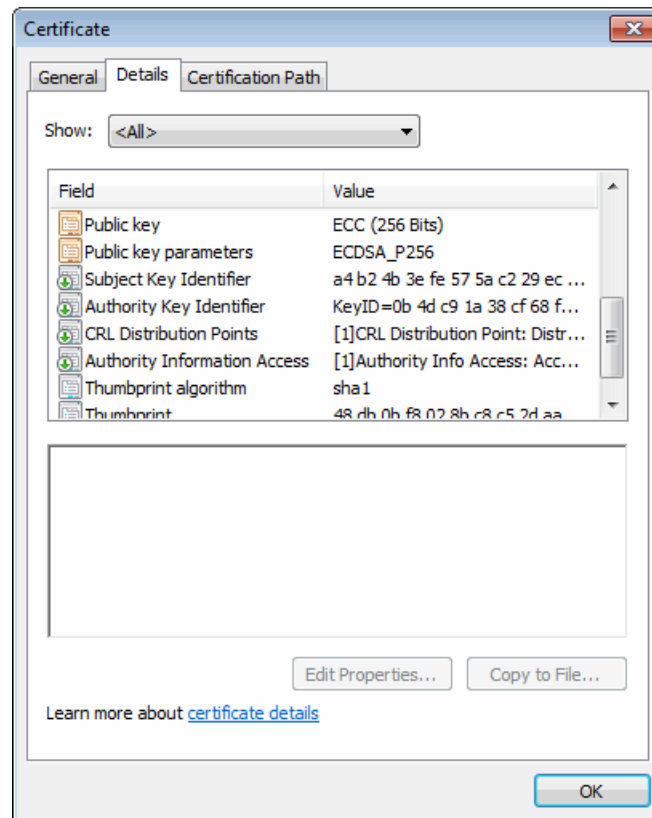
1. Open an Internet Explorer 8 browser and point to the server to which you want to connect.
2. Click the lock icon located at the end of the address bar and then click the **View Certificate** link. See [Figure 62 on page 884](#).

**Figure 62: Viewing the Connection Certificate Information**



3. Click the **Details** tab and scroll down until you see the Public key field. In this example, the public key value is ECC (256 Bits) which matches the server port p3 certificate shown in [Figure 61 on page 883](#). See [Figure 63 on page 884](#).

**Figure 63: Certificate Public Key**



**Related Documentation**

- [Understanding ECC Certificates on page 875](#)
- [Using TCP Dump to View Cipher Information on page 885](#)



## Using TCP Dump to View Cipher Information

You can use the TCP Dump tool to view which cipher each client uses to connect to the server. TCP Dump is a packet analyzer that intercepts (sniffs) and displays TCP/IP and other packets transmitted or received between the server and clients.



**NOTE:** To permit debugging, it is recommended that the ECC certificate be replaced by an RSA certificate so that an RSA cipher suite gets selected and then the application data can be decoded.

To capture packet headers:

1. Select **Maintenance > Troubleshooting > Tools > TCP Dump**.
2. Select the interface, internal or external or both, you wish to sniff and then the VLAN port.
3. Click **Start Sniffing**.

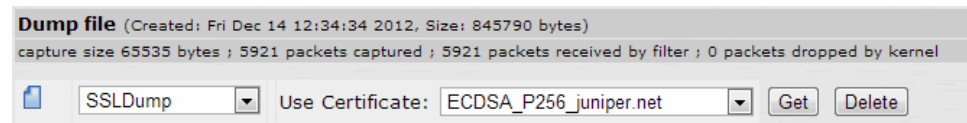
The next time a user points a browser window to the server or logs in to the server, handshake information is obtained.

4. Click **Stop Sniffing** when done.

To view the packet headers:

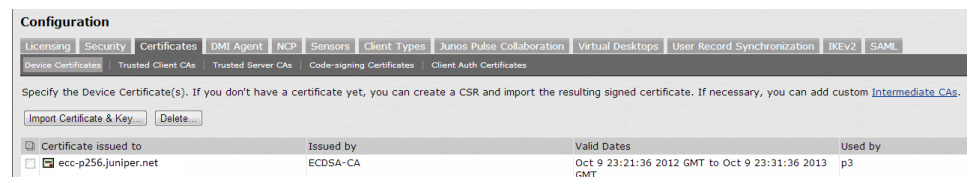
1. Select **Maintenance > Troubleshooting > Tools > TCP Dump**.
2. Under Dump file, select **SSLDump** from the file menu and the certificate to use. See [Figure 64 on page 885](#).

**Figure 64: Viewing the TCP Dump Output**



The certificate names in the TCP Dump window are the same as the “Certificate issued to” names in the Device Certificates window. Select the certificate corresponding to the port you wish to view packet information. See [Figure 65 on page 885](#).

**Figure 65: Issued to Certificate on the Device Certificates Pages**



3. Click **Get**.

Portions of a TCP dump output follow.

The client starts a handshake with the server:

```
1 1 0.0007 (0.0007) C>S Handshake
```

The client then lists its supported cipher suites:

```
cipher suites
 TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
 TLS_ECDH_ECDSA_WITH_AES_256_SHA384
 TLS_ECDH_ECDSA_WITH_AES_256_SHA
 TLS_ECDH_ECDSA_WITH_DES_CBC3_SHA
 ...
```

The server acknowledges the handshake:

```
1 2 0.0010 (0.0003) S>C Handshake
```

The server compares the cipher suites on the client with the ones on the server and picks the cipher suite that is preferred by the server based on SSL options:

```
cipherSuite TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
```

### Example TCP Dump Output

```

New TCP connection #1: 10.64.8.3(46200) <-> 10.64.90.21(443)
1 1 0.0007 (0.0007) C>S Handshake
 ClientHello
 Version 3.3
 cipher suites
 TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
 TLS_ECDH_ECDSA_WITH_AES_256_SHA384
 TLS_ECDH_ECDSA_WITH_AES_256_SHA
 TLS_ECDH_ECDSA_WITH_DES_CBC3_SHA
 TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA384
 TLS_ECDH_ECDSA_WITH_AES_128_SHA256
 TLS_ECDH_ECDSA_WITH_AES_128_SHA
 TLS_ECDH_ECDSA_WITH_RC4_SHA
 Unknown value 0xc001
 TLS_EMPTY_RENEGOTIATION_INFO_SCSV
 compression methods
 NULL
 ClientHello Extensions [113]=
 00 6f 00 0b 00 04 03 00 01 02 00 0a 00 34 00 32
 00 0e 00 0d 00 19 00 0b 00 0c 00 18 00 09 00 0a
 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00 04
 00 05 00 12 00 13 00 01 00 02 00 03 00 0f 00 10
 00 11 00 23 00 00 00 0d 00 22 00 20 06 01 06 02
 06 03 05 01 05 02 05 03 04 01 04 02 04 03 03 01
 03 02 03 03 02 01 02 02 02 03 01 01 00 0f 00 01
 01
1 2 0.0010 (0.0003) S>C Handshake
 ServerHello
 Version 3.3
 session_id[32]=
 a3 07 40 6e 73 12 c2 4d f3 7d b9 77 f8 97 e1 94
 fc 1b 51 6a 66 3c 99 d6 c7 7d 0e fa 29 2e d0 c4
 cipherSuite TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
 compressionMethod NULL
 ServerHello Extensions [20]=
 00 12 ff 01 00 01 00 00 0b 00 04 03 00 01 02 00
 0f 00 01 01
1 3 0.0010 (0.0000) S>C Handshake
 Certificate
1 4 0.0010 (0.0000) S>C Handshake
 ServerHelloDone
1 5 0.1413 (0.1403) C>S Handshake
 ClientKeyExchange
1 6 0.1413 (0.0000) C>S ChangeCipherSpec
1 7 0.1413 (0.0000) C>S Handshake
1 8 0.1464 (0.0051) S>C ChangeCipherSpec
1 9 0.1464 (0.0000) S>C Handshake
1 10 9.2389 (9.0924) C>S application_data
1 11 9.5828 (0.3438) C>S application_data
1 12 9.5833 (0.0004) S>C application_data
1 9.5833 (0.0000) S>C TCP FIN
1 13 9.5999 (0.0166) C>S Alert
1 9.5999 (0.0000) C>S TCP FIN

```

### Related Documentation

- [Understanding ECC Certificates on page 875](#)
- [Example: Assigning an ECC P-256 Certificate to an External Virtual Port and Giving Preference to Suite B Ciphers on page 877](#)



# System Archiving

- [About System Archiving on page 889](#)
- [Specifying Archive Schedules on page 891](#)
- [Creating Local Backups of Secure Access Service Configuration Files on page 894](#)
- [Importing and Exporting Secure Access Service Configuration Files on page 896](#)
- [Importing and Exporting IVS Configuration Settings on page 900](#)
- [Importing and Exporting XML Configuration Files on page 901](#)
- [Importing and Exporting XML Configuration Data on page 910](#)
- [System Restarts on page 916](#)
- [XML Import/Export Use Cases on page 918](#)
- [Importing to a System with the Management Port on page 922](#)
- [Using Operation Attributes on page 922](#)
- [Using the Push Configuration Feature on page 924](#)
- [Defining Push Configuration Targets on page 926](#)
- [Pushing Configuration Settings on page 928](#)
- [Archiving Junos Pulse Collaboration Meetings on page 929](#)

## About System Archiving

---

The Secure Access Service provides different ways to backup and restore configuration files containing user and system data. The Secure Access Service utilities you can use to backup and restore data preserve the configuration data in two different formats: binary and XML. The method you choose to use depends on your requirements.

The Secure Access Service enables you to use SCP (Secure Copy) or FTP to automatically archive a binary copy of your system logs, configuration files, and user accounts on a daily or weekly basis. The Secure Access Service encrypts the configuration files and user accounts to ensure secure transmission and secure storage on other servers, and then archives the files to the server and directory you specify on the chosen day(s) and time.

If the archive process fails, archiving restarts at the next scheduled time. The Secure Access Service does not continue to retry the process if it fails. Log files are not deleted if the archive process fails.

Automatic archiving occurs only at the scheduled time. No “unscheduled” archiving is done automatically. For example, if a log file exceeds the maximum file size, the archiving process does not automatically backup the file prior to the scheduled time to prevent data loss.

SCP is a file transfer utility similar to FTP. SCP encrypts all data during transfer. When the data reaches its destination, it is rendered in its original format. SCP is included in most SSH distributions, and is available on all major operating system platforms.

The name of archive files have the following format:

- System events: `JuniperAccessLog-[clustername|standalone]-[nodename|hostname]-[IVSname|root]-[date]-[time]`
- User events: `JuniperEventsLog-[clustername|standalone]-[nodename|hostname]-[IVSname|root]-[date]-[time]`
- Administrator events: `JuniperAdminLog-[clustername|standalone]-[nodename|hostname]-[IVSname|root]-[date]-[time]`
- System configuration files: `JuniperConf-[clustername|standalone]-[nodename|hostname]-[IVSname|root]-[date]-[time]`
- User accounts: `JuniperUserAccounts-[clustername|standalone]-[nodename|hostname]-[IVSname|root]-[date]-[time]`

Following are some examples of file names. In these examples, “gen” is the cluster name.

- `JuniperAccessLog-gen-node1-Root-20090109-1545.gz`
- `JuniperEventsLog-gen-node1-Root-20090109-1545.gz`
- `JuniperAdminLog-gen-node1-Root-20090109-1545.gz`
- `JuniperConf-gen-node1-Root-20090109-1545`
- `JuniperUserAccounts-gen-node2-Root-20090109-1542`

System archiving capabilities are available on all Secure Access Service products—you do not need a special license to use them. However, the following archiving tools may are not available on the SA700 Series Appliance:

- Archiving local backups
- Push configuration

**Related Documentation**

- [Specifying Archiving Parameters on page 891](#)
- [Creating Local Backups of Secure Access Service Configuration Files on page 894](#)
- [Importing and Exporting Secure Access Service Configuration Files on page 896](#)
- [Importing and Exporting XML Configuration Files on page 901](#)
- [Exporting and Importing IVS Configuration Files on page 1050](#)
- [Using the Push Configuration Feature on page 924](#)

---

## Specifying Archive Schedules

---

- [Specifying Archiving Parameters on page 891](#)
- [Archiving Debug Logs on page 892](#)
- [Archiving System Snapshots on page 893](#)

## Specifying Archiving Parameters

To specify archive parameters:

1. In the admin console, select **Maintenance > Archiving > Archiving Servers**.
2. Under **Archive Settings**, specify the destination server, a directory, and your credentials for that server. Do not include a drive specification for the destination directory, such as: juniper/log.
  - For UNIX computers, although you can specify an absolute or relative path, depending on the user's home directory, we recommend using a full path instead.
  - For Windows computers, specify a path that is relative to the ftproot directory. We recommend using a full path to the directory.
3. For **Method**, specify SCP or FTP. SCP is the default method.
4. Under **Archive Schedule**, specify one or more of the following components to archive by enabling its associated checkbox:
  - Archive events log
  - Archive user access log
  - Archive admin access log
  - Archive Sensors log
  - Archive client-side log uploads
  - Archive system configuration
  - Archive user accounts
  - Archive IVS
  - Archive XML configuration
  - Archive Debug Log
  - Archive Periodic SnapShots
5. Specify an archive schedule for each selected component. Through the options for each component, schedule archives on any combination of weekdays including weekends.



**NOTE:** If you schedule an archival operation to occur during the hour that your system switches to Daylight Savings Time (DST) the operation may not occur as scheduled. For example, if your system is set to change to DST at 1:00 a.m. and you have scheduled an archival operation to occur at anytime between 1:01 a.m. and 1:59 a.m., the operation is not accomplished, because at 1:00 a.m. the system clock is moved forward to 2:00 a.m. and the system never reaches your archival time for that date.

6. Define a specific time when you want the Secure Access Service to archive data or elect to archive data every hour, which produces twenty-four files with unique timestamps.



**NOTE:** We recommend you schedule an archival operation during hours when traffic is light in order to minimize its impact to your users. The automatic archiving process compresses files and, if the system is busy, can degrade performance for users. Also, a cluster node may appear unresponsive if the system is busy with traffic and performing archiving simultaneously.

7. Select a log filter from the drop-down list.
8. Specify to clear system events, access, and administrator log files after archiving (optional).



**NOTE:** If an archive process fails, log files are not deleted.

9. Provide a password if you want to encrypt system configuration or user account archives with a password (optional).
10. Click **Save Changes**.

#### Related Documentation

- [About System Archiving on page 889](#)
- [Importing and Exporting XML Configuration Files on page 901](#)
- [Importing and Exporting XML Configuration Data on page 910](#)
- [Logging and Monitoring Overview on page 931](#)

## Archiving Debug Logs

The Secure Access Service maintains two debug log files:

- debuglog
- debuglog.old



When the size of the debuglog file reaches its configured maximum file size, it is renamed to debuglog.old and logs are written into a new debuglog file. If debug log archiving is enabled through the Archiving Servers window (select **Maintenance > Archiving**), a check occurs every five minutes to see if the debuglog file has been renamed to debuglog.old. If it has been renamed, the file is archived.

If you use extensive logging, we recommend that you set the debuglog file size to the maximum value. If you set the debuglog file size to a small value and use extensive logging, there is a chance that the debuglog file can be rolled over twice within the five minute period. In this case, you will lose one archive.

The **Clear log after Archiving** option deletes the **debuglog.old** file immediately after the archival process.

Figure 66: Archiving Debug Logs

**Archive Schedule**

Select one or more components to schedule an archive.

- Archive events log
- Archive user access log
- Archive admin access log
- Archive Sensors log
- Archive client-side log uploads
- Archive system configuration
- Archive user accounts
- Archive XML configuration
- Archive Debug Log
  - Clear log after archiving
- Archive Periodic SnapShots

**Related Documentation** • [Archiving System Snapshots on page 893](#)

## Archiving System Snapshots

If periodic snapshots are enabled (select **Schedule automatic snapshots** in the **Maintenance > Troubleshooting > System Snapshots** window ) and **Archive Periodic SnapShots** is selected in the Archive Server window, a check is made every five minutes to see if a new snapshot has been generated. If a new snapshot is found, it is archived.

When the number of snapshots collected reaches 10, or the total memory taken by the snapshots reaches 500Mb, the oldest snapshot is automatically deleted.

If both debuglog archiving and periodic snapshots are enabled, we recommend you disable the **Include debug log** option in the **Maintenance > Troubleshooting > System Snapshots** window to reduce the snapshot file size. Since debug logs are archived in the Archive Server window it is not necessary to include the debug logs in the snapshot file.

**Figure 67: Including Debug Logs in System Snapshots**

**System snapshot options**

Include system config

Include debug log

Schedule automatic snapshots

You should enable automatic scheduled snapshots only when asked to do so by Juniper Networks Support as part of a troubleshooting operation. Enabling this feature can affect system performance. In most situations, a four-hour snapshot schedule captures the needed data without impacting system performance. Do not set a schedule interval of less than 30 minutes as this can affect system performance.

Take a snapshot every:  hours (0 - 336 hours)

minutes (0 - 59 minutes)

Max size allocated for periodic snapshots:  MB (60 - 500 MB)

Stop taking snapshots after: Date:  (mm/dd/yyyy)

Time:  AM  (hh:mm)

Disable debug logs at stop time:

**Related Documentation** • [Archiving Debug Logs on page 892](#)

## Creating Local Backups of Secure Access Service Configuration Files

Secure Access Service enable you to save backups of your current system configuration and user accounts directly to the Secure Access Service in binary format. You may then use these configurations to restore the Secure Access Service or a cluster of Secure Access Services to the state contained in the encrypted file. Note that these files only contain configuration information—they do not include logs.



**NOTE:** During an import operation to a cluster node, the sync rank of the node may change temporarily to allow the propagation of the imported data to all nodes. The sync rank will be returned to its original value after the import operation is complete.

You may save up to 5 system configuration backups and 5 user account backups on the Secure Access Service. If you try to exceed this limit, the Secure Access Service overwrites the oldest backup with the new backup. If you do not want to overwrite the oldest backup, choose another backup to delete instead, before saving the most current one.

To save your current system configuration:

1. In the admin console, choose **Maintenance > Archiving > Local Backups**.
2. Click **Save Configuration** or **Save User Accounts**. The Secure Access Service adds a new backup to the list, naming it with the current date and time.

You may use system and user backups to update a single Secure Access Service or a cluster. If you choose to restore the Secure Access Service that is enabled as part of a cluster, that Secure Access Service automatically pushes the configuration to all other cluster members. The cluster is disabled until all cluster members have updated their settings using the backup configuration. Then, they restart and re-enable the cluster.

You can save a backup of your current configuration or to restore your system or user account state from a backup.

To override your configuration with settings from a backup file:

1. In the admin console, choose **Maintenance > Archiving > Local Backups**.
2. Select the checkbox next to the system configuration or user account backup file that you want to use to restore your system.
3. If you are restoring from a system configuration, indicate whether or not you want to use the certificate, IP address, and network settings contained in the configuration file.



**NOTE:** If you are upgrading an entire cluster, you should use caution when including network settings. Since IP addresses and other settings may not apply to all members of the cluster, cluster members may not be able to communicate with one another if the settings are pushed out to all members.

If you are upgrading an SA Series FIPS Appliance, you must choose a certificate that uses a FIPS-compliant private key if you choose to import a certificate. To ensure FIPS-compliance, select a certificate and corresponding security world private keys were generated on an SA Series FIPS Appliance.

4. Click **Restore**. The Secure Access Service must restart before changes can take effect. After the Secure Access Service restarts, you must sign back in to the Secure Access Service in order to access the admin console.

To save a local backup of your IVS configuration files:

1. In the admin console, choose Maintenance > Archiving > Local Backups.
2. Click Save IVS.

The resulting backup includes:

- IVS Profiles
  - IVS System
  - IVS Authentication
  - IVS Administrators
  - IVS Users
  - IVS Resource Policies
  - IVS Maintenance
3. When restoring, if you want to include IVS network settings, select IVS Profile Network Settings, then click Restore.

By selecting the IVS Profile Network Settings you can import references to VLAN ports and virtual ports in the imported IVS profiles.

**Related  
Documentation**

- [Specifying Archiving Parameters on page 891](#)
- [Importing and Exporting Secure Access Service Configuration Files on page 896](#)

## Importing and Exporting Secure Access Service Configuration Files

The Secure Access Service enables you to import and export Secure Access Service system and network settings using binary Secure Access Service configuration files. When importing a system configuration file, you can exclude the device certificate and the

Secure Access Service server's IP address or network settings from the imported information. For example, to set up multiple Secure Access Services behind a load balancer, import everything except for the IP address. To set up the Secure Access Service as a backup server, import everything except for the digital certificate and the network settings.



NOTE:

- Binary import of system and user configuration across different hardware platforms is not supported. For example, exporting a system configuration from an SA6000 device and importing it to an SA4500 device is not supported and may result in unexpected behavior.
- When importing a configuration file that contains licenses, the Secure Access Service gives precedence to any existing licenses that are currently installed on the Secure Access Service. Archived licenses are only imported if no licenses currently exist on the Secure Access Service.
- You may import an SA Series FIPS configuration file into a non-SA Series FIPS machine and vice versa provided that you do not include the certificate and security world in the import process.
- When importing certificates, note that the Secure Access Service only imports device certificates—not the chains corresponding to the device certificates or trusted client CAs.

The Secure Access Service also enables you to import and export all local user accounts you have defined for any local authentication servers.



NOTE:

- If you want to export resource policies, you must export user accounts, not the system settings. You can export resource policies on the Maintenance > Import/Export > Import/Export Users tab.
- To export or import client-side logs, export or import both the system and user configuration files.
- Sensor configurations are included in the system configuration file while sensor event policies are included in the user configuration file. To export or import sensor-related configuration to the Secure Access Service, export or import both the system and user configuration files.

The user configuration file, not the system configuration file, includes resource profiles, resource policies, and the local user database. To perform a complete backup, export both the system and user configuration files.

### Exporting a System Configuration File

Export the system configuration file to export:

Export the system configuration file to export:

- Network settings
- Cluster configuration
- Licenses
- SNMP settings

To export a binary system configuration file:

1. In the admin console, choose **Maintenance > Import/Export > Configuration**.
2. Under **Export**, enter a password if you'd like to password-protect the configuration file.
3. Click **Save Config As** to save the file.



**NOTE:** When exporting an SA Series FIPS configuration file, note that information about the machine's security world is included in the file. Therefore, you need an administrator card that is associated with the security world in order to successfully import the configuration file into another machine.

### Importing a System Configuration File



**NOTE:** Existing node-specific settings are erased when the Secure Access Service node joins a cluster. These settings including network interface addresses, route tables, virtual ports, ARP caches, VLAN interface, SNMP settings, and so forth. The administrator must manually re-configure these settings for the newly-joined node. You can not use the Import system configuration feature to import these configurations and settings onto the Secure Access Service node that has been joined to the cluster.

To import a configuration file:

1. Select **Maintenance > Import/Export > Import/Export > Configuration** in the admin console.
2. Specify whether you want to import the Secure Access Service certificate. The certificate is not imported unless you check the **Import Device Certificate(s)?** checkbox.



**NOTE:** When importing a device certificate in to an SA Series FIPS Appliance, note that you must choose a certificate that uses a FIPS-compliant private key. To ensure FIPS-compliance, select a certificate and corresponding security world private keys were generated on an SA Series FIPS Appliance.

3. Choose one of the following import options.
  - **Import everything (except Device Certificate(s))**—This option imports all configuration setting except Secure Access Service certificates.
  - **Import everything but the IP address**—This option excludes only the IP address from the imported configuration file. If you exclude the IP address, the server's IP address does not change when you import the file. When you select this option, the Secure Access Service also imports any SNMP settings that you have defined. In other words, choosing this option preserves the IP address, netmask, default gateway, VIPs, ARPs, and routes of the network interfaces on the target device.
  - **Import everything except network settings and licenses**—This option imports all configuration settings except the network and license settings.



**NOTE:** Always use this option when importing into a cluster. When importing into a cluster, we strongly suggest that you do not use any other option except this.

- **Import only Device Certificate(s)**—This option imports only the Secure Access Service server certificates. Be sure to enable the Import Device Certificate(s)? checkbox when using this option.
4. Browse to the configuration file, which is named `system.cfg` by default.
  5. Enter the password you specified for the file. If you did not specify a password before exporting the file, then leave this field blank.
  6. Click **Import Config**.



**NOTE:** When you import a binary configuration file, the selected Junos Pulse version of the device from which you are importing is included in the configuration. To prevent unexpected upgrade or downgrade of the client, select the Junos Pulse version that you wish to be active from the **Users > Junos Pulse > Components** page after you have imported the configuration.

When importing a device certificate and corresponding security world in to an SA Series FIPS Appliance, you must finish initializing the security world using the serial console and an administrator card that is associated with the new, imported security world.

### Exporting Local User Accounts or Resource Policies

Export the user accounts if you want to export:

- Sign in settings (includes sign in policies, sign in pages, and all authentication servers)
- Authentication realms
- Roles
- Network Access

- Resource profiles/resource policies
- User accounts
- Meeting configurations

To export local user accounts or resource policies:

1. In the admin console, choose **Maintenance > Import/Export > Import/Export User Accounts**.
2. Under **Export**, enter a password if you'd like to password-protect the configuration file.
3. Click **Save Config As** to save the file.

#### **Importing Local User Accounts or Resource Policies**

To import local user accounts or resource policies:

1. In the admin console, choose **Maintenance > Import/Export > Import/Export Users**.
2. Browse to the configuration file, which is named user.cfg by default.
3. Enter the password you specified for the file. If you did not specify a password before exporting the file, then leave this field blank.
4. Click **Import Config**.

#### **Related Documentation**

- [About System Archiving on page 889](#)
- [Specifying Archiving Parameters on page 891](#)
- [Importing and Exporting XML Configuration Files on page 901](#)
- [Importing and Exporting XML Configuration Data on page 910](#)
- [Using Operation Attributes on page 922](#)

---

## **Importing and Exporting IVS Configuration Settings**

Exporting IVS configuration saves the following settings in an encrypted file:

- IVS Profiles
- IVS System
- IVS Authentication
- IVS Administrators
- IVS Users
- IVS Resource Policies
- IVS Maintenance



To export IVS settings:

1. In the admin console, choose **Maintenance > Import/Export > Import/Export IVS**.
2. Under Export, enter a password if you'd like to password-protect the configuration file.
3. Click **Save Config As** to save the file.

To import IVS settings:

1. In the admin console, choose **Maintenance > Import/Export > Import/Export IVS**.
2. Browse to the configuration file, which is named `ivs.cfg` by default.
3. Enter the password you specified for the file. If you did not specify a password before exporting the file, then leave this field blank.
4. Select the **Import IVS Profile Network Settings** option to import references to VLAN ports and virtual ports listed in the imported IVS profiles.
5. Click **Import Config**.

**Related  
Documentation**

- [Importing and Exporting XML Configuration Files on page 901](#)
- [Importing and Exporting XML Configuration Data on page 910](#)

## Importing and Exporting XML Configuration Files

The XML Import/Export feature enables you to make significant changes to your system configuration and provides a number of benefits, particularly when it comes to making a large number of repetitive changes, or when you want to add, update, and delete configuration data all at once.

Some of the tasks you might want to perform using exported XML configuration files include:

- Adding a large number of users
- Deleting all or many of your auth servers, users, or other Secure Access Service objects
- Tracking configuration changes by performing a diff on weekly exports
- Modifying multiple instances of a single setting, for example, an auth server name
- Creating a configuration template to use when setting up new Secure Access Services



**NOTE:** You can only export and import XML instance files between Secure Access Services that have the same version of the Secure Access Service system software. You cannot use the XML Import/Export feature to upgrade an older product release from configuration files exported from a new product release. You also cannot downgrade a newer product release using configuration files exported from an older release of the product.

The Secure Access Service enables you to export several types of configuration data, including some network settings, sign-in settings, auth servers, realms, roles, resource policies, and users. You can then import those settings into the same or another Secure Access Service.



**NOTE:** When importing AD authentication server configuration with an XML file or through Push Config, the Computer Object name needs to be changed manually after the import. Unexpected problems might arise if two systems join an AD domain using the same Computer Object name.

You can export XML configuration files containing settings in the following list. Additional settings may also be available.

- **System Settings**—Licenses, certificates, Network Connect server IP address, nodes, node identifiers, DNS servers, DNS domains, hosts, NICs, NIC identifiers, virtual port addresses, source IP aliases, ARP cache, ARP ping timeout, default gateway, IP address, MTU, NIC name, net mask, static routes, link speed, NIC type, host name, licenses, and WINS address, SNMP settings, including trap settings and limits.



**NOTE:** You must never modify the two NIC identifiers in the XML instance file. The Secure Access Service relies on knowing that each appliance has two interface cards, known as NIC0 and NIC1.

The identifiers appear in the NIC elements `<NICIdentifier>0</NICIdentifier>` and `<NICIdentifier>1</NICIdentifier>`.

- **Sign-in Settings**—Authentication servers, password options, password management options, standard sign-in pages, custom text, header options, custom error messages, help options, page name, sign-in URLs, and page type.
- **Endpoint Security**—Host Checker policies, ESAP and Remote IMV servers and IMVs.
- **Authentication Realms**—User and admin realms, realm names, realm types, primary and secondary server settings, dynamic policy evaluation settings, authentication policies, limits, password policies, role mapping settings, and role processing option.
- **Roles**—User roles, admin roles, role names, enabled features, restrictions, session options, UI options, VLAN source IP, Windows and UNIX file settings, WSAM and JSAM settings, Web options, Junos Pulse Collaboration options, Network Connect options, Telnet options, terminal server options, Admin system options, and resource policy settings.
- **Resource Policies**—Web policies, file access policy lists, Telnet/SSH, Network Connect, Terminal Connect, and SAM policies.
- **Junos Pulse**—Component sets and Connection sets for Junos Pulse.
- **Local User Accounts**—Users, auth server name, email address, full name, login name, password, change password option, user status, and user type.

- **Maintenance Settings**—System options, push configuration targets, archiving and snapshot.
- **Meeting Configuration**—Meeting configuration settings.



**NOTE:** This may not provide a complete listing of settings. For a complete list of supported settings, consult the XML Import/Export page and the Push Config page on the admin console.

The basic process for exporting and importing an XML configuration file is as follows:

- Choose the configuration settings you want to modify.
- Export the file from the Secure Access Service.
- Open the file and edit configuration data in a text editor.
- Save and close the file.
- Import the file to the Secure Access Service.

## Creating and Modifying XML Instances

When you export your configuration file, the Secure Access Service saves the file as an XML instance. The instance is the file you will modify.

The XML file uses the same schema as push config and NSM. You can use XML files to troubleshoot instances of these files.

### The XML Instance

Upon export, the instance file shows you the current state of the Secure Access Service configuration. The XML instance is based on an XML schema. The schema is a separate file that defines the metadata, and which serves as a model or a template for the instance file. You will only use the schema file for reference purposes, if at all.

The data in the instance file is based on the selections you make on the XML Import/Export tab in the admin console when you perform the export operation.

Instance files usually end with the .xml file extension.

### Creating an Instance File

You can create an instance file by exporting an XML configuration file from the Secure Access Service. Even if you want to replace all of your existing configuration settings for a given object, you should start with an exported instance file. The exported instance file contains all of the required XML processing instructions and namespace declarations, which must be included exactly as defined.

### Editing the Instance File

All of the Secure Access Service's XML instance files share a similar structure. Once you become familiar with the basic structure, you should be able to navigate the files easily.

The files can become large, so you might find it more efficient to use a commercial or open source XML editor. XML editors often separate the editable data from the structural display. This separation reduces or eliminates the chance of accidentally modifying an XML element rather than its data, which is possible when editing in a simple text editor.

Despite the potential advantages of using an XML editor, you can do an adequate job of editing your configuration data using a simple text editor.

### Instance Elements

An element is a discrete XML unit that defines the Secure Access Service object or part of an object. The element typically consists of a pair of tags that may or may not surround string data. Tags are delimited by angle brackets (< >). You can find several examples of tags in the following discussion.

Every tag fits into one of the following tag types:

- **Start tag**—Defines the beginning of an element. The start tag consists of an open angle bracket (<), a name, zero or more attributes, and a close angle bracket (>). Every start tag must be followed by an end tag at some point in the document.
- **End tag**—Defines the end of an element. The end tag consists of an open angle bracket and a forward slash (</), followed by the same name defined in its corresponding start tag, and ends with a close angle bracket (>).
- **Empty tag**—The empty tag is denoted in two forms. If a tag pair has no data between them, the tag pair is considered an empty tag. Officially, according to the XML specification, an empty tag looks something like this:

```
<<empty tag example/>>
```

In this form, the empty tag consists of an open angle bracket (<), followed by an element name, a slash and a close angle bracket (>). When you see an empty tag in your configuration files, it signifies an element that the schema requires to be included in the instance file, but whose data is optional.

Start tags can contain attributes, and tag pairs (elements) can contain additional elements. The following example shows an XML instance file for the Users object. In this example, you see only the Administrator configuration settings. Italicized items signify user data.

```
<configuration xmlns="http://xml.juniper.net/ive-sa/6.2R1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <authentication>
 <auth-servers>
 <auth-server>
 <local>
 <users>
 <user>
 <username>admin</username>
 <fullname>Platform Administrator</fullname>
 <password-encrypted>3u+U</password-encrypted>
 <one-time-use>>false</one-time-use>
 <enabled>>true</enabled>
 <change-password-at-signin>>false</change-password-at-signin>
```

```

 </user>
 </users>
</local>
 <name>Administrators</name>
</auth-server>

```

You make your changes to the string data that appears between start and end tags. For example, from the preceding example, you can add to or change the following elements:

- <name>**Administrators**</name>
- <fullname>**Platform Administrator**</fullname>
- <username>**adminusername**</username>
- <password-cleartext>**password**</password-cleartext>
- <change-password-at-signin>**false**</change-password-at-signin>



**NOTE:** If you change a user for a given auth server or an auth server for a given user, you are creating a different user, not updating an existing user or auth server. User and auth server together logically define a unique user.

The preceding sample displays the Password element's data as encrypted data, indicating that you cannot change the password value. By default, the XML export operation provides encrypted passwords with a password-encrypted. You can modify the password, if you change the element to password-cleartext. If you modify the password in the instance file, the password value is visible until it is imported back into the Secure Access Service. Once imported, the Secure Access Service encrypts the password.

If you enter passwords for new users in cleartext format, the passwords are visible in the instance file, therefore, you might consider setting the Change Password at Next Login option to true.



**NOTE:**

- Because passwords are encrypted by default, they are fully portable from one system to another.
- You should never attempt to encrypt a password manually in the XML file. The Secure Access Service rejects any attempt to do so. Use the passwordcleartext and enter a text password when changing passwords through the XML file.

## Namespaces

Namespaces allow you to use the same words or labels in your code from different contexts or XML vocabularies. Prefixing elements with namespace qualifiers allows an instance file to include references to different objects that originate in different XML vocabularies and that share the same name. If you do not prefix elements with namespace

qualifiers, the namespace is the default XML namespace and you refer to element type names in that namespace without a prefix.

A namespace declaration looks like:

```
<configuration xmlns="http://xml.juniper.net/ive-sa/6.2R1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
```

When you see namespace identifiers in your instance files, you do not need to be concerned about them, as long as you do not delete or modify the identifiers.

### Element Sequence

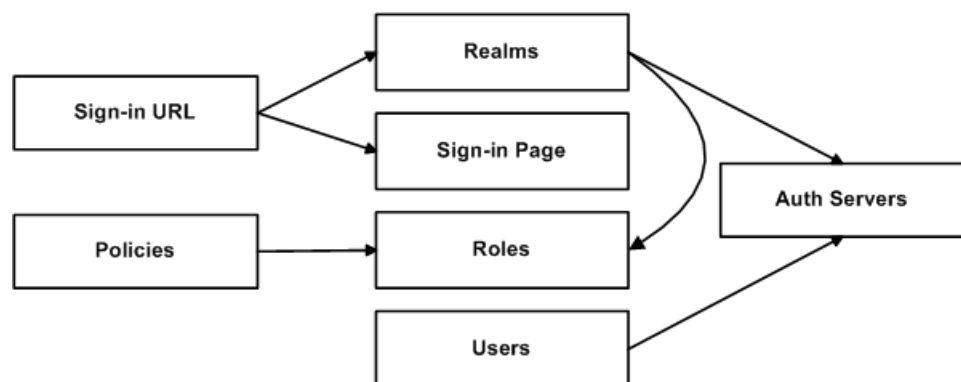
You should avoid changing the sequence of elements in the instance file, whenever possible. Although the schema does not enforce sequence in all cases, you gain no benefit from changing the order of elements from the order in which they appear in the exported instance file, and, in some cases, you might invalidate an instance document by changing element sequence.

## Integrity Constraints

Secure Access Service configuration objects are part of a data model that is enforced through the use of referential integrity constraints. You cannot change these constraints, but you should understand them before you attempt to delete objects that maintain dependencies to other objects.

If you violate the Secure Access Service referential integrity constraints, your import operation fails. The following diagram illustrates the relationships among several Secure Access Service objects.

**Figure 68: Secure Access Service Object Referential Integrity Constraints**



In [Figure 68 on page 906](#) the boxes represent Secure Access Service object types and the arrows represent dependent relationships between the object types. Arrows point from dependent objects to objects.

The system does not allow you to delete an object upon which another object depends. Conversely, when you add an object, you must add any other objects upon which that object depends.

In [Figure 68 on page 906](#), sign-in URLs depend upon realms and sign-in pages. Realms depend upon both auth servers and roles. Policies depend upon roles. Users depend upon auth servers.

Consider the following scenarios based on [Figure 68 on page 906](#):

- If you add sign-in URLs, you must add realms, sign-in pages, roles, and auth servers. You need to add an auth server and at least one role to support the realm, and you need to add the realm and the sign-in page to support the new sign-in URL.
- If you add a user, you must be able to assign it to an auth server. If there is no auth server on the target Secure Access Service yet, you must add one in the instance file.
- If you add a policy, you must be able to assign it to a role. If there is no role on the target Secure Access Service yet, you must add one in the instance file.
- If you delete an auth server, you might strand realms and users, therefore, you need to make sure no realms or users depend on the auth server before you attempt to delete it.
- If you delete a role, you might strand policies and realms. To delete a role, you must first delete any policy that depends upon the role, or reassign associated policies to another role. Also, to delete a role, you must first delete or reassign any realm that depends upon that role.
- If you delete a sign-in page, you might strand one or more sign-in URLs. To delete a sign-in page, you must first delete any associated sign-in URLs or reassign them to other sign-in pages.

Referential integrity checks are performed only during XML Import.

## Mapping the XML Instance to UI Components

The elements in the XML instance are closely related to the objects and their options as you see them in the admin console. The element names in the XML instance file correlate closely with the displayed object and option names.

For example, go to **Users > User Roles > [Role] > General > Session Options** in the admin console. The admin console renders the possible values for a roaming session as a radio button group, consisting of the values:

- **Enabled**
- **Limit to subnet**
- **Disabled**

The following snippet, from the exported configuration file, shows the session options for the Users role. The roaming session option is set to disabled:

```
<session-options>
 <idle-timeout>10</idle-timeout>
 <max-timeout>60</max-timeout>
 <reminder-time>5</reminder-time>
 <session-timeout-warning>>false</session-timeout-warning>
 <session-timeout-relogin>>true</session-timeout-relogin>
```

```
<roaming>disabled</roaming>
<netmask></netmask>
<persist-session-cookie>disabled</persist-session-cookie>
<persist-passwords>disabled</persist-passwords>
<request-follow-through>disabled</request-follow-through>
<session-idle-timeout-skip>disabled</session-idle-timeout-skip>
</session-upload-log>>false</session-upload-log>
```

In the schema file, you can locate the allowable values for the roaming session option:

```
<Attribute roaming:START>
<xsd:element name="roaming" minOccurs="0" >
...
<xsd:enumeration value="enabled">
...
<xsd:enumeration value="limit-to-subnet">
...
<xsd:enumeration value="disabled">
...
</xsd:element>
<Attribute roaming:END>
```

If you want to change the value for the roaming session from disabled to limit to subnet, replace disabled with limit-to-subnet.

This example shows you that the admin console often provides all of the allowable values, displayed either in a radio button group, as checkboxes, as drop down listboxes, or as other types of user interface components. The instance file displays only the current state of your Secure Access Service configuration. The schema file displays all of the actual values for the configuration options that are supported in the XML Import/Export feature.

For more information about specific elements, review the schema files directly.

## Downloading the Schema File

You can download the schema (.xsd) file for the Secure Access Service objects, if you want to review the structure and rules that apply to the objects.

You can download the schema file in two ways:

- From the XML Import/Export pages, by clicking a hyperlink.
- Directly, by accessing the URL where the files are stored on the system.

To access the .xsd file, access the following URL, either directly or by way of a script:

```
https://<IP-or-hostname>/dana-admin/cached/xml/config.xsd
```

where IP-or-hostname is the Secure Access Service's IP address or hostname. Using this method, you do not need to sign in to the Secure Access Service.





---

**NOTE:**

This feature might change in the future. Be aware of this if you use scripts to access the zip file by way of the URL. The items that might change are:

- The URL
  - The filename
  - The file extension
- 

## Strategies for Working With XML Instances

The following strategies might be useful to you when exporting and importing XML instance files:

- Define your goal for a given XML Import/Export operation.
  - What Secure Access Service object or objects do you need to add, update, or delete?
  - Do you need to complete all modifications in one operation, or can you modify the configuration in separate operations?
  - Will your process be a one-time operation, or will you need to perform the same operation multiple times?
  - Are you updating an existing Secure Access Service, or are you using one Secure Access Service configuration as a template for configuring other Secure Access Services?
- Document the changes to the Secure Access Service objects you intend to modify.
  - Make a list of objects to be added, updated, or deleted.
  - For objects to add or update, list specific attribute data.
  - List pages or tabs from the admin console that correspond to the objects and attributes you intend to change.
- Make a binary system snapshot or a binary configuration backup immediately before performing the import.
- Make a plan to verify that the completed configuration meets your goals.
  - Check the Admin Access log to make sure the export and import operations succeeded.
  - Perform a random check of the modified items. Make sure items were added, updated, or deleted as you expected.

You will almost always need to use the XML instance file and the admin console in combination, particularly when you first begin modifying the XML instance files. You may also need to view the XML schema files.

Use the XML instance file to:

- Identify the configuration objects, expressed as XML elements.
- Locate and modify the configuration data.

Use the admin console to:

- Correlate visual components to XML schema and instance elements.
- Confirm the accuracy of modifications to specific objects.

Use the XML schema file to:

- Identify the structure and sequence of configuration objects.
- Identify optional and required elements, allowable values, default values, and other attributes of the configuration objects.

**Related  
Documentation**

- [Importing and Exporting IVS Configuration Settings on page 900](#)
- [System Restarts on page 916](#)
- [XML Import/Export Use Cases on page 918](#)
- [Using Operation Attributes on page 922](#)

---

## Importing and Exporting XML Configuration Data

### Importing XML Configuration Data

To import XML configuration data:

1. Choose **Maintenance > Import/Export > Export XML** in the admin console.
2. Under Schema Files, click the link to download the XML Schema (.xsd) files that describe the Secure Access Service objects (Optional).
3. Browse to, and select, the XML data file that you want to import. You can import a valid XML fragment file if you want to import only a partial configuration.
4. Click Import. The Import XML Results page displays containing information about the imported network settings, roles, resource policies, and other settings.

If there are errors in the XML, the import operation stops and rolls back the configuration to the previous state. Error messages are displayed on the Import XML Results page.

5. Click **OK** to return to the Import page.

Please note the following when importing XML configuration data:

- An import resource policy is associated with a role that does not exist on the target Secure Access Service and the role does not exist in the XML file. The XML import process fails.
- An import resource profile is associated with a role that does not exist on the target Secure Access Service and the role does not exist in the XML file. The XML import process fails.
- An imported resource profile contains a bookmark and an associated role but the bookmark reference within the role is missing.
- An imported resource profile is associated with a role. That role is associated with a bookmark but the bookmark is missing in the resource profile.
- An import resource profile contains a resource policy not present in the list of resource policies. The resource policy reference is re-created on the target Secure Access Service and an error is logged.
- The imported resource profile is a child of another resource profile but the parent profile does not exist. The XML import process fails.
- Hosted Java applets are treated as BLOB data types and are imported as base 64 encoded chunks of data.
- Code signing certificates can not be imported or exported.
- An imported role bookmark is a child of a resource profile but the resource profile is not present in the configuration file. The bookmark is not imported and an error is logged. This can occur when, for example, you export a role without exporting the resource profile and then import this configuration file to a new Secure Access Service.
- An imported child resource policy is missing a parent profile in the configuration data. The child resource policy is deleted (not imported).
- A child resource policy contains a detailed rule that does not exist in the parent resource profile. The import validation process fails and the XML import process fails.
- (when only resource profiles are exported) If new resource policy references are created on the Secure Access Service that does not already have those resource policies, the new resource policies are inserted ahead of the existing resource policies.  
  
For example, suppose there are four resource policies: resource\_policy\_A, resource\_policy\_B, resource\_policy\_C, and resource\_policy\_D and resource\_policy\_B and resource\_policy\_D are child resource policies of resource\_policy\_parent. Export only resource\_policy\_parent from the source Secure Access Service and import that policy onto the target Secure Access Service. Resource\_policy\_B and resource\_policy\_D are created on the target Secure Access Service. Now export all four resource policies from the source Secure Access Service and import them in the target Secure Access Service. The resulting order of the resource policies is resource\_policy\_A, resource\_policy\_C, resource\_policy\_B, resource\_policy\_D.
- (when only resource profiles are exported) Any settings with device certificates configured for SOAP client authentication are not imported since device certificates are not portable.

- (when only resource profiles are exported) Importing CDPs is not supported.
- An ESAP package does not contain support for a product that is configured in any of the Host Checker rules. Importing the ESAP package fails.
- The following Host Checker conditions must be met, otherwise an error occurs:
  - Custom expressions defined in a Host Checker policy must only reference rules configured within that Host Checker policy.
  - Host Checker policies must contain only rule types valid for that platform. For example, you can not have Predefined AV rules for Macintosh or Linux platforms.
  - Antivirus, firewall, and spyware policies must contain only the types that are available in the currently activated ESAP packages.
- You can import a license only on to the same system. You can not import a license from a different Secure Access Service (an error is logged).
- Importing clustering is not supported.

### Exporting XML Configuration Data

Note the following when exporting XML configuration data:

- Resource policies that exist in resource profiles are exported. However, the resource policy entry in the resource policies table are not exported.
- Resource profile bookmarks are exported but the same bookmark entry under Roles is not exported.
- Role associations are exported but individual role data is not.
- Hosted Java applets are treated as BLOB data types and are exported as base 64 encoded chunks of data.
- Exporting CDPs is not supported.
- Jedi-package files are exported as encrypted BLOBs.
- Third-party policies are exported as the main policy plus the Jedi package (as a zip file) and a set of sub-policies. You can not export any of these items separately.
- ESAP packages are exported as encrypted BLOBs.
- The AV signature data file associated with Virus Signature Version Monitoring is exported as an encrypted BLOB.
- There is no option to select VLAN/Source IP settings for exporting. However, these settings are exported with the role to which they are associated.

To export XML configuration data:

1. Choose **Maintenance > Import/Export > Export XML** in the admin console.
2. (optional) Under Schema Files, click the link to download the XML Schema (.xsd) file that describe the Secure Access Service objects (Optional).

3. Click **Expand All** to view all settings; click **Select All** to select all settings identified on the page. Otherwise, select the specific information you want to export. Within each section, you can click Select All to select all settings within that particular section:
4. Select the **System Settings** checkbox to export network settings, including internal port settings, external port settings, and licensing information. Options include:
  - **System date and time**—exports the server time zone and Network Time Protocol (NTP) settings.
  - **Cockpit page**—exports settings on the System Status Overview page, such as the graphs to display and the refresh rate.
  - **Licenses**—exports the licenses in an encrypted format.

**NOTE:**

The following rules apply to exported and imported licenses:

- You cannot edit the license data that is exported, as it is encrypted.
- An XML import of licenses is only valid if the machine importing the license does not currently have a license installed. If there is a license installed already, any imported licenses are dropped. If you still intend to import a license, you must perform a factory reset on the Secure Access Service, then perform the import operation.
- If you import a license after deleting a temporary license from the Secure Access Service, the imported license will be dropped, because you might still be able to reactivate the deleted license and the import operation attempts to preserve any licensing data currently on the Secure Access Service.

- **DMI Agent**—exports the DMI Agent settings, such as primary server and port number, back-up server and port number, device ID and realm.



**NOTE:** The DMI Agent is used for interfacing with network management applications over the DMI interface. Do not select this option unless instructed to do so by Juniper Networks Technical Support.

- **NCP**—exports the NCP options, such as auto-select value, read connection timeout and idle connection timeout.
- **Sensors**—exports sensor events and sensor policies.
- **Client Types**—exports the client types and their matching user-agent string pattern.
- **Junos Pulse Collaboration**—export Junos Pulse Collaboration configuration settings, such as session lifetime settings, root meeting URL, and email meeting notification settings,
- **Security**—exports security configuration settings, including SSL and TLS versions, encryption strength, SSL handshake timeout value, and cookie options.

- **Overview**—exports settings on the Network Settings Overview tab, such as DNS, WINS and bandwidth management.
  - **Internet Port**—exports settings on the Network Settings Internal Port tab, such as IP address, netmask, default gateway, link speed, ARP ping timeout, and MTU.
  - **External Port**—exports settings on the Network Settings External Port tab, such as IP address, default gateway, link speed, ARP ping timeout and MTU.
  - **VLANs**—exports settings on the Network Settings VLAN tab, such as name, ID, IP address, netmask and gateway.
  - **Routes**—exports settings on the Network Settings Routes tab, such as IP address, netmask, gateway and interface.
  - **Hosts**—exports settings on the Network Settings Hosts tab, such as IP address and name.
  - **Clustering**—exports clustering properties, such as the cluster name, configuration settings, synchronization settings, and network healthcheck settings. This option is visible only when the device is part of a cluster.
  - **Events**—exports event log settings, such as max log size, syslog server, and which event to log.
  - **User Access**—exports user access log settings, such as max log size, syslog server, and which event to log.
  - **Admin Access**—exports admin access log settings, such as max log size, syslog server, and which event to log.
  - **Sensors**—exports sensor log settings, such as max log size and syslog server.
  - **Client Logs**—exports client log settings, such as which client-side feature to log and disk space size.
  - **SNMP**—export SNMP log settings, including node name, system name and location, trap settings and limits.
5. Select the **Sign-in Settings** checkbox to export Authentication servers, password options, password management options, standard sign-in pages, custom text, header options, custom error messages, help options, page name, sign-in URLs, and page type.
    - From Sign-in URLs, choose **ALL sign-in URLs** to export all sign-in URLs or choose **SELECTED sign-in URLs** to specify which sign-in URLs to export.
    - From Sign-in Pages, select **ALL Pages** to export all sign-in pages, **SELECTED pages** to specify which sign-in pages to export, or **ONLY pages used by URLs selected above** to export only those pages that are valid for the sign-in URLs selected above.
    - From Authentication servers, select **ALL auth servers** to export all authentication servers or **SELECTED auth servers** to specify which authentication servers to export.
  6. Select the **Endpoint Security** checkbox to export Host Checker and Cache Cleaner settings.

- From Host Checker, choose **Host Checker options** to export settings in the Endpoint Security Host Checker tab, including live update settings and interval and timeout values. The exported antivirus signature data file associated with the virus signature version monitoring option is encrypted.
  - Select **ALL policies** to export all Host Checker policies or choose **SELECTED** policies to specify which Host Checker policies to export. JEDI package files are encrypted. Third-party policies are exported as the main policy plus the JEDI package plus any sub-policies. You can not separate out these packages for export.
  - Select **Remote IMV** to export all remote IMV servers settings and remote IMV rules.
  - Select **ESAP** to export all ESAP settings. ESAP packages are encrypted when exported.
  - Select **Cache Cleaner settings** to export Cache Cleaner options defined in the Endpoint Security Cache Cleaner tab, including update frequency, browser cache settings and file and folder settings.
7. Select the **Authentication Realms** checkbox to export administrator and user authentication realms.
- Within each group,
- Select **ALL resource realms** to export all realms within that group.
  - Select **SELECTED realms**, select realms from the Available Realms list, and click **Add** to export only those selected authentication realms.
8. Select the **Roles** checkbox to export admin and user roles.
- Choose **ALL roles** to export all roles within that group.
  - Choose **SELECTED roles**, select roles from the Available Roles list, and click **Add** to export only those selected roles.
9. Select the **Resource Profiles** checkbox to export resource profile settings, including the list of associated resource policies, bookmarks and roles.
- Select **Hosted Java Applets** to export all applets that have been uploaded to the system. You can not select individual java applets to export.
- Choose **ALL resource profiles** to export all resource profiles within that group.
  - Choose **SELECTED resource profiles**, select profiles from the Available Profiles list, and click **Add** to export only those selected profiles.
- Within each group,
10. Select the **Local User Accounts** checkbox to export local user accounts.
- Choose **From ALL local auth servers** to export all local user accounts from all of the local authentication servers.
  - Choose **From SELECTED local auth servers**, select authentication servers from the Available Servers list, and click **Add** to export local users from only those authentication servers.
11. Select the **Maintenance Settings** checkbox to export

- **System Options**—exports the settings on the System Maintenance Options tab.
  - **Push Config Targets**—exports selected targets and whether this device can accept push configurations.
  - **Archiving**—exports archive settings, such as the archive server, destination directory, username and password, and the components to archive.
  - **Snapshot**—exports system snapshot options, including automatic snapshot settings and whether to include system configuration and debug logs.
12. Select the IVS Settings checkbox to export IVS settings and profiles. You can not export an IVS's local user settings from this window.
- Choose **All IVSes** to export settings from all IVSes.
  - Choose **SELECTE IVSes**, select an IVS from the Available Servers list, and click **Add** to export settings from only those IVSes.
  - Select **IVS Profiles** to export all IVS profile information. The IVS profile defines the subscriber IVS and any elements required to reach the subscriber's intranet, such as DNS settings and authentication servers.
  - Select **IVS Configuration** to export IVS configuration data. This does not include an IVS's local user account information.
13. Click **Export** to save the information in an XML file.

**Related Documentation**

- [Importing and Exporting XML Configuration Files on page 901](#)
- [System Restarts on page 916](#)
- [XML Import/Export Use Cases on page 918](#)
- [Using Operation Attributes on page 922](#)

## System Restarts

While every attempt has been made to reduce the number of restarts, some changes still require restarting the server. The following table lists the system behavior when certain options are changed. Restarts occur after you change and save these settings and when you import an XML configuration that contains different values.

**Table 56: System Behavior When Editing Options**

Window	System Behavior
System > Status > Overview	All processes update their time zone settings when updating the System Date and Time time zone.
Authentication > Auth Servers > NIS Server	Restarts Linux YP services
System > Log/Monitoring > SNMP	SNMP Server restarts



Table 56: System Behavior When Editing Options (*continued*)

Window	System Behavior
Authentication > Signing In > Sign-in Policies	Web server restarts
System > Configuration > NCP	Web server restarts
Users > Resource Policies > Files > Options	dsstartws restarts when you change the encoding and the browser server restarts.
System > Configuration > NCP	Web server restarts
Maintenance > System > Options	Web server restarts
System > Configuration > Security	Changing the following options restarts the web server with new SSL settings: <ul style="list-style-type: none"> <li>• Allows SSL and TLS version</li> <li>• Allowed Encryption Strength</li> <li>• Encryption Strength Option</li> <li>• SSL Handshake Timeout</li> </ul>
Auth Servers	Creating a nete auth server or changing any nete option restarts the nete server
Users > Resource Policies > Email Client	Turns on or off dspopd, dsimapd, and dssmtpd depending on the state of "email-state-support" and the corresponding mail server settings
Maintenance > System > Options	Restarts dscrld and dsstartws. Starts rwcached if the option is currently off.
System > Configuration > Certificates > Trusted Client CAs > <i>certificate name</i> > CRL Checking Options	Rescans the CDPs (CRL Distribution Points)
System > Network > Internal Port	Restarts network services and then the web server
System > Network > Management	Restarts network services which in return restarts the web server
System > Network > Port 1/External Port	Restarts network services which in return restarts the web server
System > Network > Routes	Restarts network services which in return restarts the web server
System > Network > Hosts	Restarts network services which in return restarts the web server
Authentication > Auth Servers > ACE	Extracts the contents of the ACE file and writes the contents to the installation directory

**Table 56: System Behavior When Editing Options (continued)**

Window	System Behavior
System > Configuration > License	Restarts various services

**Related Documentation**

- [Importing and Exporting XML Configuration Files on page 901](#)
- [Importing and Exporting XML Configuration Data on page 910](#)
- [XML Import/Export Use Cases on page 918](#)
- [Using Operation Attributes on page 922](#)

## XML Import/Export Use Cases

The following use cases illustrate common examples of how you can use the XML Import/Export feature. Each use case consists of a brief description and a procedure for accomplishing the use case. These use cases are abbreviated and do not cover all of the intricacies and details of performing a full set of procedures. The use cases are included solely as illustrations of the potential uses for the XML Import/Export feature.

**Use Case: Adding Multiple New Users to the Secure Access Service**

You have just added a new Secure Access Service to your network, and you want to add your two thousand users to the system. You do not want to add them one at a time in the admin console, but would like to perform a mass import and force the users to change their passwords the first time they log in to the system. You can export the user accounts, extract the relevant XML that defines users, replicate each element as needed, then import them to the Secure Access Service.

In this procedure, you only see examples for User 1, User 2, and User 2000. All other users are assumed as being included in your import file. You set the passwords to numbered instances of the word password, such as password1, password2, and so on. All users in this example are assigned to the same auth server, although you can specify any combination of auth servers that are valid on your system.

To add multiple new users to the Secure Access Service:

1. In the admin console, go to **Maintenance > Import/Export > Export XML**.
2. Follow the instructions to export local user accounts.
3. Save the exported file as *users.xml*.
4. Open the *users.xml* file.
5. Copy and paste the User container element until you have added the necessary number of users. Although the example shows only three new users, you might add hundreds of new users to the file.
6. Update the appropriate data in each User container element, as shown in the following example:



## NOTE:

- The formatting in the following example has been modified from the original to improve readability. The actual XML code may appear differently.
- You must change password to password-cleartext, otherwise the Secure Access Service assumes a default of encrypted.

```
<configuration xmlns="http://xml.juniper.net/ive-sa/6.2R1"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
 <authentication>
 <auth-servers>
 <auth-server>
 <local>
 <users>
 <user>
 <username>user1</username>
 <fullname>User1</fullname>
 <password-cleartext>password1

 </password-cleartext>
 <one-time-use>>false</one-time-use>
 <enabled>>true</enabled>
 <change-password-at-signin>>true

 </change-password-at-signin>
 </user>
 <user>
 <username>user2</username>
 <fullname>User2</fullname>
 <password-cleartext>password2

 </password-cleartext>
 <one-time-use>>false</one-time-use>
 <enabled>>true</enabled>
 <change-password-at-signin>>true

 </change-password-at-signin>
 </user>
 </name>System Local</name>
 </auth-server>
 </auth-servers>
 </authentication>
 </configuration>
```

7. Save the *users.xml* file.
8. In the admin console, go to **Maintenance > Import/Export > XML Import/Export > Import**.
9. Click **Browse** and locate your *users.xml* file.
10. Click **Import**.

## Use Case: Updating Policies

You want to change all ActiveX rewriting policies from an action of `rewrite-url-response-static-dynamic` to another action, but you do not want to enter each policy separately in the admin console. Instead, you can export an instance file, make your changes, then import the file back to the Secure Access Service.

To update policies on the Secure Access Service:

1. In the admin console, select **Maintenance > Import/Export > XML Import/Export > Export**.
2. Export your resource policies and save the exported file as `policy.xml`.
3. Open the exported file.
4. Open the `policy.xsd` schema file on your system, using either a text editor or an XML editor. In the schema file, search for the action value `rewrite-url-response-static-dynamic`. The schema definition includes the current policy action value, as well as the other possible values, as shown in the following example:

```
<xsd:simpleType>
 <xsd:restriction base="xsd:token">
 <xsd:enumeration value="rewrite-url-response-static">
 <xsd:annotation>
 <xsd:appinfo>
 <dmi:enum-info>
 <title>Rewrite URL and response (Static HTML
 <only></title>
 </dmi:enum-info>
 </xsd:appinfo>
 </xsd:annotation>
 </xsd:enumeration>
 <xsd:enumeration value="rewrite-url-response-static-dynamic">
 ...
 <xsd:enumeration value="rewrite-url-static">
 ...
 <xsd:enumeration value="rewrite-url-static-dynamic">
 ...
 <xsd:enumeration value="rewrite-hostname-static">
 ...
 <xsd:enumeration value="rewrite-hostname-static-dynamic">
 ...
 <xsd:enumeration value="rewrite-url-hostname">
 ...
 <xsd:enumeration value="rewrite-data">
 ...
 <xsd:enumeration value="no-rewrite">
 </xsd:restriction>
</xsd:simpleType>
```

5. In the exported `policy.xml` file, search and replace `rewrite-url-response-static-dynamic` with the action value of, for example, `rewrite-url-static-dynamic`.



**NOTE:** The following example shows only a fragment of the actual policy.xml file. Also, the formatting has been modified from the original to improve readability. The actual XML code may appear differently.

```
<activex-param>
 <classid>5BDBA960-6534-11D3-97C7-00500422B550</classid>
 <description>iNotes Discussion </description>
 <params>
 <param>
 <parameter>FullUrl</parameter>
 <!-- Change the following data -->
 <action>rewrite-url-response-static-dynamic</action>
 </param>
 </params>
</activex-param>
```

6. Save the policy.xml file.
7. In the admin console, select **Maintenance > Import/Export > XML Import/Export > Import**.
8. Click **Browse** and locate your policy.xml file.
9. Click **Import**.

#### Use Case: Using XML Import/Export in a Clustered Environment

You can use the XML Import/Export feature in a clustered environment. You must, however, adhere to certain rules and you must follow a particular procedure to complete the operation successfully.

- The XML instance you want to import must contain the same set of nodes as the original cluster. The signature used to synchronize the cluster when the nodes are re-enabled is derived from the IP addresses of the cluster nodes, so the remaining nodes cannot rejoin the cluster if the imported configuration yields a different signature.
- Do not modify node name, IP address, or IP netmask in the instance file.
- Do not change any network settings in the instance file that render the primary node unreachable. For example, do not change the default gateway configuration for a multi-site cluster.
- On import, the instance file overwrites the node-specific cluster configuration network settings of the remaining nodes. If you change these node-specific network settings, make sure you do not make the remaining nodes unreachable.
- Do not modify existing virtual port settings or add new virtual port settings in the instance file.
- When performing an import operation on a cluster, all of the cluster nodes should be enabled and running. If you attempt to import a configuration into a cluster in which a node is not running, the import operation may hang or your import results may be unpredictable.

- Related Documentation**
- [Importing and Exporting XML Configuration Files on page 901](#)
  - [Importing and Exporting XML Configuration Data on page 910](#)
  - [System Restarts on page 916](#)
  - [Using Operation Attributes on page 922](#)

---

## Importing to a System with the Management Port

If you import a configuration from a system that does not support a management port into a system that has an enabled management port and you import everything, including licenses, the management port on the target system will appear to be removed. The management port actually continues to be operational and will reappear along with its original configuration when you reapply the management port license for the target system. If you import to the target but specify the option `Import everything except network settings and licenses`, the management port and its configuration persist on the target system and the port is operational.

- Related Documentation**
- [Troubleshooting the Management Port on page 835](#)

---

## Using Operation Attributes

Data editing operations are determined by the operation attribute of the element in imported XML data. Operation attributes define the positioning or action of XML data within the schema. If you do not specify an operation attribute, the modified data is merged by default.

The operation attribute is applied to all children objects unless a new operation attribute is defined in children objects.

XML data with an operation attribute has the following format:

```
<object1 xc:operation="operator for object1 and its children unless new operator is defined">

 <object2>
 ...
 <object3 xc:operation="operator for object3">
 ...
 </object3>
 ...
 </object2>
 ...
</object1>
```

Following are the supported operation attributes:

- **Merge**—The configuration data identified by the element containing this attribute is merged with the configuration at the corresponding level in the configuration datastore identified by the target parameter. This is the default behavior.
- **Replace**—The configuration data identified by the element containing this attribute replaces any related configuration in the configuration datastore identified by the target parameter. Only the configuration actually present in the config parameter is affected.
- **Create**—The configuration data identified by the element containing this attribute is added to the configuration if and only if the configuration data does not already exist on the device.
- **Delete**—The configuration data identified by the element containing this attribute is deleted in the configuration datastore identified by the target parameter.
- **Insert before**—Change the position of a configuration element in an ordered set.
- **Insert after**—Change the position of a configuration element in an ordered set.
- **Rename**—Change the name of one or more of a configuration object's identifiers.

If you are merging a listing of objects to an existing list of objects in the configuration store, the results of the merged list of objects could be unexpected. During a merge operation the order of the objects in the new list is not maintained. If you are importing a listing of objects and would like to preserve the order of the new list, you should use the replace operation attribute. You can also use insert before or insert after to ensure that you produce the hierarchy that you intended.

Operation attributes are applied to elements recursively unless new operators are also defined within lower level elements. There are limitations on the legal operator that can be used in child elements without conflict with the parent operator. [Table 57 on page 923](#) displays the legal operator relationships between parent and child elements.

**Table 57: Legal Operation Attribute Relationships**

Child > V-Parent	Create	Merge	Replace	Delete	Insert before	Insert after	Rename
None	OK	OK	OK	OK	OK	OK	OK
Create	OK	OK	Error	Error	OK	OK	Error
Merge	OK	OK	OK	OK	OK	OK	OK
Replace	Error	OK	OK	Error	OK	OK	Error
Delete	Error	OK	Error	OK	Error	Error	Error
Insert before	OK	OK	OK	OK	OK	OK	OK
Insert after	OK	OK	OK	OK	OK	OK	OK

**Table 57: Legal Operation Attribute Relationships (continued)**

Rename	OK	OK	OK	OK	OK	OK	OK
--------	----	----	----	----	----	----	----

Following are two examples of the import operation:

Example 1: Set the MTU to 1500 on an interface named "Ethernet0/0" in the running configuration.

```
<interface>
 <name>Ethernet0/0</name>
 <mtu>1500</mtu>
</interface>
```

Example 2: Add an interface named "Ethernet0/0" to the running configuration, replacing any previous interface with that name.

```
<interface xc:operation="replace">
 <name>Ethernet0/0</name>
 <mtu>1500</mtu>
 <address>
 <name>192.0.2.4</name>
 <prefix-length>24</prefix-length>
 </address>
</interface>
```

## General Import Rules

The default import modes have equivalent attributes on the root object of the configuration tree:

- Standard Import is always a merge operation.
- Quick Import is a create operation.
- Full Import is a replace operation.

### Related Documentation

- [Importing and Exporting XML Configuration Files on page 901](#)
- [Importing and Exporting XML Configuration Data on page 910](#)
- [System Restarts on page 916](#)
- [XML Import/Export Use Cases on page 918](#)

## Using the Push Configuration Feature

You use the Push Configuration feature to synchronize configurations for multiple Junos Pulse Secure Access Service installations. You might want to do this, for example, to push the initial configuration to a newly deployed device; or to roll out changes to policies, feature configuration, or network settings to a group of devices.

Like the Export XML feature, the user interface for the Push Configuration feature allows you to select all configuration settings or selected configuration settings.



The user interface includes the following tabbed pages:

- Configuration Push—Select source settings and targets. Run the Push Configuration operation.
- Targets—Configure a target list, including connection details and certificate-based security.
- Results—View messages related to Push Configuration jobs.

The Push Configuration job processes the target list in order. If a push operation fails, the Push Configuration process continues to the next target in the list until all identified targets are updated. The results page displays the status and any problems encountered during the process.



**NOTE:** You can also push configuration elements to a Junos Pulse Access Control Service to distribute a Junos Pulse client configuration. A common configuration among Junos Pulse services is required to enable location awareness for Junos Pulse clients.

Note the following when pushing configurations:

- The source and target Secure Access Service software must have the same build version and number.
- If either the source or target has an IVS license, you must push all configuration settings. You cannot select which settings to push.
- You cannot push the following configurations: licensing, clustering, networking and timezone.
- When importing Active Directory (AD) authentication server configuration with Push Configuration (or with XML import), the Computer Object name needs to be changed manually after the import. Unexpected problems might arise if two systems join an AD domain using the same Computer Object name.
- During the configuration update, administrators are automatically logged out of the target device Admin Console.
- Targets do not display notifications or event messages indicating they are receiving pushed configurations.
- After the target configuration has been updated, the target device restarts its services. Brief interrupts may occur while the service restarts. We recommend you perform Push Configuration operations when targets are idle or when you can accommodate brief interruptions.
- The source pushes data only over the internal port or the Management Port (on the Juniper Networks SA 6000, if configured.) The target can receive data over the internal, external, or Management Port (on the Juniper Networks SA 6000, if configured.)

- You can push up to 8 targets per push operation; up to 25 push operations can be run simultaneously. The maximum number of targets is 200.
- The Results tab displays messages for the last 25 jobs.

The Push Configuration feature depends on the ability of Push Configuration process to sign into the target without any human interaction. Follow these guidelines when configuring administrator accounts:

- You must map the administrator account to the .Administrators role, thereby creating a “super administrator” with full administration privileges. Use the Authentication > Auth Servers > Administrator Server > Users tab to perform this mapping.
- The target administrator account must use static password authentication or two-factor tokens that do not use challenge-response type authentication. For example, certificates, Soft ID, and Defender Authentication are not supported. Use settings in the Administrators > Admin Realms > [Administrator Realm] > General tab to select the proper authentication server for the administrator realm.
- You must not configure the administrator account in a way that requires the administrator to select a role to sign in to the target. For example, you must not map a single user to multiple roles, including the push configuration administrator role, and then fail to permissively merge those roles. We recommend creating an account exclusively for push configuration administrators to guarantee that the administrator does not need to choose a role during the sign-in process and to clearly distinguish the actions of push configuration administrators in your log files. Use settings in the Administrators > Admin Realms > [Administrator Realm] > Role Mapping tab to set the appropriate role-mapping rules.

The source SA Series Appliance connects to the target SA Series Appliances on port 443. Apart from port 443, there is no need to open other ports for pushing configurations.

**Related  
Documentation**

- [Defining Push Configuration Targets on page 926](#)
- [Pushing Configuration Settings on page 928](#)

---

## Defining Push Configuration Targets

---

You use the Push Config > Targets page to build a list of Junos Pulse Secure Access Service hosts to which to push configuration settings. Targets added to this list can then be selected on the Push Config > Push Configuration page.

In terms of configuration push operations, the Secure Access Service to which you are logged in is called the *source*. Other Secure Access Service deployments are possible *targets* that can receive configuration information from the source.

Observe the following guidelines when you define configuration push targets:

- A target must *not* belong to the same cluster as the source. Cluster configurations are synchronized using a different method.
- A target must be set up with an admin user account, with full administration privileges, that is accessed during the configuration push operation.
- A target must have Push Config > Targets > “Allow this Junos Pulse Secure Access Service to be a target” setting enabled. This setting is enabled by default.
- We recommend you enable the Push Config > Targets > “Validate target server certificate” option to prevent possible man-in-the-middle attacks (for example, an attacker impersonating a target in order to receive Secure Access Service configuration data). The option is disabled by default to preserve backward compatibility. When enabled, the Push Config feature validates the target server certificate before pushing configuration settings. If validation fails, the configuration push fails and failure notification appears in the Push Config > Results page. To use this option, you must first import (into the source device) the trusted sever CA cert for target devices. Use the Configuration > Certificates > Trusted CAs > Import Trusted Server CA button.
- You cannot edit or delete target settings while the push operation is pushing configuration data to that target.

To add a new target to the target list, click **New Target**. On the New Target page:

1. In the admin console, choose **Maintenance > Push Config > Targets**.
2. In the Name field, enter a name for the target. Target names cannot be edited once they are created.
3. In the Sign-in URL field, enter the target Secure Access Service Sign-in URL. The Sign-in URL is the one defined in the Authentication > Signing In > Sign-In Policies page. Target sign-in URLs cannot be edited once they are created.
4. Enter the username, password, and authentication realm of target Secure Access Service administrator account. The administrator account you specify must have full administration privileges.
5. Click **Save Changes** to save settings and close the New Target page.

To delete a configuration from the target list:

1. Select the checkbox next to the target you want to delete.
2. Click **Delete** and then confirm that you want to delete the target.

When deleting a target, all push configuration results associated with that target are also deleted.

**Related  
Documentation**

- [Using the Push Configuration Feature on page 924](#)

## Pushing Configuration Settings

You use the Push Config > Push Configuration page to select source settings, to select targets, and to run the operation.

To push configuration settings:

1. In the admin console, choose **Maintenance > Push Config**.
2. If you have not done so, click the Targets tab and create a target list.
3. Select one of the following options from the “What to push” list:
  - **Entire configuration.** This option includes most settings and user data, including user bookmarks and preferences. This option does not include the following groups of settings: Network, Licenses, Cluster, Certificates, SNMP, Syslog, Push Configuration Targets.
  - **Selected configuration.** Select this option and use the selection controls to choose specific settings to push.



**NOTE:** You cannot use the Push Configuration feature to propagate network settings. Instead, use the XML Import/Export feature to do this.

4. Use the Available Targets / Selected Targets controls to create a list of targets for the Push Configuration job.
5. Select the **Overwrite duplicate settings** checkbox to resolving naming conflicts by overwriting target settings.



**NOTE:**

- If **Overwrite duplicate settings** is off, and if the name of any setting in the imported file matches the name of a corresponding setting on the target, then Push Configuration does not copy the values for that setting to the target. Push Configuration only copies new objects to the target.
- If **Overwrite duplicate settings** is on, Push Configuration copies all new and updated objects to the target.

6. Click **Push Configuration** to run the job.
7. Click the Results tab to review messages about the Push Configuration job.



**NOTE:** Once you click Push Configuration, you cannot halt the process or change target settings until the entire push configuration process completes.

If there are errors during the push process, the operation stops and rolls back the configuration to the previous state. Error messages are displayed on the Results page. Correct the problems indicated and run the job again.

- Related Documentation**
- [Using the Push Configuration Feature on page 924](#)
  - [Defining Push Configuration Targets on page 926](#)

## Archiving Junos Pulse Collaboration Meetings

The Secure Access Service enables you to archive Junos Pulse Collaboration instances. You can:

- Set up a recurring archival process.
- Perform a one-time archive.
- Archive the deleted meetings into an XML file for later download or deletion. One file is created for each archive run.
- Define the number of days a meeting instance remains on the Secure Access Service before archiving (instances older than x days are archived).
- Define which node in a cluster performs the archive.

The archival process removes completed standalone meetings, completed recurring meeting instances and completed MyMeeting instances. For recurring meeting with end dates already passed, the recurring meetings and their parent meeting are removed. The parent meeting, however, is not archived since the parent meeting information is already captured in the recurring instances. The archival process does not remove meetings in progress or scheduled (future) meetings.



**NOTE:** By default, archiving Junos Pulse Collaboration is turned off. Also by default, MyMeetings instances older than 90 days are removed. If the Junos Pulse Collaboration archive feature is turned off, the automatic deletion of MyMeetings is not saved into the archive file.

In a cluster configuration, only one node performs the archival task and only the files stored on that node are archived. You must log in to the archive node using the node IP instead of the virtual IP to download or delete the archived files.

For IVS, you must configure the settings on each IVS you want to archive meetings.

Shown below is an example snippet of an XML file created by the Junos Pulse Collaboration archival process:

```
<meetings>
 <meeting>
 <id>20993310</id>
 <creator><![CDATA[gary (Users)]></creator>
 <name><![CDATA[Support Meeting (20993310)]></name>
 <agenda><![CDATA[]></agenda>
 <teleconference_info><![CDATA[]></teleconference_info>
 <date><![CDATA[4:11 PM May 15, 2007 (GMT-08:00) Pacific Time (US &
Canada); Tijuana]]></date>
```

```

<duration>1 hour</duration>

<meeting_type>support</meeting_type>
<invitees>
<invitee><![CDATA[gary (System Local) Host]]></invitee>
...
</invitees>
<attendees>
<attendee>
<name><![CDATA[gary]]></name>
<join_time>04:11 PM</join_time>
<duration>50 minutes </duration>
</attendee>
...
</attendees>
...
</meeting>
...
</meetings>

```

To archive meetings:

1. In the admin console, choose **Maintenance > Archiving > Junos Pulse Collaboration**.
2. To schedule a recurring archival process, select the **Perform automatic clean up every** option and specify how often the archiving process should run.
3. In the Delete meetings older than field, enter how old (in days) meetings must be before being archived. Meetings older than this number are archived and removed from the system.
4. To archive meetings in a cluster configuration, select the **Archive meeting records on node** option and then select the node that performs the archive.
5. Click **Clean Up Now** to perform the archive process immediately. Meetings older than the specified age are archived and removed from the system.
6. Click **Save Changes** to save your edits.

Once the archive process completes, the archive files are listed in the Junos Pulse Collaboration archive table.

To view or download an archive file, click its name.

To delete an archive file, select the checkbox next to its name and click **Delete**.

#### Related Documentation

- [Junos Pulse Collaboration Overview on page 691](#)

# Logging and Monitoring

- [Logging and Monitoring Overview on page 931](#)
- [Viewing and Deleting User Sessions on page 934](#)
- [Configuring Log Monitoring Features on page 935](#)
- [Monitoring the Secure Access Service as an SNMP Agent on page 939](#)
- [Viewing System Statistics on page 947](#)
- [About Client-Side Logs on page 948](#)
- [Enabling and Viewing Client-Side Log Uploads on page 949](#)
- [Viewing General Status on page 950](#)
- [Configuring the System Date and Time on page 954](#)
- [Monitoring Active Users on page 955](#)
- [Viewing and Cancelling Scheduled Meetings on page 956](#)
- [Adding Real Source IP Addresses to Log Messages on page 957](#)

## Logging and Monitoring Overview

---

The Secure Access Service provides logging and monitoring capabilities to help you track events and user activities. This topic describes the various logging and monitoring features included with the Secure Access Service.

Logging and monitoring capabilities are available on all Secure Access Service products—you do not need a special license to use them. However, the following advanced logging and monitoring tools are not available on the SA700 Series Appliance:

- Sensors log
- Custom & dynamic log filters
- System capacity and critical events dashboard graphs
- Junos Pulse Collaboration logging and monitoring

Secure Access Service log files are text files stored on the Secure Access Service that track system events. the Secure Access Service produces the following types of log files:

- **Events log**—This log file contains a variety of system events, such as session timeouts (including idle and maximum length session timeouts), system errors and warnings, requests to check server connectivity, and Secure Access Service service restart notifications. (The Secure Access Service Watchdog process periodically checks the Secure Access Service and restarts it if the Secure Access Service does not respond.)
- **User Access log**—This log file contains information about when users access the appliance, including the number of simultaneous users at each one hour interval (logged on the hour), user sign-ins and sign-outs, user file requests, session timeouts (including idle and maximum length session timeouts) and Web requests.
- **Administrator Access log**—This log file contains administration information, including administrator changes to user, system, and network settings, such as changes to session timeouts, the option to enable/disable URL browsing and user-created bookmarks, and machine and server information. It also creates a log entry whenever an administrator signs in, signs out, or changes licenses on the appliance.
- **Sensors log**—This log file contains informational and attack alert messages generated by an associated IDP device monitoring client traffic for possible network intrusion.
- **Client upload log**—This log file contains session initiation, connection, and termination log information that you can use to help diagnose and troubleshoot problems users may have connection to the Secure Access Service.

The System > Log/Monitoring pages lets you specify which events are logged, the maximum file size for the system log, and whether to log events to the syslog server in addition to logging them locally. The System > Log/Monitoring pages also let you view the specified number of events, save the log files to a network, and clear the logs.

When one of the logs reaches the configured maximum log file size (200MB by default), the current data is rolled over to a backup log file. A new, empty, file is then created for all subsequent (new) log messages. Using the log viewer, the administrator can see the most recent 5000 log messages (the viewer's display limit). If the current log file contains less than 5000 log messages, older log messages from the backup log file are displayed, up to a total of 5000 log messages. This makes the log files appear as one, even though they are stored separately, according to the configured maximum log file size.

When you choose to save the log messages or use the FTP archive function on the Maintenance > Archiving page, the backup log file is appended to the current log file, and is then downloaded as one log file. If the log files are not archived or saved by the time they are rolled over once again, the oldest log messages (saved in the backup log file) are lost.

Additionally, you can use a network management tool such as HP OpenView to monitor the Secure Access Service as an SNMP agent. The Secure Access Service supports SNMP v2, implements a private MIB (management information base), and defines its own traps. To enable your network management station to process these traps, you need to download the Juniper Networks MIB file and specify the appropriate information to receive the traps. You can configure some of the traps to suit your needs. For more information on setting trap thresholds.



To monitor vital system statistics, such as CPU utilization, load the UC-Davis MIB file into your SNMP manager application. You can obtain the MIB file from:

<http://net-snmp.sourceforge.net/docs/mibs/UCD-SNMP-MIB.txt>.

## Log File Severity Levels

The events, user access, and administrator access log files rank events according to these guidelines:

- **Critical (severity level 10)**—When the Secure Access Service cannot serve user and administrator requests or loses functionality to a majority of subsystems, it writes a critical event to the log.
- **Major (severity levels 8-9)**—When the Secure Access Service loses functionality in one or more subsystems, but users can still access the appliance for other access mechanisms, the Secure Access Service writes a major event to the log.
- **Minor (severity levels 5-7)**—When the Secure Access Service encounters an error that does not correspond to a major failure in a subsystem, it writes a minor event to the log. Minor events generally correspond to individual request failures.
- **Info (severity levels 1-4)**—When the Secure Access Service displays a notification message, when an end-user makes a request, or when an administrator makes a modification, the Secure Access Service writes an informational event to the log.

## Custom Filter Log Files

The Central Manager package allows you to filter and format the data in your events, user access, and administrator access log files.

When you filter log files, the Secure Access Service only saves those messages specified within the filter query. For example, you may create a query that only logs entries for a particular range of IP addresses or for users who are signed into a specific realm. To create a query, use the Secure Access Service custom expression language.

When you format log files, the Secure Access Service simply changes the “look” of the log messages based on your specifications. Log formats do not affect which data the appliance saves; formats only affect how the appliance displays the data. The Secure Access Service includes standard, WELF, and W3C log formats, but you may also choose to create your own custom format. To create a custom format, use log fields.

## Dynamic Log Filters

The Central Manager package provides administrators with the ability to quickly change the log view by clicking on any data log variable link in the currently viewed log. For instance, if you want to temporarily view the User Access Log based on a particular IP address, create a “quick filter” by clicking on any occurrence of that IP address in the current log and the Secure Access Service immediately redraws the log to show all entries containing the specified IP address. Furthermore, clicking on additional data log variable links expands the quick filter and updates the current view of the log.

As with custom log filters, dynamic log filters change only the current view of the log — not the data that the Secure Access Service saves.

Although quick filters act as temporary filter agents, the Secure Access Service gives you the option of saving the temporary query strings as new custom filters.

**Related  
Documentation**

- [Viewing and Deleting User Sessions on page 934](#)
- [Configuring Log Monitoring Features on page 935](#)

---

## Viewing and Deleting User Sessions

---

The configuration page for most Secure Access Service servers contain a Users tab that you can use to view and delete active Secure Access Service user sessions. Authentication server types that do not display this tab include:

- **Anonymous server**—The Secure Access Service cannot display individual session data about users who sign in through an anonymous server, because it does not collect usernames or other credentials for users signing in through an anonymous server.
- **Local authentication server**—The Secure Access Service displays a Local Users tab instead of a Users tab for local authentication servers, allowing you to add and delete user accounts instead of user sessions.

For all other types of authentication servers, you may view and delete active user sessions using the instructions below.

To view or delete an active user session:

1. In the admin console, select **Authentication > Auth. Servers**.
2. Click the appropriate link in the Authentication/Authorization Servers list.
3. Select the **Users** tab.
4. Perform any of the following tasks:
  - Enter a username in the Show users named field and click Update to search for a specific user.  
  
Alternately, you can use an \* character as a wildcard, where an \* represents any number of zero or more characters. For example, if you want to search for all usernames that contain the letters jo, enter \*jo\* in the Show users named field. The search is case-sensitive. To display the entire list of accounts again, either enter an \* character, or delete the field's contents and click Update.
  - Enter a number in the Show N users field and click **Update** to control the number of users displayed on the page.
  - Click the checkbox next to individual users and click **Delete** to terminate their Secure Access Service sessions.

You can find several access statistics for any user account on the Users tab in the Last Access Statistics columns. These columns appear on any of the Users tabs anywhere they appear in the admin console. The statistics include the last sign-in date and time a user successfully signed in and the browser type and version.

- Related Documentation**
- [Configuring Log Monitoring Features on page 935](#)

## Configuring Log Monitoring Features

---

Use Secure Access Service Log Monitoring features to monitor events, user access, and administrator access, as well as logs for client-side applications, such as Host Checker, Cache Cleaner, Junos Pulse Collaboration, WSAM, JSAM, Terminal Services, and VPN Tunneling.

This topic includes the following information:

- [Configuring Events, User Access, Admin Access, and Sensor Logs on page 935](#)
- [Creating, Resetting, or Saving a Dynamic Log Query on page 936](#)
- [Specifying Which Events to Save in the Log File on page 936](#)
- [Creating, Editing, or Deleting Log Filters on page 937](#)
- [Example: Using IP Address Filters on page 938](#)

### Configuring Events, User Access, Admin Access, and Sensor Logs

Use the System > Log/Monitoring > Events, User Access, Admin Access, and Sensor, pages to save log files, create dynamic log queries, specify which events to save in the log files, and create custom filters and formats.

The events, user access, and admin access logs are three distinct files. Although the basic configuration instructions for each is the same, modifying the settings for one does not affect settings for another.

To save, view, or clear the events log file:

1. In the admin GUI, select **System > Log/Monitoring**.
2. Select either the **Events**, **User Access**, **Admin Access**, or **Sensors**, and then choose **Log**.
3. Enter a number in the Show field and click **Update** if you want to change the number of log entries that the system displays at one time.
4. Click **Save Log As**, navigate to the desired network location, enter a filename, and then click **Save** to manually save the log file. We recommend you retain the system generates log name, which follows a consistent convention:  
**juniper.logtype.nodename.log**.
5. Click the **Save All Logs** button on the Events Log, User Access, Admin Access, and Sensors tabs. It generates a file that includes event, user access, admin access, sensor logs, and XML data for all of the system statistics and graphs shown on the Status > Overview page. After you click **Save All Logs**, you are prompted to download a file named **juniperlogs-graphs.tar.gz** to your local host.
6. Click the **Clear All Logs** button on the Events Log, User Access, Admin Access, and Sensors tabs. It clears event, user access, admin access, sensor logs, and XML data for all of the system statistics and graphs shown on the Status > Overview page.

When you clear the local log, events recorded by the syslog server are not affected. Subsequent events are recorded in a new local log file.

## Creating, Resetting, or Saving a Dynamic Log Query

To create, reset, or save a dynamic log filter query:

1. Select **System > Log/Monitoring** in the admin GUI.
2. Select the **Events, User Access, Admin Access, or Sensors** tab, and then choose **Log**.
3. Click any data log variable link in the current log. The log immediately redraws based on the chosen variable.
4. Continue adding variables in the same manner (optional). Each data log variable link you select adds a variable to the Edit Query text field and the log updates with each added variable.
5. Click the **Reset Query** button to clear the Edit Query text field and reset the log to the view determined by the filter specified in the View by filter field (optional).
6. Click the **Save Query** button to save the dynamic log query as a custom filter (optional). The Filters tab displays with the Query field prepopulated with the variables you selected from the log. Next:
  - a. Enter a name for the filter.
  - b. Make the new filter the default filter by selecting **Make default** (optional).
  - c. Set the start and end dates for the filter:
    - In the Start Date section, click **Earliest Date** to write all logs from the first available date stored in the log file. Or, manually enter a start date.
    - In the End Date section, click **Latest Date** to write all logs up to the last available date stored in the log file. Or, manually enter an end date.
7. Choose a format in the Export Format section.
8. Save the configuration.

## Specifying Which Events to Save in the Log File

Use options in the Settings tab to specify what the Secure Access Service writes to the log file, which syslog servers it uses to store the log files, and the maximum file size.

You can also use the Archiving page to automatically save the logs to an FTP accessible location.

To specify events log settings:

1. In the admin GUI, select **System > Log/Monitoring**.
2. Select **Events, User Access, Admin Access, or Sensors** tab, and then choose **Settings**.
3. In the Maximum Log Size field, specify the maximum file size for the local log file. (The limit is 500 MB.) The system log displays data up to the amount specified.

Maximum Log Size is an internal setting that most closely corresponds with the size of logs formatted with the Standard format. If you choose to use a more verbose format such as WELF, your log files may exceed the limit that you specify here.

4. Under Select Events to Log, select the checkbox for each type of event that you want to capture in the local log file.

If you disable the Statistics checkbox in the Events Log tab, the Secure Access Service does not write statistics to the log file, but continues to display them in the System > Log/Monitoring > Statistics tab.

5. Under Syslog Servers, enter information about the syslog servers where you want to store your log files (optional):
  - a. Enter the name or IP address of the syslog server
  - b. Enter a facility for the server. The Secure Access Service provides eight facilities (LOCAL0-LOCAL7), which you can map to facilities on your syslog server.
  - c. (Central Manager only) Choose which filter you want to apply to the log file.
  - d. Click **Add**.
  - e. Repeat for multiple servers if desired, using different formats and filters for different servers and facilities.

Make sure your syslog server accepts messages with the following settings: facility = LOG\_USER and level = LOG\_INFO.

6. Save the configuration.

## Creating, Editing, or Deleting Log Filters

Use options in the Filters tab to specify which data is written to your log files as well as its format. This option is only available with the Central Manager package.

1. In the admin GUI, select **System > Log/Monitoring**.
2. Select the **Events, User Access, Admin Access, or Sensors** tab, and then choose **Filters**.

The list includes the following predefined log filters:

- Standard (default)—This log filter format logs the date, time, node, source IP address, user, realm, and the Secure Access Service event ID and message.
- WELF—This customized WebTrends Enhanced Log Format (WELF) filter combines the standard WELF format with information about the Secure Access Service's realms, roles, and messages.
- WELF-SRC-2.0-Access Report—This filter adds access queries to our customized WELF filter. You can easily use this filter with NetIQ's SRC to generate reports on user access methods.
- W3C—The World Wide Web Consortium's extended log file format is a customizable ASCII format with a variety of different fields. Visit <http://www.w3.org> for more information about this format. Only the User Access log offers this filter as an option.

3. If desired, do one of the following:
  - Modify an existing filter by clicking its name.
  - Create a new filter by clicking **New Filter**.
4. Enter a name for the filter.

If you select a format and then create a name for it in the Filter Name field, the Secure Access Service does not create a new custom filter format that is based on the existing format. Instead, it overwrites the existing format with the changes you make.
5. Click **Make Default** to define the selected filter as the default for the log file type. You may set different default filters for the events, user access, and administrator access logs.
6. Use options in the Query section to control which subset of data the Secure Access Service writes to the log:
  - a. In the Start Date section, click **Earliest Date** to write all logs from the first available date stored in the log file. Or, manually enter a start date.
  - b. In the End Date section, click **Latest Date** to write all logs up to the last available date stored in the log file. Or, manually enter a end date.
  - c. In the Query section, use the custom expression language to control which subset of data the system writes to the log.

Any string (including a \* wildcard character) you manually enter in a query, must be enclosed in double-quotes. For example, the query protocol="UDP" AND sourceip=172.27.0.0/16 AND port=\* must be presented as protocol="UDP" AND sourceip=172.27.0.0/16 AND port="\*" or the logging component returns an error.
7. Use options the Export Format section to control the format of the data in the log:
  - Select the **Standard**, **WELF**, or **W3C** to format the log entries using one of these standardized formats.
  - Select **Custom** and enter the format you want to use in the Format field. When entering a format, surround variables with percentage symbols (for example %user%). All other characters in the field are treated as literals.
8. Save the configuration.

### Example: Using IP Address Filters

When drilling into logs to verify behavior or troubleshoot an issue with a dual-stack device, it is helpful to redisplay the log collection filtered on the IP address.

To filter on an IP address:

1. In the admin GUI, select **System > Log/Monitoring**.

2. To create the filter:
  - a. Select **User Access** and then **Filter**.
  - b. Define the filter expression, name the filter, and click **Save**. In this example, we create a filter based on source IP address and name it `IPv6_Address_Filter:Standard`.
3. To use the filter:
  - a. Select **Logs** to display the user logs table.
  - b. Under “View by filter,” select `IPv6_Address_Filter:Standard`, as shown in [Figure 69 on page 939](#).
  - c. If desired, under “Edit Query,” edit the value of the `sourceip=` variable expression to filter on different source IP addresses.
  - d. Click **Update** to apply the filter and redisplay the log collection.

**Figure 69: Using IP Address Filters**



**Related Documentation** • [Viewing and Deleting User Sessions on page 934](#)

## Monitoring the Secure Access Service as an SNMP Agent

You can use a network management tool such as HP OpenView to monitor the Secure Access Service as an SNMP agent. The system supports SNMP (Simple Network Management Protocol) v2 and SNMPv3, implements a private MIB (management information base), and defines its own traps. To enable your network management station to process these traps, you need to download the Juniper Networks MIB file and specify the appropriate information to receive the traps.

To monitor vital system statistics, such as CPU utilization, load the UC-Davis MIB file into your SNMP manager application. You can obtain the MIB file from:

<http://net-snmp.sourceforge.net/docs/mibs/UCDSNMP-MIB.txt>. The system supports standard MIB objects, including the system uptime (sysUpTime) object. The system uptime (sysUpTime) object returns the time elapsed (in hundredths of a second) since the SNMP agent was started.

The User-Based Security Model (USM) is the default Security Module for SNMPv3. Secure Access Services supports only one user at a time to be registered with an SNMP engine. Editing the SNMPv3 user attributes overwrite any already registered SNMPv3 user. The SNMPv3 user has read-only access on all MIBs supported by the Secure Access device. The SNMPv3 user configuration attributes are also used for SNMP traps.

To specify SNMP settings:

1. In the admin console, select **System > Log/Monitoring > SNMP**.
2. Click the **Juniper Networks MIB file** link to access the MIB file, and then save the file from your browser to a network location. For descriptions of the Get and Trap objects in the MIB file.
3. Under **SNMP Version**, select **v2c** or **v3**.
  - If you select **v3**, both queries and traps use SNMPv3.
4. Under **Agent Properties** enter information in the following fields:
  - Enter information in the **System Name**, **System Location**, and **System Contact** fields that describes the Secure Access Service agent (optional).
  - Enter the community string (required only for SNMPv2c).
    - To query the Secure Access Service, your network management station must send the community string to the Secure Access Service.
    - To stop the SNMP system, clear the community field.
5. If you selected SNMP version 3, enter the SNMPv3 configuration values:
  - Enter the SNMPv3 user name.
  - Select the desired security level and enter the following information based on the level selected.

	No Auth, NoPriv	Auth, NoPriv	Auth, Priv
Auth Protocol	NA	Select either MD5 (HMAC-MD5-96) or SHA (HMAC-SHA-96).	Select either MD5 (HMAC-MD5-96) or SHA (HMAC-SHA-96).
Auth Password	NA	Enter an authentication password. The password can contain any ASCII characters and must be at least 8 characters in length.	Enter an authentication password. The password can contain any ASCII characters and must be at least 8 characters in length.
Priv Protocol	NA	NA	Select either CBC-DES or CFB-AES-128.



	No Auth, NoPriv	Auth, NoPriv	Auth, Priv
Priv Password	NA	NA	Enter a privacy password. The password can contain any ASCII characters and must be at least 8 characters in length.

6. Under Trap Thresholds, set the values for the following traps (optional). Setting a threshold value to 0 disables that respective trap.
  - Check Frequency
  - Log Capacity
  - Users
  - Memory
  - Swap Memory
  - Disk
  - Meeting Users
  - CPU
7. Under Optional traps, select one or both of the following (optional):
  - Critical Log Events
  - Major Log Events
8. Under SNMP Servers, specify servers to which you want the Secure Access Service to send the traps that it generates by entering information in the following fields, and then clicking **Add**:
  - The server's host name or IP address.
  - The port on which the server listens (typically port 162).
  - The community string required by the network management station (if applicable). The community string is applicable only for SNMPv2c.
9. Click **Save Changes**. If the version is changed from v2 to v3, the Secure Access Service generates two engine IDs. Both IDs are displayed.
10. At your network management station:
  - a. Download the Juniper Networks MIB file.
  - b. Specify the community string required when querying the Secure Access Service (see step 4). The community string is applicable only for SNMPv2c.
  - c. Configure the network management software to receive Secure Access Service traps.

- d. If SNMPv3 is selected, the SNMPv3 user details must be configured as in Step 5 above.
- e. The agent engine ID must be configured for SNMP queries; the trap engine ID must be configured to receive SNMPv3 traps from the device.

**Table 58: Configuration Objects**

Object	Description
logFullPercent	Returns the percentage of the available file size filled by the current log as a parameter of the logNearlyFull trap.
signedInWebUsers	Returns the number of users signed in to the Secure Access Service through a Web browser.
signedInMailUsers	Returns the number of users signed in to the Email client.
blockedIP	Returns the IP address—blocked due to consecutive failed login attempts—sent by the iveTooManyFailedLoginAttempts trap. The system adds the blocked IP address to the blockedIPList table.
authServerName	Returns the name of an external authentication server sent by the externalAuthServerUnreachable trap.
productName	Returns the Secure Access Service licensed product name.
productVersion	Returns the Secure Access Service system software version.
fileName	Returns the file name sent by the archiveFileTransferFailed trap.
meetingUserCount	Returns the number of concurrent meeting users sent by the meetingUserLimit trap.
iveCpuUtil	Returns the percentage of CPU used during the interval between two SNMP polls. This value is calculated by dividing the amount of CPU used by the amount of CPU available during the current and previous SNMP polls. If no previous poll is available, the calculation is based on the interval between the current poll and system boot.
iveMemoryUtil	Returns the percentage of memory utilized by the Secure Access Service at the time of an SNMP poll. The system calculates this value by dividing the number of used memory pages by the number of available memory pages.
iveConcurrentUsers	Returns the total number of users logged in for the Secure Access Service node.
clusterConcurrentUsers	Returns the total number of users logged in for the cluster.
iveTotalHits	Returns the total number of hits to the Secure Access Service since last reboot. Includes total values from iveFileHits, iveAppletHits, meetingHits, and iveWebHits.

Table 58: Configuration Objects (*continued*)

Object	Description
iveFileHits	Returns the total number of file hits to the Secure Access Service since last reboot. Incremented by the web server with each GET/POST corresponding to a file browser request.
iveWebHits	Returns the total number of hits by means of the Web interface since last reboot. Incremented by the web server for each http request received by the Secure Access Service, excluding file hits, applet hits, and meeting hits.
iveAppletHits	Returns the total number of applet hits to the Secure Access Service since last reboot. Incremented by the web server for each GET request for a Java applet.
ivetermHits	Returns the total number of terminal hits to the Secure Access Service since last reboot.
logName	Returns the name of the log (admin/user/event) for the logNearlyFull and iveLogFull traps.
iveSwapUtil	Returns the percentage of swap memory pages used by the Secure Access Service at the time of an SNMP poll. The system calculates this value by dividing the number of swap memory pages used, by the number of available swap memory pages.
diskFullPercent	Returns the percentage of disk space used in the Secure Access Service for the iveDiskNearlyFull trap. The system calculates this value by dividing the number of used disk space blocks by the number of total disk space blocks.
blockedIPList	Returns a table with the 10 most recently blocked IP addresses. The blockedIP MIB adds blocked IP addresses to this table
ipEntry	An entry in the blockedListIP table containing a blocked IP address and its index (see IPEntry).
IPEntry	The index (ipIndex) and IP address (ipValue) for an entry in the blockedIPList table.
ipIndex	Returns the index for the blockedIPList table.
ipValue	A blocked IP address entry in the blockedIPList table.
logID	Returns the unique ID of the log message sent by the logMessageTrap trap.
logType	Returns a string sent by the logMessageTrap trap stating whether a log message is major or critical.
logDescription	Returns a string sent by the logMessageTrap trap stating whether a log message is major or critical.

Table 58: Configuration Objects (*continued*)

Object	Description
ivsName	Returns the name of a virtual system.
ocspResponderURL	Returns the name of an OCSP responder.
fanDescription	Returns the status of the Secure Access Service fans.
psDescription	Returns the status of the Secure Access Service power supplies.
raidDescription	Returns the status of the Secure Access Service RAID device.
iveLogNearlyFull	<p>The log file (system, user access, or administrator access) specified by the logName parameter is nearly full. When this trap is sent, the logFullPercent (%of log file full) parameter is also sent. You can configure this trap to be sent at any percentage. To disable this trap, set the Log Capacity trap threshold to 0%. The trap's default value is 90%.</p> <p><b>NOTE:</b> When SNMP traps are enabled, the iveLogNearlyFull and iveLogFull traps are sent when the log files are 90% full and 100% full respectively, even if the threshold is set to 0 (disabled).</p>
iveLogFull	<p>The log file (system, user access, or administrator access) specified by the logName parameter is completely full.</p> <p><b>NOTE:</b> When SNMP traps are enabled, the iveLogNearlyFull and iveLogFull traps are sent when the log files are 90% full and 100% full respectively, even if the threshold is set to 0 (disabled).</p>
iveMaxConcurrentUsersSignedIn	Maximum number of allowed concurrent users are currently signed in. You can configure this trap to be sent at any percentage. To disable this trap, set the Users trap threshold to 0%. The trap's default value is 100%.
iveTooManyFailedLoginAttempts	<p>A user with a specific IP address has too many failed signin attempts. Triggered when a user fails to authenticate according to the settings for the Lockout options on the Security Options tab.</p> <p>When the system triggers this trap, the system also triggers the blockedIP (source IP of login attempts) parameter.</p>
externalAuthServerUnreachable	<p>An external authentication server is not responding to authentication requests.</p> <p>When the system sends this trap, it also sends the authServerName (%of log file full) (name of unreachable server) parameter.</p>
iveStart	Secure Access Service has just been turned on.
iveShutdown	Secure Access Service has just been shut down.
iveReboot	Secure Access Service has just been rebooted.

Table 58: Configuration Objects (*continued*)

Object	Description
archiveServerUnreachable	Secure Access Service is unable to reach configured FTP or SCP Archive server.
archiveServerLoginFailed	Secure Access Service is unable to log into configured FTP or SCP Archive server.
archiveFileTransferFailed	Secure Access Service is unable to successfully transfer archive to configured FTP or SCP Archive server. When the system sends this trap, it also sends the fileName parameter.
iveRestart	Supplies notification that the Secure Access Service has restarted according to the administrator's instruction.
iveDiskNearlyFull	Supplies notification that the Secure Access Service's disk drive is nearly full. When the system sends this trap, it also sends the diskFullPercent parameter. You can configure this trap to be sent at any percentage. To disable this trap, set the Disk trap threshold to 0%. This trap's default value is 80%.
iveDiskFull	Supplies notification that the Secure Access Service's disk drive is full.
logMessageTrap	The trap generated from a log message. When the system sends this trap, it also sends the logID, logType, and logDescription parameters.
memUtilNotify	Supplies notification that the system has met the configured threshold for memory utilization. To disable this trap, set the Physical Memory trap threshold to 0. The threshold is 0%, by default.
cpuUtilNotify	Supplies notification that the system has met the configured threshold for CPU utilization. To disable this trap, set the CPU trap threshold to 0. The threshold is 0%, by default.
swapUtilNotify	Supplies notification that the system has met the configured threshold for swap file memory utilization. To disable this trap, set the Swap Memory trap threshold to 0. The threshold is 0%, by default.
iveFanNotify	Supplied notification that the status of the fans has changed.
ivePowerSupplyNotify	Supplies notification that the status of the power supplies has changed.
iveRaidNotify	Supplies notification that the status of the RAID device has changed.
iveNetExternalInterfaceDownTrap (nicEvent)	Supplies the type of event that brought down the external interface. The nicEvent parameter can contain values of "external" for an external event and "admin" for an administrative action.
iveNetInternalInterfaceDownTrap (nicEvent)	Supplies the type of event that brought down the internal interface. The nicEvent parameter can contain values of "external" for an external event and "admin" for an administrative action.

Table 58: Configuration Objects (*continued*)

Object	Description
iveClusterDisableNodeTrap (clusterName,nodeList)	Supplies the name of the cluster that contains disabled nodes, as well as a string containing the names of all disabled nodes. Node names are separated by white space in the string.
iveClusterChangedVIPTrap(vipType, currentVIP, newVIP)	Supplies the status of a virtual IP for the cluster. The vipType indicates whether the changed VIP was external or internal. The currentVIP contains the VIP prior to the change, and newVIP contains the VIP after the change.
iveNetManagementInterfaceDownTrap (nicEvent)	Supplies the type of event that brought down the management port. The nicEvent parameter can contain values of "external" for an external event and "admin" for an administrative action.
iveClusterDelete(nodeName)	Supplies the name of the node on which the cluster delete event was initiated.
iveSAMHits	The total number of SAM hits since the last reboot.
iveNCHits	The total number of Network Connect hits since the last reboot.
meetingHits	The total number meeting hits since the last reboot.
meetingCount	The number of concurrent meetings.
clusterName	The name of the cluster.
nodeList	The list of disabled nodes.
vipType	Indicates whether the VIP is internal or external.
currentVIP	The current value of the VIP being changed.
nicEvent	The type of event (admin or external) that generated the trap.
nodeName	The name of the node.
iveTemperature	The temperature of the MAG service modules. Other devices, such as the Secure Access Service or Access Control Service devices return a 0.
iveVPNTunnels	The number of concurrent Pulse IPsec and Network Connect users.
iveSSLConnections	The total number of SSL connections.
esapVersion	The active ESAP version.
vipChangeReason	The reason for the VIP node change.
meetingUserLimit	The concurrent user count over the license limit.

Table 58: Configuration Objects (*continued*)

Object	Description
meetingLimit	The concurrent meeting count over the license limit.
iveMaxConcurrentUsersVirtualSystem	The maximum number of concurrent virtual system users signed in.
ocspResponderConnectionFailed	Cannot connect to the OCSP responder.
iveNetManagementInterfaceDownTrap	A nicEvent caused the management interface to go down.
iveTemperatureNotify	The device temperature is above the threshold value.
iveVIPNodeChanged	Notifies that the VIP node has changed. nodeName is the new node hosting the VIP. vipChangeReason describes the reason for the change.

The options for sending SNMP traps for critical and major events are set to OFF by default, for security purposes.

- Related Documentation**
- [Viewing System Statistics on page 947](#)
  - [Viewing General Status on page 950](#)

## Viewing System Statistics

Every hour, the Secure Access Service logs the following data.

- Peak load of Web users
- Peak load of Mail users
- Number of URLs accessed
- Number of files accessed

The Statistics page displays that information for the past seven days. The Secure Access Service writes that information to the system log once a week. Note that upgrading the Secure Access Service clears all statistics. If you configure the system to log statistics hourly, however, old statistics are still available in the log file after an upgrade.

To view system statistics:

1. In the admin console, select **System > Log/Monitoring > Statistics**.
2. Scroll the page to view all four categories of data.

- Related Documentation**
- [Viewing General Status on page 950](#)

## About Client-Side Logs

---

The Secure Access Service includes the following options for enabling and viewing client-side logs:

- **Logging activity for individual features**—You can use options in the System > Log/Monitoring > Client Logs > Settings page of the admin console to enable client-side logging for individual Secure Access Service client applications such as Host Checker and VPN Tunneling, to set log limit sizes, and to enable log alerts. You must enable client-side logs on this page in order to use client-side options.
- **Uploading log files to the Secure Access Service**—You can use options in the Users > User Roles > Select Role > General > Session Options page of the admin console to configure the Secure Access Service to upload log files to the admin console when initiated by an end-user.
- **Viewing uploaded logs**—You can use options in the System > Log/Monitoring > Client Logs > Uploaded Logs page of the admin console to view the logs that end-users push to the Secure Access Service.

## Enabling Client-Side Logging and Global Options

Client-side logging is useful when working with the Juniper Networks Support team to debug problems with the Secure Access Service client-side feature. When you enable logging for a feature, the Secure Access Service writes a log to any client computer that uses the feature. (These settings are global, which means that the Secure Access Service writes a log file to all clients that use the enabled feature.) The Secure Access Service then appends to the log file each time the feature is invoked during subsequent user sessions. Once the Secure Access Service has written a log file to a user's computer, it does not remove it. If users want to remove the log files, they must manually delete them from their computers.

You can enable client-side logging for the Host Checker, Cache Cleaner, Junos Pulse Collaboration, WSAM, JSAM and Java Applet Rewriter, VPN Tunneling, and Terminal Services features. For information about where the Secure Access Service installs log files for each of these features, see Client-Side Changes.



**NOTE:** The Secure Access Service only logs information for the VPN Tunneling feature if you enable logging through the admin console using the procedure that follows and the end-user enables logging through the end-user's status window.

---

When you use the Secure Access Service as an Instant Virtual System (IVS) appliance, keep the following guidelines in mind:



- The options available in the tabs on the System > Log/Monitoring > Client Logs page on the Secure Access Service featuring one or more IVS systems can only be configured by the root administrator—this right includes disk space allocation and alert settings on the Secure Access Service, which are shared among all IVS systems on the Secure Access Service.
- Each IVS administrator has rights to enable client-side logging for the roles associated with the IVS system's user roles.
- IVS administrators can only manipulate (save, delete) log files within their respective IVS systems.
- Root administrators can save and delete log files from all IVS systems.
- An IVS administrator can configure the system to receive a User Access Event when their IVS log uploads.

**Related  
Documentation**

- [Enabling and Viewing Client-Side Log Uploads on page 949](#)

## Enabling and Viewing Client-Side Log Uploads

If you enable client-side logging for Secure Access Service features, you can also enable automatic upload of those logs at the role level. When you do, Secure Access Service end-users and Junos Pulse Collaboration attendees who are members of the enabled roles can choose to push their log files up to the Secure Access Service at will. Then, you can view the uploaded files through the System > Log/Monitoring > Client Logs > Uploaded Logs page of the admin console.

When you upload log files to the Secure Access Service that is a node in a cluster, keep the following guidelines in mind:

- You can use the Log Node column on the System > Log/Monitoring > Client Logs > Uploaded Logs tab to view the location of existing log files collected by nodes in the cluster. This is specific to a cluster setup and does not apply to a single Secure Access Service deployment.
- The user uploads logs to the cluster node to which he is connected.
- You can view upload log entries across all nodes in a cluster. You can save and unzip your uploaded log files from the respective nodes in the cluster where the user uploaded the logs.
- You can view upload log entries across all nodes in a cluster. You can save and unzip your uploaded log files from the respective nodes in the cluster where the user uploaded the logs.
- When a node is removed from a cluster, the Secure Access Service deletes the logs of that node from the Uploaded Log List in the cluster and from the node.

To enable end-users to upload logs to the Secure Access Service:

1. In the admin console, select **Users > User Roles > Select Role > General > Session Options**.

2. In the Upload logs section, select the **Enable Upload Logs** checkbox.
3. Click **Save Changes**.

### Viewing Uploaded Client-Side Logs

If you enable end-users to push log files up to the Secure Access Service, you can view the uploaded logs through the System > Log/Monitoring > Client Logs > Uploaded Logs page of the admin console. This page displays a list of uploaded log files from clients, featuring information such as the file name, date, associated user and/or realm, client access component type, and the log node.



**NOTE:** The Secure Access Service does not preserve uploaded logs when you upgrade the Secure Access Service. To preserve the logs, you may archive them using options in the Maintenance > Archiving > Archiving Servers page of the admin console. You can also set the log-related SNMP traps to capture log events during the log upload using options in the System > Log/Monitoring > SNMP page of the admin console.

To view client log upload details:

1. In the admin console, choose **System > Log/Monitoring > Client Logs > Uploaded Logs**.
2. (Optional) Refresh uploaded client log details by clicking the **Refresh Logs** button.
3. (Optional) View or save an uploaded log by clicking on its respective link.
4. (Optional) Delete an uploaded log by clicking the trash can icon in the right side of the log's column. Note that once you delete a log from a node, those logs are lost.

**Related Documentation**

- [About Client-Side Logs on page 948](#)

## Viewing General Status

---

When you sign in to the admin console, the Secure Access Service displays the System > Status page, showing the Overview tab. This tab summarizes details about the Secure Access Service server and system users. When you make changes on other admin console pages, the Secure Access Service updates corresponding information on the Overview tab.

This tab is the home page for all administrators, including delegated administrators without read or write access to the System > Status tabs.

## Viewing System Capacity Utilization

The Central Manager dashboard for Secure Access Service provides system capacity utilization graphs that allow you to easily view and understand how much of your system capacity you are using on a regular basis.

To use this information for data reporting elsewhere, export it as an XML file using options on the Maintenance > Import/Export > Configuration page.

These graphs are displayed in the System > Status > Overview tab when you open the admin console, and allow you to easily view:

- **Concurrent Users**—This graph shows the total number of users currently logged in to the device.
- **Hits Per Second**—This graph shows the number of hits currently being processed by the Secure Access Service. In a clustered environment, you may choose the Secure Access Service from the drop-down list to determine which node's data is displayed in the graph. The graph includes four lines: number of hits, number of Web hits, number of file hits, and number of client/server hits.
- **CPU and Virtual (Swap) Memory Utilization**—This graph shows the percentage of the CPU and available memory currently being used. In a clustered environment, you may choose the Secure Access Service from the dropdown list to determine which node's data is displayed in the graph.
- **Throughput**—This graph shows the amount of data (in KB) currently being processed. In a clustered environment, you may choose the Secure Access Service Controller from the drop-down list to determine which node's data is displayed in the graph. The graph includes four lines: external in, external out, internal in, and internal out.
- **Rate**—This graph shows the login and connection statistics. The graph contains the following information:
  - **Attempted Login** – The number of login attempts the Secure Access Service received per minute
  - **Successful Login** – The number of successful logins the Secure Access Service received per minute
  - **Attempted VPN** – The total number of Network Connect or Pulse connection attempts the Secure Access Service received per minute
  - **Successful VPN** – The number of successful Network Connect or Pulse connections the Secure Access Service received per minute
  - **HC** – The total number of Host Checker updates the Secure Access Service received per minute



**NOTE:** The dashboard graphs may not display properly if the Secure Access System system time has been adjusted prior to the time the data was recorded.

You may also use the Page Settings window to configure which graphs the Secure Access Service displays in the dashboard and the period of time that the Secure Access Service tracks.

To download the graph data to an XML file:

1. In the admin console, select **System > Status > Overview**.
2. Click the Download link that corresponds to the graph that you want to download.
3. Click **Save**, specify the directory where you want to save the XML file, and click **Save**.

## Specifying Time Range and Data to Display in Graphs

You can specify the time range and other data to display in the graphs.

1. In the admin console, choose **System > Status > Overview**.
2. Click **Page Settings**.
3. Select which utilization graphs to display.
4. Select the range of time that you want to plot in the graphs. Graphing intervals range from 1 hour to 1 year.
5. Indicate how often you want to refresh the graphs.
6. Click **Save Changes**.

## Configuring Graph Appearance

You can specify colors and line weights, to change the appearance of the graphs on the Status page.

1. In the admin console, choose **System > Status > Overview**.
2. Click the **Edit** link that corresponds to the graph that you want to modify.
3. Use settings in the Graph Settings dialog box to edit the background color, graph line colors, text color, line color, and line width displayed in the graph.
4. Click **Save Changes**.

The dashboard for the Secure Access Service allows you to easily view the last 10 critical system events. Using the Event Monitor window, you can quickly access and address any critical system problems. Once you have opened the Event Monitor window, you may keep it open and continually monitor system events while navigating through the admin console to perform standard maintenance and configuration tasks.

To quickly review critical system events:

1. In the admin console, choose **System > Status > Overview**.
2. Click **Critical Events**. The Event Monitor window displays the severity and message of any critical events recorded in the system's log file.
3. Click **Refresh** to view the most up-to-date events (optional).
4. Click **See All** to navigate to the System > Log/Monitoring > Events > Log tab, where all events—ranging from informational to critical—are displayed (optional).

## Viewing Critical System Events

The Central Manager dashboard allows you to easily view the last 10 critical system events. Using the Event Monitor window, you can quickly access and address any critical system problems. Once you have opened the Event Monitor window, you may keep it open and continually monitor system events while navigating through the admin console to perform standard maintenance and configuration tasks.

To quickly review critical system events:

1. In the admin console, choose **System > Status > Overview**.
2. Click **Critical Events**. The Event Monitor window displays the severity and message of any critical events recorded in the system's log file.
3. Click **Refresh** to view the most up-to-date events (optional).
4. Click **See All** to navigate to the **System > Log/Monitoring > Events > Log** tab, where all events—ranging from informational to critical—are displayed (optional).

## Downloading the Current Service Package

You can download the service package currently installed on the Secure Access Service for backup and to install it onto another Secure Access Service.

1. In the admin console, choose **System > Status > Overview**.
2. Click **Download Package** (Central Manager versions) or the link next to System Software Pkg Version.
3. Click **Save**.
4. Specify a name and location for the service package.
5. Click **Save**.

- Related Documentation**
- [Configuring the System Date and Time on page 954](#)
  - [Configuring Log Monitoring Features on page 935](#)

## Configuring the System Date and Time

You must set the server time in order to accurately record system events and user file transfers. You can use a Network Time Protocol (NTP) server to synchronize the Secure Access Service with a series of computers, or you can set the Secure Access Service time manually. Secure Access Service supports NTPv4, which is backwards compatible with NTPv3 and NTPv2.



**NOTE:** Secure Access System does not support automatic time synchronization across cluster nodes. You must configure your cluster nodes to use the same NTP server to ensure they are synchronized. If the cluster nodes are not synchronized, time-based features (such as Junos Pulse Collaboration) do not function properly.

To edit the system date and time:

1. In the admin console, choose **System > Status > Overview**.
2. In the System Date & Time section, click **Edit**.
3. Select a time zone from the Time Zone menu. The Secure Access Service automatically adjusts the time for Daylight Saving Time.
4. To set the time using an NTP server:
  - a. Select the **Use NTP server** option.
  - b. Enter the NTP server's name or IP address.
  - c. (optional) If you are using NTPv4, enter the symmetric key.

The key must be pre-synchronized with the NTP server. For example, if you want to configure NIST's clock as the NTP server, you must request a key beforehand and have NIST send that key to you.

The key for MD5 is in the following format:

*KeyNumber M KeyValue*

The key for SHA1 is in the following format:

*KeyNumber SHA1KeyValue*

where M indicates the key is in MD5 format. The key value is case-sensitive and must be entered exactly as received.

- d. (optional) Enter a secondary NTP server's name or IP address.

Secure Access Service first tries to contact the primary NTP server. If it fails three times to reach the primary server or if the authentication fails three times, Secure Access Service attempts to contact the secondary NTP server.

- e. (optional) Enter the symmetric key authentication for the secondary NTP server.
  - f. Specify an update interval. The maximum interval is 999999 (enforced by the user interface).
5. To set the time manually:
    - a. Select the **Set Time Manually** option.
    - b. Enter the current date and time. You can click **Get from Browser** to automatically populate the Date and Time fields.
  6. Click **Save Changes**.

**Related Documentation**

- [Viewing General Status on page 950](#)

## Monitoring Active Users

You can monitor users signed in to the Secure Access Service. Each user's name, authentication realm, role, and sign-in time are listed on the Active Users page.



**NOTE:** Non-Secure Access Service users who are signed into a Junos Pulse Collaboration are listed as members of the "Pulse Collaboration User Role" role. The Secure Access Service displays "N/A" in the Realm and Role columns for non-Secure Access Service users who are signed in to the Secure Access Service to attend a Junos Pulse Collaboration.

To monitor users signed in to the Secure Access Service:

1. In the admin console, choose **System > Status > Active Users**.
2. Perform these tasks (optional):
  - Sign users out of their Secure Access Service sessions:
    - To forcibly sign out one or more end-users or administrators, select the checkbox next to the appropriate names and then click **Delete Session**.
    - To forcibly sign out all end-users who are currently signed-in, click **Delete All Sessions**.
  - Perform a dynamic policy evaluation of all signed-in users:
    - To manually evaluate all authentication policies, role mapping rules, role restrictions, user roles, and resource policies for all currently signed-in users, click **Refresh Roles**. Use this button if you make changes to an authentication policy, role mapping rules, role restrictions, or resource policies and you want to immediately refresh the roles of all users.
  - Configure which data is shown and its order:

- To display a specific user, enter the username in the Show Users Named field and click Update. If you do not know the user's exact username, use the \* wildcard character. For example, if you have a user named "Joseph Jones," but you do not remember if the username is "Joe" or "Joseph," enter Jo\* in the **Show Users Named** field. The Secure Access Service returns a list of all users whose usernames start with the letters jo.
- To control how many users and administrators are displayed in the Active Users page, enter a number in the Show N users field and click **Update**.
- To sort the table of currently signed-in users and administrators, click a column header
- To refresh the page's content, click **Update**.
- Link to related tabs:
  - To edit a user's authentication realm, click the **Realm** link next to the name.
  - To edit a user's role, click the **Role** link next to the name.

- Related Documentation**
- [User Roles Overview on page 105](#)
  - [Authentication Realm Overview on page 305](#)

---

## Viewing and Cancelling Scheduled Meetings

---

You can view all of the meetings currently scheduled on the Secure Access Service or cancel meetings.

To view and cancel scheduled meetings:

1. In the admin console, choose **System > Status > Meeting Schedule**. The Secure Access Service displays real-time information about all of the meetings that are currently running or scheduled, including:
  - **Time and Status**—Displays the time and duration that the meeting is scheduled to run, as well as the current status of the meeting.
  - **Meeting Details**—Displays the meeting name, ID, and password requirements. This column also includes a Details link that you can use to view information about the meeting and to join the meeting.
  - **Meeting Role**—Displays the role of the meeting creator. If the creator was signed into multiple roles when he created the meeting (i.e., he is a member of multiple roles and the appliance is configured for a permissive merge).
  - **Attendee Roles**—Displays the roles of the attendees who are signed into the meeting, the number of attendees signed into each role, and each role's meeting attendee limit. Note that non-Secure Access Service attendees are displayed under the meeting creator's user role.
2. Use either of the following methods to change the meeting view (optional):



- Select a time frame (Daily, Weekly, In Progress, Scheduled) from the drop-down list to control which meetings are displayed.
  - Click on any of the underlined column headers to control the order in which currently displayed meetings are sorted.
3. Click the **Details** link under a meeting to view information about the meeting and optionally to join the meeting (optional).
  4. Choose **MyMeeting URLs** from the View drop menu to view personal URLs your users have created.
  5. Click the delete icon in the right column to cancel a meeting or to delete a MyMeeting URL (optional).

Canceling a meeting permanently deletes from the Secure Access Service. You cannot restore a meeting after cancelling it.

**Related Documentation**

- [Junos Pulse Collaboration Overview on page 691](#)

## Adding Real Source IP Addresses to Log Messages

When a Juniper Networks DX appliance or similar load balancer is deployed in front of the Secure Access Service in proxy mode, the real client IP address can be preserved in a DX custom HTTP header and passed to the Secure Access Service. This real client IP address can be recorded within the Secure Access Service's logs when a user logs into the Secure Access Service (or a user roams), allowing you to audit and report on the username/real source IP pair using the Secure Access Service logs.

The remainder of this topic refers to Juniper Networks' DX appliance. See your load balancer's documentation for information on sending an "X-Forwarded-For" log header.

The real source IP address is retrieved from the DX custom header when a user logs in and is placed into the session record. The real source IP address is used in place of the DX IP address in the event, user, admin, and sensors log if it is present in the context data. Otherwise, the source IP address in the context data is used.

To enable the passing of this custom header to the Secure Access Service, perform the following tasks on your DX appliance:

1. Create a cluster and configure the VIP and target hosts.
2. Define the target and listen sides on the cluster configuration page.
3. In the DX Server page, set the Custom IP Log Header to "X-Forwarded-For".

See your DX documentation for more information on configuring the DX appliance.

The following log messages are updated on the Secure Access Service:

- AUT24326 (user and admin login)
- AUT20919 (user roaming)

- [ADM22896 \(admin roaming\)](#)

**Related  
Documentation**

- [Logging and Monitoring Overview on page 931](#)

# Troubleshooting

- [About Troubleshooting on page 959](#)
- [Simulating and Tracking Events on page 960](#)
- [Simulating Events That Cause a Problem on page 960](#)
- [Tracking Events Using Policy Tracing on page 962](#)
- [Recording a Trace File on page 963](#)
- [Creating System State Snapshot Files on page 964](#)
- [Creating TCP Dump Files on page 965](#)
- [Troubleshooting TCP and UDP Port Status on page 966](#)
- [Secure Access Service Network Connectivity Tools on page 969](#)
- [Using UNIX Commands to Test Network Connectivity on page 971](#)
- [Running NSLookup to Test Name Server Connectivity on page 971](#)
- [Running Debugging Tools Remotely on page 971](#)
- [Creating Debugging Logs on page 972](#)
- [Monitoring Cluster Nodes on page 973](#)
- [Configuring Group Communication Monitoring on a Cluster on page 974](#)
- [Configuring Network Connectivity Monitoring on a Cluster on page 974](#)

## About Troubleshooting

---

The Secure Access Service provides several troubleshooting utilities that enable you to monitor the state of your system, including clusters, if you use them. These topics provide an overview of the various troubleshooting tasks that are available by using the Secure Access Service:

Troubleshooting capabilities are available on all Secure Access Service products—you do not need a special license to use them. Note, however, that the following advanced features are not available on the SA700 Series Appliance:

- Session recording
- Monitoring and configuring clusters

- Related Documentation**
- [Simulating and Tracking Events on page 960](#)
  - [Creating System State Snapshot Files on page 964](#)
  - [Creating TCP Dump Files on page 965](#)

## Simulating and Tracking Events

---

You can determine why your Secure Access Service does not allow you to accomplish a task that you desire by simulating and tracking problematic Secure Access Service events using settings in the Maintenance > Troubleshooting > User Sessions > Policy Tracing page of the admin console.

The events in question are related to authentication, authorization, and access for a particular user. They are entirely driven by what happens during a user session. This applies to both simulation and policy tracing.

The events that are captured do not include any other system related events. The Secure Access Service merely uses the events as a filtering mechanism to reduce the number of logs and highlight the problem.

- Related Documentation**
- [Simulating Events That Cause a Problem on page 960](#)
  - [Tracking Events Using Policy Tracing on page 962](#)

## Simulating Events That Cause a Problem

---

The Secure Access Service allows you to troubleshoot problems by simulating the events causing the problem. Using the Maintenance > Troubleshooting > User Sessions > Simulation page, you can create virtual user sessions without requiring actual end-users to sign in to the Secure Access Service and recreate their problems. In addition, you can also use the Simulation tab to test new authentication and authorization policies before using them in a production environment.

To use the simulator, you must specify which events you want to simulate (for example, you can create a virtual session in which “John Doe” signs into the “Users” realm at 6:00 AM from an Internet Explorer browser). Then, you must specify which events you want to record and log in the simulation. You can log three major types of events to the simulation log:

- **Pre-Authentication**—The Secure Access Service events that are captured will not include any other system related events. Events are merely used as a filtering mechanism to reduce the number of logs and highlight the problem.
- **Role Mapping**—The Secure Access Service events that are captured will not include any other system related events. Events are merely used as a filtering mechanism to reduce the number of logs and highlight the problem.
- **Resource Policies**—The Secure Access Service events that are captured will not include any other system related events. Events are merely used as a filtering mechanism to reduce the number of logs and highlight the problem.

To simulate a user session:

1. In the admin console, choose **Maintenance > Troubleshooting > User Sessions > Simulation**.
2. In the Query Name field, enter a name for the query.
3. In the Username field, enter the username of the Secure Access Service user whose experience you want to simulate. Note that you may use a wildcard character (\*) in place of a username. For example, if your users are signing into an anonymous server, you may want to use the wildcard character (\*) since you cannot know the internal username that the Secure Access Service will assign to the user.
4. From the Realm drop down menu, select the realm of the Secure Access Service user whose experience you want to simulate.
5. If you want to determine whether the Secure Access Service applies a specific type of resource policy to a user's session, enter the specific resource you want to simulate in the Resource field and select a policy type from the Resource drop-down list. Then:
  - If you want to determine whether a user can successfully sign in to the Secure Access Service, select the **Pre-Authentication** checkbox.
  - If you want to determine whether a user can successfully map to a specific role, select the Role Mapping checkbox. Note that this option controls whether role mapping results are logged to the simulator log, not whether the Secure Access Service runs role mapping rules. The Secure Access Service always runs role mapping rules, even if you do not select this checkbox.
  - Specify the types of policies you want to log using the checkboxes in the Events to Log section.  
  
For example, if you want to test whether a user can access the Yahoo Web site, enter "http://www.yahoo.com" in the Resource field, select Web from the drop-down list, and select the Access checkbox in the Events to Log section.
6. In the Variables section, use a combination of text and variables to create a custom expression that reflects the exact same values as in the real session of the user who is facing a problem. For example, if you want to create a session in which the user signs in to the Secure Access Service at 6:00 AM, enter "time = 6:00 AM" in the Variables field. For complete instructions on how to create a custom expression. You may also view the syntax for a given variable by clicking the arrow next to it in the Variables Dictionary.  
  
If you fail to create a custom expression that includes the virtual user's IP address, the Secure Access Service uses your current IP address instead. Also note that if you use the role variable to specify the role of the virtual user (for example, role="Users"), the Secure Access Service ignores results from role mapping rules and assigns the virtual user to the role(s) you specify.
7. Choose one of the following options:
  - **Run Simulation**—Runs the specified simulation and creates an on-screen log file.
  - **Save Query**—Saves the query.

- **Save Query and Run Simulation**—Runs the specified simulation and also saves it for later use.
8. After running the simulation, choose **Save Log As** to save the simulation results to a text file.

**Related Documentation**

- [Simulating and Tracking Events on page 960](#)

## Tracking Events Using Policy Tracing

The Secure Access Service allows you to troubleshoot problems by tracking events when a user signs into a realm. The Maintenance > Troubleshooting > User Sessions > Policy Tracing page allows you record a policy trace file for an individual user, the Secure Access Service displays log entries that list the user's actions and indicates why he is allowed or denied access to various functions such as accessing the Web or a file server.

For example, you may create a "Human Resources" realm and create two role-mapping rules within the realm:

- **All Employees**—Within this role, you only enable web browsing. You map users to the role using the rule: if username = \*; map to "All Employees." In other words, any user who is allowed to sign into the realm automatically maps to the "All Employees" role.
- **Human Resources Staff**—Within this role, you enable web, file, and meeting functionality. You map users to the role using the rule: if LDAP group=human resources, map to "Human Resources Staff." In other words, a user must belong to the "humanresources" group on the LDAP authentication server in order to map to the role.

You may think that Joe should be a member of both roles, but when he signs into the Secure Access Service, he cannot access the file browsing or Junos Pulse Collaboration functionality enabled in the "Human Resources Staff" role. When you turn on policy tracing to determine why Joe cannot access all of expected functionality, you will see log entries.



**NOTE:** User access logs are only reported for policies that are checked under **Events to Log**.

By reviewing the trace file, you can determine the problem (an example is shown here):

```
joe(human resources realm)-No match on rule 'group.humanresources'
```

This entry shows that the Secure Access Service did not map Joe to the "Human Resource Staff" role because he is not a member of the "humanresources" group on the LDAP server.

Use this tab if your users are having problems accessing functions they expect to use in their roles. The events logged in the policy trace file may help you diagnose these problems.

To create a policy trace file:

1. In the admin console, select **Maintenance > Troubleshooting > User Sessions > Policy Tracing**.
2. In the **User** field, enter the Secure Access Service username of the user you want to trace. Note that you may use a wildcard character (\*) in place of a username. For example, if your users are signing into an anonymous server, you may want to use the wildcard character (\*) since you cannot know the internal username that the Secure Access Service will assign to the user.
3. In the **Realm** field, select the user's realm. Note that the Secure Access Service does not allow you to select a realm that maps to an anonymous authentication server.
4. Under **Events to log**, select the types of events you want to write to the policy tracing log file.
5. Click **Start Recording**. Ask the user to sign into the Secure Access Service after you have started recording.
6. Click **View Log** to see the log entries.
7. Click **Stop Recording** when you have obtained enough information.
8. Review messages in the log file to determine what is causing the unexpected behavior. If you cannot determine and fix the problem, click **Save Log As** to save a copy of the log file to a location on your network. Then, send the file to Juniper Networks Support for review.
9. Click **Clear Log** to clear the contents of the log file, or click **Delete Trace** to clear the contents of the log file and to remove the default entries from the username and realm fields.

**Related  
Documentation**

- [Creating TCP Dump Files on page 965](#)

## Recording a Trace File

---

When a Web site does not display properly through the Secure Access Service, the **Maintenance > Troubleshooting > User Sessions > Session Recording** tab allows you to record a trace file that lists a user's actions. In addition, you can use this tab when connecting to a client/server application that does not behave as expected through the Secure Access Service.

When you start recording a trace file, the Secure Access Service signs out the specified user and then starts recording all user actions after the user signs in again and is authenticated. Note that the Secure Access Service notifies the user after authentication that user actions are being recorded.

To record a trace file:

1. In the admin console, choose **Maintenance > Troubleshooting > User Sessions > Session Recording**.
2. Enter the username of the user whose session you want to record.
3. Select the **Web (DSRecord)** checkbox to record the user's web session and then select the Ignore browser cache checkbox if you want to ignore cached copies of the problem Web site, which the Secure Access Service would not otherwise record as a part of the trace file (optional).
4. Select the **Client/Server (for JCP)** checkbox to record Java Communication Protocol client/server application sessions (optional).
5. Click **Start Recording**. The Secure Access Service signs out the user.
6. Instruct the user to sign in again and browse to the problem Web site or connect to the client/server application through the Secure Access Service.
7. Click **Stop Recording**.
8. Download the trace file(s) from the Current Trace File section:
  - a. Click the **DSRecord Log** link to download the Web trace file.
  - b. Click the **JCP or NCP Client-Side Log** link to download the client/server application trace file.
9. Email the file(s) to Juniper Networks Support for review.
10. Select the Delete button to remove the trace file(s) you just created (optional).

**Related Documentation**

- [Simulating and Tracking Events on page 960](#)

---

## Creating System State Snapshot Files

You use the Maintenance > Troubleshooting > System Snapshot page to set up automatic snapshots or to create a user-generated snapshot of the Secure Access Service system state for analysis by JTAC. The snapshot feature runs various utilities to gather details on system state, such as the amount of memory in use, paging performance, the number of processes running, system uptime, the number of open file descriptors, ports in use, and FIPS log messages. The system snapshot file also contains the last 100 lines of event, user, and admin logs. The timestamp for these logs is the IVE OS Secure Access Service operating system timestamp.

[Table 59 on page 965](#) describes snapshot configuration options and details.



Table 59: Snapshot Configuration Options and Details

Configuration Options / Details	Notes
Files to include	You can choose to include or exclude system configuration and debug logs. However, debug logs are particularly important in the event of a problem. You will need to set the debug log at a certain level and add the events list as directed by your Support representative. Recreate the problem or event and then take a snapshot and send it to Support. The debug log is encrypted; you cannot view it.
Filenames	Admin generated snapshot files are named <b>juniper-state-admin-nodeName-X-YYYYMMDD-HHSSMM.encrypted</b> . Automatic snapshot files are named <b>juniper-state-watchdog-nodeName-X-YYYYMMDD-HHSSMM.encrypted</b> . JTAC uses internal processes to decrypt the file so that its contents can be analyzed.
Storage	The system stores up to ten snapshot files. If you take more than ten snapshots, the snapshot feature overwrites the oldest snapshot file with the new snapshot. If the system runs out of disk space, it does not store the newest snapshot. Instead, it logs a message in the Event log. Though the system compresses the files first and then performs the encryption to minimize file size, we recommend that you download the snapshots in a timely manner to avoid losing them.
Automatic snapshots	<p>When you select <b>Schedule automatic snapshots</b>, the user interface expands to display options to specify frequency and maximum disk utilization. The snapshot utility uses resources and space. Adjust frequency and maximum size properties accordingly.</p> <p><b>CAUTION:</b> You should enable automatic scheduled snapshots only when asked to do so by Juniper Networks Support as part of a troubleshooting operation. Enabling this feature can affect system performance. In most situations, a four-hour snapshot schedule captures the needed data without impacting system performance. Do not set a schedule interval of less than 30 minutes as this can affect system performance.</p>
Clusters	<p>For clusters, system snapshot options are not synchronized. The settings on each node determine snapshot behavior, and snapshot files are stored on individual nodes, not collected for clusters. You can, however, use the Maintenance &gt; Troubleshooting &gt; System Snapshot &gt; "Take Snapshot on All Nodes" button to run the snapshot operation on all nodes with one click.</p> <p><b>NOTE:</b> Do not click <b>Take Snapshot on All Nodes</b> repeatedly in a short time. Doing so might cause unexpected behavior.</p>

- Related Documentation**
- [Tracking Events Using Policy Tracing on page 962](#)
  - [Creating TCP Dump Files on page 965](#)

## Creating TCP Dump Files

To sniff network packet headers:

1. In the admin console, choose **Maintenance > Troubleshooting > Tools > TCP Dump**.
2. Select the Secure Access Service port on which you want to sniff network packet headers.

3. If you are operating with an IVS license, you can also select a VLAN port to sniff packet headers for a subscriber intranet.
4. Turn off **Promiscuous mode** to sniff only for packets intended for the Secure Access Service.
5. Create a custom filter using TCPDump Filter Expressions (optional). This option provides the ability to filter the sniffed network packets so that the resulting dump file contains only the information you require.
6. Click **Start Sniffing**.
7. Click **Stop Sniffing** to stop the sniffing process and create an encrypted file.
8. Click **Download** to download the file to a network machine.
9. Email the file to Juniper Networks Support for review.

**Related Documentation** • [Simulating and Tracking Events on page 960](#)

## Troubleshooting TCP and UDP Port Status

**Problem** The system makes several connections to back-end servers using various port numbers. If communication between the system and the back-end servers stops, it can be difficult to determine the source of the problem.

**Solution** You can use the Portprobe command to display the Transmission Control Protocol (TCP) or the User Datagram Protocol (UDP) port status (open or closed).



**NOTE:** Only the system internal ports, management port and internal VLAN ports support the Portprobe command.

A TCP port can be closed under two conditions:

- The system sends a connection request to the back-end server port and the back-end server closes the connection (sends an RST packet).
- The connection request times out because the back-end server is not found or the back-end server is too busy to respond to the connection request.

If either of these conditions occurs, the system sends a ping command to the back-end server. If the ping command is successful, the back-end server is considered reachable but the back-end server port is closed. If the ping command fails, the back-end server is considered unreachable.

For UDP ports, the system sends a UDP datagram with a ping to the back-end server port. If the back-end server responds with Internet Control Message Protocol (ICMP) port unreachable or ICMP unreachable, the back-end port is considered unreachable. If the back-end server responds with ICMP host unreachable then the back-end server is considered unreachable.

To troubleshoot the TCP or UDP port:

1. Select **Maintenance > Troubleshooting > Tools > Commands**.
2. Select the **Portprobe** command.
3. Select either **TCP** or **UDP**.
4. Enter the target server and port number. You can enter an IP address, hostname or FQDN for the target server.
5. Enter the probe count. This is the number of times the system attempts to communicate with the back-end server port. The default for TCP is one; the default for UDP is five.
6. Enter the probe timeout. This is the number of seconds the system waits for a response from the back-end server port.
7. Select either the internal port or the management port. If the management port is not configured, it is not displayed.
8. If using an internal port, select the internal VLAN port from the list.
9. Click **OK**.

[Figure 70 on page 968](#) and [Figure 71 on page 969](#) show an example of a successful and an unsuccessful port probe.

Figure 70: Successful TCP Port Probe

**Troubleshooting**

User Sessions | Monitoring | Tools | System Snapshot | Remote Debugging

TCP Dump | Commands | Kerberos

IPv6 is not supported

Command: Portprobe

Protocol: TCP

Target Server: www.google.com Target port[1-65535]: 80

Probe Count: 6 (default: tcp = 1, udp = 5, max = 100)

Probe Timeout: 1 (default: 1 secs, max = 180 secs)

Interface:  Internal Port

VLAN Port: Internal Port (10.64.78.34)

OK Clear

Output:

```
Resolving IP address for www.google.com
Resolved IP address: 74.125.129.147
Starting port probing

Tcp probe : 74.125.129.147:80 Open
Tcp probe : 74.125.129.147:80 Open
Tcp probe : 74.125.129.147:80 Open
Tcp probe : 74.125.129.147:80 Open
Tcp probe : 74.125.129.147:80 Open
Tcp probe : 74.125.129.147:80 Open
Operation complete
```

Figure 71: Unsuccessful UDP Port Probe

**Troubleshooting**

User Sessions | Monitoring | Tools | System Snapshot | Remote Debugging

TCP Dump | Commands | Kerberos

IPv6 is not supported

Command:

Protocol:

Target Server:  Target port[1-65535]:

Probe Count:  (default: tcp = 1, udp = 5, max = 100)

Probe Timeout:  (default: 1 secs, max = 180 secs)

Interface:  Internal Port  Management Port

VLAN Port:

Output:

```
Resolving IP address for 10.209.118.10
Resolved IP address: 10.209.118.10
Starting port probing

UDP probe: 10.209.118.10:8888 Close (Destination port is unreachable)
UDP probe: 10.209.118.10:8888 Close (Destination port is unreachable)
UDP probe: 10.209.118.10:8888 Close (Destination port is unreachable)
UDP probe: 10.209.118.10:8888 Close (Destination port is unreachable)
UDP probe: 10.209.118.10:8888 Close (Destination port is unreachable)

Operation complete
```

Related Documentation

- [Creating TCP Dump Files on page 965](#)

## Secure Access Service Network Connectivity Tools

The Maintenance > Troubleshooting > Tools > Commands tab allows you to run UNIX commands such as arp, ping, ping6, traceroute, traceroute6, NSlookup, and AvgRTTs to test Secure Access Service network connectivity. You can use these connectivity tools to see the network path from the Secure Access Service to a specified server. If you can ping or traceroute to the Secure Access Service and the Secure Access Service can ping the target server, any remote users should be able to access the server through the Secure Access Service.



**NOTE:** If you enable the external port (System > Network > External Port), the troubleshooting tools and commands pages contain option buttons for you to specify Internal Port or External Port. Select the port from which you want to send the command.

## Address Resolution Protocol

Use the arp command to map IP network addresses to the hardware addresses. The Address Resolution Protocol (ARP) allows you to resolve hardware addresses.

To resolve the address of a server in your network, a client process on the Secure Access Service sends information about its unique identify to a server process executed on a server in the intranet. The server process then returns the required address to the client process.

## Ping or Ping6

Use the ping command to verify that the Secure Access Service can connect to other systems on the network. In the event of a network failure between the local and remote nodes, you do not receive a reply from a pinged device. In that case, contact your LAN administrator for help.

The ping command sends packets to a server and returns the server response, typically a set of statistics including the target server's IP address, the time spent sending packets and receiving the response, and other data. You can ping unicast or multicast addresses, and you must include the target server name in the request.

Select **ping** to ping an IPv4 address or hostname. Select **ping6** to ping an IPv6 address. We do not support DNS resolution for hosts with IPv6 addresses. Hence, ping6 does not support pings to hostnames.

## Traceroute or Traceroute6

Use the traceroute command to discover the path that a packet takes from the Secure Access Service to another host. Traceroute sends a packet to a destination server and receives an ICMP TIME\_EXCEEDED response from each gateway along its path. The TIME\_EXCEEDED responses and other data are recorded and displayed in the output, showing the path of the packet round-trip.

Select **traceroute** to target an IPv4 address or hostname. Select **traceroute6** to target an IPv6 address. We do not support DNS resolution for hosts with IPv6 addresses. Hence, traceroute6 does not support traceroute to hostnames.

## NSlookup

Use NSlookup to get detailed information about a name server on the network. You can query on several different types of information, including a server's IP address, alias IP address, start-of-authority record, mail exchange record, user information, well-known services information, and other types of information.

## AvgRTTs

Use AvgRTTs to display the average round-trip time (RTT) to the localhost.

### Related Documentation

- [Using UNIX Commands to Test Network Connectivity on page 971](#)

---

## Using UNIX Commands to Test Network Connectivity

---

To run a UNIX command to test Secure Access Service network connectivity:

1. In the admin console, choose **Maintenance > Troubleshooting > Tools > Commands**.
2. From the Command list, select the command to run.
3. In the Target Server field, enter the IP address of the target server.
4. If you are operating on an IVS license, you can select a VLAN port, to test connectivity to a subscriber intranet.
5. Enter other arguments or options.
6. Click **OK** to run the command.

**Related  
Documentation**

- [Secure Access Service Network Connectivity Tools on page 969](#)

---

## Running NSLookup to Test Name Server Connectivity

---

To run NSLookup to test name server connectivity:

1. In the admin console, choose **Maintenance > Troubleshooting > Tools > Commands**.
2. From the Command list, select **NSLookup**.
3. Select the type of query to use from the Query Type drop down menu.
4. Enter the query, which is a host name, an IP address, or other information, depending on your selection of query type.
5. Enter the DNS server name or IP address.
6. If you are operating on an IVS license, you can select a VLAN port, to test connectivity to a subscriber intranet.
7. Enter other options.
8. Click **OK** to run the command.

**Related  
Documentation**

- [Troubleshooting VLANs on page 1053](#)

---

## Running Debugging Tools Remotely

---

The Juniper Networks Support team can run debugging tools on your production Secure Access Service if you configure it to do so through the Maintenance > Troubleshooting > Remote Debugging page. To enable this option, you must work with Juniper Networks Support to obtain a debugging code and host to which your Secure Access Service connects.

To enable remote debugging:

1. Contact Juniper Networks Support to set up the terms of a remote debugging session.
2. In the admin console, choose **Maintenance > Troubleshooting > Remote Debugging**.
3. Enter the debugging code provided by Juniper Networks Support.
4. Enter the host name provided by Juniper Networks Support.
5. Click **Enable Debugging** to allow the Juniper Networks Support team to access the Secure Access Service.
6. Notify Juniper Networks Support that your Secure Access Service is accessible.
7. Click **Disable Debugging** when Juniper Networks Support notifies you that the remote debugging session is over.

**Related Documentation**

- [Secure Access Service Network Connectivity Tools on page 969](#)

## Creating Debugging Logs

If you have a problem, a Juniper Networks Support representative may ask you to create debugging logs to assist with debugging Secure Access Service internal issues. When you enable logging, Secure Access Service records certain events and messages based on event codes you enter into admin console on the Maintenance > Troubleshooting > Monitoring > Debug Log tab. Using the debug log that results, the support team can identify the code flow for any discrepancies. Your support representative gives you all of the information you need to create the log file, including the debug detail log level and the event codes.



**NOTE:** Running debug logging can impact your system performance and stability. You should only generate debug logs when directed by your Juniper Networks Support representative.

To enable the debug log:

1. In the admin console, choose **Maintenance > Troubleshooting > Monitoring > Debug Log**.
2. Select the **Debug Logging On** checkbox.
3. Enter the **MAX debug log size**.
4. Enter the **Debug log detail level**.



**NOTE:** Setting the detail level to 0 displays only Critical messages, it does not disable logging completely.

5. Select the **Include logs** check box to include log details.



6. Enter the **Event Codes** specified by Juniper Networks Support.
7. Click **Save Changes**.
8. Choose the **Maintenance > Troubleshooting > System Snapshot** tab.
9. Check the **Include debug log** checkbox.
10. Click **Take snapshot** to create a file that contains the debug log. Secure Access Service compresses the files and then encrypts them to minimize file size.
11. Click **Download**.
12. Attach the snapshot file in an email message and send it to Juniper Networks Support.

**Related  
Documentation**

- [Secure Access Service Network Connectivity Tools on page 969](#)

## Monitoring Cluster Nodes

---

If you have a problem with a cluster, a Juniper Networks Support representative may ask you to create a snapshot that includes node monitoring statistics to assist with debugging the cluster problem. When you enable the node monitor on the **Maintenance > Troubleshooting > Monitoring > Node Monitor** tab, the Secure Access Service captures certain statistics specific to the cluster nodes on your system. Using the snapshot that results, the support team can identify important data, such as network statistics and CPU usage statistics.

To enable node monitoring:

1. Enable the node monitor on the **Maintenance > Troubleshooting > Monitoring > Node Monitor** tab
2. Enter the maximum size for the node monitor log.
3. Enter the interval, in seconds, at which node statistics are to be captured.
4. Select the **Node monitoring enabled** checkbox to start monitoring cluster nodes.
5. For **Maximum node monitor log size**, enter the maximum size (in MB) of the log file. Valid values are 1-30.
6. Specify the interval (in seconds) that defines how often nodes are to be monitored.
7. Select the commands to use to monitor the node.  
If you select **dsstatdump**, enter its parameters as well.
8. Click **Save Changes**.
9. If you want to include the node monitoring results in the system snapshot, choose **Maintenance > Troubleshooting > System Snapshot**, and select the **Include debug log** checkbox.
10. Take a system snapshot to retrieve the results.

- Related Documentation**
- [Configuring Group Communication Monitoring on a Cluster on page 974](#)
  - [Configuring Network Connectivity Monitoring on a Cluster on page 974](#)
  - [Task Summary: Deploying a Cluster on page 981](#)

## Configuring Group Communication Monitoring on a Cluster

---

To enable group communication monitoring:

1. Enter the maximum size for the statistics log.
2. Enter the interval, in seconds, at which events are to be logged.
3. If you want to monitor all cluster nodes from the current local node, select the **Monitor all cluster nodes from this node** checkbox. If you do not check this option, the group communication monitor gathers statistics only for the local node.



**NOTE:** If you select the Monitor all cluster nodes from this node option, the cluster nodes must be able to communicate over UDP port 6543.

4. Select the **Enable group communication monitoring** checkbox to start the monitoring tool.
5. Click **Save Changes**.
6. If you want to include the node monitoring results in the system snapshot, choose **Maintenance > Troubleshooting > System Snapshot**, and select the Include debug log checkbox.
7. Take a system snapshot to retrieve the results.

- Related Documentation**
- [Configuring Network Connectivity Monitoring on a Cluster on page 974](#)

## Configuring Network Connectivity Monitoring on a Cluster

---

If you have a problem with a cluster, a Juniper Networks Support representative may ask you to enable the cluster node troubleshooting server. When you enable the server on the **Maintenance > Troubleshooting > Cluster > Network Connectivity** tab, the Secure Access Service attempts to establish connectivity between the node on which the server resides and another node you specify. As the nodes communicate, the Secure Access Service displays network connectivity statistics on the page. The **Maintenance > Troubleshooting > Cluster > Network Connectivity** tab appears only when you enable clustering on your system. On a standalone Secure Access Service, you do not have access to the **Maintenance > Troubleshooting > Cluster > Network Connectivity** tab.

Use the Network Connectivity page to enable the cluster node troubleshooting server and to select a node on which to perform troubleshooting tasks. The troubleshooting tool allows you to determine the network connectivity between cluster nodes.

The server component of this tool runs on the node to which connectivity is being tested. The client component runs on the node from which connectivity is being tested. The basic scenario for testing connectivity is this:

- The administrator starts the server component on the passive node.
- The administrator then tests the connectivity to the server node from the Active node, by starting the client component on the Active node and contacting the Passive node running the server component.

When troubleshooting a standalone server, you must specify the client IP address in the Client Node field. In this case, the client IP address is the IP address of the standalone server. When troubleshooting a server within a cluster node, you do not have to specify the client IP address in the Client Node field.

Standalone nodes must be pinged as a standalone and not as part of a cluster.



**NOTE:** The troubleshooting server must be turned off before you join a cluster.

To enable network connectivity monitoring:

1. Select the **Enable cluster network troubleshooting server** checkbox to enable the server component.



**NOTE:** This option is not available in the NSM user interface.

2. If you are troubleshooting a standalone server, enter the server's IP address in the Client Node field.
3. Click **Save Changes**.
4. On another machine, select **Maintenance > Troubleshooting > Cluster > Network Connectivity**.
5. Perform one of the following steps:
  - Select a node from the drop-down list.
  - Enter the IP address of the server node.
6. Click **Go** to begin troubleshooting the machine on which the server component is running.
7. Click the **Details** link that appears on the page below the fields, to view the results.

#### Related Documentation

- [Monitoring Clusters on page 999](#)



## CHAPTER 35

# Clustering

- [About Clustering on page 977](#)
- [Cluster Licensing on page 978](#)
- [Task Summary: Deploying a Cluster on page 981](#)
- [Defining and Initializing a Cluster on page 982](#)
- [Joining an Existing Cluster on page 983](#)
- [Re-adding a Node to a Cluster on page 984](#)
- [Deploying Two Nodes in an Active/Passive Cluster on page 985](#)
- [Failing Over the VIP to Another Node on page 986](#)
- [Deploying Two or More Units in an Active/Active Cluster on page 986](#)
- [Synchronizing the Cluster State on page 988](#)
- [Specifying Active/Passive, Active/Active, and Other Cluster Settings on page 990](#)
- [Adding Multiple Cluster Nodes on page 992](#)
- [General Cluster Maintenance on page 993](#)
- [Migrating Cluster Configurations to a Replacement Cluster on page 994](#)
- [Changing the IP Address of a Cluster Node on page 995](#)
- [Deleting a Cluster on page 996](#)
- [Restarting or Rebooting Clustered Nodes on page 996](#)
- [Configuring the External VIP for An Active/Passive Cluster on page 996](#)
- [Admin Console Procedures on page 997](#)
- [Monitoring Clusters on page 999](#)
- [Troubleshooting Clusters on page 1000](#)
- [Serial Console Procedures on page 1002](#)
- [Joining the Secure Access Service to a Cluster Through Its Serial Console on page 1002](#)
- [Disabling a Clustered Secure Access Service Using Its Serial Console on page 1004](#)

## About Clustering

---

Secure Access Service supports Active/Passive or Active/Active clustering across a LAN to provide high availability, increased scalability, and load balancing capabilities.

You define a cluster on one Secure Access Service by specifying three pieces of data:

- A name for the cluster
- A password for the cluster members to share
- A name to identify the machine in the cluster

Entering this information enables you to initiate the first member of your cluster. You then need to specify which Secure Access Service you want to add to the cluster. After the Secure Access Service is identified as an intended member, you may add it to the cluster through either the admin console or the serial console (if the machine is in the initial factory state).

When the Secure Access Service joins a cluster, it initializes its state from the existing member that you specify. The new member sends a message to the existing member requesting synchronization. The existing member sends the system state to the new member, overwriting all system data on that machine. After that point, the cluster members synchronize data when there is a state change on any member. Cluster member communication is encrypted to prevent attacks from inside the corporate firewall. Each Secure Access Service uses the shared password to decrypt communication from another cluster member. For security reasons, the cluster password is not synchronized across Secure Access Services.

During synchronization, the new node receives the service package, which upgrades the node if it is running an older service package.

**Related  
Documentation**

- [Viewing General Status on page 950](#)
- [Task Summary: Deploying a Cluster on page 981](#)
- [Cluster Licensing on page 978](#)
- [Defining and Initializing a Cluster on page 982](#)
- [Joining an Existing Cluster on page 983](#)

---

## Cluster Licensing

Secure Access Service software 7.0 introduces several clustering license changes including:

- A license is no longer required to create a cluster.
- CL licenses are no longer necessary but are still supported.
- A 10 day *cluster grace period* to provide license flexibility when a node crashes or loses connectivity with the rest of the cluster.
- Juniper Networks recommends that you distribute your ADD licenses equally across the cluster to avoid losing large number of licenses when a node disconnects from the cluster.



**NOTE:** The clustering feature is not available on the SA700 Series Appliance. You can run the Secure Access Service with an IVS license in a cluster.

If you are content with your current licensing process, you can carry that forward with the new license scheme. Upgrading may result in a few changes if you have mismatched concurrent user and CL licenses. A cluster that was once “unqualified” may become “qualified” and will be able to support user loads. Your user capacity should not decrease when upgrading to the new licensing scheme.

The maximum number of concurrent users allowed in a cluster is the sum of all user licenses of all connected nodes. If a node disconnects from the cluster (either A/A or A/P), up until the grace period ends the maximum license per each remaining node is their current license plus the minimum of their own license and the licenses of the other nodes. The following examples explain this in more detail.

### Example 1: Licenses Distributed Equally Among Nodes

Suppose Node A and Node B are part of a cluster and each node has 500 concurrent user licenses. As long as both nodes are connected, the maximum number of licenses is 1000.

Suppose Node B disconnects from the cluster. Up until the clustering grace period ends, the maximum number of licenses on Node A is 500 (from Node A's original license) + minimum (licenses on Node A (500), licenses on Node B (500)) = 500 + 500 = 1000.

After the grace period ends, the maximum number of licenses on Node A reverts to its original license of 500.

### Example 2: Licenses Distributed Unequally Among Nodes

Suppose Node A and Node B are part of a cluster. Node A has 600 ADD licenses and Node B has 400 ADD licenses. As long as both nodes are connected, the maximum number of licenses is 1000.

Suppose Node B disconnects from the cluster. Up until the clustering grace period ends, the maximum number of licenses on Node A is 600 (from Node A's original license) + minimum (licenses on Node A (600), licenses on Node B (400)) = 600 + 400 = 1000. After the grace period ends, the maximum number of licenses on Node A is 600.

Suppose Node A disconnects from the cluster. Up until the clustering grace period ends, the maximum number of licenses on Node B is 400 (from Node B's original license) + minimum (licenses on Node A (600), licenses on Node B (400)) = 400 + 400 = 800. After the grace period ends, the maximum number of licenses on Node B is 400.

### Example 3: Licenses Distributed Unequally Among Nodes (Extreme Case)

Suppose Node A and Node B are part of a cluster. Node A has 1000 ADD licenses and Node B has 0 ADD licenses. As long as both nodes are connected, the maximum number of licenses is 1000.

Suppose Node B disconnects from the cluster. Up until the clustering grace period ends, the maximum number of licenses on Node A is 1000 (from Node A's original license) + minimum (licenses on Node A (1000), licenses on Node B (0)) = 1000 + 0 = 1000. After the grace period ends, the maximum number of licenses on Node A is 1000.

Suppose Node A disconnects from the cluster. Up until the clustering grace period ends, the maximum number of licenses on Node B is 0 (from Node B's original license) + minimum (licenses on Node A (1000), licenses on Node B (0)) = 0 + 0 = 0. After the grace period ends, the maximum number of licenses on Node B is 0.

Given the scenarios in Examples 2 and 3, we recommend you distribute the licenses equally amongst the nodes.

## Upgrading From Previous Versions

Prior to Secure Access Service software version 7.0, to create an  $n$ -node cluster supporting  $cccc$  concurrent users, you were required to purchase one ADD- $cccc$ E license for one cluster node, and  $n-1$  CL licenses (one for each of the remaining cluster nodes). For example, to create a 4-node cluster supporting 2000 concurrent users, you needed to purchase one ADD-2000E license and 3 CL licenses.

When upgrading to Secure Access Service software version 7, your existing licenses will continue to work. The total concurrent user capacity is still the sum total of all user licenses as long as all nodes are connected. However, when a node disconnects the capacity computation changes as follows:

- Licenses on connected nodes count towards the total cluster capacity.
- If user licenses are present on the computing node, that same number of user licenses can be borrowed from each disconnected node that falls within the cluster grace period.
- If CL licenses are present on the computing node, user licenses can be borrowed from the disconnected nodes so that they total the number of CL licenses.

The following example explains this in more detail.

Suppose you have the following four-node cluster configuration:

- Node A with 1000 user licenses is connected to the cluster
- Node B with 400 user licenses and 200 CL licenses is connected to the cluster
- Node C with 500 user licenses and 500 CL licenses is disconnected from the cluster for 17 hours
- Node D with 1000 user licenses is disconnected from the cluster for 6 days

The total cluster capacity from Node B's point of view is as follows:

- 1000 licenses from Node A because it is connected.
- 400 licenses from Node B because that's its own license.



- Node C falls within the cluster grace period of 10 days. Using bullet 2 from the above computation notes, since Node B has 400 user licenses it can borrow 400 licenses from Node C's 500 licenses.

Node B also has 200 CL licenses. However, it already borrowed 400 of Node C's 500 user licenses so only 100 of Node C's user licenses remain to be used towards Node B's CL license count.

Node B counts  $400+100=500$  licenses from Node C.

- Since Node D has been disconnected from the cluster longer than the cluster grace period, Node B can not borrow Node D's user licenses.

Node B has 200 CL licenses. It already borrowed 100 user licenses from Node C, therefore it can borrow 100 user licenses from Node D.

Node B counts 100 licenses from Node D.

The total cluster capacity from Node B's point of view is  $1000+400+500+100=2000$ .

#### Related Documentation

- [Task Summary: Deploying a Cluster on page 981](#)

## Task Summary: Deploying a Cluster

We recommend that you deploy a cluster in a staging environment first and then move to a production environment after testing authentication realm, user role, and resource policy configurations, as well as any applications your end-users may access.

To create the Secure Access Service cluster:

1. Ensure that all intended Secure Access Service nodes use the same hardware platform (for example, all are SA6500 Series Appliances).
2. Ensure that all intended Secure Access Service nodes have been initially configured (for example, Secure Access Service host name is specified and the internal and external IP addresses are assigned), and they are running the same service package version.

At this stage, do not configure anything more than the internal and external IP addresses. You should have just the minimal network configuration prior to joining the nodes to a cluster. For example, do not configure VIPs, VLAN and VPORTS. After joining the nodes to a cluster, you can then create the VIPs, VLAN and VPORTS, and so forth.

3. From the System > Clustering > Create Cluster page, initialize the Secure Access Service cluster by defining the cluster name and adding the first/primary Secure Access Service to the cluster.
4. From the System > Clustering > Status page, add the names and IP addresses of future cluster members.
5. From the System > Clustering > Join Cluster page, populate the cluster with additional members as necessary.

6. When using Pulse clients with an active/active cluster, you must split the IP address pool across the nodes to ensure proper routing from the backend to the end user. This is a requirement whether the IP address pool is provisioned statically on the Secure Access Service or dynamically by way of DHCP.

The client IP pool configuration is synchronized among all nodes in a cluster; however, you may configure each node to use a certain subset of the global IP pool.

7. If you are creating a cluster of SA Series FIPS Appliances, manually update the security world on each of the machines.

**Related Documentation**

- [Defining and Initializing a Cluster on page 982](#)
- [Joining an Existing Cluster on page 983](#)
- [Serial Console Procedures on page 1002](#)
- [Admin Console Procedures on page 997](#)

---

## Defining and Initializing a Cluster

---

You use the primary node admin GUI graphical user interface to create the cluster and add members. The primary node is added as part of the cluster creation operation. When you add members, you are prompted for settings unique to the member, such as the name and IP address configuration for the internal and external interfaces. A few additional settings are also unique, namely the management port and VLAN port settings, so you add these manually after the add node procedure that follows, but before the join cluster operation.

To create a cluster and add members:

1. Select **System > Clustering > Create** and enter a name for the cluster, a cluster password, and a name for this node, such as Node-1.

You need to enter the password again when specifying additional nodes to join the cluster. All nodes in the cluster use this password to communicate.

2. Click **Create Cluster**. When prompted to confirm the cluster creation, click **Create**. After the Secure Access Service initializes the cluster, the Clustering page displays the Status and Properties tabs.
3. Click **Add Members** to specify the additional cluster nodes:
  - a. Enter a name for the member; for example, Node-2.
  - b. Enter the internal IP address. If both IPv4 and IPv6 are enabled on the internal port on Node-1, the system prompts for both IPv4 and IPv6 settings for the internal port for Node-2. Note, however, that in Release 7.3, intracluster communication uses the IPv4 corporate network.
  - c. Enter the external IP address. If both IPv4 and IPv6 are enabled on the external port on Node-1, the system prompts for both IPv4 and IPv6 settings for the external port for Node-2.

- d. Change the netmask/prefix-length and gateway settings for the node if necessary.
- e. Click **Add Node**. When prompted to confirm adding the new member, click **Add**.  
When the add node operation has completed, Node-2 is shown as an unreachable member of the cluster.
- f. The add node procedure does not prompt you to configure management port or VLAN port settings. As needed, go to the node port configuration page and configure these settings. For example, after the add node operation has completed for Node-2, go to its System > Network > Port > Settings page and configure its management port.
- g. Repeat this procedure for each node you intend to add to a cluster.

- Related Documentation**
- [Task Summary: Deploying a Cluster on page 981](#)
  - [Joining an Existing Cluster on page 983](#)

## Joining an Existing Cluster

---

Existing node-specific settings are erased when the Secure Access Service node joins a cluster. These settings include network interface addresses, route tables, virtual ports, ARP caches, VLAN interface, SNMP settings, and so forth. You must manually reconfigure these settings for the newly joined node. You cannot use the Import system configuration feature to import these configurations and settings onto the Secure Access Service node that has been joined to the cluster.

The method you use to add the Secure Access Service to a cluster depends on whether or not the Secure Access Service is configured or uninitialized (still in its factory state). This topic describes how to use the admin GUI to join a cluster. For the Secure Access Service in its factory state, we recommend that you use the serial console procedure because it requires you to enter minimal information for the machine to join a cluster. See [“Serial Console Procedures” on page 1002](#).

In an FIPS environment, you must use the admin console to add the Secure Access Service to a cluster. You also must have physical access to:

- The cryptographic modules installed in the front panels of the cluster members' Secure Access Services
- A smart card reader
- An administrator card that is pre-initialized to the active cluster member's security world

The primary node joins the cluster as part of the creation process. Use the following procedure to join additional nodes to the cluster.

To join a node to the cluster:

1. From an existing cluster member, select the **System > Clustering > Cluster Status** tab and specify the Secure Access Service you want to add to the cluster.
2. From the admin GUI of the Secure Access Service you want to join to a cluster:
  - a. Select the **System > Clustering > Join** tab and enter:
    - The name of the cluster to join.
    - The cluster password you specified when defining the cluster.
    - The IPv4 address for the internal port of an active cluster member.
  - b. Click **Join Cluster**. When prompted to confirm joining the cluster, click **Join**.

The join cluster operation validates IPv4 and IPv6 settings for all the physical ports (internal/external/management) against those present in the existing cluster. For example, the external port IPv6 settings present on Node-2 are compared against external port IPv6 settings that were specified for the Node-2 add member operation entered on the primary node (Node-1). If there is a mismatch, the join operation fails with an appropriate error message.

While the new node synchronizes its state with the existing cluster member, each node's status indicates **Enabled**, **Enabled, Transitioning**, or **Enabled, Unreachable**.

When the node finishes joining the cluster, its Clustering page shows the Status and Properties tabs.

After the node joins the cluster, you might need to sign in again.

**Related  
Documentation**

- [Serial Console Procedures on page 1002](#)
- [Importing and Exporting Secure Access Service Configuration Files on page 896](#)

---

## Re-adding a Node to a Cluster

---

With some maintenance operations, it may be necessary to remove a node from a cluster, then re-add and re-join it to the cluster.

When the Secure Access Service node joins a cluster, all of its node-specific settings (including network interface addresses, route tables, virtual ports, ARP caches, VLAN interface, SNMP settings) are overwritten by the corresponding configuration setting it receives from the cluster.

To populate the newly joined node with the correct node-specific settings:

1. Add the node to the cluster.
2. From any of the existing nodes in the cluster, manually configure the desired node-specific settings for the newly added node.
3. Join the node to the cluster.

When the node joins the cluster, it receives its newly configured node-specific settings from the cluster.



**NOTE:** You configure the node-specific settings for the newly added node manually because binary import options are not useful. The only recommended binary import option into a cluster is “Import everything except network settings and licenses” from the Maintenance > Import/Export > Configuration page which restores cluster-wide configuration (sign-in, realms, roles, resource policies etc.) from a backup binary file. Because this option skips node-specific settings, you must perform step 2 as a manual step in order to populate the newly-joined node with the right set of node-specific settings.

**Related Documentation**

- [Joining an Existing Cluster on page 983](#)

## Deploying Two Nodes in an Active/Passive Cluster

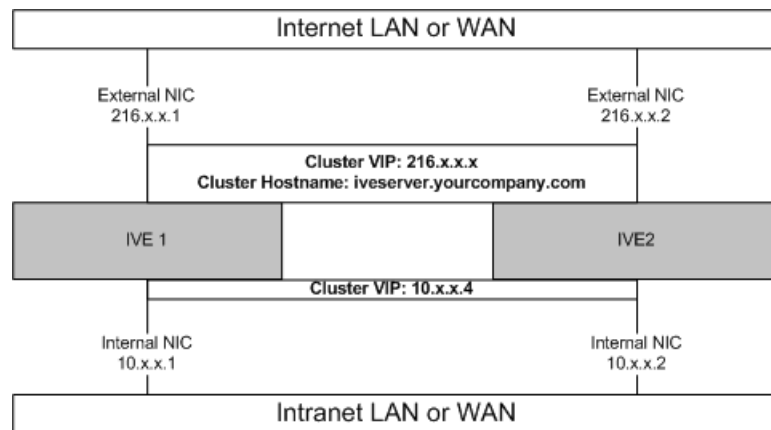
You can deploy Secure Access Services as a cluster pair in Active/Passive mode. In this mode, one Secure Access Service actively serves user requests while the other Secure Access Service runs passively in the background to synchronize state data, including system state, user profile, and log messages. User requests to the cluster VIP (virtual IP address) are passed to the active Secure Access Service. If the active Secure Access Service goes off-line, the standby Secure Access Service automatically starts servicing user requests. Users do not need to sign in again, however some Secure Access Service session information entered a few seconds before the active machine went off-line, such as cookies and passwords, may not have been synchronized on the current Secure Access Service, in which case users may need to sign in to back-end Web servers again.

You might need to fail-over the cluster VIP to the other node, manually. You can perform a manual failover by using the Fail-Over VIP button on the Clustering Status page.

The following figure illustrates an active/passive Secure Access Service cluster configuration using two Secure Access Services that have enabled external ports. Note that this mode does not increase throughput or user capacity, but provides redundancy to handle unexpected system failure.

User requests are directed to the cluster VIP, which then routes them to the currently active machine.

Figure 72: Active/Passive Cluster Pair



#### Related Documentation

- [Failing Over the VIP to Another Node on page 986](#)
- [Specifying Active/Passive, Active/Active, and Other Cluster Settings on page 990](#)
- [Using Device Certificates on page 839](#)

## Failing Over the VIP to Another Node

In an active/passive cluster, you might need to fail-over the VIP to the other node, regardless of which node you are currently using.

To failover the VIP:

1. Select **System > Clustering > Cluster Status** from the admin console.
2. Click the **Fail-Over VIP** button to move to the other node. The Fail-Over VIP button is a toggle button, so you can move from one node to the other, regardless of which is the leader.

The failover occurs immediately.



**NOTE:** VIP failover does not occur when the management port fails.

#### Related Documentation

- [Deploying Two Nodes in an Active/Passive Cluster on page 985](#)

## Deploying Two or More Units in an Active/Active Cluster

In Active/Active mode, all the machines in the cluster actively handle user requests sent by an external load balancer. The load balancer hosts the cluster VIP and routes user requests to the Secure Access Service defined in its cluster group based on source-IP routing. If the Secure Access Service goes off-line, the load balancer adjusts the load on the active Secure Access Services. Users do not need to sign in again, however some Secure Access Service session information entered a few seconds before the active

machine went off-line, such as cookies and passwords, may not have been synchronized on the current Secure Access Service, in which case users may need to sign in to back-end Web servers again.



**NOTE:**

When choosing and configuring a load balancer for your cluster, we recommend that you ensure the load balancer:

- Supports IPsec
- Listens for traffic on multiple ports
- Can be configured to manage traffic using assigned source and destination IP addresses (not destination port)

The Secure Access Service cluster itself does not perform any automatic fail-over or load-balancing operations, but it does synchronize state data (system, user, and log data) among cluster members. When an off-line Secure Access Service comes back online, the load balancer adjusts the load again to distribute it among all active members. This mode provides increased throughput and performance during peak load but does not increase scalability beyond the total number of licensed users.

The Secure Access Service synchronizes state data on all nodes if you add or delete the host entry by using the Network Settings pages. If you add or delete the host entry using the Clustering tab for a cluster member, the state data only affects the node and the Secure Access Service does not synchronize the data across the entire cluster.

The Secure Access Service hosts an HTML page that provides service status for each Secure Access Service in a cluster. External load balancers can check this resource to determine how to effectively distribute the load among all the cluster nodes.

To perform the Layer 7 health check for a node:

- **From a browser**—Enter the URL:

```
https://<Secure Access Service
Controller-Hostname>/dana-na/healthcheck/healthcheck.cgi
```

- **From an external load balancer**—Configure a health check policy that sends the following request to cluster nodes:

```
GET /dana-na/healthcheck/healthcheck.cgi HTTP/1.1\r\nHost: localhost\r\n\r\n
```

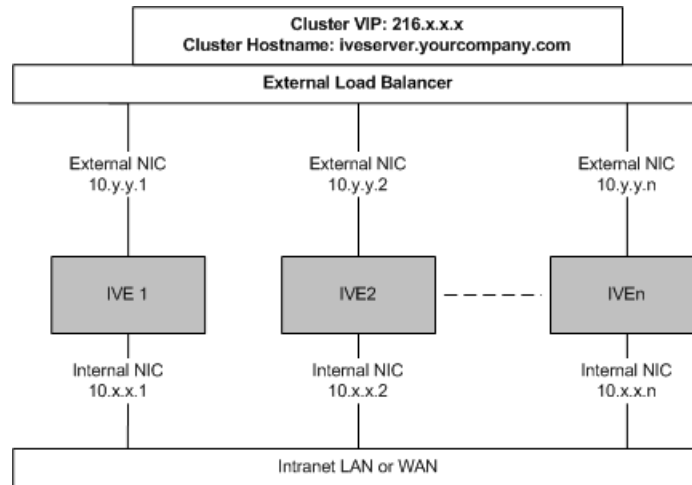
The node returns one of two values:

- **“Security gateway is accessible” string**—This value means the node is active.
- **500**—This value denotes an error and cluster Secure Access Services stop forwarding user requests to the node.

[xref target has no title] illustrates an active/active Secure Access Service cluster configuration in which the Secure Access Services have enabled external ports.

This active/active cluster configuration is deployed behind an external load balancer. You can deploy a cluster pair or multi-unit cluster in active/active mode. Secure Access Service user requests are directed to the cluster VIP defined on the load balancer, which routes them to the appropriate machine.

Figure 73: Active/Active Configuration



- Related Documentation**
- [Specifying Active/Passive, Active/Active, and Other Cluster Settings on page 990](#)
  - [Synchronizing the Cluster State on page 988](#)
  - [Using Device Certificates on page 839](#)

## Synchronizing the Cluster State

Secure Access Service state synchronization occurs only by means of the internal network interface cards (NICs), and each cluster member is required to possess the cluster password to communicate with other members. Cluster members synchronize data when there is a state change on any member. Secure Access Service cluster state data is either persistent—permanently stored on the Secure Access Service—or transient—stored on the Secure Access Service only for the user's session. Secure Access Service state data is divided into the following major categories:

- **System state**—This state is persistent and does not change often.
  - Network settings
  - Authentication server configurations
  - Authorization group configurations, such as access control list, bookmark, messaging, and application data
- **User profile**—This data can be either persistent or transient, depending on whether or not you have enabled persistent cookies and persistent password caching. If you have not enabled these features, then the data is transient and falls into the next category.
  - User bookmarks—persistent



- Persistent user cookies—if the persistent cookies feature is enabled, the Secure Access Service stores user cookies for Web sites that issue persistent cookies
- Persistent user passwords—if the password caching feature is enabled, the user can choose to store her credentials for applications and Web sites
- **User session**—This state is transient and dynamic. The user session consists of the following data:
  - The user Secure Access Service session cookie
  - Transient user profile information, which includes cookies and passwords stored only for during the user's session
- **Monitoring state**—This persistent information consists of log messages.

Whether you deploy a cluster in Active/Passive or Active/Active mode, the Secure Access Service is responsible for synchronizing data between cluster members. The Secure Access Service synchronizes all system data, user profile data, and the Secure Access Service user session cookies immediately, so if one cluster member goes off-line, users do not need to sign in to the Secure Access Service again. A small amount of latency occurs when the Secure Access Service synchronizes user session profile and monitoring state data, so if a member goes off-line, the user may need to sign in to some back-end Web applications again and administrators may not have access to the logs on the failed machine.

If you notice too much latency occurring on one or more nodes, you might need to change the Clustering Timeouts Settings.

When you add the Secure Access Service to a cluster, the cluster leader does not send log messages to the new member. Log messages are also not synchronized between cluster members when one member restarts its services or when an offline machine comes back online. Once all machines are online, however, log messages are synchronized.



**NOTE:** If you are running an active/active cluster, you must not allow the cluster to switch to active/passive mode unless the active/active and active/passive clusters share compatible spread timeout settings.

You may also configure synchronization settings to improve performance:

- **Specify the synchronization protocol**—When running three or more Secure Access Services in a multi-unit or multi-site cluster, you can choose to use the synchronization protocol (Unicast, Multicast, or Broadcast) that best suits your network topology.



**NOTE:** Multicast or broadcast for cluster communication is not supported on the MAG Series Junos Pulse Gateways.

- **Synchronize log messages**—Log messages may create a huge payload on the network and affect cluster performance. This option is disabled by default.

- **Synchronize user sessions**—This option synchronizes all user session information (instances of access to intranet services, for example) among all Secure Access Services in the cluster.
- **Synchronize last access time for user sessions**—This option allows you to propagate user access information in the cluster. If this option is the sole synchronization item among the cluster nodes, you can significantly reduce CPU impact among the cluster Secure Access Services.



NOTE:

- If you configure your cluster as active/passive, the Synchronize user sessions and Synchronize last access time for user sessions options are automatically checked.
- If you select both the both Synchronize log messages and Synchronize user sessions check boxes, everything is replicated on the cluster nodes, including networking information. Even though networking information, including syslog and SNMP settings, can be configured per node or per cluster, all of the networking information is synchronized between nodes when these two options are set.
- If your cluster node configurations have diverged due to changes made to one node while another is disabled or unavailable, the Secure Access Service manages the remerging of the configurations automatically, for up to 16 updates. Beyond the maximum number of allowable updates, you may need to intervene and remerge the configurations manually. In some instances, the Secure Access Service may be unable to remerge the configurations if there is not enough overlapping configuration information between two nodes to manage the internode communication.

For example, given a two-node cluster in which the two nodes are partitioned from each other because of a network outage, if the internal network IP address of one of the nodes gets changed in one of the partitions, the two partitions are unable to rejoin, even when the network is repaired. In such a case, you must manually remerge the configurations.

**Related Documentation**

- [Deploying Two Nodes in an Active/Passive Cluster on page 985](#)
- [Deploying Two or More Units in an Active/Active Cluster on page 986](#)
- [Specifying Active/Passive, Active/Active, and Other Cluster Settings on page 990](#)

## Specifying Active/Passive, Active/Active, and Other Cluster Settings

Use the Properties page to change the name of a cluster, specify in which configuration to run a cluster (active/passive or active/active), specify synchronization and network healthcheck settings, or delete a cluster.

To modify cluster properties:

1. From the admin console of an active cluster member, select the **System > Clustering > Cluster Properties** page.
2. Edit the name of the cluster in the **Cluster Name** field to change the cluster's name (optional).
3. Under Configuration Settings, select one of the following options:
  - **Active/Passive** to run a cluster pair in active/passive mode. Then, specify an internal VIP (virtual IP address) and an external VIP if the external port is enabled.



**NOTE:** To run a two-unit cluster in active/passive mode, the Secure Access Services must reside on the same subnet.

- **Active/Active** runs a cluster of two or more nodes in active/active mode using an external load balancer.



**NOTE:** To change a two-unit active/passive cluster to an active/active cluster with more than two nodes, first change the configuration of the two-unit cluster to active/active and then add the additional nodes.

4. Under Synchronization Settings, specify one or more types of data to synchronize using the following options:
  - **Synchronize log messages**—Propagates all log messages among all of the Secure Access Services in the cluster.
  - **Synchronize user sessions**—Synchronizes all user session information (instances of access to intranet services, for example) among all Secure Access Services in the cluster.
  - **Synchronize last access time for user sessions**—Propagates the latest user access information across the cluster.



---

**NOTE:**

- If you select both Synchronize log messages and Synchronize user sessions check boxes, everything is replicated on the cluster nodes, including networking information. Even though networking information, including syslog and SNMP settings, can be configured per node or per cluster, all of the networking information is synchronized between nodes when these two options are set.
- If you are using a load balancer in conjunction with the Secure Access Service, we recommend you clear the Synchronize last access time for user sessions check box.
- Clearing the Synchronize last access time for user sessions check box to disable it off can greatly improve cluster synchronization performance, disabling this option while users are connected to the Secure Access Service can result in client-side warnings informing the user that the session is about to expire. These warnings are automatically generated because of time-stamp mismatches and the user sessions do not actually disconnect.

- 
5. Under Network Healthcheck Settings, specify the number of ARP ping failures allowed before the Secure Access Service's internal interface is disabled and whether or not to disable the Secure Access Service's external interface if the internal interface fails.
  6. Select the **Advanced Settings** check box to specify the timeouts for the underlying cluster system. Do not change any values under this setting unless instructed to do so by Juniper Networks Technical Support.
  7. Click **Save Changes**.

**Related Documentation**

- [Task Summary: Deploying a Cluster on page 981](#)
- [Deploying Two Nodes in an Active/Passive Cluster on page 985](#)
- [Deploying Two or More Units in an Active/Active Cluster on page 986](#)

---

## Adding Multiple Cluster Nodes

To add multiple nodes to a cluster:

1. Select **System > Clustering > Cluster Status**.
2. Click **Add Members**.
3. Enter the node name and internal IP address.
4. Modify or add the default internal netmask and internal gateway addresses, if necessary.
5. Click **Add**.

6. Repeat the process until you have added all of the nodes.
7. Click **Save Changes** to save the node configurations.

The Secure Access Service automatically enables the added clusters, even if they are unreachable.

**Related  
Documentation**

- [Task Summary: Deploying a Cluster on page 981](#)
- [Deploying Two Nodes in an Active/Passive Cluster on page 985](#)
- [Deploying Two or More Units in an Active/Active Cluster on page 986](#)

## General Cluster Maintenance

---

### Managing Network Settings for Cluster Nodes

To modify the network settings for a cluster or each individual node in a cluster, click System > Network. You can make your changes on the Network Settings pages. After you create a cluster, these pages provide a drop-down list from which you can select the entire cluster or a specific node to modify. When you save changes on a Network page, the settings are saved for the specified cluster or cluster node. If you change network settings for an entire cluster, they propagate to every node in the cluster.

You can access a node-specific Network page by clicking System > Clustering > Cluster Status on the node's name in the Member Name column.

### Upgrading Clustered Nodes

The Secure Access Service offers the ability to easily upgrade every node in a cluster. You simply install a newer service package on one node and, once the installation completes and the node reboots, the node pushes the service package to all nodes in the cluster.

### Upgrading the Cluster Service Package

Install a newer service package on one cluster node only. When the installation process completes and the cluster node reboots, it instructs the other nodes to upgrade.

**Related  
Documentation**

- [Synchronizing the Cluster State on page 988](#)
- [Adding Multiple Cluster Nodes on page 992](#)

## Migrating Cluster Configurations to a Replacement Cluster

To migrate system and user configurations from a Secure Access Service cluster (C1) to a replacement cluster (C2) using different Secure Access Service devices:

1. Export the system, user and IVS configuration from C1's primary node (PN1).

Note the following information:

- Cluster name
  - Cluster password
  - Name of the node where the export was done (PN1)
  - Internal IP address of PN1
  - Internal network mask of PN1
  - Internal network gateway of PN1
  - Name of all other nodes in the C1 cluster, including their internal network IP address, network masks and gateways
2. Shut down all Secure Access Service devices in cluster C1.
  3. Power on one of the new Secure Access Services (must be running software release 6.1R1 or later) that is part of cluster C2 and is on the same network to which PN1 was attached. This Secure Access Service device is called PN2 for the remainder of these steps.
  4. When prompted, configure the internal network settings of PN2 to the same internal network settings of PN1 as noted in Step 2.
  5. Install the new primary license on PN2.
  6. From the admin GUI on PN2, select **System > Clustering > Create Cluster**. Create the cluster C2 using the same cluster name and cluster password that were in use at cluster C1. Node PN2 must also be assigned the same node name as PN1 (see Step 2).
  7. Open the cluster status page and add the remaining nodes to the cluster configuration. Nodes being added must be assigned the same names that existed in original cluster C1. The internal network settings of the newly added nodes must also match the corresponding settings in the original cluster C1.



**NOTE:** Do not join the newly added nodes to cluster C2 yet.

8. Import the data exported from PN1 (see Step 1) into PN2.

When importing the system configuration, select the option **Import everything (except Device Certificate(s))**.

9. Power on the remaining new Secure Access Services devices assigned to cluster C2. Configure the bare minimal internal network settings needed to bring up the machine. The network settings must match what has already been configured on node PN2.



**NOTE:** Do not do make any other configuration changes on these machines as they will be lost when these machines join the cluster. Do not add licenses on these machines yet.

10. Join the Secure Access Services in Step 9 to cluster C2 and wait for the cluster status to stabilize.
11. Install the CL licenses on the newly joined nodes.

**Related Documentation**

- [Importing and Exporting Secure Access Service Configuration Files on page 896](#)

## Changing the IP Address of a Cluster Node

Changing the IP address of a cluster while it belongs to a cluster is not supported. In order to change the IP address, you must first remove it from the cluster, update the IP address and then add it back.



**NOTE:** If you attempt to change the IP address of a node while it belongs to a cluster, you may experience unpredictable results.

For example:

1. Select **System > Clustering > Cluster status**.
2. Select the check box next to the name of the node whose IP address you want to change.
3. Click **Remove**.
4. After the node is removed, sign in to that node, change its IP address and click **Save Changes**.
5. In the main node, add the changed node to the cluster configs.
6. Log in to the changed node and rejoin the cluster.

The following is an example for changing both node IP addresses in an active/passive cluster:

1. Select **System > Clustering > Cluster status**.
2. Click **Delete Cluster**.
3. Change the IP address of each node.
4. Log in to the main node and re-create the cluster, changing from active/active to active/passive and defining the internal and/or external VIP addresses.

5. Add the other node to the cluster configs.
6. Log in to the passive node and join it to the cluster.

**Related Documentation**

- [Deploying Two Nodes in an Active/Passive Cluster on page 985](#)
- [General Cluster Maintenance on page 993](#)
- [Deleting a Cluster on page 996](#)

## Deleting a Cluster

---

If you delete a cluster, all of the nodes begin running as stand alone Secure Access Service devices.

To delete a cluster:

1. From the admin console of an active cluster member, select the **System > Clustering > Cluster Status** page.
2. Select the checkbox next to each cluster node you want to delete.
3. Click the **Remove Cluster** button.
4. When prompted, click **Remove**.

**Related Documentation**

- [General Cluster Maintenance on page 993](#)

## Restarting or Rebooting Clustered Nodes

---

When you create a cluster of two or more Secure Access Service devices, the clustered Secure Access Services act as a logical entity. As such, when you restart or reboot one of the clustered Secure Access Services using either the serial console or the admin console, all Secure Access Service devices in the cluster restart or reboot.

**Related Documentation**

- [Serial Console Procedures on page 1002](#)

## Configuring the External VIP for An Active/Passive Cluster

---

To add an external VIP to an existing A/P cluster:

1. Create an A/P cluster with only the internal port configured.
2. Select **System > Clustering > Clustering Properties** and add the internal VIP.
3. Select **System > Network > External Port**.
4. From the Settings for menu, select “entire cluster”.
5. Add the Netmask and Default Gateway but leave the external port disabled.



6. For each node, select **System > Network > External Port** and configure the external port IP address but leave the external port disabled.
7. Add the external cluster VIP.
8. Select **System > Network > External Port**, select “entire cluster” from the Settings for menu and enable the external port.

**Related Documentation**

- [Specifying Active/Passive, Active/Active, and Other Cluster Settings on page 990](#)

## Admin Console Procedures

Table 60 on page 997 describes the information displayed on the Status tab and the various management tasks you can perform, including disabling, enabling, and removing the Secure Access Service node from a cluster.

**Table 60: Cluster Status Page Information**

User Interface Element	Description
Status Information labels	Screen displays the cluster name, type, configuration, internal VIP, and external VIP for an active/passive cluster.
Add Members button	Click this button to specify the Secure Access Service that will join the cluster. You must perform this step for Secure Access Service you intend to add to the cluster. By clicking this button, you can add multiple nodes at the same time.
Enable button	Click this button to add a node that was previously disabled. When you add a node, all state information is synchronized on the node.
Disable button	Click this button to disable a node within the cluster. The node retains awareness of the cluster, but does not participate in state synchronizations or receive user requests unless members sign in to the node, directly.
Remove button	Click this button to remove the selected node or nodes from the cluster. Once removed, the node runs in stand-alone mode.
Fail-Over VIP button	Click this button to fail-over the VIP to the other node in the active/passive cluster. Only available if cluster is configured as active/passive.
Member Name column	Lists all nodes belonging to the cluster. You can click on a node's name to modify its name and network settings.
Internal Address column	Shows the internal IP address of the cluster member using Classless Inter Domain Routing (CIDR) notation.

Table 60: Cluster Status Page Information (*continued*)

User Interface Element	Description
External Address column	Shows the external IP address of the cluster member using CIDR notation. Note that this column only shows the external IP address of the cluster leader unless you specify a different address for the node on its individual network settings page, which is accessible by clicking on its name in the <b>Member Name</b> column. If you change the external IP address on the <b>Network &gt; Network Settings</b> page, the change affects all cluster nodes.
<b>Status</b> column	Shows the current state of the node: <ul style="list-style-type: none"> <li>• <b>Green light/enabled</b>—The node is handling user requests and participating in cluster synchronization.</li> <li>• <b>Yellow light/transitioning</b>—The node is joining cluster.</li> <li>• <b>Red light/disabled</b>—The node is not handling user requests or participating in cluster synchronization.</li> <li>• <b>Red light/enabled, unreachable</b>—The node is enabled, but due to a network issue, it cannot be reached.</li> </ul> <p><b>Note:</b> A node's state is considered "stand-alone" when it is deployed outside of a cluster or after being removed from a cluster.</p>
<b>Notes</b> column	Shows the status of the node's connection to the cluster: <ul style="list-style-type: none"> <li>• <b>OK</b>—The node is actively participating in the cluster.</li> <li>• <b>Transitioning</b>—The node is switching from the stand-alone state to the enabled state.</li> <li>• <b>Unreachable</b>—The node is not aware of the cluster. A cluster member may be "unreachable" even when it's online and can be pinged. Possible reasons include: its password is incorrect, it doesn't know about all cluster nodes, it's configured with a different group communication mode, it's running a different service package version, or the machine is turned off.</li> </ul>
<b>Sync Rank</b> column	Specifies the synchronization order for nodes when rejoining a cluster. Accepts sync ranks from 0 (lowest rank) to 255 (highest rank). The highest rank takes precedence. Where two nodes have identical sync ranks, the alpha-numeric rank of the member name is used to determine precedence. <p>Note:</p>
<b>Update</b> button	Updates the sync rank after you change the precedence of the nodes in the <b>Sync Rank</b> column.

**Related Documentation**

- [Task Summary: Deploying a Cluster on page 981](#)
- [General Cluster Maintenance on page 993](#)
- [Monitoring Clusters on page 999](#)

## Monitoring Clusters

You can monitor clusters using the standard logging tools provided by the Secure Access Service. In particular, you can use several cluster-specific SNMP traps to monitor events that occur on your cluster nodes, such as:

- External interface down
- Internal interface down
- Disabled node
- Changed virtual IP (VIP)
- Deleted cluster node (cluster stop)



**NOTE:** Generally, it is desirable to configure your SNMP traps on a cluster-wide basis, so that any given cluster node can send its generated traps to the right target. Setting up cluster-wide configuration for the traps is particularly important when you also use a load balancer, because you may not know which node is responsible for a specific operation. In that case, the load balancer may independently determine which cluster node can manage an administrative session.

You can use SNMP traps that are included in the Juniper Networks Standard MIB to monitor these events. These traps include:

- **iveNetExternalInterfaceDownTrap**—Supplies type of event that brought down the external interface.
- **iveNetInternalInterfaceDownTrap**—Supplies type of event that brought down the internal interface.
- **iveClusterDisableNodeTrap**—Supplies the cluster name on which nodes have been disabled, along with a space separated list of disabled node names.
- **iveClusterChangedVIPTrap**—Supplies the type of the VIP, whether external or internal, and its value before and after the change.
- **iveClusterDelete**—Supplies the name of the cluster node on which the cluster delete event was initiated.

These traps are always enabled and available in the MIB. You cannot disable the traps.

### Related Documentation

- [Defining and Initializing a Cluster on page 982](#)
- [Synchronizing the Cluster State on page 988](#)
- [Troubleshooting Clusters on page 1000](#)

## Troubleshooting Clusters

When you have problems with cluster communication, you may be directed by your Juniper Networks Support representative to use the cluster node troubleshooting tools.

To use the cluster node troubleshooting tools:

From the admin console, select **Maintenance > Troubleshooting > Monitoring > Node Monitor**, in **Maintenance > Troubleshooting > Clustering Network Connectivity**, and in **Maintenance > Troubleshooting > Clustering Group Communication**.

You can use a built-in feature on the clustering Status page to identify the status of each cluster node. Pause the mouse pointer over the Status light icon and the system displays a tool tip containing a hexadecimal number. The hexadecimal number is a snapshot of the status of the Secure Access Service. It is a bit mask indicating a number of states as shown in [Table 61 on page 1000](#).

**Table 61: Cluster Status**

Value	Meaning
0x000001	Secure Access Service is in standalone mode.
0x000002	Secure Access Service is in cluster disabled state.
0x000004	Secure Access Service is in cluster enabled state.
0x000008	Unable to communicate (because it is offline, has wrong password, has different cluster definition, different version, or a related problem).
0x00002000	The node owns the VIPs (on) or not (off).
0x000100	Secure Access Service is syncing state from another Secure Access Service (initial syncing phase).
0x000200	Secure Access Service is transitioning from one state to another.
0x00020000	The group communication subsystems at the local and remote nodes are disconnected from each other.
0x00040000	Management interface (mgt0) appears disconnected.
0x00080000	Management gateway is unreachable for ARP ping.
0x000800	Secure Access Service int0 appears disconnected (no carrier).
0x001000	This node is configured to be a cluster member.
0x002000	Secure Access Service is syncing its state to another Secure Access Service that is joining.

Table 61: Cluster Status (*continued*)

Value	Meaning
0x004000	Initial Synchronization as master or slave is taking place.
0x008000	This Secure Access Service is the leader of the cluster.
0x010000	The group communication subsystem is functional.
0x020000	The gateway on int0 is unreachable for ARP pings (see log file).
0x040000	The gateway on int1 is unreachable for ARP pings (see log file).
0x080000	Leader election is taking place.
0x100000	Server life cycle process (dsmon) is busy.
0x200000	System performs post state synchronization activities.
0x30004	<ul style="list-style-type: none"> <li>The group communication subsystem is functional.</li> <li>The gateway on int0 is unreachable for ARP pings (see log file).</li> <li>Secure Access Service is in cluster enabled state.</li> </ul>
0x80000000	Cluster keystore or security world has not been associated with the FIPS card.

Each code, as you see it in the Secure Access Service, may relate specifically to one state. However, each code may represent a combination of states, and so the actual code does not appear in [Table 61 on page 1000](#). Instead, the code you see in the Secure Access Service is the sum of several of the hexadecimal numbers shown in [Table 61 on page 1000](#). You will need to factor out the codes, as in the following example:

- 0x38004—The right-most digit (4) in this hexadecimal number corresponds to:
  - 0x000004 The Secure Access Service is in cluster enabled state.
- 0x038004—The digit in the fourth position from the right (8) corresponds to:
  - 0x008000 This Secure Access Service is the leader of the cluster.
- 0x38004—The left-most digit (3) in this hexadecimal number does not exist in the table, which indicates that it corresponds to the sum of two other digits, in this case, 1 and 2, as shown in the following codes:
  - 0x020000—The gateway on int0 is unreachable for ARP pings (see log file).
  - 0x010000—The group communication subsystem is functional.

### “Management IP Address Differs From the Management IP Address” Error Message

If you receive the following error when joining a standalone SA6000/SA6500 node to a cluster even though the management port is configured and enabled:

Management IP address (x.x.x.x) for the local system differs from the Management IP address (not entered) configured for this system in the remote system.

then perform the following steps to add the node:

1. From the admin console of the primary node, select System > Network > Management Port.
2. Select the node to add from the drop down list next to the “Setting for” label.
3. Enable the management port and enter the IP address, netmask and default gateway for the joining node.
4. Click Save Changes.
5. From the admin console of the joining node, join the cluster again.

**Related Documentation**

- [Monitoring Clusters on page 999](#)

---

## Serial Console Procedures

---

You can add the Secure Access Service to a cluster through its serial console, except when running a FIPS environment, which requires that you add each Secure Access Service through its admin console.

If you are adding a factory-set Secure Access Service to a cluster, we recommend that you use the serial console, which enables you to join an existing cluster during the initialization process by entering minimal information. When the Secure Access Service joins a cluster, it receives the cluster state settings, which overwrites all settings on a machine with an existing configuration and provides new machines with the required preliminary information.

You can also use the Secure Access Service' serial console to disable the Secure Access Service within a cluster. If the Secure Access Service is in synchronization state, you cannot access its admin console. Therefore, if you need to upgrade or reboot the Secure Access Service, for example, you need to first disable the Secure Access Service from a cluster through its serial console.

**Related Documentation**

- [Joining the Secure Access Service to a Cluster Through Its Serial Console on page 1002](#)
- [Disabling a Clustered Secure Access Service Using Its Serial Console on page 1004](#)

---

## Joining the Secure Access Service to a Cluster Through Its Serial Console

---

Before a configured or factory-set Secure Access Service can join a cluster, you need to make its identity known to the cluster.

**NOTE:**

- If you want to add the Secure Access Service currently running as a stand-alone machine to a cluster through its admin console, it must be running the same or a more recent version service package on the same hardware platform as the other members.
- If you add the Secure Access Service running a previous version service package to a cluster, the Secure Access Service automatically detects the mismatch, gets the newer package from the cluster, and joins the cluster.

To add the Secure Access Service to a cluster through its serial console:

1. From the admin console of an existing cluster member, select the **System > Clustering > Cluster Status** tab and specify the Secure Access Service you want to add to the cluster.
2. Connect to the serial console of the machine you want to add to the cluster.
3. Reboot the machine and watch its serial console. After the system software starts, a message displays stating that the machine is about to boot as a standalone Secure Access Service and to press the Tab key for clustering options. Press the Tab key as soon as you see this option.



**NOTE:** The interval to press the Tab key is five seconds. If the machine begins to boot in stand alone mode, wait for it to finish and then reboot again.

4. Enter the number instructing the Secure Access Service to join an existing cluster.
5. Enter the requested information, including:
  - The internal IP address of an active member in the cluster
  - The cluster password, which is the password you entered when defining the cluster
  - The name of the machine you wish to add
  - The internal IP address of the machine you wish to add
  - The netmask of the machine you wish to add
  - The gateway of the machine you wish to add

The active cluster member verifies the cluster password and that the new machine's name and IP address match what you specified in the admin console by clicking **System > Clustering > Cluster Status > Add Cluster Member**. If the credentials are valid, the active member copies all of its state data to the new cluster member, including license key, certificate, user, and system data.

6. Enter the number instructing the Secure Access Service to continue the join cluster operation. When you see the message confirming that the machine has joined the cluster, click **System > Clustering > Cluster Status** tab in the admin console of any

active cluster member to confirm that the new member's Status is green, indicating that the Secure Access Service is an enabled node of the cluster.

- Related Documentation**
- [Defining and Initializing a Cluster on page 982](#)
  - [Serial Console Procedures on page 1002](#)
  - [Disabling a Clustered Secure Access Service Using Its Serial Console on page 1004](#)

## Disabling a Clustered Secure Access Service Using Its Serial Console

---

To disable the Secure Access Service within a cluster using its serial console:

1. Connect to the serial console of the machine you want to disable within the cluster.
2. Enter the number corresponding to the Secure Access Service' System Operations option.
3. Enter the number corresponding to the Disable Node option.
4. Enter **y** when the serial console prompts if you are sure you want to disable the node.
5. Verify that the Secure Access Service has been disabled within the cluster by selecting **System > Clustering > Status** in the admin console of any active cluster member to confirm that the disabled member's Status is red.

- Related Documentation**
- [Serial Console Procedures on page 1002](#)



# Delegating Administrator Roles

- [About Delegating Administrator Roles on page 1005](#)
- [Creating and Configuring Administrator Roles on page 1006](#)
- [Specifying Management Tasks to Delegate on page 1007](#)

## About Delegating Administrator Roles

---

The Secure Access Service access management system enables you to delegate various Secure Access Service management tasks to different administrators through system administrator roles and security administrator roles. System and security administrator roles are defined entities that specify Secure Access Service management functions and session properties for administrators who are mapped to those roles. You can customize an administrator role by selecting the Secure Access Service feature sets, user roles, authentication realms, resource policies, and resource profiles that members of the administrator role are allowed to view and manage. Note that system administrators may only manage user roles, realms, and resource policies; only security administrators can manage administrator components.

For example, you can create a system administrator role called “Help Desk Administrators” and assign users to this role who are responsible for fielding tier 1 support calls, such as helping users understand why they cannot access a Web application or Secure Access Service page. In order to help with troubleshooting, you may configure settings for the “Help Desk Administrators” role as follows:

- Allow the help desk administrators Write access to the System > Log/Monitoring page so they can view and filter the Secure Access Service logs, tracking down critical events in individual users’ session histories, as well as the Maintenance > Troubleshooting page so they can trace problems on individual users’ systems.
- Allow the help desk administrators Read access to the Users > User Roles pages so they can understand which bookmarks, shares, and applications are available to individual users’ roles, as well as the Resource Policy or Resource Profile pages so they can view the policies that may be denying individual users access to their bookmarks, shares, and applications.
- Deny the help desk administrators any access to the remaining System pages and Maintenance pages, which are primarily used for configuring system-wide settings—such as installing licenses and service packages—not for troubleshooting individual users’ problems.



**NOTE:** In addition to any delegated administrator roles that you may create, the Secure Access Service also includes two basic types of administrators: super administrators (.Administrators role), who can perform any administration task through the admin console and read-only administrators (.Read-only Administrators role), who can view—but not change—the entire Secure Access Service configuration through the admin console.

You can also create a security administrator role called “Help Desk Manager” and assign users to this role who are responsible for managing the Help Desk Administrators. You might configure settings for the “Help Desk Manager” role to allow the Help Desk Manager to create and delete administrator roles on his own. The Help Desk Manager might create administrator roles that segment responsibilities by functional areas of the Secure Access Service. For example, one administrator role might be responsible for all log monitoring issues. Another might be responsible for all Network Connect problems.

The delegated administration feature is not available on the SA 700 appliance. Note, however, that all Secure Access Service devices allow members of the .Administrators role to configure general role settings, access management options, and session options for the .Administrators and .Read-Only Administrators roles.



**NOTE:** On certain pages, such as the role mapping page, the delegated administrator can view the role names even though the administrator does not have read/write access. However, the delegated administrator can not view the details of that role.

**Related  
Documentation**

- [Creating and Configuring Administrator Roles on page 1006](#)
- [Specifying Management Tasks to Delegate on page 1007](#)

## Creating and Configuring Administrator Roles

You can use the Administrators > Admin Roles pages to set default session and user interface options for delegated administrator roles.

To create individual administrator accounts, you must add the users through the appropriate authentication server (not the role). For example, to create an individual administrator account, you may use settings in the Authentication > Auth. Servers > Administrators > Users page of the admin console. For detailed instructions on how to create users on the Administrators server and other local authentication servers. For instructions on how to create users on third-party servers, see the documentation that comes with that product.

To create an administrator role:

1. In the admin console, choose **Administrators > Admin Roles**.
2. Do one of the following:

- Click **New Role** to create a new administrator role with the default settings.
  - Select the checkbox next to an existing administrator role and click **Duplicate** to copy the role and its custom permissions. Note that you cannot duplicate the system default roles (.Administrators and .Read-Only Administrators).
3. Enter a name (required) and description (optional) for the new role and click **Save Changes**.
  4. Modify restrictions, session options, and UI options according to your requirements.



**NOTE:** If you select one of the Secure Access Service's default administrator roles (.Administrators or .Read-Only Administrators), you can only modify settings in the General tab (since the default Secure Access Service administrators roles always have access to the functions defined through the System, Users, Administrators, and Resource Policies tabs).

You cannot delete the .Administrators and .Read Only Administrators roles since they are default roles defined on the Secure Access Service.

#### Related Documentation

- [Specifying Management Tasks to Delegate on page 1007](#)
- [Role Restrictions on page 110](#)
- [Specifying Role Session Options on page 111](#)
- [Customizing the Secure Access Service Welcome Page on page 115](#)

## Specifying Management Tasks to Delegate

This topic contains information about delegating management tasks to various delegated administrator roles.

### Delegating System Management Tasks

Use the **Administrators > Admin Roles > Select Role > System** tab to delegate various Secure Access Service system management tasks to different administrator roles. When delegating privileges, note that:

- The Secure Access Service allows all administrators read-access (at minimum) to the admin console home page (System > Status > Overview), regardless of the privilege level you choose.
- The Secure Access Service does not allow delegated administrators write-access to pages where they can change their own privileges. Only those administrator roles that come with the system (.Administrators and .Read-Only Administrators) may access these pages:
  - Maintenance > Import/Export (Within this page,.Read-Only Administrators can export settings, but cannot import them.)
  - Maintenance > Push Config

- Maintenance > Archiving > Local Backups
- Delegation access to the Meeting Schedule page is controlled through the Meetings option on the Administrators > Admin Roles > Select Role > Resource Policies page.

## Delegating User and Role Management

Use the **Administrators > Admin Roles > Select Role > Users > Roles** sub-tab to specify which user roles the administrator role can manage. When delegating role management privileges, note that:

- Delegated administrators can only manage user roles.
- Delegated administrators cannot create new user roles, copy existing roles, or delete existing roles.
- If you allow the delegated administrator to read or write to any feature within a user role, the Secure Access Service also grants the delegated administrator read access to the Users > User Roles > Select Role > General > Overview page for that role.
- If you grant a delegated administrator write access to a resource policy through the Administrators > Admin Roles > Select Administrator Role > Resource Policies page, he may create a resource policy that applies to any user role, even if you do not grant him read access to the role.

## Delegating User Realm Management

Use the **Administrators > Admin Roles > Select Role > Users > Authentication Realms** tab to specify which user authentication realms the administrator role can manage. When delegating realm management privileges, note that:

- System administrators can only manage user realms.
- System administrators cannot create new user realms, copy existing realms, or delete existing realms.
- If you allow the system administrator to read or write to any user realm page, the Secure Access Service also grants the system administrator read-access to the Users > User Realms > Select Realm > General page for that role.

## Delegating Administrative Management

Use the **Administrators > Admin Roles > Select Roles > Administrators** tab to specify which system administrator roles and realms the security administrator role can manage. When delegating security administrative privileges, note that:

- The security administrator role provides control over all administrative roles and realms.
- You can give a security administrator control exclusively over administrator roles, over administrator realms, or over both.
- You can restrict or grant the security administrator the permission to add and delete administrator roles and administrator realms.

## Delegating Resource Policy Management

Use the **Administrators > Admin Roles > Resource Policies** tab to specify which user resource policies the administrator role can manage. When delegating resource policy management privileges, note that delegated system administrators cannot modify the following characteristics of resource policies:

- The resource itself (that is, the IP address or host name).
- The order in which the Secure Access Service evaluates the resource policies.

## Delegating Resource Profile Management

Use the **Administrators > Admin Roles > Resource Profiles** tab to specify which user resource profiles the administrator role can manage. When delegating resource profile management privileges, note that delegated system administrators cannot modify the following characteristics of resource profiles:

- The resource itself (that is, the IP address or host name)
- The order in which the Secure Access Service evaluates the resource policies.

## Delegating Access to IVS Systems

If you are running an IVS license, you can also delegate administrative access and responsibilities to specific IVS systems. You can delegate read/write access or read-only access to all IVS systems, or to selected IVS systems..

### Related Documentation

- [About Delegating Administrator Roles on page 1005](#)



## CHAPTER 37

# Instant Virtual System

- [Instant Virtual System \(IVS\) Overview on page 1012](#)
- [Deploying an IVS on page 1014](#)
- [Virtualized Secure Access Service Architecture on page 1016](#)
- [Signing In to the Root System or the IVS on page 1017](#)
- [Navigating to the IVS on page 1020](#)
- [IVS Configuration Worksheet on page 1021](#)
- [Administering the Root System on page 1023](#)
- [Configuring the Root Administrator on page 1023](#)
- [IVS Provisioning Process Overview on page 1025](#)
- [Configuring Sign-In Ports for IVS on page 1026](#)
- [Virtual Local Area Network \(VLAN\) on Subscriber IVS on page 1028](#)
- [Configuring VLANs on the Virtualized Secure Access Service on page 1029](#)
- [Adding Static Routes to the VLAN Route Table on page 1030](#)
- [Deleting a VLAN on page 1031](#)
- [Loading the Certificates Server on page 1032](#)
- [Creating a Virtual System \(IVS Profile\) on page 1032](#)
- [IVS Initial Config Via Copy from the Root System or Another IVS on page 1034](#)
- [Signing In Directly to the IVS as an IVS Administrator on page 1036](#)
- [About Role-Based Source IP Aliasing on page 1037](#)
- [Associating Roles with Source IP Addresses in an IVS on page 1037](#)
- [Configuring Policy Routing Rules on the IVS on page 1038](#)
- [Clustering a Virtualized Secure Access Service on page 1040](#)
- [Accessing a DNS Server on the MSP Network on page 1041](#)
- [Accessing a DNS Server on a Subscriber Company Intranet on page 1042](#)
- [Configuring VPN Tunneling for Use on a Virtualized Secure Access Service on page 1043](#)
- [Configuring a Centralized DHCP Server on page 1046](#)
- [About Authentication Servers on page 1047](#)
- [Delegating Administrative Access to IVS Systems on page 1049](#)

- [Accessing Standalone Installers on an IVS System on page 1050](#)
- [Exporting and Importing IVS Configuration Files on page 1050](#)
- [Using XML Import and XML Export on IVS Systems on page 1052](#)
- [Monitoring Subscribers on page 1053](#)
- [Troubleshooting VLANs on page 1053](#)
- [IVS Use Case: Policy Routing Rules Resolution on page 1055](#)
- [Use Case: Configuring a Global Authentication Server for Multiple Subscribers on page 1060](#)
- [Use Case: Configuring a DNS/WINS Server IP Address per Subscriber on page 1061](#)
- [Use Case: Configuring Access to Web Applications and Web Browsing for Each Subscriber on page 1061](#)
- [Use Case: Configuring File Browsing Access for Each Subscriber on page 1062](#)
- [Use Case: Setting Up Multiple Subnet IP Addresses for a Subscriber's End-Users on page 1063](#)
- [Use Case: Configuring Multiple IVS Systems to Allow Access to Shared Server on page 1064](#)

## Instant Virtual System (IVS) Overview

---

The Instant Virtual System (IVS) gives managed service providers (MSPs) the opportunity to offer cost-effective secure remote access, disaster recovery and managed extranet services to small and medium sized companies. To meet this opportunity, MSPs can deliver managed security solutions from equipment that is located on the subscriber company's premises (Customer Premises Edge router-based) or within the MSP network (Carrier Edge router-based or network-based). Network-based managed security solutions centralize the security gateway equipment in the MSP network. A virtualized Secure Access Service allows the MSP to provide managed, network-based SSL VPN services to multiple customers from the same equipment. The basic business model might work something like this:

- The MSP manages the SSL VPN equipment at the MSP site.
- Small and medium-sized companies subscribe to monthly services from the MSP.
- The MSP is responsible for the management of the equipment, but delegates portal administration to an IVS administrator designated by each subscriber company.
- The virtual system supports and enforces an architectural and administrative separation between subscriber companies, providing a completely secure and individualized view for each subscriber.

This system provides a number of benefits to service providers:



- Expand market share—The ability to provide secure SSL VPN capabilities to many subscriber companies from one Secure Access Service offers the MSP economies of scale and the opportunity to expand market share with services targeting small and medium sized businesses.
- Simplify administration—Each subscriber administrator can manage their company's IVS instance with no visibility into another subscriber company's administrative interface. The MSP root administrator can manage all hosted companies and can easily monitor or configure hosted company systems.
- Enhance subscriber security—Each subscriber company maintains complete separation from other subscriber companies. As far as the subscriber administrator or subscriber users are concerned, they are operating on a completely independent and protected SSL VPN system.
- Optimize traffic management—Traffic from end-users or corporate intranet servers stays within each company's VLAN. Subscriber end-users never see services located on another subscriber's intranet.

The standalone client installers are not accessible directly from the admin UI of an IVS. As a workaround, the root administrator can make the following link available to IVS administrators if the IVS administrators need to download standalone installers:

<https://myive/dana-admin/sysinfo/installers.cgi>

where myive is the hostname of your Secure Access Service.



**NOTE:** IVS does not support Junos Pulse for Windows.

You must have an IVS license to create IVS systems. (Note that IVS licenses are not available for SA 700 or SA 2000 appliances.)

You must have both an IVS license and a Network Connect license to provide centralized DHCP support to your subscribers.

Suppose your Secure Access Service has a VLAN license but no IVS license. When you create VLANs, they are available for the entire system. However, when an IVS license is applied to the Secure Access Service, the VLANs are not applied to the Root IVS. They must manually be assigned to the Root IVS or other IVSes that you create.



**NOTE:** IVS is not supported on the MAG Series Junos Pulse Gateways.

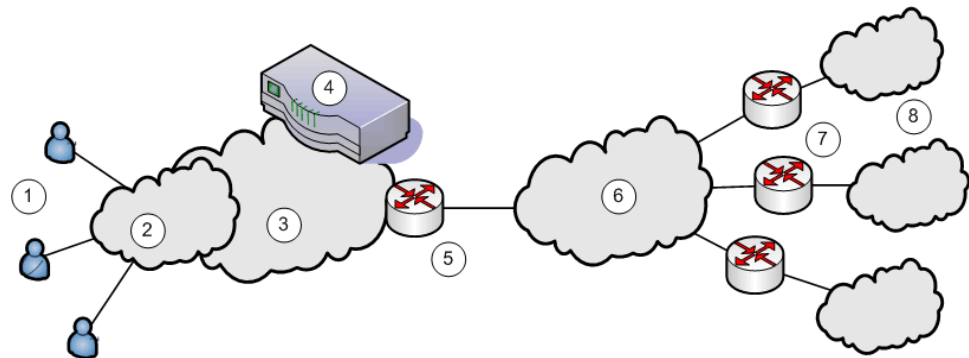
#### Related Documentation

- [Deploying an IVS on page 1014](#)
- [IVS Provisioning Process Overview on page 1025](#)
- [Creating a Virtual System \(IVS Profile\) on page 1032](#)
- [IVS Use Case: Policy Routing Rules Resolution on page 1055](#)

## Deploying an IVS

For each subscriber company, the virtualized Secure Access Service provides a secure portal for the company's end-users (mobile employees, customers, or partners) to access its internal resources. Authentication servers that reside either on the subscriber's premises or in the MSP network, authenticate end-users who sign in to the IVS. Once authenticated, end-users establish secure sessions through the IVS to their respective company's back-end servers.

**Figure 74: MSP Deployment Scenario**



The following numbered list items correspond to the labeled objects in the above figure.

1. End-users sign in to different subscriber company intranets on specified IP addresses.
2. End-users sign-in over an Internet connection using a standard SSL-enabled Web browser.
3. All traffic is directed into the Managed Service Provider's (MSP) network. The MSP is the customer who holds the license to the virtualized Secure Access Service hardware and software.
4. All traffic is directed to the virtualized Secure Access Service. Each message is evaluated based on its sign-in IP address and, by the virtualized Secure Access Service, is assigned a VLAN tag containing a VLAN ID that corresponds to a subscriber company. The Secure Access Service supports up to 240 IVS systems, each one representing a single subscriber company Secure Access Service. The subscriber is any company that subscribes to hosted SSL VPN services from the MSP.

The number of VLANs supported depends on the number of IVS systems. The number of IVS systems plus the number of VLANs must be less than or equal to 240.

Although you can create up to 240 IVS systems, it is strongly recommended that you do not create and use more than 16 IVS systems without first consulting the Performance Metrics and Testing application note. Contact Juniper Networks Technical Support for more information on this application note.

5. The MSP carrier-edge (CE) router or other Layer 2 device acts as a VLAN termination point, and routes traffic over a secure tunnel to a customer premises edge (CPE) router. Based on the VLAN ID, the router directs the traffic to the appropriate subscriber intranet. During this part of the process, the CE router removes the VLAN tag containing

the VLAN ID, as once the message is correctly destined for the appropriate intranet, the ID and tag are no longer needed. The term subscriber intranet is interchangeable with the term company intranet.

6. The CE router routes messages over the service provider backbone to the appropriate customers' premises edge routers through encrypted tunnels, such as IPsec, GRE, PPP, and MPLS tunnels. Untagged traffic is sent over these tunnels to the customer intranet.
7. The CPE routers within the customer intranet on the customer premises can act as a VLAN termination point and routes traffic from the secure tunnel connected to the CE Router, to the customer intranet.
8. The end-user traffic reaches the correct subscriber company's backend resources. The Secure Access Service processes any return messages to the end-users from the subscriber intranets following a similar set of steps.

In a typical MSP deployment, firewalls are present in front of the Secure Access Service in the MSP's DMZ, behind the Secure Access Service, in the MSP network or in the customer's intranet DMZ, or both. Note that a virtualized firewall could potentially exist behind the Secure Access Service (a Vsys cluster, for example), in which case it should have the ability to accept VLAN tagged traffic from the Secure Access Service and forward it to the proper customer VLAN (and vice versa). Also, most, if not all deployments have Domain Name Server (DNS) or Application servers located either in the MSP network or on the customer intranet.

In a virtualized Secure Access Service deployment, the front-end is considered the external interface and is the end-user or Internet-facing interface. The back-end is considered the internal interface and is the subscriber company intranet-facing interface.

The Secure Access Service tags inbound traffic sent by end-users and destined for a server in the subscriber intranet or MSP network, with VLAN tags containing the VLAN ID. Inbound traffic can arrive over the Secure Access Service's internal interface or external interface.

Outbound traffic, which is traffic transmitted over the Secure Access Service backend and destined for servers located on MSP network or subscriber intranet, can be sourced by the Secure Access Service itself. For example, traffic destined for authentication, DNS, or application servers, is outbound traffic, as is traffic forwarded by the Secure Access Service, such as Network Connect traffic.

If the traffic arrives as inbound traffic to an IP address that has been designated for an IVS system that uses a VLAN, that traffic is tagged with the VLAN tag on arrival. When it has been identified and directed to the proper backend destination, the VLAN termination device strips the VLAN tag from the Ethernet frame and forwards the traffic to the backend destination.

#### Related Documentation

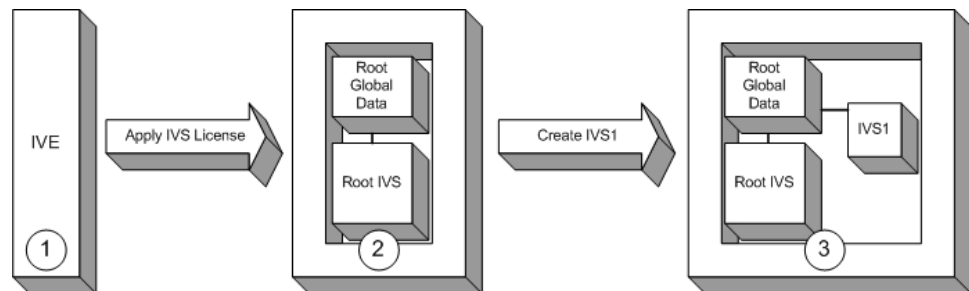
- [Signing In Directly to the IVS as an IVS Administrator on page 1036](#)
- [Signing In to the Root System or the IVS on page 1017](#)
- [IVS Configuration Worksheet on page 1021](#)

## Virtualized Secure Access Service Architecture

The virtualized Secure Access Service framework consists of a root system and any subscriber IVS systems the MSP root administrator creates subsequently. Subscriber IVS administrators can only manage resources on their particular IVS system. The root administrator can manage resources on all IVS systems on the appliance.

The IVS license converts the Secure Access Service to a root system that is functionally identical to the Secure Access Service, with the added capability of provisioning virtual systems. The root system consists of system-level global data and a single default root IVS, which encompasses the access management subsystem.

**Figure 75: IVS Architecture**



The root administrator (root administrator) is the super-administrator of the root system. Often, the root administrator is the same thing as the Secure Access Service administrator. The root administrator has administrative control over the root system and all subscriber IVS systems. The root administrator can provision IVS systems on the root system, create IVS administrators, edit IVS configuration. The root administrator can override configuration changes made by any IVS administrator.



**NOTE:** The instructions for configuring the root and IVS systems are meant to be read by a root administrator. The pronoun you, in these sections, denotes the root administrator. If a task can be performed by someone in a role other than the root administrator, the text makes a distinct reference to the role in the task description.

As shown in the above figure:

1. The Secure Access Service administrator applies an IVS license to the Secure Access Service containing a Secure Access Service license.
2. The resulting system contains the root global data and a root IVS, in effect, a virtualized Secure Access Service.
3. From the root IVS, the root administrator can create multiple subscriber IVS systems, each IVS completely separate from any other IVS.

The root system contains a superset of all capabilities of the system. You, as the root administrator, define all global network settings and root administrator settings on the

root system. For each subscriber, you provision one or more IVS systems and manage them from the root system.

The subscriber IVS contains a unique instance of the access management framework. When you create an IVS for each subscriber company, you also create an IVS administrator (IVS administrator) account. The IVS administrator has complete administrative control over the IVS. The IVS administrator uses an administrative admin console that contains a subset of the root administrator capabilities.

- Related Documentation**
- [Signing In to the Root System or the IVS on page 1017](#)
  - [Deploying an IVS on page 1014](#)

## Signing In to the Root System or the IVS

---

You can configure sign-in URLs using different methods:

- Sign-in URL prefix per IVS
- Virtual ports
- VLAN ports

You can use all of these methods on the same IVS.

### Signing-In Using the Sign-In URL Prefix

This feature enables end-users to access an IVS by way of a single hostname and IVS-specific sign-in URL prefix. By using this method, administrators can ensure that users can access multiple IVS systems by way of a single IP address on the Secure Access Service.

Additionally, the use of path-based URLs results in:

- Savings in certificate costs—You need only supply one device certificate.
- Fewer DNS entries—You need only one DNS entry across all IVS systems hosted on a single Secure Access Service.

Administrators and end-users can sign into an IVS system using sign-in URLs similar to the following (assuming the managed service provider URL is `www.msp.com`):

- Company A sign-in URL: `www.msp.com/companyA`
- Company B sign-in URL: `www.msp.com/companyB`
- Company A IVS administrator sign-in URL: `www.msp.com/companyA/admin`
- Company B IVS administrator sign-in URL: `www.msp.com/companyB/admin`

You can continue to restrict access by implementing additional sign-in URLs that are segregated by certain criteria, as follows:

- `www.msp.com/companyA/sales`

- www.msp.com/companyA/finance
- www.msp.com/companyA/hr

If you do not specify a URL prefix, the Secure Access Service defaults to sign-in over virtual ports. If you do specify a path-based sign-in URL prefix, the following rules apply:

- You cannot specify a multilevel path for the URL prefix, by using the / character.
- End-users and administrators can sign in to an IVS on the internal port, external port, VLAN interface, or virtual port that has not already been assigned to an IVS using the selected URL prefix, in other words, where the hostname is the DNS name assigned to one of the interface IP addresses.

For example, assume that your Secure Access Service ports are assigned to specific DNS names, as follows:

- Internal Port = MSP-internal
- External Port = MSP-external
- VLAN Port 10 = MSP-vlan10
- Virtual Port X = MSP-virtualx

Now, consider that VLAN Port 10 and Virtual Port X are not assigned to an IVS. If you host the Company A IVS, and the Company A sign-in URL prefix is specified as companyA in the IVS profile, then end-users can sign-in to the Company A IVS using any of the following URLs:

- MSP-internal/companyA
- MSP-external/companyA
- MSP-vlan10/companyA
- MSP-virtualx/companyA

The path-based URL feature carries a few restrictions, as follows:

- An end-user or administrator can sign into only one IVS from a given browser instance. If you attempt to sign in to another IVS from a new browser window of the same browser instance, your sign in attempt is rejected. You must create a new browser instance to sign in to multiple IVS systems.
- You cannot establish multiple concurrent sessions, with all sessions using Host Checker, from the same end-point to different Secure Access Services. You cannot establish multiple concurrent sessions from the same end-point to multiple IVS systems, regardless of the sign-in method.
- If you configure an IVS with a path-based sign-in URL prefix, you cannot use the persistent session cookie (DSID) and maintain the ability to sign in to multiple IVS systems from the same browser using the URL prefix. The limitation does not apply to users signing in to the IVS with a sign-in IP address, because the system creates a different DSID per target IVS in that case.

- Pass-through proxy based on port numbers is supported. However, you cannot specify a pass-through proxy policy when using virtual hosts, unless the virtual host DNS entry maps to the IVS sign-in IP address. If the virtual host DNS entry points to the Secure Access Service, when the user signs in he will sign-in to the root IVS sign-in page.
- When using Junos Pulse Collaboration, if a user is not already signed in to their IVS and you have enabled the option require Secure Access Service users, all meeting invitation emails will contain a link to the root IVS sign-in page.
- If an IVS user bookmarks pages while using web rewriting, signs out, then reopens the browser and selects the bookmark, he will display the root IVS sign-in page.

### Signing-In Over Virtual Ports

You may have reasons for configuring virtual ports for sign in. Virtual ports provide significant segregation of traffic. If you choose to use virtual ports, keep in mind that:

- Must provide multiple certificates—You need to supply one device certificate per virtual port address.
- Must configure multiple DNS entries—You need to supply DNS entries for each IVS system hosted on a single Secure Access Service.
- If multiple IVS's share the same virtual port for sign-in, the security settings of either IVS (allowed SSL/TLS version or encryption strength) can be associated to the virtual port. Once an IVS's security settings are associated to the virtual port, these settings are effective for sign-ins (ie SSL sessions) to that virtual port. To guarantee deterministic selection/association of security settings to virtual ports, IVSs that share the same virtual port for sign-in should have the same security settings.
- If an IVS is configured to have different security settings relative to the root system, the security settings of the root take effect for sign-in to the IVS via sign-in URL prefix, whereas the security settings of the IVS take effect for sign-in to the IVS via sign-in over virtual ports. For an IVS with strong encryption (such as AES) on the Secure Access Service with a root system having weaker encryption settings the following situation occurs: Signing in to the IVS via sign-in over virtual ports from an IE6 browser fails because the effective security settings for the SSL session is AES, which is not supported by IE6. However, the same user signing in to the same IVS from the same IE 6 browser through the sign-in URL prefix can succeed if the browser security settings are compatible with the root system's weaker security settings.

The sign-in request's target IP address drives the sign-in to the root system or IVS. To sign in to the root system or an IVS, users browse to a hostname-based URL. You map the URL, by way of external DNS, to the IP address or to an IP alias of the Secure Access Service's external interface.

For example, consider an MSP with host name msp.com, that provides SSL VPN gateway services to two subscribers: s1 and s2.

- Root administrator sign-in URL: <http://www.msp.com>
- S1 sign-in URL: <http://www.s1.com>
- S2 sign-in URL: <http://www.s2.com>

External DNS must map these URLs to unique IP addresses, which must correspond to IP addresses or aliases hosted on the Secure Access Service, typically a virtual port defined on either the internal or external port.

To summarize signing-in, IVS users can sign in on:

- A virtual port configured on the external interface of the Secure Access Service.
- A virtual port configured on the internal interface of the Secure Access Service (untagged).
- A VLAN interface configured on the internal interface (tagged).

Root system users can also sign in directly over the internal or external interface.

## Signing-In Over a VLAN Interface

In addition to the sign-in capabilities provided over the external interface (or the internal interface, if configured) by the root administrator, end-users can sign in over any VLAN interface the root administrator assigns to their IVS. In other words, the IVS administrator can provide the VLAN port IP address to end-users for sign-in.

You cannot map an explicit device certificate to any IP addresses mapped to a VLAN. When signing in over a VLAN interface, the system chooses the device certificate that is already assigned to the IVS. If there is no certificate associated with the IVS, the system assigns the certificate from the top of the Secure Access Service device certificate list. This list can be re-ordered when a certificate is added or removed, which can result in an unpredictable certificate during configuration. Once an IVS is in a production state, this should not present a problem, as the IVS VIP is mapped to a specific certificate.

### Related Documentation

- [Using VLANs with Secure Access Service on page 799](#)
- [Navigating to the IVS on page 1020](#)

---

## Navigating to the IVS

Only root administrators can navigate to an IVS from the root system. On the virtualized Secure Access Service, the admin console navigation for the root system includes an additional drop-down menu listing the configured IVS systems, on all page headers. You can navigate to an IVS and administer it by selecting an IVS from the drop-down menu. IVS administrators must sign-in directly to the IVS through a standard administrative sign-in page.

The root administrator creates the initial IVS administrator account. An IVS administrator can create additional IVS administrator accounts, using the standard procedure for creating administrator accounts.

### Related Documentation

- [Signing In to the Root System or the IVS on page 1017](#)



## IVS Configuration Worksheet

In order to configure the system to properly steer inbound traffic to the correct subscriber IVS, and outbound traffic to the correct VLAN, the MSP root administrator needs to compile a profile for each subscriber company.

When creating a new virtual system, you must create a number of other system objects, and specify several pieces of data, including IP addresses, VLAN IDs, virtual ports, and DNS settings. You can use this worksheet to plan and keep track of the system data while creating each IVS. The worksheet presents data in the general order in which you should define the IVS.

Depending on the specific topology of the subscribers' networks, you may need to collect additional information, or may not use all of the information listed on the form.

Date:	Created By:
Subscriber:	
Account #:	
Comment:	

### Subscriber VLAN (System > Network > VLANs)

#### VLAN Settings

VLAN Port Name:

VLAN ID (1-4094):

#### VLAN Port Information

IP Address:

Netmask:

Default Gateway:

### Subscriber Sign-in Virtual Port Configuration (System > Network > Port 1 > Virtual Ports > New Virtual Port)

External Virtual Port Name  
(for sign-in):

IP Address:

Internal Virtual Port Name  
(optional):

IP Address:

---

**Install Device Certificate for IVS hostname**

IVS Hostname:

Internal Port:

External Port:

---

**Subscriber IVS (System > Virtual Systems > New Virtual System)**

Name (Subscriber):

Description:

IVS Hostname:

---

**Administrator**

Username:

Password (at least 6  
characters in length):

---

**Properties**

Max Concurrent Users:

Default VLAN:

Selected Virtual Ports:  
(Internal Interface)

Selected Virtual Ports:  
(External Interface)

Network Connect IP Pool:

---

**Static Routes (System > Network > Routes > New Routes)**

Destination Network/IP:

Netmask:

Gateway:

Interface:

Metric:

---

### DNS Settings (Subscriber IVS > System > Network > Overview)

Hostname:
Primary DNS:
Secondary DNS:
DNS Domain(s):
WINS:

---

**Related Documentation** • [Deploying an IVS on page 1014](#)

---

## Administering the Root System

Once you apply the IVS license to the Secure Access Service, the new Virtual Systems tab appears in the administrator UI. After you apply the IVS license, you can see an explicit display of the root system in the drop down menu that appears in the admin console header area.

Setting up the system requires a series of basic procedures. Once the hardware is connected:

1. Boot the system.
2. Apply the IVS license through the Maintenance > System > Upgrade/Downgrade page of the admin console.
3. Configure the root system from the admin console.

Regardless of how many subscriber administrators you define on the subscriber IVS systems, you always maintain control over the entire system and have visibility into the settings on all IVS systems.

**Related Documentation** • [Signing In to the Root System or the IVS on page 1017](#)

---

## Configuring the Root Administrator

Configuring the root administrator is similar to the task of creating a new administrator on a standalone Secure Access Service. You can create an administrator account through the Authentication > Auth. Servers > Administrators > Users page of the admin console, or by using the serial console.

If you upgrade from an older Secure Access Service software version to the 5.1 version or later, the system considers any administrator in the root system who maps to the Administrators role to be a root administrator for the Secure Access Service. If you

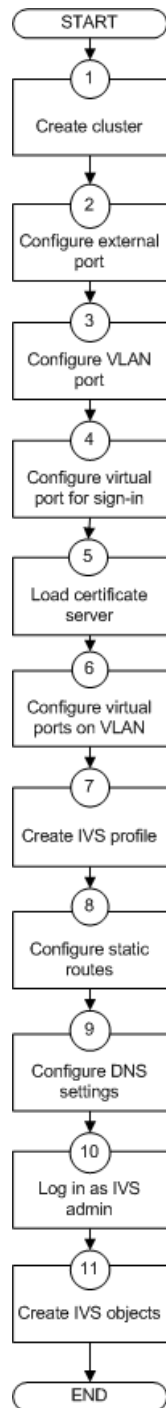
re-image the Secure Access Service or install a brand new piece of hardware, you create a primary administrator during the initial configuration steps, in the serial console.

**Related  
Documentation**

- [Creating and Configuring Administrator Roles on page 1006](#)
- [Signing In Directly to the IVS as an IVS Administrator on page 1036](#)

## IVS Provisioning Process Overview

The following figure illustrates the basic tasks required to provision an IVS.



Provisioning an IVS consists of the following steps:

1. Configure one or more clusters, if needed, through the System > Clustering > Create Cluster page.
2. Configure and enable external port. The external port is in a disabled state, by default. You must enable the port and configure it, to provide sign-in capabilities from outside the network.
3. Create at least one VLAN port for each subscriber company. You must define a unique ID for each VLAN. A subscriber company can have multiple VLANs on the Secure Access Service.
4. Configure at least one virtual port on the external port to enable end-users to sign in. You can also configure virtual ports on the internal port, for signing in from behind the firewall, if needed.
5. Load one certificate server per subscriber company.
6. If you intend to use virtual ports, for example, to support IP sourcing, create them at this point in the process.
7. Create an IVS profile for each subscriber company. The IVS profile establishes the connection between the company, the VLAN, and the available virtual ports.
8. Configure static routes to backend servers. If you intend to provide shared access to resources on the MSP network, you add static routes to the VLAN route tables that point to those resources.
9. Configure DNS settings, so that any traffic destined for resources on the MSP network first goes through the MSP's DNS server.
10. Log in as the IVS administrator.
11. Configure users, roles, realms, and resource policies for the IVS.

When you create the IVS, the IVS name appears in the drop down menu located in the header of the admin console. You can perform operations on each IVS by selecting the IVS name in the drop down menu and clicking the Go button.

- Related Documentation**
- [Deploying an IVS on page 1014](#)
  - [Signing In to the Root System or the IVS on page 1017](#)

---

## Configuring Sign-In Ports for IVS

---

You must configure virtual ports by which end-users can sign in to the subscriber company intranet. A virtual port activates an IP alias on a physical port and shares all of the network settings of that port.

### Configuring the External Port

To enable and configure the external port:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than Root, select Root from the menu and click Go.
2. Select **System > Network > Port 1 > Settings**.
3. Select **Enabled**.
4. Enter a valid IP address for the external port.
5. Enter a valid netmask for the IP address.
6. Enter the default gateway address.
7. Click **Save Changes**.

The system enables the port.

### Configuring a Virtual Port for Sign-In on the External Port

You need to configure a virtual port to enable IVS end-users to sign-in from outside the network over the external port. For example, if users sign in over the Internet, they use the virtual port defined on the external port.

To configure the virtual port for sign-in:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than Root, select Root from the menu and click Go.
2. Select **System > Network > Port 1 > Virtual Ports**.
3. Click **New Port**.
4. Enter a unique name for the virtual port.
5. Enter a valid IP address, provisioned by the subscriber company's network administrator.
6. Click **Save Changes**.

The system adds the port, displays the Virtual Ports tab, and restarts the network services. You can assign this virtual port to an IVS profile. Define as many virtual ports as needed for sign-in.

### Configuring a Virtual Port for Sign-In on the Internal Port

You need to enable and configure the internal port to allow IVS end-users to sign in from inside the network.

To configure the virtual port for sign-in:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than Root, select Root from the menu and click Go.
2. Select **System > Network > Internal Port > Virtual Ports**.
3. Click **New Port**.
4. Enter a unique name for the virtual port.
5. Enter a valid IP address, provisioned by the subscriber company's network administrator.
6. Click **Save Changes**.

The system adds the port, displays the Virtual Ports tab, and restarts the network services. You can assign this virtual port to an IVS profile. Define as many virtual ports as needed for sign-in.

**Related Documentation**

- [IVS Provisioning Process Overview on page 1025](#)
- [Virtual Local Area Network \(VLAN\) on Subscriber IVS on page 1028](#)
- [Configuring VLANs on the Virtualized Secure Access Service on page 1029](#)

---

## Virtual Local Area Network (VLAN) on Subscriber IVS

---

By defining at least one Virtual Local Area Network (VLAN) on each subscriber IVS, the MSP can take advantage of VLAN tagging, by which the virtualized Secure Access Service tags traffic with 802.1Q VLAN IDs before transmitting the traffic over the backend. The carrier infrastructure uses the VLAN tag to direct the packets to the appropriate subscriber intranet.

VLAN tagging provides separation of the traffic the Secure Access Service transmits over the backend, destined for subscriber intranets. Traffic coming in over the front-end—that is, inbound traffic—does not have VLAN tags. The IVS adds the tag to a message upon its arrival over one of the Secure Access Service ports.

Each VLAN is assigned a VLAN ID which is part of an IEEE 802.1Q-compliant tag that is added to each outgoing Ethernet frame. The VLAN ID uniquely identifies each subscriber and all subscriber traffic. This tagging allows the system to direct all traffic to the appropriate VLAN and to apply respective policies to that traffic.

The VLAN termination point is any device on which VLAN-tagged traffic is identified, stripped of the VLAN tag, and forwarded to the appropriate tunnel to the backend. The VLAN termination point can be a CE router, CPE router, L2 switch, firewall, or other device capable of VLAN routing.

You must define a VLAN port for each VLAN. The root administrator assigns the specific VLAN ID when defining the VLAN port.



For each VLAN you configure, the virtualized Secure Access Service provisions a unique, logical VLAN interface, or port, on the internal interface. There is no relationship between the internal port IP address and any VLAN port IP address. Each VLAN port has its own route table.

Each VLAN port definition consists of:

- **Port Name**—Must be unique across all VLAN ports that you define on the virtualized Secure Access Service or cluster.
- **VLAN ID**—An integer in the range from 1 to 4095 that uniquely identifies the subscriber/customer VLAN.
- **IP Address/Netmask**—Must be an IP address or netmask from the same network as the VLAN termination point, because the virtualized Secure Access Service connects to the VLAN termination point on a Layer 2 network connection. VLAN IP addresses must be unique. You cannot configure a VLAN to have the same network as the internal port. For example, if the internal port is 10.64.4.30/16 and you configure a VLAN as 10.64.3.30/16, you may get unpredictable results and errors.
- **Default gateway**—The IP address of the default router, typically the CE or CPE router. The default gateway could act as the VLAN termination point, or could reside behind the VLAN termination point.
- **Other network settings**—Inherited from the internal port.



**NOTE:** If you do not specify a VLAN for the subscriber company, you must configure the IVS to transmit traffic over the internal interface by selecting it as the default VLAN.

## Configuring VLANs on the Virtualized Secure Access Service

The relationship between a VLAN and a given IVS allows the root system to separate and direct traffic to different subscribers.

### Configuring a VLAN Port

Before creating a new virtual system, create a VLAN port to identify the specific subscriber traffic.

To create a VLAN port:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than Root, select Root from the menu and click **Go**.
2. Select **System > Network > VLANs** to open the VLAN Network Settings tab.
3. Click **New Port**.
4. Under VLAN settings, enter a name for the VLAN port.
5. Enter a VLAN ID.

The VLAN ID must be between 1 and 4095 and must be unique on the system. The root system uses untagged traffic and cannot be changed.

6. Enter the IP address for the VLAN.
7. Enter a netmask for the VLAN.
8. Enter a default gateway for the VLAN.
9. Click **Save Changes**.

#### **Assigning a VLAN to the Root IVS**

In order to assign a VLAN to a role, you must first assign the VLAN to the root IVS. If you have not assigned a VLAN to the root IVS, the VLAN is not available in the VLAN drop down menu in the Users > User Roles > Select Role > VLAN/Source IP page.

To assign a VLAN to the root IVS

1. Select **System > Virtual Systems > Root**.
2. Under Properties, select the VLAN from the Available VLANs list.
3. Click **Add ->** to move the VLAN name to the Selected VLANs list.
4. Click **Save Changes**.

#### **Related Documentation**

- [Using VLANs with Secure Access Service on page 799](#)

---

## **Adding Static Routes to the VLAN Route Table**

When you create a new VLAN port, the system creates two static routes, by default:

- The default route for the VLAN, pointing to the default gateway.
- The interface route to the directly connected network.

In addition, you can static routes to shared servers in the MSP network.

To add static routes to a VLAN route table:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than Root, select Root from the menu and click **Go**.
2. Select **System > Network > VLANs**.
3. Either click **New Port** or select an existing VLAN for which to add a static route.
4. At the bottom of the VLAN port page, click the Static Routes link.
5. From the drop-down menu, select the VLAN for which to create static routes, if not already selected.
6. Click **New Route**.
7. On the New Route page, enter the destination network/IP address.

8. Enter the destination netmask.
9. Enter the destination gateway.
10. Select the interface from the Interface drop down menu.
11. Enter the metric.

The metric is a number between 0 and 15, and usually signifies the number of hops that traffic can make between hosts. You can set the metric of each route to specify precedence. The lower the number, the higher the precedence. Therefore, the device chooses a route with a metric of 1 over a route with a metric of 2. A router that uses metrics compares a dynamic route metric with the static route metric and chooses the route with the lowest metric.

12. If you want to add static routes to shared services, for example, you should perform one of the following steps:
  - Click **Add to [VLAN] route table**, where [VLAN] is the name of an available VLAN, to add the route to a selected VLAN. This action adds the static route to a particular subscriber company's VLAN route table and excludes access from all other VLANs, including from users of the MSP network.
  - Click **Add to all VLAN route tables** to add the route to all VLANs defined on the system. For example, if the root administrator wants to share some service among all end-users of all subscriber company's, select this option.

You can also use static routes if you want to configure shared services on the MSP network. To accomplish this:

- Add a static route to the shared resource in either your own VLAN route table, if the root system has a VLAN, or in the main Secure Access Service route table, if the root system uses the internal interface.
- Click **Add to all VLAN route tables**, which populates all VLAN route tables with the static route. When you add the static route to all VLAN route tables, all IVS profiles can access the shared services.

#### Related Documentation

- [Adding Static Routes to the Management Route Table on page 832](#)

## Deleting a VLAN

You cannot delete a VLAN that is associated with an IVS. First, you must either delete the IVS or remove the relationship between the IVS and the VLAN port.

To delete a VLAN:

1. Select **System > Network > VLANs**.
2. Select the checkbox next to the name of the VLAN to delete.
3. Click **Delete**.

- Related Documentation**
- [Creating a Virtual System \(IVS Profile\) on page 1032](#)

## Loading the Certificates Server

---

On the root system, you can load certificates. You must associate the virtual ports that you have defined as sign-in ports for IVS end-users with the device certificate. You can specify virtual ports on the Certificate Details page.

On an IVS, you can only import Trusted Client CAs and Trusted Server CAs.



**NOTE:** You cannot share certificates across IVS systems. You must have a unique IP and certificate for each IVS.

You can only configure the root IVS to re-sign applets/controls in the admin console. The admin consoles for subscriber IVS systems do not show the re-signing option. You should take note of the following information:

- All root and subscriber end-users see the same applets/controls: either all of the default Juniper controls, or all of the controls signed by the root IVS.
- If you do not want subscriber IVS systems to see controls signed by the certificate from the root IVS, then you should not re-sign the controls. If you re-sign the controls, the subscriber IVS systems have access to them.

- Related Documentation**
- [Importing Certificates Into the Secure Access Service on page 840](#)
  - [Using a Trusted Client CA on page 846](#)
  - [Using Trusted Server CAs on page 864](#)

## Creating a Virtual System (IVS Profile)

---

The IVS profile defines the subscriber IVS and any elements required to reach the subscriber's intranet, such as DNS settings and authentication servers.

To define the IVS profile:

1. Make sure you are in the root context. If the IVS drop down menu in the admin console header bar displays something other than Root, select Root from the menu and click **Go**.
2. Select **System > Virtual Systems**.
3. Click **New Virtual System** to display the IVS - Instant Virtual System page.
4. Enter the name of the subscriber company.
5. Enter a description (optional).
6. Select **Enabled**, if it is not already selected.

If you ever need to prohibit a subscriber and the subscriber's end-users from accessing the IVS due to billing or other problems, disable their account here. By disabling the account, you can resolve any customer issues and then enable access without having to delete the subscriber account and lose all the configuration data.

7. Under Initial Configuration, select the configuration to initialize the IVS.
  - **Default Configuration**—Populates the IVS with system-generated defaults,
  - **Root**—Copies the root system configuration to the new IVS, or any of the existing IVS's on the system
  - **IVS name**—Copies the configuration from the selected IVS to the new IVS.
8. Under Administrator, create a username and password for the IVS administrator.
 

The IVS administrator username and password are available in the IVS profile the first time you create the IVS. Subsequently, if you edit the IVS, these fields are not available, for security purposes. However, if you need to access the IVS administrator username and password, you can do so through the IVS configuration page, by going to the Administrators authentication server.
9. Under User Allocation, you can limit the number of concurrent users on the IVS. Specify the limit values for these options:
  - **Minimum Guaranteed Users**—You can specify any number of users between one (1) and the maximum number of concurrent users defined by the Secure Access Service's user license.
  - **Burstable Maximum Users (optional)**—You can specify any number of concurrent users from the minimum number you specified up to the maximum number of licensed users. If left blank, the Minimum Guaranteed Users value limits the number of concurrent users on the IVS.



**NOTE:** If you later reduce the Burstable Maximum Users setting, you must also edit the realm limits. The realm limits are not automatically updated when you change the Burstable Maximum Users setting.

10. Under Properties, specify the sign-in properties, VLAN, and port settings for the IVS.
  - a. Select a VLAN from the Available list box and click **Add ->** to move the name of the VLAN to the Selected VLANs list box. You can add multiple VLANs to an IVS. You can select the internal port as a VLAN even if you have added other VLANs to the Selected VLANs list. Unlike other VLAN interfaces, you can add the internal port to multiple IVS profiles. If you have not defined a VLAN, you must select the internal interface instead.
  - b. To specify the default VLAN for the IVS, select the VLAN name in the Selected VLANs list box, then click **Set Default VLAN**. The IVS marks the VLAN name with an asterisk (\*). The virtualized Secure Access Service uses the default VLAN to provide authentication server access. The Secure Access Service consults the default VLAN's route table to look up the route to authentication servers for a given IVS.

You must specify a default VLAN for each IVS. The significance of the default VLAN for a given IVS is that when an end-user attempts to sign into a particular realm within that IVS, the IVS sends traffic to the authentication server for that realm over the default VLAN interface.



**NOTE:** You must specify the internal port as the default VLAN for the root IVS.

- c. If you want to define a sign-in URL prefix that your end-users can sign in over rather than over a virtual port, add the prefix to the Sign-in URL Prefix field. The prefix is the equivalent of the first node in the URL, for example, companyA in the following URL:

`http://www.mycompany.com/companyA`

- d. If you have defined virtual ports for either the internal interface or the external interface, you can select them in the Available list boxes and click **Add ->** to move them to the Selected Virtual Ports list boxes for the respective interfaces.
- e. Enter the address or range of IP addresses that are available for Network Connect clients (end-users). If you intend to configure a DNS server on the IVS, for a server located on the subscriber intranet, you must add the available Network Connect IP address pool values here.



**NOTE:** Unlike the NC Profile page, you can not specify a subnet range in the IVS profile page. In other words, entering 172.19.48.0/24 is not allowed. You can however, specify arbitrarily large IP ranges such as 172.19.48.0-172.19.48.255.

11. Click **Save Changes**.

#### Related Documentation

- [Using Virtual Ports on page 802](#)
- [Signing In Directly to the IVS as an IVS Administrator on page 1036](#)

## IVS Initial Config Via Copy from the Root System or Another IVS

When creating a new IVS profile, you have the option to copy the configuration of a root system or an existing IVS to “initialize” the new IVS. The resulting IVS combines the information you specify in the new IVS profile along with the configuration copied from the root system or existing IVS. Settings in the IVS profile override the copied settings.

Note that the copy is a one-time operation, with no on-going relationship between the source of the copy and the target of the copy. Subsequent configuration changes in the copy source are not reflected in the copy target or vice-versa.

#### Caveats

After performing an IVS config copy, some manual reconfiguration is required on the target.

- DNS settings are always left blank regardless of whether or not the configuration was copied from another IVS.
- When copying from an existing IVS, you should check all references to VLANs and virtual ports. For example, you may need to update the association of roles to VLAN interfaces or virtual ports.
- When copying from an existing IVS, you should check all NC connection profiles and reconfigure them, as needed, to meet the requirements of the NC IP range in the IVS profile.
- When copying from a root system, you must configure the admin roles and admin realm role mappings manually. These settings are not copied from the root system.
- Based on license restrictions of the new IVS, some admin and user realm limits may get reset. Check the admin and user realms and configure as needed.
- The Initial Configuration option allows you to select the configuration to initialize the IVS. This option does not copy the configurations of the archive servers regardless of whether you select the root system or any other IVS.

The copy operation can result in populating the target IVS with unsuitable settings. When an IVS is configured by copying the configuration from the root system or another IVS, the entire configuration from the source is copied to the target, including ACLs, resource policies, resource profiles, PAC files, and so forth, which frequently refer to specific backend servers by name, URL or IP address. In the common case, these resources tend to be company/department intranet-specific (that is, private to a particular IVS), and should not be exposed to end-users of other IVSs.

It is the responsibility of the root admin to go through the entire target IVS configuration manually and purge references to any backend network resources and IP addresses that are not applicable to the target IVS.

## Use Cases for IVS Initial Config Via Copy

### An IVS is created from a “template” IVS

An example of this use case is provisioning virtual systems. A service provider may want to provision three categories of subscribers: Gold, Silver and Bronze. The administrator creates three IVSs (called Gold, Silver, and Bronze) and manually configures the authentication servers, roles, resource policies, etc. appropriate to the subscriber category. These IVSs are not actually used in production, but as sample configuration “templates” that can be applied to real subscriber IVSs. When provisioning a new subscriber IVS, the administrator “clones” the template by copying initial configuration for the new IVS from the Gold, Silver or Bronze “template” IVS.

It is the responsibility of the root admin to carefully craft the template IVSs to contain only those settings that are meant to be shared across multiple IVSs, such as centralized auth servers, host checker policies etc. The template IVSs should not contain references

to private resources that are not meant to be exposed to/reachable from the real subscriber IVSs.

#### **the Secure Access Service deployment is converted to an IVS deployment**

This use case is for copying the config from the root system. When an existing standalone Secure Access Service deployment is converted to an IVS deployment by applying an IVS license and then creating multiple IVSs, the new IVSs can be configured by copying the configuration from the root system or other IVSs, and then following the steps mentioned in the caveats above.

#### **Related Documentation**

- [Importing and Exporting IVS Configuration Settings on page 900](#)

---

## **Signing In Directly to the IVS as an IVS Administrator**

Signing in directly to the IVS as an IVS administrator is different than picking the IVS from the virtual system drop down menu in the Web-based administrator UI console. If you, as the root administrator, want to sign in the same way that all IVS administrators must sign in to the IVS, perform the following steps:

1. Sign-out of the root Secure Access Service.
2. Enter the sign-in URL in the address bar of a valid browser, using either the hostname or the IP address. For example:

```
https://www.company.com/admin
https://10.9.0.1/admin
```

This example assumes that you assigned the IP address 10.9.0.1 as a virtual port for sign-in. The format depends on whether or not you defined a DNS entry for the sign-in host name. When logging in, the administrator can enter the host name or the IP address defined as the virtual port for sign-in. If the administrator signs in from within the network, he should use the IP address you configured for signing in over the internal port. If the administrator signs in from outside the network, he should use the IP address you configured for signing in over the external port.

3. Press **Enter**.
4. Enter the IVS administrator username.
5. Enter the IVS password.
6. Click the **Sign in** button.

Assuming the credentials are valid, the System Status page for the IVS appears.

When either the root or an IVS administrator exits the IVS, the appliance immediately severs the connection.

#### **Related Documentation**

- [Signing In to the Root System or the IVS on page 1017](#)
- [Navigating to the IVS on page 1020](#)



---

## About Role-Based Source IP Aliasing

---

If the subscriber company employs policy evaluation devices/firewalls in their network for the purpose of separating traffic based on the source IP address as it enters the intranet from the IVS, you, the root administrator, must configure the IVS to generate traffic with different source IP addresses. The role-based source IP aliasing feature, also known as VIP sourcing, provides the capability to map end-user roles to VLANs and specific source IP addresses (the IP address of any one of the virtual ports hosted on the VLAN interface). All traffic generated by the IVS over the back-end on behalf of the end-user carries the source IP address configured for the end-user's role.

For example, assume that the traffic to a particular subscriber intranet needs to be differentiated based on whether it originates from customers, partners, or employees. There are two ways to accomplish this:

- Provision three different VLANs for the subscriber, create three roles corresponding to customers, partners and employees, and map each role to a different VLAN.
- Provision a single VLAN for the subscriber, configure three virtual ports with unique IP addresses, and map customers, partners and employee roles to the same VLAN but to different source IP addresses.

You can use role-based source IP aliasing whether or not you have defined a VLAN. In the case of a non-VLAN configuration, you define a virtual port, then assign that port to a role's source IP.

When using a VLAN, you can set the source IP address of a role to either the VLAN port IP address or to an IP alias configured on a VLAN port.

### Related Documentation

- [Associating Roles with Source IP Addresses in an IVS on page 1037](#)
- [Using Virtual Ports on page 802](#)

---

## Associating Roles with Source IP Addresses in an IVS

---

Assuming that the root administrator has already configured a VLAN, virtual ports for the VLAN, and the IVS, the IVS administrator can associate roles with the virtual ports as follows:

1. Log in to the IVS as the IVS administrator.
2. Choose **Users > User Roles**.
3. Click **New Role**.
4. Enter a name for the role.
5. Select the **Source IP** checkbox.
6. Select any other options and the features you want a user with this role to be able to access (Optional).
7. Click **Save Changes**.

The page refreshes and a set of tabs now appears.

8. Select the VLAN/Source IP tab.
9. Select the VLAN, if the root administrator has defined more than one VLAN for this IVS.
10. Select the source IP from the Select Source IP drop down menu.
11. Click **Save Changes**.
12. Repeat the process for each new role.

When creating new users, the IVS administrator can then assign each user to one of the roles, which determines what source IP address each user can access.

**Related  
Documentation**

- [About Role-Based Source IP Aliasing on page 1037](#)

---

## Configuring Policy Routing Rules on the IVS

---

The virtualized Secure Access Service uses a policy routing framework that depends on rules, route tables, and route entries that are configured on the system.

When you create a VLAN, the system provisions a new route table for that VLAN. VLAN route tables exist in addition to the main route table for the Secure Access Service. Only the root administrator can manage VLAN route tables. IVS administrators cannot view or access the route tables.

Each VLAN route table contains the following route entries:

- Automatically-created route entries
- Manually-created route entries

### Automatically-Created Route Entries

The default route 0.0.0.0 points to the default gateway you have configured for the VLAN interface. The Secure Access Service creates this route internally when it creates the VLAN interface. End-users can reach most of their company's resources through the default route.

The interface route is the network route corresponding to the VLAN interface IP address.

### Manually-Created Route Entries

Static routes to servers within the same VLAN that are accessible through routers other than the default gateway.

Static routes to server IP addresses on other VLAN ports within the same subscriber company intranet, or VLAN ports within the MSP network. For example, you might define in a VLAN route table static routes to DNS or authentication servers in either a subscriber company intranet or in the MSP network.

Static routes to server IP addresses accessible through the internal interface. These are usually required if your MSP network is connected to the internal interface.

## Routing Rules

A number of rules have been built into the system to enable the correct routing of traffic to the appropriate subscriber intranets. For example, rules exist to map:

- The Network Connect IP pool address for each Network Connect end-user session to a corresponding VLAN route table.

To construct this rule, the system determines an end-user's role when the user establishes a Network Connect session. The system can then search the role for the associated VLAN.

- A configured source IP address to a corresponding VLAN route table.

The system creates this rule whenever you configure a virtual port or source IP alias on a VLAN port.

There are no explicit rules governing the flow of traffic between the subscriber or MSP networks and end-users. Traffic arriving at the Secure Access Service over the backend has a destination IP address set to the configured IP address of one of the network interfaces, either the external interface, VLAN interface, or a Network Connect tunnel interface. The Secure Access Service application automatically handles the processing.

You cannot access the rules table. This section includes a description of the rules table and how rules are constructed to help you understand how the system operates.

## Overlapping IP Address Spaces

The virtualized Secure Access Service supports overlapping IP addresses in subscriber intranets, and overlapping source IP addresses for Network Connect. At this time, the virtualized Secure Access Service does not support multiple VLAN interfaces with identical IP addresses.

The virtualized Secure Access Service supports overlapping IP addresses among customer networks that are tied to VLANs in different IVS systems, because IVS systems do not share route tables.

Assume that Company 1 and Company 2 both have internal networks that use IP addresses 10.64.0.0/16. Because these addresses are internal to each company's network, and because each company has a completely separate IVS, identified by a unique VLAN ID, the MSP can support them, even though, technically, they overlap.

## Define Resource Policies

Both you, as the root administrator, and the IVS administrator can create policies for end-users.

You can also customize which policies are visible to IVS administrators. However, you must customize each IVS independently. Also, if you are in the root IVS context and you customize the admin console, you are only customizing the console as it appears to you

or other administrators who are permitted to view the root IVS console. To customize any IVS admin console, you must be in the context of that IVS.

**Related  
Documentation**

- [Resource Policy Components on page 144](#)
- [Customizable Admin and End-User UIs on page 1103](#)

---

## Clustering a Virtualized Secure Access Service

---

You can cluster the entire Secure Access Service, including all IVS systems. You cannot cluster an individual IVS system. The clustering rules and conditions in a standard Secure Access Service network also apply to clusters in an IVS network, with the following exceptions:

- Virtual port replication—Any virtual port you define on the Active node is replicated to the Passive node. The virtual port's name and address is the same on both Active and Passive nodes.
- Virtual port source IP—Given an end-user who maps to a particular role, and a backend connection from any node on behalf of that end-user, the source IP of the backend connection is the same as the source IP of the virtual port configured for the end-user's role.
- VLAN port replication—When you create or delete a VLAN port on an Active cluster node, the Secure Access Service automatically adds or deletes the VLAN port on the Passive node.
- VLAN definition—For any given VLAN port, the slot, logical name, VLAN ID, netmask, and default gateway are the same across all cluster nodes.
- VLAN port IP address—The IP address for each VLAN port is node-specific. Corresponding VLAN ports on an Active/Passive cluster are configured on the same IP network. You can only configure an IP address/netmask combination for a VLAN port on the standby node if the resulting network corresponds to the VLAN port in the Active cluster node. VLAN IP addresses must be unique. You cannot configure a VLAN to have the same network as the internal port. For example, if the internal port is 10.64.4.30/16 and you configure a VLAN as 10.64.3.30/16, unpredictable behavior and errors can occur.
- Policy routing—You can configure route settings per node and per interface, either physical or VLAN, however, those route settings are synchronized across the cluster when you edit them.
- IVS profiles—IVS profiles are replicated across cluster nodes, and are not partitioned across cluster nodes.
- Network Connect—If you deploy the virtualized Secure Access Service as an Active/Passive cluster, the Network Connect connection profile that you or an IVS administrator configures within each IVS is propagated to the standby node.

- Network Connect in Active/Active cluster—In an Active/Active cluster, the Network Connect IP address pool for each IVS is split across individual cluster nodes by way of role-level settings.
- Failover behavior—In the event of a failover, the VLAN interface does not disappear. Both Active and Passive nodes should contain the VLAN interface.



**NOTE:** When using Network Connect, you should always define virtual ports for each VLAN port you create. If you have defined a Network Connect IP address pool, and you are running in Active/Passive cluster mode, you must configure your routers to direct traffic to one of the VLAN's virtual ports as the next-hop gateway. Otherwise, Network Connect sessions may not recover gracefully from a failover.

**Related Documentation**

- [About Clustering on page 977](#)

## Accessing a DNS Server on the MSP Network

In the root system, you can configure access so that any traffic destined for resources on the MSP network goes through the DNS server on the MSP network.

To access a DNS server on the MSP network:

1. In the admin console, **choose System > Network > Overview.**
2. Under DNS name resolution, provide the primary DNS address, secondary DNS address, and the DNS domains.

When you add the DNS addresses, each one is added to the resolv.conf file on the Secure Access Service, in a nameserver directive.

3. If you are using WINS, provide the WINS server address.
4. Click **Save Changes.**
5. Configure the Network Connect connection profile.

You can provide DNS services to non-Network Connect users by specifying a global DNS/WINS server in the MSP network. The global DNS/WINS server hosts DNS for all participating subscriber companies. As an alternative, you can configure a HOSTS file on the Secure Access Service with DNS entries for all participating subscriber companies.

When you configure a global DNS/WINS server in this way, it provides DNS services to any requesting entity, including from Network Connect users of participating subscriber companies that do not have DNS servers in their intranets.

**Related Documentation**

- [Creating VPN Tunneling Connection Profiles on page 761](#)

## Accessing a DNS Server on a Subscriber Company Intranet

---

In each IVS system, you can configure access so that any traffic destined for resources on the IVS subscriber's network goes through the DNS server on their internal company network.

To access a DNS server on a subscriber intranet:

1. If you did not add a valid Network Connect IP address pool to the IVS profile when you created the virtual system, modify the IVS profile to include the Network Connect IP addresses.
2. In the admin console, select the name of the subscriber IVS from the drop down menu in the console header bar.
3. Click **Go**.
4. On the subscriber IVS admin console page, choose **System > Network > Overview**.
5. Under DNS name resolution, provide the primary DNS address, secondary DNS address, and the DNS domains.
6. If you are using WINS, provide the WINS server address.
7. Click **Save Changes**.
8. Configure the Network Connect Connection Profiles.
  - a. Choose **Users > Resource Policies > Network Connect > Network Connect Connection Profiles**.
  - b. Click **New Profile**.
  - c. Provide a name for the Connection Profile.
  - d. In the IP Address Pool field, enter the range of IP addresses available for use by Network Connect users.
  - e. Select any other connection settings, or take the defaults.
  - f. Choose a role to which to apply the settings, if necessary. By default, if you do not choose a role, the policy applies to all roles.
  - g. Click **Save Changes**.
  - h. Click the DNS tab.
  - i. Select the **Use Custom Settings** checkbox.
  - j. Add the Primary DNS, Secondary DNS (optional), the DNS domain name, and WINS server IP addresses.

- k. Select the DNS search order. When you enter custom settings for the IVS, the root system searches the subscriber DNS server first, then the MSP DNS server, by default.
- l. Click **Save Changes**.



**NOTE:** You must perform this task for every IVS.

**Related  
Documentation**

- [IVS Provisioning Process Overview on page 1025](#)

## Configuring VPN Tunneling for Use on a Virtualized Secure Access Service

You, as the root administrator, must work with the IVS administrator to configure VPN Tunneling so that end-users can send traffic to the subscriber intranet and receive traffic back from the subscriber intranet.

If you want to use VPN Tunneling on a subscriber company's IVS (rather than just by way of VPN Tunneling running on the MSP network) you must configure a DNS server on the IVS.

For clients to be able to establish VPN Tunneling sessions to an IVS, DNS settings must be set for the IVS. Otherwise, the VPN Tunneling session initiation fails and displays an error message.

### Configuring the VPN Tunneling Connection Profile

Configure the VPN Tunneling connection profile using the IP addresses from the range specified in the IP pool in the IVS profile.

1. Select **Users > Resource Policies > VPN Tunneling > VPN Tunneling Connection Profiles**.
2. Click **New Profile**.
3. Enter the IP addresses in the IP Address Pool text box, one address per line. The Help text in the admin console shows examples of valid ranges.
4. Change the transport, encryption, and compression settings from the defaults, if necessary.
5. Add the appropriate role from the Available roles listbox to the Selected roles listbox.
6. Click **Save Changes**.

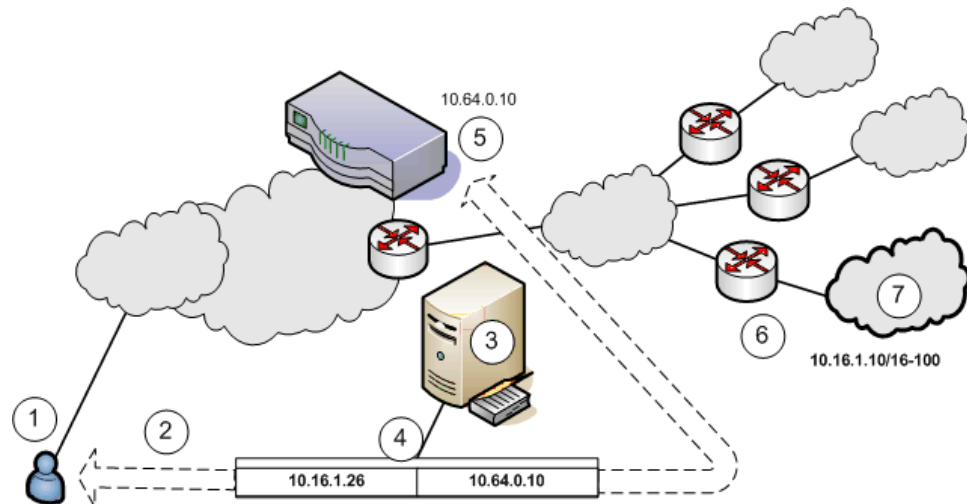
### Configuring VPN Tunneling on Backend Routers

Both you, as the root administrator, and the IVS administrator must configure static routes on the backend to ensure that each end-user can be reached from the subscriber intranet, and if needed, the MSP network.

If you want VPN Tunneling users to be able to access the MSP network's DNS server, configure a static route in the route table of each application server or DNS server to the

end-user's VPN Tunneling IP pool address. Set the next-hop gateway to the IP address of the root system's internal interface.

**Figure 76: Setting a Static Route in MSP Network DNS or Application Servers**



1. End-users sign in over an Internet connection, using an IP address from a VPN Tunneling IP address pool, to reach the DNS server on the MSP network.
2. The root administrator specifies a static route in the DNS server route table to point to an IP address from the VPN Tunneling IP address pool. The subscriber company must define the IP address pool in its intranet.
3. The DNS server resides on the MSP network and serves all end-users of all subscriber companies.
4. The DNS server's route table contains a static route to the VPN Tunneling IP address pool and the next-hop gateway IP address.
5. The Secure Access Service's internal interface is the DNS server's next-hop gateway address.
6. The subscribers' CPE routers perform the proper traffic routing to the subscriber company intranets.
7. Each subscriber company that intends its users to pass through the MSP DNS or application servers must define a corresponding VPN Tunneling IP address pool.

As shown the following figure, the IVS administrator can configure the subscriber CPE router with a static route to the end-user's IP address, with the next-hop gateway set to the IP address of the corresponding CE router on the MSP network.

Alternately, the subscriber can configure a default route on the CPE router to point to the MSP CE router as the next-hop gateway. In this case, you do not need to add individual static routes to the VPN Tunneling IP pool addresses.

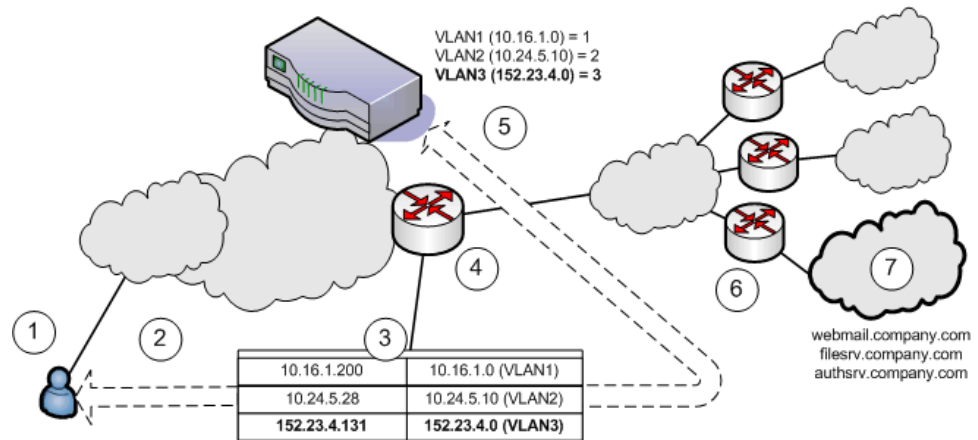


1. End-users sign in over an Internet connection using an IP address agreed upon by the MSP and the subscriber company.
2. Specify a static route in the subscriber company's CPE router's route table to point to the end-user sign-in IP addresses.
3. You must also specify the next-hop gateway in the CPE router's route table.
4. You use the MSP CE router's IP address as the next-hop IP in the CPE router's route table.
5. The CPE router resides on the subscriber company's intranet. Using this arrangement, each subscriber company must specify the static route to their own end-user sign-in address and must specify the MSP's CE router IP as the next-hop gateway in the CPE router's route table.
6. Once the MSP VLAN termination point (in this example, a CE router) determines the intended subscriber intranet, the termination point directs the traffic to the appropriate CPE router, which sends the traffic to the proper resource in the subscriber intranet.

As shown in the following figure, you can configure a static route in the CE router to point to the end-user's IP address, with the next-hop gateway set to the IP address of the subscriber's VLAN port.

Alternately, you can configure a default route on the CE router with the next-hop gateway set to the IP address of the subscriber VLAN port. In this case, you do not need to add individual static routes to the VPN Tunneling IP pool addresses.

You can also allocate an entire network to a VPN Tunneling IP address pool.



1. End-users sign in over an Internet connection using an IP address agreed upon by the MSP and the subscriber company.
2. Specify a static route in the MSP's VLAN termination point (in this example, a CE router) route table to point to the end-user sign-in IP addresses for each subscriber company.
3. You must also specify the next-hop gateway in the CE router's route table.

4. In the CE route table, specify all end-user sign-in IP addresses as static routes, and all corresponding VLAN port IP addresses as defined in the virtualized Secure Access Service.
5. Define at least one unique VLAN ID for each subscriber company. Use the IP addresses of each VLAN as the next-hop gateway addresses in the CE router's route table.
6. The subscribers' CPE routers perform the proper traffic routing to the subscriber company intranets.
7. Each subscriber company must provide sign-in pages for the IP addresses defined as static routes for end-user sign-in.

Once the MSP VLAN termination point (in this example, a CE router) determines the intended subscriber intranet, the termination point directs the traffic to the appropriate CPE router, which sends the traffic to the proper resource in the subscriber intranet.

**Related  
Documentation**

- [About VPN Tunneling on page 734](#)

---

## Configuring a Centralized DHCP Server

---

You can configure one or more centralized DHCP servers if you want to provide VPN Tunneling IVS users with dynamic IP addressing, without requiring each IVS subscriber to support an IVS-specific DHCP server.

The DHCP server maintains separate IP address pools for each IVS, using the IVS name property, defined in the IVS profile, to uniquely identify the IVS-specific pools.

Upon receiving a request from an IVS, the DHCP server selects an IP address based on the IVS name and the IP address of the node from which the request originated, which is delivered in the `giaddr` field of the request. Using this combination of data points, the DHCP server picks an available IP address from the appropriate pool and returns the address in the DHCP offer.

To configure your system to support a centralized DHCP server

The following notes apply to the use of a centralized DHCP server in an IVS configuration:

- You can configure the same DHCP server IP address for VPN Tunneling roles in multiple IVS systems.
  - Within a VPN Tunneling role, if you configure both an NC IP pool and a DHCP server for the same role, the DHCP server takes precedence.
  - DHCP IP address assignment can co-exist with IP address assignment by way of NC IP pools within an IVS.
  - You can employ multiple DHCP servers in the service provider network, with different groups of IVS systems pointing to different central servers.
1. Configure the DHCP server entry in the VPN Tunneling Connection Profile, for each VPN Tunneling role that will acquire IP addresses by way of DHCP.

2. Configure the DHCP server itself, by configuring classes and subclasses on the DHCP server to distinguish between requests from different IVS systems and to provide IP addresses from IVS-specific IP address pools.

To configure the DHCP server entry in the VPN Tunneling Connection Profile

1. In the Root context, choose **Users > Resource Policies > VPN Tunneling**.
2. Click the **VPN Tunneling Connection Profiles** tab.
3. Click **New Profile**.
4. Enter a name for the profile.
5. Under IP address assignment, select the **DHCP Server** radio button.
6. Enter the DHCP server name or IP address.
7. Under Roles, select the applicable roles in the Available roles list box and click **Add** to move them to the Selected roles list box.
8. Click **Save Changes**.
9. Repeat the procedure for each IVS that should use the DHCP server., making sure to enter the same DHCP server name or IP address that you entered for the Root.

**Related  
Documentation**

- [Creating VPN Tunneling Connection Profiles on page 761](#)

## About Authentication Servers

You can configure authentication servers, such as RADIUS and Active Directory, on both the MSP network and the subscriber company intranets. The authentication server authenticates the incoming traffic differently depending on whether the traffic is authenticated when it comes into the MSP network or when it reaches the customer intranet.



**NOTE:** If you connect an authentication server to the internal port, you must set the default VLAN to the internal port when configuring the IVS.

The following authentication servers are supported on a subscriber IVS:

- Local Authentication
- LDAP Server
- RADIUS Server
- Active Directory/Windows NT
- Anonymous Server
- Certificate Server

The following authentication servers are supported on the root system:

- Local Authentication
- LDAP Server
- NIS Server
- ACE Server
- RADIUS Server
- Active Directory/Windows NT
- Anonymous Server
- SiteMinder Server
- Certificate Server

### Rules Governing Access to Authentication Servers

The following rules apply to the access of authentication servers on the MSP network or on the subscriber company network. Each IVS profile must include settings for:

- The default VLAN, which can also be the internal port, if provisioned as the default VLAN.
- The default VLAN interface IP is the source IP address used to contact the authentication server.
- Static routes in the VLAN that point to the appropriate authentication servers, which can reside in the MSP network (with an assigned VLAN ID or untagged on the internal port), or on the subscriber company network.

### Configuring Authentication on a RADIUS Server

You must configure the RADIUS server in each IVS. If you have a RADIUS server on the MSP network as well, all of the IVS RADIUS servers can point to the same MSP RADIUS IP address.

To configure the RADIUS server:

1. Select the context:
  - If you are in an IVS context, and you want to define a RADIUS server on the MSP network, select Root from the context drop down menu in the admin console header bar and click Go.
  - If you are in the root context, and you want to define a RADIUS server on a subscriber intranet, select the IVS name from the context drop down menu in the admin console header bar and click Go.
2. Follow the same steps as you would for configuring a RADIUS server instance.



**NOTE:** In the current release, ACE authentication is not available for individual IVS systems. If you want to use RSA 2 factor token-based authentication, you should use RADIUS from the IVS to access RSA ACE.

## Configuring Authentication on Active Directory

You must configure the AD/NT server in each IVS. If you have an AD/NT server on the MSP network as well, all of the IVS AD/NT servers can point to the same MSP AD/NT IP address.

To configure the Active Directory server:

1. Select the context:
  - If you are in an IVS context, and you want to define an AD/NT server on the MSP network, select Root from the context drop down menu in the admin console header bar and click Go.
  - If you are in the root context, and you want to define an AD/NT server on a subscriber intranet, select the IVS name from the context drop down menu in the admin console header bar and click Go.
2. Follow the same steps as you would for configuring an Active Directory or NT Domain instance.

### Related Documentation

- [Configuring a RADIUS Server Instance on page 191](#)
- [Defining an Active Directory or Windows NT Domain Server Instance on page 164](#)

## Delegating Administrative Access to IVS Systems

As the root administrator, you can delegate administrative access and responsibilities to specific IVS systems. You can delegate read/write access or read-only access to all IVS systems, or to selected IVS systems.

To delegate administrative access to IVS systems

1. Select Administrators > Admin Roles > *Role* where *Role* indicates one of the listed administrator roles. You can also create a new administrator role, if you prefer.
2. Click the **IVS** tab.
3. To give the administrator read/write access to the IVS, select one of the following:
  - To give the administrator read/write access to all IVS systems, select the **Administrator can manage ALL IVSs** checkbox.
  - To limit the administrator's access to specific IVS systems, select the **Administrator can manage SELECTED IVSs** checkbox, then select the IVS systems from the Available IVSs list and click **Add** to move them to the Selected IVSs list.
4. To give the administrator read only access to the IVS, select one of the following:

- If you want to give the administrator read only access to all IVS systems, select the **Administrator can view (but not modify) ALL IVSs** checkbox.
  - If you want to limit the administrator's access to specific IVS systems, select the **Administrator can view (but not modify) SELECTED IVSs** checkbox, then select the IVS systems from the Available IVSs list and click **Add** to move them to the Selected IVSs list.
5. Click **Save Changes**.

By adding these access rights to a given role, you can exercise different levels of control over different MSP administrators.

**Related  
Documentation**

- [Creating and Configuring Administrator Roles on page 1006](#)

---

## Accessing Standalone Installers on an IVS System

The IVS administrator might need to access the Host Checker, WSAM, or other standalone installers. To give IVS administrators access to the installers, which are located on the Maintenance > System > Installers page, you can delegate the access to them by way of the Administrators > Admin Roles > SelectRole > IVS page. Once you have delegated access, the IVS administrator can see the Installers page from within the context of the IVS admin console.

**Related  
Documentation**

- [Downloading Application Installers on page 813](#)

---

## Exporting and Importing IVS Configuration Files

Use the Secure Access Service binary import/export feature to export and import root system and user settings, and also to export and import subscriber IVS settings and profiles. The two types of operations are mutually exclusive: if exporting IVS settings, the exported configuration file does not contain root system settings; if exporting root system settings, the exported configuration file does not contain subscriber IVS settings.

Use the XML import/export feature to export and import system configuration. This feature enables you to make significant changes to your system configuration and provides a number of benefits, particularly when it comes to make a large number of repetitive changes, or when you want to update configuration data all at once.

You perform export and import operations from the context of the root system. On the Maintenance > Import/Export > Import/Export Configuration page, the Maintenance > Import/Export > Import XML and Export XML pages, and on the Maintenance > Import/Export > Import/Export Users page, you can find the standard controls for exporting root system and user configuration. A subscriber IVS administrator cannot export or import data from or to a subscriber IVS. Only you, as the root administrator, can perform these tasks.

Note the following:

- You can only import/export all IVS systems in a single operation. You cannot import/export an individual IVS system's configuration.
- When creating an IVS using XML import, an XML containing the IVS profile should be imported first before importing the IVS configuration.
- The schema for XML import/export of a root IVS (click the Download the schema files link in the XML export page) is different from the XML import/export schema of a non-root IVS.
- You can also use the Secure Access Service binary archiving feature to perform local backups of your IVS system.

### Exporting IVS Configurations

To export IVS configurations:

1. Select **Maintenance > Import/Export > Import/Export IVS**.
2. Enter a password to password protect the configuration file.
3. Click **Save Config As**.
4. Click **Save**.
5. Provide a file name and target location for the file.
6. Click **Save** and **Close**, if necessary.

The saved configuration file contains the following settings for all IVS systems:

- IVS Profiles
- IVS System Settings
- IVS Signing In Settings
- IVS Administrators
- IVS Users
- IVS Resource Policies
- IVS Maintenance Settings

### Importing IVS Configurations

To import IVS configurations:

1. Select **Maintenance > Import/Export > Import/Export IVS**.
2. Click **Browse**.
3. Locate and select the file and click **Open**.
4. Enter a password to password protect the configuration file.

5. To import the network settings in the IVS profile, such as VLAN ports and virtual ports, select the **Import IVS Profile Network Settings** checkbox.



**NOTE:** Importing network settings as described in above only works if you export the system and IVS configurations from the same system.

The network settings themselves do not get imported; only the references to the network settings get imported. Network settings are only imported/exported when importing/exporting the root system settings.

6. Click **Import Config**.

The IVS provides a confirmation message if the import operation succeeds. The IVS then restarts certain services, which may require several minutes.



**NOTE:** You can use the XML Import/Export feature to export and import XML-based configuration files on the root IVS.

You can use Push Config to copy one root IVS configuration to another root IVS. You cannot use Push Config to copy configuration data between subscriber IVS systems or from a root IVS to a subscriber IVS.

**Related Documentation**

- [Importing and Exporting XML Configuration Files on page 901](#)

---

## Using XML Import and XML Export on IVS Systems

---

XML import and export provides a way to make a large number of repetitive changes all at once by importing and exporting system configuration. As with the binary import/export, a subscriber IVS administrator cannot export or import data from or to a subscriber IVS. Only the root administrator can perform this task. You can not create or delete an IVS through XML import.

The process for importing and exporting IVS system configuration is the same as for Secure Access Service and will not be described here. Note that you will see fewer XML export options on the IVS as compared to Secure Access Service as not all Secure Access Service options are applicable to IVS.

As with Secure Access Service, some services might be restarted after performing an IVS XML import due to changes in configuration. The following configuration changes result in service restarts:

- NCP option changes
- Windows/UNIX file browsing config changes
- Security option changes



The IVS root administrator can restrict IVS administrators from changing configuration data that can cause service restarts (both from the admin console and through XML import) by selecting **System > Virtual Systems > Virtual Systems** and then selecting the **Restrict IVS administrator access to configuration without system-wide impact** option.

**Related Documentation**

- [Importing and Exporting XML Configuration Files on page 901](#)

## Monitoring Subscribers

Log files contain detailed information about events, user access, administrator access and more. The log entries specify the context of each entry, whether the entry was caused by a root action or an action on one of the IVS systems. The root entries contain the word **Root**. For example, the following entries show access by two administrators, the first being **Root** and the second, an administrator called **Test**:

```
ADM20716 2005-05-10 10:52:19 - ive - [10.11.254.160]
Root::administrator(administrator Users)[.Administrators] - User Accounts modified.
Added Unspecified Name with username testuser1 to authentication server System
Local.
```

```
Info ADM20716 2005-05-10 10:35:26 - ive - [10.11.254.160]
Test::administrator(administrator Users)[.Administrators]!Root - User Accounts
modified. Added IVE Platform Administrator with username omiadmin to authentication
server Administrators.
```

### Suspending Subscriber Access to the IVS

To suspend subscriber access to the IVS:

1. Select **System > Virtual Systems**.
2. Click the **Disabled** radio button.

By performing this step, you make the IVS unavailable to any user of the IVS, including the IVS administrator. To provide access to the IVS, set the radio button to the **Enabled** state.

**Related Documentation**

- [Virtual Local Area Network \(VLAN\) on Subscriber IVS on page 1028](#)

## Troubleshooting VLANs

In addition to the standard troubleshooting features provided by the Secure Access Service, the virtualized Secure Access Service provides several enhancements, specifically for managing IVS systems. You can use the following troubleshooting features on either the root system or each IVS, separately:

- Policy simulation
- Policy tracing
- Session recording

Functionally, these utilities are the same as the standard Secure Access Service capabilities. The key difference is a matter of context. If you initiate one of these three utilities from the root system context, you get results for users, policies, and sessions on the root system or from the MSP network. If you initiate the utilities from a subscriber IVS context, you get results for users, policies, and sessions on the IVS or the subscriber intranet.

The TCPDump, Ping, Traceroute, NSLookup, and ARP commands are enhanced for use in virtualized Secure Access Service systems. You can initiate these commands on the internal and external ports, as well as on selected VLAN ports, which you might do if you want to troubleshoot traffic on a subscriber VLAN. The basic functionality of the commands is unchanged, except for the ability to specify a VLAN port

### Running TCPDump on a VLAN

To perform a TCPDump on a VLAN:

1. If you are not in the root system context, select **Root** from the IVS drop down menu in the admin console header, and then click **Go**.
2. Choose **Maintenance > Troubleshooting > Tools > TCP Dump**.
3. With Internal Port selected, select the VLAN from the VLAN Port drop down menu.
4. (optional) Add a filter to the Filter text box.
5. Click **Start Sniffing**.
6. To retrieve the results, click **Stop Sniffing**.
7. Choose the type of Dump file from the Dump File drop down menu.
8. Click **Get**.
9. Open the file with the appropriate editor.

### Using Ping, traceroute, NSLookup, ARP Commands on a VLAN

1. If you are not in the root system context, select **Root** from the IVS drop down menu in the admin console header, and then click **Go**.
2. Choose **Maintenance > Troubleshooting > Tools > Commands**.
3. Select a command from the Command drop down menu.
4. Enter the target server.
5. Select the VLAN from the VLAN Port drop down menu.
6. Enter the other settings, depending on the command you choose.
7. Click **OK**.

#### Related Documentation

- [About Troubleshooting on page 959](#)
- [Creating TCP Dump Files on page 965](#)

## IVS Use Case: Policy Routing Rules Resolution

This use case illustrates how policy routing takes place in an MSP deployment. The first part of the use case details two subscriber company configurations and how end-users access their respective subscriber company networks. The second part of the use case describes what happens when you create a VLAN on the MSP network to provide shared services to the subscriber companies' end-users.

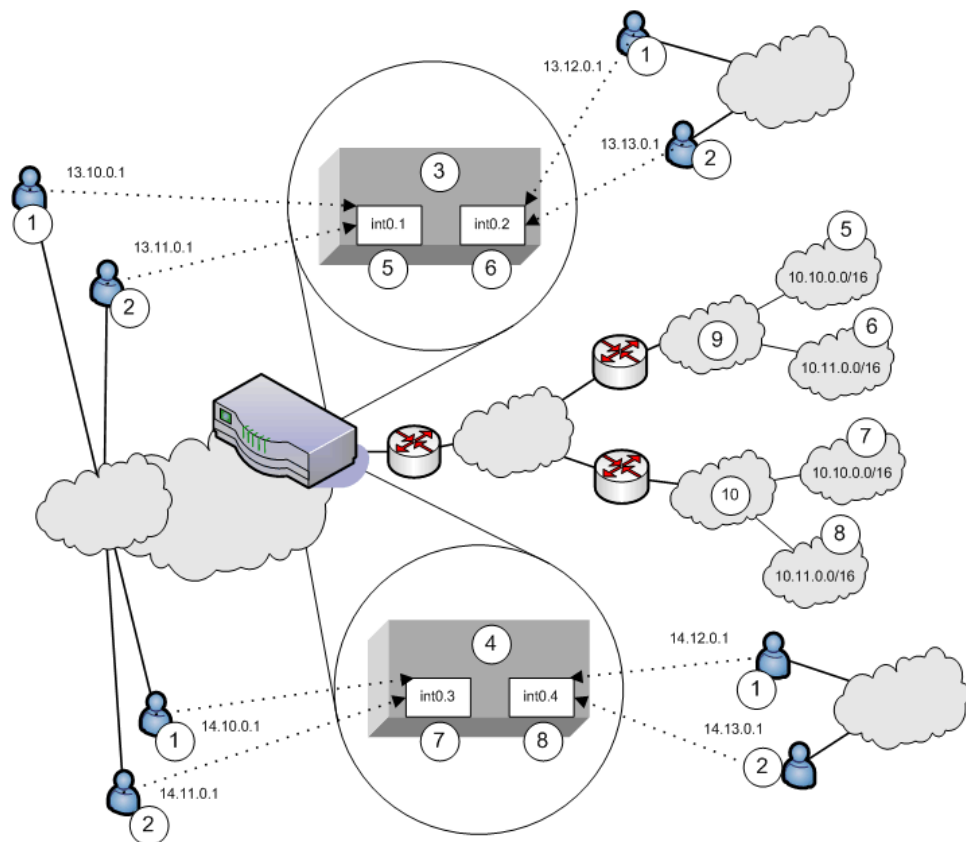
Company 1 and Company 2 are hosted companies on the MSP network. The following table shows the VLANs, VLAN IDs, interfaces and roles defined for each company. Company 1 has defined two VLANs, one for Sales and one for Human Resources. Each company has an associated role defined for each VLAN. The root administrator creates each VLAN, providing a unique VLAN ID for each, and indicating a given port. In this case, the root administrator has created all four VLANs on the internal interface

	VLAN	VLAN ID	Interface	Role
Company 1	Sales	1	int0.1	SALES
	HR	2	int0.2	HR
Company 2	Employee	3	int0.3	EMPLOYEE
	Partner	4	int0.4	PARTNER



**NOTE:** The labels for ports have been changed. The port name eth0 (internal port) is now called int0 and eth1 (external port) is now ext0. You can only see the route table device names (such as int0.1) from the serial console. You can view the route table by selecting menu item 1, then menu item 2 from the serial console.

The following figure illustrates the MSP and subscriber company deployments.



**NOTE:** IVS VLANs are not explicitly tied to subscriber intranets by configuration on the Secure Access Service. The association of a VLAN to a subscriber intranet is accomplished by mapping VLAN interfaces to private tunnels in the subscriber intranet within the CE->CPE router framework.

In the above figure, VPN Tunneling end-users get their source IP addresses from configured VPN Tunneling IP address pools that the root administrator has defined for the IVS. Also, in the figure, non-VPN Tunneling users can still access specified realms based on their roles and on role-based source IP (VIP sourcing) addresses that you define as virtual ports on the VLAN.

The following list describes each item that is marked with a numbered label in the above figure.

The following list describes each item that is marked with a numbered label in the above figure.

1. VPN Tunneling end-users get IP addresses from VPN Tunneling IP pools. Traffic from these users is routed through the appropriate subscriber VLAN, which you define on the internal port.
2. Non-VPN Tunneling end-users get IP addresses from virtual IP (VIP) pools. Traffic from these users is sourced through the appropriate subscriber VLAN.

3. In Figure 67, this numbered box represents a subscriber IVS, which contains two VLANs that are defined on ports int0.1 and int0.2.
4. In Figure 67, this numbered box represents a second subscriber IVS, which contains two VLANs that are defined on ports int0.3 and int0.4.
5. The subscriber defines a role for “Sales” on VLAN1. End-users signing in to IP 13.10.0.1 over the Internet are routed to the Company 1 intranet, to the appropriate backend resources located in the “Sales” realm at 10.10.0.0/16. End-users signing in on IP 13.11.0.1 are VIP sourced to the Company 1 intranet, also to the appropriate backend resources located in the “Sales” realm at 10.10.0.0/16.
6. The subscriber defines a role for “HR” on VLAN2. End-users signing in on IP 13.12.0.1 over the Internet are routed to the Company 1 intranet, to the appropriate backend resources located in the “HR” realm at 10.11.0.0/16. End-users signing in on IP 13.13.0.1 are VIP sourced to the Company 1 intranet, also to the appropriate backend resources located in the “HR” realm at 10.11.0.0/16.
7. The subscriber defines a role for “Employee” on VLAN3. End-users signing in on IP 14.10.0.1 over the Internet are routed to the Company 2 intranet, to the appropriate backend resources located in the “Employee” realm at 10.10.0.0/16. End-users signing in on IP 14.11.0.1 are VIP sourced to the Company 2 intranet, also to the appropriate backend resources located in the “Employee” realm at 10.10.0.0/16.
8. The subscriber defines a role for “Partner” on VLAN4. End-users signing in on IP 14.12.0.1 over the Internet are routed to the Company 2 intranet, to the appropriate backend resources located in the “Partner” realm at 10.11.0.0/16. End-users signing in on IP 14.13.0.1 are VIP sourced to the Company 2 intranet, also to the appropriate backend resources located in the “Partner” realm at 10.11.0.0/16.
9. The Company 1 intranet supports two realms: “Sales” at 10.10.0.0/16 and “HR” at 10.11.0.0/16. These realms correspond to the roles defined on VLAN1 and VLAN2/
10. The Company 2 intranet supports two realms: “Employee” at 10.10.0.0/16 and “Partner” at 10.11.0.0/16.



**NOTE:** The realms are valid even though they contain overlapping IP addresses. Because the roles are defined for different VLANs, the VLAN IDs provide the separation that allows them to overlap without danger of mixed traffic.

The route tables for each VLAN appear as follows:

**Table 62: VLAN1 Route Table**

Destination IP	Gateway	Output Port
0.0.0.0	Default gateway on VLAN1	int0.1
10.10.0.0/16	0.0.0.0	int0.1

Table 63: VLAN2 Route Table

Destination IP	Gateway	Output Port
0.0.0.0	Default gateway on VLAN2	int0.2
10.10.0.0/16	0.0.0.0	int0.2

Table 64: VLAN3 Route Table

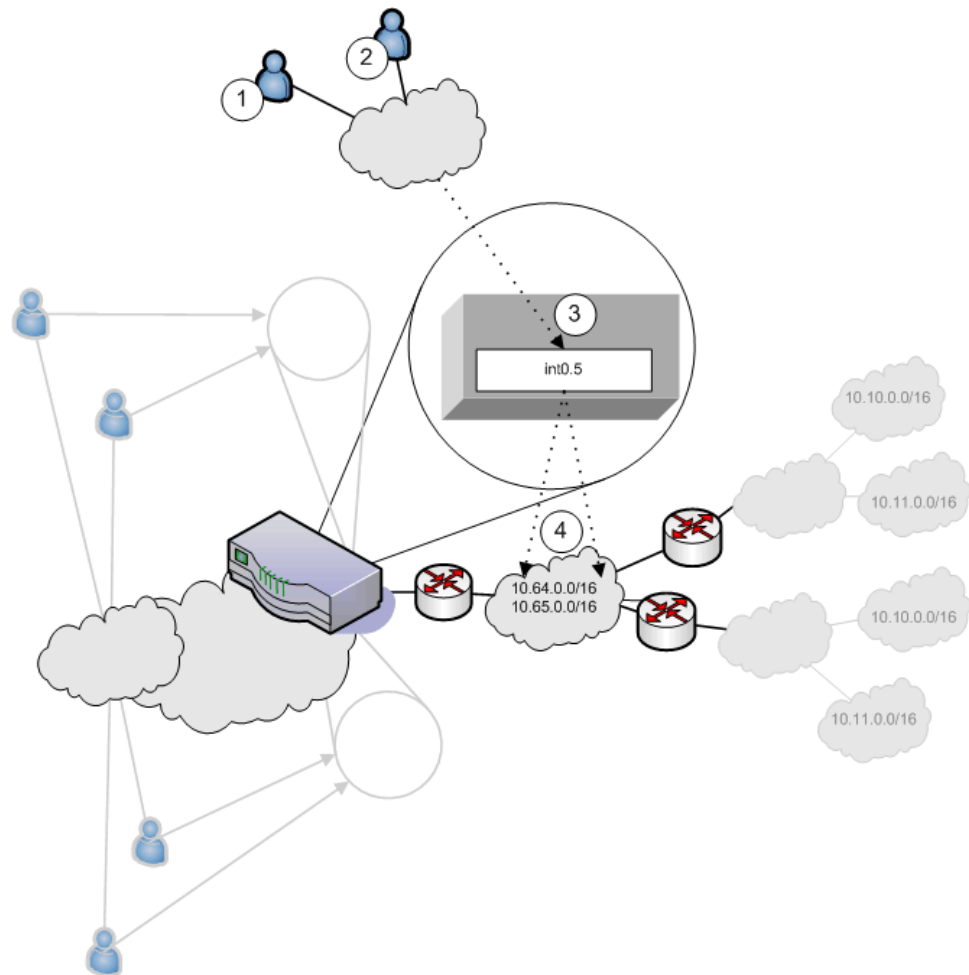
Destination IP	Gateway	Output Port
0.0.0.0	Default gateway on VLAN3	int0.3
10.10.0.0/16	0.0.0.0	int0.3

Table 65: VLAN4 Route Table

Destination IP	Gateway	Output Port
0.0.0.0	Default gateway on VLAN4	int0.4
10.10.0.0/16	0.0.0.0	int0.4

Now consider the situation in which the MSP decides to provide shared services to end-users of Company 1 and Company 2. Assume the MSP network is also on a VLAN (VLAN5). If you want to provide services on 10.64.0.0/16 to both Company 1 and Company 2, and services on 10.65.0.0/16 to Company 2 only, you can configure either VPN Tunneling pools or virtual ports for those addresses.

Figure 68 illustrates this situation. Some details from this figure have been removed or greyed out to improve readability.



1. Company 1 end-users sign-in over the Internet to the MSP network and the MSP VLAN, VLAN5 (represented as number 3 in the illustration).
2. Company 2 end-users sign-in over the Internet to the MSP network and the MSP VLAN, VLAN5 (represented as number 3 in the illustration).
3. The MSP VLAN5 provides access to shared services on the MSP network.
4. You must define separate IP addresses for each subscriber company's end-users, even though they share MSP services.

Once you configure routes to support users who have access to shared services on the MSP network and to support users who also have access to restricted MSP network services, the VLAN route tables appear as follows.

**Table 66: VLAN1 Route Table**

Destination IP	Gateway	Output Port
0.0.0.0	Default gateway on VLAN1	int0.1
10.64.0.0	Router on VLAN5	int0.5

Table 67: VLAN2 route table

Destination IP	Gateway	Output Port
0.0.0.0	Default gateway on VLAN2	int0.2
10.64.0.0	Router on VLAN5	int0.5

Table 68: VLAN3 route table

Destination IP	Gateway	Output Port
0.0.0.0	Default gateway on VLAN3	int0.1
10.64.0.0	Router on VLAN5	int0.5
10.65.0.0	Router on VLAN5	int0.5

Table 69: VLAN4 route table

Destination IP	Gateway	Output Port
0.0.0.0	Default gateway on VLAN4	int0.2
10.64.0.0	Router on VLAN5	int0.5
10.65.0.0	Router on VLAN5	int0.5

If the MSP network is connected to the untagged port (internal), the route entries are similar, but the output port is int0 only.

**Related Documentation**

- [IVS Provisioning Process Overview on page 1025](#)

## Use Case: Configuring a Global Authentication Server for Multiple Subscribers

If your subscriber companies prefer to lease or purchase authentication services from you, the service provider, you can configure a global authentication server on your network. In that case, you must perform several tasks:

1. Configure one or more authentication servers on your MSP network.
2. Configure path-based URLs or virtual ports for sign-in on your MSP network.
3. Configure VLANs and IVS systems to map to the authentication servers on the MSP network.

**Related Documentation**

- [IVS Provisioning Process Overview on page 1025](#)



---

## Use Case: Configuring a DNS/WINS Server IP Address per Subscriber

---

If you want to configure a particular DNS/WINS server IP address per subscriber, you can do so from within each IVS.

To configure a DNS/WINS server IP address:

1. Configure your IVS systems.
2. Select an IVS from the system drop down menu in the admin console header area and then click **Go**. Within the IVS context, the header color changes and displays the name of the subscriber.
3. Select **System > Network > Overview**.
4. Enter the DNS/WINS settings that correspond to the DNS/WINS server on the subscriber intranet.
5. Click **Save Changes**.

**Related Documentation** • [IVS Provisioning Process Overview on page 1025](#)

---

## Use Case: Configuring Access to Web Applications and Web Browsing for Each Subscriber

---

The IVS administrator may want to configure specific Web browsing policies for the IVS end-users.

To configure Web browsing access, the IVS administrator needs to configure the following pages:

- Users > User Roles > *RoleName* > Web
- Users > Resource Policies > Web

### Configuring Web Browsing Access

To configure Web browsing access:

1. Choose **Users > User Roles > RoleName > Web**.
2. Select the **Bookmarks** tab.
3. Click **New Bookmark**.
4. Supply settings to configure the bookmark to a given Web URL.
5. Click **Save Changes** or **Save + New** if you want to add multiple bookmarks.

The bookmarks you define here appear in the Secure Access Service Web bookmarks section to which end-users have access.

6. Select the **Options** tab.
7. Select the Web browsing privileges you want to provide to your end-users.

8. Choose the other options you want, including setting the timeout value for the HTTP connection.
9. Click **Save Changes**.

### Configuring Web Browsing Access Policies

To configure Web browsing access policies:

1. Choose **Users > Resource Policies > Web**.
2. Supply the appropriate settings on each of the tabs.

#### Related Documentation

- [IVS Provisioning Process Overview on page 1025](#)

---

## Use Case: Configuring File Browsing Access for Each Subscriber

---

The IVS administrator may want to configure specific file-browsing access policies for the IVS end-users. The IVS administrator can perform this type of operation based on roles.

To configure file browsing, the IVS administrator needs to configure the following pages:

- Users > User Roles > *RoleName* > General
- Users > User Roles > *RoleName* > Files
- Users > Resource Policies > Files

### Configuring File Browsing Access

To configure file browsing access:

1. Choose **Users > User Roles > RoleName > General**.
2. Under Access Features, select the **Files** checkbox (for Windows).
3. Click **Save Changes**.
4. Select the **Files** tab.
5. Select the **Options** page.
6. Depending on the file system type, select the options that apply to the IVS end-user access.
7. Click **Save Changes**.

### Configuring File System Access Policies

To configure file system access policies:

1. Make sure you are in the IVS context. If the IVS drop down menu in the admin console header bar displays Root, select the IVS name from the menu and click Go.
2. Select **Users > Resource Policies > Files > Access > Windows**.

3. Choose the role from the Show policies that apply to drop down menu, and click **Update**.
4. Click **New Policy**.
5. Supply the appropriate settings.
6. Click **Save Changes**.
7. Select the Credentials tab.
8. Supply the appropriate settings.
9. Click **Save Changes**.
10. Repeat these steps for each role.
11. Select the **Encoding** tab to select the language encoding and click **Save Changes**.
12. Select the **Options** tab to set options, such as IP based matching for Hostname based policy resources and click **Save Changes**.



**NOTE:** UNIX/NFS file resource policies are supported only on the root IVS.

**Related  
Documentation**

- [IVS Provisioning Process Overview on page 1025](#)

## Use Case: Setting Up Multiple Subnet IP Addresses for a Subscriber's End-Users

Assume that the subscriber wants to create subnets within the intranet to support traffic separation between subscriber end-users from three different departments: Marketing, Finance, and Engineering. The procedures needed to accomplish this task are divided between those performed by the root administrator and those performed by the IVS administrator.

### Tasks Performed by the Root Administrator

1. Create subscriber VLAN.
2. Create subscriber IVS.
3. Create path-based URLs or virtual ports for sign-in.
4. Create virtual ports for role-based source IP aliasing.

### Tasks Performed by the IVS Administrator

1. Create users.
2. Assign roles to VLAN/Source IP.
3. Assign users to roles.

**Related  
Documentation**

- [IVS Provisioning Process Overview on page 1025](#)
- [Configuring VLANs on the Virtualized Secure Access Service on page 1029](#)

- [Creating a Virtual System \(IVS Profile\) on page 1032](#)
- [Using Virtual Ports on page 802](#)
- [About Role-Based Source IP Aliasing on page 1037](#)
- [User Roles Overview on page 105](#)
- [Associating Roles with Source IP Addresses in an IVS on page 1037](#)
- [Creating User Accounts on a Local Authentication Server on page 186](#)

## Use Case: Configuring Multiple IVS Systems to Allow Access to Shared Server

There may be cases in which you want to provide end-users of multiple subscriber companies to access a shared server on the MSP network.

The following steps describe a simple use case and solutions.

### **Solution #1**

To configure access to a shared server, assuming two IVS systems for two subscribers:

1. Add the internal port to the IVS1 list of selected VLANs.
2. Add the internal port to the IVS2 list of selected VLANs.
3. Edit the internal port's route table and configure a static route pointing to the shared server, with the internal interface as the output port.

### **Solution #2**

To configure access to a shared server, assuming two IVS systems for two subscribers:

1. Add VLAN1 to the IVS1 selected VLAN list and set it as the default VLAN.
2. Add VLAN2 to the IVS2 selected VLAN list and set it as the default VLAN.
3. Edit the route tables for both VLAN1 and VLAN2 and configure a static route in each that points to the shared server, with the internal interface as the output port.

### **Related Documentation**

- [Configuring VLANs on the Virtualized Secure Access Service on page 1029](#)
- [IVS Provisioning Process Overview on page 1025](#)
- [Creating a Virtual System \(IVS Profile\) on page 1032](#)

## CHAPTER 38

# IPv6 Support

- [Understanding IPv6 on page 1065](#)
- [IPv6 Support Overview on page 1069](#)
- [IPv6 Feature Configuration Task Summary on page 1075](#)
- [Managing the Neighbor Discovery Cache on page 1077](#)
- [Example: Creating a Cluster That Supports IPv6 Client Access on page 1077](#)

## Understanding IPv6

---

IP version 6 (IPv6) is an Internet Protocol designed to succeed IP version 4 (IPv4). This topic provides an overview of IPv6. It includes the following information:

- [About IPv6 on page 1065](#)
- [About IPv6 Address Types on page 1066](#)
- [About IPv6 Address Text Representation on page 1066](#)
- [About the IPv6 Unspecified Address on page 1067](#)
- [About the IPv6 Loopback Address on page 1067](#)
- [About IPv6 Address Prefixes on page 1067](#)
- [System Normalization of IPv6 Addresses on page 1067](#)
- [About Neighbor Discovery Protocol on page 1068](#)

## About IPv6

The ongoing expansive growth of the Internet and the need to provide IP addresses to accommodate it is escalating the emergent use of a new IP protocol. IPv6 was designed to satisfy the current and anticipated near future requirements.

IPv4 is widely used throughout the world today for the Internet, intranets, and private networks. IPv6 builds upon the functionality and structure of IPv4 in many aspects, including:

- **Larger address space**—IPv6 addresses are 128 bits long instead of 32 bits. This expands the address space from 4 billion addresses to over 300 trillion trillion addresses.
- **New datagram format**—The packet header is both simplified and enhanced to enable more secure and efficient routing.

- Improved fragmentation and reassembly—The maximum transmission unit (MTU) has been increased to 1280 bytes, for example.
- Transition mechanisms—Various network address translation (NAT) and tunneling mechanisms have been developed to support the transition to IPv6.

On February 3, 2011 Internet Assigned Numbers Authority (IANA) allotted the last block of IPv4 addresses to Regional Internet Registries (RIR), so the free pool of IPv4 addresses is now fully depleted. It is expected that in the near future Internet service providers (ISPs) will start issuing IPv6 addresses to their customers.

## About IPv6 Address Types

[RFC 4291, IP Version 6 Addressing Architecture](#), describes the following types of IPv6 addresses:

- Unicast. An identifier for a single interface. A packet sent to a unicast address is delivered to the interface identified by that address.
- Anycast. An identifier for a set of interfaces. A packet sent to an anycast address is delivered to *one* of the interfaces identified by that address.
- Multicast. An identifier for a set of interfaces. A packet sent to a multicast address is delivered to *all* interfaces identified by that address.

The *link-local address* is a special IPv6 unicast address that is used in self-traffic and essential network communication, like Neighbor Discovery Protocol (NDP). When you enable IPv6 on a Secure Access Service interface, the system generates a link-local address that is derived from the interface MAC address.

When you configure IPv6 addresses for the Secure Access Service interfaces, you manually specify a routable address, such as *global unicast address* or an *anycast address*, depending on your routing implementation and your Secure Access Service deployment. A global unicast address must be globally unique so that it can be specified globally without need for modification. An anycast address represents a service rather than a specific device. An anycast address is not unique, but instead might be configured on each device in a cluster. You are not likely to use multicast addressing with the Secure Access Service.

## About IPv6 Address Text Representation

All IPv6 addresses are 128 bits long, written as 8 sections of 16 bits each. They are expressed in hexadecimal representation, so the sections range from 0 to FFFF. Sections are delimited by colons, and leading zeroes in each section may be omitted. If two or more consecutive sections have all zeroes, they can be collapsed to a double colon.

IPv6 addresses consist of 8 groups of 16-bit hexadecimal values separated by colons (:). IPv6 addresses have the following format:

```
aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa:aaaa
```

Each *aaaa* is a 16-bit hexadecimal value, and each *a* is a 4-bit hexadecimal value. The following is a sample IPv6 address:

```
2001:0DB8:0000:0000:0008:0800:200C:417A
```

You can omit the leading zeros of each 16-bit group, as follows:

```
2001:DB8:0:0:8:800:200C:417A
```

You can compress 16-bit groups of zeros to double colons (::) as shown in the following example, but only once per address:

```
2001:DB8::8:800:200C:417A
```

### About the IPv6 Unspecified Address

In the IPv6 address space, the special “unspecified address” is 0:0:0:0:0:0:0:0. The compressed representation of the unspecified address is the double-colon (::). The unspecified address must never be assigned to a physical or virtual interface.

### About the IPv6 Loopback Address

The special loopback address is the unicast address 0:0:0:0:0:0:0:1. The compressed representation of the loopback address is ::1. The loopback address may be used by a node to send an IPv6 packet to itself. It must not be assigned to a physical or virtual interface. In Release 7.3 and Release 7.4, the loopback address shown in Secure Access Service Event logs is the special IPv4 loopback address (127.0.0.1). The IPv6 loopback address (::1) is not used in Event logs.

### About IPv6 Address Prefixes

An IPv6 address prefix is a combination of an IPv6 prefix address and a prefix length used to represent a block of address space (or a network), similar to the use of an IPv4 subnet address and netmask combination to specify a subnet. An IPv6 address prefix takes the form *ipv6-prefix/prefix-length*. The *ipv6-prefix* variable follows general IPv6 addressing rules. The */prefix-length* variable is a decimal value that indicates the number of contiguous, higher-order bits of the address that make up the network portion of the address. For example, 2001:DB8::/32 is an IPv6 address prefix, indicating that the first 32 bits make up the network portion of the address.

### System Normalization of IPv6 Addresses

The Secure Access Service validates and normalizes IPv6 addresses entered by administrators. The normalized address is the address processed by the system, and it is the address that appears in logs.

[Table 70 on page 1067](#) gives examples of how the Secure Access Service system normalizes IPv6 address entries.

**Table 70: System Normalization of IPv6 Addresses**

Example Entry	Normalized Address	Explanation
2001:DB8:1:1::3	2001:DB8:1:1::3	An address specified in compressed format is validated; the system uses the compressed form as the normalized form.
0:0:0::122	::122	Address is validated and normalized to compressed format.
FF01:0:0:0:0:0:101	FF01::101	Address is validated and normalized to compressed format.

Table 70: System Normalization of IPv6 Addresses (*continued*)

Example Entry	Normalized Address	Explanation
2001:DB8::10.204.50.122	2001:DB8::ACC:327A	Address is validated and normalized to hexadecimal representation.
::FFFF:10.204.50.122	::FFFF:10.204.50.122	An address specified in compressed format is validated; the system uses the compressed form as the normalized form.

## About Neighbor Discovery Protocol

**Neighbor discovery protocol** (NDP) allows different nodes on the same link to advertise their existence to their neighbors, and to learn about the existence of their neighbors.

Routers and hosts (nodes) use NDP messages to determine the link-layer addresses of neighbors that reside on attached links and to overwrite invalid cache entries. Hosts also use NDP to find neighboring routers that can forward packets on their behalf.

In addition, nodes use NDP to actively track the ability to reach neighbors. When a router (or the path to a router) fails, nodes actively search for alternatives to reach the destination.

IPv6 NDP corresponds to a number of the IPv4 protocols — ARP, ICMP Router Discovery, and ICMP Redirect. However, NDP provides many improvements over the IPv4 set of protocols. These improvements address the following:

- Router discovery—How a host locates routers residing on an attached link.
- Prefix discovery—How a host discovers address prefixes for destinations residing on an attached link. Nodes use prefixes to distinguish between destinations that reside on an attached link and those destinations that it can reach only through a router.
- Parameter discovery—How a node learns various parameters (link parameters or Internet parameters) that it places in outgoing packets.
- Address resolution—How a node uses only a destination IPv6 address to determine a link-layer address for destinations on an attached link.
- Next-hop determination—The algorithm that a node uses for mapping an IPv6 destination address into a neighbor IPv6 address (either the next router hop or the destination itself) to which it plans to send traffic for the destination.
- Neighbor unreachability detection—How a node determines that it can no longer reach a neighbor.
- Duplicate address detection—How a node determines whether an address is already in use by another node.

A router periodically multicasts a router advertisement from each of its multicast interfaces, announcing its availability. Hosts listen for these advertisements for address autoconfiguration and discovery of link-local addresses of the neighboring routers. When a host starts, it multicasts a router solicitation to ask for immediate advertisements.



The router discovery messages do not constitute a routing protocol. They enable hosts to discover the existence of neighboring routers, but they are not used to determine which router is best to reach a particular destination.

NDP uses the following Internet Control Message Protocol version 6 (ICMPv6) messages: router solicitation, router advertisement, neighbor solicitation, neighbor advertisement, and redirect.

NDP for IPv6 replaces the following IPv4 protocols: Router Discovery (RDISC), Address Resolution Protocol (ARP), and ICMPv4 redirect.

#### Related Documentation

- [IPv6 Support Overview on page 1069](#)
- [IPv6 Feature Configuration Task Summary on page 1075](#)
- [Juniper Networks Day One: Exploring IPv6](#)

## IPv6 Support Overview

This topic describes Junos Pulse Secure Access Service support for IP Version 6 (IPv6) networks. It includes the following information:

- [Client Access Summary on page 1069](#)
- [Network Topologies on page 1070](#)
- [IPv6 Support and Limitations for Secure Access Service Features on page 1071](#)

### Client Access Summary

Secure Access Service Release 7.4 supports use of VPN Tunneling Connection Profile features to enable dual-stack endpoints to connect the Secure Access Service and access corporate network IPv4 and IPv6 resources. [Table 71 on page 1069](#) summarizes supported access scenarios.

**Table 71: Secure Access Service Release 7.4 Client Access Scenarios**

Endpoint	SA Interface	Resource Access	Description of the Connection
IPv4	IPv4	IPv4/IPv6	Access to IPv6 resources using VPN Tunneling connection profiles only.
IPv6	IPv6	IPv4	ISP connectivity is end-to-end IPv6 or uses 6to4, Teredo, or other client-side mechanism to make a connection to the SA IPv6 interface. Access to IPv6 resources is not supported.
IPv6	IPv4	IPv4	Uses NAT64, NATPT, or DS-Lite to make a connection to the SA IPv4 interface. Access to IPv6 resources is not supported.
IPv4	IPv6	—	Not supported. An IPv4-only endpoint cannot connect to the Secure Access Service IPv6 interface.

## Network Topologies

Secure Access Service Release 7.4 supports Junos Pulse client access to the IPv6 corporate network using VPN Tunneling Connection Profile features.

Figure 77 on page 1070 shows a dual-stack-enabled endpoint that has been assigned an IPv4 address by its ISP. The endpoint might also have an IPv6 assigned to it by the ISP, but it uses the IPv4 address to connect to the Secure Access Service IPv4 interface. The role-based VPN Tunneling Connection Profile determines whether IPv4 and IPv6 addresses can be assigned to the Junos Pulse client virtual adapter. To enable access to IPv4 resources, the user must map to a role with a VPN Tunneling Connection Profile that includes an IPv4 address assignment configuration. All connection options and resource policies are supported for access to IPv4 resources.

To enable access to IPv6 resources, the user must map to a role with a VPN Tunneling Connection Profile that includes an IPv6 address assignment configuration. In addition, to support access to IPv6 resources, the DNS server used by the Secure Access Service must be reachable by IPv4 and must be able to resolve both A and AAAA DNS queries. Only the VPN Tunneling Connection Profile is supported for access to IPv6 resources. All other connection options and resource policies are not supported for access to IPv6 resources.

Depending on your configuration, the endpoint might be assigned two virtual IP addresses, but both IPv4 and IPv6 traffic are transported through a single VPN tunnel.

Figure 77: IPv4 Endpoint Access to IPv6 Resources

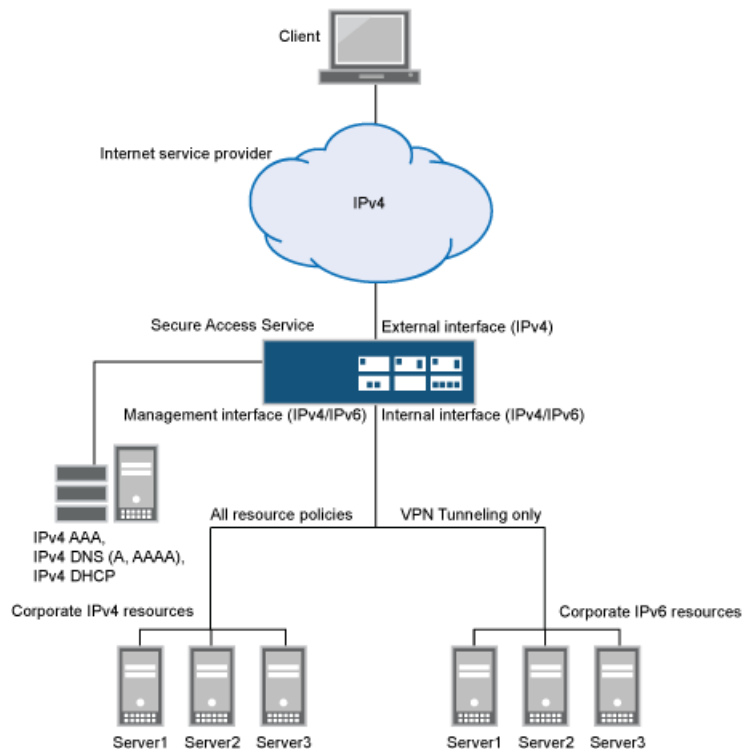
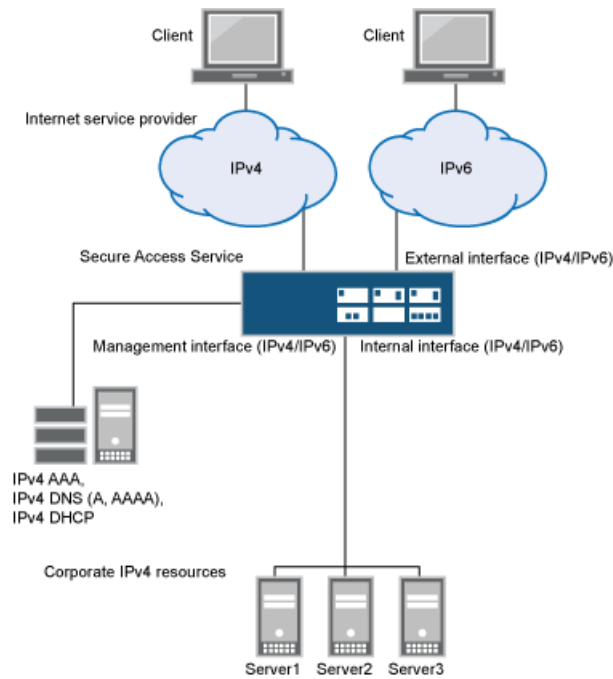


Figure 78 on page 1071 shows dual-stack endpoints that might have been assigned an IPv4 address, an IPv6 address, or both by their Internet service provider. These endpoints can connect to the Secure Access Service IPv4 or IPv6 interface. All connection and resource policy options are supported for access to IPv4 resources.

In Release 7.3 and Release 7.4, an endpoint can use its IPv6 address to connect to the Secure Access Service IPv6 interface. You can use the VPN Tunneling connection profile to assign the Junos Pulse client virtual adapter an IPv4 address so that it can access corporate IPv4 resources. However, when connected to the IPv6 interface, the endpoint cannot access IPv6 resources.

Figure 78: IPv6 Endpoint Access to IPv4 Resources



## IPv6 Support and Limitations for Secure Access Service Features

Table 72 on page 1072 summarizes IPv6 support and limitations for Secure Access Service features for Release 7.4.

Table 72: Summary of IPv6 Support

Feature	Release 7.4
Junos Pulse client access	<p>Only the Junos Pulse client supports IPv6. The legacy Network Connect client does not support IPv6. The following behavior is expected for this release:</p> <ul style="list-style-type: none"> <li>• Endpoints must have dual-stack enabled in order to access IPv6 resources over IPv4 networks.</li> <li>• VPN Tunneling Connection Profiles support IPv4 and IPv6 address pools.</li> <li>• VPN Tunneling Connection Profiles do not support ESP mode for IPv6 resource access. If a connection is configured for ESP mode, the tunnel created for IPv4 traffic uses ESP mode and the tunnel created for IPv6 traffic automatically falls back to use SSL mode.</li> <li>• On dual-stack endpoints, VPN Tunneling split tunneling rules are supported for IPv4-based routes only. The IPv4 traffic allowed by a split tunneling policy is forwarded to the Secure Access Service in an IPv4/IPv6 tunnel.</li> <li>• VPN Tunneling features are not supported for IPv6 in the IVS.</li> <li>• Junos Pulse SAM, Legacy WSAM, and Legacy JSAM do not support IPv6.</li> </ul> <p>Junos Pulse clients on the following platforms support VPN Tunneling connections for IPv6 resource access:</p> <ul style="list-style-type: none"> <li>• Windows 7 (32 and 64 bit)</li> <li>• Windows 8 (32 and 64 bit)</li> <li>• Mac OS/X Snow Leopard, Lion, Mountain Lion</li> </ul> <p>Junos Pulse clients on Windows XP do not support VPN Tunneling connections for IPv6 resource access.</p> <hr/> <p>Host Checker supports IPv6. Third-party Host Checker functionality is supported to the extent that it is IPv6-capable. For example, the following third-party components might require endpoints to connect over IPv4:</p> <ul style="list-style-type: none"> <li>• Downloading antivirus signature updates from third-party vendors</li> <li>• Downloading Windows Patches from Microsoft download servers.</li> <li>• Downloading WebRoot signature updates for EES.</li> </ul> <hr/> <p>Pulse Collaboration does not support IPv6.</p>
Administrator and management access	<p>The internal interface and management interface can be configured with an IPv4 address or dual stack (IPv4 and IPv6). The internal interface and management interface cannot be configured with only an IPv6 address because the system uses IPv4 for the connections with network services, including AAA, DHCP, and DNS.</p> <p>Typically, administrators access the administrator GUI through the internal interface or management interface, but you may enable administrator access through the external interface on the Authentication &gt; Admin Realms &gt; Admin Users &gt; Authentication Policy &gt; Source IP page.</p>
Configuration through the serial console	You cannot view or configure IPv6 network settings with the serial console.
External interface configuration	IPv4, IPv6, or both is supported.

Table 72: Summary of IPv6 Support (*continued*)

Feature	Release 7.4
Internal interface configuration	IPv4 or both is supported. In other words, the internal interface must be configured for IPv4 connections; in addition, it may be configured for IPv6 connections. It may not be configured for IPv6 only.
Management interface configuration	IPv4 or both is supported. In other words, the internal interface must be configured for IPv4 connections; in addition, it may be configured for IPv6 connections. It may not be configured for IPv6 only.
Virtual interface configuration	An interface alias may include IPv4 addresses, IPv6 addresses, or both. However, the corresponding IP protocol must be enabled on the physical interface for the address(es) to take effect.
VLAN configuration	IPv4-only.
Clustering	<p>This release supports IPv6 configuration for active/active clusters. The existing intracluster communication mechanism is preserved. The intracluster communication occurs over the IPv4 corporate network through the internal interfaces.</p> <p>IPv6 is not supported for active/passive clusters. If a device belongs to an active/passive cluster, you cannot enable IPv6 on its ports. If a device has IPv6 enabled on its ports, it cannot be added to an active/passive cluster.</p>
License server	IPv4 must be enabled for the "preferred network" you select for licensing protocol communication.
Web server	The implementation for IPv6 does not require reconfiguration of the Secure Access Service after upgrade. The Web server can listen for and accept IPv4 or IPv6 clients, and it can differentiate between them for internal purposes and for logging purposes.
ActiveSync	The implementation for IPv6 does not require reconfiguration of the Secure Access Service after upgrade. ActiveSync functionality is available to users connecting from IPv4 or IPv6 endpoints to an IPv4 backend server. Connection to an IPv6 backend server is not supported.
Connection profiles	<p>After upgrading to Release 7.4, you can update your VPN Tunneling Connection Profile configuration to enable IPv6 address assignments to Junos Pulse clients. You must configure a static IPv6 address pool. DHCPv6 is not supported.</p> <p>Also note that the IP address server configuration on the System &gt; Network &gt; VPN Tunneling page does not support filtering for IPv6 address pools. In active/active clusters, separate connection profiles need to be created with different IPv6 address pools for each node.</p> <p>Split Tunneling policies are not supported for IPv6 resources.</p> <p>WINS is not used in IPv6 networks; therefore, WINS settings are not applicable for connection profiles used for IPv6 access.</p> <p>The server-side proxy feature does not support IPv6.</p>

Table 72: Summary of IPv6 Support (*continued*)

Feature	Release 7.4
Resource policies	<p>You can configure VPN Tunneling Connection Profiles to enable access to all IPv6 resources in your corporate network; however, you cannot configure VPN Tunneling Access Control Policies to allow or deny access to particular IPv6 resources. As a workaround for this Release 7.4 limitation, we recommend you deploy firewall security to restrict access to IPv6 resources.</p> <p><b>NOTE:</b> To enable access to IPv6 resources, the DNS server used by the Secure Access Service must be reachable by IPv4 and must be able to resolve AAAA DNS queries.</p> <hr/> <p><b>Core Access - Rewriter</b></p> <p>The implementation for IPv6 does not require reconfiguration of the Secure Access Service after upgrade. After upgrade, IPv6 endpoints can access internal IPv4 resources through Secure Access Service. This applies to all Secure Access Service content rewriters: HTML, Java Script, Applets, VB Script, Flash, CSS, XML, PDF.</p> <p>You cannot configure Web Rewriting Policies for IPv6 resources.</p> <hr/> <p><b>Core Access - Passthrough proxy</b></p> <p>The Secure Access Service passthrough proxy modes are based on hostnames or ports, not IP addresses. Therefore, the implementation for IPv6 does not require reconfiguration of the Secure Access Service after upgrade. Note, however, that in virtual hostname mode, your DNS server must be configured to resolve the virtual hostname to the Secure Access Server IP address, which can be an IPv4 or IPv6 address. Update entries in your DNS server accordingly.</p> <p>You cannot configure Passthrough Proxy Policies for IPv6 resources.</p> <hr/> <p><b>Core Access - Hosted Java applets</b></p> <p>The implementation for IPv6 does not require reconfiguration of the Secure Access Service after upgrade. All hosted Java applets, including the premier Java RDP applet, work on IPv4 or IPv6 clients.</p> <p>You cannot configure policies that require access to hosted Java applets at IPv6 addresses.</p>
User role VPN Tunneling options	<p>The Split Tunneling option is not supported for IPv6. If it is enabled for a role, the system treats it as disabled.</p> <hr/> <p><b>Route Precedence:</b></p> <ul style="list-style-type: none"> <li>• If <b>Tunnel Route</b> is selected, the client cannot access its local IPv6 network and IPv6 traffic is blocked, except DHCPv6, ICMPv6, and loopback traffic going to the physical adapter. If Route Monitoring is enabled, only IPv4 route monitoring is performed.</li> <li>• If <b>Endpoint Route</b> is selected, the client can access its local IPv6 network. Route Monitoring should be disabled.</li> </ul> <hr/> <p>The Multicast option is not supported for IPv6 resources.</p>

Table 72: Summary of IPv6 Support (*continued*)

Feature	Release 7.4
Role/Realm Source IP restrictions	<p>You can specify IPv4 or IPv6 Source IP restrictions at both the role and the realm level.</p> <p>If Secure Access Service is deployed behind a NAT64 device, Secure Access Service sees traffic coming from an IPv4 address. In this case, your Source IP restrictions should be based on the NATed IPv4 addresses.</p>
Session roaming	<p>You can manage session roaming across IPv6 subnets. If you enable unlimited session roaming, a session is maintained within an IPv4 network, within an IPv6 network, or from IPv4 to IPv6 and vice versa. If you configure limited session roaming, you can specify IPv4 or IPv6 subnets within which the session is maintained. However, with limited session roaming, you cannot allow sessions to roam from IPv4 to IPv6 networks, or vice versa.</p>
Logging	<p>The logging system can process and parse logs containing IPv6 addresses.</p> <p>Release 7.4 supports communication with external log systems and utilities, such as syslog, SNMP, and archiving that are reachable by IPv4 only.</p>
Network tools	<p>Beginning with Release 7.3, the ping6 and traceroute6 were added to the admin graphical user interface console network tools page. We do not support DNS resolution for hosts with IPv6 addresses. Hence, you cannot use hostname targets with ping6 and traceroute6.</p>

- Related Documentation**
- [Understanding IPv6 on page 1065](#)
  - [IPv6 Feature Configuration Task Summary on page 1075](#)

## IPv6 Feature Configuration Task Summary

IPv6-related features are not enabled by default. After you upgrade to Junos Pulse Secure Access Service 7.4, perform the tasks summarized in [Table 73 on page 1075](#) to make the Secure Access Service ready for IPv6 traffic.

Table 73: IPv6 Feature Configuration Task Summary

Action	Documentation
Enable IPv6 for the external port and configure an IPv6 address.	<a href="#">“Configuring the Internal and External Ports” on page 792</a>
Enable IPv6 for the internal port and configure an IPv6 address.	<a href="#">“Configuring the Internal and External Ports” on page 792</a>
Enable IPv6 for the management port and configure an IPv6 address.	<a href="#">“Configuring Management Port Network Settings” on page 830</a>
Configure IP aliases and IPv6 addresses for virtual ports.	<a href="#">“Using Virtual Ports” on page 802</a>

Table 73: IPv6 Feature Configuration Task Summary (*continued*)

Action	Documentation
Re-create a cluster deployment with IPv6 configuration for external interfaces.	<a href="#">“Example: Creating a Cluster That Supports IPv6 Client Access” on page 1077</a>
If you use source IP policies, configure them so that source IP restrictions are based on IPv6 addresses.	<a href="#">“Specifying Source IP Access Restrictions” on page 79</a>
Configure IPv6 address assignment for VPN Tunneling Connection Profiles.  DHCPv6 is not supported. Also note that the IP address server configuration on the System > Network > VPN Tunneling page does not support filtering for IPv6 address pools.	<a href="#">“Creating VPN Tunneling Connection Profiles” on page 761</a>
If you permit roaming sessions but limit to roaming within the specified subnet, configure the role session option so that the subnet is defined by netmask for IPv4 and prefix length for IPv6 networks.	<a href="#">“Specifying Role Session Options” on page 111</a>
View and manage the neighbor discovery cache. In Release 7.4, you can view discovered neighbors or clear the entire cache, but you cannot add neighbors or delete individual entries.	<a href="#">“Managing the Neighbor Discovery Cache” on page 1077</a>
View IPv6 routes in the IP route table. In Release 7.4, you can view discovered IPv6 routes, but you cannot add or delete them from the route table.	<a href="#">“Configuring Static Routes for Network Traffic” on page 805</a>
Review logs. The logging infrastructure accommodates IPv6 addresses, and you can create custom filters based on IPv6 address patterns.	<a href="#">“Configuring Log Monitoring Features” on page 935</a>
Become familiar with IPv6 network connectivity test tools, such as ping6 and traceroute6.	<a href="#">“Secure Access Service Network Connectivity Tools” on page 969</a>

- Related Documentation**
- [Understanding IPv6 on page 1065](#)
  - [IPv6 Support Overview on page 1069](#)



## Managing the Neighbor Discovery Cache

You use the **System > Network > Port > ND Cache** page to manage the Secure Access Service Neighbor Discovery cache. *Port* is Internal Port, External Port, or Management Port.

IPv6 hosts use **Neighbor Discovery Protocol (NDP)** to determine the link-layer addresses for neighboring hosts and routers. The Secure Access Service uses NDP to maintain a cache of neighboring routers that are reachable and can forward packets on its behalf.



**NOTE:** In Secure Access Service Release 7.3 and Release 7.4, you can view discovered neighbors or clear the entire cache, but you cannot add neighbors or delete individual entries.

To view or clear the neighbor discovery cache:

1. Select **System > Network > Port > ND Cache**.
2. Review the table summary of IPv6 neighbor nodes.
3. Optional. If necessary, click **Delete Dynamic Entries** to clear the cache.

### Related Documentation

- [Understanding IPv6 on page 1065](#)
- [IPv6 Support Overview on page 1069](#)
- [IPv6 Feature Configuration Task Summary on page 1075](#)

## Example: Creating a Cluster That Supports IPv6 Client Access

This example describes the tasks involved in creating a cluster that supports IPv6 client access. It includes the following information:

- [Overview on page 1077](#)
- [Before You Begin on page 1078](#)
- [Defining and Initializing a Cluster on page 1078](#)
- [Joining Nodes to the Cluster on page 1079](#)
- [Advanced Configuration on page 1080](#)

### Overview

Release 7.3 and Release 7.4 support an IPv6 configuration for active/active clusters. The previous intracluster communication mechanism is preserved. The intracluster communication occurs over the IPv4 corporate network through the internal interfaces.

Release 7.3 and Release 7.4 do not support an IPv6 configuration for active/passive clusters. If a device belongs to an active/passive cluster, you cannot enable IPv6 on its

ports. If a device has IPv6 enabled on its ports, it cannot be added to an active/passive cluster.

If you attempt to change the IP address of a node while it belongs to a cluster, you might experience unpredictable results. Whenever you change the IP address configuration for a cluster, you must re-create the cluster. Therefore, to add support for IPv6 addresses, you must re-create the cluster.

## Before You Begin

We recommend that you deploy a cluster in a staging environment first and then move to a production environment after testing authentication realm, user role, and resource policy configurations, as well as any applications your end users might access.

Before you begin a cluster configuration:

1. Ensure that all intended Secure Access Service nodes use the same hardware platform (for example, all are SA6500 Series Appliances).
2. Ensure that all intended Secure Access Service nodes have been initially configured (for example, Secure Access Service hostname is specified and the internal and external IP addresses are assigned), and they are running the same service package version.
3. Designate one node as the primary node. On the primary node, configure system and user settings. When other nodes join the cluster, the primary node propagates its configuration to the new cluster member during the join cluster operation.

## Defining and Initializing a Cluster

You use the primary node admin GUI graphical user interface to create the cluster and add members. The primary node is added as part of the cluster creation operation. When you add members, you are prompted for settings unique to the member, such as the name and IP address configuration for the internal and external interfaces. A few additional settings are also unique, namely the management port and VLAN port settings, so you add these manually after the add node procedure that follows, but before the join cluster operation.

To create a cluster and add members:

1. Select **System > Clustering > Create** and enter a name for the cluster, a cluster password, and a name for this node, such as Node-1.

You need to enter the password again when specifying additional nodes to join the cluster. All nodes in the cluster use this password to communicate.

2. Click **Create Cluster**. When prompted to confirm the cluster creation, click **Create**. After the Secure Access Service initializes the cluster, the Clustering page displays the Status and Properties tabs.

3. Click **Add Members** to specify the additional cluster nodes:
  - a. Enter a name for the member; for example, Node-2.
  - b. Enter the internal IP address. If both IPv4 and IPv6 are enabled on the internal port on Node-1, the system prompts for both IPv4 and IPv6 settings for the internal port for Node-2. Note, however, that intracluster communication uses the IPv4 corporate network.
  - c. Enter the external IP address. If both IPv4 and IPv6 are enabled on the external port on Node-1, the system prompts for both IPv4 and IPv6 settings for the external port for Node-2.
  - d. Change the netmask/prefix-length and gateway settings for the node if necessary.
  - e. Click **Add Node**. When prompted to confirm adding the new member, click **Add**.  
When the add node operation has completed, Node-2 is shown as an unreachable member of the cluster.
  - f. The add node procedure does not prompt you to configure management port or VLAN port settings. As needed, go to the node port configuration page and configure these settings. For example, after the add node operation has completed for Node-2, go to its **System > Network > Port > Settings** page and configure its management port.
  - g. Repeat this procedure for each node you intend to add to a cluster.

## Joining Nodes to the Cluster

The primary node joins the cluster as part of the creation process. Use the following procedure to join additional nodes to the cluster.

To join a node to the cluster:

1. From an existing cluster member, select the **System > Clustering > Cluster Status** tab and specify the Secure Access Service you want to add to the cluster.
2. From the admin GUI of the Secure Access Service you want to join to a cluster:
  - a. Select the **System > Clustering > Join** tab and enter:
    - The name of the cluster to join.
    - The cluster password you specified when defining the cluster.
    - The IPv4 address for the internal port of an active cluster member.
  - b. Click **Join Cluster**. When prompted to confirm joining the cluster, click **Join**.

The join cluster operation validates IPv4 and IPv6 settings for all the physical ports (internal/external/management) against those present in the existing cluster. For example, the external port IPv6 settings present on Node-2 are compared against external port IPv6 settings that were specified for the Node-2 add member operation entered on

the primary node (Node-1). If there is a mismatch, the join operation fails with an appropriate error message.

While the new node synchronizes its state with the existing cluster member, each node's status indicates **Enabled**, **Enabled, Transitioning**, or **Enabled, Unreachable**.

When the node finishes joining the cluster, its Clustering page shows the Status and Properties tabs.

After the node joins the cluster, you might need to sign in again.

## Advanced Configuration

Table 74 on page 1080 summarizes advanced configuration guidelines.

**Table 74: Secure Access Service Clusters: Advanced Configuration Guidelines**

Topic	Guideline
Active/Active	<p>When using Pulse clients with an active/active cluster, you must split the IP address pool across the nodes to ensure proper routing from the backend to the end user. This is a requirement whether the IP address pool is provisioned statically on the Secure Access Service or dynamically by way of DHCP.</p> <p>The client IP pool configuration is synchronized among all nodes in a cluster; however, you may configure each node to use a certain subset of the global IP pool.</p> <p>If you are running Network Connect on a multisite cluster where nodes reside on different subnets:</p> <ol style="list-style-type: none"> <li>1. Configure an IP address pool policy on the Users &gt; Resource Policies &gt; VPN Tunnelling: Connection Profiles &gt; New Profile page that accounts for the different network addresses used by each node in the cluster.</li> <li>2. For each node in the cluster, use settings in the System &gt; Network &gt; VPN Tunneling page of the admin GUI to specify an IP filter that filters out only those network addresses available to that node.</li> </ol> <p><b>NOTE:</b> Release 7.3 and Release 7.4 do not support IP filters for IPv6 addresses.</p> <ol style="list-style-type: none"> <li>3. Create a static route on your gateway router that indicates the IP address of the internal port of each cluster node. Each IP address specified on the router needs to be in the same subnetwork as the corresponding cluster node.</li> </ol>
FIPS	<p>If you are creating a cluster of SA Series FIPS Appliances, manually update the security world on each of the nodes.</p>

- Related Documentation**
- [About Clustering on page 977](#)
  - [General Cluster Maintenance on page 993](#)

# Secure Access Service and IDP Interoperability

- [About IDP on page 1081](#)
- [IDP Deployment Scenarios on page 1082](#)
- [Configuring the Secure Access Service to Interoperate with IDP on page 1083](#)
- [Configuring IDP Sensor Policies on page 1084](#)
- [Defining Automatic Response Sensor Event Policies on page 1086](#)
- [Identifying and Managing Quarantined Users Manually on page 1088](#)

## About IDP

---

Securing intranet work application and resource traffic is vital to protecting your network from hostile outside intrusion. You can add levels of application security to your remote access network by integrating a Juniper Networks Secure Access Service with a Juniper Networks Intrusion Detection and Prevention (IDP) Sensor. The IDP device may provide the following types of protection in this solution (some forms of protection depend upon the specific configuration):

The IDP sensor monitors the network on which the IDP system is installed. The sensor's primary task is to detect suspicious and anomalous network traffic based on specific rules defined in IDP rulebases.

The IDP device provides the following types of protection (some forms of protection depend upon the specific configuration):

- Protects against attacks from user to application and from application to user (from a server-side endpoint)
- Detects and blocks most network worms based on software vulnerabilities
- Detects and blocks non-file-based Trojan Horses
- Detects and blocks effects of spyware, adware, and key loggers
- Detects and blocks many types of malware
- Detects and blocks zero day attacks through the use of anomaly detection



**NOTE:** An IDP Sensor can send logs to one Secure Access Service only. However, the Secure Access Service can receive logs from more than one IDP Sensor.

You do not need a special license from Juniper Networks to enable interaction between the Secure Access Service and the IDP.

Using the Secure Access Service admin console, you can configure and manage interaction attributes between the Secure Access Service and an IDP, including the following:

- Global configuration parameters such as the IDP hostname or IP address, the TCP port over which the sensor communicates with the Secure Access Service, and the one-time password the Secure Access Service and IDP use to authenticate with one another.
- Dynamically changing the IDP configuration from the Secure Access Service and alerting the IDP of changes in the IP address pool available to remote users.
- Various levels of attack severity warnings.

The IDP sits behind the Secure Access Service on your internal network and monitors traffic flowing from the Secure Access Service into the LAN. Any abnormal events detected by the IDP Sensor are reported to the Secure Access Service, which you configure to take appropriate action based on the severity level of the reported events. The IDP Sensor performs reporting functions in addition to any normal logging the IDP has been configured to undertake.

You can use an IDP Sensor on the Secure Access Service cluster, if the cluster is configured with a virtual IP (VIP) address.

## Licensing: IDP Availability

The IDP integration feature is not available on the SA 700.

### Related Documentation

- [IDP Deployment Scenarios on page 1082](#)
- [Configuring the Secure Access Service to Interoperate with IDP on page 1083](#)
- [Configuring IDP Sensor Policies on page 1084](#)

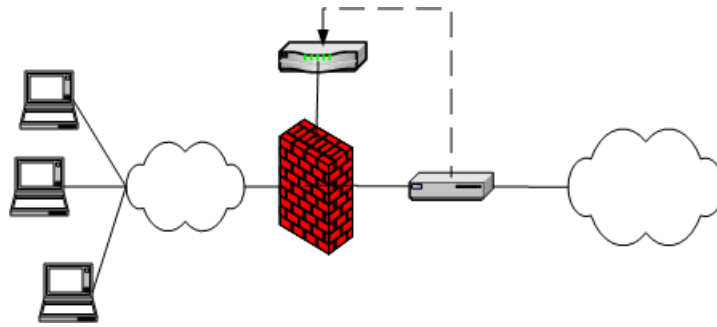
## IDP Deployment Scenarios

---

The two most likely deployment scenarios are as follows:

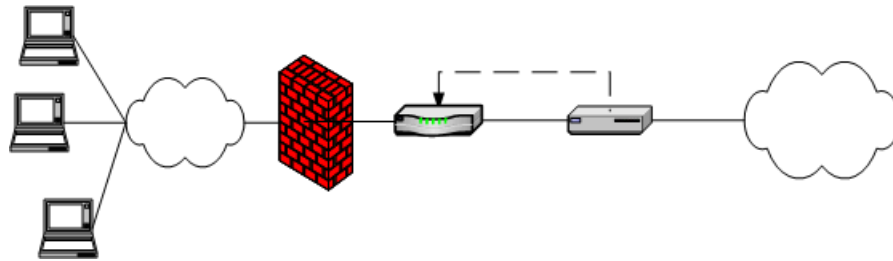
- Customer use of the Secure Access Service for extended enterprise access and IDP for security of all perimeter traffic including but not limited to traffic from the Secure Access Service. The following figure illustrates this scenario, in which the Secure Access Service is deployed in the DMZ or on the LAN and the IDP is deployed in-line behind the firewall and in front of the LAN.

Figure 79: Secure Access Service and IDP Topology Scenario 1



- In the second deployment scenario, IDP is only used to protect traffic that comes through the Secure Access Service but not in-line with other perimeter traffic. The following figure illustrates this deployment scenario.

Figure 80: Secure Access Service and IDP Topology Scenario 2



**Related  
Documentation**

- [About IDP on page 1081](#)
- [Configuring the Secure Access Service to Interoperate with IDP on page 1083](#)

## Configuring the Secure Access Service to Interoperate with IDP

The IDP Sensor is a powerful tool to counter users who initiate attacks. Integration with the Secure Access Service allows you to configure automatic responses as well as manually monitor and manage users.

To configure the Secure Access Service to interoperate with an associated standalone IDP Sensor, you must first ensure the IDP has been configured according to the instructions described in the Signaling Setup appendix of [IDP Series Concepts and Examples Guide, Version 5.1rX](#).

Once the IDP Sensor has been set up, you can specify the events you want the IDP to watch for and the actions that the Secure Access Service takes once a particular event has been noted and reported.

There are two locations on the Secure Access Service where you can specify actions to be taken in response to users that perform attacks:

- **Sensor Event policies page**—Define the policy on this page to generate an automatic response to users who perform attacks.

- **Users page**—Manually identify and quarantine or disable users on the System > Status > Active Users page, which lists users who have performed attacks.

## Interaction Between the IC Series and IDP

The Secure Access Service reads attack information as it is being sent by the IDP sensor. The Secure Access Service receives the source and destination IP addresses and port numbers of the attacking host and the resource against which the attack was launched, along with the attack identifier, severity of the attack, and the time at which the attack was launched.

The Secure Access Service incorporates and displays the attack information received from the IDP sensor on the System > Status > Active Users page. Based on the attacker's IP address and port number, the Secure Access Service can uniquely identify the user's session.

You can choose automatic or manual actions for attacks detected by the IDP sensor. For manual action, you look up the information available on the Active Users page and decide on an action. For automatic action, you configure the action in advance when you define your IDP policies.

### Related Documentation

- [Configuring IDP Sensor Policies on page 1084](#)

---

## Configuring IDP Sensor Policies

The Sensors tab allows you to specify the system settings the Secure Access Service uses to establish a connection to a Juniper Network's Intrusion Detection and Prevention (IDP) device.

Use the System > Configuration > Sensors > Sensors tab to perform a number of tasks related to configuring and managing interaction between the Secure Access Service and an IDP Sensor. The main Sensor page displays the sensor, the network address, the state (enabled), the version, and the status of any configured sensors.

**Creating a New IDP Sensor Entry** In IDP versions prior to 5.0, the Secure Access Service sends only the user IP address. With version 5.0, the Secure Access Service sends session information including the user, user role and IP address.

To enable or disable existing IDP Sensor entries on the Secure Access Service:

1. In the admin console, choose **System > Configuration > Sensors**.



**NOTE:** To use the IDP sensor with the Secure Access Service you must enable logging for the applicable policies.

---

2. Click **New Sensor**. The admin console displays the New Sensor page.
3. Under Sensor Properties, specify the following information:



- **Name**—A name the Secure Access Service uses to identify the new connection entry
- **Hostname**—The hostname or IP address of the IDP Sensor to which the Secure Access Service connects in order to receive application and resource attack alert messages
- **Port**—The TCP port on the IDP Sensor to which the Secure Access Service listens when receiving application and resource attack alert messages
- **One-time password**—The encrypted password the Secure Access Service uses when conducting the initial Transport Layer Security (TLS) handshake with the IDP Sensor. You must enter the encrypted Secure Access Service OTP password as displayed on the IDP ACM configuration summary screen.



**NOTE:** The hostname, TCP port, and one-time password must already be configured on the IDP Sensor before this configuration can be successful.

4. Under **Monitoring Options**, specify IP addresses to monitor and the minimum alert severity level the IDP Sensor will record and submit to the Secure Access Service:
  - In the Addresses to Monitor field, specify individual IP addresses and address ranges, one entry per line. IDP reports attack information only for the IP addresses that you specify. If you want IDP to report all events to the Secure Access Service, enter 0.0.0.0/0. If you want IDP to report only selected events, enter <default> to permit IDP to report events for events with source IPs that have an active user session on the Secure Access Service, and /or enter one or more addresses or address ranges for any endpoint that you want the IDP sensor to report.
  - Select one of the severity options available in the Severity filter drop down list. The severity level is a number on a scale from 1 to 5, where 1 is informational and 5 is critical. This option represents the severity of messages the IDP should send to the Secure Access Service.
5. Click **Save Changes**.

### Enabling or Disabling IDP Sensors

To enable or disable existing IDP Sensor entries on the Secure Access Service:

1. In the admin console, choose **System > Configuration > Sensors**.
2. Select the checkbox next to one or more IDP Sensor entries you want to enable or disable.
3. Click **Enable** or **Disable** to enable or disable the specified IDP Sensor entries, respectively.

You can delete existing IDP Sensor entries that define a connection between the Secure Access Service and an IDP Sensor.

To delete one or more existing IDP Sensor entries from the Secure Access Service:

1. In the admin console, choose **System > Configuration > Sensors**.
2. Select the checkbox next to the IDP Sensor entry or entries you want to delete.
3. Click **Delete** and then confirm that you want to delete the sensor entry or entries.

#### **Reconnecting to an IDP Sensor**

When the connection to an IDP Sensor is down, you can use the admin console on the Secure Access Service to re-establish the connection. You can also use the admin console to refresh the status of existing connections between the Secure Access Service and the IDP Sensor.

If you need to re-establish communication with an IDP Sensor, you must generate a new One-time Password.

To reconnect to an associated IDP Sensor:

1. In the admin console, choose **System > Configuration > Sensors**.
2. Select the checkbox next to the IDP Sensor to which you want to reconnect.
3. Click **Reconnect**.

The admin console displays a message informing you that the Secure Access Service is currently attempting to re-establish connection to the specified IDP Sensor. This page automatically refreshes each second during the reconnection process. Otherwise, the connection status page automatically refreshes once every 30 seconds.

#### **Refreshing and Displaying the Connection Status**

To refresh and display the connection status for the specified IDP Sensor:

1. In the admin console, choose **System > Configuration > Sensors**.
2. Select the checkbox next to one or more IDP Sensor entries for which you want to display current connection status.
3. Click **Refresh**.

#### **Related Documentation**

- [About IDP on page 1081](#)
- [Configuring the Secure Access Service to Interoperate with IDP on page 1083](#)

---

## **Defining Automatic Response Sensor Event Policies**

Use the **System > Configuration > Sensors > Sensor Event Policies** tab to specify one or more rules that specify the action(s) the Secure Access Service takes when it receives attack alert messages from an IDP Sensor.

To create a new IDP rule:

1. In the admin console, select **System > Configuration > Sensors > Sensor Event Policies**.
2. On the Sensor Event Policies page, click **New Rules**.
3. On the Juniper IDP Rule page, in the Rule: On Receiving... section:
  - Select an existing event from the Event drop-down list.
  - Click **Events** to edit an existing event or create a new type of event and add it to the options in the Events drop-down list:
    - a. Specify a name for the event.
    - b. Populate the Expressions field by manually entering expressions or by selecting one or more clauses from the Expressions Dictionary and clicking Insert Expression.  
  
For example, to check for all critical/highest severity level attacks, enter the following expression:  
  
`idp.severity >= 4`  
  
To check for all critical/highest severity level attacks for HTTP traffic, enter the following expression:  
  
`idp.severity >= 4 AND idp.attackStr = "*HTTP*"`
    - c. When you have finished entering the expressions you want to apply to this event, click **Add Expression**.
    - d. Click **Close**.
4. In the **Count this many times** section, specify a number between 1 and 256 to determine the number of times an event must occur before action is taken.
5. In the **...then perform this action** section, specify one of the following actions:
  - **Ignore (just log the event)**—Specifies that the Secure Access Service should log the event, but take no further action against the user profile to which this rule applies. This option is best used to deal with very minor “informational” attack alert messages that come from the IDP Sensor.
  - **Terminate User Session**—Specifies that the Secure Access Service should immediately terminate the user session and require the user to sign in to the Secure Access Service again.
  - **Disable user account**—Specifies that the Secure Access Service should disable the user profile associated with this attack alert message, thus rendering the client unable to sign in to the Secure Access Service until the administrator re-enables the user account. (This option is only applicable for users who have a local Secure Access Service user account.)
  - **Replace user’s role with this one**—Specifies that the role applied to this user’s profile should change to the role you select from the associated dropdown list. This new role remains assigned to the user profile until the session terminates. This feature allows you to assign a user to a specific controlled role of your choice, based

on specific IDP events. For example, if the user performs attacks, you might assign the user to a restricted role that limits the user's access and activities.

- Choose to **make this role assignment**:
  - **Permanent**—User remains in the quarantined state across subsequent logins until the administrator releases the user from the quarantined state.
  - **For this session only**—Default. User can log in to another session.
- 6. In the **Roles** section, specify:
  - **Policy applies to ALL roles**—To apply this policy to all users.
  - **Policy applies to SELECTED roles**—To apply this policy only to users who are mapped to roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
  - **Policy applies to all roles OTHER THAN those selected below**—To apply this policy to all users except for those who are mapped to the roles in the Selected roles list. Make sure to add roles to this list from the Available roles list.
- 7. Click **Save Changes**.

**Related  
Documentation**

- [Configuring the Secure Access Service to Interoperate with IDP on page 1083](#)

---

## Identifying and Managing Quarantined Users Manually

---

When the Secure Access Service quarantines a user based on an attack, you can display and manage the states by locating the user link in the **System > Status > Active Users** page.

- A small warning icon displayed in front of the user name.
- The hyperlinked user name.
- An enabled Quarantined option button on the specific user's page. If the user is not quarantined, the option button is disabled.

You can manage quarantined users from either the admin GUI or by logging in as a user with administrative rights on the local authentication server.

To manage quarantined users:

1. Identify quarantined users at **System > Status > Active Users**.
2. Locate the quarantined user from the **Authentication > Auth. Servers > System Local** on the admin GUI or from the **Admin Users** window on the local authentication server. You must be logged in to the local authentication server as an administrator user in order to see the Admin User option.
3. Click the username link. The user page opens, showing a number of options.

Figure 81: Managing Quarantined Users

Auth Servers > System Local >  
**Update Local User test1**

Full Name:

Authenticate using: System Local

Password:

Confirm Password:

**One-time use (disable account after the next successful sign-in)**

Enabled

Disabled

Quarantined

Require user to change password at next sign in

Note: You must also configure password management on the [Authentication server Settings](#) with 'Allow users to change their passwords' option enabled. Use options on the Administrators/Users > Authentication > [Realm] > Authentication Policy > Password page to specify which realms should inherit the server's password management capabilities.

4. Click **Disabled** to disallow a user from authenticating.
5. Click **Quarantined** to leave a user in a quarantined state. The Quarantined option is only enabled if the user is already quarantined.



**NOTE:** The Secure Access Service assigns quarantined users to the quarantined role, regardless of their login realm.

6. Click **Save Changes**.
7. To re-enable previously quarantined or disabled users, select **Authentication > Auth. Servers > Select Server > Users** and click the link for the given user.



**NOTE:** You can also disable users from this location.

8. Click **Enabled** to release the user from quarantine.
9. Click **Save Changes**.

All Sensor events are logged at System > Log/Monitoring > Sensors > Log.

#### Related Documentation

- [Defining Automatic Response Sensor Event Policies on page 1086](#)
- [Monitoring Active Users on page 955](#)



# Routing AAA Over the Management Port for Virtual Appliances

- [About Traffic Segregation on page 1091](#)
- [Configuring AAA Traffic Over the Management Port on page 1092](#)
- [Configuring AAA Traffic Through Both the Internal and Management Ports on page 1093](#)

## About Traffic Segregation

---

Service providers often need a way to cleanly segregate the Secure Access Service-generated network traffic across interfaces (such as Internal, Management and VLAN ports), to differentiate AAA traffic from others.

Two typical service provider deployment models are:

- Authentication server of the customer is hosted by the customer
- Authentication server for the customer is hosted and managed by the service provider

In both models, the service provider's authentication server is always hosted in the service provider's network and is reachable either through the internal or management port. In the first model, the customer's authentication servers are reachable through the internal port of the virtual appliance. In the second model, the customer's authentication server must be routed either through the internal or management port, depending on where the service provider has hosted the customer's authentication server.

A Traffic Segregation menu is available only on virtual appliances to allow system providers to configure the interface and traffic. The "Default Network" is used as the primary logical network for the service provider and customer configuration. If traffic segregation across different logical networks is needed, the "Administrative Network" can be used.

You can differentiate AAA traffic from other traffic and route it through the management port. This is useful when the only the authentication servers are hosted on the network reachable through the management port and all other resources uses a different port. This option is available on both the Default Network and the Administrative Network.

The configurations to do on the virtual appliance depend on the logical network setup around the virtual appliance and the type of service provider deployment model:

- If both the service provider's and customer's authentication server are reachable through the same interface, the entire configuration for the service provider and customer is done under the Default Network. It is not necessary to enable the Administrative Network.
- If the service provider's and customer's authentication servers are located on two different networks, the Administrative Network must be created. [Table 75 on page 1092](#) shows where the administrator configures the options in the Secure Access Service GUI.

**Table 75: Configuring Traffic Segregation Options**

Task	For Service Provider	For Customer
AAA configuration for administrators	Under Administrative Network	Delegated admin under Default Network (only if needed)
AAA configuration for users	Not required	Under Default Network
System configuration	Under Default Network	Not required

**Related Documentation**

- [Configuring AAA Traffic Over the Management Port on page 1092](#)
- [Configuring AAA Traffic Through Both the Internal and Management Ports on page 1093](#)

## Configuring AAA Traffic Over the Management Port

This topic describes how to configure all AAA traffic through the management port. Note that if the management port is enabled, system management traffic (like SNMP) continues to flow through the management port. All other traffic flows through the internal port. When all authentication servers are hosted in the same network, you need only to configure the Default Network.

To configure AAA traffic over the management port:

1. Select **System > Traffic Segregation**.
2. Click **Default Network**.
3. Click the **Send AAA Traffic via Management Port** checkbox.
4. Click **Save Changes**.

**Related Documentation**

- [About Traffic Segregation on page 1091](#)
- [Configuring AAA Traffic Through Both the Internal and Management Ports on page 1093](#)



## Configuring AAA Traffic Through Both the Internal and Management Ports

When authentication servers are hosted in two different networks, enable the Administrative Network to allow the servers to be reachable through two different virtual appliance interfaces. Service provider authentication server settings are defined under the Administrative Network. User authentication servers are configured in the Default Network using the internal port.

To enable the Administrative Network and set the Management Port as the default:

1. Select **System > Traffic Segregation**.
2. Check the **Enable Administrative Network** checkbox.
3. Click **Save Changes**.  
The Administrative Network appears in the Traffic Segregation table.
4. Click **Administrative Network**.
5. Under Interface: Available Interface, select **Management Port** and click **Add**.
6. Under Selected Interfaces, select **Management Port** and click **Set default interface**.
7. Click **Save Changes**.

To configure service provider AAA settings on the Administrative Network:

1. Select **Administrative Network** from the menu in the upper left corner and click **Go**.  
A limited set of options are available on the Administrative Network.
2. Select **Authentication > Auth Servers** and configure your service provider AAA configurations as needed.

By default, the Default Network uses the internal port so no additional configuration is needed for the Default Network.

To log in to the virtual appliance through the administrative network, either:

- Use the internal or external port (<https://virtual-appliance/VA/adminnet/admin>)
- Assign a virtual port to the administrative network and log in through that virtual port (<https://virtual-appliance-VIP/admin>)



**NOTE:** If you enable AAA traffic over the management port, the next time you log in to the virtual appliance over the management port the administrator sign-in page appears with “Welcome to the Junos Pulse Secure Access Service” and not “Sign in via Administrative Network to the Junos Pulse Secure Access Service.”

### Related Documentation

- [About Traffic Segregation on page 1091](#)

- [Configuring AAA Traffic Over the Management Port on page 1092](#)

## PART 6

# System Services

- [Secure Access Service Serial Console on page 1097](#)
- [Customizable Admin and End-User UIs on page 1103](#)
- [SA6000 Series Appliance on page 1105](#)
- [SA4500 and SA6500 Series Appliances on page 1109](#)
- [Secure Access FIPS on page 1119](#)
- [SA4500 and SA6500 FIPS Appliances on page 1131](#)
- [FIPS Level 1 Support on page 1141](#)
- [Compression on page 1157](#)
- [Multi-Language Support on page 1161](#)
- [Handheld Devices and PDAs on page 1165](#)
- [Using IKEv2 with the Secure Access Service on page 1173](#)
- [Writing Custom Expressions on page 1181](#)



# Secure Access Service Serial Console

- [Using the Serial Console on page 1097](#)
- [Rolling Back to a Previous System State Through the Serial Console on page 1098](#)
- [Resetting a Secure Access Service Device to the Factory Setting Using the Serial Console on page 1099](#)
- [Performing Common Recovery Tasks with the Serial Console on page 1100](#)

## Using the Serial Console

---

The serial console provides a limited set of powerful capabilities to help you manage your Secure Access Service, and is available through your operating system's command window.

Before performing any tasks through the Secure Access Service's serial console, you need to connect to the console using a terminal console or laptop.

To connect to a Secure Access Service's serial console:

1. Plug a null modem crossover cable from a console terminal or laptop into the Secure Access Service. This cable is provided in the product box. Do not use a straight serial cable.
2. Configure a terminal emulation utility, such as HyperTerminal, to use these serial connection parameters:
  - 9600 bits per second
  - 8-bit No Parity (8N1)
  - 1 Stop Bit
  - No flow control
3. Press Enter until the Secure Access Service serial console appears.



**NOTE:** If you are running a FIPS system and are connecting to the serial console for the first time, you must also set the mode switch on the cryptographic module to I (initialization mode).

---

If you are using a non-FIPS platform, your serial console will look similar to this:

Please choose from among the following options:

1. Network Settings and Tools
2. Create admin username and password
3. Display log/status
4. System Operations
5. Toggle password protection for the console (Off)
6. Create a Super Admin session.
7. System Maintenance
8. Reset allowed encryption strength for SSL
10. Toggle SSL HW Acceleration (system will reboot when this setting is modified): on

If you are using a FIPS platform, your serial console will look similar to this:

Please choose from among the following options:

1. Network Settings and Tools
2. Create admin username and password
3. Display log/status
4. System Operations
5. Toggle password protection for the console (Off)
6. Create a Super Admin session.
7. System Maintenance
8. Reset allowed encryption strength for SSL
9. FIPS options

**Related  
Documentation**

- [Rolling Back to a Previous System State Through the Serial Console on page 1098](#)
- [Resetting a Secure Access Service Device to the Factory Setting Using the Serial Console on page 1099](#)
- [Performing Common Recovery Tasks with the Serial Console on page 1100](#)

---

## Rolling Back to a Previous System State Through the Serial Console

---

If you cannot access the admin console, connect to the serial console to perform a system rollback to the previous system state.

If you have not yet performed a Secure Access Service OS service package upgrade, there is no previous state to roll back to and this option is not available. If you have performed a Secure Access Service OS service package upgrade, any system and user configuration data created after the upgrade is lost unless you export the most current configuration files before rolling back the system and then import them afterwards.

To roll back to the previous Secure Access Service OS service package:

1. Connect to your Secure Access Service's serial console.
2. In a browser window, sign in to the admin console.
3. Select **Maintenance > System > Platform**.

4. Click **Reboot Now** and then go back to the console utility window. The window displays a message that the system is restarting.
5. After several moments, you are prompted to hit the Tab key for options. Press the **Tab** key, and when prompted for the configuration to load, type `rollback` and then press the **Enter** key.

After clicking Reboot Now on the Maintenance > System > Platform page, the server's rollback status is output to the screen, and when complete, you are prompted to hit the Return key (Enter) to modify system settings, which returns you to the initial setup options. When you are finished entering data, simply close the utility window.

If you wait more than 5 seconds to enter your choice, the current system configuration is automatically loaded and you'll need to go back to the admin console and click Reboot Now to start the process again. If you have already performed a system rollback, the rollback option is not available again until you upgrade the Secure Access Service OS service package again.

**Related Documentation**

- [Using the Serial Console on page 1097](#)

## Resetting a Secure Access Service Device to the Factory Setting Using the Serial Console

---

In rare cases, you may need to reset your Secure Access Service to its original factory settings. Before performing this advanced system recovery option, please contact Juniper (<http://www.juniper.net/support/>). If possible, export the most current system and user configuration data before performing a factory reset.

To perform a factory-reset:

1. Connect to the serial console.
2. In a browser window, sign in to the admin console.
3. Select **Maintenance > System > Platform**.
4. Click **Reboot** and then go back to the console utility window. The window displays a message that the system is restarting.
5. After several moments, you are prompted to hit the Tab key for options. Press the **Tab** key, and when prompted for the configuration to load, type `factory-reset` and then press the **Enter** key.

If you wait more than 5 seconds to enter your choice, the current system configuration is automatically loaded and you'll need to go back to the admin console and click Reboot Now to start the process again.

6. When you are prompted to confirm performing a factory-reset, type `proceed` and then press **Enter**.

The system begins the process of resetting the machine to its original settings and outputs several screens of data. After several minutes, you are prompted to hit the Tab key to choose configuration choices.

7. When prompted to hit the Tab key, either:
  - Wait for the default selection (current) to automatically start, or
  - Press **Tab**, type **current**, and then press **Enter**.

You are then prompted to enter the initial machine configuration settings. For details on how to proceed, see the Getting Started Guide provided in the product packaging or on the Juniper Networks Support site.

After completing the initialization process, you may upgrade to the latest Secure Access Service OS service package and import saved system and user configuration files to return to the last good working state of your machine.

You might receive errors from the Secure Access Service during the initial setup or on a factory reset. Before the Secure Access Service starts services it monitors the network port for a maximum of 120 seconds. The Secure Access Service checks the link status and performs an ARPing on the default gateway. If there is a problem, after 5 seconds, the Secure Access Service displays a message on the serial console that starts with NIC:..... If the link recovers within 120 seconds, the startup process continues. If the link does not recover, the following message appears:

```
Internal NIC:[Down code=0x1]
```

Two codes can appear:

- 0x1 means that the interface link status reported by the NIC remains off (for example, a disconnected cable or a cable in the wrong port).
- 0x2 means that the gateway is unreachable. The Secure Access Service boots but is not reachable from IP addresses bound to that network port.

**Related Documentation**

- [Using the Serial Console on page 1097](#)

---

## Performing Common Recovery Tasks with the Serial Console

---

If you forget your Secure Access Service administrator username and/or password, lock yourself out of your machine due to configuration errors, or change the Secure Access Service IP address and can no longer reach the machine, you can modify the machine settings through the serial console. Connect the serial cable and then choose the appropriate configuration task.

- **Network Settings and Tools**—Enables you to change standard network settings; print a routing table; print or clear an ARP cache; ping another server, trace a route to a server, remove static routes, and add an ARP entry.
- **Create admin username and password**—Enables you to create a new superadministrator account.



- **Display log/status**—Enables you to display system configuration, user logs, or administrator access logs through the serial console. Note that must enter “q” to return to serial console options after viewing the logs.
- **System Operations**—Enables you to reboot, shutdown, restart, rollback, or factory reset the Secure Access Service appliance without using the admin console.
- **Toggle password protection for the console**—Enables you to password protect the serial console. When you toggle this option to “on,” only superadministrators are allowed access.
- **Create a Super Admin session**—Enables you to create a recovery session to the admin console, even if you have configured the Secure Access Service to block access to all administrators. When you select this option, the appliance generates a temporary token that is valid for 3 minutes. Enter the following URL into a browser window:  

```
https://<SA-Series-host>/dana-na/auth/recover.cgi
```

Then, enter the temporary token when prompted in order to sign into the admin console.
- When you choose this option, the Secure Access Service blocks any additional administrators from signing in to the admin console until you sign in to the specified URL and initiate a session using your token. The appliance blocks additional sign-in attempts so that you can fix any configuration problems that the Secure Access Service may have encountered without conflicting with another session.
- **System Maintenance**—Enables you to take a system snapshot without using the admin console or perform remote debugging.

When you select system snapshot, the Secure Access Service takes the snapshot immediately. You can then send the snapshot file, by way of SCP, to a remote system. The system prompts you for the destination server port, user ID, password, and the destination path to the remote directory.

If you choose not to send the snapshot file to a remote system, the Secure Access Service saves the file locally. The next time you log in to the admin console, the System Snapshot tab contains a link to the snapshot file.

- **Reset allowed encryption strength for SSL**—
- **FIPS Options** (for FIPS devices only)—Enables you to create additional administrator cards for a security world. See the following section for details.



**NOTE:** If you are running a FIPS device and you press the clear switch on the cryptographic module, set the cryptographic module's mode switch to O (operational mode) and restart the system. You do not need to access the serial console for recovery.

#### Related Documentation

- [Using the Serial Console on page 1097](#)



# Customizable Admin and End-User UIs

- [Customizable Admin and End-User UIs on page 1103](#)

## Customizable Admin and End-User UIs

---

The Secure Access Service enables you to customize a variety of elements in both the admin console and the end-user interface. This section contains information about which elements you can customize and where you can find the appropriate configuration options.

The Secure Access Service enables you to customize the look and feel of the following user interface elements in the admin console:

- **Sign-in pages (default and custom)**—You can customize the page that administrators see when they sign into the admin console using settings in the Authentication > Signing In > Sign-in Pages page. Using settings in this page, you can create welcome messages, sign out messages and other instructions; control page headers; customize select error messages; and create a link to a custom help page within the default Secure Access Service sign-in page. Or, you can upload your own custom sign-in page to the Secure Access Service.
- **UI look and feel**—You can customize the header, background color, and logo displayed in the admin console using settings in the Administrators > Admin Roles > Select Role > General > UI Options page. You can also use settings in this page to enable or disable the “fly out” hierarchical menus that appear when you mouse over one of the menus in the left panel of the admin console.
- **System utilization graphs**—You can choose which system utilization graphs the Secure Access Service displays on the opening page of the admin console using settings in the System > Status > Overview page. You can also use settings in this page to fine-tune the look and data within each of the graphs.
- **Show auto-allow options**—You can show or hide the auto-allow option from yourself or other administrators who create new bookmarks for roles using settings in the Maintenance > System > Options page.
- **User role views**—You can use customization options on the Users > User Roles page to quickly view the settings that are associated with a specific role or set of roles.
- **User realm views**—You can use customization options on the Users > User Realms page to quickly view the settings that are associated with a specific user realm or set of user realms.

- **Resource policy views**—You can limit which resource policies the Secure Access Service displays on any given resource policy page based on user roles. For instance, you can configure the Users > Resource Policies > Web page of the admin console to only display those resource policies that are assigned to the “Sales” user role. You can customize these using settings in the Users > Resource Policies > Select Policy Type page of the admin console.
- **Web resource policy views**—You can limit which Web resource policy configuration pages the Secure Access Service displays using settings in Users > Resource Policies > Web > Policy Type of the admin console.
- **Administrator roles**—You can delegate select responsibilities to other administrators using settings in the Administrators > Admin Roles section of the admin console. In doing so, you can restrict the visibility of certain options and capabilities to those other administrators.

## Customizable End-User Interface Elements Overview

The Secure Access Service enables you to customize the look and feel of the following elements in the end-user interface:

- **Sign-in pages (default and custom)**—You can customize the page that users see when they sign into the admin console using settings in the Authentication > Signing In > Sign-in Pages page. Using settings in this page, you can create welcome messages, sign out messages and other instructions; control page headers; customize select error messages; and create a link to a custom help page within the default Secure Access Service sign-in page. Or, you can upload your own custom sign-in page to the Secure Access Service.
- **UI look and feel**—You can customize the header, background color, and logo displayed in the admin console using settings in the Users > User Roles > Select Role > General > UI Options page. You can also use settings in this page to specify the first page the users see after they sign into the Secure Access Service, the order in which the Secure Access Service displays bookmarks, the help system that the Secure Access Service displays to users, and various toolbar settings.
- **Default messages and UI look and feel**—You can specify what the default look and feel should be for all user roles using settings in Users > User Roles > [Default Options] pages of the admin console. You can also use settings in these pages to define the default errors that users see when they try to access a blocked site, SSO fails, or SSL is disabled.

# SA6000 Series Appliance

- [SA6000 Series Appliance on page 1105](#)
- [SA6000 Field-Replaceable Units on page 1106](#)

## SA6000 Series Appliance

---

The Juniper Networks SA6000 Series Appliance is a next-generation appliance featuring a number of notable hardware design upgrades relative to the other members of the Secure Access Service family.

The SA6000 chassis features the following hardware components:

- Console port—You can use the console port to initially set up the SA6000 before you fully integrate it as the secure gateway to your internal network. You can also use the console port to perform certain configuration and clustering tasks after the Secure Access Service begins operating as the secure gateway.
- Port 0 (internal) and Port 1 (external) Ethernet ports—The SA6000's primary connections to the corporate network and the outside world are the internal and external Ethernet ports, respectively. You can configure the internal and external interfaces via the System > Network page of the admin console.
- Management port—The SA6000's management port is now available and:
  - Enables seamless integration into a dedicated Management Network.
  - Provides continuously available management access to the Secure Access Service.
  - Enables you to perform management activities without impacting user traffic.
  - Allows you to separate administrative access from user access between the Secure Access Service and Enterprise devices on the internal network.

You can configure the Management port information and advanced settings via the admin console, just as you would configure the internal port.

- Dual SFP ports—The SA 6000 includes two Small Form-factor Pluggable (SFP) Gigabit Ethernet ports (designated ports 2 and 3 on the front of the SA 6000) that offer you the ability to further increase your connectivity to internal network components.
- Status LEDs—The front of the SA 6000 chassis features the following LEDs:

- PWR (green)—Indicates that the appliance has power and is turned on.
- HD (amber)—Indicates that the hard disk is in use (writing or reading data).
- TEMP (red)—A blinking LED indicates that one of the fans has failed or is not seated properly in its port, or that a fan has failed and needs to be replaced. A solid LED indicates a high internal temperature reading that may result in system failure if not addressed.
- PS FAIL (red)—Indicates that one of the power supplies is faulty, has been unplugged, or has experienced an outright failure.
- Port 0 1000 and Port 1 1000 (green)—Indicates that the link speed of the INT 0 (internal) or INT 1 (external) Ethernet interfaces is a Gigabit Ethernet connection.
- Port 0 100 and Port 1 100 (green)—Indicates that the link speed of the INT 0 (internal) or INT 1 (external) Ethernet interfaces is a 100BaseT Ethernet connection.



**NOTE:** If both the Port 0 1000 and Port 0 100 (internal) or Port 1 1000 and Port 1 100 (external) LEDs are active, the link speed for that interface is 10BaseT.

- Internal and external Ethernet LINK TX/RX (green)—Indicates that the internal or external Ethernet interface is currently transmitting or receiving data
- SFP port 2 and 3 LINK (green)—Indicates that SFP port 2 or 3 is enabled.
- SFP port 2 and 3 TX/RX (green)—Indicates that SFP port 2 or 3 is sending or receiving traffic.

**Related Documentation**

- [SA6000 Field-Replaceable Units on page 1106](#)

## SA6000 Field-Replaceable Units

The SA6000 chassis features three types of field-replaceable units (FRUs) that you can add or replace. The FRUs are “hot-swappable,” meaning you do not have to first shut down the SA6000 before adding or replacing any of the FRUs.

- Hard disks—The SA6000 ships with one hard disk, however, you can add an optional second hard disk to the SA6000 chassis to offer component redundancy and help minimize the Secure Access Service down time. When a second (redundant) hard disk is installed, it maintains an exact copy of the software image and configuration information on the working hard disk. Therefore, if the working hard disk fails, the redundant hard disk immediately assumes responsibility for all Secure Access Service operations. This function is referred to as the Redundant Array of Independent Disks (RAID) mirroring process.



**NOTE:** The SA6000 hard disk modules are hot-swappable. You must make sure that the Secure Access Service finishes booting and is operating correctly before removing, replacing, or upgrading a hard disk module. Once a new hard disk module is inserted, you must wait until the RAID mirroring process is completely finished—which takes approximately 40 minutes—before rebooting or turning off the Secure Access Service.

- **Power supplies**—The SA6000 ships with one AC power supply installed in the back of the chassis. You can add an optional second power supply to support redundancy and load-sharing features. In addition, if you need to replace one of the power supplies, you can “swap” the faulty power supply for a replacement while the optional second power supply assumes responsibility for the entire power load, thus avoiding a situation where you have to power off the Secure Access Service before replacing the removable unit.
- **Cooling fans**—The SA6000 ships with two cooling fans installed in the back of the chassis. If you need to replace one of the cooling fans, you can “swap” the faulty fan for a replacement during operation in a matter of moments. You can purchase additional cooling fans from your vendor when you order your SA6000, or you can purchase them in the future to replace faulty or failed cooling fans, as necessary, in the future. Juniper strongly recommends that you run the SA 6000 with two cooling fans.

For information about installing or replacing any of the hardware mentioned here, see the *SA6000 Field Replaceable Units Removal and Installation Guide* on the Juniper Networks Customer Support Center.

**Related  
Documentation**

- [SA6000 Series Appliance on page 1105](#)





# SA4500 and SA6500 Series Appliances

- [SA4500 and SA6500 on page 1109](#)
- [Device Status LED Behavior on page 1111](#)
- [Ethernet Port LED Behavior on page 1112](#)
- [Replacing the Cooling Fans on page 1113](#)
- [Replacing a Hard Drive on page 1114](#)
- [Replacing IOC Modules on page 1114](#)
- [Replacing a Power Supply on page 1116](#)

## SA4500 and SA6500

---

The SA4500 and SA6500 (SA 4500/6500) are next-generation appliances featuring a number of notable hardware features.

### Standard Hardware

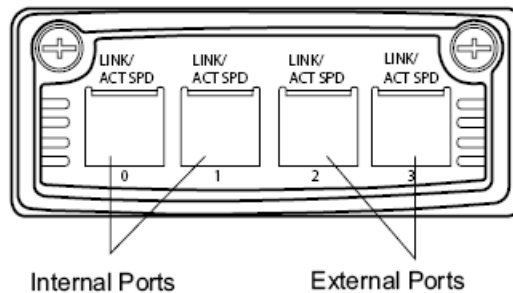
The SA 4500/6500 chassis features the following hardware components:

- **Console port**—You use the console port to initially set up the SA 4500/6500 before you fully integrate it as the secure gateway to your internal network. You can also use the console port to perform certain configuration and clustering tasks after the Secure Access Service begins operating as the secure gateway.
- **Bonding ports**—By default, on the SA6500 only, the Secure Access Service uses bonding of the multiple ports to provide failover protection. Bonding two ports on the Secure Access Service automatically shifts traffic to the secondary port when the primary port fails.

The SA6500 appliance bonds ports as follows:

- Internal port = Port 0+Port 1

- External port = Port 2+Port 3



The Secure Access Service indicates in a message on the System > Network > Overview page of the administrator admin console whether or not the failover functionality is enabled.

Bonding ports cannot span separate networks (multi-homed).

- Management port—The SA6500's management port:
  - Enables seamless integration into a dedicated Management Network.
  - Provides continuously available management access to the Secure Access Service.
  - Enables you to perform management activities without impacting user traffic.
  - Allows you to separate administrative access from user access between the Secure Access Service and Enterprise devices on the internal network.

You can configure the Management port information and advanced settings via the admin console, just as you would configure the internal port.

- SFP ports—4-port Small Form-factor Pluggable (SFP) ports are available as an optional feature for link redundancy to internal switches.
- Status LEDs—Three device status LEDs are located on the left-side of the front panel to display power, hard disk access and fault status.
- Ethernet Port LEDs—The Ethernet port LEDs show the status of each Ethernet port.

The appliance supports up to four node active/active clusters or 2 node active/passive.

## SA Series 6500 Field-Replaceable Units

The SA 6500 chassis features three types of field-replaceable units (FRUs) that you can add or replace. The FRUs are “hot-swappable,” meaning you do not have to first shut down the SA 6500 before adding or replacing any of the FRUs. The SA4500 has a “cold-swappable” power supply.

For safety information, refer to the *Juniper Networks Products Safety Guide* available on the Juniper Networks Support site.

- **Hard disks**—The SA6500 ships with one hard disk, however, you can add an optional second hard disk to the SA6500 chassis to offer component redundancy and help minimize the Secure Access Service down time. When a second (redundant) hard disk is installed, it maintains an exact copy of the software image and configuration

information on the working hard disk. Therefore, if the working hard disk fails, the redundant hard disk immediately assumes responsibility for all Secure Access Service operations. This function is referred to as the Redundant Array of Independent Disks (RAID) mirroring process.



**NOTE:** The SA6500 hard disk modules are hot-swappable. You must make sure that the Secure Access Service finishes booting and is operating correctly before removing, replacing, or upgrading a hard disk module. After you insert a new hard disk module, you must wait until the RAID mirroring process is completely finished—which takes approximately 40 minutes—before rebooting or turning off the Secure Access Service.

- **Power supplies**—The SA6500 ships with one AC power supply installed in the back of the chassis. You can add an optional second power supply to support redundancy and load-sharing features. In addition, if you need to replace one of the power supplies, you can “swap” the faulty power supply for a replacement while the optional second power supply assumes responsibility for the entire power load, thus avoiding a situation where you have to power off the Secure Access Service before replacing the removable unit.
- **Cooling fans**—The SA6500 ships with two cooling fans installed in the back of the chassis. If you need to replace one of the cooling fans, you can “swap” the faulty fan for a replacement during operation in a matter of moments. You can purchase additional cooling fans from your vendor when you order your SA6500, or you can purchase them in the future to replace faulty or failed cooling fans, as necessary, in the future.

**Related Documentation**

- [Device Status LED Behavior on page 1111](#)
- [Ethernet Port LED Behavior on page 1112](#)
- [Replacing the Cooling Fans on page 1113](#)
- [Replacing a Hard Drive on page 1114](#)
- [Replacing IOC Modules on page 1114](#)
- [Replacing a Power Supply on page 1116](#)

## Device Status LED Behavior

Startup takes approximately one minute to complete. If you want to turn the device off and on again, we recommend you wait a few seconds between shutting it down and powering it back up.

There are three device status LEDs located on the left-side of the front panel:

- Power
- Hard disk access
- Fault

Table 76 on page 1112 lists the name, color, status, and description of each device status LED.

**Table 76: Device Status LEDs**

Name	Color	State	Description
POWER	Green	Off	Device is not receiving power
		On Steady	Device is receiving power
HARD DISK ACCESS	Yellow	Off	Hard disk is idle
		Blinking	Hard disk is being accessed
FAULT	Red	Off	Device is operating normally
		Slow blinking	Power supply fault
		Fast blinking	Fan failure
		Solid	Thermal failure

**Related Documentation**

- [SA4500 and SA6500 on page 1109](#)
- [Ethernet Port LED Behavior on page 1112](#)
- [Replacing the Cooling Fans on page 1113](#)
- [Replacing a Hard Drive on page 1114](#)
- [Replacing IOC Modules on page 1114](#)
- [Replacing a Power Supply on page 1116](#)

## Ethernet Port LED Behavior

The Ethernet port LEDs show the status of each Ethernet port.

**Table 77: 4-Port Copper Gigabit Ethernet LEDs (available on IC4500 and IC6500)**

LED	Color and State	Description
Link/Activity	Green	Link
	Blinking green	Activity

**Table 77: 4-Port Copper Gigabit Ethernet LEDs (available on IC4500 and IC6500) (continued)**

LED	Color and State	Description
Link Speed	Off	10 Mbps
	Green	100 Mbps
	Yellow	1 Gbps

**Related Documentation**

- [SA4500 and SA6500 on page 1109](#)
- [Device Status LED Behavior on page 1111](#)
- [Replacing the Cooling Fans on page 1113](#)
- [Replacing a Hard Drive on page 1114](#)
- [Replacing IOC Modules on page 1114](#)
- [Replacing a Power Supply on page 1116](#)

## Replacing the Cooling Fans

The SA 6500 ships with two cooling fans installed in the back of the chassis. If you need to replace one of the cooling fans, you can “hot-swap” the faulty fan for a replacement during operation in a matter of moments. You can purchase additional cooling fans from your authorized Juniper reseller, or you can purchase them in the future to replace faulty or failed cooling fans, as necessary.

To remove and install a cooling fan module:

1. To release the cooling fan module, do one of the following:
  - Press and slide the release trigger toward the center of the cooling fan module
  - Loosen the thumbscrews
2. Grasp the cooling fan module and carefully pull it out.



**CAUTION:** Once you remove the cooling fan module, it is important that you replace it with a replacement cooling fan. The second fan is required for proper air flow across the chassis’s internal components; it is not a redundant fan.

3. Line the a cooling fan module up with an empty cooling fan port on the back of the chassis.
4. Slowly slide the module into the chassis until it clicks into place.
5. If your cooling fan is equipped with thumb screws, tighten the screws.

- Related Documentation**
- [SA4500 and SA6500 on page 1109](#)
  - [Replacing a Hard Drive on page 1114](#)
  - [Replacing IOC Modules on page 1114](#)
  - [Replacing a Power Supply on page 1116](#)

---

## Replacing a Hard Drive

The SA 6500 ships with two standard hard drives to offer component redundancy and help minimize down time. The second (redundant) hard disk maintains an exact copy of the software image and configuration information on the working hard disk. Therefore, if the working hard disk fails, the redundant hard disk immediately assumes responsibility for all operations. This function is referred to as the Redundant Array of Independent Disks (RAID) mirroring process.



**NOTE:** The hard disk modules are hot-swappable. Once a new hard disk module is inserted, you should wait until the RAID mirroring process has completed before rebooting or turning off the appliance.

To remove and install a hard drive:

1. On the hard drive module, press the blue handle release trigger in and to the right to release the insertion and removal handle.
2. Grasp the handle and pull the hard drive module straight out of the chassis.  
  
Once you have removed the hard drive module, be sure to replace it with a replacement hard drive.
3. With the insertion and removal handle on the hard drive module in the released/out position, line the hard drive module up with an empty hard drive port on the front of the chassis.
4. Carefully slide the hard drive module into the chassis until it clicks into place.

Retract the handle by swinging it back across the face of the hard drive until it is completely flush with the face of the hard drive module.

- Related Documentation**
- [SA4500 and SA6500 on page 1109](#)
  - [Replacing the Cooling Fans on page 1113](#)
  - [Replacing IOC Modules on page 1114](#)
  - [Replacing a Power Supply on page 1116](#)

---

## Replacing IOC Modules

This section contains information about removing and installing IOC Modules (IOMs) in the SA 6500.



**CAUTION:** Power off the device before removing or installing IOMs. IOMs are not hot-swappable.

### Removing a Blank IOM Faceplate

To maintain proper airflow through the device, leave blank faceplates in place over slots that do not contain IOMs. Do not remove a blank faceplate unless you are installing an IOM in the empty slot.

To remove a blank faceplate:

1. Unplug the power cord.
2. Loosen the thumbscrews on each side of the faceplate.
3. Grasp the thumbscrews and pull to remove the faceplate.

### Installing an IOM

1. Unplug the power cord.
2. Line the IOM up with an empty port on the front of the chassis.
3. Carefully slide the IOM in until it seats firmly in the device.
4. Tighten the screws on each side of the IOM faceplate.
5. Insert the appropriate cables into the cable connectors on the IOM.
6. If necessary, arrange the cables to prevent them from dislodging or developing stress points:
  - Secure the cable so that it is not supporting its own weight as it hangs to the floor.
  - Place excess cable out of the way in a neatly coiled loop.
  - Use fasteners to maintain the shape of cable loops.
7. Insert the power cord into the AC power receptacle.

### Removing an IOM

To remove an IOM:

1. Unplug the power cord.
2. Disconnect the cables from the IOM.
3. If necessary, arrange the cables to prevent them from dislodging or developing stress points.
4. Loosen the thumb screws on each side of the IOM faceplate.
5. Grasp the thumbscrews and pull to remove the IOM.

If you are not reinstalling an IOM into the empty slot, install a blank IOM faceplate over the empty slot to maintain proper airflow.

- Related Documentation**
- [SA4500 and SA6500 on page 1109](#)
  - [Replacing a Hard Drive on page 1114](#)
  - [Replacing a Hard Drive on page 1114](#)
  - [Replacing a Power Supply on page 1116](#)

## Replacing a Power Supply

---

### Removing and Installing an AC Power Supply

The Juniper Networks appliance ships with one AC power supply installed in the back of the chassis. You can add an optional second power supply to support redundancy and load-sharing features. In addition, if you need to replace one of the power supplies, you can “hot-swap” the faulty power supply for a replacement while the optional second power supply assumes responsibility for the entire power load, thus avoiding a situation where you have to power off the Secure Access Service before replacing the removable unit.

To remove and install an AC power supply module:

1. Press the release trigger in and to the right to release the module.
2. Grasp the insertion and removal handle and pull the power supply module straight out of the chassis.

Once you have removed the supply module, be sure to replace it with a replacement power supply or the “dummy” power supply port cover installed in your chassis at the time of shipping.

3. Line the new power supply module up with an empty power supply port on the back of the chassis.
4. Slowly slide the power supply module into the chassis until it clicks into place.

### Removing and Installing a DC Power Supply

To remove and install a DC power supply module:

1. Unplug the power cord.
2. Disconnect the DC supply wires from the lugs on the DC power supply.
3. Press the release trigger in and to the right to release the module.
4. Grasp the power supply module and pull it straight out of the chassis.
5. Slowly slide the new module into the chassis until it clicks into place.
6. Connect the DC supply wires to the module using the lugs. Be sure to attach the ground wire.
7. Attach the power cord



- Related Documentation**
- [SA4500 and SA6500 on page 1109](#)
  - [Replacing the Cooling Fans on page 1113](#)
  - [Replacing a Hard Drive on page 1114](#)
  - [Replacing IOC Modules on page 1114](#)



# Secure Access FIPS

- [SA FIPS on page 1119](#)
- [SA FIPS Execution on page 1120](#)
- [Creating Administrator Cards on page 1121](#)
- [Deploying a Cluster in a Secure Access FIPS Environment on page 1122](#)
- [Creating a New Security World on page 1124](#)
- [Recovering an Archived Security World on page 1127](#)

## SA FIPS

---

FIPS, or Federal Information Processing Standards, are National Institute of Standards and Technology regulations for handling keys and encrypting data. Juniper Networks SA FIPS is a standard SA4000 or SA6000 NetScreen Instant Virtual Extranet equipped with a FIPS-certified cryptographic module. The tamper-proof hardware security module installed on an SA FIPS Series Appliance is certified to meet the FIPS 140-2 level 3 security benchmark. The module handles private cryptographic key management and SSL handshakes, simultaneously, ensuring FIPS compliance and off-loading CPU-intensive public key infrastructure (PKI) tasks from the Secure Access Service to a dedicated module.

The configuration process for SA FIPS administrators is almost exactly the same as for the non-SA FIPS administrators, requiring only minor configuration changes during the initialization, clustering, and certificate generation processes. In the few cases where administration tasks are different, this guide includes the appropriate instructions for both SA and SA FIPS administrators. For end-users, SA FIPS is exactly the same as a standard Secure Access Service system.

SA FIPS is a hardware feature that is built into selected Secure Access Services. It is not available on SA700 Series Appliances.

### Related Documentation

- [SA FIPS Execution on page 1120](#)
- [Creating Administrator Cards on page 1121](#)
- [Creating a New Security World on page 1124](#)
- [Recovering an Archived Security World on page 1127](#)
- [SA FIPS Execution on page 1120](#)

## SA FIPS Execution

---

When you first install a FIPS system, the Secure Access Service serial console walks you through the process of creating a security world through the serial console. A security world is a key management system used by SA FIPS consisting of the following elements:

- **Cryptographic module**—The cryptographic module (also sometimes called the hardware security module, or HSM) included with SA FIPS Appliance includes hardware and firmware installed directly on the appliance. A security world may contain a single cryptographic module (standard environment) or multiple modules (clustered environment). However, a single Secure Access FIPS appliance is always equipped with a single cryptographic module.
- **Security world key**—A security world key is a unique Triple DES encrypted key that protects all other application keys within a security world. As required by the Federal Information Processing Standards, you cannot import this key into a security world—you must directly create it from a cryptographic module. In a clustered environment, all of the modules within the security world share the same security world key.
- **Smart cards**—A smart card is a removable key device that looks like a credit card. A smart card authenticates users, allowing them access to various data and processes controlled by the cryptographic hardware module. During the initialization process, you must insert one of your smart cards into the reader (built-in or external, depending upon which device model you own). As part of the initialization process, the smart card is transformed into an administrator card that allows the card holder access to the security world.
- **Encrypted data**—Encrypted host data in a Secure Access FIPS environment includes keys and other data required to share information in a secure manner.

These elements interlock to create a comprehensive security world. When you start the appliance, it confirms that the security world is valid and that the cryptographic module is in operational mode before starting normal operations.

You can set the cryptographic module into operational mode using a hardware switch on the outside of the module. The switch's settings include:

- **I**—Initialization mode. Use this setting when initializing the cryptographic module with a new security world or when adding a module to an existing security world in a Secure Access cluster. Note that once you set the switch to I and begin initialization, you must complete the process. Otherwise, your security world is only partially initialized, making it unusable.
- **O**—Operational mode. Use this setting to place the cryptographic module into operational mode after initialization. Note that you must set the switch to O before the module powers up in order to alert the unit that you want to begin day-to-day processing. Otherwise, the module prompts you through the serial console to join the existing security world or initialize a new one.
- **M**—Maintenance mode. In future releases, this setting will be used to upgrade the firmware on the cryptographic module. (Not yet supported.)

- Related Documentation**
- [SA FIPS on page 1119](#)
  - [Creating Administrator Cards on page 1121](#)
  - [Creating a New Security World on page 1124](#)
  - [Recovering an Archived Security World on page 1127](#)

## Creating Administrator Cards

---

When you receive your Secure Access FIPS product, you receive 6 smart cards as part of the package. A smart card is a removable key device that you must use in order to gain access to some of the critical data and processes controlled by the cryptographic module. Secure Access FIPS first requires you to use one of your smart cards while initializing the cryptographic module through the serial console. During this process, Secure Access FIPS creates a security world and transforms the smart card into an administrator card that gives the holder access only to that security world.

Once the module is initialized, you do not need the administrator card for normal Secure Access operations. However, you are required to use the administrator card whenever you want to add another Secure Access FIPS machine to a cluster, reinitialize a module with a new or different security world or replace administrator cards.

As a rule-of-thumb, any Secure Access FIPS operation that you must execute through the Secure Access serial console requires an administrator card.



**NOTE:** Whenever you change your security world, you must determine how to handle your existing administrator cards. Your choices include:

- Reset your existing administrator cards to the new security world.
- Use administrator cards that are pre-initialized to the new security world and leave your existing administrator cards unchanged. Note that if you choose this option, however, you cannot use the old, unchanged cards to access the new security world.

---

### Administrator Card Precautions

Since administrator cards are so critical to Secure Access FIPS operations and the security of the keys within your security world, we strongly recommend that you take the following precautions:

- Create multiple administrator cards—You cannot replace an administrator card unless you have another valid card and the pass phrase for that card; the cryptographic module does not store administrator card recovery data. Therefore, we strongly recommend that you create at least one administrator card for standard administrative operations and another for backup purposes. Otherwise, you run the risk of losing your only administrator card and subsequently losing access to your security world and all the data it stores. You can only create a set of administrator cards, all at once. You cannot add additional cards to an existing set.
- Store a backup administrator card in a secure location—Always keep your backup administrator card(s) in a secure location separate from the card you use for standard administrative operations to ensure that you do not lose all of your administrator cards to the same event (such as a fire or theft).
- Overwrite all remaining administrator cards if one gets lost—If you lose or damage an administrator card, immediately create a new security world and overwrite all remaining cards from the old security world. Otherwise, an attacker with an old administrator card may be able to access old host data stored on a backup tape or another host. With the old host data and an old card, the attacker may then be able to re-create your keys.
- Protect the administrator card's pass phrase—For maximum security, you should never write down your pass phrase, tell it to untrusted users, or use a pass phrase that is easy to guess. Protecting your pass phrase adds an extra level of security to your operations.
- Only use your administrator card with known, trusted sources—Always obtain smart cards from a trusted source, never insert a smart card into an untrusted smart card reader, and never insert untrusted smart cards into your smart reader.

**Related Documentation**

- [SA FIPS on page 1119](#)
- [Creating a New Security World on page 1124](#)
- [Recovering an Archived Security World on page 1127](#)

---

## Deploying a Cluster in a Secure Access FIPS Environment

---

In addition to sharing state, user profile, user session, and monitoring state data, the members of a Secure Access FIPS cluster also share security world data. All cluster members share the same private key and are accessible using the same administrator cards. Since changing a security world requires physical access to a cryptographic module, however, Secure Access FIPS cluster members cannot share all of their data using the standard Secure Access synchronization process. Instead, to create a Secure Access FIPS cluster, you must:

- Create a cluster of Secure Access FIPS machines through the admin console—As with a standard Secure Access cluster, each cluster node in a Secure Access FIPS cluster is initialized using system state data from the specified cluster member, overwriting all existing data on the node machine.
- Manually update the security world on each of the machines—After creating a cluster, you must initialize each cluster node with the specified member's security world using

an administrator card that is pre-initialized to the security world and the serial console. Prior to joining a cluster, each node is in its own security world. As a consequence, after a node joins the cluster, the administrator card from the joining node will be invalid. Only the administrator card set from the cluster will be valid.

Similarly, if you want to modify an existing security world on a cluster, you must individually update each cluster member's cryptographic module using an administrator card and the Secure Access serial console.

The basic process for creating a cluster follows these high-level steps:

1. Initialize one Secure Access from the serial console, creating administrator cards.
2. Create the cluster from this Secure Access' admin console.
3. Add nodes to the cluster from this Secure Access' admin console.
4. Reboot the joining node from the serial console.
5. When prompted, supply the cluster details, including the current node's IP address, netmask, and domain.
6. When prompted, insert an administrator card from the cluster's set of cards. The node's administrator card, if any, will become invalid as the node joins the security world of the cluster.

To initialize a FIPS cluster member's security world via the serial console:

1. Insert an administrator card that is pre-initialized with the active cluster member's security world into the smart card slot with the contacts facing up.



**NOTE:** If you have already performed the procedures required to configure the FIPS appliance, as described in the Quick Start Guide, you might be able to skip this step.

2. Switch the cryptographic module's mode switch to I (initialization mode) if it is not already in that position.
3. Connect to the machine's serial console.
4. Cycle the power to reboot the machine and watch its serial console. After the system software starts, you will see a message that the machine is about to boot as a stand-alone Secure Access and to hit Tab for clustering options. Press the Tab key as soon as you see this option.



**NOTE:** The interval to press the Tab key is five seconds. If the machine begins to boot in stand-alone mode, wait for it to finish and then reboot again.

5. Enter the number 2 to join the existing cluster or 1 to continue as a standalone Secure Access.

6. Enter the initialization information as prompted, including:

- Cluster name
- Cluster password
- IP address of a node in the cluster
- IP address of the node you are adding
- Netmask
- Gateway IP address



**NOTE:** After you initialize members of a Secure Access FIPS cluster with the same security world, you may disable and re-enable the cluster through the admin console. You are no longer required to use the serial console once the cluster members are all members of the same security world.

7. Select 1 to continue joining the cluster.

8. After the FIPS appliance initializes the card, switch the cryptographic module's mode switch to O (operational mode).

**Related  
Documentation**

- [Using the Serial Console on page 1097](#)

## Creating a New Security World

You cannot begin using a Secure Access FIPS machine until you create a security world on it. However, in some case you may need to overwrite that security world with a new one. For example, if you lose an administrator card, we recommend that you create a brand new security world to prevent an untrusted source from finding the card and accessing your security world. You may also need to create a new security world if you cannot remember your original administrator cards pass phrases.

In order to create a new security world, you must have physical access to:

- The cryptographic module(s) that belong to the security world.
- A smart card reader (if you use an older model Secure Access device that does not contain a built-in card reader).
- One or more unformatted smart cards or administrator cards containing data that you can safely overwrite.



**NOTE:** Your old administrator cards will not work with the new security world until you reformat them with the new security world's data. Also note that once you set the switch to I and begin initialization, you must complete the process. Otherwise, your security world is only partially initialized, making it unusable.





**WARNING:** You must obtain one or more new device certificates from your CA whenever you create a new security world.

### Creating a Security World on a Stand-Alone Secure Access

To create a new security world on a stand-alone Secure Access:

1. Insert an un-formatted smart card or an administrator card containing data that you can safely overwrite into the card slot with the card contacts facing up.
2. Set the mode switch on the cryptographic module to I (initialization mode).
3. Access the Secure Access serial console and reboot the Secure Access device. After the Secure Access device reboots, you are prompted on the serial console with the following question: **Do you want to use the currently installed security world (y/n)?**
4. Perform one of the following:
  - If you want to create a new security world, then:
    - a. Enter n and press Enter.
    - b. You are asked to confirm this choice with the prompt "Are you sure you want to delete your existing Security World (including server certificates) (y/n)?" If you choose to continue enter y and press Enter.
    - c. Enter the number of administrator cards you want to create and press Enter.
    - d. Enter y and press Enter to confirm the number of cards you want to create.
  - If you want to use the currently installed security world, then:
    - a. Enter y and press Enter.
    - b. Proceed to the next numbered step in this procedure.
5. Reset the cryptographic module's mode switch to O (operational mode).
6. Add the common name and company name when prompted. The system uses the existing self-signed certificate temporarily.
7. Create a new device certificate that shares the new security world's private key.



**WARNING:** You must obtain one or more new server certificates from your CA whenever you create a new security world.

### Creating a Security World in a Clustered Environment

To create a new security world in a clustered environment:

1. Sign in to the admin console of a cluster node. To access a node's admin console, enter its internal IP address followed by "/admin" in a browser. For example:  
  
`https://x.x.x.x/admin`
2. On the System > Clustering > Status tab, select the checkbox for all nodes other than the current node in the Cluster Members column and then click **Disable**.
3. Initialize the cluster member with a security world. If this is the first node in the cluster, create a new security world.
4. Return to the node's System > Clustering > Status tab, select the checkbox next to disabled nodes in the Cluster Members column, and then click **Enable**.
5. Wait for all the cluster members to go into an "Enabled" state.
6. Set the mode switch on the cryptographic modules of cluster members that were earlier disabled to I (initialization mode).
7. Reboot each of these nodes from the serial console.
8. After a node joins the security world, reset its cryptographic module's mode switch to O (operational mode).

### Replacing Administrator Cards

You can replace an administrator card by selecting the **Replace Administrator Card Set** option from the serial console. You cannot increase the number of administrator cards in an existing set. If you want to do this, you have to create a new security world which replaces all of the existing cards in a set and allow you to create a set with a larger or smaller number of cards.



**NOTE:** Replacing administrator cards restarts services on your standalone Secure Access device or cluster.

---

If you need to replace administrator cards for a security world, you must have physical access to:

- A cryptographic module that belongs to the security world.
- A smart card reader (if you use an older model Secure Access device that does not contain a built-in card reader).
- An administrator card that is pre-initialized with the security world.
- An un-formatted smart card or administrator card containing data that you can safely overwrite.
- The same number of unformatted smart cards or administrator cards as in the original set containing data that you can safely overwrite.



**NOTE:** If you need to replace administrator cards, you must replace the same number of cards that you first initialized for the security world. You cannot replace a subset of the cards.



**NOTE:** If you require additional smart cards, please contact your Secure Access Reseller.

To replace all administrator cards or to create a larger number of cards for a security world:

1. Create a new security world.
2. Choose **Replace Administrator Card Set** from the list of configuration tasks.
3. Enter the pass phrase for the security world.
4. When prompted, insert an un-formatted smart card or an administrator card whose data you can safely overwrite into the smart card reader with the contacts facing up.
5. Enter the additional initialization information for which you are prompted.
6. Repeat steps 4 and 5 for as many cards as you want to create.
7. Store at least one of the administrator cards in a secure location.

**Related  
Documentation**

- [Recovering an Archived Security World on page 1127](#)

## Recovering an Archived Security World

In rare cases, you may need to recover your system using an archived security world. The archived security world may be an older version of the security world that already exists on your system or the same version. In order to recover your system, you must have access to the system configuration file (by default, `system.cfg`) that holds the archived security world and its corresponding certificate.

In addition, if you are overwriting your security world with a different security world, you must have physical access to:

- All of the cryptographic modules that belong to the security world.
- A smart card reader (if you use an older model Secure Access device that does not contain a built-in card reader).
- An administrator card that is pre-initialized with the security world and administrator passphrase that you want to import.

### Importing a Security World Into a Stand-Alone Secure Access Device

To import an existing security world into a stand-alone Secure Access device:

1. Import the system configuration file that contains the archived security world and its corresponding certificate into the Secure Access device, and then initialize the security world if necessary. If the configuration file contains an archive of:
  - The same security world that was already present on the machine, no further configuration is required.
  - A different security world than was already present on the machine, you must initialize the new security world.



**NOTE:** If you import a configuration file containing a different security world, note that your existing administrator cards will not work with the imported security world until you reformat them with the new security world's data. Also note that once you set the switch to I and begin initialization, you must complete the process. Otherwise, your security world is only partially initialized, making it unusable.

2. Insert an administrator card that is pre-initialized with the imported security world into the smart card reader slot with the contacts facing up.
3. Set the mode switch on the cryptographic module to I (initialization mode).
4. Access the Secure Access device's serial console and reboot the Secure Access device.
5. Reset the cryptographic module's mode switch to O (operational mode) when prompted.

### Importing a Security World Into a Cluster

To import an existing security world into a cluster:

1. Sign in to the admin console of a cluster node. To access a node's admin console, enter its internal IP address followed by "/admin" in a browser. For example:  
`https://x.x.x.x/admin`
2. On the System > Clustering > Status tab, select the checkbox for all nodes other than the current node in the Cluster Members column and then click **Disable**.
3. Import an archived security world in to the cluster member.
4. When the installation process completes, return to the node's System > Clustering > Status tab, select the checkbox next to the disabled nodes in the Cluster Members column, and then click **Enable**.
5. Wait for all the cluster members to go into the "Enabled" state.
6. Set the mode switch on the cryptographic modules of cluster members' that were earlier disabled to I (initialization mode).

7. Reboot each of these nodes from the serial console.
8. After a node joins the security world, reset its cryptographic module's mode switch to O (operational mode).

**Related Documentation** • [Creating a New Security World on page 1124](#)



# SA4500 and SA6500 FIPS Appliances

- [FIPS Overview on page 1131](#)
- [Name and Password Restrictions on page 1132](#)
- [Initializing a Keystore on page 1133](#)
- [Reinitializing the Keystore on page 1133](#)
- [Joining a Cluster on page 1134](#)
- [Importing Device Certificates on page 1135](#)
- [Changing the Security Officer Password on page 1135](#)
- [Changing the Web User Password on page 1136](#)
- [Resetting the HSM Card In Case Of An Error on page 1137](#)
- [Upgrading the HSM Firmware on page 1137](#)
- [Binary Importing and Exporting of the Keystore on page 1138](#)
- [FIPS Device Status LED Behavior on page 1138](#)

## FIPS Overview

---

The Juniper Networks SA 4500 and 6500 FIPS is a standard SA4500 or SA6500 appliance equipped with a FIPS-compliant crypto card. The tamper-proof hardware security module installed on a Secure Access FIPS system is certified to meet the FIPS 140-2 level 3 security benchmark.

The configuration process for Secure Access FIPS administrators is almost exactly the same as for the non-FIPS Secure Access administrators, requiring only minor configuration changes during the initialization, clustering, and certificate generation processes. In the few cases where administration tasks are different, this guide includes the appropriate instructions for both Secure Access and Secure Access FIPS administrators. For end-users, Secure Access FIPS is exactly the same as a standard Secure Access system.

The FIPS-compliant crypto card is a host bus adapter card that combines IPsec and SSL cryptographic acceleration with Hardware Security Module (HSM) features. This combination of a dedicated HSM, advanced cryptographic security and secure key management meet the security and performance needs for any service.

This card has two main roles: a security officer and a user role. The FIPS-compliant crypto card replaces the need for administrator cards with the concept of a security officer who

is responsible for key and password management. The security officer credential protects the keystore from being exported and imported onto another FIPS-compliant crypto card.

User roles perform cryptographic operations such as accessing keying material within the keystore as well as performing bulk encryption operations.

The security officer credentials, user credentials, and RSA private keys are stored in the HSM encrypted keystore located on the Secure Access disk. You are prompted to provide these credentials whenever any operation requires them. Credentials are not automatically retrieved from the HSM keystore.

Keystores are stored on the disk and are encrypted with a master key. The master key is stored in the crypto card firmware and can be backed up by a security officer using a restore password. This restore password can then be used to restore the master key onto the same or different FIPS-compliant crypto cards allowing the keystore to be shared across a cluster, for example.

#### Related Documentation

- [Name and Password Restrictions on page 1132](#)
- [Initializing a Keystore on page 1133](#)
- [Reinitializing the Keystore on page 1133](#)
- [Joining a Cluster on page 1134](#)
- [Importing Device Certificates on page 1135](#)
- [Changing the Security Officer Password on page 1135](#)
- [Changing the Web User Password on page 1136](#)
- [Resetting the HSM Card In Case Of An Error on page 1137](#)
- [Upgrading the HSM Firmware on page 1137](#)
- [Binary Importing and Exporting of the Keystore on page 1138](#)

## Name and Password Restrictions

Security officer names and usernames must adhere to the following requirements:

**Table 78: Security Officer Name and Username Requirements**

Security Officer Name and Username Requirement	Description
Minimum Length	At least one character
Maximum Length	63 characters
Valid Characters	Alphanumeric, underscore (_), dash (-) and period (.)
First Character	Must be alphabetic



Passwords must be at least six characters and no more than 63 characters. Three characters must be alphabetic and one character must be non-alphabetic.

**Related Documentation**

- [FIPS Overview on page 1131](#)

## Initializing a Keystore

When the FIPS appliance is powered on from a factory-reset or when its configuration is reset, the serial console requires the initialization of a keystore and a self-signed device certificate. The steps for initialization are:

- During the boot process, the current release's HSM firmware is installed on the FIPS-compliant crypto card HSM.
- You are prompted to create a new keystore. As part of the new keystore creation, you must provide the following data:
  - The security officer name and password. Save these credentials as they are required for such tasks as creating new restore passwords and for changing the security officer password.
  - The keystore restore or HSM master key backup password. Every time you export the system configuration, save the current restore password for the archived keystore.
  - Web username and password for running cryptographic operations using keys stored in the HSM's keystore.
- The self-signed certificate creation proceeds as normal except that the HSM is used to generate a secure RSA private key which is stored in the HSM's database.

**Related Documentation**

- [FIPS Overview on page 1131](#)

## Reinitializing the Keystore

If there is a change in the security policy of the deployment that requires the creation of new RSA key pairs and corresponding certificates, you will need to reinitialize the keystore. You can reinitialize the keystore from either a stand-alone node or from a cluster.

To reinitialize the keystore from a stand-alone node:

1. Reboot the stand-alone node.
 

During the boot process, you are prompted to re-initialize the keystore.
2. Press `y` to delete the current keystore and server certificates.



**NOTE:** If you do not press `y` within 10 seconds, the appliance will proceed to boot normally.

To reinitialize the keystore from a cluster:

1. Reboot a node within the cluster.

During the boot process, you are prompted to re-initialize the keystore.

2. Press **y** to delete the current keystore and server certificates. A new keystore is initialized.



**NOTE:** If you do not press **y** within 10 seconds, the appliance will proceed to boot normally.

3. On the node that you rebooted, open the cluster status page in the admin console and wait for all nodes to exit from the “Transitioning” state.
4. For all other nodes in the cluster, connect to the serial console and enter 9 to select FIPS Options and then 1 to select Complete import of keystore and server certificates.
5. Enter the restore password when prompted.

**Related  
Documentation**

- [FIPS Overview on page 1131](#)

---

## Joining a Cluster

Joining a cluster involves using both the admin console and serial console. To join a cluster:

1. If you have not already done so, define and initialize a cluster

If you are currently running stand alone appliances that you want to cluster, we recommend that before you create a cluster, you first configure system and user settings on one machine. After doing so, use the same machine to create the cluster. This machine joins the cluster as part of the creation process. When other Secure Access devices join the cluster, this machine propagates its configuration to the new cluster member.

2. Before you can add an appliance to a cluster, you need to make its identity known to the cluster.
3. Join the appliance to the cluster through the admin console or through the serial console.
  - When joining a node to a cluster using the serial console, you are prompted for the cluster keystore’s restore password. If the restore password fails, enter 9 to select FIPS Option and then enter 1 to select Complete import of keystore and server certificates.

When a cluster is created on a node, the node’s keystore becomes the cluster’s keystore. Any node joining the cluster must import the cluster’s keystore. You need the current keystore restore password to do this.

4. When you see the message confirming that the machine has joined the cluster, click the System > Clustering > Cluster Status tab in the admin console of any active cluster member.
5. When all nodes have exited from the “Transitioning” state, connect to the serial console of each node that has a non-CL license and enter 9 to select FIPS Options and then 1 to select Complete import of keystore and server certificates.
6. Enter the cluster keystore restore password.

**Related Documentation**

- [FIPS Overview on page 1131](#)

## Importing Device Certificates

To import a device certificate, generate a CSR from the appliance and then import its corresponding certificate after it is validated by a CA. Each CSR request generates a new RSA key pair.



**NOTE:** Device certificates without a CSR request from the appliance cannot be imported.



**NOTE:** The SA Series FIPS appliance is said to be in a disassociated state when the key store state in the cache and on disk are different. As a security measure, you cannot create or delete a CSR when the appliance is in a disassociated state. The options are grayed-out. To resolve a disassociated state, connect to the serial console and reload the FIPS keystore database (Option 9 > Sub-option 1).

**Related Documentation**

- [FIPS Overview on page 1131](#)

## Changing the Security Officer Password

Occasionally you may want to change the security officer password. In a cluster, you can perform this operation from any node. The new security officer password is updated to the other nodes automatically.



**NOTE:** Changing the security officer password restarts the web server.

To change the security officer password:

1. Connect to the serial console of the FIPS appliance you want to reset.
2. Enter 9 to select FIPS Option.

3. Enter 2 to select Change security officer password.
4. Enter the existing security officer password.
5. Enter the new password.
6. Re-enter the new password when prompted to confirm.



**NOTE:** The SA Series FIPS appliance is said to be in a disassociated state when the key store state in the cache and on disk are different. As a security measure, you cannot change the security officer password when the appliance is in a disassociated state. The option is disabled. To resolve a disassociated state, connect to the serial console and reload the FIPS keystore database (Option 9 > Sub-option 1).

**Related Documentation**

- [FIPS Overview on page 1131](#)

---

## Changing the Web User Password

---

The web username and password are used to securely store the RSA private keys in the HSM's encrypted database. These credentials are used by the Secure Access Service processes to carry out RSA operations. The keys will never be available for use outside the HSM. You can later change the web password but not the web username.

In a cluster, you can perform this operation from any node. The new password is updated to the other nodes automatically.



**NOTE:** Changing the web user password restarts the web server.

To change the web password:

1. Connect to the serial console of the FIPS appliance you want to reset.
2. Enter 9 to select FIPS Option.
3. Enter 3 to select Change web user password.
4. Enter the existing web user password.
5. Enter the new password.



**NOTE:** The SA Series FIPS appliance is said to be in a disassociated state when the key store state in the cache and on disk are different. As a security measure, you cannot change the web user password when the appliance is in a disassociated state. The option is disabled. To resolve a disassociated state, connect to the serial console and reload the FIPS keystore database (Option 9 > Sub-option 1).

**Related Documentation** • [FIPS Overview on page 1131](#)

## Resetting the HSM Card In Case Of An Error

---

If the FIPS card LEDs indicates an error or fault, try resetting the HSM card prior to rebooting your appliance.

To reset the HSM card:

1. Connect to the serial console of the FIPS appliance you want to reset.
2. Enter 9 to select FIPS Option.
3. Enter 5 to select Reset the HSM.
4. Observe the LEDs on the FIPS card. If they do not eventually turn green, reboot your appliance.

**Related Documentation** • [FIPS Overview on page 1131](#)

## Upgrading the HSM Firmware

---

Some system software upgrades may also require firmware updates. Typically, firmware upgrades occur during the boot process. After the system software updates, the serial console prompts you for the keystore restore password before upgrading the HSM's firmware. If you do not remember the password, you have the option of upgrading the firmware at a later date using the serial console. Note that the web server may not function properly if the firmware upgrade is required and is not updated.

To upgrade the firmware using the serial console:

1. Click **System > Clustering > Cluster Status** tab in the admin console and wait for the node to be in the "FIPS disassociated" state.
2. Open a serial console and enter 9 to select the FIPS option.
3. Enter 6 to select Load Firmware.



**NOTE:** The SA Series FIPS appliance is said to be in a disassociated state when the key store state in the cache and on disk are different. As a security measure, you cannot load firmware when the appliance is in a disassociated state. The option is disabled. To resolve a disassociated state, connect to the serial console and reload the FIPS keystore database (Option 9 > Sub-option 1).

**Related Documentation** • [FIPS Overview on page 1131](#)

## Binary Importing and Exporting of the Keystore

---

Select **Maintenance > Import/Export** from the admin console to import and export the keystore. You can do this from a stand-alone node or from a node within a cluster. The keystore is exported as part of the system settings configuration file. Safely store the restore password associated with the archived keystore as you will need it for various FIPS operations. If you forget the restore password you can create a new one from the serial console and then re-export the configuration.

To import the keystore, select the **Import Key Store and Device Certificate(s)** checkbox and import your configuration. After the import process has completed, open a serial console for that FIPS appliance and enter 9 for FIPS Options and then 1 to select Complete import of keystore and server certificates. If the keystore is different from the one installed on the HSM you will be prompted for the keystore's restore password.



**NOTE:** If you reboot the FIPS appliance without performing the serial console step above, you are prompted to import the keystore during the boot process. Enter y to import the keystore. If you do not enter y within five seconds, the FIPS appliance continues to boot normally. If this occurs, perform the serial console step after the FIPS appliance completes its boot process.

If the FIPS appliance is in a cluster, go to each node within the cluster and perform the serial console step above to complete the keystore import process.

**Related Documentation**

- [FIPS Overview on page 1131](#)

## FIPS Device Status LED Behavior

---

There are three device status LEDs located on the FIPS card:

- S (Status)
- F (FIPS)
- I (INIT)

Table 79: Status LED

LED	Color and State	Description
STATUS	Off	Bootstrap firmware is executing
	Blinking green	IDLE, OPERATIONAL, or FAILSAFE state
	Green	POST or DISABLED state (driver not attached)
	Blinking red	Error occurred during boot process
	Red	HALTED (fatal error) state or when a low-level hardware initialization failure occurred
FIPS	Off	Operating in non-FIPS mode
	Green	Operating in FIPS mode
	Blinking yellow	Zeroize jumper is present
INIT	Off	Board is not initialized
	Green	Board initialized by security officer
	Yellow	POST, DIAGNOSTIC or FAILSAFE (firmware not upgraded) state
	Blinking yellow	Running diagnostics

**Related Documentation**

- [FIPS Overview on page 1131](#)





## CHAPTER 47

# FIPS Level 1 Support

- [Understanding Juniper Networks FIPS Level 1 Support on page 1141](#)
- [FIPS Supported Platforms and Licensing on page 1142](#)
- [Enabling FIPS Level 1 Support on page 1143](#)
- [Turning Off FIPS Level 1 Support from the Serial Console on page 1146](#)
- [Installing a Self-Signed Certificate From the Serial Console on page 1147](#)
- [Supported Cipher Suites when FIPS Level 1 Support is Enabled and Disabled on page 1148](#)

## Understanding Juniper Networks FIPS Level 1 Support

- [What Is FIPS? on page 1141](#)
- [What Is FIPS Level 1 Support? on page 1142](#)

### What Is FIPS?

Federal Information Processing Standard (FIPS) are a set of standards that define security requirements for products that implement cryptographic modules used to secure sensitive but unclassified information. The most recent standards are defined in the FIPS Publication 140-2.

The FIPS documents define, among other things, security levels for computer and networking equipment. U.S. Federal Government departments, and other organizations, use FIPS to evaluate the cryptographic capabilities of the equipment they consider for purchase. Cryptographic modules are validated against separate areas of the FIPS specification. An overall certification level is assigned based on the minimum level achieved in any area. Although primarily aimed at environments requiring strict security, FIPS levels are increasingly enforced as qualifying criteria for all U.S. Federal Government contracts. Security-conscious private enterprises might also use FIPS levels as an equipment evaluation benchmark. FIPS levels also serve as a customer-neutral description of vendor requirements. Vendors can engineer security products to FIPS levels and extend the applicability and eligibility of these products across a broad customer base, thereby eliminating exhaustive and time-consuming customer-by-customer product qualification procedures.

## What Is FIPS Level 1 Support?

Juniper Networks offers FIPS level 1 support starting with Secure Access Service release 7.4 and Access Control Service release 4.4. Both services use a 140-2 level 1 certified cryptographic module to comply with FIPS. When FIPS level 1 support is enabled applications, such as browsers, accessing the web server must support Transport Layer Security (TLS), the latest version of Secure Socket Layer (SSL). If the platform features hardware acceleration, then for SSL processing SSL hardware acceleration is disabled as hardware acceleration does not comply with FIPS validation. Only FIPS approved algorithms are used when in FIPS level 1 support is enabled.



**NOTE:** You cannot run FIPS level 1 support on a hardware FIPS platform such as the SA6500 FIPS SSL VPN Appliance. For more information on the hardware FIPS platform, see the *Secure Access Service Administration Guide* and the *Access Control Service Administration Guide*.

### Related Documentation

- [FIPS Supported Platforms and Licensing on page 1142](#)
- [Enabling FIPS Level 1 Support on page 1143](#)

---

## FIPS Supported Platforms and Licensing

The following platforms support FIPS level 1:

- Junos Pulse Gateway MAG2600
- Junos Pulse Gateway MAG4610
- Junos Pulse Gateway MAG-SM160
- Junos Pulse Gateway MAG-SM360
- Secure Access Service and Access Control Service virtual appliances

FIPS licenses are time-bound, subscription feature licenses that must be installed if you intend to use the FIPS feature. For example, the ACCESS-FIPS-3YR license enables FIPS level 1 support for three years.

For a comprehensive list of FIPS licensing SKUs, see your *Juniper Networks Service Guide* or contact your Juniper Networks sales representative.

For virtual appliances you must install a FIPS license on the license server, one license for each virtual appliance where you intend to turn on FIPS level 1 support.

### Related Documentation

- [Understanding Juniper Networks FIPS Level 1 Support on page 1141](#)
- [Enabling FIPS Level 1 Support on page 1143](#)

## Enabling FIPS Level 1 Support

You can enable FIPS level 1 support after you purchase the FIPS license and only on specific platforms. Once you enable FIPS level 1 support, your browser is restricted to specific custom cipher strengths. A list of supported ciphers is shown during the enabling process.

When you enable FIPS level 1 support, the following events occur on the system:

- The Web server restarts and turns on FIPS level 1 support. The Web server now allows only TLSv1.0, TLSv1.1 and TLSv1.2 protocols that include FIPS approved cryptographic algorithms which include Suite B cipher suites.



**NOTE:** Once FIPS level 1 support is enabled, new client sessions will use FIPS if the client supports FIPS. Existing client sessions may not be using FIPS. To ensure FIPS capable clients are in FIPS level 1 support, all client sessions should be terminated after the FIPS level 1 support is enabled. Administrators can use the **System > Status > Active Users** page to terminate client sessions.

- If the platform features hardware acceleration, when FIPS level 1 support is enabled SSL processing does not utilize the hardware acceleration. IPSec hardware acceleration is not affected.



**NOTE:** You cannot enable FIPS level 1 support on a Juniper Networks FIPS platform, such as the SA6500 FIPS SSL VPN Appliance.

The following event logs are generated for FIPS level 1 support:

- SYS30966 when the web server turns FIPS level 1 support on.
- ADM30965 when the administrator turns FIPS level 1 support on or off.
- ERR30967 when the web server fails to turn on FIPS level 1 support.

To enable FIPS level 1 support:

1. Select **System > Configuration > Security > SSL Options**.
2. Under SSL FIPS Mode option, select **Turn on FIPS mode**. See [Figure 82 on page 1144](#).

Figure 82: Enabling FIPS Level 1 Support

**Configuration**  
Security

SSL Options Miscellaneous

**SSL FIPS Mode option**  
When this option is enabled, the web service will be placed in FIPS Mode and all non-FIPS ciphers will be disabled. The web service will restart and will not use SSL hardware acceleration.

Turn on FIPS mode\*

\* Additional license purchase required

**Allowed SSL and TLS Version**  
The older SSL V2 protocol has known security issues addressed by SSL V3 and TLS. Older browsers may only support SSL V2. Here TLS stands for TLS 1.0, 1.1 and 1.2.

Accept only TLS (maximize security with reduced compatibility)  
 Accept only SSL V3 and TLS (maximize security)  
 Accept SSL V2 and V3 and TLS (maximize browser compatibility)

**Allowed Encryption Strength**  
Strong ciphers (rated by the number of bits in the cipher) improve the security of SSL encryption, but some browsers may only support 40-bit ciphers. When there is more than one acceptable cipher, the Junos Pulse Secure Access Service will give preference to the cipher with the fastest data transfer rate, regardless of its relative encryption strength. Changing the encryption strength will cause the web service to restart. Please see the Setting Security Options section in the Admin guide for more details.

Accept only 168-bit and greater (maximize security)  
 Accept only 128-bit and greater (security and browser compatibility)  
 Accept 40-bit and greater (maximize browser compatibility)  
 Custom SSL Cipher Selection

**Note:** Custom cipher selection disables the Encryption Strength option.

Cipher Suite	High (>=168-bit)	Medium (>=128-bit and <168-bit)	Low (>=40-bit and <128-bit)	Description
AES/3DES	<input checked="" type="checkbox"/>			cipher suites using triple DES and AES (Maximizes security)
AES	<input checked="" type="checkbox"/>			cipher suites using AES (Maximizes performance)
DES		<input checked="" type="checkbox"/>		cipher suites using DES (not triple DES)
RC4			<input checked="" type="checkbox"/>	cipher suites using RC4

Recommended for FIPS deployment

**Encryption Strength option**  
Normally, the allowed encryption strength is enforced after an SSL session is established, so that a user that connects using a disallowed encryption strength will receive a web page describing the problem. The option below will prevent a browser with a weak cipher from establishing a connection. Changing this option will cause the web service to restart.

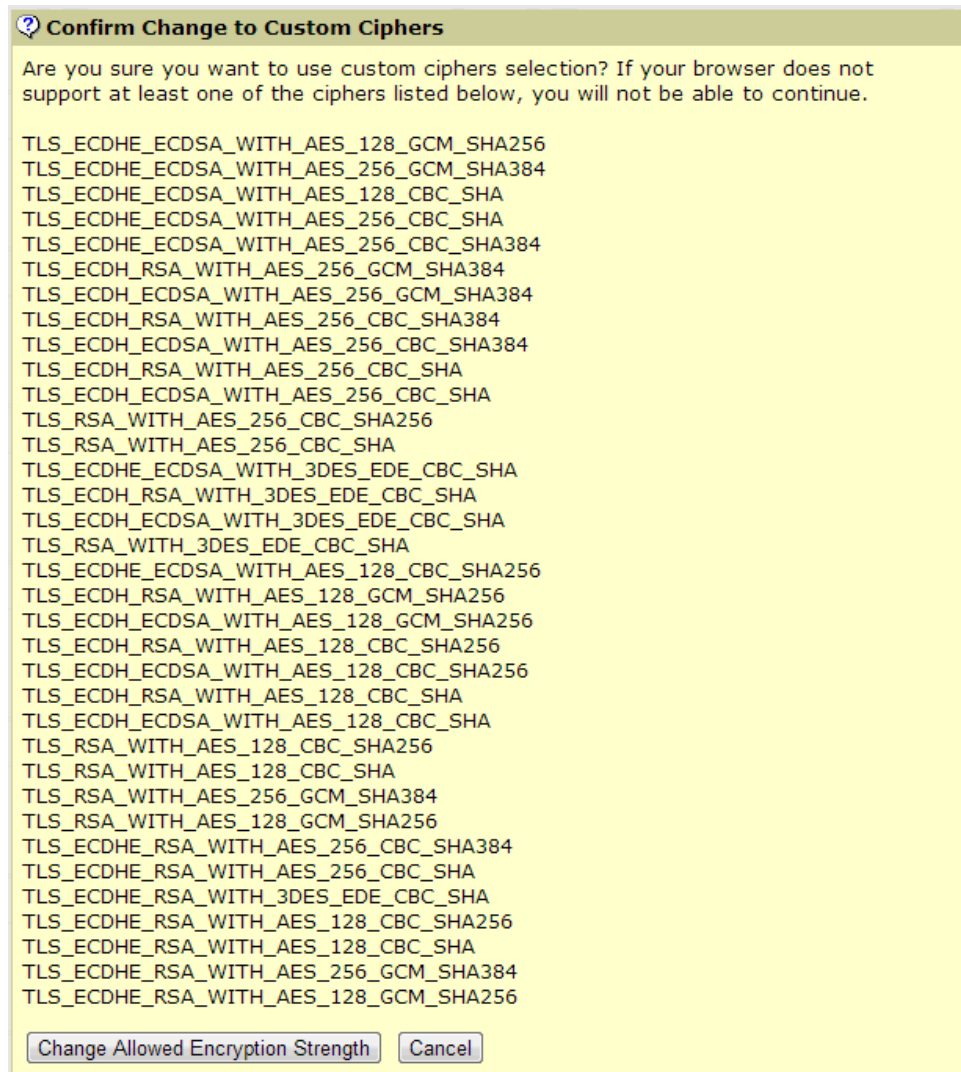
Do not allow connections from browsers that only accept weaker ciphers

Once you turn on FIPS level 1 support, the following changes are made:

- Under Allowed SSL and TLS Version, the **Accept only TLS** option is selected. .
  - Under Allowed Encryption Strength, the Custom SSL Cipher Selection is set. See [Figure 82 on page 1144](#). Only FIPS approved algorithms are selected. All other options under this section are disabled. See “Supported Cipher Suites when FIPS Level 1 Support is Enabled and Disabled” on page 1148
  - Under Encryption Strength, the **Do not allow connections from browsers that only accept weaker ciphers** option is selected. You cannot disable this selection.
3. Click **Save Changes**.

A window shows the supported custom ciphers. See [Figure 83 on page 1145](#) for an example. Your output may be different.

Figure 83: Example of Allowed Encryption Strengths



4. Click **Change Allowed Encryption Strength**.

FIPS Level 1 support is now enabled on the device. If your browser does not support any of the listed ciphers, you will not be able to log in to the device.

Entries are made in the Events logs (see [Figure 84 on page 1146](#)) and Admin Access logs (see [Figure 85 on page 1146](#)) to show that FIPS level 1 support is enabled.

Figure 84: Events Log Entries for FIPS Level 1

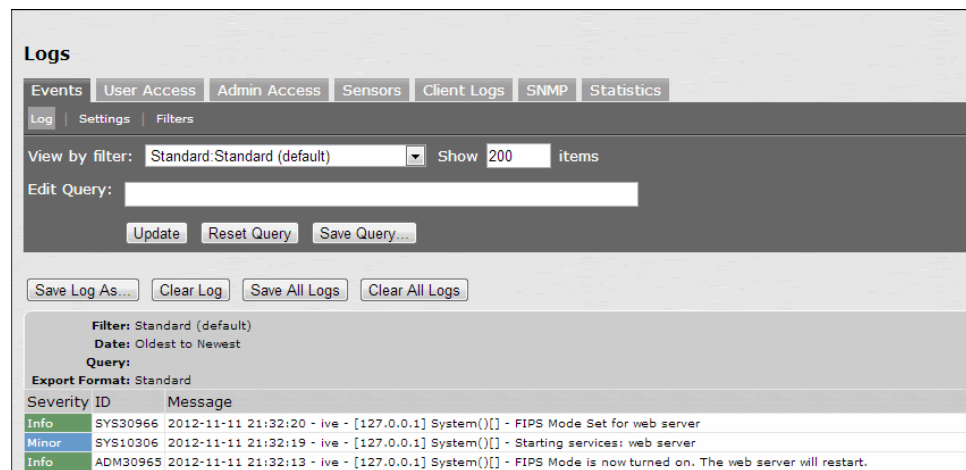
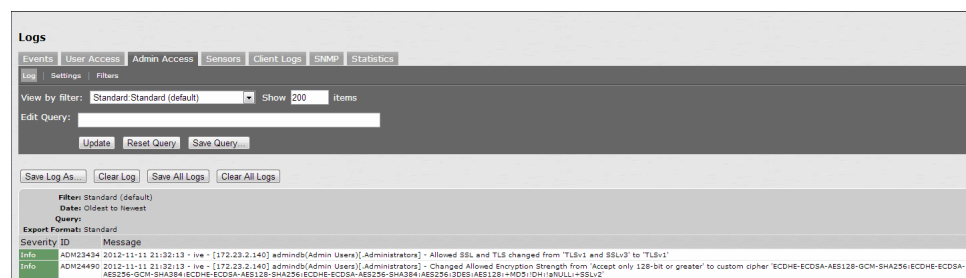


Figure 85: Admin Access Logs for FIPS Level 1 Encryption Strength Changes



**Related Documentation**

- [Understanding Juniper Networks FIPS Level 1 Support on page 1141](#)
- [FIPS Supported Platforms and Licensing on page 1142](#)
- [Supported Cipher Suites when FIPS Level 1 Support is Enabled and Disabled on page 1148](#)

**Turning Off FIPS Level 1 Support from the Serial Console**

**Problem** If you have FIPS level 1 support enabled and your browser does not support the required cipher suites, you cannot access the device. If this happens to an administrator account, you can no longer administer or configure the system.

**Solution** You can turn off FIPS level 1 support and reset the encryption strength from the device's serial console. After choosing that option, SSL options are reset to **Accept only SSL V3 and TLS** and to **Accept only 128-bit and greater encryption strength**.

Open a serial console to your device and select option **8. Turn off FIPS Mode and reset allowed encryption strength for SSL**.

**Turning Off FIPS Level 1 and Resetting Encryption Strength**

- Please choose the operation to perform:
1. Network Settings and Tools
  2. Create admin username and password
  3. Display log/status

## From the Serial Console

4. System Operations
  5. Toggle password protection for the console (Off)
  6. Create a Super Admin session.
  7. System Maintenance
  8. Turn off FIPS Mode and reset allowed encryption strength for SSL
- Choice: 8



**NOTE:** Once you turn off FIPS level 1 support, option 8 is relabeled “Reset allowed encryption strength for SSL.”

- Related Documentation**
- [Enabling FIPS Level 1 Support on page 1143](#)
  - [Installing a Self-Signed Certificate From the Serial Console on page 1147](#)

## Installing a Self-Signed Certificate From the Serial Console

**Problem** An administrator can be locked out of the system if their browser does not support the certificate assigned to the network port. For example, if your system has an ECC certificate assigned to the internal port and your browser does not support ECC certificates you cannot log in to the device using the internal port.

**Solution** You can use the serial console to create and install a self-signed RSA certificate onto the internal port to allow access. Once you connect to the serial console, select option **4. System Operations** followed by Option **7. Install self-signed certificate**. It may take a few minutes for the 2048-bit key size self-signed certificate to be created and installed on your device. Once the certificate is installed, you can now log in to the device.

### Creating and Installing an RSA Certificate

- Please choose the operation to perform:
1. Network Settings and Tools
  2. Create admin username and password

## From the Serial Console

```

3. Display log/status
4. System Operations
5. Toggle password protection for the console (Off)
6. Create a Super Admin session.
7. System Maintenance
8. Turn off FIPS Mode and reset allowed encryption strength for SSL
Choice: 4

```

Please choose the operation to perform:

```

1. Reboot this Junos Pulse Secure Access Service
2. Shutdown this Junos Pulse Secure Access Service
3. Restart services at this Junos Pulse Secure Access Service
4. Rollback this Junos Pulse Secure Access Service
5. Factory reset this Junos Pulse Secure Access Service
6. Clear all configuration data at this Junos Pulse Secure Access Service
7. Install self-signed certificate
Choice: 7

```

Are you sure you want to install a newly-created RSA self-signed certificate on the internal port? (y/n) y

Please provide information to create a self-signed Web server digital certificate.

```

Common name (example: secure.company.com): myname.mycompany.com
Organization name (example: Company Inc.): MyCompany Inc.

```

Please enter some random characters to augment the system's random key generator. We recommend that you enter approximately thirty characters.

```

Random text (hit enter when done):abcdef1234567

```

```

Creating self-signed digital certificate - this may take several minutes...
The self-signed digital certificate was successfully created.

```

**Related Documentation**

- [Enabling FIPS Level 1 Support on page 1143](#)

## Supported Cipher Suites when FIPS Level 1 Support is Enabled and Disabled

The tables in this topic list the cipher suites that are supported by the web server when the FIPS level 1 support is disabled and enabled.

### Supported Cipher Suites When FIPS Level 1 Support is Disabled

When the FIPS level 1 support is disabled and when SSL hardware acceleration is not present or is disabled, the web server gives preference to cipher suites that use RC4 for bulk encryption. When SSL hardware acceleration is present and enabled, the web server gives preference to AES128, AES256 and 3DES over RC4, in that order.

**Table 80: Supported Cipher Suites With FIPS Level 1 Support Off, Hardware Acceleration Enabled and RSA Server Certificates In Use**

Cipher Suite	Protocol
--------------	----------



**Table 80: Supported Cipher Suites With FIPS Level 1 Support Off, Hardware Acceleration Enabled and RSA Server Certificates In Use (continued)**

TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_128_CBC_SHA	SSLv3 and above
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_256_CBC_SHA	SSLv3 and above
TLS_RSA_WITH_3DES_EDE_CBC_SHA	SSLv3 and above
TLS_RSA_WITH_RC4_128_SHA	SSLv3 and above
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	SSLv3 and above
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	SSLv3 and above
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	SSLv3 and above
TLS_ECDHE_RSA_WITH_RC4_128_SHA	SSLv3 and above
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_RSA_WITH_RC4_128_MD5	SSLv3 and above

**Table 81: Supported Cipher Suites With FIPS Level 1 Support Off, Hardware Acceleration Enabled and ECC Server Certificates In Use**

Cipher Suite	Protocol
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	SSLv3 and above
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2

**Table 81: Supported Cipher Suites With FIPS Level 1 Support Off, Hardware Acceleration Enabled and ECC Server Certificates In Use (continued)**

Cipher Suite	Protocol
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	SSLv3 and above
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	SSLv3 and above
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	SSLv3 and above
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	SSLv3 and above
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	SSLv3 and above
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	SSLv3 and above
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	SSLv3 and above
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	SSLv3 and above
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	SSLv3 and above
TLS_ECDH_RSA_WITH_RC4_128_SHA	SSLv3 and above
TLS_ECDH_ECDSA_WITH_RC4_128_SHA	SSLv3 and above

**Table 82: Supported Cipher Suites With FIPS Level 1 Support Off, Hardware Acceleration Enabled and RSA Server Certificates In Use**

Cipher Suite	Protocol
--------------	----------

**Table 82: Supported Cipher Suites With FIPS Level 1 Support Off, Hardware Acceleration Enabled and RSA Server Certificates In Use (continued)**

TLS_RSA_WITH_RC4_128_SHA	SSLv3 and above
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_128_CBC_SHA	SSLv3 and above
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_256_CBC_SHA	SSLv3 and above
TLS_RSA_WITH_3DES_EDE_CBC_SHA	SSLv3 and above
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDHE_RSA_WITH_RC4_128_SHA	SSLv3 and above
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	SSLv3 and above
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	SSLv3 and above
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	SSLv3 and above
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_RSA_WITH_RC4_128_MD5	SSLv3 and above

**Table 83: Supported Cipher Suites With FIPS Level 1 Support Off, Hardware Acceleration Disabled and ECC Server Certificates In Use**

Cipher Suite	Protocol
TLS_ECDHE_ECDSA_WITH_RC4_128_SHA	SSLv3 and above
TLS_ECDH_RSA_WITH_RC4_128_SHA	SSLv3 and above
TLS_ECDH_ECDSA_WITH_RC4_128_SHA	SSLv3 and above
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2

**Table 83: Supported Cipher Suites With FIPS Level 1 Support Off, Hardware Acceleration Disabled and ECC Server Certificates In Use (continued)**

Cipher Suite	Protocol
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	SSLv3 and above
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	SSLv3 and above
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	SSLv3 and above
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	SSLv3 and above
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	SSLv3 and above
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	SSLv3 and above
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	SSLv3 and above
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	SSLv3 and above
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	SSLv3 and above

### Supported Cipher Suites When FIPS Level 1 Support is Enabled

When FIPS level 1 support is enabled, only TLSv1.0, v1.1, v1.2 and AES256, 3DES and AES128 are allowed. The order of the cipher suites is not dependent on the SSL hardware acceleration module since hardware acceleration is not used when FIPS level 1 support is enabled.

When FIPS level 1 support is enabled, the following settings are automatically configured:

- In the SSL Options window:
  - Under Allowed SSL and TLS Version, the **Accept only TLS** option is selected. All other options under this section are disabled.
  - Under Allowed Encryption Strength, the **Custom SSL Cipher Selection** option is selected. Only FIPS approved algorithms are selected. All other options under this section are disabled.
  - Under Encryption Strength Option, the **Do not allow connections from browsers that only accept weaker ciphers** option is selected.
- SSL hardware acceleration is disabled. IPsec hardware acceleration is not affected by the FIPS level 1 support being enabled.

In [Table 84 on page 1153](#), the first four cipher suites are given preference due to the requirements in RFC 6460. The first two cipher suites meeting the requirement for Suite B Profile for TLS 1.2. The next two meeting the requirement for Suite B Transitional Profile for TLS 1.0 and 1.1.

**Table 84: Supported Cipher Suites With FIPS Level 1 Support On and ECC Server Certificates In Use**

Cipher Suite	Protocol
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	TLSv1.0 and above
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	TLSv1.0 and above
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	TLSv1.0 and above
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	TLSv1.0 and above
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and above
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and above

**Table 84: Supported Cipher Suites With FIPS Level 1 Support On and ECC Server Certificates In Use (continued)**

Cipher Suite	Protocol
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and above
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	TLSv1.0 and above
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	TLSv1.0 and above

**Table 85: Supported Cipher Suites With FIPS Level 1 Support On and RSA Server Certificates In Use**

Cipher Suite	Protocol
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1.0 and above
TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and above
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1.0 and above
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.0 and above
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	TLSv1.0 and above
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.0 and above

**Table 85: Supported Cipher Suites With FIPS Level 1 Support On and RSA Server Certificates In Use (continued)**

Cipher Suite	Protocol
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2

- Related Documentation**
- [Enabling FIPS Level 1 Support on page 1143](#)
  - [Example: Assigning an ECC P-256 Certificate to an External Virtual Port and Giving Preference to Suite B Ciphers on page 877](#)





# Compression

- [About Compression on page 1157](#)
- [Enabling System-Level Compression on page 1159](#)

## About Compression

---

Secure Access improves performance by compressing common types of Web and file data such as HTML files, Word documents, and images.

Secure Access determines whether it should compress the data accessed by users by using the following process:

1. Secure Access verifies that the accessed data is a compressible type. Secure Access supports compressing many common data types such as HTML files, and Word documents.
2. If the user is accessing Web data, Secure Access verifies that the user's browser supports compression of the selected data type.

Secure Access determines compression supportability based on the browser's user-agent and the accept-encoding header. Secure Access supports the compression of all of the standard Web data types if it determines that the user-agent is compatible with Mozilla 5, Internet Explorer 5, or Internet Explorer 6. Secure Access only supports compressing HTML data, however, if it determines that the browser's user-agent is only compatible with Mozilla 4.

3. Secure Access verifies that compression is enabled at the system level. You can enable system-level compression through the Maintenance > System > Options page of the admin console.
4. Secure Access verifies that compression resource policies or autopolicies are enabled for the selected data type. Secure Access comes with resource policies that compress data. You may enable these policies or create your own through the following pages of the admin console:
  - Users > Resource Policies > Web > Compression.
  - Users > Resource Policies > Files > Compression.

You may also create resource profile compression autopolicies through the Users > Resource Profiles > Web > Web Applications/Pages page of the admin console.

If all of these conditions are met, the Secure Access Service runs the appropriate resource policy either compresses or does not compress the data accessed by the user based on the configured action.

If all of these conditions are not met, the Secure Access Service does not run the appropriate resource policy and no resource policy items appear in the Secure Access Service log files.

The Secure Access Service comes pre-equipped with three resource policies that compress Web and file data. If you are upgrading from a pre-4.2 version of the Secure Access Service software and you previously had compression enabled, these policies are enabled. Otherwise, if you previously had compression disabled, these policies are disabled.

The Web and file resource policies created during the upgrade process specify that the Secure Access Service should compress all supported types of Web and File data, including types that were not compressed by previous versions of the appliance. All data types that were not compressed by previous product versions are marked with an asterisk (\*) in the supported data types list below.

The Secure Access Service supports compressing the following types of Web and file data:

- text/plain (.txt)
- text/ascii (.txt)\*
- text/html (.html, .htm)
- text/css (.css)
- text/rtf (.rtf)
- text/javascript (.js)
- text/xml (.xml)\*
- application/x-javascript (.js)
- application/msword (.doc)
- application/ms-word (.doc)\*
- application/vnd.ms-word (.doc)\*
- application/msexcel (.xls)\*
- application/ms-excel (.xls)\*
- application/x-excel (.xls)\*
- application/vnd.ms-excel (.xls)\*
- application/ms-powerpoint (.ppt)\*
- application/vnd.ms-powerpoint (.ppt)\*



**NOTE:** The data types denoted by an asterisk \* were not compressed by pre-4.2 versions of the Secure Access Service software.

Also note that the Secure Access Service does not compress files that you upload—only files that you download from the Secure Access Service.

Additionally, the Secure Access Service supports compressing the following types of files:

- text/html (.html, .htm)
- application/x-javascript (.js)
- text/javascript (.js)
- text/css (.css)
- application/perl (.cgi)

**Related  
Documentation**

- [Enabling System-Level Compression on page 1159](#)

## Enabling System-Level Compression

To enable system-level compression:

1. In the admin console, choose **Maintenance > System > Options**.
2. Select the **Enable gzip compression** checkbox to reduce the amount of data sent to browsers that support HTTP compression. Note that after you enable this option, you must also configure Web and file resource policies specifying which types of data the Secure Access Service should compress.



**NOTE:** Gzip compression is not supported on the MAG Series Junos Pulse Gateways.

3. Click **Save Changes**.

**Related  
Documentation**

- [About Compression on page 1157](#)



# Multi-Language Support

- [About Multi-Language Support for the Secure Access Service on page 1161](#)
- [Encoding Files for Multi-Language Support on page 1162](#)
- [Localizing the User Interface on page 1162](#)
- [Localizing Custom Sign-In and System Pages on page 1163](#)

## About Multi-Language Support for the Secure Access Service

---

Secure Access Service provide multi-language support for file encoding, end-user interface display, and customized sign-in and system pages. The Secure Access Service support the following languages:

- English (US)
- Chinese (Simplified)
- Chinese (Traditional)
- French
- German
- Japanese
- Korean
- Spanish



**NOTE:** Juniper Networks translates the Secure Access Service end-user console and help systems into the languages listed above. Note, however, that the translated end-user help is not available in the first release of the product. Juniper Networks makes a translated version of the help available in the first maintenance release after the general availability release.

---

### Related Documentation

- [Encoding Files for Multi-Language Support on page 1162](#)
- [Localizing the User Interface on page 1162](#)
- [Localizing Custom Sign-In and System Pages on page 1163](#)

## Encoding Files for Multi-Language Support

---

Character encoding is a mapping of characters and symbols used in written language into a binary format used by computers. Character encoding affects how you store and transmit data. The encoding option in **Users > Resource Policies > Files > Encoding** allows you to specify the encoding to use when communicating with Windows and NFS file shares. The encoding option does not affect the end-user language environment.

To specify the internationalization encoding for Secure Access Service traffic:

1. In the admin console, choose **Users > Resource Policies > Files > Encoding**.
2. Select the appropriate option:
  - Western European (ISO-8859-1) (default) (Includes English, French, German, Spanish)
  - Simplified Chinese (CP936)
  - Simplified Chinese (GB2312)
  - Traditional Chinese (CP950)
  - Traditional Chinese (Big5)
  - Japanese (Shift-JIS)
  - Korean
3. Click **Save Changes**.

### Related Documentation

- [About Multi-Language Support for the Secure Access Service on page 1161](#)
- [Localizing the User Interface on page 1162](#)
- [Localizing Custom Sign-In and System Pages on page 1163](#)

## Localizing the User Interface

---

The Secure Access Service provides a means to display the end-user interface in one of the supported languages. Combining this feature with (custom) sign-in and system pages and a localized operating system provides a fully localized user experience.

When you specify a language, the Secure Access Service displays the user interface, including all menu items, dialogs generated by the Secure Access Service, and the help file in the chosen language for all users regardless of which realm they sign in to.

To configure localization options:

1. In the admin console, choose **Maintenance > System > Options**.
2. Use the End-user Localization drop-down list to specify the language in which to display the end-user interface (optional). If you do not specify a language, the end-user interface displays based on the settings of the browser.

3. Click **Save Changes**.

**Related  
Documentation**

- [About Multi-Language Support for the Secure Access Service on page 1161](#)
- [Encoding Files for Multi-Language Support on page 1162](#)
- [Localizing Custom Sign-In and System Pages on page 1163](#)

## Localizing Custom Sign-In and System Pages

---

The Secure Access Service provides several zip files that contain different sets of sample template files for various pages that may appear during the sign-in process. Use these template files along with the template toolkit language to create localized custom sign-in and system pages for your end-users.

Editing the default sign-in page using text in the language of your choice is a quick way to provide your users with a localized sign-in page.

**Related  
Documentation**

- [About Multi-Language Support for the Secure Access Service on page 1161](#)
- [Encoding Files for Multi-Language Support on page 1162](#)
- [Localizing the User Interface on page 1162](#)





# Handheld Devices and PDAs

- [Handheld Devices and PDAs on page 1165](#)
- [Task Summary: Configuring the Secure Access Service for PDAs and Handhelds on page 1166](#)
- [Defining Client Types on page 1168](#)
- [Enabling WSAM on PDAs on page 1169](#)
- [Enabling ActiveSync For Handheld Devices on page 1170](#)

## Handheld Devices and PDAs

---

In addition to allowing users to access the Secure Access Service from standard workstations and kiosks, the Secure Access Service also allows end-users to access the Secure Access Service from connected PDAs, handhelds and smart phones such as i-mode and Pocket PC. When a user connects from a PDA or handheld device, the Secure Access Service determines which pages and functionality to display based on settings in the System > Configuration > Client Types page of the admin console. By default, settings in this page specify that when accessing the Secure Access Service using a(n):

- **i-mode device**—The Secure Access Service displays compact HTML (cHTML) pages without tables, images, JavaScript, Java, or frames to the user. Depending on which features you enable through the admin console, the end-user may browse the Web, link to Web bookmarks, single sign-on to other applications, and edit their preferences (including clearing their cache and editing their Secure Access Service/LDAP password). The Secure Access Service allows i-mode users to access supported features using access keys on their phone's keypad as well as through standard browse-and-select navigation.
- **Pocket PC device**—The Secure Access Service displays mobile HTML pages with tables, images, JavaScript and frames, but does not process Java. Depending on which features you enable through the admin console, the end-user may access Mobile Notes and OWA email applications, browse the Web, link to Web bookmarks, single sign-on to other applications, and edit their preferences (including clearing their cache and editing their Secure Access Service/LDAP password).

PDA and handheld users cannot access the admin console or most of the Secure Access Service's advanced options, including file browsing, VPN Tunneling, Junos Pulse Collaboration, Telnet/SSH, Email Client, Host Checker, and Cache Cleaner, since PDA

and handheld devices do not generally support the ActiveX, Java, or JavaScript controls on which these features depend.

Also note that i-mode users cannot access cookie-based options, including session cookies and SiteMinder authentication and authorization, since most i-mode browsers do not support HTTP cookies. The Secure Access Service rewrites hyperlinks to include the session ID in the URL instead of using cookies. The Secure Access Service reads the session ID when the user accesses the URL.



**NOTE:** In order to improve the response time, the following icons are not displayed when accessing the Secure Access Service home page: help, sign out, open bookmark in new page, and WSAM.

**Related Documentation**

- [Task Summary: Configuring the Secure Access Service for PDAs and Handhelds on page 1166](#)
- [Defining Client Types on page 1168](#)
- [Enabling WSAM on PDAs on page 1169](#)
- [Enabling ActiveSync For Handheld Devices on page 1170](#)

## Task Summary: Configuring the Secure Access Service for PDAs and Handhelds

To properly configure the Secure Access Service to work with PDAs and handheld devices, you must:

1. **Enable access at the system level**—If you want to support browsers other than the defaults provided with the Secure Access Service, you must enter the user agent strings of the PDA and handheld operating systems that you want to support in the System > Configuration > Client Types tab. For a complete list of PDA and handheld browsers that are supported with the Secure Access Service, see the Supported Platforms document posted on the Support website.
2. **Evaluate your user roles and resource policies**—Depending on which Secure Access Service features you have enabled, you may need to either modify your existing roles and resource policies for PDA and handheld users or create new ones. Note that:
  - Mobile device users cannot access roles or policies that require Host Checker or Cache Cleaner since handheld devices do not generally support the ActiveX, Java, or JavaScript controls on which these features depend. You can disable these options through the following tabs:
    - Users > User Roles > Role > General > Restrictions
    - Resource Policies > Web > Access > Web ACL > Policy > Detailed Rules
  - Mobile device users may have trouble reading long role names on their small screens. If you require users to pick from a list of roles when they sign in, you may want to shorten role names in the Users > User Roles > Role > General > Overview tab.

- Mobile device users may have trouble reading long bookmark names on their small screens. You can edit Web bookmarks in the following tabs:
    - Users > Resource Profiles > Web Application Resource Profiles > *Profile* > Bookmarks
    - Users > User Roles > *Role* > Web > Bookmarks
    - Resource Policies > Web > Access > Web ACL > *Policy* > General
  - Although advanced features such as file browsing are not supported for PDAs and handhelds, you do not need to disable them in the roles and resource policies used by mobile device users. The Secure Access Service simply does not display these options to mobile device users.
3. **Evaluate your authentication and authorization servers**—The Secure Access Service supports all of the same authentication and authorization servers for PDA and handheld users as standard users, except the eTrust SiteMinder policy server. SiteMinder is dependent on cookies, which are not supported with i-mode browsers.
  4. **Evaluate your realms**—Depending on which Secure Access Service features you have enabled, you may need to either modify your existing realms for PDA and handheld users or create new ones. Note that:
    - Mobile device users cannot access the Secure Access Service when they try to sign into a realm that requires Host Checker or Cache Cleaner since handheld devices do not generally support the ActiveX, Java, or JavaScript controls on which these features depend. You can disable these options through sub-tabs in the System > Configuration > Security page.
    - Mobile device users cannot authenticate against an eTrust SiteMinder server. You can choose a different authentication server for the realm in the Users > User Realms > *Realm* > General tab.
    - Mobile device users may have trouble reading long realm names on their small screens. If you require users to pick from a list of realms when they sign in, you may want to shorten realm names in the Users > User Realms > *Realm* > General tab.
  5. **Evaluate your sign-in policy to use**—If you want to use a different sign-in page for Pocket PC users, you can define it in the Authentication > Signing In > Sign-in Pages tab and then create a sign-in policy that references the page using options in the Authentication > Signing In > Sign-in Policies tab. Or, you can create a custom sign-in page using the Pocket PC template files that are available in sample.zip.
  6. **Specify allowed encryption strength**—Different types of devices allow different encryption strengths. You should specify the encryption strength in the Secure Access Service to match the requirement of your devices. For example, mobile phones often only accept 40-bit encryption. Review your end-users' device requirements and specify the allowed encryption strength on the System > Configuration > Security tab.

**Related Documentation**

- [Defining Client Types on page 1168](#)
- [Enabling WSAM on PDAs on page 1169](#)
- [Enabling ActiveSync For Handheld Devices on page 1170](#)

## Defining Client Types

The Client Types tab allows you to specify the types of systems your users may sign in from and the type of HTML pages the Secure Access Service displays when they do.

To manage user agents:

1. In the admin console, choose **System > Configuration > Client Types**.
2. Enter the user agent string that corresponds to the operating system(s) that you want to support. You may be as broad or specific as you want. For example, you can use the Secure Access Service default setting of `*DoCoMo*` to apply to all DoCoMo operating systems, or you can create a string such as `DoCoMo/1.0/P502i/c10` to apply to a single type of DoCoMo operating system. You may use the `*` and `?` wildcard characters in your string. Note that user agent strings on the Secure Access Service are case-insensitive.
3. Specify which type of HTML the Secure Access Service should display to users who sign in from the operating system specified in the previous step. Options include:
  - **Standard HTML**—The Secure Access Service displays all standard HTML functions, including tables, full-size graphics, ActiveX components, JavaScript, Java, frames, and cookies. Ideal for standard browsers, such as Firefox, Mozilla, and Internet Explorer.
  - **Compact HTML (iMode)**—The Secure Access Service displays small-screen HTML-compatible pages. This mode does not support cookies or the rendering of tables, graphics, ActiveX components, JavaScript, Java, VB script, or frames. (The only difference between this option and the Smart Phone HTML Basic option is the user interface.) Ideal for iMode browsers.



**NOTE:** Form Post SSO is not supported on iMode appliances.

- **Mobile HTML (Pocket PC)**—The Secure Access Service displays small-screen HTML-compatible pages that may contain tables, small graphics, JavaScript, frames, and cookies, but this mode does not facilitate the rendering of java applets or ActiveX components. Ideal for Pocket PC browsers.
- **Smart Phone HTML Advanced**—The Secure Access Service displays small-screen HTML-compatible pages that may contain tables, small graphics, frames, cookies, and some JavaScript, but this mode does not facilitate the rendering of java applets, ActiveX components, or VB scripts. Ideal for Treo and Blazer browsers.
- **Smart Phone HTML Basic**—The Secure Access Service displays small-screen HTML-compatible pages. This mode does not support cookies or the rendering of tables, graphics, ActiveX components, JavaScript, Java, VB script, or frames. (The only difference between this option and the Compact HTML option is the user interface.) Ideal for Opera browsers on Symbian.



**NOTE:** The Secure Access Service rewrites hyperlinks to include the session ID in the URL instead of using cookies.

4. Specify the order that you want the Secure Access Service to evaluate the user agents. The Secure Access Service applies the first rule in the list that matches the user's system. For example, you may create the following user agent string/HTML type mappings in the following order:

- a. User Agent String: \*DoCoMo\* Maps to: Compact HTML
- b. User Agent String: DoCoMo/1.0/P502i/c10 Maps to: Mobile HTML

If a user signs in from the operating system specified in the second line, The Secure Access Service will display compact HTML pages to him, not the more robust mobile HTML, since his user agent string matches the first item in the list.

To order mappings in the list, select the checkbox next to an item and then use the up and down arrows to move it to the correct place in the list.

5. Select the **Enable password masking for Compact HTML** checkbox if you want to mask passwords entered in iMode and other devices that use compact HTML. (Devices that do not use compact HTML mask passwords regardless of whether or not you select this checkbox.) Note that if your iMode users' passwords contain non-numeric characters, you must disable password masking because iMode devices only allow numeric data in standard password fields. If you disable masking, passwords are still transmitted securely, but are not concealed on the user's display.
6. Click **Save Changes**.



**NOTE:** To enable rewriting support for Vodafone phones, enter Vodafone for the user agent string and select Compact HTML as the client type. For support of the KDDI phone, enter KDDI for the user agent string and select Compact HTML as the client type.

#### Related Documentation

- [Task Summary: Configuring the Secure Access Service for PDAs and Handhelds on page 1166](#)
- [Enabling WSAM on PDAs on page 1169](#)
- [Enabling ActiveSync For Handheld Devices on page 1170](#)

## Enabling WSAM on PDAs

When defining client/server applications to secure through Windows Secure Application Manager (WSAM) on PDA devices, you should define PDA-specific applications through the Users > User Roles > Select Role > SAM > Applications > Add Application page.

Listed below are some PDA-specific executable files that you might want to enable for PSA devices:

- **tmail.exe**—Specifies the Pocket Outlook application

The Secure Access Service supports the following modes through Pocket Outlook:

- S-IMAP/S-POP and S-SMTP
  - ActiveSync—If the supported PDAs to which you are providing Pocket Outlook access are using ActiveSync, you must ensure that the IP address of the Exchange Server appears in the list of destination hosts defined within the user role. Direct Push, a feature built into Exchange Server 2007, is supported however you must set HTTPServerTimeout to 20 minutes or less.
- **mstsc40.exe**—Specifies the Windows Terminal Services application
  - **ieexplore.exe**—Specifies the Pocket Internet Explorer application



**NOTE:** When using an existing WSAM role configuration originally set up for Windows PC users to provide secure access PDA users, ensure that the list of destination hosts defined within the user role is no larger than 1500 bytes. Very large lists of destination hosts can lock up the WSAM launcher on PDA devices due to memory buffer constraints.

---

For Windows Mobile 5 users, WSAM adds log files to the \Program Files\Juniper Networks\WSAM\Log directory.

#### Related Documentation

- [Task Summary: Configuring the Secure Access Service for PDAs and Handhelds on page 1166](#)
- [Defining Client Types on page 1168](#)
- [Enabling ActiveSync For Handheld Devices on page 1170](#)

---

## Enabling ActiveSync For Handheld Devices

Using ActiveSync, you can synchronize data between a Windows-based desktop computer and handheld devices. The Secure Access Service can be used as a reverse proxy to allow users to synchronize their data without installing an additional client application, such as WSAM, on their handheld devices. More than 1000 concurrent connections is supported on an SA 6500.

Please note the following:

- Supports Windows Mobile 5.0 and 6.0 only.
- Supports Exchange Server 2003, 2007 and 2010.
- ActiveSync does not use up concurrent user licenses, even when configured with certificate authentication.
- Both NTLM & Basic Auth on the Exchange server are supported.

- Both HTTP and HTTPS between the Secure Access Service and Exchange server are supported.
- If the Secure Access Service is used for OWA & ActiveSync, the hostnames for OWA access and ActiveSync must be different.
- Direct Push is supported with ActiveSync, however you must set HTTPServerTimeout to 20 minutes or less. Direct Push is a feature built into Exchange Server 2007.
- ActiveSync does not work through a back-end web proxy.
- VIP sourcing settings are ignored for ActiveSync sessions. ActiveSync traffic from the Secure Access Service to a backend server is always sent with the Internal Port's source IP address.

To configure the Secure Access Service as a reverse proxy for use with ActiveSync:

1. In the admin console, choose **Authentication > Signing In > Sign-in Policies**.
2. To create a new authorization only access policy, click **New URL** and select **authorization only access**. Or, to edit an existing policy, click a URL in the Virtual Hostname column.
3. In the **Virtual Hostname** field, enter the name that maps to the Secure Access Service IP address. The name must be unique among all virtual host names used in pass-through proxy's hostname mode. The hostname is used to access the Exchange server entered in the Backend URL field. Do not include the protocol (for example, http:) in this field.

For example, if the virtual hostname is myapp.ivehostname.com, and the backend URL is http://www.xyz.com:8080/, a request to https://myapp.ivehostname.com/test1 via the Secure Access Service is converted to a request to http://www.xyz.com:8080/test1. The response of the converted request is sent to the original requesting web browser.

4. In the **Backend URL** field, enter the URL for the Exchange server. You must specify the protocol, hostname and port of the server. For example, http://www.mydomain.com:8080/.\*

When requests match the hostname in the Virtual Hostname field, the request is transformed to the URL specified in the Backend URL field. The client is directed to the backend URL unaware of the redirect.

5. Enter a Description for this policy (optional).
6. Select the server name or **No Authorization** from the Authorization Server drop down menu. If you select a server, ensure that the front-end server provides the SMSESSION cookie otherwise you will receive an error.
7. Select a user role from the Role Option drop down menu.

Only the following user role options are applicable for Autosync.

- HTTP Connection Timeout (Users > User Roles > *RoleName* > Web > Options > View advanced options)
- Allow browsing un-trusted SSL websites (Users > User Roles > *RoleName* > Web > Options > View advanced options)

- Source IP restrictions (Users > User Roles > *RoleName* > General > Restrictions)
- Browser restrictions (Users > User Roles > *RoleName* > General > Restrictions)

Ensure the user role you select has an associated Web Access policy.

8. Select the **Allow ActiveSync Traffic only** option to perform a basic of validation of the HTTP header to ensure the request is consistent with ActiveSync protocol. If you select this option only ActiveSync protocol requests can be processed. If validation fails, a message is created in the user's event log. If you do not select this option, both ActiveSync and non-ActiveSync requests are processed.

9. Click **Save Changes**.

The System Status Overview page displays the number of current active concurrent connections and a histogram of the active concurrent connections (Authorization Only Access Active Connections plot in the Concurrent SSL Connections graph).

To enable certificate authentication for handheld devices like, for example, an iPhone, see Client Certificate Validation on the External and Virtual Ports.

**Related  
Documentation**

- [Task Summary: Configuring the Secure Access Service for PDAs and Handhelds on page 1166](#)
- [Defining Client Types on page 1168](#)
- [Enabling WSAM on PDAs on page 1169](#)



# Using IKEv2 with the Secure Access Service

- [About IKEv2 on page 1173](#)
- [Task Summary: Configuring Secure Access for IKEv2 on page 1176](#)
- [Defining the IKEv2 Role Mapping Rule on page 1177](#)
- [Enabling the IKEv2 Access Feature on page 1178](#)
- [Configuring the IKEv2 Ports on page 1178](#)

## About IKEv2

---

IKE or IKEv2 (Internet Key Exchange) is the protocol used to set up a SA (security association) in the IPsec protocol suite. Microsoft Windows 7 fully supports the IKEv2 standard through Microsoft's Agile VPN functionality and can operate with a VPN gateway using these protocols. Information on IKE and IKEv2 is widely available on the Internet. It is not the intent of this guide to describe details about IKE and IKEv2.

Secure Access Service supports IKEv2, enabling interoperability with clients or devices, such as smartphones, that have a standards-based IPsec VPN client.

IKEv2 clients count toward the total number of sessions. Thus, the total number of sessions = number of IKEv2 sessions + number of NCP sessions.

Secure Access Service supports the following methods for authenticating IKEv2 clients:

- Client certificate-based authentication
- Authentication using EAP methods



**NOTE:** IKEv2 uses port 500 exclusively. Do not configure port 500 in your VPN Tunneling profiles.

## Extensible Authentication Protocol

EAP (Extensible Authentication Protocol) is an authentication framework frequently used in wireless communication. It provides functions and negotiation of authentication

methods called EAP methods. Secure Access Service supports the following EAP methods:

- EAP-MSCHAP-V2 (Microsoft Challenge-Handshake Authentication Protocol version 2)— a mutual authentication method that supports password-based user or computer authentication. During the EAP-MS-CHAP v2 authentication process, both the client and the authentication server must prove that they have knowledge of the user's password for authentication to succeed. Mutual authentication is provided by including an authenticator packet returned to the client after a successful server authentication. Supported authentication servers using EAP-MSCHAP-V2 are:
  - Local Authentication server
  - Active Directory/Windows NT
- EAP-MD5-Challenge – described in RFC 2284, enables an authentication server to authenticate a connection request by verifying an MD5 hash of a user's password. The server sends the client a random challenge value, and the client proves its identity by hashing the challenge and its password with MD5. EAP-MD5-Challenge is typically used on trusted networks where risk of packet sniffing or active attack are fairly low. Because of significant security vulnerabilities, EAP-MD5-Challenge is not usually used on public networks or wireless networks, because third parties can capture packets and apply dictionary attacks to identify password hashes. Because EAP-MD5-Challenge does not provide server authentication, it is vulnerable to spoofing (a third party advertising itself as an access point).

Only the local authentication server is supported with EAP-MD5-Challenge.

IKEv2 provides a tunnel mechanism for EAP authentication; it does not perform authentication itself. Instead it proxies EAP messages from a client to the EAP server and back.

## Client Certificate-Based Authentication

Secure Access Service supports IKEv2 authentication using client certificates. Note that only certificate authentication server on Secure Access Service supports client certification authentication of IKEv2 clients. When using client certificates for authentication, it is not necessary to configure the Realm/Protocol Set Mapping section under System > Configuration > IKEv2.

## Client Requirements

Your IKEv2 client should support the following requirements in order to work with Secure Access:

- Ability to establish IPSec Security Associations in Tunnel mode (RFC 4301).
- Ability to utilize the AES 128-bit encryption function (RFC 3602).
- Ability to utilize the SHA-1 hashing function (RFC 2404).
- Ability to utilize Diffie-Hellman Perfect Forward Secrecy in "Group 2" mode (RFC 2409).
- Ability to utilize IPSec Dead Peer Detection (RFC 3706).

- Ability to utilize the MD5 hashing function (RFC 1321).
- Ability to handle Internal Address on a Remote Network utilizing CFG\_REQUEST-CFG\_REPLY exchange.

Optional but recommended requirements include:

- Ability to adjust the Maximum Segment Size of TCP packets entering the VPN tunnel (RFC 4459).
- Ability to reset the “Don’t Fragment” flag on packets (RFC 791).
- Ability to fragment IP packets prior to encryption (RFC 4459).

In addition, your client must support certificate authentication and ESP/SHA1.

## Supported Features

The following features are unavailable to the end-user since you are using a third-party client that are neither controlled nor configured by Juniper Networks.

- Host Checker
- Cache Cleaner
- Idle timeout notifications
- Upload Logs
- Route monitoring feature of split tunnel
- Windows interactive user logon options
- Session startup scripts
- NCP tunnel mode
- DNS search order
- Proxy server settings

The following table outlines the behavior of the Network Connect client and the IKEv2 client for certain split tunnel options:

Option	IKEv2 Client	Network Connect Client
Disable split tunnel mode	Resource—through tunnel	Resource—through tunnel
	Internet—through tunnel	Internet—through tunnel
	local subnet( client)—through physical adapter	local subnet( client)—through tunnel
Enable split tunnel mode	Resource—through tunnel	Internet—through physical adapter
	Internet—through tunnel but fails because the resource is not in split tunnel configuration.	local subnet( client)—through physical adapter
	local subnet( client)—through physical adapt	

Allow local access subnet	Resource—through tunnel Internet—through tunnel local subnet( client)— through physical adapter ( same as disable split tunnel mode)	Internet & other traffic—through tunnel local subnet( client)—through physical adapter
Enable split tunnel mode with route monitor( NC proprietary)	Resource—through tunnel Internet—through tunnel but fails because the resource is not in split tunnel configuration. local subnet( client)— through physical adapter Note: route table delete is not monitored.	Resource—through tunnel Internet—through physical adapter local subnet( client)—through physical adapter Note: route table delete is monitored
Enable ST with Allow local access subnet	Resource—through tunnel Internet —through tunnel but fails because the resource is not in split tunnel configuration. local subnet( client)— through physical adapter	Resource—through tunnel Internet—through physical adapter local subnet( client)—through physical adapter

Please note the following:

- IKEv2 does not support automatic cluster failover. After cluster failover, IKEv2 users must reconnect to Secure Access Service.
- For IKEv2 with client certification authentication to work with Windows 7 IKEv2 client, the certificate imported in to Secure Access Service must have the enhanced key usage (EKU) value set to **serverAuth(1.3.6.1.5.7.3.1)**

#### Related Documentation

- [Task Summary: Configuring Secure Access Service for IKEv2](#)
- [Defining the IKEv2 Role Mapping Rule on page 1177](#)
- [Enabling the IKEv2 Access Feature on page 1178](#)

## Task Summary: Configuring Secure Access for IKEv2

IKEv2 EAP supports the following authentication server types:

- Local authentication
- Active Directory

If you are using IKEv2 EAP authentication on a local authentication server, you must select the **Password stored as clear text** checkbox in the Auth Server page of the admin console. Note that you can not edit an existing local authentication server instance to select this option. If you require IKEv2 EAP authentication on a local authentication server, you must create a new local authentication server instance.



**NOTE:** IKEv2 EAP does not work with any pre-existing local authentication servers since they do not store passwords in clear text.

To configure Secure Access Service support for IKEv2, you must:

1. Configure your client for using IKE. For more information, see your mobile device's documentation.
2. Install client (only if using certificate authentication) and device certificates.
  - You need a Certificate Authority (CA) that can issue client certificates.
  - On the client side, install this client certificate (only if using certificate authentication) along with the CA certificate.
  - If you are using client certification authentication to authenticate IKEv2 clients, on the server side (Secure Access Service), install the CA certificate under Configuration/Certificates/Trusted Client CAs.
3. Select the authentication server to authenticate IKEv2 users under Users > User Realms > User > General.
4. Define an IKEv2 rule under the Users > User Realms > User > Role Mapping page of the admin console.
5. Select the IKEv2 access feature under the Users > User Roles > User > General > Overview page of the admin console.
6. Enable VPN Tunneling for the Role and configure a VPN Tunneling Connection Profile (IP pool) to use for that Role.
7. Configure the port/realm mapping and the realm/EAP protocol mapping.

When a client uses IKEv2 to connect to Secure Access Service, the Agent Type column of the Active Users page displays IKEv2.

#### Related Documentation

- [Defining the IKEv2 Role Mapping Rule on page 1177](#)
- [Enabling the IKEv2 Access Feature on page 1178](#)
- [Defining a Local Authentication Server Instance on page 184](#)

## Defining the IKEv2 Role Mapping Rule

Role mapping rules are conditions a user must meet in order for Secure Access Service to map the user to one or more user roles.



**NOTE:** The procedure described in this topic is required only if you want to create a separate role mapping rule specific for IKEv2 users. If you use regular username, group or custom expression-based role mapping rules (typically used for general access to Secure Access Service), the procedure described below is not required.

1. Select **User > User Realms > User > Role Mapping** in the admin console.
2. Click **New Rule**.
3. Select Custom Expressions as the type of condition on which to base the rule.
4. Click **Update** to display the Expressions list.
5. Click the Expressions button to display the Expressions tab of the server catalog.
6. Create a rule: **userAgent = "IKEv2"**.
7. Click **Add Expression** and then **Close**.
8. Select the rule you just created from the Available Expressions list and click **Add** to move it to the Selected Expressions list.
9. Specify the roles to assign to the authenticated user by adding roles to the Selected Roles list.
10. (optional) Check the Stop processing rules when this rule matches checkbox if you want the Secure Access Service to stop evaluating role mapping rules when the user meets the conditions specified for this role.
11. Click **Save Changes**.

**Related  
Documentation**

- Task Summary: Configuring Secure Access Service for IKEv2
- [Enabling the IKEv2 Access Feature on page 1178](#)

---

## Enabling the IKEv2 Access Feature

---

Roles specify the Secure Access Service session properties, including enabled access features, for users who are mapped to the role.

To enable the IKEv2 access feature:

1. Select **User > User Roles > Role Name > General > Overview** from the admin console.
2. Under Access Features, check the **VPN Tunneling** checkbox.
3. Click **Save Changes**.

**Related  
Documentation**

- Task Summary: Configuring Secure Access Service for IKEv2
- [Defining the IKEv2 Role Mapping Rule on page 1177](#)

---

## Configuring the IKEv2 Ports

---

To configure the IKEv2 ports and EAP protocol:

1. Select **System > Configuration > IKEv2** in the admin console.
2. Enter the DPD timeout value in seconds. Valid values are 400-3600.

DPD is a form of keepalive. When a tunnel is established but idle, one or both sides may send a “hello” message and the other replies with an acknowledgement. If no response is received, this continues until the DPD time value has elapsed. If there still isn’t any traffic or acknowledgement, the peer is determined to be dead and the tunnel is closed.

3. Under Port/Realm Mapping, select the port and the realm to use that port.

To add additional port/realm mapping sets, click **Add**.

To delete a port/realm mapping set, select the checkbox next to the set to remove and click **Delete**.

4. Under Realm / Protocol Set Mapping, select the realm and the EAP protocol set to use for that realm.

To add additional realm/protocol mapping sets, click **Add**.

To delete a realm/protocol mapping set, select the checkbox next to the set to remove and click **Delete**.

5. Click Save Changes.



.....

**NOTE:** Changing IKEv2 configuration (**System > Configuration > IKEv2**) in the admin console will disconnect connections from IKEv2 clients, VPN Tunneling and Pulse. VPN Tunneling and Pulse will reconnect automatically.

.....





# Writing Custom Expressions

- [Custom Expressions on page 1181](#)
- [Elements Used in Custom Expressions on page 1182](#)
- [Wildcard Matching on page 1185](#)
- [Distinguished Name Variables and Functions on page 1186](#)
- [System Variables and Examples on page 1186](#)
- [Using System Variables in Realms, Roles, and Resource Policies on page 1197](#)
- [Using Multi-Valued Attributes on page 1198](#)
- [Specifying Multi-valued Attributes in a Bookmark Name on page 1199](#)
- [Specifying Fetch Attributes in a Realm on page 1199](#)
- [Specifying the homeDirectory Attribute for LDAP on page 1200](#)
- [Using Custom Variables and Macros on page 1200](#)

## Custom Expressions

---

The Secure Access Service enables you to write custom expressions that are evaluated in role mapping rules, resource policies, and log filter queries. A *custom expression* is a combination of variables that the Secure Access Service evaluates as a boolean object to true, false, or error. Custom expressions enable you to better manage resource access control by providing a means to specify complex statements for policy evaluation and log queries.

You can write custom expressions in the following formats. Note that elements of these formats are described in greater detail in the table that follows:

- *variable comparisonOperator variable*
- *variable comparisonOperator simpleValue*
- *variable comparisonOperator (simpleValue)*
- *variable comparisonOperator (OR Values)*
- *variable comparisonOperator (AND Values)*
- *variable comparisonOperator (time TO time)*
- *variable comparisonOperator (day TO day)*

- isEmpty (variable)
- isUnknown (variable)
- (customExpr)
- NOT customExpr
- ! customExpr
- customExpr OR customExpr
- customExpr || customExpr
- customExpr AND customExpr
- customExpr && customExpr

**Related Documentation**

- [Elements Used in Custom Expressions on page 1182](#)
- [Wildcard Matching on page 1185](#)
- [Distinguished Name Variables and Functions on page 1186](#)
- [System Variables and Examples on page 1186](#)

## Elements Used in Custom Expressions

**Table 86: Custom Expression Elements**

<i>variable</i>	<p>Represents a system variable. A variable name is a dot-separated string, and each component can contain characters from the set [a-z A-Z 0-9_] but cannot start with a digit [0-9]. Variable names are case-insensitive. For system variables that you may use in role mapping rules and resource policies.</p> <p>When writing a custom expression in a log query field, you need to use system log variables. These variables are described in the <b>Filter Variables Dictionary</b> on the Filter page (<b>System &gt; Log/Monitoring &gt; Events   User Access   Admin Access &gt; Filters &gt; Select Filter</b> tab).</p>
	<p>Quoting syntax for variables:</p> <p>The Secure Access Service supports a quoting syntax for custom expression variables that allows you to use any character except '.' (period) in a user attribute name. To escape characters in an attribute name, quote some or all of the variable name using {} (curly-braces). For example, these expressions are equivalent:</p> <ul style="list-style-type: none"> <li>• userAttr.{Login-Name} = 'xyz'</li> <li>• userAttr.Login{-}Name = 'xyz'</li> <li>• {userAttr.Login-Name} = 'xyz'</li> <li>• userA{ttr.L}{ogin-}Name = 'xyz'</li> </ul>
	<p>Escape characters supported within quotes:</p>
\\	represents a \ (backslash)

Table 86: Custom Expression Elements (*continued*)

\{	represents a { (left curly-brace)
\}	represents a } (right curly-brace)
\hh	represents a hexadecimal value where hh is two characters from [0-9A-Fa-f]
<p><i>Examples:</i></p> <ul style="list-style-type: none"> <li>• userAttr.{Tree Frog} = 'kermit'</li> <li>• userAttr.{Tree\20Frog} = 'kermit'</li> </ul>	
<p><i>Notes:</i></p> <ul style="list-style-type: none"> <li>• There is no limit to the number of quotes you can use in a variable name.</li> <li>• You can use the quoting syntax with any variable—not just userAttr.* variables.</li> <li>• You need to use curly-brace quotes only when writing custom expressions.</li> </ul>	
<i>comparisonOperator</i>	is one of the following:
=	equal to — Use with strings, numbers, and DNs.
!=	not equal to — Use with strings, numbers, and DNs.
<	less than — Use with numbers
<=	less than or equal to — Use with numbers
>	greater than — Use with numbers
>=	greater than or equal to — Use with numbers

Table 86: Custom Expression Elements (*continued*)

<i>simpleValue</i>	<p>is one of the following:</p> <ul style="list-style-type: none"> <li>• <i>string</i> — quoted string that may contain wildcards.</li> <li>• <i>IP Address</i> — a.b.c.d</li> <li>• <i>subnet</i> — a.b.c.d/subnetBitCount or a.b.c.d/netmask</li> <li>• <i>number</i> — positive or negative integer</li> <li>• <i>day</i> — SUN MON TUE WED THU FRI SAT</li> </ul> <p><i>Notes about strings:</i></p> <ul style="list-style-type: none"> <li>• A string may contain all characters except &lt;nl&gt; (newline) and &lt;cr&gt; (carriage return).</li> <li>• Strings can be any length.</li> <li>• String comparisons are case-insensitive.</li> <li>• Strings can be quoted with single- or double-quotes. A quoted string may contain wildcards, including star(*), question mark (?), and square brackets ([ ]).</li> <li>• <i>variable comparisonOperator variable</i> comparisons are evaluated without wildcard matching.</li> <li>• Use a backslash to escape these characters:        single-quote (') — \'        double-quote (") — \        backslash (\) — \        hexadecimal — \hh [0-9a-fA-F]</li> </ul> <p><i>Note about day:</i></p> <p>Day and time comparisons are evaluated in the Secure Access Service's time zone. Day range (<i>day TO day</i>) calculations start with the first day and step forward until the second day is reached. In time range (<i>time TO time</i>) calculations, the first value must be earlier than the second value. Only time variables can be compared to day and time values. The time variables are: time.* and loginTime.*</p>
<i>time</i>	<p>is the time of day in one of the following formats:</p> <ul style="list-style-type: none"> <li>• <i>HH:MM</i> — 24-hour</li> <li>• <i>HH:MMam</i> — 12-hour</li> <li>• <i>HH:MMpm</i> — 12-hour</li> <li>• <i>H:MM</i> — 24-hour</li> <li>• <i>H:MMam</i> — 12-hour</li> <li>• <i>H:MMpm</i> — 12-hour</li> </ul> <p>Day and time comparisons are evaluated in the Secure Access Service' time zone. Day range (<i>day TO day</i>) calculations start with the first day and step forward until the second day is reached. In time range (<i>time TO time</i>) calculations, the first value must be earlier than the second value. Only time variables can be compared to day and time values. The time variables are: time.* and loginTime.*</p>
OR Value	<p>is a string containing one or more OR comparisons:</p> <ul style="list-style-type: none"> <li>• <i>variable comparisonOperator (number OR number ...)</i></li> <li>• <i>variable comparisonOperator (string OR string ...)</i></li> </ul>

Table 86: Custom Expression Elements (*continued*)

AND Value	<p>is a string containing one or more AND comparisons</p> <ul style="list-style-type: none"> <li>• <i>variable comparisonOperator (number AND number ...)</i></li> <li>• <i>variable comparisonOperator (string AND string ...)</i></li> </ul>
isEmpty	<p>is a function that takes a single variable name (<i>variable</i>) argument and returns a boolean value. isEmpty() is true if the variable is unknown or has a zero-length value, zero-length strings, and empty lists.</p> <p><i>Example:</i> isEmpty(userAttr.terminationDate)</p>
isUnknown	<p>is a function that takes a single variable name (<i>variable</i>) argument and returns a boolean value. isUnknown() is true if the variable is not defined. User attributes (userAttr.* <i>variables</i>) are unknown if the attribute is not defined in LDAP or if the attribute lookup failed (such as if the LDAP server is down).</p> <p><i>Example:</i> isUnknown(userAttr.bonusProgram)</p>
NOT, !	<p>is the logical negation <i>comparisonOperator</i>. The negated expression evaluates to true if the <i>customExpr</i> is false and evaluates to false if the <i>customExpr</i> is true. The operators NOT, AND, and OR are evaluated from highest to lowest precedence in this order: NOT (from right), AND (from left), OR (from left).</p>
OR,	<p>is the logical operator OR or   , which are equivalent. The operators NOT, AND, and OR are evaluated from highest to lowest precedence in this order: NOT (from right), AND (from left), OR (from left).</p>
AND, &&	<p>is the logical AND or &amp;&amp;, which are equivalent. The operators NOT, AND, and OR are evaluated from highest to lowest precedence in this order: NOT (from right), AND (from left), OR (from left).</p>
<i>customExpr</i>	<p>is an expression written in the Custom Expression Syntax (see above).</p>

#### Related Documentation

- [Wildcard Matching on page 1185](#)
- [Distinguished Name Variables and Functions on page 1186](#)
- [System Variables and Examples on page 1186](#)

## Wildcard Matching

You may use wildcards within a quoted string. Supported wildcards include:

- **star (\*)**—A star matches any sequence of zero or more characters.
- **question mark (?)**—A question mark matches any single character.
- **square brackets ([ ])**—Square brackets match one character from a range of possible characters specified between the brackets. Two characters separated by a dash (-) match the two characters in the specified range and the lexically intervening characters. For example, 'dept[0-9]' matches strings "dept0", "dept1", and up to "dept9".

To escape wildcard characters, place them inside square brackets. For example, the expression ' **userAttr.x** = " *value* [\*]" ' evaluates to true if attribute x is exactly "*value*\*".

**Related  
Documentation**

- [Elements Used in Custom Expressions on page 1182](#)
- [Distinguished Name Variables and Functions on page 1186](#)
- [System Variables and Examples on page 1186](#)

---

## Distinguished Name Variables and Functions

You can compare a distinguished name (DN) to another DN or to a string, but the Secure Access Service ignores wildcards, white space, and case. Note, however, that the Secure Access Service takes the order of DN keys into consideration.

When the Secure Access Service compares an expression to a DN to a string, it converts the string to a distinguished name before evaluating the expression. If the Secure Access Service cannot convert the string due to bad syntax, the comparison fails. The DN variables are:

- **userDN**
- **certDN**
- **certIssuerDN**

The Secure Access Service also supports DN suffix comparisons using the `matchDNSuffix` function. For example:

```
matchDNSuffix(certDn, "dc=danastreet,dc=net")
```

Within the parenthesis, the first parameter is the " full" DN and the second is the suffix DN. You can use a variable or string for each parameter. Note that this first parameter should have more keys than the second (suffix parameter). Otherwise, if they are equal, it is the same as `<firstparam> = <secondparam>`. If the second parameter has more keys, `matchDNSuffix` returns false.

**Related  
Documentation**

- [Elements Used in Custom Expressions on page 1182](#)
- [Wildcard Matching on page 1185](#)
- [System Variables and Examples on page 1186](#)

---

## System Variables and Examples

The following table lists and defines system variables, gives an example for each system variable, and provides a guide as to where you may use system variables.



**NOTE:** This list does not include variables used in a filter query or an export format for a system log. These variables are described in the Filter Variables Dictionary on the Filter page (System > Log/Monitoring > Events | User Access | Admin Access > Filters > *Select Filter* tab).

**Table 87: System Variables and Examples**

Variable	Description	Examples
authMethod  Available in:  role mapping rules  resource policy rules role mapping rules	Type of authentication method used to authenticates a user.	authMethod = 'ACE Server'
cacheCleanerStatus	The status of Cache Cleaner. Possible values:  1 - if it is running  0 - if otherwise	cacheCleanerStatus = 1 cacheCleanerStatus = 0
certAttr.<cert-attr>  Available in:  <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> <li>• LDAP configuration</li> </ul>	Attributes from a client-side certificate. Examples of certAttr attributes include:  <ul style="list-style-type: none"> <li>• C - country</li> <li>• CN - common name</li> <li>• description - description</li> <li>• emailAddress - email address</li> <li>• GN - given name</li> <li>• initials - initials</li> <li>• L - locality name</li> <li>• O - organization</li> <li>• OU - organizational unit</li> <li>• SN - surname</li> <li>• serialNumber- serial number</li> <li>• ST - state or province</li> <li>• title - title</li> <li>• UI - unique identifier</li> </ul> Use this variable to check that the user's client has a client-side certificate with the value(s) specified.	certAttr.OU = 'Retail Products Group'

Table 87: System Variables and Examples (*continued*)

Variable	Description	Examples
<p>certAttr.altName.&lt;Alt-attr&gt;</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> <li>SSO parameter fields</li> <li>LDAP configuration</li> </ul>	<p>Subject alternative name value from a client-side certificate where &lt;Alt-attr&gt; may be:</p> <ul style="list-style-type: none"> <li>Email</li> <li>EmailId</li> <li>EmailDomain</li> <li>DNS</li> <li>registeredId</li> <li>ipAddress</li> <li>UPN</li> <li>UPNid</li> <li>UPNDomain</li> <li>fascn</li> <li>fascnAC</li> <li>fascnSC</li> <li>fascnCN</li> <li>fascnCS</li> <li>fascnCI</li> <li>fascnPI</li> <li>fascnOC</li> <li>fascnOI</li> <li>fascnPOA</li> <li>fascnLRC</li> </ul>	<ul style="list-style-type: none"> <li>certAttr.altName.email = "joe@company.com"</li> <li>certAttr.altName.ipAddress = 10.10.83.2</li> </ul>
<p>certAttr.serialNumber</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> <li>SSO parameter fields</li> <li>LDAP configuration</li> </ul>	<p>Client certificate serial number.</p> <p>Note that all characters other than [0-9 a-f A-F] are stripped out of a string before comparison with certAttr.SN. Wildcards are not supported.</p>	<ul style="list-style-type: none"> <li>certAttr.SerialNumber = userAttr.certSerial</li> <li>certAttr.SerialNumber = "6f:05:45:ab"</li> </ul>
<p>certDN</p> <p>Available in:</p> <p>role mapping rules</p> <p>resource policy rules</p>	<p>Client certificate subject DN. Wildcards are not permitted.</p>	<ul style="list-style-type: none"> <li>certDN = 'cn=John Harding,ou=eng,c=Company'</li> <li>certDN = userDN (match the certificate subject DN with the LDAP user DN)</li> <li>certDN = userAttr.x509SubjectName</li> <li>certDN = ('cn=John Harding,ou=eng,c=Company' or 'cn=Julia Yount,ou=eng,c=Company')</li> </ul>



Table 87: System Variables and Examples (*continued*)

Variable	Description	Examples
certDN.<subject-attr> Available in: <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> <li>• LDAP configuration</li> </ul>	Any variable from the client certificate subject DN, where <b>subject-attr</b> is the name of the RDN key.  Use to test the various subject DN attributes in a standard x.509 certificate.	<ul style="list-style-type: none"> <li>• certDN.OU = 'company'</li> <li>• certDN.E = 'joe@company.com'</li> <li>• certDN.ST = 'CA'</li> </ul>
certDNText Available in: <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> </ul>	Client certificate user DN stored as a string. Only string comparisons to this value are allowed.	certDNText = 'cn=John Harding,ou=eng,c=Company'
certIssuerDN Available in: <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> </ul>	Client certificate-issuer subject DN. This variable works like a standard DN attribute such as CertDN. Wildcards are not permitted.	<ul style="list-style-type: none"> <li>• certIssuerDN = 'cn=John Harding,ou=eng,c=Company'</li> <li>• certIssuerDN = userAttr.x509Issuer</li> <li>• certIssuerDN = ('ou=eng,c=Company' or 'ou=operations,c=Company')</li> </ul>
certIssuerDN.<issuer-attr> Available in: <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> </ul>	Any variable from the client certificate-issuer subject DN, where <b>issuer-attr</b> is the name of the RDN key.	<ul style="list-style-type: none"> <li>• certIssuerDN.OU = 'company'</li> <li>• certIssuerDN.ST = 'CA'</li> </ul>
certIssuerDNText Available in: <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> </ul>	Client certificate-issuer subject DN stored as a string. Only string comparisons to this value are allowed.	certIssuerDNText = 'cn=John Harding,ou=eng,c=Company'
defaultNTDomain Available in: <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> </ul>	Contains the Domain value set in the Secure Access Service authentication server configuration when you use AD/NT authentication.	defaultNTDomain=" CORP"

Table 87: System Variables and Examples (*continued*)

Variable	Description	Examples
<p><code>group.&lt;group-name&gt;</code></p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> </ul> <p>Only those groups evaluated for role mapping rules are available in the detailed rules (conditions) in the resource policies. We recommend that you use the <b>groups</b> variable instead of <b>group.&lt;group-name&gt;</b>, which is supported only for backwards compatibility.</p>	<p>User's group membership as provided by the realm authentication or directory server.</p>	<ul style="list-style-type: none"> <li><code>group.preferredPartner</code></li> <li><code>group.goldPartner</code> or <code>group.silverPartner</code></li> <li><code>group.employees</code> and <code>time.month = 9</code></li> </ul> <p>Combination examples: Allow all partners with active status from Monday to Friday but preferred partners Monday through Saturday: <code>((group.partners and time = (Mon to Fri)) or (group.preferredPartners and time = (Mon to Sat))) and userAttr.partnerStatus = 'active'</code></p> <p><b>NOTE:</b> Spaces are not supported, such as, <code>group.sales managers</code></p>
<p><code>groups</code></p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> <li>SSO parameter fields</li> </ul>	<p>List of groups as provided by the realm authentication or directory server.</p> <p><b>NOTE:</b> You can enter any characters in the groupname, although wildcard characters are not supported.</p>	<p><code>groups=('sales managers')</code></p>
<p><code>hostCheckerPolicy</code></p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> <li>SSO parameter fields</li> </ul>	<p>Host Checker polices that the client has met.</p>	<p><code>hostCheckerPolicy = ('Norton' and 'Sygate')</code> and <code>cacheCleanerStatus = 1</code> <code>hostCheckerPolicy = ('Norton' and 'Sygate')</code></p>
<p><code>loginHost</code></p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> <li>SSO parameter fields</li> <li>LDAP configuration</li> </ul>	<p>Host name or IP address that the browser uses to contact the Secure Access Service.</p>	<p><code>loginHost = 10.10.10.10</code></p>
<p><code>loginTime</code></p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> <li>SSO parameter fields</li> </ul>	<p>The time of day at which the user submits his credentials to the Secure Access Service. The time is based on the Secure Access Service time.</p> <p><b>NOTE:</b> When using this variable in an SSO parameter field, the variable returns the UNIX string time.</p>	<ul style="list-style-type: none"> <li><code>loginTime = (8:00am)</code></li> <li><code>loginTime= (Mon to Fri)</code></li> </ul>

Table 87: System Variables and Examples (*continued*)

Variable	Description	Examples
<p>loginTime.day</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> </ul>	<p>The day of month on which the user submits his credentials to the Secure Access Service, where day is 1-31. The time is based on the Secure Access Service time.</p> <p>You cannot use the TO operator with this variable.</p>	<p>loginTime.day = 3</p>
<p>loginTime.dayOfWeek</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> </ul>	<p>The day of the week on which the user submits his credentials to the Secure Access Service, where dayOfWeek is in the range [0-6] where 0 = Sunday.</p> <p>The Secure Access Service does not support the <b>TO</b> operator with time.dayOfWeek expressions if you use numbers instead of strings. In other words, "loginTime.dayOfWeek = (2 TO 6)" does not work, but "loginTime.dayOfWeek = (mon to fri)" does work.</p>	<ul style="list-style-type: none"> <li>• loginTime.dayOfWeek = (0 OR 6)</li> <li>• loginTime.dayOfWeek = (mon TO fri)</li> <li>• loginTime.dayOfWeek = (1)</li> <li>• loginTime.dayOfWeek = 5</li> </ul>
<p>loginTime.dayOfYear</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> </ul>	<p>The numeric day of the year on which the user submits his credentials to the Secure Access Service, where dayOfYear can be set to [0-365].</p> <p>You cannot use the TO operator with this variable.</p>	<p>loginTime.dayOfYear = 100</p>
<p>loginTime.month</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> </ul>	<p>The month in which the user submits his credentials to the Secure Access Service, where month can be set to [1-12] where 1 = January.</p> <p>You cannot use the TO operator with this variable.</p>	<p>loginTime.month &gt;= 4 AND loginTime.month &lt;= 9</p>
<p>loginTime.year</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> </ul>	<p>The year in which the user submits his credentials to the Secure Access Service, where year can be set to [1900-2999].</p> <p>You cannot use the TO operator with this variable.</p>	<p>loginTime.year = 2005</p>
<p>loginURL</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> <li>• LDAP configuration</li> </ul>	<p>URL of the page that the user accessed to sign in to the Secure Access Service. The Secure Access Service gets this value from the Administrator URLs User URLs column on the <b>Authentication &gt; Signing In &gt; Sign-in Policies</b> page of the admin console.</p>	<p>loginURL = */admin</p>

Table 87: System Variables and Examples (*continued*)

Variable	Description	Examples
networkIf  Available in:  <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> </ul>	The network interface on which the user request is received. Possible values: internal, external	sourceIp = 192.168.1.0/24 and networkIf = internal
ntdomain  Available in:  <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• SSO parameter fields</li> </ul>	The NetBIOS NT domain used in NT4 and Active Directory authentication.	ntdomain = jnpr
ntuser  Available in:  <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• SSO parameter fields</li> </ul>	The NT username used in Active Directory authentication	ntuser = jdoe
password  password[1]  password[2]  Available in:  <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> </ul>	The password entered by the user for the primary authentication server (password and password[1]) or the secondary authentication server (password[2]).	<b>password = A1defo2z</b>
realm  Available in:  <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> </ul>	The name of the authentication realm to which the user is signed in.	Realm = ('GoldPartners' or 'SilverPartners')  <b>NOTE:</b> AND condition will always fail as a user is only allowed to sign in to a single realm in a session.
role  Available in:  <ul style="list-style-type: none"> <li>• resource policy rules</li> <li>• SSO parameter fields</li> </ul>	List of all the user roles for the session.  In SSO, if you want to send all the roles to back-end applications, use <role sep = ";"> - where sep is the separator string for multiple values. The Secure Access Service supports all separators except " and >.	<ul style="list-style-type: none"> <li>• Role = ('sales' or 'engineering')</li> <li>• Role = ('Sales' AND 'Support')</li> </ul>

Table 87: System Variables and Examples (*continued*)

Variable	Description	Examples
<p>sourceIP</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> <li>SSO parameter fields</li> </ul>	<p>The IP address of the machine on which the user authenticates. You can specify the netmask using the bit number or in the netmask format: '255.255.0.0'. Note that you can evaluate the <b>sourceIP</b> expression against a string variable such as an LDAP attribute.</p>	<ul style="list-style-type: none"> <li>sourceIP = 192.168.10.20</li> <li>sourceIP = 192.168.1.0/24 and networkIf internal</li> <li>userAttr.dept = ('eng' or 'it') and sourceIP = 10.11.0.0/16</li> <li>sourceIP = 192.168.10.0/24 (Class C) is the same as: sourceIP = 192.168.10.0/255.255.255.0</li> <li>sourceIP=userAttr.sourceip</li> </ul>
<p>time</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> </ul>	<p>The time of day at which the role mapping rule or resource policy rule is evaluated. The time of the day can be in 12-hour or 24-hour format.</p>	<ul style="list-style-type: none"> <li>time = (9:00am to 5:00pm)</li> <li>time = (09:00 to 17:00)</li> <li>time = (Mon to Fri)</li> </ul> <p>Combination examples: Allow executive managers and their assistants access from Monday to Friday:</p> <p>userAttr.employeeType = ('*manager*' or '*assistant*') and group.executiveStaff and time = (Mon to Fri)</p>
<p>time.day</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> </ul>	<p>The day of month on which the user submits his credentials to the Secure Access Service, where day is 1-31. The time is based on the Secure Access Service time.</p>	<p>loginTime.day = 3</p>
<p>time.dayOfWeek</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> </ul>	<p>The day of the week on which the role mapping rule or resource policy rule is evaluated, where dayOfWeek is in the range [0-6] where 0 = Sunday.</p>	<ul style="list-style-type: none"> <li>loginTime.dayOfWeek = (0 OR 6)</li> <li>loginTime.dayOfWeek = (1 to 5)</li> <li>loginTime.dayOfWeek = 5</li> </ul>
<p>time.dayOfYear</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> </ul>	<p>The day of the year on which the role mapping rule or resource policy rule is evaluated. Possible values include: 1-365.</p>	<p>time.dayOfYear = 100</p>

Table 87: System Variables and Examples (*continued*)

Variable	Description	Examples
<p>time.month</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> </ul>	<p>The month in which the role mapping rule or resource policy rule is evaluated. Possible values include: 1-12</p>	<ul style="list-style-type: none"> <li>time.month &gt;= 9 and time.month &lt;= 12 and time.year = 2004</li> <li>group.employees and time.month = 9</li> </ul>
<p>time.year</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> </ul>	<p>The year in which the role mapping rule or resource policy rule is evaluated, where year can be set to [1900-2999].</p>	<p>time.year = 2005</p>
<p>user</p> <p>user@primary_auth_server_name</p> <p>user@secondary_auth_server_name</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> <li>SSO parameter fields</li> </ul>	<p>Secure Access Service username for the user's primary authentication server (user and user@primary_auth_server_name) or secondary authentication server (user@secondary_auth_server_name). Use when authenticating against an Active Directory server, domain and username.</p> <p>primary_auth_server_name is the name of the primary auth server. If there are spaces or special characters in the name, it can be enclosed in curly brackets. For example user@{My Primary Auth Server}</p> <p>secondary_auth_server_name is the name of the secondary auth server. If there are spaces or special characters in the name, it can be enclosed in curly brackets. For example user@{My Secondary Auth Server}</p> <p><b>NOTE:</b> When including a domain as part of a username, you must include two slashes between the domain and user. For example: user='yourcompany.net\joeuser'.</p>	<ul style="list-style-type: none"> <li>user = 'steve'</li> <li>user = 'domain\steve'</li> </ul>

Table 87: System Variables and Examples (*continued*)

Variable	Description	Examples
username username@primary_auth_server_name username@secondary_auth_server_name	Secure Access Service username for the user's primary authentication server (username and username@primary_auth_server_name) or secondary authentication server (username@secondary_auth_server_name). If the user is signing in to a certificate authentication server, then the user's Secure Access Service username is the same as CertDN.cn.	<ul style="list-style-type: none"> <li>username = 'steve' and time = mon</li> <li>username = 'steve'</li> <li>username = 'steve*'</li> <li>username = ('steve' or '*jankowski')</li> </ul>
Available in:	primary_auth_server_name is the name of the primary auth server. If there are spaces or special characters in the name, it can be enclosed in curly brackets. For example user@{My Primary Auth Server}	
<ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> <li>SSO parameter fields</li> </ul>	secondary_auth_server_name is the name of the secondary auth server. If there are spaces or special characters in the name, it can be enclosed in curly brackets. For example user@{My Secondary Auth Server}	
userAgent	The browser's user agent string.	The browser's user agent string.
Available in:		
<ul style="list-style-type: none"> <li>role mapping rules</li> <li>resource policy rules</li> <li>SSO parameter fields</li> </ul>		

Table 87: System Variables and Examples (*continued*)

Variable	Description	Examples
<p>userAttr.&lt;auth-attr&gt;</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> </ul>	<p>User attributes retrieved from an LDAP, RADIUS, or SiteMinder authentication or directory server.</p>	<ul style="list-style-type: none"> <li>• userAttr.building = ('HQ*' or 'MtView[1-3]')</li> <li>• userAttr.dept = ('sales' and 'eng')</li> <li>• userAttr.dept = ('eng' or 'it' or 'custsupport')</li> <li>• userAttr.division = 'sales'</li> <li>• userAttr.employeeType != 'contractor'</li> <li>• userAttr.salaryGrade &gt; 10</li> <li>• userAttr.salesConfirmed &gt;= userAttr.salesQuota</li> </ul> <p><i>Negative examples:</i></p> <ul style="list-style-type: none"> <li>• userAttr.company != "Acme Inc" or not group.contractors</li> <li>• not (user = 'guest' or group.demo)</li> </ul> <p><i>Combination examples:</i></p> <p>Allow executive managers and their assistants access from Monday to Friday:</p> <p>userAttr.employeeType = ('*manager*' or '*assistant*') and group.executiveStaff and time = (Mon to Fri)</p> <p>Allow all partners with active status from Monday to Friday but preferred partners Monday through Saturday:</p> <p>((group.partners and time = (Mon to Fri)) or (group.preferredPartners and time = (Mon to Sat))) and userAttr.partnerStatus = 'active'</p>
<p>userDN</p> <p>Available in:</p> <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> </ul>	<p>The user DN from an LDAP server. If the user is authenticated by the LDAP server, then this DN is from the authentication server; otherwise, the DN comes from the realm's Directory/Attribute server. Wildcards are not permitted.</p>	<ul style="list-style-type: none"> <li>• userDN = 'cn=John Harding,ou=eng,c=Company'</li> <li>• userDN = certDN</li> </ul>



Table 87: System Variables and Examples (*continued*)

Variable	Description	Examples
userDN.<user-attr>  Available in: <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> </ul>	Any variable from the user DN, where user-attr is the name of the RDN key.	Any variable from the user DN, where user-attr is the name of the RDN key.
userDNText  Available in: <ul style="list-style-type: none"> <li>• role mapping rules</li> <li>• resource policy rules</li> <li>• SSO parameter fields</li> </ul>	User DN stored as a string. Only string comparisons to this value are allowed.	userDNText = 'cn=John Harding,ou=eng,c=Company'

**Related Documentation**

- [Elements Used in Custom Expressions on page 1182](#)
- [Wildcard Matching on page 1185](#)
- [Distinguished Name Variables and Functions on page 1186](#)

## Using System Variables in Realms, Roles, and Resource Policies

You can use system variables to define user realm attributes, role settings, and resource policies. Using system variables in this way allows you the flexibility to configure certain parameters dynamically based on LDAP attributes or other information available for the user.

When specifying variables, use the standard variable syntax `<variable>` as in `<user>` and `<time>`. When adding an attribute to a variable, use the syntax `<variable.attribute>` as in `<userAttr.SourceIP>` and `<group.sales>`.

The Secure Access Service allows the use of system variables when configuring the following user roles settings:

- **Web bookmarks**—Bookmarked resource (actual URL)
- **Windows/NFS File bookmarks**—File resource (server, share or path)
- **Telnet/SSH**—host name
- **JSAM**—Exchange Servers, Custom Client-server host names
- **WSAM**—host names and IP/Netmasks
- **Terminal Services**—Application hosts
- **UI Options\Custom Welcome Text**—The greeting message can contain any system variables

You can use the <USER> substitution variable in ACLs for web pages, telnet, files, and SAM. You cannot use the variable in VPN Tunneling ACLs.

**Related  
Documentation**

- [Elements Used in Custom Expressions on page 1182](#)
- [Wildcard Matching on page 1185](#)
- [Distinguished Name Variables and Functions on page 1186](#)
- [System Variables and Examples on page 1186](#)

---

## Using Multi-Valued Attributes

Multi-valued attributes—attributes that contain two or more values—provide you with a convenient method for defining resources that expand into multiple individual bookmarks on the users' bookmarks page.

For example, assume that the user's LDAP directory contains the multi-valued attribute HomeShares: \\Srv1\Sales;\\Srv2\Marketing. When you configure the Windows File share resource definition using the HomeShares multi-valued attribute, \\<userAttr.HomeShares>, the user sees two bookmarks:

- \\Srv1\Sales
- \\Srv2\Marketing

Now let's assume the user's LDAP directory contains a second multi-valued attribute defined as HomeFolders: Folder1;Folder2;Folder3. When you configure the Windows File share resource using both of the multi-valued attributes, \\<userAttr.HomeShares>\\<userAttr.HomeFolders>, the user sees the following six bookmarks:

- \\Srv1\Sales\Folder1
- \\Srv1\Sales\Folder2
- \\Srv1\Sales\Folder3
- \\Srv2\Marketing\Folder1
- \\Srv2\Marketing\Folder2
- \\Srv2\Marketing\Folder3

The only exception to this functionality is when the variable includes an explicit separator string. In this case, only one bookmark containing multiple resources displays on the users' bookmark page.

You specify the separator string in the variable definition using the syntax `sep='string'` where string equals the separator you want to use. For example, to specify a semi-colon as the separator, use the syntax `<variable.Attr sep='; '>`.

Use the following syntax for multi-valued attributes handling. Note that <variable> refers to a session variable such as <userAttr.name> or <CertAttr.name>:

- `<variable[Index]>`—You specify indexes in a variety of ways. If, for example, the total number of values for a given index is 5, and you want to specify the entire range of values you use `<variable[ALL]>`. If you want to specify only the fourth value, you use `<variable[4]>`.
- `<variable>` is the same as `<variable[ALL]>`.
- `<variable>` is the same as `<variable[ALL]>`.
- `<variable sep='str'>` and `<variable[All] sep='str'>` — These variable definitions always refer to a single string value with all the tokens expanded out with separator strings between the values.



**NOTE:** Variable names cannot contain spaces.

## Specifying Multi-valued Attributes in a Bookmark Name

Another common case of using multi-valued attributes occurs when you include a variable in a bookmark name and in a URL or file server/share field.

For example, again assume that the user's LDAP directory contains the multi-valued attribute `HomeShares: \\Srv1\Sales; \\Srv2\Marketing`. When you configure the Windows File share resource definition using the `HomeShares` multi-valued attribute, `<<userAttr.HomeShares>`, and you use the same attribute in the bookmark name field, `<userAttr.HomeShares>`, the Secure Access Service creates two bookmarks:

- `Srv1\Sales` bookmark pointing to `\\Srv1\Sales`
- `Srv2\Marketing` bookmark pointing to `\\Srv2\Marketing`

This does not create a situation in which you end up with the following set of conditions:

- `Srv1\Sales` bookmark pointing to `\\Srv1\Sales`
- `Srv1\Marketing` bookmark pointing to `\\Srv1\Marketing` (error)
- `Srv2\Sales` bookmark pointing to `\\Srv1\Sales` (error)
- `Srv2\Marketing` bookmark pointing to `\\Srv2\Marketing`

## Specifying Fetch Attributes in a Realm

To facilitate the support for various parameterized settings in user roles and resource policies, you have the ability to specify additional "fetch attributes." The Secure Access Service stores the fetch attributes when users log in so that you can use them in parameterized role or resource policy definitions.

the Secure Access Service pulls all the attributes that are currently stored in the Sever Catalog for the user's authentication or authorization LDAP server. So, make sure to add the LDAP user attributes that are used in role or resource policy definitions in the LDAP Server Catalog first.

When a user logs in, the Secure Access Service retrieves user attributes that are referenced in the role mapping rules plus all of the additional attributes referenced in the Server Catalog and stores all these values. Note that this should not incur a significant performance overhead because all the user attributes are retrieved in one single LDAP query.



**NOTE:** When you substitute variables, such as in IP/Netmasks, host names, etc., the values in the session are appropriately converted into the data type that is required by the particular application definition.

---

## Specifying the homeDirectory Attribute for LDAP

You can create a bookmark that automatically maps to a user's LDAP home directory. You can accomplish this using the LDAP attribute homeDirectory. You need to configure a realm that specifies the LDAP server instance as its auth server, and you need to configure role-mapping rules and a bookmark that points to the LDAP homeDirectory attribute.

---

## Using Custom Variables and Macros

- [About Custom Variables and Macros on page 1200](#)

### About Custom Variables and Macros

Custom variables, like system variables, are name-value pair tags that you can use when defining role mapping rules, resource policy rules and SSO parameter fields.

Custom variables are created in the Server Catalog (for example, Authentication > Auth Server > *Name* > Settings) by using a pre-defined macro on a system variable. Available macros are:

- REGMATCH – Matches a regular expression pattern against a string text.
- APPEND – Appends a text string to another text string.
- DAYSDIFF – Calculates the difference between two dates.



**NOTE:** These macros are located under Variable Operators in the Variables tab of the Server Catalog window.

A custom variable name is a dot-separated string. Each component can contain characters from the set [a-z A-Z 0-9 \_] but cannot start with a digit [0-9]. Custom variable names are case-insensitive.

Custom variables are referenced as **customVar.<variableName>**. For example, if you create a custom variable with the name **check-prefix**, you reference this custom variable as **customVar.check-prefix**.

### Using Macros in Custom Expressions

---

The macros listed above can also be used in custom expressions. For example, instead of creating a custom variable that is used only in a custom expression, simply embed the macro into the custom expression. Standard custom expression syntax applies.

For example, you can create the following regular expression using the APPEND macro:

```
{APPEND (userName, "@juniper.net") = "admin@juniper.net"}
```

## append

---

**Syntax** APPEND (attr, TextString)

APPEND (attr, attr2)

**Description** Append a text string to an attribute or append an attribute to another attribute and store the resulting string in the custom variable.

**Options** **attr**—System variable of type string.

**TextString**—Quoted ASCII string.

**attr2**—System variable of type string.

**Output Fields** Returns a String value. If no match is found, returns an empty string.

If the system variable is multi-valued, the custom variable is also multi-valued and uses the same order as the system variable.

### Sample Output

```
APPEND (userName, "@juniper.net")
```

In this example, the string "@juniper.net" is appended to the userName value.

## daysdiff

---

**Syntax** DAYSDIFF (attr, timeformat)

**Description** Calculates the number of days between the attribute and the current time.

**Options** **attr**—System variable of type string.

**timeformat**—Output time format. Valid values are: UTC, TIMET, MMDDYYYY

**Output Fields** Returns an Integer value.

### Sample Output

```
DAYSDIFF (certAttr.validUpto, UTC)
```

In this example, calculate the difference in days between the current time and the value of certAttr.validUpto and express the time in UTC (Coordinated Universal Time).

## regmatch

---

<b>Syntax</b>	REGMATCH (attr, regex, groupingNumber)
<b>Description</b>	Match the regular expression pattern against an attribute and store the result in the custom variable.
<b>Options</b>	<b>attr</b> —System variable of type string. <b>regex</b> —Quoted string containing the regular expression to be applied to the attr option. <b>groupingNumber</b> —The group value to assign to the custom variable.
<b>Additional Information</b>	The regular expression supports the Perl Compatible Regular Expressions (PCRE) syntax. A grouping (capture buffer) in the regex pattern can also be used to define a custom variable.
<b>Output Fields</b>	Returns a String value. If no match is found, returns an empty string.  If the system variable is multi-valued, the custom variable is also multi-valued and uses the same order as the system variable.

### Sample Output

```
REGMATCH (mailId, "^(.*)@juniper.net$", 1)
```

In this example, a mailId of myName@juniper.net creates a custom variable with value "myName".



PART 7

# Index

- [Index on page 1207](#)



# Index

## Symbols

128-bit encryption.....	824
6500, 4500.....	1109
UAC (802.1X)	
connection, Pulse Secure Access Service.....	46

## A

Access-Accept RADIUS attribute.....	199
Access-Challenge RADIUS attribute.....	199
Access-Reject RADIUS attribute.....	199
Access-Request RADIUS attribute.....	199
accounting server, <i>See</i> authentication server, RADIUS	
Accounting-Request RADIUS attribute.....	199
Accounting-Response RADIUS attribute.....	199
Acct-Authentic RADIUS attribute.....	197, 199
Acct-Delay-Time RADIUS attribute.....	199
Acct-Input-Gigawords RADIUS attribute.....	199
Acct-Input-Octets attribute.....	198
Acct-Input-Octets RADIUS attribute.....	199
Acct-Input-Packets RADIUS attribute.....	199
Acct-Interim-Interval RADIUS attribute.....	200
Acct-Link-Count RADIUS attribute.....	197, 200
Acct-Multi-Session-Id RADIUS attribute.....	197, 200
Acct-Output-Gigawords RADIUS attribute.....	200
Acct-Output-Octets attribute.....	198
Acct-Output-Octets RADIUS attribute.....	200
Acct-Output-Packets RADIUS attribute.....	200
Acct-Session-Id RADIUS attribute.....	197, 200
Acct-Session-Time RADIUS attribute.....	197, 200
Acct-Status-Type RADIUS attribute.....	197, 200
Acct-Terminate-Cause RADIUS attribute.....	197, 198, 200
Acct-Tunnel-Connection RADIUS attribute.....	200
Acct-Tunnel-Packets-Lost RADIUS attribute.....	200
ACE server.....	44
ACE/Server, <i>See</i> authentication server, ACE/Server	
Active Directory, <i>See</i> authentication server, Active Directory	
ActiveX	
Installation Delay.....	428

ActiveX rewriting	
creating resource policies.....	546
ActiveX, and Host Checker.....	376
adapter type.....	46
administrator	
realms.....	305, 1008
<i>See also</i> realms	
roles.....	1008
super administrator account, creating.....	1100
administrator access log.....	932
advanced endpoint defense.....	379
AES encryption, support.....	158
agentless	
sign-in notifications.....	327, 328
allow saving logon information	
Pulse Secure Access Service.....	44
allow user connections	
Pulse Secure Access Service.....	45
allow user to override connection policy	
connection option.....	47
connection option, App Acceleration.....	47
connection option, SRX.....	47
allowclipboard	
parameter.....	682
AND custom expression comparison	
operator.....	1181, 1182, 1185
antispypware.....	379
antispypware rule, Host Checker.....	387
antivirus, Host Checker rule.....	384
append.....	1200, 1202
ARAP-Challenge-Response RADIUS attribute.....	198
ARAP-Features RADIUS attribute.....	198
ARAP-Password RADIUS attribute.....	199
ARAP-Security RADIUS attribute.....	199
ARAP-Security-Data RADIUS attribute.....	199
ARAP-Zone-Access RADIUS attribute.....	199
archiving parameters, specifying.....	891
archiving, system.....	889
ARP	
command.....	1100
Ping Timeout, configuring.....	792
ARP cache, configuring.....	806
attributes	
configuring.....	309
authentication access policies	
configuring.....	307
authentication policies	
defined.....	305
authentication realms, <i>See</i> realms	

authentication server	
ACE/Server	
Agent configuration file.....	159
configuring.....	159
configuring for a cluster.....	161
overview.....	158
RADIUS protocol support.....	191
restrictions.....	158
SecurID authentication.....	207, 210
supported modes and features.....	158
Active Directory	
configuring.....	164
group lookup support.....	172
multi-domain configuration.....	169
overview.....	163
restrictions.....	164
supported server features.....	164
anonymous server	
configuring.....	157
certificate server	
defined.....	846
custom expressions variable.....	1187
defined.....	305
general	
configuration.....	155
overview.....	155
LDAP	
configuring.....	175, 176
configuring attributes.....	309
group lookup.....	176
overview.....	175
password management.....	179
referral chasing.....	178
restrictions.....	176
local authentication	
accounting.....	197
configuring.....	155, 184
creating users.....	186
managing user accounts.....	187
password management.....	184, 186
restrictions.....	185
mapping to realm.....	306
NIS server.....	190
RADIUS.....	190
accounting.....	193
ACE/Server protocol.....	158
CASQUE authentication.....	191
configuring.....	192
configuring attributes.....	309
multiple sessions.....	197
NAS.....	192
overview.....	191
PassGo Defender.....	191
password management.....	159, 192
role-mapping attributes.....	198
SSO.....	159, 192
start attributes.....	196, 197
stop attributes.....	196
supported server features.....	191
user experience.....	191
SiteMinder	
ACE SecurID authentication.....	210
agents.....	212, 222
authentication schemes.....	210, 213
automatic sign-in.....	207, 221, 227
certificate authentication.....	210
configuration (general).....	217
configuring the SiteMinder policy	
server.....	211
cookie domain.....	219
cookie provider domain.....	219
debugging.....	227
failover mode.....	219
overview.....	207
password management.....	213
policy domains.....	215
protected resources.....	215, 217, 219
protection levels.....	217
realms.....	215, 221
response.....	216
restrictions.....	209
role-mapping.....	227
rules.....	216
SMSESSION cookie.....	207
SSO.....	207, 209, 210, 221, 227
supported versions.....	209
user attributes.....	218
usernames, determining.....	210
authentication settings, for users.....	413
authMethod custom expression variable.....	1187
automatic upgrade UAC agent, enabling,	
disabling.....	811
automatic Pulse Client upgrades.....	811
<b>B</b>	
backup, configuration files.....	894

- base CRL
  - .....858
  - See also* CRL
  - defined.....858
  - See also* CRL
- bitmapcaching
  - parameter.....684
- bmname
  - parameter.....681
- bookmarks
  - custom expressions in.....1197
  - file
    - creating through resource profiles.....566
    - creating through roles.....568, 569, 576
    - restrictions.....566
- bound and unbound clients
  - software upgrades.....811
- browser
  - restrictions, configuring.....82
  - sign-in restrictions, user.....82
  - SiteMinder security settings.....221
- browsing
  - options
    - specifying file.....570, 577
  - options, specifying file.....570, 577
- C**
- cacheCleanerStatus custom expression
  - variable.....1187
- caching
  - Lotus iNotes files.....535
  - OWA files.....535
- Callback-Id RADIUS attribute.....200
- Callback-Number RADIUS attribute.....200
- Called-Station-Id RADIUS attribute.....201
- Calling-Station-Id RADIUS attribute.....201
- canonical format
  - file configuration.....571
- capacity, log.....932
- capacity, system.....950
- CASQUE authentication support, *See*
  - authentication server, RADIUS
- CDP, *See* CRL distribution point
- certAttr.altName.Alt-attr custom expression
  - variable.....1188
- certAttr.cert-attr custom expression variable.....1187
- certAttr.serialNumber custom expression
  - variable.....1188
- certDN custom expression variable.....1188
- certDN.subject-attr custom expression
  - variable.....1189
- certDNText custom expression variable.....1189
- certificate
  - attributes, configuring.....309
  - CA certificate
    - enabling CRL checking.....861
    - uploading to the Secure Access
      - Service.....846
    - verifying.....861
  - client-side certificate
    - defined.....838
    - SiteMinder.....210
  - CRLs, enabling.....861
  - custom expression variables.....1187
  - device certificate
    - creating CSR.....842
    - defined.....838
    - importing CSR.....843
    - importing existing.....840, 844
    - multiple certificates, enabling.....839
  - hierarchy
    - defined.....846
    - discussed.....844
  - intermediate certificate, defined.....846
  - key
    - import existing.....840
    - importing existing.....844
  - machine certificate
    - checking using Host Checker.....394
    - overview.....846
  - revocation list
    - defined.....846
    - discussed.....858
  - revocation, defined.....846
  - selection.....44
  - self-signed.....839
  - server certificate, defined.....838
  - signing request
    - creating.....842
    - importing.....843
    - importing certificate from.....843
    - SiteMinder security settings.....221
    - supported formats.....839, 846
    - wildcard certificate, defined.....846
- certificate restrictions, specifying for a realm or
  - role.....84
- certificate revocation list, *See* certificate,
  - revocation list

certIssuerDN custom expression variable.....	1189	component set options	
certIssuerDN.issuer-attr custom expression		server.....	55
variable.....	1189	component sets, configuring for Junos Pulse.....	56
certIssuerDNText custom expression		concurrent sessions, limiting the number of.....	86
variable.....	1189	concurrent users, SiteMinder security settings.....	221
chained certificate, <i>See</i> certificate, intermediate		configuration files, exporting and importing.....	896
certificate		Configuration-Token RADIUS attribute.....	201
challenge-response protocols disabled, LDAP.....	176	Connect-Info RADIUS attribute.....	201
changing cluster node IP address.....	995	connectComPorts	
CHAP-Challenge RADIUS attribute.....	200	parameter.....	682
CHAP-Password RADIUS attribute.....	200	connectDrives	
Citrix		parameter.....	682
WSAM support.....	587, 590	connection option	
Class RADIUS attribute.....	201	allow user to override connection policy, App	
clear text.....	1176	Acceleration.....	47
client upload log.....	932	allow user to override connection policy,	
clientPort		firewall.....	47
parameter.....	680	connection rules	
cluster		configuring.....	53
ACE/Server support.....	158	connection set options	
active/active.....	987	adapter type.....	46
deployment overview.....	987	allow saving logon information.....	44
active/passive.....	985	allow user connections.....	45
deploying overview.....	985	allow user to override connection policy.....	47
configuring.....	983	community string.....	47
initializing.....	977, 981	display splash screen.....	45
joining.....	983	dynamic certificate trust.....	45
logging.....	988, 989	dynamic connections.....	45
managing.....	983	FIPS mode.....	45
modifying properties.....	990, 993	hiding or displaying.....	45
password.....	988	non-broadcast.....	46
restart, reboot, shut down.....	807	outer username.....	46
state synchronization.....	988	Pulse Secure Access Service.....	44, 45, 46
status defined.....	997	scan list.....	46
synchronization.....	977, 988	server certificate DN.....	46
system data.....	807	wireless suppression.....	45
cluster nodes, restarting.....	996	connection set, configuring for Junos Pulse.....	51
cluster, deleting.....	996	connectivity, testing.....	807
cluster, status.....	997	connectPrinters	
clustering, admin console.....	997	parameter.....	682
clustering, configuring with serial console.....	1002	console, serial, <i>See</i> serial console	
clusters, monitoring.....	999	cookies	
clusters, troubleshooting.....	1000	blocking.....	543
colorDepth		cookies, deleting at session termination.....	824
parameter.....	681	cooling fans, replacing.....	1113
command line launcher		credential provider	
examples.....	67	Secure Access Service.....	746
community string.....	47		

- CRL distribution point
  - discussed.....858
  - downloading CRLs from .....861
- CRL, *See* certificate, revocation list
- CSR
  - creating.....842
  - importing.....843
  - importing certificate from.....843
- CSS
  - rewriting.....541
- custom expressions
  - comparison operators
    - AND.....1181, 1185
    - defined.....1183
    - NOT.....1181, 1185
    - OR.....1181, 1184, 1185
    - TO.....1181
  - DN variables and functions.....1186
  - formats.....1181
  - functions
    - isEmpty.....1181, 1185
    - isUnknown.....1181, 1185
    - matchDNSuffix.....1186
  - licensing.....1181
  - overview.....1181
  - using
    - general.....309
    - in LDAP configurations.....1187
    - in log filters.....1182
    - in role mapping rules.....1187
    - in Windows bookmarks.....1197
  - values, defined.....1184
  - variables
    - authMethod.....1187
    - cacheCleanerStatus.....1187
    - certAttr.altName.Alt-attr.....1188
    - certAttr.cert-attr.....1187
    - certAttr.serialNumber.....1188
    - certDN.....1186, 1188
    - certDN.subject-attr.....1189
    - certDNText.....1189
    - certIssuerDN.....1186, 1189
    - certIssuerDN.issuer-attr.....1189
    - certIssuerDNText.....1189
    - defaultNTDomain.....1189
    - group.group-name.....1190
    - groups.....1190
    - hostCheckerPolicy.....1190
    - loginHost.....1190
    - loginTime.....1190
    - loginTime.day.....1191
    - loginTime.dayOfWeek.....1191
    - loginTime.dayOfYear.....1191
    - loginTime.month.....1191
    - loginTime.year.....1191
    - loginURL.....1191
    - networklf.....1192
    - ntdomain.....1192
    - ntuser.....1192
    - overview.....1182
    - password.....1192
    - quoting syntax.....1182
    - realm.....1192
    - role.....1192
    - sourceIP.....1193
    - time.....1184, 1193
    - time.day.....1193
    - time.dayOfWeek.....1193
    - time.dayOfYear.....1193
    - time.month.....1194
    - time.year.....1194
    - user.....1194
    - userAgent.....1195
    - userAttr.auth-attr.....1196
    - userDN.....1186, 1196
    - userDN.user-attr.....1197
    - userDNText.....1197
    - username.....1195
    - wildcard matching.....1185
  - custom expressions: using
    - using
      - in UI options & custom text.....1197
  - custom filter log files.....933
  - custom variables.....1200
    - macros.....1200
  - customer support.....xxxviii
    - contacting JTAC.....xxxviii
  - customizable UI
    - admin console, resource policy settings.....559
  - customized realm UI views.....318
- D**
  - date and time.....954
  - daysdiff.....1200, 1203
  - defaultNTDomain custom expression
    - variables.....1189
  - defaults, Pulse configuration.....39

Defender support, <i>See</i> authentication server, RADIUS	
deleting a cluster.....	996
deleting user sessions.....	934
deployment options	
overview.....	39
desktopbackground	
parameter.....	683
desktopcomposition	
parameter.....	684
digital certificate.....	838
defined.....	838
<i>See also</i> certificate	
disaster recovery license.....	822
DLL requirements, Host Checker <i>See</i> Host Checker, server integration interface <i>See</i> Host Checker, client interface	
DMI communication.....	27
DMI connection, configuring (NSM).....	28
DMZ, interface.....	791
DNS	
name resolution, configuring.....	790
doc files	
caching.....	536
documentation	
comments on.....	xxxviii
domain custom expression variables.....	1189, 1192
domain name, stripping.....	176
DTD	
rewriting.....	541
dynamic certificate trust	
Pulse Secure Access Service.....	45
dynamic connections.....	39
Pulse Secure Access Service.....	45
dynamic log filters.....	933
dynamic policy evaluation.....	77
<b>E</b>	
EAP-Message RADIUS attribute.....	201
EES (Enhanced Endpoint Security).....	379
eligible roles, defined.....	308
emergency mode.....	822
activating.....	818
deactivating.....	818
Enable Mobile Security Check checkbox.....	431
encryption	
custom SSL ciphers.....	824
strength.....	824
encryption strength option.....	824
endpoint localization.....	811
Endpoint Security Assessment Plug-In, upgrading.....	419
Enhanced Endpoint Security (EES).....	379
eTrust, <i>See</i> authentication server, SiteMinder	
events log.....	932
exporting configuration files.....	897
external user records management.....	813
<b>F</b>	
failover, VIP.....	986
federation, troubleshooting.....	101
field-replaceable hardware.....	1110
file	
check, configuring.....	394
file rewriting	
autopolicies	
access control.....	564
SSO.....	565
general options	
UNIX/NFS.....	581
Windows.....	575
resource policies	
defining resources.....	562
UNIX/NFS.....	578, 579
file system auto-clean.....	811
Filter-Id RADIUS attribute.....	201
FIPS	
limitations for SAML.....	241
FIPS device, clustering.....	1134
FIPS overview.....	1131
FIPS, custom cipher selection.....	824
FIPS, device certificate.....	1135
firewall rule, Host Checker.....	386
Flash	
rewriting.....	541
fontsmoothing	
parameter.....	684
Forget Saved Settings.....	44
Framed-AppleTalk-Link RADIUS attribute.....	201
Framed-AppleTalk-Network RADIUS attribute.....	201
Framed-AppleTalk-Zone RADIUS attribute.....	201
Framed-Compression RADIUS attribute.....	201
Framed-IP-Address RADIUS attribute.....	196, 201
Framed-IP-Netmask RADIUS attribute.....	201
Framed-IPX-Network RADIUS attribute.....	201
Framed-MTU RADIUS attribute.....	201
Framed-Pool RADIUS attribute.....	201



- Framed-Protocol RADIUS attribute.....201
- Framed-Route RADIUS attribute.....202
- Framed-Routing RADIUS attribute.....202
- G**
- gateway
  - configuring.....792
- graphs, configuring.....952
- graphs, system display.....952
- group membership
  - custom expression variables.....1190
  - LDAP.....309
- group.groupname custom expression
  - variable.....1190
- groups custom expression variable.....1190
- H**
- handheld devices
  - WSAM support.....591
- hard drive, replacing.....1114
- hard token.....44
- hardware requirements.....40
- hardware token, using to sign in.....158
- hardware, about.....1109
- health check URL.....987
- host
  - parameter.....680
- Host Checker
  - custom expression variables.....1190
  - execution.....413
  - for iOS clients, configuring.....433
  - for iOS clients, enabling.....435
  - for iOS clients, overview.....432
  - frequency check.....425
  - installer
    - directory.....413
    - enabling.....414
  - logging, disabling.....430
  - machine certificate
    - .....846
    - See also* certificate, machine certificate
    - configuring.....394
    - overview.....846
    - See also* certificate, machine certificate
  - overview.....374
  - remediation
    - overview.....416
  - SiteMinder security settings.....221
  - specifying restrictions
    - realm level.....412, 414
    - role level.....412, 414
    - uninstalling.....413
  - Host Checker patch assessment policies.....390, 401
  - Host Checker remediation, user experience.....417
  - Host Checker variables.....399
  - Host Checker, configuration task summary.....376
  - Host Checker, implementing.....412
  - Host Checker, installing manually.....429
  - hostCheckerPolicy custom expression
    - variable.....1190
  - hostname
    - configuring.....790
    - defining in resource policies.....562, 571, 578
    - resolving.....807
  - HSM card, resetting (FIPS device).....1137
  - HSM firmware, upgrading (FIPS device).....1137
  - HTC
    - rewriting.....541
  - HTML
    - rewriting.....541
  - html files
    - caching.....536
  - HTTP
    - protocol resource policies.....555
- I**
- Idle-Timeout RADIUS attribute.....202
- IDP configuration.....1081
- IDP deployment examples.....1082
- IDP interaction.....1084
- IDP licensing.....1082
- IDP sensor policies.....1084
- IDP, automatic response.....1086
- IDP, interoperability.....1083
- IDP, quarantining users manually.....1088
- IDP, using with UAC.....1081
- images
  - caching.....536
- IMCs and IMVs, overview.....375
- importing configuration files.....898
- IMV, third-party Host Checker policy.....405
- initializing keystore (FIPS device).....1133
- installation
  - requirements.....40
- installers
  - preconfigured.....59, 63
- installers, downloading.....813

integrity measurement collectors (IMCs) and verifiers (IMVs).....	375
interaction: clients, servers, and endpoints in an IF-MAP federated network.....	93
intermediate certificate, <i>See</i> certificate, intermediate certificate	
internal port, configuring.....	791
IP address	
configuring.....	792
defining in resource policies.....	562, 571, 578
resolving.....	807
restrictions.....	79, 82, 414
SiteMinder security settings.....	221
specifying user requirements.....	79
IP address. cluster.....	995
IP alias	
activating, <i>See</i> virtual port	
defined.....	802
isEmpty custom expression function.....	1182, 1185
isUnknown custom expression function.....	1182, 1185
<b>J</b>	
jail breaking detection	
for iOS clients.....	432
java applets	
enabling.....	537
Java applets	
signed	
configuration.....	538
java instrumentation caching.....	811
Javascript	
rewriting.....	541
join domain.....	170
JSAM	
overview.....	602
using custom expressions in hostnames.....	1197
Juniper Installer Service, described.....	813
Junos Pulse	
sign-in notifications.....	327, 328
Junos Pulse and security certificates.....	38
Junos Pulse Collaboration Suite	
defining a server.....	718
server SSO.....	719
session migration.....	719
session sharing.....	719
Junos Pulse Collaboration Suite,	
enabling.....	47
Junos Pulse connections, configuring.....	51
Junos Pulse installer, creating.....	59, 63
Junos Pulse, configuring as a role option.....	42
Junos Pulse, configuring components.....	56
Junos Pulse, location awareness overview.....	38
Junos Pulse, platform support.....	40
Junos Pulse, user experience.....	39
JVM	
certificate requirements.....	538
<b>K</b>	
Kaspersky	
and application acceleration.....	47
Keep-Alives RADIUS attribute.....	202
kernel watchdog.....	811
key	
private, <i>See</i> private key	
keystore, importing and exporting (FIPS device).....	1138
keystore, initializing (FIPS device).....	1133
<b>L</b>	
L7 Health Check URL.....	987
LAN, modifying network settings.....	791
LDAP	
mapping Windows bookmarks to.....	570
LDAP server catalog.....	314
LDAP server, <i>See</i> authentication server, LDAP	
learned user settings.....	44
led, device status.....	1111
led, ethernet.....	1112
LEDs (FIPS device).....	1138
licenses	
entering license.....	818
overview.....	815
subscription-based.....	821
licensing, IDP.....	1082
limiting user sessions.....	88
link speed, configuring.....	792
load balancer, using with active/active cluster.....	987
localized	
sign-in notifications.....	328
location awareness	
and push config.....	925
configuring.....	53, 54
location awareness rules.....	49
location awareness, with Junos Pulse.....	38
lockout options.....	826
log capacity.....	932
log file severity.....	933
log filters.....	937

- log filters, dynamic.....933
  - log monitoring, configuring.....935
  - logging
    - client logs
      - disabling.....430
      - clusters.....988, 989
  - logging, monitoring overview.....931
  - login notifications
    - agentless.....327, 328
    - Junos Pulse.....327, 328
  - Login-IP-Host RADIUS attribute.....202
  - Login-LAT-Group RADIUS attribute.....202
  - Login-LAT-Node RADIUS attribute.....202
  - Login-LAT-Port RADIUS attribute.....202
  - Login-LAT-Service RADIUS attribute.....202
  - Login-Service RADIUS attribute.....202
  - Login-TCP-Port RADIUS attribute.....202
  - loginHost custom expression variable.....1190
  - loginTime custom expression variable.....1190
  - loginTime.day custom expression variable.....1191
  - loginTime.dayOfWeek custom expression variable.....1191
  - loginTime.dayOfYear custom expression variable.....1191
  - loginTime.month custom expression variable.....1191
  - loginTime.year custom expression variable.....1191
  - loginURL custom expression variable.....1191
  - loopback addresses, JSAM.....607
  - Lotus Notes
    - WSAM support.....587, 590
- M**
- MAC address, configuring requirement in Host
    - Checker policy.....394
  - machine authentication
    - certificate authentication.....311
    - configuration summary.....311
    - realm and role preferences.....312
  - machine-only
    - authentication.....312
  - Macintosh
    - support
      - JSAM.....606
  - macro
    - append.....1200, 1202
    - daysdiff.....1200, 1203
    - regmatch.....1200, 1204
  - maintenance tasks, delegating.....1007
  - malware, Host Checker policy.....379
  - manuals
    - comments on.....xxxviii
  - maximum transmission unit, configuring.....792
  - MDM.....434
  - Microsoft Outlook
    - WSAM support.....587
  - Microsoft Outlook/Exchange
    - WSAM support.....590
  - Microsoft OWA
    - caching OWA files.....553
  - Mobile Device Management.....434
  - Mobile Security detection
    - for iOS clients.....432
  - monitoring users.....955
  - monitoring, logging overview.....931
  - MS-Acct-Auth-Type RADIUS attribute.....202
  - MS-Acct-EAP-Type RADIUS attribute.....202
  - MS-ARAP-Challenge RADIUS attribute.....202
  - MS-ARAP-Password-Change-Reason RADIUS attribute.....202
  - MS-BAP-Usage RADIUS attribute.....202
  - MS-CHAP-Challenge RADIUS attribute.....203
  - MS-CHAP-CPW-1 RADIUS attribute.....202
  - MS-CHAP-CPW-2 RADIUS attribute.....203
  - MS-CHAP-Domain RADIUS attribute.....203
  - MS-CHAP-Error RADIUS attribute.....203
  - MS-CHAP-LM-Enc-PW RADIUS attribute.....203
  - MS-CHAP-MPPE-Keys RADIUS attribute.....203
  - MS-CHAP-NT-Enc-PW RADIUS attribute.....203
  - MS-CHAP-Response RADIUS attribute.....203
  - MS-CHAP2-CPW RADIUS attribute.....203
  - MS-CHAP2-Response RADIUS attribute.....203
  - MS-CHAP2-Success RADIUS attribute.....203
  - MS-Filter RADIUS attribute.....203
  - MS-Link-Drop-Time-Limit RADIUS attribute.....203
  - MS-Link-Utilization-Threshold RADIUS attribute.....203
  - MS-MPPE-Encryption-Policy RADIUS attribute.....203
  - MS-MPPE-Encryption-Types RADIUS attribute.....203
  - MS-MPPE-Recv-Key RADIUS attribute.....203
  - MS-MPPE-Send-Key RADIUS attribute.....204
  - MS-New-ARAP-Password RADIUS attribute.....204
  - MS-Old-ARAP-Password RADIUS attribute.....204
  - MS-Primary-DNS-Server RADIUS attribute.....204
  - MS-Primary-NBNS-Server RADIUS attribute.....204
  - MS-RAS-Vendor RADIUS attribute.....204
  - MS-RAS-Version RADIUS attribute.....204

MS-Secondary-DNS-Server RADIUS attribute.....	204
MS-Secondary-NBNS-Server RADIUS attribute.....	204
MTU, configuring.....	792

## N

NAS, <i>See</i> authentication server, RADIUS, NAS	
NAS-Identifier RADIUS attribute.....	196, 204
NAS-IP-Address RADIUS attribute.....	196, 204
NAS-Port RADIUS attribute.....	196, 204
NAS-Port-Id RADIUS attribute.....	204
NAS-Port-Type RADIUS attribute.....	204
NetBIOS file browsing	
WSAM support.....	587
NetBIOS, configuring requirement in Host Checker policy.....	394
netmask	
configuring.....	792
defining user requirements.....	79
Network Access Server, <i>See</i> authentication server, RADIUS, NAS	
network settings	
configuring.....	791, 1100
networkIf custom expression variable.....	1192
networkIf custom expression variables.....	1192
New PIN mode support.....	158
Next Token mode support.....	158
NIS authentication server, <i>See</i> authentication server, NIS	
nodes, cluster.....	983
NOT custom expression comparison	
operator.....	1182, 1185
NSM, using with Secure Access Service.....	25
NT Domain, <i>See</i> authentication server, Active Directory	
ntdomain custom expression variable.....	1192
ntuser custom expression variable.....	1192

## O

OCSP, enabling.....	863
Online Certification Status Protocol.....	863
Optical Responder tokens, <i>See</i> authentication server, RADIUS, CASQUE	
OR custom expression comparison	
operator.....	1181, 1182, 1184, 1185
OS detection	
for iOS clients.....	432

outer username	
802.1X connection, Pulse Secure Access Service.....	46

## P

PassGo Defender support, <i>See</i> authentication server, RADIUS	
password	
custom expression variable.....	1192
management	
LDAP.....	179
local authentication server.....	184, 186
RADIUS.....	159, 192
SiteMinder.....	213
parameter.....	681
SiteMinder security settings.....	221
password restrictions, specifying for a realm or role.....	85
password stored as clear text.....	1176
Password-Retry RADIUS attribute.....	204
passwords	
one-time.....	44
patch assessment rule, configuring.....	403
patch assessment version monitoring.....	388
patch assessment, in Host Checker	
policy.....	390, 401
path	
defining in resource policies.....	562, 571, 578
pdf files	
caching.....	536
persistent data, defined.....	988
ping command.....	1100
PKI, defined.....	838
platform, upgrading.....	810
port	
.....	845
<i>See also</i> virtual port	
external.....	791
internal.....	791
modifying.....	791
requirements, configuring.....	394
<i>See also</i> virtual port	
port 3578	
and application acceleration.....	47
Port-Limit RADIUS attribute.....	204
post-authentication sign-in notifications, configuring.....	328
power supply, replacing.....	1116

- ppt files
    - caching.....536
  - pre-authentication sign-in notifications,
    - configuring.....328
  - preconfigured installer.....39, 59, 63
  - predefined Host Checker policies.....383
  - process check, configuring.....394
  - Prompt RADIUS attribute.....205
  - protecting against malware, spyware.....379
  - proxy server, Host Checker updates.....389
  - Proxy-State RADIUS attribute.....205
  - public key infrastructure, defined.....838
  - Pulse Collaboration Suite,
    - enabling.....47
  - Pulse Launcher
    - examples.....67
  - command line launcher
    - examples.....67
  - push config
    - and location awareness.....925
  - push configuration.....924
- R**
- RADIUS server.....44
  - RADIUS, *See* authentication server, RADIUS
  - realm
    - administrator.....1008
    - custom expression variable.....1192
    - managing.....1008
    - mapping to sign-in policy.....324
  - reason strings, for IMV/IMC remediation
    - reason strings.....416
  - rebooting the Secure Access Service device.....807
  - redundancy, Active/Passive mode.....985
  - referral chasing support.....178
  - registry setting checks, configuring.....394
  - regmatch.....1200, 1204
  - remediation
    - overview.....416
  - remediation, antivirus Host Checker rule.....384
  - remediation, Host Checker firewall rule.....386
  - remediation, user experience.....417
  - Remote Authentication Dial-In User Service, *See*
    - authentication server, RADIUS
  - remote IMV server, configuring.....406
  - Reply-Message RADIUS attribute.....205
  - resource policies
    - file
      - compression.....580
      - Windows.....570
      - Windows access control.....572
      - Windows compression.....574
      - Windows SSO.....573
    - Web
      - general options.....558
      - Java code signing.....538
      - passthrough proxy.....542
  - resource profiles
    - autopolicies
      - file access control.....563
      - file.....563
  - restarting the Secure Access Service device.....807
  - restarts.....916
  - restoring, system data.....889
  - restting HSM card (FIPS device).....1137
  - role
    - administrator.....1008
    - custom expression variable.....1192
    - mapping.....305, 308, 309
    - sign-in restrictions
      - by Host Checker policy.....413
  - role mapping.....308
  - Routes tab.....805
  - RSA
    - RADIUS support, *See* authentication server,
      - RADIUS
  - rule, configuring for role mapping.....309
- S**
- SA 4500/6500 FIPS overview.....1131
  - scan list
    - 802.1X connection, Pulse Secure Access
      - Service.....46
    - schema file, downloading.....908
    - SCP, system snapshot.....1100
  - screenSize
    - parameter.....681
  - scripts
    - Pulse Secure Access Service.....757
  - Secure Meeting.....47
  - SecurID tokens, *See* authentication server,
    - ACE/Server, SecurID
  - security administrator.....1008
  - security certificates, with Junos Pulse.....38

security officer password, changing (FIPS device).....	1135
security officer, name and password restrictions (FIPS device).....	1132
security options, configuring.....	823
selective rewriting	
overview.....	540
sensor policies for IDP, configuring.....	1084
sensors log.....	932
serial console, using for system tasks.....	1097
serial console, using to configure cluster properties.....	1002
server	
catalog, configuring.....	314
defining in resource policies.....	562, 571, 578
server certificate DN	
802.1X connection, Pulse Secure Access Service.....	46
serverPort	
parameter.....	680
service package	
installing.....	810, 828
installing in a cluster.....	993
service package, downloading.....	953
Service-Type RADIUS attribute.....	205
session scripts	
Pulse Secure Access Service.....	757
session-export policies, advanced	
configuration.....	100
session-export policies, configuring.....	98
Session-Timeout RADIUS attribute.....	205
sessions, deleting.....	934
sessions, federation client.....	101
severity, log files.....	933
share	
defining in resource policies.....	562, 571
showDragContents	
parameter.....	683
showMenuAnimation	
parameter.....	683
shutting down the Secure Access Service	
device.....	807
sign-in	
management tasks, delegating.....	1007
options, user restrictions.....	82, 413
pages	
mapping to sign-in policies.....	324
policies	
changing order.....	326
configuring.....	324
evaluating.....	326
sign-in notifications	
agentless.....	327, 328
Junos Pulse.....	327, 328
localized.....	328
sign-in policies, configuring.....	324
Silverlight.....	492
SiteMinder, <i>See</i> authentication server, SiteMinder	
smart card authentication.....	44
SMS (System Management Server).....	392, 402
SMSESSION cookie, <i>See</i> authentication server, SiteMinder	
snapshots, creating.....	1100
snmp agent.....	939
snmp, using to monitor cluster.....	999
soft token.....	44
SoftID tokens, <i>See</i> authentication server, ACE/Server	
software	
installing.....	828
installing in a cluster.....	993
token, using to sign in.....	158
software requirements.....	40
soundoptions	
parameter.....	684
sourceIP custom expression variable.....	1193
SSL	
encryption strength allowed.....	824
version allowed.....	824
SSL ciphers, selecting.....	824
SSL Legacy Renegotiation Support option.....	825
IVS.....	825
startApp	
parameter.....	681
startDir	
parameter.....	681
State RADIUS attribute.....	205
state synchronization.....	988
static routes.....	805
statistics, viewing.....	947
Steelbelted-RADIUS support, <i>See</i> authentication server, RADIUS	
super administrator account, creating.....	1100
support, technical <i>See</i> technical support	

- system
  - administrator.....1008
  - configuration.....807
  - data.....807
  - management tasks, delegating.....1007
  - software, installing.....828
  - state data described.....988
- system archiving.....889
- system management server (SMS) with Host
  - Checker policy.....392, 402
- system restarts.....916
- system status, viewing.....950
  
- T**
- tabs, Routes.....805
- technical support
  - contacting JTAC.....xxxviii
- Telephone-number RADIUS attribute.....205
- Telnet/SSH
  - bookmarks
    - custom expressions in.....1197
- Terminal Services
  - bookmarks
    - custom expressions in.....1197
- Termination-Action RADIUS attribute.....205
- themes
  - parameter.....683
- third-party IMVs, configuring.....405
- time custom expression variable.....1193
- time.day custom expression variable.....1193
- time.dayOfWeek custom expression variable.....1193
- time.dayOfYear custom expression variable.....1193
- time.month custom expression variable.....1194
- time.year custom expression variable.....1194
- TLS, version allowed.....824
- TO custom expression comparison operators.....1181
- token authentication.....44
- token, using to sign in.....158
- traceroute command.....1100
- transient data, defined.....988
- troubleshooting
  - application acceleration.....47
- troubleshooting, IF-MAP federation.....101
- trusted CA certificate, *See* certificate, trusted CA certificate
- Trusted Computing Group (TCG).....374
- Trusted Network Connect (TNC).....374
- Tunnel-Assignment-ID RADIUS attribute.....205
- Tunnel-Client-Auth-ID RADIUS attribute.....205
- Tunnel-Client-Endpoint RADIUS attribute.....205
- Tunnel-Link-Reject RADIUS attribute.....205
- Tunnel-Link-Start RADIUS attribute.....205
- Tunnel-Link-Stop RADIUS attribute.....205
- Tunnel-Medium-Type RADIUS attribute.....205, 206
- Tunnel-Password RADIUS attribute.....206
- Tunnel-Preference RADIUS attribute.....206
- Tunnel-Private-Group-ID RADIUS attribute.....206
- Tunnel-Reject RADIUS attribute.....206
- Tunnel-Server-Auth-ID RADIUS attribute.....206
- Tunnel-Server-Endpoint RADIUS attribute.....206
- Tunnel-Start RADIUS attribute.....206
- Tunnel-Stop RADIUS attribute.....206
- Tunnel-Type RADIUS attribute.....206
- txt files
  - caching.....536
- type
  - parameter.....680
  
- U**
- UDP port 3578
  - and application acceleration.....47
- UI views, customizing.....318
- UNIX, authentication server, *See* authentication server, NIS
- upgrading
  - Endpoint Security Assessment Plug-In.....419
  - service package.....810
- URLs sign-in URLs, defining.....324
- user
  - accounts
    - creating.....186
    - attributes, configuring.....309
    - creating.....186
    - custom expression variable.....1194
    - managing accounts.....187
    - parameter.....681
    - session data.....988
    - sign-in restrictions
      - by browser.....82
  - user access log.....932
  - user roles, configuring for Junos Pulse.....42
  - user sessions, deleting.....934
  - user-after-desktop
    - authentication.....312
  - User-Name RADIUS attribute.....196, 206
  - User-Password RADIUS attribute.....206
  - userAgent custom expression variable.....1195



userAttr.auth-attr custom expression variable.....	1196	configuration overview.....	584
userDN custom expression variable.....	1196	debugging.....	586
userDN.user-attr custom expression variable.....	1197	IP/hostname matching.....	596
userDNText custom expression variable.....	1197	resource policies	
username		general options.....	596
custom expression variable.....	1195	specifying servers.....	594
users, monitoring.....	955	resource profiles	
<b>V</b>		autopolicies.....	588
valid roles, defined.....	308	client application profiles.....	587
variables, in Host Checker rules.....	399	destination network profiles.....	588
VBScript		overview.....	586
rewriting.....	541	role settings	
version monitoring.....	811	configuring applications.....	589
version monitoring virus signatures and		general options.....	593
firewall.....	388	scripts	
VIP, failing over.....	986	running.....	598, 599
virtual		using custom expressions in hostnames.....	1197
hostname		App Acceleration connection option	
configuring.....	790	community string.....	47
port		<b>X</b>	
associating with a certificate.....	846	xls files	
defined.....	845	caching.....	536
enabling.....	802	XML	
virtual hostname		rewriting.....	541, 543
configuring.....	542	xml files, using.....	907
virus signature version monitoring.....	388	xml import, export.....	910
virus signatures		xml operation attributes.....	922
checking age.....	394	xml schema file.....	908
VLANs, using with Secure Access Service.....	799	xml use case.....	918
VPN Tunneling		xml, creating.....	903
using with WSAM.....	585	xml, importing and exporting configuration	
<b>W</b>		files.....	901
web user password, changing (FIPS device).....	1136	xml, working with.....	909
wildcard certificate, defined.....	846	XMLHttpRequest object.....	557
Windows Internet Naming Service server,		XSLT	
configuring.....	790	rewriting.....	541
Windows NT authentication, <i>See</i> authentication		<b>Z</b>	
server, Active Directory		zip files	
WINS		caching.....	536
for external port.....	791		
server, configuring.....	790		
wireless suppression			
Pulse Secure Access Service.....	45		
WSAM			
auto-allow application servers.....	593		
auto-launch.....	593		