



Junos[®] Pulse

Administration Guide

Release

4.0



Published: 2013-02-08

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
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 Administration Guide
Copyright © 2013, Juniper Networks, Inc.
All rights reserved.

Revision History
2010-06-09—Release 1.0
2010-07-01—Release 1.0 - updated for iOS device support
2011-01-31—Release 2.0
2011-06-01—Release 2.1
2012-03-19—Release 3.0
2012-06-15—Release 3.0 - updated for Pulse for Android R4.0 support
2012-10-05—Release 3.1
2013-02-04—Release 4.0

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.

Table of Contents

	About This Guide	xi
	Objectives	xi
	Audience	xi
	Document Conventions	xi
	Related Documentation	xi
	Obtaining Documentation	xii
	Documentation Feedback	xii
	Requesting Technical Support	xii
	Self-Help Online Tools and Resources	xiii
	Opening a Case with JTAC	xiii
Part 1	Junos Pulse	
Chapter 1	Junos Pulse Overview	3
	Introducing Junos Pulse	3
	The Junos Pulse Client for Windows	4
	The Pulse Client for Mac OS X	4
	User Experience	6
	Location Awareness	6
	Session Migration	6
	Centralized Control	6
	Security Certificates	7
	Compliance and Remediation	8
	Two-factor Authentication	9
	Junos Pulse Collaboration Suite Integration	9
	Bound and Unbound Clients	9
	Sign-in Notifications	10
	Automatic Software Updates	10
	Installation Requirements	10
	Junos Pulse Client Error Messages Overview	11
	Accessing Junos Pulse Client Error Messages on Mac OS X Endpoints	11
	Junos Pulse Client Log Files	12
	Deleting the Junos Pulse Client Log Files	15
	Migrating From Odyssey Access Client to Junos Pulse Client	15
	Wireless Connectivity, OAC, and Junos Pulse	15
	Migrating From Network Connect to Junos Pulse	16
	Predictable Pulse Server Host Name Resolution with IPv6	16
Chapter 2	Configuring Junos Pulse Access Control Service	17
	Before You Begin	18
	Junos Pulse Access Control Service Overview	18

	Pulse Access Control Service and Pulse Secure Access Service Deployment Options	19
	Application Acceleration Deployment Options	20
	SRX Series Gateway Deployment Options	21
	Configuring a Role for Junos Pulse Access Control Service	21
	Client Connection Set Options for Junos Pulse Access Control Service	24
	Machine Connection Preferences	29
	User Connection Preferences	30
	Creating a Client Connection Set for Junos Pulse Access Control Service	30
	Securing the Connection State on the Junos Pulse Client	33
	Machine Authentication for Pulse Access Control Service Overview	33
	Configuring machine-only Machine Authentication for a Junos Pulse Connection	34
	Configuring user-after-desktop Machine Authentication for a Junos Pulse Connection	35
	Preferred Realm and Role for Junos Pulse Machine Authentication	36
	Remote Desktop Protocol Compatibility with Junos Pulse 802.1X Machine Authentication Connection	38
	Credential Provider Authentication for Pulse Access Control Service Overview	38
	Configuring user-at-credprov Credential Provider Authentication for a Junos Pulse Connection	40
	Configuring machine-then-user-at-credprov Credential Provider Authentication for a Junos Pulse Connection	41
	Machine and User Authentication Through a Pulse Connection for Pulse Access Control Service	43
	Configuring Location Awareness Rules for Junos Pulse	44
	Junos Pulse Access Control Service Component Set Options	46
	Creating a Client Component Set for Junos Pulse Access Control Service	48
	Endpoint Security Monitoring and Management for Pulse Access Control Service	49
	Remediation Options	50
	Issuing a Remediation Message with Junos Pulse Access Control Service	53
	Using SMS/SCCM Remediation with Junos Pulse Access Control Service	54
	Configuring Shavlik Remediation with Pulse Access Control Service	55
	Enabling Enhanced Endpoint Security for Junos Pulse Access Control Service	57
	Pushing Junos Pulse Configurations Between Junos Pulse Servers of the Same Type	59
	Enabling or Disabling Automatic Upgrades of the Junos Pulse Client	60
	Upgrading Junos Pulse Client Software	61
Chapter 3	Configuring Junos Pulse Secure Access Service	63
	Before You Begin Configuring Junos Pulse Secure Access Service	64
	Junos Pulse Secure Access Service Overview	64
	Junos Pulse and IVS	66
	About Sign-In Notifications	66
	Configuring and Implementing Sign-in Notifications	67

Configuring a Role for Junos Pulse Secure Access Service	69
Configuring General Role Options for Pulse Secure Access Service	70
Configuring Role Options for Pulse Secure Access Service	72
Configuring Role Options for Host Checker for Pulse Secure Access Service	74
Machine Authentication for Pulse Secure Access Service Overview	75
Credential Provider Authentication for Pulse Secure Access Service Overview	76
Configuring user-at-credprov Credential Provider Authentication for a Junos Pulse Connection	77
Configuring machine-then-user-at-credprov Credential Provider Authentication for a Junos Pulse Connection	78
Machine and User Authentication Through a Pulse Connection for Pulse Secure Access Service	80
Configuring Junos Pulse for Secure Application Manager	81
Pulse Connection Set Options for Pulse Secure Access Service	87
Junos Pulse Connection Options	89
Connection is Established Settings	91
Location Awareness Rules	92
Machine Connection Preferences	93
User Connection Preferences	93
Pre-login Connection Preferences	93
Securing the Connection State on the Junos Pulse Client	94
Creating a Client Connection Set for Junos Pulse Secure Access Service	94
Configuring Location Awareness Rules for Junos Pulse	96
Component Set Options for Junos Pulse Secure Access Service	98
Creating a Client Component Set for Junos Pulse Secure Access Service	99
Endpoint Security Monitoring and Management for Pulse Secure Access Service	101
Remediation Options	102
Issuing a Remediation Message with Junos Pulse Secure Access Service	105
Using SMS/SCCM Remediation with Junos Pulse Secure Access Service	105
Configuring Shavlik Remediation with Junos Pulse Secure Access Service	107
Enabling Enhanced Endpoint Security with Junos Pulse Secure Access Service	108
Pushing Junos Pulse Configurations Between Junos Pulse Servers of the Same Type	110
Enabling or Disabling Automatic Upgrades of the Junos Pulse Client	112
Upgrading Junos Pulse Client Software	113
Integrating iPass Open Mobile with Junos Pulse for Windows Client	114
Pulse Collaboration Suite Overview	115
Task Summary: Configuring Pulse Collaboration Suite on the Pulse Secure Access Server	116
Configuring Pulse Connections to Support Meetings	116
Scheduling Meetings Through the Pulse Secure Access Service User Web Portal	117
Scheduling Meetings Through Microsoft Outlook	118

Chapter 4	Configuring Junos Pulse on SRX Series Gateways	121
	Junos Pulse and SRX Series Gateways	121
	Junos Pulse and Dynamic VPN Configuration Overview	122
Chapter 5	Configuring Junos Pulse Application Acceleration Service	125
	Installing the Junos Pulse Client	125
	Configuring Personal Firewalls for Junos Pulse Acceleration	126
	Downloading the Junos Pulse Client from a Pulse Secure Access Server	126
	Downloading the Junos Pulse Client from a Pulse Application Acceleration Gateway	127
	Uninstalling the Junos Pulse Client	128
	Managing Software, Configurations, and Policies	128
	Enabling Pulse Client Downloads	128
	Enabling Pulse Client Adjacencies	129
	Configuring Pulse Client Policies	129
	Viewing the Status of Pulse Clients	130
	Viewing the Pulse Client Configuration	130
	Uploading Pulse Client Software	130
	Distributing the Pulse Client	131
	Distributing the Pulse Client Through an SA Series Gateway	131
	Distributing the Pulse Client Through Microsoft SMS/SCCM	132
Chapter 6	Session Migration	135
	Understanding Session Migration	135
	Session Migration Overview	135
	Session Migration and Session Timeout	137
	How Session Migration Works	137
	Session Migration and Session Lifetime	138
	Session Migration and Load Balancers	138
	Authentication Server Support	138
	Task Summary: Configuring Session Migration	139
	Configuring Session Migration for the Pulse Client	140
	Configuring an IF-MAP Federated Network for Session Migration	140
Chapter 7	Deploying Junos Pulse Client Software	143
	Junos Pulse Client Installation Overview	143
	Adding a Pulse Configuration to a New Pulse Installation	146
	Installing Junos Pulse Client from the Web	148
	Launching Junos Pulse from the Pulse Server Web Portal	149
	Usage Notes	150
	Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File	150
	Installing the Pulse Client Using Advanced Command Line Options	151
	Examples	153
	Repairing a Pulse Installation on a Windows Endpoint	154
	Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File	154
	Installing the Pulse Client on OS X Endpoints Using Command Line Options	155
	Junos Pulse Command-line Launcher	155

	Using jamCommand to Import Junos Pulse Connections	158
Part 2	Junos Pulse Compatibility	
Chapter 8	Client Software Feature Comparison	163
	Comparing Odyssey Access Client and Junos Pulse	163
	Comparing Network Connect and Junos Pulse	167
	Pulse Split Tunneling	169
Part 3	Junos Pulse for Mobile Devices	
Chapter 9	Junos Pulse for Mobile Devices and Junos Pulse Mobile Security Suite . .	173
	Junos Pulse for Mobile Devices Overview	173
	Junos Pulse Mobile Security Gateway	174
	Junos Pulse Mobile Clients and User Agent Strings	174
Chapter 10	Junos Pulse for Apple iOS	177
	Junos Pulse for Apple iOS Overview	177
	Before You Begin	179
	Configuring a Role and Realm for Junos Pulse for Apple iOS	180
	Allowing Junos Pulse for iOS Users to Save Webmail Password	183
	Host Checker for Pulse iOS Clients	183
	Configuring Host Checker for Junos Pulse iOS Clients	184
	Implementing Host Checker Policies for Junos Pulse for iOS Devices	186
	Installing the Junos Pulse for Apple iOS App	187
	Using iPhone Configuration Utility Profiles for Junos Pulse for iOS	188
	Collecting Log Files from Junos Pulse for iOS	189
	Junos Pulse for iOS Error Message Reference	189
Chapter 11	Junos Pulse for Google Android	191
	Junos Pulse for Android Overview	191
	Configuring a Role and Realm for Pulse for Android	192
	Allowing Junos Pulse for Android Users to Save Webmail Password	194
	Host Checker for Pulse Android Clients	194
	Configuring Host Checker for Junos Pulse Android Clients	195
	Implementing Host Checker Policies for Junos Pulse for Android Clients	197
	Junos Pulse for Android Error Message Reference	198
	Launching the Junos Pulse for Android App Using a Command	200
	Junos Pulse for Android VPN API Reference	201
	Explicit Intent Target Component	201
	Explicit Intent API — VPN Connect	201
	Explicit Intent API — VPN Disconnect	202
	Explicit Intent API — VPN Check Status	203
	Explicit Intent API — Example	204
Chapter 12	Junos Pulse for Nokia Symbian Devices	205
	Junos Pulse for Symbian Overview	205
	Configuring Pulse Secure Access Service for Junos Pulse on Symbian Devices	205

Chapter 13	Junos Pulse for Windows Mobile Devices	209
	Junos Pulse for Windows Mobile Overview	209
	Pulse Release 1.0, 2.0, and 3.0 and Pulse SAM Connectivity	209
	Configuring Junos Pulse Secure Access Service for Windows Mobile	
	Endpoints	211
	Configuring Host Checker for Junos Pulse for Windows Mobile Clients	215
	Junos Pulse Mobile Security Overview	217
 Part 4	 Index	
	Index	221

List of Tables

	About This Guide	xi
	Table 1: Notice Icons	xi
	Table 2: Junos Pulse Documentation	xii
Part 1	Junos Pulse	
Chapter 1	Junos Pulse Overview	3
	Table 3: Junos Pulse Event Log Messages	12
Chapter 2	Configuring Junos Pulse Access Control Service	17
	Table 4: Configurable Options for Junos Pulse Connection Sets	25
Chapter 3	Configuring Junos Pulse Secure Access Service	63
	Table 5: Pulse/SAM Client Version Summary	82
	Table 6: Pulse Connection Options	89
Chapter 5	Configuring Junos Pulse Application Acceleration Service	125
	Table 7: Personal Firewall Exceptions for Pulse Acceleration	126
Chapter 7	Deploying Junos Pulse Client Software	143
	Table 8: Pulse Launcher Arguments	156
	Table 9: Pulse Launcher Return Codes	157
Part 2	Junos Pulse Compatibility	
Chapter 8	Client Software Feature Comparison	163
	Table 10: Odyssey Access Client and Junos Pulse Feature Comparison	163
	Table 11: Network Connect and Junos Pulse Feature Comparison	167
	Table 12: Pulse Split Tunneling	169
Part 3	Junos Pulse for Mobile Devices	
Chapter 9	Junos Pulse for Mobile Devices and Junos Pulse Mobile Security Suite ..	173
	Table 13: User Agent String Client Type Pairings for Mobile Devices	175
Chapter 10	Junos Pulse for Apple iOS	177
	Table 14: Junos Pulse for iOS Error Messages	189
Chapter 11	Junos Pulse for Google Android	191
	Table 15: Junos Pulse for Android Error Messages	198
Chapter 13	Junos Pulse for Windows Mobile Devices	209
	Table 16: Pulse/SAM Client Version Summary	210

About This Guide

- [Objectives on page xi](#)
- [Audience on page xi](#)
- [Document Conventions on page xi](#)
- [Related Documentation on page xi](#)
- [Obtaining Documentation on page xii](#)
- [Documentation Feedback on page xii](#)
- [Requesting Technical Support on page xii](#)

Objectives

The *Junos Pulse Administration Guide* describes Junos Pulse and includes procedures for network administrators who are responsible for setting up and maintaining network access using Junos Pulse client software.



Audience

The *Junos Pulse Administration Guide* is for network administrators who are responsible for setting up and maintaining network access using Junos Pulse client software. This guide describes the procedures for configuring Junos Pulse as the access client.

Document Conventions

[Table 1 on page xi](#) 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.

Related Documentation

[Table 2 on page xii](#) describes related Junos Pulse documentation.

Table 2: Junos Pulse Documentation

Title	Description
<i>Junos Pulse Mobile Security Administration Guide</i>	Describes the Pulse Mobile Security Suite and includes procedures for network administrators who are responsible for setting up and managing security on mobile devices.
<i>Junos Pulse Secure Access Service Administration Guide</i> (Formerly titled <i>Secure Access Administration Guide</i> .)	Describes how to configure and maintain a Juniper Networks SA Series SSL VPN Appliance.
<i>Junos Pulse Access Control Service Administration Guide</i> (Formerly titled <i>Unified Access Control Administration Guide</i> .)	Describes how to configure and maintain the Unified Access Control solution and the IC Series 4500 and 6500 devices.
<i>Junos Pulse Application Acceleration Administration Guide</i>	Describes how to use the JWOS Web interface to configure, monitor, and manage the Junos Pulse Application Acceleration Service.
<i>Junos Security Configuration Guide</i>	Describes how to use and configure security features on SRX Series Gateways running Junos OS.

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/>.

To order a documentation CD, which contains this guide, contact your sales representative.

Copies of the Management Information Bases (MIBs) available in a software release are included on the documentation CDs and at <http://www.juniper.net/>.

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 or topic name
- URL or page number
- Software release version (if applicable)

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

Junos Pulse

- [Junos Pulse Overview on page 3](#)
- [Configuring Junos Pulse Access Control Service on page 17](#)
- [Configuring Junos Pulse Secure Access Service on page 63](#)
- [Configuring Junos Pulse on SRX Series Gateways on page 121](#)
- [Configuring Junos Pulse Application Acceleration Service on page 125](#)
- [Session Migration on page 135](#)
- [Deploying Junos Pulse Client Software on page 143](#)

CHAPTER 1

Junos Pulse Overview

- [Introducing Junos Pulse on page 3](#)
- [Installation Requirements on page 10](#)
- [Junos Pulse Client Error Messages Overview on page 11](#)
- [Accessing Junos Pulse Client Error Messages on Mac OS X Endpoints on page 11](#)
- [Junos Pulse Client Log Files on page 12](#)
- [Deleting the Junos Pulse Client Log Files on page 15](#)
- [Migrating From Odyssey Access Client to Junos Pulse Client on page 15](#)
- [Migrating From Network Connect to Junos Pulse on page 16](#)
- [Predictable Pulse Server Host Name Resolution with IPv6 on page 16](#)

Introducing Junos Pulse

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 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.

The Junos Pulse Client for Windows

The Junos Pulse client interface (see [Figure 1 on page 4](#)) displays the deployed Pulse services in the left pane and details about the selected item in the right pane. The Connections item lists the Pulse connections. Each connection is a set of properties that enables network access through a specific Pulse server. The Security item is visible only when optional security options are deployed, such as the Juniper Networks Enhanced Endpoint Security (EES) application. If a Pulse server is licensed to provide EES, you can enable EES and deploy it as part of the Host Checker configuration. The Acceleration item is active when the Pulse client has an adjacency with Pulse Application Acceleration Service.

The Pulse client interface also supports select third-party applications. [Figure 1 on page 4](#) shows one such application, iPass Networks, integrated into the Pulse client interface.

Figure 1: Junos Pulse Client Interface



The Pulse Client for Mac OS X

Pulse 3.0 and higher supports Apple computers running Mac OS X. You deploy Pulse to Mac endpoints the same way you deploy the Windows client. [Figure 2 on page 5](#) shows the Pulse for Mac client interface.

Figure 2: Junos Pulse for Mac Client Interface



Pulse for Mac endpoints supports the following:

- Connections to Junos Pulse Access Control Service
- Connections to Junos Pulse Secure Access Service

Pulse clients connect to the Pulse Secure Access Service in SSL fallback mode.

- Host Checker

Host Checker for Mac OS X supports the following rules and remediation actions:

- Port
- Process
- File
- Custom IMC
- Enable Custom Instructions
- Kill Processes
- Delete Files
- Send reason strings



NOTE: Pulse for the Mac does not support soft token authentication.

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.

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 rules that you define. For example, you can define rules to enable Junos Pulse to automatically establish a secure tunnel to the corporate network through Junos Pulse Secure Access Service when the user is at home, and to establish a Junos Pulse Access Control Service connection when the user is in the office and connected to the corporate network over the LAN. Location awareness rules are based on the client's IP address and network interface information.

Session Migration

If you configure your access environment to support the Junos Pulse session migration feature, users can log in once through a Pulse server on the network, and then securely access additional Pulse servers without needing reauthentication. For example, a user can connect from home through Junos Pulse Secure Access Service, and then arrive at work and connect through Junos Pulse Access Control Service without having to log in again. Session migration also enables users to access different resources within the network without repeatedly providing credentials. IF-MAP Federation is required to enable session migration for users.

Centralized Control

Centralized configuration management is a key feature of Junos Pulse. To achieve centralized management, you can use Junos Pulse Access Control Service or Junos Pulse Secure Access Service to configure all of the connections that clients need, and then push those configurations to the other servers using the Push Configuration feature. In a network that includes more than one Junos Pulse server, you can bind clients to a particular server. The client can automatically pick up new connections from other Pulse servers but only the binding server can update the client's basic configuration settings.

You can define Junos Pulse connections on the server and pass them to the client or users can add connections directly on the client. (You can disable the users' ability to add connections.) A connection includes all of the information that a Pulse client needs to connect to a specific Pulse server. Connections can be installed on the endpoint when Junos Pulse is installed and they can be added or updated later. Options within each Junos Pulse connection allow an administrator to define the level of control over the clients. A connection has the following options:

- By default, a network connection through Junos Pulse allows users to save their logon credentials. The Junos Pulse admin interface lets you disable this feature so that users must always provide credentials.
- You can allow or deny users the ability to manually configure new network connections to their existing Junos Pulse connection set.
- You can allow dynamic connections to provide easy distribution of connection settings. A dynamic connection is automatically downloaded to an existing Pulse client when the user successfully logs into the Pulse server's Web portal and launches Pulse from there. It is also installed as part of a Web install of Junos Pulse. 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 server's Web interface.
- You can allow or deny a client's ability to trust unknown certificates.
- You can choose to control the client's wireless connection environment. Junos Pulse relies on the endpoint's native wireless supplicant, but you can have Pulse disconnect all wireless connections when the client is connected to a wired network through a Pulse connection. You can also specify the permitted wireless networks (scan list) that are available when the Pulse client is connected through a wireless interface.

Security Certificates

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

An 802.1x connection enables an added layer of certificate verification. When you define an 802.1x connection on the Pulse server, you can specify server certificate distinguished names for each CA.

Compliance and Remediation

Pulse supports the Host Checker application to assess endpoint health and update critical software. Host Checker is a client side agent that is based on Trusted Network Connect standards. You configure rules in Host Checker policies for Junos Pulse Secure Access Service and Junos Pulse Access Control Service to specify the minimum criteria for the security compliance of endpoints that are allowed to enter the network. Endpoints that fail can be connected through a role that provides limited access, a remediation role. Host Checker can be deployed from a Pulse server to Pulse clients on Windows and Mac OS X endpoints and it will be downloaded and run when a browser is used on a Windows or Mac OS X endpoint to connect to the Pulse server Web portal.

Host checker for mobile clients (iOS, Android, and Windows Mobile) is included as part of the app and it runs if Host Checker policies are configured and enabled on the server. Host Checker is not supported in the use case where the user employs a browser on the mobile device to connect to the Pulse server Web portal.

For Mac and OS X clients, you can use Host Checker to perform the following:

- Malware protection through Enhanced Endpoint Security (EES)

EES ensures that malware, spyware, viruses, or worms are not present on endpoints, and you can restrict or quarantine these endpoints depending on your Host Checker policy configuration. EES is an optional licensed feature of Pulse Secure Access Service and Junos Pulse Access Control Service.

- Virus signature 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. You can configure automatic remediation for those endpoints that do not meet the specified criteria.

- Patch Management Info Monitoring and Patch Deployment

You can configure Host Checker policies that check for Windows endpoints' operating system service pack, software version, or desktop application patch version compliance.

server and Junos Pulse Access Control 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).

- Patch Remediation Options

Pulse and Host Checker support endpoint remediation through Microsoft System Management Server or Microsoft System Center Configuration Manager (SMS/SCCM) or the Shavlik patch deployment engine. With SMS/SCCM, Pulse triggers a pre-installed SMS/SCCM client to get patches from a pre-configured SMS/SCCM server. Shavlik uses a patch deployment engine that Pulse downloads to any endpoint which needs remediation. Shavlik provides patches directly from Microsoft and other vendors' Web sites. (Internet connectivity is needed for Shavlik remediation.) Shavlik patch

management is an optional feature. A separate license is required for Shavlik patch monitoring and deployment.

- Endpoint configuration

You can configure custom rules to allow Host Checker to check for third party applications, files, process, ports, registry keys, and custom DLLs.

Pulse mobile clients support a set of Host Checker functions that vary from one OS to the next. For complete information on Host Checker for mobile clients, see [“Implementing Host Checker Policies for Junos Pulse for iOS Devices” on page 186](#), [“Implementing Host Checker Policies for Junos Pulse for Android Clients” on page 197](#), and [“Junos Pulse Mobile Security Overview” on page 217](#).

Two-factor Authentication

Pulse supports RSA SecurID authentication through soft token, hard token, and smart card authenticators. The SecurID software (RSA client 4.1 and later) must already be installed on the client machine.

Junos Pulse Collaboration Suite Integration

Junos Pulse Collaboration Suite is accessible through the Pulse interface on Windows, Mac OS X, Android, and iOS. (Android clients must be R4.0 or later. iOS clients must be R3.2 or later.) Junos Pulse Collaboration Suite enables users to schedule and attend secure online meetings. In meetings, users can share their desktops and applications with one another over a secure connection. Meeting attendees can collaborate by enabling remote-control of their desktops and through text chatting.

Bound and Unbound Clients

Another feature of Pulse configuration management is the ability to bind Pulse clients to a single Pulse server. The binding server is the one that provides the initial Pulse configuration. Binding Junos Pulse clients to a particular server ensures that the client does not receive different configurations when accessing other Pulse servers. [“Adding a Pulse Configuration to a New Pulse Installation” on page 146](#) explains in more detail how the binding process works.

The following describes the behaviors of bound and unbound Junos Pulse clients.

- Bound client—A bound client is managed by a particular Pulse server. The Pulse administrator defines the Junos Pulse connections and software components that are installed on the endpoint. When the Pulse client connects to the Pulse server that is managing it, the server automatically provisions configuration and software component updates. The administrator can permit the user to add and remove connections and to modify connections. The administrator can also allow dynamic connections, (connections added by Pulse servers when the user logs into the server using a browser). A dynamic connection enables a bound client to add connections from Pulse servers other than the one the client is bound to. 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 server’s Web interface.

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.

- **Unbound client**—An unbound client is managed by its user. The Junos Pulse client software is installed without any connections. The user must add connections manually. Dynamic connections can be added by visiting the Web portals of Pulse servers. An unbound client does not accept configuration updates from a Pulse server even if client configurations are defined on that server.

Sign-in Notifications

The notifications feature on Pulse Secure Access Service and Pulse Access Control Service allows the network administrator to display notifications to Pulse client users prior to the user logging in and after the user has already logged in. For example, you could display a legal statement or a message stating who is allowed to connect to the server prior to showing the Pulse credentials dialog. After the user has connected, you could display a message that notifies the user of scheduled network or server maintenance or an upcoming company meeting.

Automatic Software Updates

After you deploy Junos Pulse client software to endpoints, software updates occur automatically. If you upgrade the Junos Pulse configuration on the server, updated software components are pushed to a client the next time it connects. (You can disable this automatic upgrade feature.)



NOTE: When you configure Junos Pulse to make 802.1x based connections, a reboot may be required on Windows XP endpoints when Pulse is upgraded.

Additional Pulse software components that are needed for new connections are pushed to the client as needed. Network connection properties are passed to the client at connect time based on the client's role as defined on the Pulse server, after which those configuration properties reside on the client computer.

Related Documentation

- [Junos Pulse for Mobile Devices Overview on page 173](#)
- [Understanding Session Migration on page 135](#)

Installation Requirements

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>.

Related Documentation

- [Introducing Junos Pulse on page 3](#)
- [Junos Pulse for Mobile Devices Overview on page 173](#)
- [Junos Pulse Mobile Security Overview on page 217](#)

Junos Pulse Client Error Messages Overview

Junos Pulse client error and warning messages reside in message catalog files on the endpoint. Each message includes a short description that states the problem and a long description that provides more details and suggests actions to resolve the issue. Some of the message catalog files are part of a Junos Pulse component and are installed on an endpoint only if that component is installed on the endpoint.

All message catalog files are localized. The file name indicates the language. For example, MessageCatalogConnMgr_EN.txt is the English-language version of the file. The following file name conventions indicate the language:

- DE—German
- EN—English
- ES—Spanish
- FR—French
- IT—Italian
- JA—Japanese
- KO—Korean
- PL—Polish
- ZH—Chinese (Traditional)
- ZH-CN—Chinese (Simplified)

Related Documentation

- [Introducing Junos Pulse on page 3](#)
-

Accessing Junos Pulse Client Error Messages on Mac OS X Endpoints

Junos Pulse client error and warning messages reside in message catalog files on the OS X endpoint. Each message includes a short description that states the problem and a long description that provides more details and suggests actions to resolve the issue. Some of the message catalog files are part of a Junos Pulse component and are installed on an endpoint only if that component is installed on the endpoint.

All message catalog files are localized. The file name indicates the language. For example, MessageCatalogPulseUI_EN.txt is the English-language version of the file. The following file name conventions indicate the language:

- DE—German
- EN—English
- ES—Spanish
- FR—French

- IT—Italian
- JA—Japanese
- KO—Korean
- PL—Polish
- ZH—Chinese (Traditional)
- ZH-CN—Chinese (Simplified)

To view Pulse catalog files on Mac OS X endpoint, use Finder to display the package contents of the Pulse application.

- Related Documentation**
- [Introducing Junos Pulse on page 3](#)
 - [Junos Pulse Client Log Files on page 12](#)

Junos Pulse Client Log Files

The Junos Pulse client writes information to Pulse log files on Windows and Apple OS X endpoints. If you need to investigate a problem with Pulse connectivity on a Pulse client endpoint, you can instruct the user to save the client logs and e-mail them to you.

The user saves logging information by opening Pulse and then clicking File > Logs > Save As. All relevant log files are added to a single file, LogsAndDiagnostics.zip. The user saves the .zip file and then makes it available to you.

Pulse maintains its own log files on all supported platforms. On Windows 7 and Windows Vista, the Pulse client also logs its major operational events into Windows Event Log. Network administrators can review the Pulse event log to help troubleshoot problems. [Table 3 on page 12](#) lists the Pulse messages that can appear in the Windows event log. To view the Pulse messages, open the Windows Event Viewer. Pulse messages reside in Applications and Services->Junos Pulse->Operational.

Table 3: Junos Pulse Event Log Messages

ID	Level	Message	Description
600	error	The connection <ID> failed authentication: Error <ID>.	802.1X EAP authentication failure.
601	informational	User has canceled authentication of the connection <ID>.	The user canceled 802.1X EAP authentication.
602	error	Failure writing wireless LAN profile for connection <ID> Error <ID>: Reason <ID>: Profile: <ID>.	A failure occurred while creating or modifying a wireless LAN profile.
603	error	Failure writing wireless LAN profile for connection <ID> Error <ID>.	A failure occurred while deleting wireless LAN profile.

Table 3: Junos Pulse Event Log Messages (*continued*)

ID	Level	Message	Description
604	error	Failure writing wired LAN profile for connection <ID> Error <ID>: Profile: <ID>.	A failure occurred creating or modifying a wired LAN profile.
605	error	Failure writing wired LAN profile for connection <ID> Error <ID>.	A failure occurred deleting a wired LAN profile.
500	informational	Pulse servicing has completed successfully. All components are up to date.	Indicates a successful pulse servicing operation.
501	informational	Pulse servicing has completed successfully. All components are up to date.	Servicing was requested but all components were up to date.
502	error	Pulse servicing has failed. Failure summary:	Pulse servicing failed.
100	informational	User requested connection <ID> to start.	The user initiated a connection request.
101	informational	User requested connection <ID> to stop.	The user initiated a disconnect request.
102	informational	Connection <ID> is starting because its policy requirements have been met. Connection Policy: <ID>.	A connection was started because of policy evaluation.
103	informational	Connection <ID>) is stopping because of its policy requirements. Connection Policy: <ID>.	A connection was stopped because of policy evaluation.
104	informational	Connection <ID> is stopping because of transition to context <ID>.	The machine-to-user connection was disconnected to transition to another identity.
105	informational	Connection <ID> is starting because of transition to context <ID>.	The machine-to-user connection was connected as part of the transition to another identity.
106	informational	Connection <ID> is disconnected due to computer suspend.	The connection to Pulse Secure Access Service was disconnected because the computer is being suspended.
107	informational	Connection <ID> is disconnected due to login error.	A credential provider connection was disconnected due to log-in error.
108	informational	Connection <ID> is disconnected because it was modified.	A connection was disconnected because it was modified.
109	informational	User requested connection <ID> to suspend.	The user initiated a suspend request.

Table 3: Junos Pulse Event Log Messages (*continued*)

ID	Level	Message	Description
110	informational	User requested connection <ID> to resume.	The user initiated a resume request.
1	informational	The Junos Pulse service version <ID> has successfully started.	The Pulse service started.
2	informational	The Junos Pulse service has stopped.	The Pulse service stopped.
200	error	No connections matching URL <ID> were found in Pulse database. Request to start a connection from the browser has failed.	Pulse failed to resume a connection from the browser.
400	error	The host check for connection <ID> has failed. Failed policies: <ID>.	Host Checker failed one or more policies.
300	informational	The connection <ID> was established successfully through web-proxy <ID>.	Pulse established a connection to Pulse Secure Access Service or Pulse Access Control Service through a web proxy.
301	informational	The connection <ID> was established successfully to address <ID>.	Pulse established a direct (non-proxy) connection to Pulse Secure Access Service or Pulse Access Control Service.
302	informational	The connection <ID> was disconnected.	The Pulse connection was disconnected from the Pulse server.
303	error	The connection <ID> encountered an error: <ID> Peer address: <ID>.	A connection encountered an error.
304	error	The connection <ID> was disconnected due to change in routing table. Interface address changed from <ID> to <ID>.	Pulse detected a change in the route to the Pulse server.
305	informational	VPN tunnel transport for connection <ID> switched from ESP to SSL mode due to missing ESP heartbeat.	ESP to SSL fallback occurred due to missing ESP heartbeats.
306	informational	VPN tunnel for connection <ID> is switched to ESP mode.	Tunnel transport switched to ESP mode.
307	error	The connection <ID> encountered an error: System error: <ID> Peer address: <ID>.	The Pulse connection failed because of a system error.
308	error	The server disconnected connection <ID> Reason <ID>: Peer address: <ID>.	The server disconnected a connection.

Related Documentation • [Deleting the Junos Pulse Client Log Files on page 15](#)

Deleting the Junos Pulse Client Log Files



NOTE: Juniper recommends that you do not delete Pulse client log files.

The Pulse client controls log file size automatically. When a current log file reaches 10MB, a new one is created and the oldest log file is deleted. If you need to delete Pulse client log files, do not delete the file without first moving it to the Recycle Bin or renaming it.

To safely delete Pulse client log files on a Windows endpoint:

1. Use a command line or Windows Explorer to locate and delete debuglog.log and, optionally, debuglog.log.old. When prompted if you want to move the file to the Recycle Bin, answer Yes. Do not press Shift+Delete, which permanently deletes a file without moving it to the Recycle bin.

The file location varies depending on which version of Windows the endpoint is running. For example, the following path is valid for a Windows 7 Enterprise 64-bit endpoint: C:\Users\Public\Juniper Networks\Logging.

2. Empty the Recycle Bin.

Alternatively, you could first rename debuglog.log and then delete it. After you delete the log file, the Pulse client creates a new one. However, that operation might take some time depending on the activities of the Pulse client.

Related Documentation

- [Junos Pulse Client Error Messages Overview on page 11](#)

Migrating From Odyssey Access Client to Junos Pulse Client

An endpoint can have Junos Pulse and Odyssey Access Client (OAC) installed at the same time. If the endpoint has an early version of OAC installed, the user must upgrade or uninstall it before installing Pulse. The Pulse installation program checks for OAC. If OAC is present and it is compatible, the Pulse installation proceeds. If the OAC is not compatible, the Pulse installation displays a message advising the user to uninstall or upgrade OAC.

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>.

Wireless Connectivity, OAC, and Junos Pulse

When OAC serves as the endpoint's wireless supplicant, it handles login requests to the wireless network, passes login credentials to the authentication server, and maintains connectivity when the endpoint is roaming. You can continue to use OAC as the endpoint's wireless supplicant, or you can uninstall OAC after installing Pulse and activate the native Windows wireless supplicant or other wireless connectivity software that might be installed on the endpoint. Junos Pulse does not include a wireless supplicant component.

If the endpoint is running Junos Pulse but not running OAC, then the endpoint must be configured to use the Windows supplicant for wireless connectivity.

- Related Documentation**
- [Comparing Odyssey Access Client and Junos Pulse on page 163](#)
 - [Comparing Network Connect and Junos Pulse on page 167](#)

Migrating From Network Connect to Junos Pulse

Junos Pulse and Network Connect (NC) can run at the same time on an endpoint.



NOTE: The Pulse installation program checks for NC. If the installation program finds NC Release 6.3 or later, the Pulse installation proceeds. If NC is not at least Release 6.3, the program displays a message telling the user to upgrade NC. 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>

On endpoints that connect to Junos Pulse Secure Access Service, if Junos Pulse is running on the Windows main desktop, you cannot launch Pulse within Secure Virtual Workspace (SVW). SVW is not supported with Pulse.

- Related Documentation**
- [Comparing Odyssey Access Client and Junos Pulse on page 163](#)
 - [Comparing Network Connect and Junos Pulse on page 167](#)

Predictable Pulse Server Host Name Resolution with IPv6

When connecting to a Pulse server, the Pulse client uses the services of the endpoint operating system to resolve the host name to an IP address. If a Pulse server host name resolves to both IPv4 and IPv6 addresses, an IPv4 or an IPv6 address is presented as the preferred IP address to Pulse. The behavior depends on the operating system and how it's configured. For example, Windows 7 adheres to IETF standards that define how to establish the default address selection for IPv6. MAC OS 10.6 does not support that standard. Also Windows 7 default settings can be changed by netsh commands so RFC compliance can be modified on the endpoint. So It is difficult to predict which Pulse server IP address would get resolved to on a given client machine.

For predictable host name resolution we recommend that you use different Pulse server host names for IPv6 and IPv4 addresses. For example, configure myserver1.mycompany.com for IPv4 addresses and myserver1-v6.mycompany.com for IPv6 addresses. The Pulse server admin can publish myserver1-v6.mycompany.com to the Pulse users who are expected to connect over IPv6 and others will continue using myserver1.mycompany.com.

- Related Documentation**
- [Introducing Junos Pulse on page 3](#)

CHAPTER 2

Configuring Junos Pulse Access Control Service

- [Before You Begin on page 18](#)
- [Junos Pulse Access Control Service Overview on page 18](#)
- [Pulse Access Control Service and Pulse Secure Access Service Deployment Options on page 19](#)
- [Application Acceleration Deployment Options on page 20](#)
- [SRX Series Gateway Deployment Options on page 21](#)
- [Configuring a Role for Junos Pulse Access Control Service on page 21](#)
- [Client Connection Set Options for Junos Pulse Access Control Service on page 24](#)
- [Creating a Client Connection Set for Junos Pulse Access Control Service on page 30](#)
- [Securing the Connection State on the Junos Pulse Client on page 33](#)
- [Machine Authentication for Pulse Access Control Service Overview on page 33](#)
- [Configuring machine-only Machine Authentication for a Junos Pulse Connection on page 34](#)
- [Configuring user-after-desktop Machine Authentication for a Junos Pulse Connection on page 35](#)
- [Preferred Realm and Role for Junos Pulse Machine Authentication on page 36](#)
- [Remote Desktop Protocol Compatibility with Junos Pulse 802.1X Machine Authentication Connection on page 38](#)
- [Credential Provider Authentication for Pulse Access Control Service Overview on page 38](#)
- [Configuring user-at-credprov Credential Provider Authentication for a Junos Pulse Connection on page 40](#)
- [Configuring machine-then-user-at-credprov Credential Provider Authentication for a Junos Pulse Connection on page 41](#)
- [Machine and User Authentication Through a Pulse Connection for Pulse Access Control Service on page 43](#)
- [Configuring Location Awareness Rules for Junos Pulse on page 44](#)
- [Junos Pulse Access Control Service Component Set Options on page 46](#)

- [Creating a Client Component Set for Junos Pulse Access Control Service on page 48](#)
- [Endpoint Security Monitoring and Management for Pulse Access Control Service on page 49](#)
- [Issuing a Remediation Message with Junos Pulse Access Control Service on page 53](#)
- [Using SMS/SCCM Remediation with Junos Pulse Access Control Service on page 54](#)
- [Configuring Shavlik Remediation with Pulse Access Control Service on page 55](#)
- [Enabling Enhanced Endpoint Security for Junos Pulse Access Control Service on page 57](#)
- [Pushing Junos Pulse Configurations Between Junos Pulse Servers of the Same Type on page 59](#)
- [Enabling or Disabling Automatic Upgrades of the Junos Pulse Client on page 60](#)
- [Upgrading Junos Pulse Client Software on page 61](#)

Before You Begin

Before you begin configuring Junos Pulse, be sure you have already configured your device network settings. Also be sure that you have defined the authentication settings, including the authentication servers and sign-in settings. Authentication Host Checker settings can directly affect a Junos Pulse installation because you can define the conditions that an endpoint must meet to be allowed access to protected resources.

Related Documentation

- [Introducing Junos Pulse on page 3](#)
- [Specifying Host Checker Access Restrictions](#)

Junos Pulse Access Control Service Overview

To enable Pulse clients to connect to Junos Pulse Access Control Service, you configure the service 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 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 Pulse server's user Web portal. After the installation is complete, users have all the connections they need to access network resources.
- 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 msixexec

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.

- Distribute Junos Pulse with no preconfiguration. You can download the default Junos Pulse installation file, 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. Users can also automatically download a Pulse server's dynamic connection by browsing to and logging into the Pulse Server's 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.

Related Documentation

- [Enabling Pulse Client Downloads on page 128](#)
- [Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 150](#)
- [Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 154](#)

Pulse Access Control Service and Pulse Secure Access Service Deployment Options

For Junos Pulse Access Control Service and Pulse Secure Access Service, you can deploy all of the connections required for Windows and Mac OS X clients to connect to any Pulse server.



NOTE: Pulse clients for mobile devices are distributed through the app stores.

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 msexec 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.

**Related
Documentation**

- [Junos Pulse for Mobile Devices Overview on page 173](#)
- [Comparing Odyssey Access Client and Junos Pulse on page 163](#)
- [Comparing Network Connect and Junos Pulse on page 167](#)

Application Acceleration Deployment Options

The Junos Pulse client accelerates traffic between the client system and a network's Junos Pulse Application Acceleration Service. Pulse Application Acceleration Service and Pulse clients discover each other automatically and begin accelerating traffic without user intervention. Junos Pulse Application Acceleration Service supports the following deployment options:

- The administrator can enable Pulse downloads and configure Pulse client configuration, and then users can download the Junos Pulse client from JWOS 6.1 or higher. When the license is present, a Junos Pulse selection appears in the task bar of the Web interface for the Pulse server.
- The Junos Pulse client can be downloaded and installed automatically when users access Junos Pulse Secure Access Service. On SA Series SSL VPN systems running software Release 7.0 or later, you can configure an App Acceleration connection for Application Acceleration Service and install it along with the Pulse client software. You can also deploy an App Acceleration connection from Junos Pulse Access Control Service. Although Pulse Access Control Service is for LAN access where WAN application acceleration is not used, Pulse Access Control Service can deploy any type of Pulse connection, which allows flexibility in how you deploy Pulse to users.



NOTE: Junos Pulse for mobile devices does not support application acceleration.

- Related Documentation**
- [Junos Pulse for Mobile Devices Overview on page 173](#)
 - [Understanding Session Migration on page 135](#)

SRX Series Gateway Deployment Options

Endpoints can use Junos Pulse client software to connect to SRX Series gateways that are running Junos OS Release 10.2, and that have dynamic VPN access enabled and configured. The following describes deployment options for SRX Series gateway connections:

- You can create connections that use the connection type “Firewall” and deploy these connections from Pulse Secure Access Service or Junos Pulse Access Control Service.
- You can download the Junos Pulse installer from a Pulse server or the Juniper Networks Web and install it using local distribution methods such as SMS/SCCM. After installing Pulse, users create a connection to an SRX gateway.

- Related Documentation**
- [Understanding Session Migration on page 135](#)

Configuring a Role for Junos Pulse Access Control Service

A role specifies network session properties for users who are mapped to the role. The following procedure describes configuration options that apply to a role that employs Junos Pulse.

To configure a role for Pulse endpoints:

1. From the admin console, select **Users > User Roles > New User Role**.
2. Enter a name for the role and, optionally, a description.
3. **Click Save Changes**. The role configuration tabs appear.
4. Set the following options:

General > Restrictions

- **Source IP**—Source IP options allow you to make an assignment to this role dependent on the endpoint's IP address or IP address range. To enable source IP address restrictions, select **Allow or deny users from the following IP addresses**, and then add IP addresses or address ranges. Select **Allow** to allow users to sign in from the specified IP address, or **Deny** to prevent users from signing in from the specified IP address. Then click **Add**. When you are finished making changes, click **Save Changes**.

If you add multiple IP addresses, move the highest priority restrictions to the top of the list by selecting the check box next to the IP address, and then clicking the up arrow button. 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.

- **Browser**—Browser options allow you to enforce the use of a particular type of browser for Web access to Pulse Access Control Service. Browser options apply only to operations that involve accessing Pulse Access Control Service through its user Web portal, such as acquiring a dynamic connection or installing Pulse through a role. Normal connection operations between the Junos Pulse client and Pulse server are not affected by browser restrictions.
- **Certificate**—Certificate options allow you to require users to sign in from an endpoint that possesses the specified client-side certificate from the proper certificate authority. Before you enable this option, be sure that you have configured the client-side certificate on the Trusted Client CAs page of the admin console.
- **Host Checker**—Host Checker options allow you to enable Host Checker policies, to choose one or more policies for the role, and specify whether the endpoint must meet all or just one of the selected Host Checker policies. The Host Checker policies that appear as Available Policies must be previously defined as part of the Endpoint Security settings in the Authentication section of the admin console.

General > Session Options

- **Session lifetime**—Session lifetime options allow you to set timeout values for user sessions. You can change the defaults for the following:
 - **Max. Session Length**—Specify the number of minutes a user session may remain open before ending. During a user session, prior to the expiration of the maximum session length, Pulse prompts the user to re-enter authentication credentials, which avoids the problem of terminating the user session without warning.
 - **Heartbeat Interval**—Specify the frequency at which the Pulse client should notify Pulse Secure Access Service to keep the session alive. You should ensure that the heartbeat interval of the agent is greater than the Host Checker interval, otherwise performance could be affected. In general, the heartbeat interval should be set to at least 50% more than the Host Checker interval.
 - **Heartbeat Timeout**—Specify the amount of time that Pulse Secure Access Service should wait before terminating a session when the endpoint does not send a heartbeat response.

- **Auth Table Timeout**—Specify a timeout value for the auth table entry to be provisioned as needed. Based on user identity and endpoint status, Pulse Access Control Service assigns the user a set of roles that specify which resources the user can access. The Pulse server pushes the roles associated with each endpoint's source IP address (called auth table entries) to the Infranet Enforcer. The Infranet Enforcer allows traffic between the endpoint and the protected resources based on resource access policies.
- **Reminder Time**—When the Enable Session Extension feature is enabled, the Reminder Time specifies the number of minutes prior to a session end when the server sends a notice through Pulse and notifies the user that the session will end soon.
- **Enable Session Extension**—You can select the Enable Session Extension check box to allow Pulse users to continue a session beyond the maximum session length. If this feature is enabled, users can extend a session through the Pulse client user interface.
- **Roaming session**—Roaming allows user sessions to work across source IP addresses. Roaming session options include the following:
 - **Enabled**—Select this option to enable roaming for users mapped to this role. A roaming user session works across source IP addresses, which allows mobile users with dynamic IP addresses to sign in to Pulse Secure Access Service from one location and continue working from other locations.
 - **Limit to subnet**—Select this option to limit the roaming session to the local subnet specified in the Netmask box. 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.
 - **Disabled**—Select this option to disable roaming user sessions for users mapped to this role. Users who sign in from one IP address may not continue an active Infranet Controller session from another IP address; user sessions are tied to the initial source IP address.

General > UI Options

The UI options allow you to define options that a user sees after a successful login to the Pulse Access Control server by means of a browser or the Pulse client. Be sure that you have already defined the authentication settings for this role.

5. Select the Agent tab. The agent is the client program for a user assigned to this role. When a user connects to the system using a Web browser, the agent is downloaded and installed if it is not already installed on the user's endpoint. Configure the following options.
 - Select **Install Agent for this role**.

Agent options appear only after you select this check box.
 - Select **Install Junos Pulse**.
6. In the **Session scripts** area, optionally specify a location for the following:

- **Windows: Session start script**—Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse connects with Pulse Access Control Service. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources. The script must be in a location (either local or on the network) that is accessible by the user.
 - **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 Access Control 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. The script must be in a location (either local or on the network) that is accessible by the user.
7. Click **Save Changes**, and then select **Agent > Junos Pulse Settings**.
 8. Select a component set that you have created, use the Default component set or select **none**. You would select **none** only if you are creating this role to distribute new or updated connections to existing Pulse users.
 9. Click **Save Changes**.
 10. Select **Users > User Realms > Select Realm > Role Mapping > New Rule** to configure role mapping rules that map Junos Pulse users to the role you configured.

Related Documentation

- [Junos Pulse Access Control Service Overview on page 18](#)
- [Endpoint Security Monitoring and Management for Pulse Access Control Service on page 49](#)
- [Specifying Host Checker Access Restrictions](#)

Client Connection Set Options for Junos Pulse Access Control Service

A Junos Pulse client connection set contains network options and allows you to configure specific connection policies for client access to any Pulse server that supports Junos Pulse. [Table 4 on page 25](#) describes connection set options.

Table 4: Configurable Options for Junos Pulse Connection Sets

Options	<p>Allow saving logon information—Controls whether the Save Settings check box is available in logon dialog boxes in the Pulse client. If you clear this check box, the Pulse client always requires users to provide credentials. If you select this check box, users have the option of saving their credentials.</p> <p>The Junos Pulse client can retain <i>learned user settings</i>. These settings are retained securely on the endpoint, evolving as the user connects through different Pulse servers. The Junos Pulse client can save the following settings:</p> <ul style="list-style-type: none"> • Certificate acceptance • Certificate selection • Realm • Username and password • Proxy username/password • Secondary username/password • Role <p>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 smartcard authentication.</p> <p>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, which clears all user saved settings.</p> <hr/> <p>Allow user connections—Controls whether connections can be added by the user.</p> <hr/> <p>Display splash screen—Clear this check box to hide the Pulse splash screen that normally appears when the Pulse client starts.</p> <hr/> <p>Dynamic certificate trust—Determines whether or not users can opt to trust unknown certificates. If you select this check box, a user can ignore warnings about invalid certificates and connect to the target Pulse server.</p> <hr/> <p>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.</p>
---------	---

Table 4: Configurable Options for Junos Pulse Connection Sets (*continued*)

<p>Wireless suppression—Disables wireless access when a wired connection is available. If the wired connection is removed, Pulse enables the wireless connections with the following properties:</p> <ul style="list-style-type: none"> • Connect even if the network is not broadcasting. • Authenticate as computer when computer information is available. • Connect when this network is in range. <p>NOTE: Wireless suppression occurs only when the wired connection is connected and authorized. If you enable wireless suppression, be sure to also configure a connection that enables the client to connect through a wired connection.</p>	
<p>When you create a connection for a connection set, you choose a connection type. The following options are available for each connection type.</p>	
<p>UAC 802.1x options</p>	<p>Adapter type—Specifies the type of adapter to use for authentication: wired or wireless.</p>
<p>Use this connection type to define authenticated connectivity to 802.1x devices, wired or wireless. Users cannot create 802.1x connections 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>	<p>Outer username—Enables users 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 anonymous@acme.com. If you leave the box blank, the client passes the user's login name (inner identity) as the outer identity.</p> <p>Scan List—Specify the wireless network SSIDs that the user can connect to in priority order.</p> <p>Support Non-broadcast SSID—Allow users to connect to a non-broadcast wireless network from within the Pulse interface.</p>
<p>Trusted Server List (for UAC 802.1x Connection)</p>	<p>Server certificate DN—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 4: Configurable Options for Junos Pulse Connection Sets (*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/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—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.</p>
	<p>Enable Junos Pulse Collaboration integration 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.</p>
	<p>This server—Specifies whether the endpoint connects to this 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 (for Dynamic VPN)	<p>Address—Specifies the IP address of the SRX device.</p>
	<p>Allow user to override connection policy—Allows users 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>Community string—The Junos Pulse client and the Junos Pulse Application Acceleration Service can form an adjacency for application acceleration 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 on the Pulse Application Acceleration Service.</p>
For all connection types, specify how the connection is established. The options vary according to the type of connection. Connections can be established using the following options:	

Table 4: Configurable Options for Junos Pulse Connection Sets (*continued*)

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 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, automatic connection 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.

Automatically when the machine starts. Connection is authenticated again when the user signs in into 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 off, the machine authentication connection is restored. In one typical use case, the machine credentials provide access to one VLAN and the user credentials provide access to a different VLAN.

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 at user login—This option 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, login to the endpoint, and login to the domain server.

NOTE: This label changed at Pulse Access Control Service R4.3. 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 R4.2.

Automatically when the machine starts. Connection is authenticated again at user login—This option 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.

For SSL VPN or UAC (L3) and SRX connections that are set to have the connection established automatically, you can define location awareness rules that 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 Junos 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.



NOTE: To create a negative location awareness rule, you first create the positive state and then use rule requirement logic to use the rule as a negative condition.

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 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 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.

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 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.
- **Select client certificate from machine certificate store**—This 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 on a Windows endpoint. For more information, see ["Machine and User Authentication Through a Pulse Connection for Pulse Access Control Service"](#) on page 43

Related Documentation

- [Machine Authentication for Pulse Access Control Service Overview on page 33](#)
- [Configuring Location Awareness Rules for Junos Pulse on page 44](#)
- [Machine and User Authentication Through a Pulse Connection for Pulse Access Control Service on page 43](#)
- [Remote Desktop Protocol Compatibility with Junos Pulse 802.1X Machine Authentication Connection on page 38](#)

Creating a Client Connection Set for Junos Pulse Access Control Service

A Junos Pulse client connection (also called a client configuration) set contains network options and allows you to configure specific connection policies for client access to any Pulse server that supports Junos Pulse.


To create a Junos Pulse client configuration:

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



NOTE: You must enter a connection set name before you can create connections.

4. Click **Save Changes**.
5. From the main Junos Pulse Connections page, select the connection set.
6. Under Options, select or clear the following check boxes:
 - **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, optionally, a description for this connection.
9. Select a type for the connection. Type can be any of the following:
 - **UAC 802.1X**
 - **SSL VPN or UAC (L3)**
 - **SRX**
 - **App Acceleration**
10. If you select **UAC 802.1X** from the type list, enter a value or select or clear the following check boxes:
 - **Adapter type**—Select Wired or Wireless.
 - **Outer username**—Enter the outer username.
 - **Scan list**—Enter the SSIDs to connect to in your order of priority.
 - **Support Non-broadcast SSID**—Allow users to connect to a non-broadcast wireless network from within the Pulse interface.
11. Click **Save Changes**.
12. If you selected **SSL VPN or UAC (L3)** for the type, select or clear the following check boxes:
 - **Allow user to override connection policy**



NOTE: 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**
 - **Support Remote Access (SSL VPN) or LAN Access (UAC) on this connection**
 - **This Server**—This connection uses the URL of the server where you are creating the connection.

- **URL**—If you did not enable **This Server**, specify the URL of the server for the connection.
 - **Client Certificate Location: Client**—Enables you to specify the certificate store that the Pulse client accesses for certificate authentication on Windows endpoints. Typically, you would use the default setting, which retrieves the certificate from the user's personal certificate store, and then certificate authentication is controlled by the **Connection is established** option. If you disable this option, the Pulse connection uses a machine certificate from the Local Computer Personal certificate store, which enables you to perform machine authentication and user authentication for the Pulse connection. If you disable this option, you must also create a sign-in policy and configure authentications servers to perform the user authentication.
13. If you select **SRX**, enter the IP address of the SRX device in the Address box and specify whether you want the user to be able to override connection policy.
 14. If you select **App Acceleration**, select the **Connect Automatically** check box to permit the client to automatically form an adjacency to an Junos Pulse Application Acceleration Service in the network.



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.

15. Specify how the connection is established, manually or automatically. These options enable you to configure machine authentication and credential provider authentication.
16. (Optional) You can enable location awareness on automatic connections by creating location awareness rules. Location awareness can force a connection to a particular interface.
17. (Optional) You can set preferred role and realm options for a machine authentication connection.
18. After you have created the client connection set, create a client component set and select this connection set.

Related Documentation

- [Client Connection Set Options for Junos Pulse Access Control Service on page 24](#)
- [Endpoint Security Monitoring and Management for Pulse Access Control Service on page 49](#)
- [Configuring Location Awareness Rules for Junos Pulse on page 44](#)
- [Preferred Realm and Role for Junos Pulse Machine Authentication on page 36](#)
- [Remote Desktop Protocol Compatibility with Junos Pulse 802.1X Machine Authentication Connection on page 38](#)

Securing the Connection State on the Junos Pulse Client

To disable user interaction with Pulse connections on the endpoint, you can configure Junos Pulse connections so that when they are deployed to the endpoint, users cannot shut down a connection, suspend or resume a connection to Pulse Secure Access Service, or shut down Pulse. Disabling user interaction with Pulse enables the Pulse administrator to control how endpoints connect to the network without allowing the user to override administrative control. For example, if you use machine authentication, the connection from endpoint to server is established automatically. By locking down the Pulse endpoint, users cannot change their connection.

To secure the Pulse endpoint from the Pulse Access Control server:

1. Click **Users > Junos Pulse Connections**.
2. Edit or create a new connection.
3. Disable the check box labeled **Allow user to override connection policy**.

Related Documentation

- [Client Connection Set Options for Junos Pulse Access Control Service on page 24](#)
- [Endpoint Security Monitoring and Management for Pulse Access Control Service on page 49](#)
- [Machine Authentication for Pulse Access Control Service Overview on page 33](#)

Machine Authentication for Pulse Access Control Service Overview

Machine authentication uses machine credentials (machine name and password or machine certificate) to authenticate the endpoint. You can enable machine authentication for Pulse Access Control Service as part of a Junos Pulse connection and distribute the connection to endpoints through the normal Pulse distribution methods. You enable Pulse machine authentication support on a Pulse connection, either Layer 2 or Layer 3.

The following describes the requirements for a machine authentication environment:

- 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.
- 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. You can specify a preferred role and realm for the connection, which eliminates realm and role selection dialogs.
- 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.

Pulse supports the following machine authentication types:

- machine-only—The connection is established using machine credentials when no user is logged in. The connection is maintained after user logon.
- user-after-desktop—The connection is established using machine credentials when no user is logged in. After user logon, the machine connection is disconnected. Once the user logs out, user connection is disconnected and machine connection is reestablished.

**Related
Documentation**

- [Preferred Realm and Role for Junos Pulse Machine Authentication on page 36](#)
- [Configuring machine-only Machine Authentication for a Junos Pulse Connection on page 34](#)
- [Configuring user-after-desktop Machine Authentication for a Junos Pulse Connection on page 35](#)
- [Machine and User Authentication Through a Pulse Connection for Pulse Access Control Service on page 43](#)
- [Remote Desktop Protocol Compatibility with Junos Pulse 802.1X Machine Authentication Connection on page 38](#)

Configuring machine-only Machine Authentication for a Junos Pulse Connection

When the Pulse connection is configured for machine-only machine authentication, the Pulse connection is established using machine credentials when no user is logged in. The connection is maintained after user logon.

To enable a Pulse connection for machine-only machine authentication:

1. Click **Users > Junos Pulse > Connections** and create or select a connection set.
2. Create or edit a connection. For the connection type, you can select either UAC (802.1X) for a Layer 2 connection or SSL VPN or UAC (L3) for a Layer 3 connection.
3. Under Connection is established, select **Automatically when the machine starts. Machine credentials used for authentication.**

Machine credentials are used to connect to the Pulse Access Control Service when the endpoint is started, before a user logs on. The connection is maintained when a users logs on, logs off, or switches to a different logon.

4. 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.
5. Specify **Realm and Role Preferences** to suppress realm or role selection dialogs during the logon process:

- **Preferred Machine Realm**—Specify the realm that for this connection. The connection ignores any other realm available for the specific logon credentials
- **Preferred Machine 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 machine realm.

Related Documentation

- [Machine Authentication for Pulse Access Control Service Overview on page 33](#)
- [Credential Provider Authentication for Pulse Access Control Service Overview on page 38](#)
- [Remote Desktop Protocol Compatibility with Junos Pulse 802.1X Machine Authentication Connection on page 38](#)

Configuring user-after-desktop Machine Authentication for a Junos Pulse Connection

When the Pulse connection is configured for user-after-desktop machine authentication, the connection is established using machine credentials when no user is logged in. After user logon, the machine connection is disconnected. Once the user logs out, user connection is disconnected and machine connection is reestablished.

To enable a Pulse connection for user-after-desktop machine authentication:

1. Click **Users > Junos Pulse > Connections** and create or select a connection set.
2. Create or edit a connection. For the connection type, you can select either UAC (802.1X) for a Layer 2 connection or SSL VPN or UAC (L3) for a Layer 3 connection.
3. Under Connection is established, select **Automatically when the machine starts. Connection is authenticated again when the user signs in to the desktop.**

Machine credentials are used to connect to the Pulse Access Control Service when the endpoint is started, before a user logs 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.

4. 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=c4kl.stnh.mycompany.net; E=ausername@mycompany.com.
5. 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.

**Related
Documentation**

- [Machine Authentication for Pulse Access Control Service Overview on page 33](#)
- [Credential Provider Authentication for Pulse Access Control Service Overview on page 38](#)
- [Remote Desktop Protocol Compatibility with Junos Pulse 802.1X Machine Authentication Connection on page 38](#)

Preferred Realm and Role for Junos Pulse 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 3 on page 37](#) shows a role mapping rule with the rule name highlighted.

Figure 3: 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

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**

- [Machine Authentication for Pulse Access Control Service Overview on page 33](#)

Remote Desktop Protocol Compatibility with Junos Pulse 802.1X Machine Authentication Connection

If you want to use Remote Desktop Protocol (RDP) to access an endpoint over a Pulse 802.1X connection, machine authentication is required. Due to a Microsoft OS limitation, an RDP connection attempt over a user-only 802.1X authenticated connection will fail. To support RDP connectivity over an authenticated 802.1X connection, you must have a machine-only connection or a machine-then-user connection. In the case of a machine-then-user connection, when you use RDP to connect to a machine over an 802.1X connection that is connected as user, the connection transitions the 802.1X connection to a machine connection. If you subsequently login to the machine directly, it transitions back to a user connection.

To access the endpoint using RDP, you must define that the connection is established using one of the following Pulse connection options:

- Automatically when the machine starts. Machine credentials used for authentication.
- Automatically when the machine starts. Connection is authenticated again when the user signs in to the desktop.

Credential Provider Authentication for Pulse Access Control Service Overview

When Microsoft introduced Windows Vista, it moved away from a login integration interface based on GINA (Graphical Identification and Authentication) in favor of credential provider authentication. The Junos Pulse credential provider integration enables connectivity to a network that is required for the user to login 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. Credential provider login is supported on Windows Vista and later Windows platforms.

You can use the Pulse support for credential provider to provide single sign-on capabilities. Pulse establishes a connection to the network and then uses the same credentials to login the Windows domain.

You enable Pulse credential provider support on a Pulse connection, (connection type 802.1X (UAC) or SSL VPN (L3)). After the connection has been downloaded to the endpoint through the normal Pulse distribution methods, Pulse annotates the credential provider tile that appears on the user login screen by adding a Pulse icon in the lower right corner of the tile.

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 logon and postponed until the user connection is established. Host Checker remediation notifications are displayed.


**Related
Documentation**

- [Configuring Location Awareness Rules for Junos Pulse on page 44](#)

Configuring user-at-credprov Credential Provider Authentication for a Junos Pulse Connection

With a user-at-credprov connection, the Pulse connection establishes the connection before a 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.

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=c4kl.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.

Related Documentation

- [Credential Provider Authentication for Pulse Access Control Service Overview on page 38](#)

Configuring machine-then-user-at-credprov Credential Provider Authentication for a Junos Pulse Connection

With a machine-then-user-at-credprov connection, Pulse establishes the connection d 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.

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=c4kl.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.

**Related
Documentation**

- [Credential Provider Authentication for Pulse Access Control Service Overview on page 38](#)
- [Machine and User Authentication Through a Pulse Connection for Pulse Access Control Service on page 43](#)

Machine and User Authentication Through a Pulse Connection for Pulse Access Control Service

Junos Pulse supports certificate authentication for establishing Layer 2 and Layer 3 connections. On Windows endpoints, a Pulse client connection accesses client certificates located in the Local Computer personal certificate store to provide machine authentication or user certificates located in a user's personal certificate store or a smart-card for user authentication. A Pulse connection can access certificates from only one location. For information on machine authentication, see [“Machine Authentication for Pulse Access Control Service Overview” on page 33](#).

You can create a Pulse connection that uses System Local, Active Directory, or RSA ACE server authentication to verify the user and a certificate to verify machine identity before establishing a connection. To do so, you must first enable an option for the Pulse connection that allows the connection to check the client certificates located in the Local Computer personal certificate store. The option, **Select client certificate from machine certificate store**, is part of the **User Connection Preferences** of a Pulse connection. User authentication is accomplished through realm authentication. Machine authentication is accomplished as part of a realm certificate restriction because the Pulse connection uses the machine certificate. If the certificate store holds more than one valid certificate for the connection, Pulse opens a dialog box that prompts the user to select a certificate.

The following list summarizes the steps to configure a Pulse connection on a Windows endpoint that authenticates both the user and the machine. For detailed procedures on how to perform each configuration task, see the related documentation links.

- Install a machine authentication certificate in the Local Computer personal certificate store of the Windows endpoint and configure the Pulse server certificate server.
- Create a Pulse connection for the target Pulse server. The connection type can be **UAC (802.1X)** or **SSL VPN or UAC (L3)**. The **Connection is established** option is typically set to **Manually by the user** or **Automatically at user login**.
- In the **User Connection Preferences** section of the connection properties, click the check box labeled **Select client certificate from machine certificate store**. This option enables the Pulse connection to perform the machine authentication as part of the Pulse connection attempt.
- Create a sign-in policy on the Pulse server that specifies a user realm. The realm authentication server can be a System Local, Active Directory, or RSA ACE server.
- Configure a certificate restriction on the realm to enable the Pulse server to request a client certificate. Be sure to enable the option labeled **Only allow users with a client-side certificate signed by Trusted Client CAs to sign in**. Because the Pulse connection is configured to use the machine certificate, the user authentication takes place by means of the realm certificate restriction.

Related Documentation

- [Using the Certificate Server Feature](#)
- [Specifying Client-Side Certificate Restrictions](#)
- [About Sign-In Policies](#)

- Specifying Client-Side Certificate Restrictions

Configuring Location Awareness Rules for Junos Pulse

The location awareness feature enables a Junos Pulse client to recognize its location and then make the correct connection when the connection is set to connect automatically. For example, a Pulse client that is started in a remote location automatically connects to Junos Pulse Secure Access Service. But that same client automatically connects to Pulse Access Control Service 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.

The following location awareness example includes two connections. The first connection is a Pulse Access Control Service connection that resolves to TRUE when the endpoint is connected to the corporate LAN. The second connection is Junos Pulse Secure Access Service connection that resolves to TRUE when the endpoint is located in a remote location.

Pulse Access Control Service connection

If the DNS server that is reachable on the endpoint's physical network interface is one of your organization's internal DNS servers, then establish the connection.

Pulse Secure Access Service connection

If the DNS server that is reachable on the endpoint's physical network interface is not one of your organization's internal DNS servers, and the DNS name of your Pulse Secure Access Service device resolves to the external facing IP address of the Pulse Secure Access Service device, then establish 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.



NOTE: To create a negative location awareness rule, you first create the positive state and then use rule requirement logic to use the rule as a negative condition.

To configure location awareness rules:

1. If you have not already done so, create a connection or open an existing connection.
You can configure location awareness rules for Firewall connections and IC or SA connections. Location awareness rules do not apply to 802.1X or App Acceleration connections.
2. In the Connection is established area, select **According to location awareness rules**, and then click **New**.
3. Specify a name for the 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.

.....

- **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.

5. Click **Save Changes**.

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 Pulse 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**

- [Understanding Session Migration on page 135](#)

Junos Pulse Access Control Service Component Set Options

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



NOTE: Client component options affect Web-based installations only. For a preconfigured installer, specify components as part of the MSIEXEC command. The preconfigured installer for OS X installations always installs all components.

Component set options include the following choices:

- **All components**—Supports all Pulse connection types. The Enhanced Endpoint Security (EES) component, which is available only if you have 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.
- **No components**—Updates existing Pulse client configurations, for example, to add a new connection. Do not use this setting for a new installation.
- **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 Secure Access Service or Pulse Access Control 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. The Host Checker component is included as part of the minimal components configuration.



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: Client component options affect Web-based installations only. For a preconfigured installer, specify components as part of the MSIEXEC command. The preconfigured installer for OS X installations always installs all components.

Related Documentation

- [Junos Pulse Client Installation Overview on page 143](#)
- [Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 150](#)
- [Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 154](#)
- [Creating a Client Component Set for Junos Pulse Access Control Service on page 48](#)

Creating a Client Component Set for Junos Pulse Access Control Service

Client component options affect Web-based installations only. For a preconfigured installer, specify components as part of the MSIEXEC command. The preconfigured installer for OS X installations always installs all components. 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 > Junos Pulse > Connections** and create a new connection set. Or you can use the default client configuration, which permits dynamic connections, supports the outer username anonymous, and allows the client to automatically connect to Pulse Access Control Service or Pulse Secure Access Service.
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 options:
 - **All components**—Includes all Junos Pulse components and supports all access methods and all features.
 - **No components**—Updates existing Pulse client configurations, for example, to add new connections. This option works on endpoints if they already have Pulse installed. Do not use this option if you are installing Pulse.
 - **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 Secure Access Service or Junos Pulse Access Control 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: Client component options affect Web-based installations only. For a preconfigured installer, specify components as part of the MSIEXEC command. The preconfigured installer for OS X installations 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 Client Installation Overview on page 143](#)
- [Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 150](#)
- [Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 154](#)
- [Endpoint Security Monitoring and Management for Pulse Access Control Service on page 49](#)

Endpoint Security Monitoring and Management for Pulse Access Control Service

You can configure Host Checker policies that verify the 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. Host Checker runs on Windows and Windows Mobile endpoints, Apple OS X and iOS endpoints, and on Google Android endpoints. The supported Host Checker features vary on each platform.



NOTE: If a realm has a Host Checker policy enabled that is for desktop clients, and a mobile device user employs a browser on the mobile device to connect to the Web portal, the login is denied because the desktop Host Checker program is not compatible with the mobile client OS. If Pulse mobile users are mapped to multiple roles, the login operation assigns them to a role where Host Checker is not enabled if possible. If all the roles have Host Checker enabled, the mobile users will not be allowed to login from the browser. You can create and enable Host Checker policies that are specific to each mobile operating system and then Host Checker runs when the Pulse client connects to the server.

The Pulse Access Control Service and Host Checker manage the flow of information between the corresponding pairs of 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 Pulse Secure Access Service and verify a particular aspect of a host's integrity. Each IMV works with the corresponding IMC on the client endpoint to verify that the endpoint meets the Host Checker rules. IMCs scan the endpoint frequently for changes in security status. For example, if the user turns off virus checking, the IMC can detect this 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 obtain the most current patch version information from a Juniper staging site. You can manually download and import the list into the Pulse server, or you can automatically import the list from the Juniper staging site or your own staging site at a specified interval.

Monitoring is 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. 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.

When you deploy Junos Pulse, Host Checker is included with the installer. You can invoke Host Checker at the role level or the realm level to specify access requirements for endpoints seeking authentication. Host Checker policies that are implemented at the realm level occur before the user is authenticated. Host Checker policies at the role level are implemented after authentication but before the user is permitted to access protected resources. When an endpoint first connects to Pulse Secure Access Service, the latest version of the IMC downloaded to the host computer. The initial check takes about 10-20 seconds to run. Outdated IMC files are automatically updated at subsequent checks.



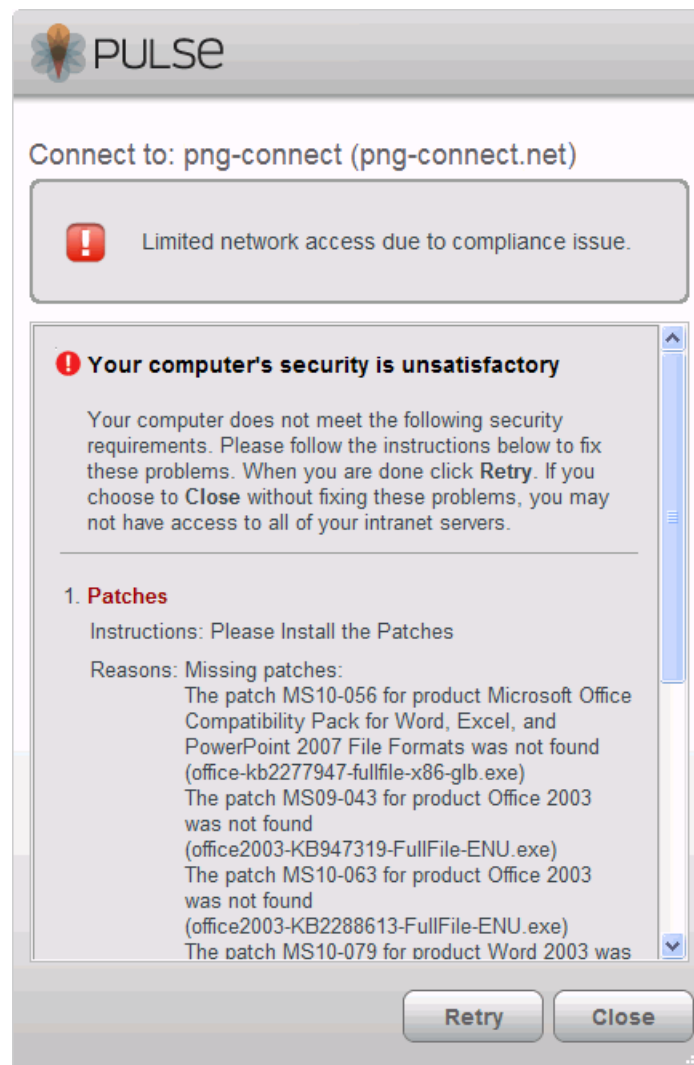
NOTE: The first time an endpoint connects to a Pulse Secure Access Service that has a patch assessment policy, if the connection is a Layer 2 connection, the IMC cannot download. In this case, you should configure a remediation role that displays instructions to direct the user to retry with a Layer 3 connection or to contact the administrator.

Remediation Options

Host Checker can identify issues on an endpoint. However, Host Checker and Pulse Secure Access Service cannot resolve issues, that is, perform remediation tasks, on non-compliant endpoints. To repair those issues Pulse Secure Access Service supports the following remediation options:

- Instructions to the user—The Pulse Secure Access Service can send a message to the user describing the non-compliant patches or software and a link to where the user can obtain the required software. [Figure 4 on page 51](#) shows a typical Pulse remediation message.

Figure 4: Pulse Remediation Instructions



- Initiate SMS/SCCM remediation—For remediation using Microsoft System Center Configuration Manager (ConfigMgr or SCCM), formerly Systems Management Server (SMS), a pre-installed SMS/SCCM client on the endpoint is triggered by Host Checker to get patches from a preconfigured SMS/SCCM server. This mechanism installs only those patches that are published on the SMS/SCCM server.
- Initiate Shavlik remediation—Pulse Access Control Service and UAC Release 4.1 and later supports Shavlik remediation. Shavlik remediation is an optional licensed feature. After running Host Checker, if the endpoint requires remediation, the user can be prompted to install the required patches. You can configure remediation options to be launched automatically. The Shavlik patch deployment engine is downloaded to the endpoint. The engine links to the vendors' patch repositories and installs the patches. [Figure 5 on page 52](#) shows the Pulse client screens that a user sees when the Pulse server is configured with Host Checker and Shavlik remediation. The prompt that allows the user to decide whether to install the patches is a configuration option.

Figure 5: Pulse Client Screens for Shavlik Patch Remediation



- Related Documentation**
- [Issuing a Remediation Message with Junos Pulse Access Control Service on page 53](#)
 - [Using SMS/SCCM Remediation with Junos Pulse Access Control Service on page 54](#)
 - [Configuring Shavlik Remediation with Pulse Access Control Service on page 55](#)
 - [Creating Global Host Checker Policies](#)

Issuing a Remediation Message with Junos Pulse Access Control Service

If a Host Checker policy finds that an endpoint is not in compliance, Host Checker can display a message through the Pulse interface that includes custom instructions and reason strings on how to bring the endpoint into conformance. The user must perform the steps described in the message before the endpoint is allowed to access protected resources.

To enable a remediation message for a Host Checker policy:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. In the **Policies** section, click **New** to create a new Host Checker policy.

For detailed information about Host Checker Rule Settings, see the *Junos Pulse Access Control Service Administration Guide*.

3. As part of the Host Checker Policy, select **Enable Custom Instructions**.

When you select this option, a text box appears. Enter the instructions to display to the user on the Host Checker remediation page. You can use the following HTML tags to format text and to 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.

`Click here to download the latest signature files.`

4. Optionally, select **Send reason strings**. Select this option to display a message to users (called a reason string) that is returned by Host Checker or IMV and that explains why the client machine does not meet the Host Checker policy requirements. Reason strings describe to users what the IMV is checking on the client machine. This option applies to predefined rules, to custom rules, and to third-party IMVs that use extensions in the Juniper Networks TNC SDK.
5. Click **Save Changes**.

Be sure to include the Host Checker policy in the realm or role you configure for Pulse users.

- Related Documentation**
- [Endpoint Security Monitoring and Management for Pulse Access Control Service on page 49](#)
 - [Using SMS/SCCM Remediation with Junos Pulse Access Control Service on page 54](#)
 - [Configuring Shavlik Remediation with Pulse Access Control Service on page 55](#)

Using SMS/SCCM Remediation with Junos Pulse Access Control Service

Junos Pulse supports the SMS/SCCM download method for patch deployment. If the Pulse Access Control Service is configured for the SMS/SCCM method for patch deployment, the Pulse client endpoint must have the SMS/SCCM client already installed on the endpoint, otherwise remediation fails.

Endpoints configured with SMS/SCCM 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/SCCM 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/SCCM update has started.

To configure SMS/SCCM to update the client when notified, set the advertisement time on the SMS/SCCM to As soon as possible.

You assign clients to a particular group or collection on the SMS/SCCM server and then server can advertise patches for that collection. You can configure roles on the Pulse Access Control Service that correspond to collections and SMS/SCCM can send the appropriate patches for a particular role.

You must have the SMS/SCCM client installed and configured correctly on endpoints, and the SMS/SCCM 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/SCCM 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.

You should inform users of the expected behavior if this feature is enabled, as there is no notification to the user until the SMS/SCCM sends back the advertisement.



NOTE: Juniper Networks recommends only one patch deployment on an endpoint at any point in time. However, there is no way to determine if an SMS/SCCM update is in progress, and so it may be possible that the patch deployment engine is started while an SMS/SCCM Update is also occurring. (This scenario is possible if Pulse is connected to two devices with one using SMS/SCCM remediation and the other using the Shavlik patch deployment engine.) Most patches do not allow two instances to be running, so one of the remediation operations will fail.

The admin console allows you to select only one Host Checker patch remediation option (either SMS/SCCM or Shavlik) for all Host Checker policies.

If Pulse is connected to both Pulse Access Control Service and Pulse Secure Access Service, and one uses SMS/SCCM remediation and the other uses Shavlik remediation, both requests are met. If both servers are configured to use Shavlik remediation, the requests are queued.

To enable SMS/SCCM assessment and remediation:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. In the **Policies** section, click **New** to create a new Host Checker policy.
3. Under Patch Remediation Options, select **SMS/SCCM Patch Deployment**.
4. Click **Save Changes**.

Be sure to include the Host Checker policy in the realm or role you configure for Pulse users.

Related Documentation

- [Endpoint Security Monitoring and Management for Pulse Access Control Service on page 49](#)
- [Issuing a Remediation Message with Junos Pulse Access Control Service on page 53](#)
- [Configuring Shavlik Remediation with Pulse Access Control Service on page 55](#)
- [Creating Global Host Checker Policies](#)

Configuring Shavlik Remediation with Pulse Access Control Service

Endpoints with Junos Pulse Release 2.0 or higher that are not in compliance with specified Host Checker patch policies can be updated with the required patches and brought into compliance automatically by the Shavlik patch deployment engine. The Host Checker IMC on the endpoint interfaces with the patch deployment engine to download and install missing patches reported by the IMV. Shavlik software runs on endpoints, downloads specified patches from vendors' Web sites, and installs patches that are required through the Host Checker policy.



NOTE: A license is required for Shavlik patch monitoring and deployment.

The Shavlik patch deployment engine is an executable file that is hosted on the Pulse server and then downloaded to endpoints as part of the Pulse deployment. During a remediation operation, the deployment engine downloads patches directly vendor Web sites so Internet connectivity is needed for Shavlik remediation. The Shavlik patch deployment engine does not work with Layer 2 without Layer 3 connectivity.

All of the files required for patch assessment are a part of a Endpoint Security Assessment Plug-in (ESAP) from the Juniper Networks Customer Support Center ESAP packages beginning with UAC R4.1. The default ESAP package shipped with UAC R4.1 contains the required patch deployment files. Any older ESAP packages fail to update on these devices.

The IMC and IMV software for patch monitoring is backward compatible. Since this feature is available from Pulse Release 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 the Shavlik deployment engine is not invoked for remediation.



NOTE: Juniper Networks recommends only one patch deployment operation on an endpoint at any point in time. However, there is no way to determine if an SMS/SCCM update is in progress, and so it may be possible that the patch deployment engine is started while an SMS/SCCM Update is also occurring. (This scenario is possible if Pulse is connected to two devices with one using SMS/SCCM remediation and the other using the Shavlik patch deployment engine.) Most patches do not allow two instances to be running, so one of the remediation operations will fail.

The admin console allows you to select only one Host Checker patch remediation option (either SMS/SCCM or Shavlik) for all Host Checker policies.

If Pulse is connected to Junos Pulse Secure Access Service and Pulse Access Control Service, and one uses SMS/SCCM remediation and the other uses Shavlik remediation, both requests are met. If both servers are configured to use Shavlik remediation, the requests are queued.

To enable SMS/SCCM assessment and remediation:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. In the **Policies** section, click **New** to create a new Host Checker policy.
3. Under Patch Remediation Options, select **Shavlik Patch Deployment**.
4. To allow users to decide whether to install patch updates, select **Prompt the user for consent before automatic patch deployment**.

Deploying patches can take some time to complete. Some patches require a system reboot.

5. If you enable the user prompt for installing patches, select a default action. The default action runs automatically if the user does not respond to the prompt within 1 minute. Select one of the following default actions:

- **Deploy patches**
- **Do not deploy patches**

6. Click **Save Changes**.

Related Documentation

- [Endpoint Security Monitoring and Management for Pulse Access Control Service on page 49](#)
- [Issuing a Remediation Message with Junos Pulse Access Control Service on page 53](#)
- [Using SMS/SCCM Remediation with Junos Pulse Access Control Service on page 54](#)

- Creating Global Host Checker Policies

Enabling Enhanced Endpoint Security for Junos Pulse Access Control Service

Host Checker includes integrated antispware functionality that can detect and update Windows endpoints. Enhanced Endpoint Security (EES) ensures that malware, spyware, viruses, or worms are not present on endpoints that attempt to connect to Pulse Access Control Service, and that you can restrict or quarantine these endpoints according to your Host Checker policy configuration. When EES is running on an endpoint, the Pulse interface displays a security pane that shows EES status.



NOTE: By default, the base license allows two simultaneous endpoints to use this feature. You can purchase a separate license to enable additional users.

EES scans processes on endpoints, monitors file system write and execution operations, and can automatically update machines that are not in compliance. EES reports threats that are detected but not remediated. In some cases the user might 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 Pulse Access Control Service. Endpoints must have access to the Internet for EES to run successfully. Additionally, if you configure default remediation roles, ensure that endpoints that are directed to remediation roles that can access `*.webroot.com`.

You can configure Pulse Access Control Service to determine the acceptable age of the signature database. The age of the database is the threshold used to determine whether a user can access resources by passing a Host Checker policy. For example, if signatures are 5 days old, and you configure the age as 3 days, the endpoint is allowed to access resources. If you configure the age as 4 days, the endpoint fails the 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 before it connects to Pulse Access Control Service, and you have chosen to implement the option to check for signature age, the policy does 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 access Pulse Access Control Service. To avoid this issue, you should create a default remediation role that allows limited access to the Internet for signature updates at `*.webroot.com`.

Any endpoint that is configured for an EES scan at Layer 2 always fails the check. To permit a network connection, you should configure the realm to reassign users to a remediation VLAN. This allows endpoint users to connect and download the required signature updates, or if connecting for the first time, the EES installer package.

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: If you configure an EES policy for endpoints, a separate EES installer (about 5 MB) is downloaded to endpoints on their first attempt to access resources protected by a Host Checker EES policy. User endpoints are scanned for offending software, and signatures are automatically installed.

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 verify that no spyware is loaded in memory. The download, update, and scan can take significant time to complete.

Any threat detected is automatically remediated by Host Checker and is 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 user of the compliance status.

To enable and use EES antispware:

1. In the admin console, click **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. To set the age of the signature definitions database, select the **Signature definitions should not be older than** check box. Enter the frequency in days (3 - 30). This number determines the maximum permissible age of signatures. It does not change the frequency of updates.
5. To enable an immediate EES scan in the background after allowing the network connection, select the **Install EES and scan endpoints after network connection is established** check box.

Choose this option to allow an immediate connection before the scan takes place. This option allows users to connect and to begin work more quickly. However, this option is less secure because it allows network access before the endpoint has been scanned for malware.

6. 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

- [Endpoint Security Monitoring and Management for Pulse Access Control Service on page 49](#)
- [Issuing a Remediation Message with Junos Pulse Access Control Service on page 53](#)
- [Using SMS/SCCM Remediation with Junos Pulse Access Control Service on page 54](#)

- [Configuring Shavlik Remediation with Pulse Access Control Service on page 55](#)

Pushing Junos Pulse Configurations Between Junos Pulse Servers of the Same Type

You can use the Push Configuration feature to centrally manage Junos Pulse connections, components, and uploaded Pulse packages. The Push Configuration feature enables you to copy all configuration settings or selected configuration settings from one Pulse server to another Pulse server of the same type, for example, from one SA Series SSL VPN Appliance to another SA Series SSL VPN Appliance to another.

The following notes apply to pushing configurations:

- You can push to a single Pulse server or to multiple Pulse servers in one operation. You can push up to 8 targets per push operation. You can run up to 25 push operations simultaneously. The maximum number of targets is 200. If a push to a target Pulse server fails, the operation proceeds to the next target until all identified targets are updated. The results page displays the status and any problems encountered during the process.
- You can push to a Pulse server that is a member of a cluster as long as the target Pulse server is not a member of the same cluster as the source.
- Target Pulse servers can refuse pushed configuration settings. The default is to accept.
- After an update, the target Pulse server restarts its services. Brief interruptions might occur while the service restarts. We recommend that you push to targets when they are idle or when you can accommodate brief interruptions.
- Target Pulse servers do not display a warning message when they receive a pushed configuration.
- The target Pulse server automatically logs out administrators during the push process.
- The source and target Pulse servers must have the same build version and number.
- The administrator account on the source Pulse server must sign in to the target Pulse server without any human intervention. For example, you cannot have dynamic credentials or multiple roles that are not merged as these both require manual interaction.

Before you use Push Configuration, you must configure your system according to the following conditions:

- You must map to the .Administrators role, thereby creating a “super administrator” with full administration privileges. Modify Authentication > Auth Servers > Administrator Server > Users settings to add yourself to the .Administrators role.
- The target Pulse server 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. Modify Administrators > Admin Realms > [Administrator Realm] > General settings to select the proper authentication server for the administrator realm.

- Do not configure the administrator account in a way that requires the administrator to select a role to sign in to the target Pulse server. For example, do not map a single user to multiple roles, including the Push Configuration administrator role, and then fail to 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 the Administrators > Admin Realms > [Administrator Realm] > Role Mapping settings to set the appropriate role-mapping rules.

To push Junos Pulse configurations from one Pulse server to other Pulse servers of the same type:

1. If you have not already done so, define the targets by selecting **Maintenance > Push Config > Targets**.
2. From the admin console, select **Maintenance > Push Config > Push Configuration**.
3. In the What to push box, select **Selected configuration** to display the configuration categories.
4. Scroll down the list and expand the item labeled Junos Pulse.
5. Select the **Select All Configurations** check box to push all Junos Pulse configurations on this Pulse server. Or chose none, all, or selected items from the following categories:
 - **Junos Pulse Connections**—Connection sets and connections.
 - **Junos Pulse Components**—Component sets.
 - **Junos Pulse Versions**—Pulse packages that were uploaded to the Pulse server.
6. Add the targets to the **Selected Targets** box.
7. Click **Push Configuration**.

**Related
Documentation**

- Importing and Exporting Secure Access Service Configuration Files

Enabling or Disabling Automatic Upgrades of the Junos Pulse Client

After you deploy Junos Pulse client software to endpoints, software updates occur automatically. If you upgrade the Pulse client configuration on your Pulse server, updated software components are pushed to a client the next time it connects.



NOTE: When you configure Junos Pulse to make 802.1x based connections, a reboot may be required on Windows XP endpoints when Pulse is upgraded.



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.

Pulse client software upgrades are enabled by default. To change the behavior of Pulse client upgrades:

1. From the admin console, select **Maintenance > System > Options**.
2. Set or clear the **Enable automatic upgrade of Junos Pulse Clients** check box.
3. Click **Save Changes**.

**Related
Documentation**

- [Upgrading Junos Pulse Client Software on page 61](#)

Upgrading Junos Pulse Client Software

The software image for each supported Pulse server includes a Junos Pulse client software package. When a newer version of Pulse is available, you can upload the new software to the Pulse server. You can have more than one version of Pulse on a Pulse server but only one Pulse client package can be active. If you activate a new version of Pulse, and if the Pulse server's automatic upgrade option is enabled, connected Pulse clients display an upgrade prompt to the user. The user can choose to install the upgrade or cancel the operation. If a user cancels, the upgrade prompt appears each time the client connects to the server. During a client software upgrade the Pulse client loses connectivity temporarily.



NOTE: When you configure Junos Pulse to make 802.1x based connections, a reboot may be required on Windows XP endpoints when Pulse is upgraded.

Figure 6: Pulse Client Upgrade Message



After you have staged the new Pulse software package in a location accessible to the Pulse server, use the following procedure to upload the software to the Pulse server:

1. In the device admin console, select **Users > Junos Pulse > Components**.
2. In the section labeled Manage Junos Pulse Client Versions, click **Browse**, and then select the software package.
3. Click **Upload**.

Only one Junos Pulse software package can be active at a time. After you upload a new package, you need to enable it.

To enable a Pulse package as the default:

1. In the admin console, select **Users > Junos Pulse > Components**.
2. In the section labeled Manage Junos Pulse Client Versions, select the radio button next to a version, and then click **Activate**.

**Related
Documentation**

- [Enabling or Disabling Automatic Upgrades of the Junos Pulse Client on page 60](#)

CHAPTER 3

Configuring Junos Pulse Secure Access Service

- [Before You Begin Configuring Junos Pulse Secure Access Service on page 64](#)
- [Junos Pulse Secure Access Service Overview on page 64](#)
- [About Sign-In Notifications on page 66](#)
- [Configuring and Implementing Sign-in Notifications on page 67](#)
- [Configuring a Role for Junos Pulse Secure Access Service on page 69](#)
- [Machine Authentication for Pulse Secure Access Service Overview on page 75](#)
- [Credential Provider Authentication for Pulse Secure Access Service Overview on page 76](#)
- [Configuring user-at-credprov Credential Provider Authentication for a Junos Pulse Connection on page 77](#)
- [Configuring machine-then-user-at-credprov Credential Provider Authentication for a Junos Pulse Connection on page 78](#)
- [Machine and User Authentication Through a Pulse Connection for Pulse Secure Access Service on page 80](#)
- [Configuring Junos Pulse for Secure Application Manager on page 81](#)
- [Pulse Connection Set Options for Pulse Secure Access Service on page 87](#)
- [Junos Pulse Connection Options on page 89](#)
- [Securing the Connection State on the Junos Pulse Client on page 94](#)
- [Creating a Client Connection Set for Junos Pulse Secure Access Service on page 94](#)
- [Configuring Location Awareness Rules for Junos Pulse on page 96](#)
- [Component Set Options for Junos Pulse Secure Access Service on page 98](#)
- [Creating a Client Component Set for Junos Pulse Secure Access Service on page 99](#)
- [Endpoint Security Monitoring and Management for Pulse Secure Access Service on page 101](#)
- [Issuing a Remediation Message with Junos Pulse Secure Access Service on page 105](#)
- [Using SMS/SCCM Remediation with Junos Pulse Secure Access Service on page 105](#)
- [Configuring Shavlik Remediation with Junos Pulse Secure Access Service on page 107](#)
- [Enabling Enhanced Endpoint Security with Junos Pulse Secure Access Service on page 108](#)

- [Pushing Junos Pulse Configurations Between Junos Pulse Servers of the Same Type on page 110](#)
- [Enabling or Disabling Automatic Upgrades of the Junos Pulse Client on page 112](#)
- [Upgrading Junos Pulse Client Software on page 113](#)
- [Integrating iPass Open Mobile with Junos Pulse for Windows Client on page 114](#)
- [Pulse Collaboration Suite Overview on page 115](#)

Before You Begin Configuring Junos Pulse Secure Access Service

Before you begin configuring Junos Pulse, be sure that you have already configured SA Series SSL VPN network settings. Also be sure that you have defined the Authentication settings, including the authentication servers and sign-in settings. The Authentication and Host Checker settings can directly affect a Pulse installation because you can define the conditions that an endpoint must meet to be allowed access to protected resources.

Related Documentation

- [Configuring Secure Access Service](#)
- [Defining a Resource Profile](#)
- [Defining an Authentication Server](#)
- [Defining an Authentication Realm](#)
- [Defining a Sign-In Policy](#)

Junos Pulse Secure Access Service Overview

To enable Junos Pulse Secure Access Service, you configure the service 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 the Pulse client software. You can use one or more of the following 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 Pulse server'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 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.
- Distribute Junos Pulse with no preconfiguration. You can download the default Junos Pulse installation file (.msi format for Windows; .dmg format for Mac) from a Pulse

server, 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 Pulse server. These connections are automatically downloaded to the installed Pulse client when users provide their login credentials to the Pulse server's 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.



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 msixec 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.

The following tasks summarize how to configure Junos 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 Network Connect 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.

Junos Pulse and IVS

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

Related Documentation

- [Creating a Client Connection Set for Junos Pulse Secure Access Service on page 94](#)
- [Configuring a Role for Junos Pulse Secure Access Service on page 69](#)

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 may 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 67](#)

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 66](#)

Configuring a Role for Junos Pulse Secure Access Service

A user role defines session settings and options, personalization settings (user interface customization and bookmarks), and 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 a user can perform Web browsing when the user is connected through the Pulse Secure Access server Web portal. 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.

To create a role for Junos Pulse endpoints:

1. Select **Users > User Roles > New User Role** in the admin console.
2. Enter a name for the role and, optionally, a description. This name appears in the list of roles on the Roles page.
3. Under Client Options, select **Junos Pulse**.

When this option is enabled, the Junos Pulse button appears on the Secure Access Service Web portal. When a user clicks it, Pulse is downloaded and installed on the user's endpoint.

Enabling this option alone does not enable Pulse as the client for the role. This option works in conjunction with the settings you enable in the Access Features section and then configure on the respective role tabs. The combination of settings determines whether you enable Junos Pulse, Junos Pulse for Secure Application Manager (SAM), or Network Connect. The following procedures describe how to enable each client option.

To enable Junos Pulse:

- a. In the role's **General > Overview > Options** section select **Junos Pulse**.

This setting applies to both Windows and Apple OS X versions of Junos Pulse.

- b. In the Access Features section select **VPN Tunneling**.

The VPN Tunneling tab enables you to specify split tunnel behavior, specify the Pulse component set, and enable 3rd-party software integrations.

To enable Junos Pulse for SAM:

- a. In the Options section select **Junos Pulse**.
- b. In the Access Features section select **Secure Application Manager** and then select **Windows version**.

The SAM tab enables you to specify applications and servers secured by SAM.

To enable Network Connect:

- a. In the Options section make sure **Junos Pulse** is disabled.
 - b. In the Access Features section select **VPN Tunneling**.
4. Click **Save Changes**. Role configuration tabs appear.



NOTE: When the Junos Pulse option is enabled and no other access method (VPN Tunneling, WSAM) is enabled, then no client will be delivered.

Configuring General Role Options for Pulse Secure Access Service

The General tab includes options for detailed control of how the client interacts with the server and the network. The following describes the options that apply to Junos Pulse.

General > Restrictions

Source IP—Control from which IP addresses users can access the Web portal sign-in page, be mapped to a role, or access a resource.

Browser—Allow or deny access to the role based on the browser's user agent string.

Certificate—Allow all users or only users with a signed client-side certificate.

Hot Checker—Select configured Host Checker policies to enforce with this role.

General > VLAN/Source IP

VLAN and Select Source IP—To direct traffic to specific sites based on the role, you can define a source IP alias for each role and then use the alias 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 the alias. 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.

General > Session Options

Idle Timeout—The maximum time a session can remain idle (no traffic) before the server ends the session.

Max. Session Length—The maximum time for a session before the server ends the session.

Reminder Time—When the Enable Session Extension feature is enabled, the Reminder Time specifies the number of minutes prior to a session end when the server sends a notice through Pulse and notifies the user that the session will end soon.

Enable Session Extension—Allows the user to extend the session. The user can choose to extend the session at any time by selecting a menu option in the Pulse client interface. If the Session Timeout Warning is selected, a notice message appears when the

Reminder Time is reached and the user can choose to extend the session from within that notice message.

Enable Session Timeout Warning—Enables or disables the session timeout warning, which notifies the user when their Pulse VPN session is close to expiring. The Reminder Time value specifies the point at which the reminder appears.

Roaming Session—Select one of the following options to specify the client's roaming behavior:

- **Enabled**—A roaming session allows a user to retain connectivity when moving a device, such as a laptop with a dynamic IP address, from one subnet to another. Disable this feature to prevent users from accessing a previously established session from a new source IP address. Disabling roaming can help protect against an attack that spoofs a user's session.
- **Limit to Subnet**—Limit the roaming session to the local subnet specified in the endpoint's IP configuration. 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.
- **Disabled**—Disable roaming user sessions for users mapped to this role.

Browser Session Cookie—Select **Enabled** to remove the Secure Access Service session cookie and log users out of their Secure Access Service web session after the Pulse client is launched. Removing the browser session cookie enhances Pulse session security.

General > UI Options

UI Options—The settings on this page define the Pulse Secure Access Service Web portal page.

SAM > Applications

Add Application—We recommend that you use resource profiles to specify the applications available to Pulse for Windows Mobile users, but you can use role and resource policy settings instead.

SAM > Options

Auto-uninstall Secure Application Manager—This feature is not applicable to the Windows Mobile client. Users must download and install Pulse for Windows Mobile before the Windows Mobile device can connect to the Pulse Secure Access Service.

Prompt for username and password for intranet sites—If you enable this option, the Pulse Secure Access Service requires users to enter sign-in credentials before connecting to sites on your internal network. This option changes Internet Explorer's intranet zone setting so that Internet Explorer always prompts the user for network sign-in credentials for an intranet site.

Auto-upgrade Secure Application Manager—This feature is not applicable to the Pulse for Windows Mobile app.

Resolve only host names with domain suffixes in the device DNS domains—If you enable this option, users can only browse to Web sites that are part of their login domain.

Session start script and Session end script—This feature is not applicable to the Pulse for Windows Mobile app.

Configuring Role Options for Pulse Secure Access Service

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

To configure role options for Junos Pulse endpoints:

1. From the admin console, select **Users > User Roles**.
2. Click the role you want to configure and then click the VPN Tunneling tab.
3. Under Split Tunneling Options, select your options:

General VPN Options apply to all layer 3 VPN clients, Junos Pulse, Network Connect, and third-party IKEv2 clients:

- **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.

Juniper Client Options apply only to Junos Pulse and Network Connect:

- **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**—Pulse can monitor the route tables and take appropriate action.

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**—Enables you 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.
- **Multicast**—Enables the multicast feature on the client when this option is selected.
- **Auto-launch**—Activates the Juniper client software automatically when the endpoint is started when this option is selected.

Options for Juniper client on Windows apply only to Junos Pulse and Network Connect on Windows endpoints:

- **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

- **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.
- **Skip if Windows Interactive User Logon Enabled**—Select this option to bypass the specified Windows session start script.

If the client signs in to their Windows Domain via the 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.

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.
4. In the **Session scripts** area, optionally specify a location for the following:
 - **Windows: Session start script**—Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse connects with Pulse Access Control Service. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources. The script must be in a location (either local or on the network) that is accessible by the user.
 - **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 Access Control 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. The script must be in a location (either local or on the network) that is accessible by the user.
 5. Click **Save Changes**.

Configuring Role Options for Host Checker for Pulse Secure Access Service

Host Checker options allow you to enable configured 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. Before you can assign Host Checker policies for a role, you must have already defined the policies.

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

- [Credential Provider Authentication for Pulse Secure Access Service Overview on page 76](#)
- [Configuring Junos Pulse for Secure Application Manager on page 81](#)
- [Machine Authentication for Pulse Secure Access Service Overview on page 75](#)
- [Specifying Role-Based Source IP Aliases](#)

Machine Authentication for Pulse Secure Access Service Overview

Machine authentication uses machine credentials (machine name and password or machine certificate) to authenticate the endpoint. You can enable machine authentication for Pulse Access Control Service as part of a Junos Pulse connection and distribute the connection to endpoints through the normal Pulse distribution methods. You enable Pulse machine authentication support on a Pulse connection, either Layer 2 or Layer 3.

The following describes the requirements for a machine authentication environment:

- 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.
- 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. You can specify a preferred role and realm for the connection, which eliminates realm and role selection dialogs.
- 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.

Pulse supports the following machine authentication types:

- machine-only—The connection is established using machine credentials when no user is logged in. The connection is maintained after user logon.
- user-after-desktopv—The connection is established using machine credentials when no user is logged in. After user logon, the machine connection is disconnected. Once the user logs out, user connection is disconnected and machine connection is reestablished.

Related Documentation

- [Configuring machine-only Machine Authentication for a Junos Pulse Connection on page 34](#)
- [Configuring user-after-desktop Machine Authentication for a Junos Pulse Connection on page 35](#)
- [Credential Provider Authentication for Pulse Secure Access Service Overview on page 76](#)
- [Machine and User Authentication Through a Pulse Connection for Pulse Access Control Service on page 43](#)
- [Creating a Client Connection Set for Junos Pulse Secure Access Service on page 94](#)
- [Configuring a Role for Junos Pulse Secure Access Service on page 69](#)

Credential Provider Authentication for Pulse Secure Access Service Overview

When Microsoft introduced Windows Vista, it moved away from a login integration interface based on GINA (Graphical Identification and Authentication) in favor of credential provider authentication. The Junos Pulse credential provider integration enables connectivity to a network that is required for the user to login 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. Credential provider login is supported on Windows Vista and later Windows platforms.

You can use the Pulse support for credential provider to provide single sign-on capabilities. Pulse establishes a connection to the network and then uses the same credentials to login the Windows domain.

You enable Pulse credential provider support on a Pulse connection, (connection type 802.1X (UAC) or SSL VPN (L3)). After the connection has been downloaded to the endpoint through the normal Pulse distribution methods, Pulse annotates the credential provider tile that appears on the user login screen by adding a Pulse icon in the lower right corner of the tile.

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.

**Related
Documentation**

- [Configuring user-at-credprov Credential Provider Authentication for a Junos Pulse Connection on page 40](#)
- [Configuring machine-then-user-at-credprov Credential Provider Authentication for a Junos Pulse Connection on page 41](#)
- [Pulse Access Control Service and Pulse Secure Access Service Deployment Options on page 19](#)

Configuring user-at-credprov Credential Provider Authentication for a Junos Pulse Connection

With a user-at-credprov connection, the Pulse connection establishes the connection before a 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.

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=c4kl.stnh.mycompany.net; E=ausername@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.

**Related
Documentation**

- [Credential Provider Authentication for Pulse Access Control Service Overview on page 38](#)

Configuring machine-then-user-at-credprov Credential Provider Authentication for a Junos Pulse Connection

With a machine-then-user-at-credprov connection, Pulse establishes the connection 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.

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.

**Related
Documentation**

- [Credential Provider Authentication for Pulse Access Control Service Overview on page 38](#)
- [Machine and User Authentication Through a Pulse Connection for Pulse Access Control Service on page 43](#)

Machine and User Authentication Through a Pulse Connection for Pulse Secure Access Service

Junos Pulse supports certificate authentication for establishing Layer 2 and Layer 3 connections. On Windows endpoints, the Pulse client connection accesses client certificates located in the Local Computer personal certificate store to provide machine authentication or user certificates located in a user's personal certificate store or a smart-card for user authentication. A Pulse connection can access certificates from only one location. For information on machine authentication, see "[Machine Authentication for Pulse Secure Access Service Overview](#)" on page 75.

You can create a Pulse connection that verifies the identity of both the machine and the user before establishing a connection. There are two options for configuring this dual authentication connection. Both options employ user authentication against a Local System, Active Directory, or ACE server for user authentication and certificate authentication to verify the machine. Both options also use a Pulse connection option. The option, Select client certificate from machine certificate store, is part of the User Connection Preferences of a Pulse connection.

Option 1: Use an additional authentication server for a realm:

- Create a Pulse connection for the target Pulse server. The connection type can be **UAC (802.1X)** or **SSL VPN or UAC (L3)**. The **Connection is established** option is typically set to **Manually by the user** or **Automatically at user login**.
- In the **User Connection Preferences** section of the connection properties, click the check box labeled **Select client certificate from machine certificate store**. This option enables the Pulse connection to perform the machine authentication as part of the Pulse connection attempt.
- Create a realm sign in policy that authenticates to a certificate server. When Pulse provides the certificate to the server, it uses the certificate from the Local Computer certificate store, which authenticates the machine. If the certificate store holds more

than one valid certificate for the connection, Pulse opens a dialog box that prompts the user to select a certificate.

- Create a secondary authentication server for the realm. The secondary server can be a Local System, Active Directory, or RSA ACE server. When the machine authentication is successful, the user is prompted to provide authentication credentials for the secondary authentication server.

Option 2 — Use realm authentication to authenticate the user and a certificate restriction on the realm to authenticate the machine.

- Create a Pulse connection for the target Pulse server. The connection type can be **UAC (802.1X)** or **SSL VPN** or **UAC (L3)**. The **Connection is established** option is typically set to **Manually by the user** or **Automatically at user login**.
- In the **User Connection Preferences** section of the connection properties, click the check box labeled **Select client certificate from machine certificate store**.
- Create a sign-in policy on the Pulse server that specifies a user realm. The realm authentication server can be a System Local, Active Directory, or RSA ACE server.
- Configure a certificate restriction on the realm to enable the Pulse server to request a client certificate. Be sure to enable the option labeled **Only allow users with a client-side certificate signed by Trusted Client CAs to sign in**.

**Related
Documentation**

- Certificate Server
- About Configuring Sign In Policies
- Specifying Client-side Certificate Restrictions
- [Junos Pulse Connection Options on page 89](#)

Configuring Junos Pulse for Secure Application Manager

Junos Pulse supports Secure Application Manager (SAM). SAM provides remote access using application names and destinations. SAM does not require a virtual adapter or virtual IP address on the endpoint. SAM provides secure access to client/server applications and thin client solutions without provisioning a VPN tunnel.

With Pulse R3.0 and later, SAM connectivity is provided through SSL VPN (Pulse connection type SSL VPN or UAC (L3)). Prior to Pulse R3.0, SAM connectivity was provided through a separate client. In addition, the Pulse for Windows Mobile app uses SAM to provide access to Windows Mobile smartphones, and that requires a different role. [Table 5 on page 82](#) describes the progression of Pulse/SAM client software.

Table 5: Pulse/SAM Client Version Summary

Pulse/SAM Version	Supported Platforms	Description	Notes
Pulse R1.0 Included with SSL/VPN software R7.0 and R7.1	Windows Mobile Windows XP Windows Vista Windows 7	SAM client that is installed from the Pulse Secure Access server.	Supports Host Checker.
Pulse R2.0	Windows Mobile (6.0, 6.1, and 6.5) Junos Pulse R2.0 is supported on touch-based Windows Mobile devices only.	Pulse for Windows Mobile smartphone app; available for download from juniper.net .	<p>If you install the Pulse 2.0 mobile client on a Windows Mobile device that already has Pulse R1.0, the installation detects the presence of the old client and removes it prior to installing the new client. It also detects and removes Host Checker. Host Checker is not supported.</p> <p>If Pulse R2.0 for Windows Mobile is installed on a Windows Mobile device, the user should not use a browser to sign into a realm that has Pulse R1.0 enabled. Pulse R1.0 cannot detect if Pulse R2.0 for Windows Mobile is already installed, and so it prompts the user to install Pulse R1.0.</p> <p>NOTE: If Pulse R2.0 is installed on a Windows Mobile device, and the user connects to a role that has Host Checker enabled, the user is prompted to install Host Checker. However, if the user allows the installation, nothing happens. To avoid this scenario, you should create a separate role for Pulse R2.0 for Windows Mobile devices.</p> <p>Pulse 2.0 for Windows Mobile supports the optional Pulse Mobile Security Suite.</p>
Pulse R3.0 and later Included with Pulse Secure Access Service software R7.2 and later.	Windows XP Windows Vista Windows 7	Pulse R3.0 incorporates SAM functionality as a native Pulse connection method.	Supports Host Checker.

This section describes how to configure Junos Pulse Secure Access Service to support Windows endpoints. Pulse Secure Access Service also supports a Java-based SAM client (JSAM). The JSAM client can be deployed from a Pulse Secure Access server to any endpoint that supports Java.

To enable SAM for Windows endpoints and configure a role:

1. Log in to the Pulse Secure Access Service admin console.
2. Select **User Roles > New User Role**.

3. On the New Role page, specify a name for the role and, optionally, a description. Make note of the name because later in this procedure, you create a realm and map realm users to this role.
4. In the Options section, select **Junos Pulse**.



NOTE: If you leave the Junos Pulse check box cleared, and then enable Secure Application Manager, Windows version in the Access Features section, you enable the Pulse/SAM for the Pulse for Windows Mobile smartphone app. The Junos Pulse check box must be selected to enable the role for Pulse for Windows endpoints.

5. In the Access Features section of the New Role page, select the **Secure Application Manager** check box and then select **Windows version**.
6. Click **Save Changes** to create the role and to display the role configuration tabs.

The General tab options (Restrictions (which includes Host Checker), VLAN/Source IP, Session Options, and UI Options) are all valid settings for a SAM role.

We recommend that you use resource profiles to specify the applications available to users, but you can use role settings instead.

To specify applications for SAM to secure as part of a role:

1. Open the role you created for Pulse/SAM.
2. Click the SAM tab.
3. In the Applications section, click **Add Application** or select an existing application in the list and then click **Add Duplicate**.
4. In the Details section, select a type from the Type list, and then specify a name and description.

If you select **Custom** to specify an application that is not included in the list, the Application Parameters section appears. Specify the following:

- **Filename**—Specify the name of the file's executable file
- **Path**—Specify the file's path
- **MD5 Hash**—Optionally specify the MD5 hash of the executable file. If you enter an MD5 hash value, Pulse verifies that the checksum value of the executable matches this value. If the values do not match, Pulse notifies the user that the identity of the application could not be verified and does not allow access.

If you select **Pick a Resource Profile**, and at least one application or destination has been configured as a Resource Profile SAM client application, a selection list appears and you can click a Resource Profile. Then, when you click **Save Application** or **Save + New**, the role is added to the profile's list of roles, and the profile's resource polices

are updated. If there are no Resource Profile SAM client applications or destinations configured, this option is not available.

5. Click **Save Application** or **Save + New**.

To specify servers for SAM to secure as part of a role:

1. Open the role you created for Pulse/SAM.
2. Click the SAM tab.
3. In the Applications section, click **Add Server** or select an existing server in the list and then click **Add Duplicate**.

If you select Standard, specify a name and a description, and then identify the server by name or IP address.

If you select **Pick a Resource Profile**, a selection list appears and you can click a Resource Profile. Then, when you click **Save Application** or **Save + New**, the role is added to the profile's list of roles, and the profile's resource policies are updated.

4. Click **Save Application** or **Save + New**.

To specify options for the SAM role:

1. Open the role you created for Pulse/SAM.
2. Click the SAM tab.
3. Click **Options**.
4. Make sure **Windows SAM** is enabled, and then choose from the following:
 - Secure Application Manager options:
 - Auto-launch Secure Application Manager—If you enable this option, Pulse Secure Access Service automatically launches Secure Application Manager services when a user signs in through the Secure Access Service Web portal. If you do not select this option, users must manually start the Secure Application Manager from the Client Applications Sessions section of the Web portal.
 - Auto-allow application servers—If you enable this option, Pulse Secure Access Service automatically creates a SAM resource policy that allows access to the servers specified for the role in the SAM tab application and server lists.
 - Windows SAM Options:
 - Auto-uninstall Secure Application Manager—This setting is not applicable to Pulse R3.0 or later. It applies to the previous WSAM client software only. If you enable it, it is ignored for connections that use Pulse R3.0 or later.
 - Prompt for username and password for intranet sites—If you enable this option, the Pulse Secure Access Service requires users to enter sign-in credentials before connecting to sites on your internal network. This option changes Internet Explorer's intranet zone setting so that Internet Explorer always prompts the user for network sign-in credentials for an intranet site.

- Auto-upgrade Secure Application Manager—This setting is not applicable to Pulse R3.0 or later. It applies to the previous WSAM client software only. If you enable it, it is ignored for connections that use Pulse R3.0 or later.
- Resolve only host names with domain suffixes in the device DNS domains—If you enable this option, users can only browse to Web sites that are part of their login domain.
- Session start script and Session end scripts—You can specify a script (.bat, .cmd, or .exe) to run on the user's endpoint after Pulse connects and disconnects. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources when the user connects. The script must be in a location (either local or on the network) that is accessible by the user.

5. Click **Save Changes**.

To use resource profiles to specify the applications available to Junos Pulse users:

1. Create resource profiles that enable access to client applications and destinations and configure the appropriate settings. Select **Users > Resource Profiles > SAM > Client Applications**.
2. Click **New Profile**.
3. From the Type list, select **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, SAM verifies that the checksum value of the executable matches this value. If the values do not match, SAM notifies the user that the identity of the application could not be verified and does not forward connections from the application to the server.
 - Lotus Notes—Select this option to have SAM intermediate traffic from the Lotus Notes fat client application.
 - Microsoft Outlook—Select this option to have SAM intermediate traffic from the Microsoft Outlook application.
 - NetBIOS file browsing—Select this option to have SAM intercept NetBIOS name lookups in the TDI drivers on ports 137 and 139.
 - Citrix—Select this option to have SAM intermediate traffic from 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 Pulse Secure Access Service in the WSAM Destination list so that LDAP and Kerberos traffic can be proxied and sent to the Pulse server.
 - Configure a WSAM Access Control Policy to allow access to all domain controllers.



NOTE: You can 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.

5. Enter a unique name and optionally a description for the resource profile.
6. In the **Autopolicy: SAM Access Control** section create supporting auto policies and assign the policies to the role:
 - a. If it is not already enabled, select the **Autopolicy: SAM Access Control** check box.
 - 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.
 - 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 server also automatically enables the SAM option in the roles General > Overview page for all of the roles you select.
9. Click **Save Changes**.
10. Select **Users > User Realms > New User Realm**.
11. Specify a name and, optionally, a description and then click **Save Changes** to create the realm and to display the realm option tabs.
12. On the Role Mapping tab for the realm, create a new rule that maps all users to the role you created earlier in this procedure.

You can also use resource profiles to configure destination servers, network subnets and hosts and then add the resource profile to a role.

To use resource profiles to specify the network endpoints available to Junos Pulse users:

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 host name or IP/netmask pairs. You may also include a port.
5. Select the **Create an access control policy allowing SAM access to this server** check box (enabled by default) to enable access to the server specified in the previous step.
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.

Related Documentation

- [Junos Pulse for Windows Mobile Overview on page 209](#)
- [Configuring Junos Pulse Secure Access Service for Windows Mobile Endpoints on page 211](#)
- Task Summary: Configuring JSAM
- Specifying Role-Based Source IP Aliases

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 logon 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 smartcard 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 or not 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.
- **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 on page 64](#)
- [Creating a Client Connection Set for Junos Pulse Secure Access Service on page 94](#)
- [Junos Pulse Connection Options on page 89](#)

Junos Pulse Connection Options

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

[Table 6 on page 89](#) lists the options available for each connection type.

Table 6: 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 users 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 anonymous@acme.com.</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 users to connect to a non-broadcast wireless network from within the Pulse interface.</p>
Trusted Server List for 802.1X Connection	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.

Table 6: 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/ 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—This option 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—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.</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 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 (host name or IP address) of the firewall.</p>
	<p>Allow user to override connection policy—Allows users 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 a 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 into 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 off, the machine authentication connection is restored.
- **Automatically at user login**—This option enables Pulse client interaction with the credential provider software on the endpoint. This option 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, login to the endpoint, and login 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**—This option 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 that enable an endpoint to connect conditionally. For example, the endpoint connects to Pulse Secure Access Service if it is connected to the company intranet or it connects to Junos Pulse Secure Access Service if it is in a remote location.

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 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.

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 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.
- 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 on a Windows endpoint. For more information, see [“Machine and User Authentication Through a Pulse Connection for Pulse Secure Access Service”](#) on page 80

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 (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 on page 44](#)
- [Creating a Client Connection Set for Junos Pulse Secure Access Service on page 94](#)
- [Preferred Realm and Role for Junos Pulse Machine Authentication on page 36](#)
- [Machine and User Authentication Through a Pulse Connection for Pulse Secure Access Service on page 80](#)

Securing the Connection State on the Junos Pulse Client

To disable user interaction with Pulse connections on the endpoint, you can configure Junos Pulse connections so that when they are deployed to the endpoint, users cannot shut down a connection, suspend or resume a connection to Pulse Secure Access Service, or shut down Pulse. Disabling user interaction with Pulse enables the Pulse administrator to control how endpoints connect to the network without allowing the user to override administrative control. For example, if you use machine authentication, the connection from endpoint to server is established automatically. By locking down the Pulse endpoint, users cannot change their connection.

To secure the Pulse endpoint from the Pulse Access Control server:

1. Click **Users > Junos Pulse Connections**.
2. Edit or create a new connection.
3. Disable the check box labeled **Allow user to override connection policy**.

**Related
Documentation**

- [Client Connection Set Options for Junos Pulse Access Control Service on page 24](#)
- [Endpoint Security Monitoring and Management for Pulse Access Control Service on page 49](#)
- [Machine Authentication for Pulse Access Control Service Overview on page 33](#)

Creating a Client Connection Set for Junos Pulse Secure Access Service

To create a Junos Pulse connection:

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



NOTE: You must enter a connection set name before you can create connections.

4. Click **Save Changes**.
5. From the main Junos Pulse Connections page, select the connection set.
6. Under Options, select or clear the following check boxes:
 - **Allow saving logon information**—Controls whether the Save Settings check box is available in logon 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.
 - **Allow user connections**—Controls whether connections can be added by the user through the Pulse client interface.
 - **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 or not users can opt to trust unknown certificates. If you select this check box, a user can ignore warnings about invalid certificates and connect to the target Pulse server.
 - **Dynamic connections**—Allows new connections to be added automatically to a Junos Pulse client when it encounters new Pulse servers through the Web browser.
 - **Wireless suppression**—Disables wireless access when a wired connection is available. Wireless suppression occurs only when the wired connection is connected and authorized.
7. Under Connections, click **New** to define a new connection.
8. Enter a name and, optionally, a description for this connection.
9. Select a type for the connection and then specify the connection . Type can be any of the following:
 - **UAC (802.1X)**—Select this type if the connection establishes connectivity to an 802.1X wired or wireless device.
 - **SSL VPN or UAC (L3)**—Select this type to define a connection for Pulse Secure Access Service or Pulse Access Control Service.
 - **SRX**—Select this type to define a connection to an SRX Series Services Gateway.
 - **App Acceleration**—Select this type to define a connection to the Pulse Application Acceleration Service.

The connection configuration options that appear depend on the connection type you select.
10. After you have created the client connection set, create a client component set and select this connection set.

Related Documentation

- [Component Set Options for Junos Pulse Secure Access Service on page 98](#)
- [Endpoint Security Monitoring and Management for Pulse Secure Access Service on page 101](#)
- [Configuring Location Awareness Rules for Junos Pulse on page 44](#)

Configuring Location Awareness Rules for Junos Pulse

The location awareness feature enables a Junos Pulse client to recognize its location and then make the correct connection when the connection is set to connect automatically. For example, a Pulse client that is started in a remote location automatically connects to Junos Pulse Secure Access Service. But that same client automatically connects to Pulse Access Control Service 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.

The following location awareness example includes two connections. The first connection is a Pulse Access Control Service connection that resolves to TRUE when the endpoint is connected to the corporate LAN. The second connection is Junos Pulse Secure Access Service connection that resolves to TRUE when the endpoint is located in a remote location.

Pulse Access Control Service connection

If the DNS server that is reachable on the endpoint's physical network interface is one of your organization's internal DNS servers, then establish the connection.

Pulse Secure Access Service connection

If the DNS server that is reachable on the endpoint's physical network interface is not one of your organization's internal DNS servers, and the DNS name of your Pulse Secure Access Service device resolves to the

external facing IP address of the Pulse Secure Access Service device, then establish 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.



NOTE: To create a negative location awareness rule, you first create the positive state and then use rule requirement logic to use the rule as a negative condition.

To configure location awareness rules:

1. If you have not already done so, create a connection or open an existing connection.
You can configure location awareness rules for Firewall connections and IC or SA connections. Location awareness rules do not apply to 802.1X or App Acceleration connections.
2. In the Connection is established area, select **According to location awareness rules**, and then click **New**.
3. Specify a name for the 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.

.....

- **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.

5. Click **Save Changes**.

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 Pulse 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**

- [Understanding Session Migration on page 135](#)

Component Set Options for Junos Pulse Secure Access Service

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 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: 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.

Related Documentation

- [Creating a Client Connection Set for Junos Pulse Secure Access Service on page 94](#)

Creating a Client Component Set for Junos Pulse Secure Access Service

Client component options affect Web-based installations 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. To create a Pulse 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 > Junos Pulse > Connections** and create a new connection set. Or you can use the default client configuration, which permits dynamic connections, supports the outer username anonymous, and allows the client to automatically connect to Pulse Access Control Service or Pulse Secure Access Service.

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 options:
 - **All components**—Includes all Junos Pulse components and supports all access methods and all features.
 - **No components**—Updates existing Pulse client configurations, for example, to add new connections. This option works on endpoints if they already have Pulse installed. Do not use this option if you are installing Pulse.
 - **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**

- [Component Set Options for Junos Pulse Secure Access Service on page 98](#)

- [Creating a Client Connection Set for Junos Pulse Secure Access Service on page 94](#)

Endpoint Security Monitoring and Management for Pulse Secure Access Service

You can configure and enable Host Checker policies to perform an endpoint security assessment before allowing the endpoint to connect. Host Checker is supported on the following operating systems:

- Windows
- Mac OS X
- Google Android
- Apple iOS
- Windows Mobile

You can invoke Host Checker at the role level or the realm level to specify access requirements for endpoints seeking authentication. Host Checker policies that are implemented at the realm level occur before the user is authenticated. Host Checker policies at the role level are implemented after authentication but before the user is permitted to access protected resources. When an endpoint first connects to Pulse Secure Access Service, the latest version of the IMC is downloaded to the host computer. The initial check can take 10-20 seconds to run. Outdated IMC files are automatically updated at subsequent checks.



NOTE: The first time an endpoint connects to Pulse Secure Access Service that has a patch assessment policy, if the connection is a Layer 2 connection, the IMC 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 to contact the administrator.



NOTE: If a realm has a Host Checker policy enabled that is for desktop clients, and a mobile device user employs a browser on the mobile device to connect to the Web portal, the login is denied because the desktop Host Checker program is not compatible with the mobile client OS. If Pulse mobile users are mapped to multiple roles, the login operation assigns them to a role where Host Checker is not enabled if possible. If all the roles have Host Checker enabled, the mobile users will not be allowed to login from the browser. You can create and enable Host Checker policies that are specific to each mobile operating system and then Host Checker runs when the Pulse client connects to the server.

For patch management on Windows systems, 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. server and Host Checker manage the

flow of information between the corresponding pairs of TNC-based integrity measurement collectors (IMCs) and integrity measurement verifiers (IMVs). IMCs are software modules that run on the endpoint and collect information such as antivirus, antispysware, patch management, firewall, and other configuration and security information about the host. IMVs are software modules that run on the server and verify a particular aspect of a host's integrity. Each IMV works with the corresponding IMC on the client endpoint to verify that the endpoint meets the Host Checker rules. IMCs scan the endpoint frequently for changes in security status. For example, if the user turns off virus checking, the IMC can detect this 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 obtain the most current patch version information from a Juniper staging site. You can manually download and import the list into the SA Series Appliance, or you can automatically import the list from the Juniper staging site or your own staging site at a specified interval.

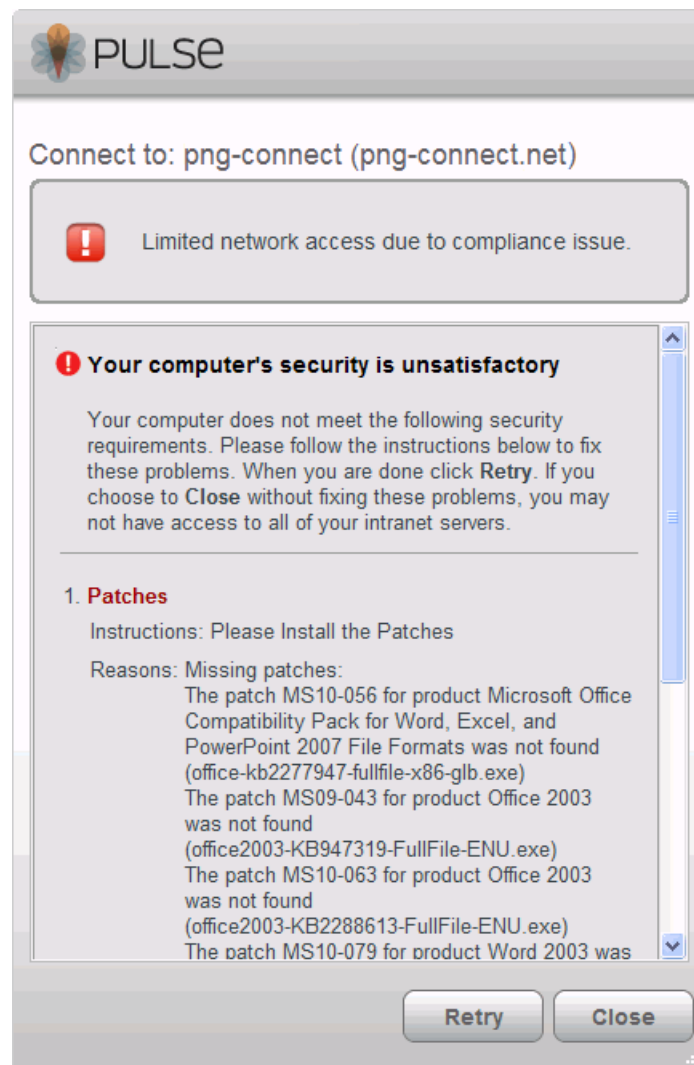
Monitoring is based on one or more specified products or on specific patches, though not in the same policy. For example, you could check for Internet Explorer Version 7 with one policy, and Patch MSOO-039: SSL Certificate Validation Vulnerabilities with a second policy. Then, apply both policies to endpoints at the role or realm level to ensure that the user has the latest browser version with a specific patch. 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.

Remediation Options

Host Checker can identify issues on an endpoint. However, Host Checker and Pulse Secure Access Service cannot resolve issues, that is, perform remediation tasks, on non-compliant endpoints. To repair those issues Pulse Secure Access Service supports the following remediation options:

- Instructions to the user— server can send a message to the user describing the non-compliant patches or software and a link to where the user can obtain the required software. [Figure 7 on page 103](#) shows a typical Pulse remediation message.

Figure 7: Pulse Remediation Instructions



- Initiate SMS/SCCM remediation—For remediation using Microsoft System Center Configuration Manager (ConfigMgr or SCCM), formerly Systems Management Server (SMS), a pre-installed SMS/SCCM client on the endpoint is triggered by Host Checker to get patches from a preconfigured SMS/SCCM server. This mechanism installs only those patches that are published on the SMS/SCCM server.
- Initiate Shavlik remediation—SA Series SSL VPN Appliance software version 7.1 and later supports Shavlik remediation. After running Host Checker, if the endpoint requires remediation, the user can be prompted to install the required patches. You can configure remediation options to be launched automatically. The Shavlik patch deployment engine is downloaded to the endpoint. The engine links to the vendors' patch repositories and installs the patches. Shavlik remediation is an optional licensed feature. [Figure 8 on page 104](#) shows the Pulse client screens that a user sees when the Pulse server is configured with Host Checker and Shavlik remediation.

Figure 8: Pulse Client Screens for Shavlik Patch Remediation



- Related Documentation**
- [Issuing a Remediation Message with Junos Pulse Secure Access Service on page 105](#)
 - [Configuring Shavlik Remediation with Junos Pulse Secure Access Service on page 107](#)
 - [Using SMS/SCCM Remediation with Junos Pulse Secure Access Service on page 105](#)
 - [Protecting Against Infected Computers and Other Security Concerns](#)

Issuing a Remediation Message with Junos Pulse Secure Access Service

If a Host Checker policy finds that an endpoint is not in compliance, Host Checker can display a message through the Pulse client interface that includes custom instructions and reason strings on how to bring the endpoint into conformance. The user must perform the steps described in the message before the endpoint is allowed to access protected resources.

To enable a remediation message for a Host Checker policy:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. In the **Policies** section, click **New** to create a new Host Checker policy.
3. As part of the Host Checker Policy, select **Enable Custom Instructions**.

When you select this option, a text box appears. Enter the instructions to display to the user on the Host Checker remediation page. You can use the following HTML tags to format text and to 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.

`Click here to download the latest signature files.`

4. Optionally, select **Send reason strings**. Select this option to display a message to users (called a reason string) that is returned by Host Checker or IMV and that explains why the client machine does not meet the Host Checker policy requirements. Reason strings describe to users what the IMV is checking on the client endpoint. This option applies to predefined rules, to custom rules, and to third-party IMVs that use extensions in the Juniper Networks TNC SDK.
5. Click **Save Changes**.

Be sure to include the Host Checker policy in the realm or role you configure for Pulse users.

- Related Documentation**
- [Configuring Shavlik Remediation with Junos Pulse Secure Access Service on page 107](#)
 - [Using SMS/SCCM Remediation with Junos Pulse Secure Access Service on page 105](#)

Using SMS/SCCM Remediation with Junos Pulse Secure Access Service

Junos Pulse supports the Microsoft System Center Configuration Manager (ConfigMgr or SCCM), formerly Systems Management Server (SMS) download method for patch deployment. If Pulse Secure Access Service is configured for the SMS/SCCM method for

patch deployment, the Pulse client endpoint must have the SMS/SCCM client already installed on the endpoint, otherwise remediation fails.

Endpoints configured with SMS/SCCM 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/SCCM 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/SCCM update has started.

To configure SMS/SCCM to update the client when notified, set the advertisement time on the SMS/SCCM to As soon as possible.

You assign clients to a particular group or collection on the SMS/SCCM server and then server can advertise patches for that collection. You can configure roles that correspond to collections and SMS/SCCM can send the appropriate patches for a particular role.

You must have the SMS/SCCM client installed and configured correctly on endpoints, and the SMS/SCCM 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/SCCM 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.

You should inform users of the expected behavior if this feature is enabled, as there is no notification to the user until the SMS/SCCM sends back the advertisement.



NOTE: Juniper Networks recommends only one patch deployment on an endpoint at any point in time. However, there is no way to determine if an SMS/SCCM update is in progress, and so it may be possible that the patch deployment engine is started while an SMS/SCCM Update is also occurring. (This scenario is possible if Pulse is connected to two devices with one using SMS/SCCM remediation and the other using the Shavlik patch deployment engine.) Most patches do not allow two instances to be running, so one of the remediation operations will fail.

The admin console allows you to select only one Host Checker patch remediation option (either SMS/SCCM or Shavlik) for all Host Checker policies.

If Pulse is connected to more than one Pulse server, and one uses SMS/SCCM remediation and the other uses Shavlik remediation, both requests are met. If both devices are configured to use Shavlik remediation, the requests are queued.

To enable SMS/SCCM assessment and remediation:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. In the **Policies** section, click **New** to create a new Host Checker policy.
3. Under Patch Remediation Options, select **SMS/SCCM Patch Deployment**.
4. Click **Save Changes**.

Be sure to include the Host Checker policy in the realm or role you configure for Pulse users.

**Related
Documentation**

- [Issuing a Remediation Message with Junos Pulse Secure Access Service on page 105](#)
- [Configuring Shavlik Remediation with Junos Pulse Secure Access Service on page 107](#)

Configuring Shavlik Remediation with Junos Pulse Secure Access Service

Endpoints with Junos Pulse 2.0 or higher that are not in compliance with specified Host Checker patch policies can be updated with the required patches and brought into compliance automatically by the Shavlik patch deployment engine. The Host Checker IMC on the endpoint interfaces with the patch deployment engine to download and install missing patches reported by the IMV. Shavlik software runs on endpoints, downloads specified patches from vendors' Web sites, and installs patches that are required through the Host Checker policy. Shavlik is an optional licensed feature.



NOTE: A separate license is required for Shavlik patch monitoring and deployment.

The Shavlik patch deployment engine is an executable file that is hosted on SA Series SSL VPN Appliance and then downloaded to endpoints as part of the Pulse deployment. During a remediation operation, the deployment engine downloads patches directly vendor Web sites so Internet connectivity is needed for Shavlik remediation. The Shavlik patch deployment engine does not work with Layer 2 without Layer 3 connectivity.

All of the files required for patch assessment are a part of a Endpoint Security Assessment Plug-in (ESAP) from the Juniper Networks Customer Support Center ESAP packages beginning with SA Series SSL VPN Appliance software version 7.1.

The IMC and IMV software for patch monitoring is backward compatible. Since this feature is available from Pulse Release 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 the Shavlik deployment engine is not invoked for remediation.



NOTE: Juniper Networks recommends only one patch deployment operation on an endpoint at any point in time. However, there is no way to determine if an SMS/SCCM update is in progress, and so it may be possible that the patch deployment engine is started while an SMS/SCCM Update is also occurring. (This scenario is possible if Pulse is connected to two devices with one using SMS/SCCM remediation and the other using the Shavlik patch deployment engine.) Most patches do not allow two instances to be running, so one of the remediation operations will fail.

The admin console allows you to select only one Host Checker patch remediation option (either SMS/SCCM or Shavlik) for all Host Checker policies.

If the Pulse client is connected to two Pulse servers, and one uses SMS/SCCM remediation and the other uses Shavlik remediation, both requests are met. If both devices are configured to use Shavlik remediation, the requests are queued.

To enable SMS/SCCM assessment and remediation:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. In the **Policies** section, click **New** to create a new Host Checker policy.
3. Under Patch Remediation Options, select **Shavlik Patch Deployment**.
4. To allow users to decide whether to install patch updates, select **Prompt the user for consent before automatic patch deployment**.

Deploying patches can take some time to complete. Some patches require a system reboot.

5. If you enable the user prompt for installing patches, select a default action. The default action runs automatically if the user does not respond to the prompt within 1 minute. Select one of the following default actions:

- **Deploy patches**
- **Do not deploy patches**

6. Click **Save Changes**.

Related Documentation

- [Issuing a Remediation Message with Junos Pulse Secure Access Service on page 105](#)
- [Using SMS/SCCM Remediation with Junos Pulse Secure Access Service on page 105](#)
- [Importing Endpoint Security Assessment Plug-in \(ESAP\) Packages with NSM](#)
- [Host Checker and Trusted Network Computing](#)

Enabling Enhanced Endpoint Security with Junos Pulse Secure Access Service

Host Checker includes integrated antispyware functionality that can detect and remediate Windows endpoints. Enhanced Endpoint Security (EES) ensures that malware, spyware,

viruses, or worms are not present on endpoints that attempt to connect to Pulse Secure Access Service, and that you can restrict or quarantine these endpoints according to your Host Checker policy configuration. When EES is running on an endpoint, the Pulse interface displays a security pane that shows EES status.



NOTE: By default, the base license allows two simultaneous endpoints to use this feature. You can purchase a separate license to enable additional users.

EES scans processes on endpoints, monitors file system write and execution operations, and can automatically remediate machines that are not in compliance. EES reports threats that are detected but not remediated. In some cases the user might 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 the Pulse server. Endpoints must have access to the Internet for EES to run successfully. Additionally, if you configure default remediation roles, ensure that endpoints that are directed to remediation roles that can access `*webroot.com`.

You can configure Pulse Secure Access Service to determine the acceptable age of the signature database. The age of the database is the threshold used to determine whether a user can access resources by passing a Host Checker policy. For example, if signatures are 5 days old, and you configure the age as 3 days, the endpoint is allowed to access resources. If you configure the age as 4 days, the endpoint fails the 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 before it connects to Pulse Secure Access Service, and you have chosen to implement the option to check for signature age, the policy does 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 access Pulse Secure Access Service. To avoid this issue, you should create a default remediation role that allows limited access to the Internet for signature updates at `*webroot.com`.

Any endpoint that is configured for an EES scan at Layer 2 always fails the check. To permit a network connection, you should configure the realm to reassign users to a remediation VLAN. This allows endpoint users to connect and download the required signature updates, or if connecting for the first time, the EES installer package.

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: If you configure an EES policy for endpoints, a separate EES installer (about 5 MB) is downloaded to endpoints on their first attempt to access resources protected by a Host Checker EES policy. User endpoints are scanned for offending software, and signatures are automatically installed.

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 verify that no spyware is loaded in memory. The download, update, and scan can take significant time to complete.

Any threat detected is automatically remediated by Host Checker and is 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 user of the compliance status.

To enable and use EES antispware:

1. In the admin console, click **Authentication > Endpoint Security > Host Checker**.
2. Under Options, select the **Advanced Endpoint Protection: Malware Protection** tab.
3. Select the **Enable Advanced Endpoint Security: Malware Protection** check box.
4. To set the age of the signature definitions database, select the **Signature definitions should not be older than** check box. Enter the frequency in days (3 - 30). This number determines the maximum permissible age of signatures. It does not change the frequency of updates.
5. To enable an immediate EES scan in the background after allowing the network connection, select the **Install EES and scan endpoints after network connection is established** check box.

Choose this option to allow an immediate connection before the scan takes place. This option allows users to connect and to begin work more quickly. However, this option is less secure because it allows network access before the endpoint has been scanned for malware.

6. 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**

- [Issuing a Remediation Message with Junos Pulse Secure Access Service on page 105](#)
- [Configuring Shavlik Remediation with Junos Pulse Secure Access Service on page 107](#)
- [Using SMS/SCCM Remediation with Junos Pulse Secure Access Service on page 105](#)

Pushing Junos Pulse Configurations Between Junos Pulse Servers of the Same Type

You can use the Push Configuration feature to centrally manage Junos Pulse connections, components, and uploaded Pulse packages. The Push Configuration feature enables

you to copy all configuration settings or selected configuration settings from one Pulse server to another Pulse server of the same type, for example, from one SA Series SSL VPN Appliance to another SA Series SSL VPN Appliance to another.

The following notes apply to pushing configurations:

- You can push to a single Pulse server or to multiple Pulse servers in one operation. You can push up to 8 targets per push operation. You can run up to 25 push operations simultaneously. The maximum number of targets is 200. If a push to a target Pulse server fails, the operation proceeds to the next target until all identified targets are updated. The results page displays the status and any problems encountered during the process.
- You can push to a Pulse server that is a member of a cluster as long as the target Pulse server is not a member of the same cluster as the source.
- Target Pulse servers can refuse pushed configuration settings. The default is to accept.
- After an update, the target Pulse server restarts its services. Brief interruptions might occur while the service restarts. We recommend that you push to targets when they are idle or when you can accommodate brief interruptions.
- Target Pulse servers do not display a warning message when they receive a pushed configuration.
- The target Pulse server automatically logs out administrators during the push process.
- The source and target Pulse servers must have the same build version and number.
- The administrator account on the source Pulse server must sign in to the target Pulse server without any human intervention. For example, you cannot have dynamic credentials or multiple roles that are not merged as these both require manual interaction.

Before you use Push Configuration, you must configure your system according to the following conditions:

- You must map to the .Administrators role, thereby creating a “super administrator” with full administration privileges. Modify Authentication > Auth Servers > Administrator Server > Users settings to add yourself to the .Administrators role.
- The target Pulse server 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. Modify Administrators > Admin Realms > [Administrator Realm] > General settings to select the proper authentication server for the administrator realm.
- Do not configure the administrator account in a way that requires the administrator to select a role to sign in to the target Pulse server. For example, do not map a single user to multiple roles, including the Push Configuration administrator role, and then fail to 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 the Administrators > Admin Realms

> [Administrator Realm] > Role Mapping settings to set the appropriate role-mapping rules.

To push Junos Pulse configurations from one Pulse server to other Pulse servers of the same type:

1. If you have not already done so, define the targets by selecting **Maintenance > Push Config > Targets**.
2. From the admin console, select **Maintenance > Push Config > Push Configuration**.
3. In the What to push box, select **Selected configuration** to display the configuration categories.
4. Scroll down the list and expand the item labeled Junos Pulse.
5. Select the **Select All Configurations** check box to push all Junos Pulse configurations on this Pulse server. Or chose none, all, or selected items from the following categories:
 - **Junos Pulse Connections**—Connection sets and connections.
 - **Junos Pulse Components**—Component sets.
 - **Junos Pulse Versions**—Pulse packages that were uploaded to the Pulse server.
6. Add the targets to the **Selected Targets** box.
7. Click **Push Configuration**.

**Related
Documentation**

- Importing and Exporting Secure Access Service Configuration Files

Enabling or Disabling Automatic Upgrades of the Junos Pulse Client

After you deploy Junos Pulse client software to endpoints, software updates occur automatically. If you upgrade the Pulse client configuration on your Pulse server, updated software components are pushed to a client the next time it connects.



NOTE: When you configure Junos Pulse to make 802.1x based connections, a reboot may be required on Windows XP endpoints when Pulse is upgraded.



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.

Pulse client software upgrades are enabled by default. To change the behavior of Pulse client upgrades:

1. From the admin console, select **Maintenance > System > Options**.
2. Set or clear the **Enable automatic upgrade of Junos Pulse Clients** check box.

3. Click **Save Changes**.

Related Documentation

- [Upgrading Junos Pulse Client Software on page 61](#)

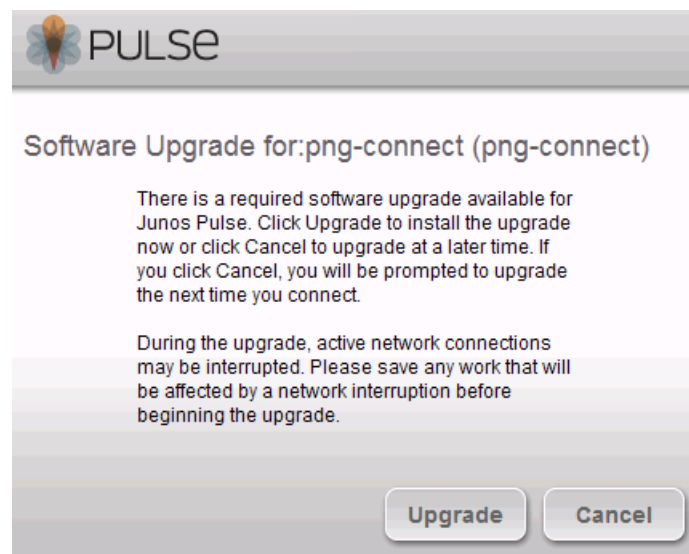
Upgrading Junos Pulse Client Software

The software image for each supported Pulse server includes a Junos Pulse client software package. When a newer version of Pulse is available, you can upload the new software to the Pulse server. You can have more than one version of Pulse on a Pulse server but only one Pulse client package can be active. If you activate a new version of Pulse, and if the Pulse server's automatic upgrade option is enabled, connected Pulse clients display an upgrade prompt to the user. The user can choose to install the upgrade or cancel the operation. If a user cancels, the upgrade prompt appears each time the client connects to the server. During a client software upgrade the Pulse client loses connectivity temporarily.



NOTE: When you configure Junos Pulse to make 802.1x based connections, a reboot may be required on Windows XP endpoints when Pulse is upgraded.

Figure 9: Pulse Client Upgrade Message



After you have staged the new Pulse software package in a location accessible to the Pulse server, use the following procedure to upload the software to the Pulse server:

1. In the device admin console, select **Users > Junos Pulse > Components**.
2. In the section labeled Manage Junos Pulse Client Versions, click **Browse**, and then select the software package.
3. Click **Upload**.

Only one Junos Pulse software package can be active at a time. After you upload a new package, you need to enable it.

To enable a Pulse package as the default:

1. In the admin console, select **Users > Junos Pulse > Components**.
2. In the section labeled Manage Junos Pulse Client Versions, select the radio button next to a version, and then click **Activate**.

**Related
Documentation**

- [Enabling or Disabling Automatic Upgrades of the Junos Pulse Client on page 60](#)

Integrating iPass Open Mobile with Junos Pulse for Windows Client

Junos Pulse Release 2.1 and later supports select third-party software integration. iPass Open Mobile Platform provides reliable, secure and high-performance deployment of iPass enterprise mobility services. Together Pulse and iPass expand secure access options for Windows XP, Windows Vista, and Windows 7 endpoints. Third-party application integration is supported by Junos Pulse Secure Access Service.

iPass Enterprise Mobility Services provide authorized connectivity to public networks for Pulse users. The user can connect to Wi-Fi, Mobile Broadband, or dial networks from the iPass Networks list when on the road. Once the Internet connection has been established, Junos Pulse provides a secure connection to the enterprise resources. iPass Enterprise Mobility Services provides authorized secure access to networks in restaurants, airports and in-flight Wi-Fi hot spots.

To enable application integration, you install an Advanced Connectivity license on the Pulse server. On the endpoint, the user must install iPass Open Mobile client software. The first time the user connects to the Pulse server where the advanced connectivity license is installed and enabled for the role, the license information is passed to the Pulse client, and then the iPass software is automatically integrated within the Pulse Connections pane. After integration, when the user is away from the corporate network, iPass automatically locates and enables connectivity to an authorized network. The user can then use Pulse to establish a VPN connection to the corporate network.

Integrating iPass and Pulse includes the following tasks:

- Install the Advanced Connectivity License on the SA Series SSL VPN Appliance.
- Enable third-party software integration for a role on the server where you installed the license.
- Each Pulse endpoint must install iPass Open Mobile. See your iPass representative for iPass client software.
- Each Pulse endpoint must connect to the role on the Pulse server that is enabled for third-party integration. This initial connection downloads the license information to the Pulse endpoint and enables the Pulse client for integration with iPass. If iPass is already installed on the Pulse endpoint, the iPass interface appears in the Pulse

Connections pane a few moments after Pulse establishes the connection with the Pulse server.

To install the Advanced Connectivity license:

1. On the Pulse server, login as an administrator, and then click **System > Configuration > Licensing**.
2. Paste or type your license key into the License keys box and then click **Add**.

To enable third-party software integration for a role:

1. Click **Users > User Roles > Role Name > Network Connect > Junos Pulse Settings**.
2. Click the check box labeled **Enable 3rd party connectivity integration**.



NOTE: The check box is present only after the Advanced Connectivity License has been installed on the system.

3. Click **Save Changes**.

Related Documentation

- [Introducing Junos Pulse on page 3](#)
- [Configuring License Options](#)

Pulse Collaboration Suite Overview

Junos Pulse Collaboration Suite (formerly Secure Meeting) allows users to schedule and attend secure online meetings. In meetings, users can share their desktops and applications with one another over a secure connection. Meeting attendees can collaborate by enabling remote-control of their desktops and through text chatting. Users can schedule meetings through the Pulse Secure Access Service user Web portal or, if they have the Microsoft Outlook Plug-in installed, through Microsoft Outlook.

In addition to regular meetings, Pulse Collaboration Suite supports Instant Meetings and Support Meetings. Instant meetings allow you to create meetings with static URLs for that particular type of meeting (for example, weekly status meetings). You do not need to schedule these types of meetings. The conductor starts the meeting and the invitees enter the URL to attend the meeting.

You can enable Pulse Collaboration Suite integration as part of a Pulse connection and push the connection to Pulse clients through an installer package or a configuration update. The SSL VPN or UAC (L3) connection type includes a check box that enables Pulse Collaboration integration on the connection. When the check box is selected, Pulse clients that have installed that connection display new menu items that enable users to access Pulse Collaboration Suite functions. A connection that is enabled for meetings can serve as a normal SSL VPN connection or it can be dedicated to meetings only. When a Pulse user clicks the tray icon menu item for meetings, Pulse launches a browser window and connects to the server's user Web portal.

Task Summary: Configuring Pulse Collaboration Suite on the Pulse Secure Access Server

The following summarizes how to enable a Pulse Secure Access server as a meeting server for Pulse Collaboration Suite meetings.

To configure Pulse Collaboration Suite:

1. In the Pulse Secure Access server admin console, click **System > Network > Overview** and specify a network identity for the server. Pulse Collaboration Suite uses this host name when constructing meeting URLs for e-mail notifications.
2. Configure role-level settings:
 - To enable Pulse Collaboration Suite at the role level, click **Users > User Roles > Role Name > General**.
 - To configure role-level meeting restrictions, click **Users > User Roles > Role Name > Meetings > Options**.
3. Configure the authentication settings:
 - To specify the authentication servers meeting creators can access and search click **Users > User Roles > Role Name > Meetings > Auth Servers**.
 - To allow meeting creators to invite users from an LDAP server, click **Authentication > Auth. Servers > Select LDAP Server > Meetings**.
4. Configure meeting sign-in policies:
 - To customize the user Web portal pages that meeting attendees see when they sign into a meeting, click **Authentication > Signing In > Sign-in Pages**.
 - To define the URL that meeting participants use to join a meeting, click **Authentication > Signing In > Sign-in Policies > Meeting Policy**. You also use this page to associate a meeting page with the URL.
 - To associate your meeting sign-in policy with a user sign-in policy, click **Authentication > Signing In > Sign-in Policies > User Policy**. The Pulse Secure Access server applies the specified meeting URL to any meeting created by a user who signs into the associated user URL.
5. To configure system-level meeting settings, include session time-outs, SMTP server information, time zone settings, and color-depth settings, click **System > Configuration > Pulse Collaboration Suite** page of the admin console.
6. To enable client-side logging, click **System > Log/Monitoring > Client Logs > Settings**.
7. To view the logs that users push to the Pulse server, click **System > Log/Monitoring > Uploaded Logs**.

Configuring Pulse Connections to Support Meetings

When you configure a Junos Pulse connection to support Pulse Collaboration Suite meetings, Pulse users on Windows endpoints can access meeting functions from the Junos Pulse tray icon. When the user clicks Start Meeting in the tray icon menu, Pulse launches a browser window that provides access to the meeting functions. The browser

shows the Meetings page of the server's user Web portal, which a user can also access by using a browser to login to the Pulse Secure Access server.

The tray icon for Pulse Collaboration Suite access is available when a Pulse connection is enabled as a meeting server connection. Pulse users cannot enable the meeting function for a connection. This task must be performed by the Pulse administrator on a connection defined on the server, and then installed on endpoints through normal methods of distributing and updating Pulse client software.

The following steps summarize how to create a Pulse connection that enables Pulse Collaboration Suite functions.

1. In a Pulse connection set, create a new Pulse connection or edit an existing connection set.

Pulse Collaboration Suite is available with SSL VPN connections (connection type SSL VPN or UAC (L3)) only.

2. Select the check box labeled **Enable Junos Pulse Collaboration integration on this connection**.
3. Distribute the connection to endpoints through normal methods of distributing and updating Pulse client software.

Scheduling Meetings Through the Pulse Secure Access Service User Web Portal

If you enable meeting creation abilities at the role level, users can create meetings through the Meetings page of the Pulse Secure Access Service user Web portal. The user scheduling the meeting 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, the user must categorize all invitees into one of two categories:

- Pulse Secure Access Service invitees—A user who signs into the same Secure Access server or cluster as the meeting creator, also called an in-network invitee. When inviting an in-network user to a meeting, the meeting creator must specify the user's username and authentication server.
- Non-Pulse Secure Access Service invitees—A user who signs into a different Secure Access server or cluster as the meeting creator, also called an out-of-network invitee. When inviting an out-of-network user to a meeting, the meeting creator must specify the user's email address.



NOTE: If an in-network invitee uses the meeting URL instead of the Meetings page in the Pulse Secure Access Service user Web portal to join a meeting, Pulse Collaboration Suite classifies the user as an out-of-network invitee.

Scheduling Meetings Through Microsoft Outlook

If you enable meeting creation abilities at the role level, Pulse Secure Access Service users can create meetings through the Microsoft Outlook calendar using the Pulse Collaboration Suite Outlook plug-in.

When installing the Pulse Collaboration Suite plug-in on Microsoft Outlook 2000, the following message appears, “The form you are installing may contain macros.” Since the Pulse Collaboration Suite form does not contain macros it does not matter whether you click Disable Macros or Enable Macros.



NOTE: You must use the same Outlook profile to remove the Pulse Collaboration Suite 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.

To use this plug-in, the user must:

1. Install the plug-in from the Meetings page in the Pulse Secure Access Service user Web portal.
2. Open the Pulse Collaboration Suite scheduling form in Outlook by choosing **New > Pulse Collaboration Suite**.
3. Use the Pulse Collaboration Suite tab to enter details about the Pulse Secure Access server on which the meeting should be scheduled as well as the user's sign-in credentials, realm, and a meeting password.



NOTE: Due to limitations with Microsoft Outlook, not all meeting details cross-populate between Microsoft Outlook and Pulse Secure Access Service. For a complete list of restrictions, see the Pulse Collaboration Suite for Outlook information available from the user help system available on the Pulse Secure Access Service user Web portal as well as the Pulse Collaboration Suite for Outlook plug-in installer.

4. Use the Scheduling and Appointment tabs to schedule the meeting and add invitees using standard Outlook functionality. Note that Pulse Collaboration Suite supports creating standard or recurring meetings through Outlook.



NOTE: The Appointment tab has a check box labeled **This is an online meeting using**. This check box is not related to the Meeting Server or the Pulse Collaboration Suite Outlook Plug-in and cannot be used by a third-party plug-in.

5. Save the calendar entry to send the information to the Pulse Collaboration Suite 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 e-mails to the invitees using the text and meeting URL link constructed by the Pulse Collaboration Suite 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 Pulse Collaboration Suite tab containing the information specified by the meeting creator in the Pulse Collaboration Suite tab. Note that the Pulse Secure Access server does not send an additional e-mail using the SMTP server.
7. To delete a meeting, click **Delete Meeting from Server** on the Pulse Collaboration Suite tab. Clicking Delete from the Outlook form does not delete the meeting.

**Related
Documentation**

- Task Summary: Configuring Junos Pulse Collaboration
- Scheduling Meetings Through the Secure Access Service End-User Console

CHAPTER 4

Configuring Junos Pulse on SRX Series Gateways

- [Junos Pulse and SRX Series Gateways on page 121](#)
- [Junos Pulse and Dynamic VPN Configuration Overview on page 122](#)

Junos Pulse and SRX Series Gateways

The dynamic virtual private network (VPN) feature of SRX Series gateways simplifies remote access by enabling users to establish Internet Protocol Security (IPsec) VPN tunnels without having to manually configure VPN settings on their endpoints. Junos Pulse supports dynamic VPN connectivity to SRX Series gateways. The VPN settings are part of a Pulse SRX connection. Depending on the version of Junos OS on the SRX gateway, you might be able to deploy Pulse to endpoints from the SRX Series gateway through a Web portal. A remote client accesses the Web portal and, after being authenticated, downloads and installs Pulse. The installation includes a Pulse connection to the SRX Series gateway. Alternatively, you can create and deploy firewall connections from Pulse Access Control Service and Pulse Secure Access Service. See the *Junos Pulse Supported Platform Guide* for details on the Junos OS versions that are able to deploy Pulse.

To configure a firewall access environment for Pulse clients, you must configure the VPN settings on the SRX Series gateway and create and deploy an SRX connection on the Junos Pulse client.



NOTE: Junos Pulse for mobile devices can access Pulse Secure Access Service only.

For SRX Series gateways that cannot deploy Junos Pulse client software, you have the following configuration and deployment options:

- In an environment that includes Pulse Secure Access Service and Pulse Access Control Service, create connections of the type SRX with a target address of your SRX Series Services gateway. Users could then install the Junos Pulse client software and the connection configurations by logging in to the Web portal of the Pulse Secure Access Service or Pulse Access Control Service and being assigned to a role that installs Junos

Pulse. After the installation, the endpoint has the Junos Pulse client software and the connection information required to connect to the SRX Series Services gateways.

- Install the default Junos Pulse software package, and then have users create new connections that point to the SRX Series gateway.

SRX Series gateways supported an earlier access client called Juniper Networks Access Manager. You must uninstall Access Manager before you deploy Junos Pulse to endpoints. The Pulse installation program checks for Access Manager. If Access Manager is present, the program displays a message instructing the user to uninstall Access Manager before installing Pulse.

**Related
Documentation**

- [Junos Pulse and Dynamic VPN Configuration Overview on page 122](#)

Junos Pulse and Dynamic VPN Configuration Overview

A dynamic VPN allows administrators to provide IPsec access for Windows endpoints to a Pulse server on a Juniper Networks device while also providing a way to distribute the Dynamic VPN software to remote clients through the use of a Web portal.

The following procedure lists the tasks for configuring a dynamic VPN. For detailed information on these topics, see the Junos OS documentation.

1. Configure authentication and address assignment for the remote clients:
 - a. Configure an XAuth profile to authenticate users and assign addresses. You can use local authentication or an external RADIUS server. Use the **profile** configuration statement at the **[edit access]** hierarchy level to configure the XAuth profile.

To use the XAuth profile for Web authentication, use the **web-authentication** configuration statement at the **[edit access firewall-authentication]** hierarchy level.
 - b. Assign IP addresses from a local address pool if local authentication is used. Use the **address-assignment pool** configuration statement at the **[edit access]** hierarchy level. A subnet or a range of IP addresses can be specified. IP addresses for DNS and WINS servers may also be specified.
2. Configure the VPN tunnel:
 - a. Configure the IKE policy. The mode must be aggressive. Basic, compatible, or standard proposal sets may be used. Only preshared keys are supported for phase 1 authentication. Use the **policy** configuration statement at the **[edit security ike]** hierarchy level.
 - b. Configure the IKE gateway. Either shared or group IKE IDs can be used. You can configure the maximum number of simultaneous connections to the gateway. Use the **gateway** configuration statement at the **[edit security ike]** hierarchy level.
 - c. Configure the IPsec VPN. Basic, compatible, or standard proposal sets may be specified with the **policy** configuration statement at the **[edit security ipsec]** hierarchy level. Use the **vpn** configuration statement at the **[edit security ipsec]** hierarchy level to configure the IPsec gateway and policy.

- d. Configure a security policy to allow traffic from the remote clients to the IKE gateway. Use the **policy** configuration statement at the **[edit security policies from-zone zone to-zone zone]** hierarchy level.



NOTE: The placement of this security policy is important. You must place it above more specific, non-VPN policies so that traffic that is intended to be sent over the VPN tunnel is processed correctly.

- e. Configure host inbound traffic to allow specific traffic to reach the device from systems that are connected to its interfaces. For example, IKE and HTTPS traffic must be allowed.
 - f. (Optional) If the client address pool belongs to a subnet that is directly connected to the device, the device would need to respond to ARP requests to addresses in the pool from other devices in the same zone. Use the **proxy-arp** configuration statement at the **[edit security nat]** hierarchy level. Specify the interface that directly connects the subnet to the device and the addresses in the pool.
3. Associate the dynamic VPN with remote clients:
 - a. Specify the access profile for use with dynamic VPN. Use the **access-profile** configuration statement at the **[edit security dynamic-vpn]** hierarchy level.
 - b. Configure the clients who can use the dynamic VPN. Specify protected resources (traffic to the protected resource travels through the specified dynamic VPN tunnel and is therefore protected by the firewall's security policies) or exceptions to the protected resources list (traffic that does not travel through the dynamic VPN tunnel and is sent in clear text). These options control the routes that are pushed to the client when the tunnel is up, therefore controlling the traffic that is sent through the tunnel. Use the **clients** configuration statement at the **[edit security dynamic-vpn]** hierarchy level.

Related Documentation • [Junos Pulse Client Installation Overview on page 143](#)

CHAPTER 5

Configuring Junos Pulse Application Acceleration Service

This chapter describes how to install and manage the Junos Pulse Application Acceleration Service.

- [Installing the Junos Pulse Client on page 125](#)
- [Managing Software, Configurations, and Policies on page 128](#)

Installing the Junos Pulse Client

Mobile and remote Windows users can obtain the benefits of application acceleration by installing the Junos Pulse client. The Junos Pulse client accelerates traffic between the client system and a remote Junos Pulse Application Acceleration Service gateway, provided the gateway is installed in the network path. The gateways and Pulse clients discover each other automatically and begin accelerating traffic without user intervention.

The Junos Pulse client can be installed from a Pulse Secure Access server or from a Pulse Application Acceleration server. Installing the Pulse client from the Pulse Secure Access server is recommended. The Pulse Secure Access server can be configured to download and install the Pulse client automatically when a user accesses the server.



NOTE: You must install the Junos Pulse client on each Windows client, not on a single Windows system that serves as a gateway for other clients.

The following sections describe how to install the Junos Pulse client:

- [Configuring Personal Firewalls for Junos Pulse Acceleration on page 126](#)
- [Downloading the Junos Pulse Client from a Pulse Secure Access Server on page 126](#)
- [Downloading the Junos Pulse Client from a Pulse Application Acceleration Gateway on page 127](#)
- [Uninstalling the Junos Pulse Client on page 128](#)

Configuring Personal Firewalls for Junos Pulse Acceleration

Personal firewalls can block connections (adjacencies) between the Pulse client and the Junos Pulse Application Acceleration Service gateway in the network path. The firewall must allow the connection software on the Pulse client (WxConnectionMethod) to receive inbound UDP packets on port 3578. The firewall policies can be changed in either of two ways:

- Administrators can create and distribute a firewall exception to users through a centrally managed firewall system.
- Users can modify the personal firewall on the client.

Some personal firewalls are updated automatically when the Pulse client is installed. [Table 7 on page 126](#) summarizes the configuration required for several common firewall systems. The version number indicates the version that has been verified by Juniper Networks.

Table 7: Personal Firewall Exceptions for Pulse Acceleration

Firewall Software Package and Version	Configuration Required to Permit Pulse Acceleration
Trend Micro IS Pro 17.50	Add a new network control protocol to allow incoming UDP packets for all IP addresses on port 3578.
McAfee Personal Firewall 12.0	McAfee displays a message to the user when it detects the WX Connection Method service. Users should respond Allow always .
Norton 4.3.0.5	No action required. Pulse updates the firewall during installation.
Kaspersky 6.0	Edit the rules for applications to allow inbound UDP packets on port 3578.
Windows XP, Windows Vista, and Windows 7	No action required. Pulse updates the firewall during installation.

Downloading the Junos Pulse Client from a Pulse Secure Access Server

The Junos Pulse client can be downloaded and installed automatically when users access a Pulse Secure Access server. For version 6.5 or 6.3 SA Series gateways, the Junos Pulse client must first be exported from a Junos Pulse Application Acceleration Service gateway and uploaded to the Pulse Secure Access server (see [“Distributing the Pulse Client” on page 131](#)). Note that version 7.0 (or higher) Pulse Secure Access servers include the Junos Pulse client, so exporting the client is not necessary.

To download the Junos Pulse client from a Pulse Secure Access server:

1. On a computer running Windows 7, Windows Vista, or Windows XP, enter the URL of the Pulse Secure Access server in a supported Web browser. For example:

`https://sa.company.net`

The Loading Components page is displayed. The Host Checker window opens for downloading the Junos Pulse client installer, followed by the Junos Pulse Client window for downloading and installing the client. Note the following:

- If the Windows Firewall is enabled, click **Unblock** when prompted to allow the Junos Pulse client to accept external connections.
- If you are prompted to stop the Network Connect client, click **OK** and restart the Network Connect client after the Junos Pulse client is installed.
- If you are prompted about improper installation of the Host Checker or Junos Pulse client, click **Try Again** to complete the installation.

When installation is complete, the Junos Pulse client starts automatically. To start the client manually, double-click the Junos Pulse icon in the system tray. Application acceleration starts automatically when a remote Junos Pulse Application Acceleration Service gateway is discovered in the network path. No additional configuration is necessary.

Downloading the Junos Pulse Client from a Pulse Application Acceleration Gateway

If you do not have a Pulse Secure Access server, you can download the Junos Pulse client from any Junos Pulse Application Acceleration Service gateway running JWOS 6.2. Before users can download the Pulse client software, you must:

- Verify that Pulse client downloads are enabled (see [“Enabling Pulse Client Downloads” on page 128](#)).
- Specify the Pulse client configuration (see [Defining the Pulse Client Configuration](#)).

To download the Pulse client to a computer running Windows 7, Windows Vista, or Windows XP:

1. If the WX Client is installed, uninstall the WX Client by selecting **Start > All Programs > Juniper Networks > WX Client > Uninstall**. The WX Client supports only JWOS 6.0 and is not compatible with the Pulse client.
2. Enter the following URL in a supported Web browser:
`https://Gateway IP address/client`
3. Enter the username and password, if needed, and click **Login**.
4. Select **Install Now**, and, if necessary, click **Install** in the Security Warning dialog box. Note the following:
 - If the Windows Firewall is enabled, click **Unblock** when prompted to allow the client to accept external connections.
 - If you are prompted to stop the Network Connect client, click **OK** and restart the Network Connect client after the Junos Pulse client is installed.

When installation is complete, the Pulse client starts automatically, and the Pulse icon is shown in the system tray in the lower-right corner of the Windows desktop. Application acceleration starts automatically when a remote Junos Pulse Application Acceleration Service gateway is discovered in the network path. No additional configuration is necessary.

Uninstalling the Junos Pulse Client

To uninstall the Junos Pulse client software, select **Start > All Programs > Juniper Networks > Junos Pulse > Uninstall**, or run the following program (if necessary, change C: to the drive where Windows is installed):

C:\Program Files\Juniper Networks\Junos Pulse\Uninstall.exe

Managing Software, Configurations, and Policies

The following topics describe how to manage Pulse clients:

- [Enabling Pulse Client Downloads on page 128](#)
- [Enabling Pulse Client Adjacencies on page 129](#)
- [Configuring Pulse Client Policies on page 129](#)
- [Viewing the Status of Pulse Clients on page 130](#)
- [Viewing the Pulse Client Configuration on page 130](#)
- [Uploading Pulse Client Software on page 130](#)
- [Distributing the Pulse Client on page 131](#)

Enabling Pulse Client Downloads

Windows users can download and install the Junos Pulse client software from a Junos Pulse Application Acceleration Service gateway that has client downloads enabled. Optionally, you can require users to log in before they can download the client software.

To enable client software downloads:

1. Select **Junos Pulse > Setup > Pulse Software Download**.
2. Verify that the displayed version of the Pulse software is correct. If a later version is available, you must upload it to the gateway (see [“Uploading Pulse Client Software” on page 130](#)).
3. Select **Allow Pulse software download** to allow users to download the client software to a new remote client.
4. Select **Allow Pulse software upgrade/downgrade** to allow users to upgrade or downgrade their current version of the Pulse client. You may want to disable Pulse client upgrades and downgrades when:
 - You upgrade the gateway software and want only new users to install the new version of the Pulse client.
 - You downgrade the gateway and want to prevent users from installing an older version of the Pulse client (downgrading the gateway also downgrades the Pulse client loaded on the gateway).
5. Select **Require user authentication** to require users to log in, and specify the required username and password.

6. Click **Submit** to activate the changes.
7. Click **Save** in the taskbar to retain your changes after the next reboot.

Enabling Pulse Client Adjacencies

By default, a Junos Pulse Application Acceleration Service gateway running JWOS 6.1 (or higher) can form an adjacency with any client that is running a supported version of the Junos Pulse client software. Traffic is accelerated after the adjacency is established. You can disable and enable client adjacencies at any time. After an adjacency is manually disabled (or disrupted for any reason), it takes about 30 seconds to reestablish the adjacency.



NOTE: The new features in JWOS 6.2, such as NSC and Exchange acceleration, require version 2.1 (or later) of the Junos Pulse client.

To enable or disable adjacencies with Junos Pulse clients:

1. Select **Junos Pulse > Setup > Pulse Adjacency**.
2. Select **Allow adjacency with Pulse clients** to enable the gateway to form adjacencies with Junos Pulse clients. If you clear the check box, all current adjacencies are disabled, and all client traffic flows are reset.
3. Click **Submit** to activate the changes.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

Configuring Pulse Client Policies

Compression and acceleration services can be configured on a Junos Pulse Application Acceleration Service gateway for each client that is currently adjacent (connected) or that has been adjacent at any time since the last time the gateway was restarted. When an adjacency is established, the enabled services are applied to the traffic sent to that client.

To define the default configuration for a client, see *Defining the Pulse Client Configuration*.

To configure the Junos Pulse client policies:






1. Select **Junos Pulse > Policies**.
2. Enable a service for one or more clients by selecting the check box for the service next to the appropriate clients. To enable or disable a service for all clients, select or clear the **Select All/Clear** check box below the list.
3. Click **Submit** to activate the changes, or click **Reset** to discard them.
4. Click **Save** in the taskbar to retain your changes after the next reboot.

Viewing the Status of Pulse Clients

The Junos Pulse Application Acceleration Service gateways display the connection status of each Junos Pulse client and the status of each service between the local gateway and each Pulse client. The list of clients includes the adjacent (connected) clients and all clients that are waiting for a connection or have been active at any time since the last time the gateway was restarted. Inactive adjacencies are disconnected after 15 minutes.

To view the status of Junos Pulse clients:

1. Select **Junos Pulse > Status**.
2. Review the status icons:

Icon	Description
	The Junos Pulse client is adjacent (connected).
	The Junos Pulse client is disconnected, waiting for a connection, or in the process of connecting or disconnecting.
	The service is operating normally.
	The service is not enabled on the local gateway. To enable the service, see “Configuring Pulse Client Policies” on page 129 .
	A problem exists, or the service is enabled on the local gateway, but disabled on the Pulse client.

Viewing the Pulse Client Configuration

The default configuration that is downloaded to Junos Pulse clients can be viewed on a Junos Pulse Application Acceleration Service gateway. Note that when you generate the Pulse client configuration from the gateway, the client configuration contains a subset of the CLI commands from the gateway configuration.

To view the client configuration:

1. Click **Junos Pulse > Admin > Display Pulse Configuration**.
2. View the client configuration. For more information about the CLI commands in the configuration, see the *Junos Pulse Application Acceleration Service Command Reference Guide*.

Uploading Pulse Client Software

When a new version of the Junos Pulse client software becomes available, you must upload it to the Junos Pulse Application Acceleration Service gateway before it can be downloaded by users or exported for distribution. You can load the Pulse client software from a local disk or from an FTP or TFTP server.

To upload a new version of the Pulse client software:

1. Select **Junos Pulse > Admin > Load Pulse Software**.
2. Verify that you want to replace the client version displayed at the top of the page.
3. Select one of the following, and specify the location of the new Pulse version:

Local disk	Specify the path and filename on a machine in your network, or click Browse and select the client software file.
TFTP server	Specify the path and filename on a TFTP server: <ul style="list-style-type: none"> • IP address of a TFTP server. • Path and filename of the software package on the server. The first character must be a slash (/).
FTP server	Specify the path and filename on an FTP server: <ul style="list-style-type: none"> • IP address of an FTP server. • Path and filename of the software package on the server. The first character must be a slash (/). • If the FTP server does not accept anonymous user access, enter a username and password for an account that has read/write privileges on the server.

4. Click **Load** to update the Junos Pulse client software.

Distributing the Pulse Client

In addition to allowing users to download the Junos Pulse client from a Junos Pulse Application Acceleration Service gateway, you can also distribute the client using either of the following methods:

- Juniper Networks SA Series SSL VPN Appliance—The Junos Pulse client can be downloaded and installed automatically when users access the Pulse Secure Access server. For version 6.5 or 6.3 SA Series gateways, you must export the Pulse client software package from a Junos Pulse Application Acceleration Service gateway, and then upload the package to the Pulse Secure Access server. Version 7.0 or higher Pulse Secure Access servers include the Pulse client, so exporting the client is not necessary. Junos Pulse configuration information for the Pulse Secure Access server is included in both the *Junos Pulse Administration Guide* and the *Junos Pulse Secure Access Service Administration Guide*.
- Microsoft System Management Server (SMS)—You can distribute the Junos Pulse client through SMS by exporting the client configuration for inclusion in the Windows installer file.

Distributing the Pulse Client Through an SA Series Gateway

Use the following procedure to distribute the Junos Pulse client through a version 6.5 or 6.3 SA Series gateway. To distribute the Pulse client through a version 7.0 or higher server, see the *Junos Pulse Administration Guide* or the *Junos Pulse Secure Access Service Administration Guide*.

1. Load or generate a Junos Pulse client configuration (see Defining the Pulse Client Configuration).
2. Select **Junos Pulse > Admin > Export Pulse Software**.
3. Export the client software package to be installed on an SA Series gateway:
 - a. Select **Create Host Checker package for use with SA** to have the Host Checker install and start the Junos Pulse client. If the client fails or is stopped manually, it is not restarted automatically.
 - b. Click **Export**, click **OK**, and then save the .zip file to a local or network folder.
4. Upload the exported software package to an SA Series gateway:
 - a. Log in as an administrator to the admin console of the SA Series gateway and select **Authentication > Endpoint Security > Host Checker**.
 - b. Verify that the **Perform check every X minutes** and **Client-side process, login inactivity timeout** are set to 10 minutes or more, and that the timeout interval is not greater than the check interval.
 - c. Select **New 3rd Party Policy**, specify a policy name, and select the exported Junos Pulse client software package as the Policies File.
 - d. Click **Save Changes**.
 - e. Select **Users > User Realms > Select Realm > Authentication Policy > Host Checker**. Select both the **Evaluate Policies** and **Require and Enforce** check boxes for the displayed Junos Pulse client policy.
 - f. Click **Save Changes** to save the Host Checker policy.

Distributing the Pulse Client Through Microsoft SMS/SCCM

To use Microsoft SMS/SCCM to distribute the Junos Pulse client, you must export the client configuration from a Junos Pulse Application Acceleration Service gateway and use it to replace the default client configuration in the Windows installer file.



NOTE: Be sure 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 msexec 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.

To distribute the Junos Pulse client through Microsoft SMS/SCCM:

1. Export the client configuration from the gateway:
 - a. Select **Junos Pulse > Admin > Export Pulse Software**.
 - b. Select **Download Configuration for MSI package**.
 - c. Click **Export**, and then save the Config_All.ini file to a local or network folder.
2. Download the Windows installer version of the Junos Pulse client software (a .msi file) to a computer that has InstallShield 2008. You can download the software from www.juniper.net/support/products/pulse/.
3. Open the downloaded file with InstallShield, and select the **Installation Designer** tab.
4. Select **Organization > Components** in the left pane, and open the first components folder in the middle pane.
5. Select the **Files** subfolder in the middle pane, right-click the Config_All.ini file displayed in the right pane, and select **Delete**.
6. Right-click the **Files** subfolder, and select **Add**.
7. Locate the Config_All.ini file that you exported from the gateway, and click **Open**.
8. Select **In a new CAB file** file, select the **Stream the new CAB file into the Windows Installer package** check box, and click **OK**.
9. Click **Save** to save your changes.

CHAPTER 6

Session Migration

- [Understanding Session Migration on page 135](#)
- [Task Summary: Configuring Session Migration on page 139](#)
- [Configuring Session Migration for the Pulse Client on page 140](#)
- [Configuring an IF-MAP Federated Network for Session Migration on page 140](#)

Understanding Session Migration

This topic describes the session migration feature. It includes the following information:

- [Session Migration Overview on page 135](#)
- [Session Migration and Session Timeout on page 137](#)
- [How Session Migration Works on page 137](#)
- [Session Migration and Session Lifetime on page 138](#)
- [Session Migration and Load Balancers on page 138](#)
- [Authentication Server Support on page 138](#)

Session Migration Overview

When you enable session migration on two or more Pulse servers, a Pulse endpoint can migrate from one location to another and connect to a different Pulse server without providing additional authentication. For example, a user can be connected from home through a Pulse Secure Access server, and then arrive at work and connect to a Pulse Access Control server without being reauthenticated. If session migration is not enabled, Pulse users must be reauthenticated each time they attempt to access the network through a different Pulse server.

Sessions can be migrated between Pulse Access Control and Pulse Secure Access servers that are in the same IF-MAP federated network: using either the same IF-MAP server, or using IF-MAP servers that are replicas of one another.

The servers must be in the same authentication group. Authentication groups are configured through authentication realms. An authentication group is a string that you define for common usage. You can use authentication groups to group together realms with similar authentication methods. Such as, , one authentication group for SecurID authentication, another authentication group for AD. A single gateway can belong to more than one authentication group, with a different authentication group per realm.

The Pulse server to which a user authenticates publishes session information to the IF-MAP server. Other IF-MAP clients in the federated network can use the information to permit access without additional authentication to users.

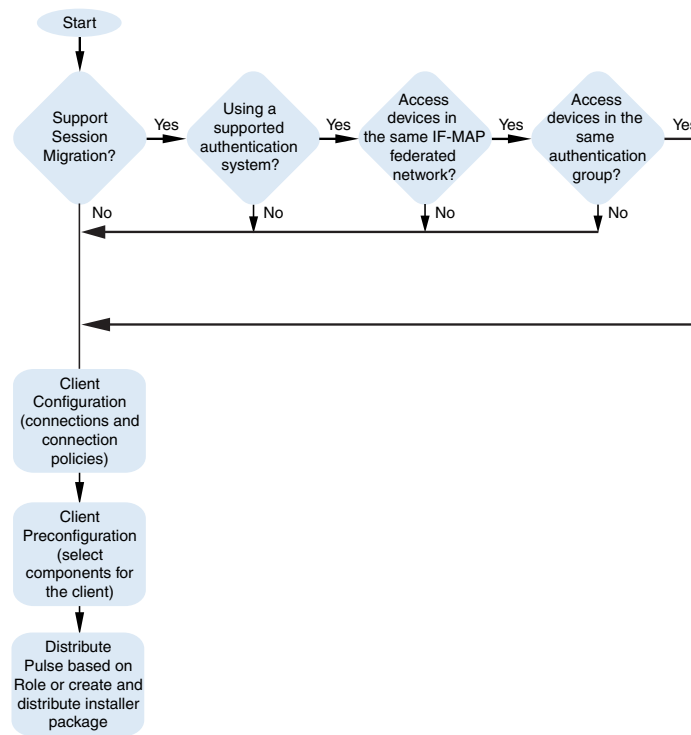
When a user session is migrated to another Pulse server, the new session information is pushed to the IF-MAP server. The IF-MAP server notifies the authenticating server, and information about the session that existed on the original server is removed leaving only session information about the current authenticating server on the IF-MAP server. The authenticating server removes information about the session from its local session table and the user license count is decremented.

When a session is migrated, realm role-mapping rules determine user access capabilities. You can import user attributes when a session is migrated, or you can configure a dedicated directory server to look up attributes for migrated user sessions. To ensure that session migration retains user sessions, configure a limited access remediation role that does not require a Host Checker policy. This role is necessary because the Host Checker timeout can be exceeded if an endpoint is in hibernation or asleep. With the new remediation role, the user's session is maintained.

If additional Host Checker policies are configured on a role or realm to which a migrated session applies, the policies are performed before allowing the user to access the role or realm. Administrators of different Pulse servers should ensure that Host Checker policies are appropriately configured for endpoint compatibility.

[Figure 10 on page 137](#) illustrates the task flow for enabling session migration for Pulse.

Figure 10: Requirements for Pulse Session Migration



Session Migration and Session Timeout

Session timeout on the authenticating server does not apply to a migrated session. Instead, session start time is applicable. The inbound server evaluates session timeout using the start time of the original session on the original server.

When a user reboots an endpoint for which session migration is enabled, the session is retained for a short time on the server. For sessions on the Pulse Access Control server, sessions are retained until the heartbeat timeout expires. For Pulse Secure Access server sessions, the idle timeout determines how long the session is retained.

If an endpoint that is connected to a Pulse Access Control server or Pulse Secure Access server is rebooted and the user does not sign out, when the endpoint is restarted and the user attempts to connect to the same access gateway, Pulse resumes the previous session without requesting user credentials if the previous session is still active.

How Session Migration Works

Session migration uses IF-MAP Federation to coordinate between servers.

When a session is established, the authenticating gateway publishes the session information, including a session identifier, to the IF-MAP server. The session identifier is also communicated to the Pulse client.

When the Pulse client connects to a migrating gateway in the same authentication group, the Pulse client sends the session identifier to the migrating gateway. The migrating gateway uses the session identifier to look up the session information in the IF-MAP server. If the session information is valid, the migrating gateway uses the session identifier to establish a local session for the endpoint that the Pulse client is running on.

The IF-MAP server notifies the authenticating gateway that the user session has migrated, and the authenticating gateway deletes the session information from the IF-MAP server.

Session Migration and Session Lifetime

Session migration is designed to give users maximum flexibility and mobility. Users are no longer tied to the office. The workplace can travel with the user, and electronic chores such as online banking can come to work. Because of this flexibility, users might be away from their machines for long periods of time, allowing their active session to expire. Session migration requires users to have an active session on the Pulse Access Control or Pulse Secure Access server.

You can adjust session lifetime to ensure that sessions do not time out while users are away from their machines. You adjust session lifetime on the gateway by selecting **Users > User Roles > Role Name > General > Session Options** in the admin console.

Session Migration and Load Balancers

A Pulse client that connects to a Pulse server that is behind a load balancer will attempt to migrate the network connection if the connected server fails. The Pulse servers must be federated and configured for session migration. For example, a load balancer that balances to 2 Pulse servers (non-clustered) balances to Server1. If Server1 fails, the load balancer then balances to Server2. A Pulse client that is connected to Server1 is migrated to Server2 without re-authentication.

Authentication Server Support

The behavior of session migration depends to some extent on the authentication server on the inbound side.

The following list provides a summary of authentication server support:

- Local authentication server—Migration succeeds if the username is valid on the local authentication server.
- LDAP server—Migration succeeds if the LDAP authentication server can resolve the username to a distinguished name (DN).
- NIS server—Migration succeeds if the NIS authentication server can find the username on the NIS server.
- ACE server—Migration always succeeds.
- RADIUS server—Migration always succeeds. If you select **Lookup Attributes using Directory Server**, no attributes are present in the user context data.
- Active Directory—Migration always succeeds. The Lookup Attributes using Directory Server option may not work, depending on your configuration.

- Anonymous—No support for migrating sessions because sessions are not authenticated.
- Siteminder—No support for migrating sessions because Siteminder SSO is used instead.
- Certificate—No support for migrating sessions because sessions are authenticated using certificates.
- SAML—No support for migrating sessions because SAML SSO is used instead.



NOTE: For local, NIS, and LDAP authentication servers, the inbound username must reflect an existing account.

Related Documentation

- [Configuring Session Migration for the Pulse Client on page 140](#)
- [Task Summary: Configuring Session Migration on page 139](#)

Task Summary: Configuring Session Migration

To permit session migration for users with the Pulse client, perform the following tasks:

1. Configure location awareness rules within a client connection set to specify locations included in the scope of session migration for users. For example, configure location awareness rules for a corporate Pulse Access Control server connection and a Pulse Secure Access server connection.
2. Configure an IF-MAP federated network, with the applicable Pulse Access Control servers and SA Series appliances as IF-MAP Federation clients of the same IF-MAP Federation server.
3. Ensure that user entries are configured on the authentication server for each gateway.
4. Ensure that user roles are configured for all users on each gateway.
5. Define a remediation role with no Host Checker policies to allow user sessions to be maintained when an endpoint is sleeping or hibernating.
6. Configure role-mapping rules that permit users to access resources on each gateway.
7. Enable and configure session migration from the User Realms page of the admin console.
8. Distribute the Pulse client to users.

Related Documentation

- [Understanding Session Migration on page 135](#)
- [Configuring Session Migration for the Pulse Client on page 140](#)
- [Understanding Federated Deployments](#)

Configuring Session Migration for the Pulse Client



NOTE: Ensure that all of the Pulse Access Control servers and Pulse Secure Access servers for which you want to enable session migration are IF-MAP Federation clients of the same IF-MAP Federation server. Additionally, make sure that each gateway is configured according to the procedures outlined in this section.

To configure session migration:

1. In 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** check box. Additional options appear.
4. In the **Authentication Group** box, enter a string that is common to all of the gateways that provision session migration for users. The authentication group is used as an identifier.
5. Select for either the **Use Attributes from IF-MAP** option button or the **Lookup Attributes using Directory Server** option.



NOTE: Select Lookup Attributes using Directory Server only if you are using an LDAP server. Attributes are served faster with an LDAP server.

Related Documentation

- [Understanding Session Migration on page 135](#)
- [Task Summary: Configuring Session Migration on page 139](#)
- [Understanding Federated Deployments](#)

Configuring an IF-MAP Federated Network for Session Migration

To successfully deploy session migration, you configure an IC Series device IF-MAP server, and you configure all of the connected IC Series devices and SA Series devices that users access as IF-MAP clients. A SA Series device can not be an IF-MAP server.

To add clients, you must specify the IP address and the security mechanism and credentials for the client.

An IF-MAP server certificate must be installed on the IF-MAP server. The client verifies the server certificate when it connects to the server. The server certificate must be signed by a Certificate Authority (CA), the client must be configured to trust certificates signed by that CA, and the hostname in the server certificate must match the hostname in the IF-MAP URL on the client.

You must identify the IF-MAP server to each IC Series device and SA Series device 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 to which the IF-MAP clients will connect.

To configure IF-MAP server settings on the IC Series device:

1. From the admin console select **System > IF-MAP Federation > Overview**.
2. On the IC Series device, under Choose whether this IC Series device runs an IF-MAP Server, an IF-MAP client, or no IF-MAP, select the **IF-MAP Server** option button.
3. Click **Save Changes**.
4. From the admin console select **System > IF-MAP Federation > This Server > Clients**.
5. Under IF-MAP Client, enter a **Name** and an optional **Description** for this client.
For example, enter the name SA-access1.corporate.com and the description Secure Access 1.
6. Type one or more IP addresses of the client. If the client is multi-homed, for best results list all of its physical network interfaces. If the client is an IC Series device or Secure Access cluster, list the internal and external network interfaces of all nodes. It is necessary to enter all of the IP addresses for all of the interfaces because equipment failures may cause traffic between the IF-MAP client and the IF-MAP server to be re-routed through a different network interface. Listing all of the IP addresses maximizes the probability that IF-MAP Federation still works in the event of a failure.
For example, enter 172.16.100.105.
7. Under Authentication, select the Client Authentication Method: **Basic or Certificate**.
 - a. If you select **Basic**, enter a Username and Password. The same information should be added to the IF-MAP server.
 - b. If you select **Certificate**, choose which Certificate Authority (CA) to use to verify the certificate for this client. Optionally, specify certificate attributes or restrictions to require values for certain client certificate attributes.
8. Click **Save Changes** to save the IF-MAP Client instance on the IF-MAP server.

To configure IF-MAP client settings on the IC Series device and SA Series device clients:

1. From the admin console select **System > IF-MAP Federation > Overview**.
2. In the IC Series device, under Choose whether this IC Series device runs an IF-MAP Server, an IF-MAP client, or no IF-MAP, select the **IF-MAP Client** option button. On the SA Series device, select **Enable IF-MAP Client** check box.
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.
For example, https://access2.corporate.com/dana-ws/soap/dsifmap.

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.

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 IF-MAP 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**

- [Understanding Session Migration on page 135](#)
- [Task Summary: Configuring Session Migration on page 139](#)

CHAPTER 7

Deploying Junos Pulse Client Software

- [Junos Pulse Client Installation Overview on page 143](#)
- [Adding a Pulse Configuration to a New Pulse Installation on page 146](#)
- [Installing Junos Pulse Client from the Web on page 148](#)
- [Launching Junos Pulse from the Pulse Server Web Portal on page 149](#)
- [Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 150](#)
- [Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 154](#)
- [Junos Pulse Command-line Launcher on page 155](#)
- [Using jamCommand to Import Junos Pulse Connections on page 158](#)

Junos Pulse Client Installation Overview

This section describes how to deploy Pulse for Windows and Pulse for Mac OS X client software from Pulse Access Control Service and Pulse Secure Access Service platforms. Pulse Application Acceleration Service supports deployment of App Acceleration connections only. See [“Installing the Junos Pulse Client” on page 125](#) for information about how to deploy Pulse through Pulse Application Acceleration Service.

server and Pulse Access Control Service include a default connection set and a default component set. These defaults enable you to deploy the Pulse client 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 Pulse Secure Access Service or Pulse Access Control Service to which the endpoint connects.

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

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

- *Web install*—With a Web install, users log in to the Pulse server’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 Pulse server is set to connect automatically. You can edit the default connection set to add connections of other Pulse servers 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*—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 msexec 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.
- *Default installer*—You can download the default Pulse installation program 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 Pulse server's Web portal. For the latter, the Pulse server's dynamic connection is downloaded automatically and the new connection is added to the Pulse client's connections list. 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.

If the Windows endpoints in your environment do not have admin privileges, you can use the Juniper Installer Service program, which is available on the admin console System Maintenance Installers page. The Juniper Installer Service allows users to download, install, upgrade, and run client applications without administrator privileges. In order to perform tasks that 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 the Pulse server and the client system.

When installing the Juniper Installer Service on client systems, note the following:

- When installing a Juniper client application on a user's Windows system, the Juniper Installer Service deploys two files on the client machine:
 - JuniperSetupSP1Control.ocx
 - AccessServiceComponent.exe

The device auto-starts this service when installing, and, then stops and removes it when uninstalling.

- Installing the Juniper Networks Installer MSI package requires administrator rights to install onto your client systems. If you plan to use the EXE version, administrator rights is not needed as long as a previous version of the access service component (deployed through, for example, JIS, Pulse, and so forth) is already present. If policies are defined for your client with the group policy “Run only Allowed Windows Application”, the following files must be allowed to run in the group policy. If not, client applications might not install.
 - dsmmf.exe
 - JuniperCompMgrInstaller.exe
 - JuniperSetupClient.exe
 - JuniperSetupClientOCX.exe
 - JuniperSetupXP.exe
 - uninstall.exe
 - x86_Microsoft.*.exe
- 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 SA Series Appliance ActiveX control. If the client systems do not contain either of these software components, the users will be unable to connect to the gateway. 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.

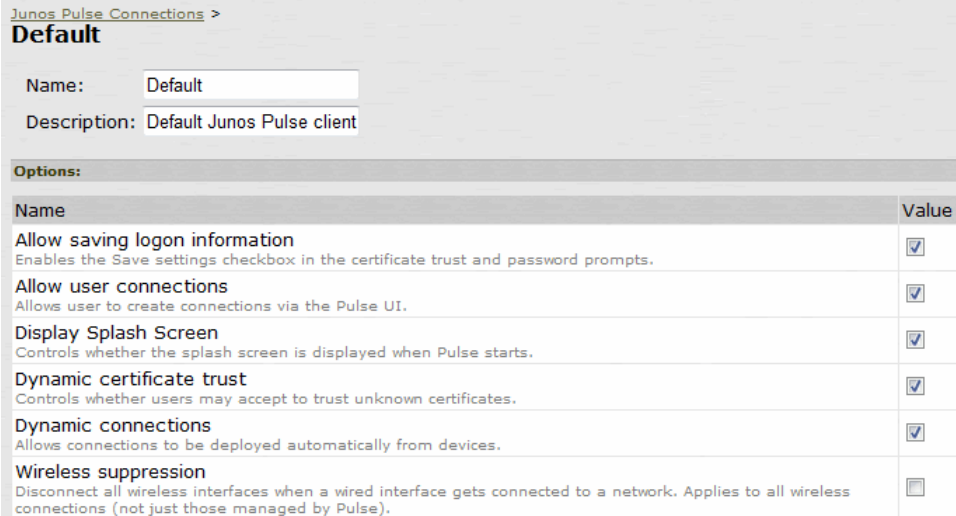
**Related
Documentation**

- [Adding a Pulse Configuration to a New Pulse Installation on page 146](#)
- [Installing Junos Pulse Client from the Web on page 148](#)
- [Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 150](#)
- [Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 154](#)

Adding a Pulse Configuration to a New Pulse Installation

When you install the Pulse client software on an endpoint using the default Pulse installer, the endpoint has all of the Pulse components it needs to connect to Pulse servers. However, the Pulse client needs a configuration that identifies the Pulse servers it can connect to, that is, the connections. Connection properties include how the connections are to be started, manually, automatically, or according to location awareness rules. The configuration also defines how Pulse and the connections behave (the connection set properties, also called machine settings). [Figure 11 on page 146](#) shows the default Pulse connection set properties, which are passed to the Pulse client as its configuration. [Figure 12 on page 147](#) shows the connection set properties as they appear in a Pulse preconfiguration file, which you can use to add the Pulse configuration when you install Pulse.

Figure 11: Junos Pulse Configuration Properties Defined on the Pulse Server



The screenshot shows the 'Junos Pulse Connections > Default' configuration page. It includes fields for 'Name' (Default) and 'Description' (Default Junos Pulse client). Below is an 'Options' section with a table of properties.

Name	Value
Allow saving logon information Enables the Save settings checkbox in the certificate trust and password prompts.	<input checked="" type="checkbox"/>
Allow user connections Allows user to create connections via the Pulse UI.	<input checked="" type="checkbox"/>
Display Splash Screen Controls whether the splash screen is displayed when Pulse starts.	<input checked="" type="checkbox"/>
Dynamic certificate trust Controls whether users may accept to trust unknown certificates.	<input checked="" type="checkbox"/>
Dynamic connections Allows connections to be deployed automatically from devices.	<input checked="" type="checkbox"/>
Wireless suppression Disconnect all wireless interfaces when a wired interface gets connected to a network. Applies to all wireless connections (not just those managed by Pulse).	<input type="checkbox"/>

There are two methods to install an initial configuration on a new Pulse client:

- Use a Pulse preconfiguration file (.jnprpreconfig) when you install Pulse on endpoints using the default Pulse installer.
- Instruct users to open a browser and login to the Pulse server Web portal.

The first time a Pulse client connects to a server that offers a Pulse configuration, the configuration settings are installed on the client and the client is bound to that server, which means that only that server can update the client's configuration. Any Pulse server can update the Pulse client software version if that feature is enabled, and any Pulse server can add a connection to an existing Pulse client configuration if the dynamic connection property is enabled. But only the binding server can update the Pulse client's configuration.

The dynamic connection enables a new Pulse connection to be added to an existing Pulse client when the user connects through the Web portal of a Pulse server. For example, a user has a Pulse connection to PulseServerA (the binding server) and it's

Pulse configuration allows dynamic connections. If the user browses to PulseServerB and successfully authenticates through the server's Web portal, the server adds a PulseServerB connection to the Pulse client configuration. This new connection is set to start manually so that it does not attempt to connect when the endpoint is restarted.

You can see a Pulse configuration by creating and viewing a .jnprpreconfig file. (To create the file, go to the Pulse Component screen, select a component set, and then click the Download Pulse Configuration button.) The .jnprpreconfig file contains a section that defines the machine settings and separate sections for each Pulse connection deployed to the client as shown in [Figure 12 on page 147](#).

Figure 12: Junos Pulse Configuration Properties in a Preconfiguration File

```
schema version {
  version: "1"
}

machine settings {
  version: "14"
  guid: "bf4801a3-527f-4f98-9ea3-7dc7e271bc9"
  connection-source: "preconfig"
  server-id: "0241ML82AOPRD1VR"
  allow-save: "true"
  user-connection: "true"
  splashscreen-display: "true"
  dynamic-trust: "true"
  dynamic-connection: "true"
  wireless-suppression: "false"
}

ive "8211f09f-6674-4bdb-a44a-e6fa8b7402eb" {
  friendly-name: "SA"
  version: "2"
  guid: "8211f09f-6674-4bdb-a44a-e6fa8b7402eb"
  server-id: "0241ML82AOPRD1VR"
  connection-source: "preconfig"
  factory-default: "true"
  uri: "10.64.78.34"
  connection-policy-override: "true"
  use-for-secure-meetings: "false"
  use-for-connect: "true"
  connection-identity: "user"
  connection-policy: "automatic"
  client-certificate-location-system: "false"
}

8021x "06cc1f68-3714-4871-9abf-458f1c0ef4b0" {
  friendly-name: "MachAuthCnxx"
  version: "2"
  guid: "06cc1f68-3714-4871-9abf-458f1c0ef4b0"
  server-id: "0241ML82AOPRD1VR"
  connection-source: "preconfig"
  adapter-type: "wireless"
  outer-username: "anonymous"
  scan-list: "juniper_wireless_network"
  non-broadcast-ssid: "false"
  connection-identity: "machine-only"
  connection-policy: "automatic"
}
```

The machine settings and each centrally configured connection (as opposed to connections created by users or added as a dynamic connection) include the server-id of the binding server. When a user browses to a Pulse server, and the server offers a new configuration, the client ignores it unless the server-id in the new configuration matches the server-id of the Pulse client's configuration.

Configuration files have a version number as well. When a Pulse client connects to its binding server, Pulse compares the version of its existing configuration to the version on the server. If the server version is greater than the existing client version, the client configuration is updated. The update might add, change, or remove connections and change machine settings.

If you have several Pulse servers and you want to provision the same configuration from all of the servers, the server-id of the Pulse configuration must be the same across all of the servers. To accomplish this, you create the configuration on one server, and then use the "push config" feature of the Pulse server to push the configuration to the other Pulse servers. This method ensures that the server-id of the configuration file is the same across all of the Pulse servers so that clients can receive a configuration update from any of the Pulse servers.

**Related
Documentation**

- [Junos Pulse Client Installation Overview on page 143](#)
- [Introducing Junos Pulse on page 3](#)

Installing Junos Pulse Client from the Web

For a Web install, you direct users to the Web interface of the Pulse server. After a successful login, a user is assigned to a role that includes an automatic download and installation of the 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, which includes the Host Checker component, and a connection to the Pulse server. 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.



NOTE: A Pulse installation causes a restart of active network connections on a Windows endpoint. When a user initiates a Pulse installation through a WAN connection to the Web interface of a Pulse server, the user might need to log in to their service provider again to reestablish network connectivity. Users need to be aware of this issue before they begin the installation.

**Related
Documentation**

- [Junos Pulse Client Installation Overview on page 143](#)
- [Launching Junos Pulse from the Pulse Server Web Portal on page 149](#)

Launching Junos Pulse from the Pulse Server Web Portal

One typical method of establishing a VPN connection is for users to browse to the Pulse server's Web portal, login, and then launch Pulse from the Web page. (This method is common in environments that used the Network Connect client.)

The following items describe the Pulse connection behaviors:

- The Pulse client has been installed on the endpoint by using the default Pulse installer. The installed Pulse client does not yet have any connections. The user browses to the Pulse server, logs into the server, and then clicks the Pulse button on the Web portal page. The following action occurs:
 1. The default Pulse connection set is automatically deployed to the client.
 2. The connection that has a URL that matches the server URL is launched.
- The Pulse client has been installed on the endpoint and it has a connection from the Pulse server. The user browses to the Pulse server, logs into the server, and then clicks the Pulse button on the Web portal page. The following action occurs:
 1. The connection that has a URL that matches the server URL is launched.
- Pulse has been installed on the endpoint and it has a connection from two different Pulse servers. The user browses to one of these Pulse servers, logs into the server, and then clicks the Pulse button on the Web portal page. The following action occurs:
 1. Only the connection that has a URL that matches the server URL is launched.
- Pulse has been installed on the endpoint. It has a connection for one Pulse server but the user browses to a different Pulse server, logs into the server, and then clicks the Pulse button on the Web portal page. The following action occurs:
 1. A new dynamic connection is created on the Pulse client for this Pulse server. (Note that the default connection on the server must be configured as a dynamic connection.) This new connection is a manual connection, that is, it does not start automatically when Pulse starts.
 2. The new connection for this Pulse server is started based on matching URLs.

Usage Notes

The Web browser method of launching Pulse is affected by the following configuration issues:

- The Pulse connection URL and the server URL must be an exact match. Pulse does not perform reverse DNS lookup to find a match.
- Connections that have the connection property **Allow user to override connection policy** disabled cannot be launched from the browser even if URLs match.

Related Documentation

- [Adding a Pulse Configuration to a New Pulse Installation on page 146](#)
- [Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 150](#)
- [Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 154](#)

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 `msiexec` command line. If you specify one or more `ADDLOCAL` options, the installer installs only the components you specify. Be sure that you specify all of 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 file name of the .jnprpreconfig file is the name of the selected component set. Make note of the file name 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 .msi installer 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 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 msixec 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 of the software components for all of 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 command line options. If you use one or more ADDLOCAL options, the preconfigured installer install 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* of 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` command line 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` programs 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 on installing Pulse on OS X endpoints, see [“Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File”](#) on page 154.

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 .jnprpreconfig 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\myconfiguration.jnprpreconfig"
```

- ADDLOCAL—This optional property specifies which features and feature options (sub-features) 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 sub-feature names are case sensitive. To specify multiple features in a single command, separate each feature with a comma.

ADDLOCAL 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.

Optional sub-features:

- Pulse8021x—Available with PulseUAC. Includes 802.1X connectivity components.
- SAEndpointDefense—Available with PulseSA. Includes Enhanced Endpoint Security 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 Enhanced Endpoint Security 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 Enhanced Endpoint Security support on a Windows 32-bit endpoint using a configuration file, use the following command line:

```
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, use the following command line:

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

To install PulseSA with Enhanced Endpoint Security and Host Checker on a 64-bit Windows endpoint using a configuration file, use the following command line:

```
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, use the following command line:

```
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, use the following command line:

```
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 154](#)

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 of 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 configurations that are the same except for the target server.

The default file name of the .jnprpreconfig file is the name of the selected component set. Make note of the file name 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:

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

2. Import the settings from the .jnprpreconfig file by running this command

```
/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 150](#)

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 9 on page 157](#) 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 8: Pulse Launcher Arguments

Argument	Action
-version	Display the Pulse Launcher version information, then exit.
-help	Display available arguments information.
-stop	Stop Pulse and disconnect all active connections.
-url <url>	Specify the Pulse server URL.
-u <user>	Specify the username.
-p <password>	Specify the password for authentication.
-r <realm>	Specify the realm on the Pulse server.

Table 8: Pulse Launcher Arguments (*continued*)

Argument	Action
-d <DSID>	Passes a cookie to Pulse Launcher for a specified Pulse server from another authentication mechanism when Pulse Launcher starts. When you use the -d argument, you must also specify the -url argument to specify the Pulse server.
-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 9: 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.

Table 9: Pulse Launcher Return Codes (*continued*)

Code	Description
7	Timeout error.
8	No user connection allowed from Pulse UI.
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 158](#)

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: What is “jam?” The working name for Junos Pulse during the early development phase was Juniper Access Manager. So many Pulse file names, directories, etc. 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 155](#)
- [Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 150](#)
- [Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 154](#)

PART 2

Junos Pulse Compatibility

This section provides detailed information about the how Junos Pulse features compare to Odyssey Access Client and Network Connect software features.

- [Client Software Feature Comparison on page 163](#)

Client Software Feature Comparison

- [Comparing Odyssey Access Client and Junos Pulse on page 163](#)
- [Comparing Network Connect and Junos Pulse on page 167](#)

Comparing Odyssey Access Client and Junos Pulse

Junos Pulse is a single integrated, multiservice network client that provides the basic services provided by the older Network Connect and Odyssey Access Client software. Pulse also provides dynamic connectivity, access control, security, and application acceleration for Microsoft Windows-based devices, secure connectivity for Mac OSX devices, and connectivity, mobile security, and mobile device management (MDM) for mobile devices, all with a simple, easy to use, elegant user experience.

[Table 10 on page 163](#) compares the features in Odyssey Access Client (OAC) and Junos Pulse to help you transition to Pulse. 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>.

Table 10: Odyssey Access Client and Junos Pulse Feature Comparison

Feature	Junos Pulse Release 4.0 OSX	Junos Pulse Release 4.0 Win	Odyssey Access Client
Wired/Wireless 802.1X Features			
Wired 802.1X support		Yes (with Microsoft Windows supplicant)	Yes
Auto scan lists		Yes (with Microsoft Windows supplicant)	Yes

Table 10: Odyssey Access Client and Junos Pulse Feature Comparison (*continued*)

Feature	Junos Pulse Release 4.0 OSX	Junos Pulse Release 4.0 Win	Odyssey Access Client
Wireless suppression		Yes (with Microsoft Windows supplicant)	Yes
Support for Network Provider (scraping passwords, listing)		Yes	Yes
Association Mode and Encryption Methods			
Association mode support (for open, shared, WPA/WPA2)		Yes (with Microsoft Windows supplicant)	Yes
Encryption (for WEP, TKIP, AES, WEP with preconfigured key, WPA/WPA2 with pre-shared key)		Yes (with Microsoft Windows supplicant)	Yes
EAP Methods			
EAP-TLS outer authentication			Yes
EAP-TTLS outer authentication	Yes	Yes	Yes
• With EAP-JUAC inner authentication		Yes	Yes
• With EAP-MSCHAPv2 inner authentication			Yes
• With EAP-GTC inner authentication			Yes
• With EAP-MD5 inner authentication			Yes
• With PAP inner authentication			Yes
• With CHAP inner authentication			Yes
• With MSCHAP inner authentication			Yes
• With MSCHAPv2 inner authentication			Yes
EAP-PEAP outer authentication			Yes

Table 10: Odyssey Access Client and Junos Pulse Feature Comparison (*continued*)

Feature	Junos Pulse Release 4.0 OSX	Junos Pulse Release 4.0 Win	Odyssey Access Client
• With EAP-JUAC inner authentication			Yes
• With EAP-DD5 inner authentication			Yes
• With EAP-GTC inner authentication			Yes
Authentication Methods			
Prompt for user name and password	Yes	Yes	Yes
Certificate support (automatic, specific)	Yes	Yes	Yes
Certificates from smart card reader		Yes	Yes
Soft token support		Yes	Yes
Machine login support		Yes	Yes
Machine authentication followed by user authentication	Yes	Yes	Yes
Credential provider on 32- and 64-bit Windows Vista, Windows 7, and Windows 8	N/A	Yes	Yes
Pre-desktop login	N/A	Yes	Yes
Configurable UAC Layer 2 connection		Yes	Yes
Configurable connection association modes			Yes
Certifications			
FIPS compliance	Supported via Web access only on Pulse Secure Access Service and Pulse Access Control Service (Pulse clients for iOS and Android support FIPS.)		Yes
Installation and Upgrade Methods			
Auto-upgrade	Yes	Yes	Yes
Web-based installation	Yes	Yes	Yes

Table 10: Odyssey Access Client and Junos Pulse Feature Comparison (*continued*)

Feature	Junos Pulse Release 4.0 OSX	Junos Pulse Release 4.0 Win	Odyssey Access Client
Standalone installation	Yes (.dmg)	Yes (.msi)	Yes
Upgrade/coordinate with previous versions	Yes	Yes	Yes
Manual Uninstall	Yes	Yes	Yes
Browser based installation and upgrades	Yes	Yes	Yes
Diagnostics and Logging			
IPsec diagnostics and configuration		Yes	Yes
Host Enforcer			Yes
Log viewer			Yes
Logging and Diagnostics	Yes Set debug level	Yes Set debug level, set file size limits	Yes
Other Features			
OPSWAT IMV support	Yes	Yes	Yes
Shavlik IMV support (patch assessment)		Yes	Yes
Automatic patch remediation		Yes via Shavlik or SMS/SCCM	Yes via SMS/SCCM
Host Checker support	Yes	Yes	Yes
Enhanced Endpoint Security support (Windows OS only)	N/A	Yes	Yes
IPsec tunneling to Policy Enforcement Points with NAT-T		Yes	Yes
Access service and plug-ins	Yes	Yes	Yes

Table 10: Odyssey Access Client and Junos Pulse Feature Comparison (*continued*)

Feature	Junos Pulse Release 4.0 OSX	Junos Pulse Release 4.0 Win	Odyssey Access Client
Block 3rd party EAP messages		N/A	Yes
Layer 3 authentication	Yes	Yes	Yes
Server-based pre-configuration of realm/role	Yes	Yes	Yes
Extend session duration	Yes	Yes	Yes
IC cardinality	Yes	Yes	Yes
Client-site management of clustered Pulse servers	Yes	Yes	Yes
Kerberos SSO		Yes	Yes
Initial configuration (intervention-less client provisioning)	Yes	Yes	Yes
Dynamically configurable	Yes	Yes	Yes

Related Documentation • [Comparing Network Connect and Junos Pulse on page 167](#)

Comparing Network Connect and Junos Pulse

Junos Pulse is a single integrated, multiservice network client that provides the basic services provided by the older Network Connect and Odyssey Access Client software. Pulse also provides dynamic connectivity, access control, security, and application acceleration for Microsoft Windows-based devices, secure connectivity for Mac OSX devices, and connectivity, mobile security, and mobile device management (MDM) for mobile devices, all with a simple, easy to use, elegant user experience.

[Table 11 on page 167](#) compares the features of NC and Pulse to help you transition from NC to Junos Pulse. 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>.

Table 11: Network Connect and Junos Pulse Feature Comparison

Feature	Junos Pulse Release 4.0 Mac	Junos Pulse Release 4.0 Win	Network Connect Release 6.3
---------	-----------------------------	-----------------------------	-----------------------------

Proxy Support

Table 11: Network Connect and Junos Pulse Feature Comparison (*continued*)

Feature	Junos Pulse Release 4.0 Mac	Junos Pulse Release 4.0 Win	Network Connect Release 6.3
Internet Explorer		Yes	Yes
Mozilla Firefox		Yes	Yes
Apple Safari	Yes		
Split Tunneling Options			
Disable split tunneling without route monitor	Yes	Yes	
Disable split tunneling with route monitor	Yes	Yes	Yes
Enable split tunneling with route monitors	Yes	Yes	Yes
Enable split tunneling without route monitors	Yes	Yes	Yes
Enable split tunneling with allowed access to local subnet	Yes	Yes	Yes
Disable split tunneling with allowed access to local subnet	Yes	Yes	Yes
Client Launch Options			
Command line launcher		Yes	Yes
Log off on connect	n/a	Yes	Yes
Launch as a standalone client	Yes	Yes	Yes
Launch from browser	Yes	Yes	Yes
GINA and Credential Provider support		Yes	Yes
Transport Mode			
SSL fallback mode	Yes	Yes	Yes
		<p>NOTE: If ESP is not available, the connection uses SSL. Once a connection switches to SSL it does not go back to ESP until the connection is restarted.</p>	
ESP	Yes	Yes	Yes
Other Features			
OPSWAT IMV support	Yes	Yes	Yes

Table 11: Network Connect and Junos Pulse Feature Comparison (*continued*)

Feature	Junos Pulse Release 4.0 Mac	Junos Pulse Release 4.0 Win	Network Connect Release 6.3
Shavlik IMV support (patch assessment)		Yes	Yes
Patch automatic remediation		Yes via Shavlik or SMS/SCCM	
Host Checker support	Yes	Yes	Yes
Enhanced Endpoint Security support (Windows OS only)	N/A	Yes	Yes
Run configured scripts when client connects/disconnects	Yes	Yes	Yes
Modify DNS server search order based on server configuration	Yes	Yes	Yes
Reconnect automatically if connection breaks	Yes	Yes	Yes
Dial-up adapter support	Yes	Yes	Yes
3G wireless adapter support	Yes	Yes	Yes
Max/Idle Session Time-outs	Yes	Yes	Yes
Logging			
Log to file	Yes	Yes	Yes
Upload log			Yes
Certifications			
FIPS			Yes

Pulse Split Tunneling

Table 12 on page 169 lists the Network Connect split tunneling options and shows how they map to Pulse split tunneling options.

Table 12: Pulse Split Tunneling

NC Split Tunnel Option	Pulse Split Tunnel Setting	Route Override State	Route Monitor State
Disable split tunnel	Disabled	Yes	Yes
Disable split tunneling but allow local access	Disabled	No	No

Table 12: Pulse Split Tunneling *(continued)*

NC Split Tunnel Option	Pulse Split Tunnel Setting	Route Override State	Route Monitor State
Enable split tunnel	Enable	Yes	No
Enable split tunnel with route monitor	Enable	Yes	Yes
Enable split tunnel, allow local access	Enable	No	No

Related Documentation • [Comparing Odyssey Access Client and Junos Pulse on page 163](#)

PART 3

Junos Pulse for Mobile Devices

- [Junos Pulse for Mobile Devices and Junos Pulse Mobile Security Suite on page 173](#)
- [Junos Pulse for Apple iOS on page 177](#)
- [Junos Pulse for Google Android on page 191](#)
- [Junos Pulse for Nokia Symbian Devices on page 205](#)
- [Junos Pulse for Windows Mobile Devices on page 209](#)

CHAPTER 9

Junos Pulse for Mobile Devices and Junos Pulse Mobile Security Suite

- [Junos Pulse for Mobile Devices Overview on page 173](#)
- [Junos Pulse Mobile Clients and User Agent Strings on page 174](#)

Junos Pulse for Mobile Devices Overview

Junos Pulse Secure Access Service supports authenticated access from mobile (handheld) devices to corporate applications such as corporate e-mail and the corporate intranet through Pulse Secure Access Service. The Pulse client software for mobile devices includes remote VPN capabilities as well as device security capabilities activated by the Junos Pulse Mobile Security Suite. The Pulse for Android and Pulse for iOS clients support Junos Pulse Collaboration for online meeting services.

The Junos Pulse Mobile Security Suite (MSS) is an optional component of Junos Pulse for mobile devices. The MSS provides (depending on the device OS) antivirus, antispam, and personal firewall services and enables an administrator to monitor and remove device applications and content, perform backup and restore operations, activate remote lock and remote wipe operations, and track devices using GPS. Each supported mobile device supports a specific list of Pulse Mobile Security Suite features.

Each supported mobile device requires that the user install the Pulse client software for the particular device type. The Pulse app is available as a free download from the app stores of the supported mobile devices, and the Windows Mobile app is available from juniper.net. The Pulse MSS is available as a separate server-based product. Pulse for mobile devices and Pulse Mobile Security Suite software cannot be deployed directly from Pulse Secure Access Service. The type of secure connectivity and the supported security features vary according to what is supported on each mobile operating system.

Updated versions of each Junos Pulse mobile client are released independently of each other. Some client features are not available in earlier client releases. If necessary, the description of a particular feature includes the minimum release required for that feature. For VPN features, the Pulse client communicates with the Junos Pulse Secure Access Service. For Pulse Mobile Security Suite features, the client communicates with the Pulse Mobile Security Gateway. As a general rule, users should upgrade to the most recent Pulse client software version to insure compatibility with all server updates.

Pulse is supported on the following mobile devices:

- Junos Pulse for Apple® iOS (iPhone, iPad, and iPod Touch)
- Junos Pulse for Google Android™
- Junos Pulse for BlackBerry
- Junos Pulse for Windows® Mobile
- Junos Pulse for Nokia® Symbian



NOTE: Although BlackBerry devices are supported by the Pulse MSS, Junos Pulse VPN software is not available for BlackBerry. However, some BlackBerry devices include support for IKEv2 and you can configure the BlackBerry IKEv2 to connect to Pulse Secure Access Service. See the *Junos Pulse Mobile Supported Platforms Guide*, which is available at <http://www.juniper.net/support/products/pulse/mobile/>, for details about BlackBerry devices that can use IKEv2.

The *Junos Pulse Mobile Supported Platforms Guide* lists the mobile device OS versions supported by Pulse and the security features supported on each mobile device OS.

Junos Pulse Mobile Security Gateway

Although you enable network access for Pulse on mobile devices using the Pulse Secure Access Service admin console, you manage the security features of the mobile devices by using the Junos Pulse Mobile Security Gateway. The administration interface of the Pulse Mobile Security Gateway enables you to protect and manage mobile devices. For more information, see the [Junos Pulse Mobile Security Gateway documentation](#).

Related Documentation

- [Junos Pulse for Apple iOS Overview on page 177](#)
- [Junos Pulse for Android Overview on page 191](#)
- [Junos Pulse for Symbian Overview on page 205](#)
- [Junos Pulse for Windows Mobile Overview on page 209](#)

Junos Pulse Mobile Clients and User Agent Strings

A user agent string is how a Web server identifies the type of browser that is requesting service. A Web server can use that information to provide content that is tailored for the browser. Portions of the Pulse user interface on a mobile device, such as the login screen and intranet bookmarks, are Web pages served from the Pulse server and displayed by the embedded browser of the Pulse client. The appearance of these Web pages can be affected by how the Pulse server is configured to map user agent strings to specific client types.

SA Series software Release 7.1 introduced new user agent string and client type pairings that are designed for each supported Pulse mobile device. If you change any of the user

agent string and client type pairings for mobile devices prior to upgrading your SA Series software to Release 7.1, your changes might cause Pulse mobile device screens to display content incorrectly. If the Pulse interface on mobile devices is not appearing as expected, you should remove your edited user agent string and client type pairings so that the Pulse clients can access the new configurations. SA Series software Release 7.2 introduced a change in how the Pulse secure access server provides the bookmarks index page so that changes to your configuration of user agent string and client type pairings do not affect how the mobile device displays the Pulse bookmarks.

To view and edit the user agent string and client type pairings on your Pulse server:

1. Click **System > Configuration > Client Types**.

To edit an existing item, click an item in the table to select it. The string pattern is available for editing in a text box and you can select the client type from a list box.

To add a new user agent string and client type pairing, type a string pattern in the edit box at the top of the list, choose a client type from the list box, and then click **Add**. You may use the * and ? wildcard characters in your string. Note that user agent strings are not case-sensitive.

2. To reorder the list, click an item to select it and then use the up and down arrow buttons to move the item up or down in the list. When a browser requests access, the user agent string submitted by the browser is compared against the list starting at the top of the list and continuing down the list until the first match is reached.

The default pairing (User Agent String = "*", Client Type = "Standard HTML") is listed as the last entry in the table to ensure that it is used only when no other pairing applies. You cannot edit, delete, or reorder the default pairing.

3. When you finish making changes to the table, click **Save Changes**.

[Table 13 on page 175](#) lists the User Agent String and Client Type pairings for supported mobile devices in SA Series software.

Table 13: User Agent String Client Type Pairings for Mobile Devices

SA Series Software	Apple iOS	Google Android	Windows Mobile	Nokia Symbian
Release 7.0 and earlier	User Agent String = "*", Client Type = "Standard HTML"	User Agent String = "*", Client Type = "Standard HTML"	User-agent string = "*Windows CE*", Client Type = "Mobile HTML (Pocket PC)".	User Agent String = "*Symbian OS*", Client-Type = "Smart Phone HTML Basic"
			User Agent String = "*", Client Type = "Standard HTML"	User Agent String = "*", Client Type = "Standard HTML"

Table 13: User Agent String Client Type Pairings for Mobile Devices (*continued*)

SA Series Software	Apple iOS	Google Android	Windows Mobile	Nokia Symbian
Release 7.1 and later	<p>User Agent String = "<i>*iPad*AppleWebKit</i>", Client type = "iPad Optimized HTML"</p> <p>User Agent String = "<i>*AppleWebKit*Mobile*</i>", Client Type = "Mobile Safari Optimized HTML (iPhone/iPod Touch) Full/Advanced/Basic"</p>	<p>User Agent String = "<i>*Android*</i>", Client Type = "Android Optimized HTML Full/Advanced/Basic"</p>	<p>User Agent String = "<i>*Windows CE*</i>", Client Type = "Mobile HTML (Pocket PC)"</p> <p>User Agent String = "<i>*"</i>", Client Type = "Standard HTML"</p>	<p>User Agent String = "<i>*Symbian*</i>", Client-Type = "Smart Phone HTML Basic"</p>



NOTE: You can also configure user agent strings at the role or the realm level to define policies for a user based on browser type.

Related Documentation

- [Junos Pulse for Apple iOS Overview on page 177](#)
- [Junos Pulse for Android Overview on page 191](#)
- [Junos Pulse for Symbian Overview on page 205](#)
- [Junos Pulse for Windows Mobile Overview on page 209](#)

CHAPTER 10

Junos Pulse for Apple iOS

- Junos Pulse for Apple iOS Overview on page 177
- Configuring a Role and Realm for Junos Pulse for Apple iOS on page 180
- Allowing Junos Pulse for iOS Users to Save Webmail Password on page 183
- Host Checker for Pulse iOS Clients on page 183
- Configuring Host Checker for Junos Pulse iOS Clients on page 184
- Implementing Host Checker Policies for Junos Pulse for iOS Devices on page 186
- Installing the Junos Pulse for Apple iOS App on page 187
- Using iPhone Configuration Utility Profiles for Junos Pulse for iOS on page 188
- Collecting Log Files from Junos Pulse for iOS on page 189
- Junos Pulse for iOS Error Message Reference on page 189

Junos Pulse for Apple iOS Overview

Junos Pulse provides Layer 3 VPN connectivity based on SSL encryption and authentication between an Apple iOS device (iPhone, iPad, iPod Touch) and Junos Pulse Secure Access Service. Junos Pulse enables secure connectivity to corporate applications and data based on identity, realm, and role. Pulse is designed to provide battery-friendly connectivity by automatically disconnecting from the VPN when the device is inactive while on Wi-Fi, automatically reestablishing VPN connectivity when the device reactivated, and maintaining connectivity when roaming from network to network. Junos Pulse is available for download from the Apple App Store.



NOTE: Mobile client features are updated frequently and each mobile client has a release number that is independent from the other clients and from the Pulse Windows and Mac clients. We recommend that you upgrade your mobile clients to the latest release to ensure that all features described in this guide are supported on your devices.

The *Junos Pulse Mobile Supported Platforms Guide*, which is available at <http://www.juniper.net/support/products/pulse/mobile/> lists the mobile device OS versions supported by Pulse and the security features supported on each mobile device OS.

The Junos Pulse VPN app supports the following features:

- Full Layer 3 tunneling of packets
- UDP/ESP and NCP/SSL modes
- Authentication by all authentication options available on the Pulse Secure Access server
- Certificate authentication followed by any other form of authentication
- Multi-factor authentication (cascading two different types of authentication)
- Host Checker



NOTE: A Host Checker policy that is configured for a VPN tunnel is not triggered if the VPN is launched automatically by VPN on Demand on iOS. If the VPN session is started through the Pulse client, Host Checker policy is correctly applied.

- Split tunneling modes:
 - Split tunneling disabled with access to local subnet
 - Split tunneling enabled
- Apple VPN on Demand

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.



NOTE:

When you configure VPN on Demand, you must create an exception for your Pulse Secure Access server hostname. For example, if the hostname is `sslvpn.example.com` and you want Pulse clients to automatically establish the VPN whenever requests are made for hosts in the `example.com` domain, the VPN on Demand configuration should contain the following rules:

- If domain name = `sslvpn.example.com`, then never initiate VPN connection
- If domain name = `example.com`, then always initiate VPN connection

There are different methods for creating VPN on Demand connections:

- Use the iPhone Configuration Utility. For complete information about how to create a VPN on Demand configuration using the iPhone Configuration utility, see the *iPhone OS Enterprise Deployment Guide*, which is available at www.apple.com.

- Use the mobile device management (MDM) features of the Junos Pulse Mobile Security Suite. Pulse Mobile Security Suite provides device management as well as security. For complete information about MDM, see the [Junos Pulse Mobile Security Gateway documentation](#).
- Create and manage VPN On Demand configurations from within the Junos Pulse for iOS client.
- Monitor and Control features of the Junos Pulse Mobile Security Suite.
- Junos Pulse for iOS also supports the Junos Pulse Mobile Security Suite (MSS) R3.0 and later. Using the Pulse Mobile Security Gateway, the security administrator can define Pulse connections and other profile settings, and then those settings are downloaded to the device when it registers with the gateway and updated periodically. For more information, see the [Junos Pulse Mobile Security Gateway documentation](#).

Before You Begin

Before you configure support for Apple iOS devices with Junos Pulse Secure Access Service, keep in mind the following client software behaviors:

- With Wi-Fi connectivity, Pulse reconnects the VPN tunnel automatically when the user wakes up the device. With 3G connectivity, the VPN reconnects when the user generates network traffic using an application like Safari or Mail.
- Establishing the VPN tunnel through a proxy is supported (regardless of the split tunnel mode), except for proxies that require authentication credentials.
- A Proxy Automatic Configuration (PAC) script takes effect only when split tunneling mode is disabled with access to local subnet. The PAC script does not work when the role's split tunnel mode is Enable split tunneling.
- Static host mapping is not created for the Pulse server/proxy hostname.
- DNS considerations:
 - When split tunneling is set to *Split tunneling disabled with access to local subnet*, Pulse uses the DNS servers that are configured the Pulse server.
 - When split tunneling is set to *Split tunneling enabled*, DNS servers that are configured on the Pulse server are used only for hostnames within the Pulse Secure Access Service domains.
- Session scripts are not supported.
- Web-based installation from a Junos Pulse server is not supported.
- Session timeout reminders are not supported.
- When you use client certificate authentication, and the user is enabled to select from among assigned roles, the user is prompted to enter the role name instead of being presented with a list of roles.
- To ensure that users see consistent bookmarks in the Pulse client UI no matter which server they are connected to, you can configure and enable user record synchronization, a feature of the Pulse Secure Access Service platform.

Related Documentation

- [Configuring a Role and Realm for Junos Pulse for Apple iOS on page 180](#)
- [Host Checker for Pulse iOS Clients on page 183](#)
- [Configuring Host Checker for Junos Pulse iOS Clients on page 184](#)
- [VPN Tunneling Proxy Support](#)
- [About User Record Synchronization](#)

Configuring a Role and Realm for Junos Pulse for Apple iOS

To enable SSL/VPN access from an Apple iOS device to Pulse Secure Access Service, the device user must download, install, and configure the Junos Pulse app, and the Pulse administrator must configure specific realm and role settings on Pulse Secure Access Service.

To configure Pulse Secure Access Service for Apple iOS device access:

1. Log in to the Pulse server admin console.
2. Select **User Roles > New User Role**.
3. On the New Role page, specify a name for the role and, optionally, a description. Make note of the name because later in this procedure, you create a realm and map realm users to this role.
4. In the Access Features section of the New Role page, select the **VPN Tunneling** check box.
5. Click **Save Changes** to create the role and to display the role configuration tabs.

Specifying Host Checker policies is part of the role configuration. However, you must first create the policy you want to assign to the role, so that procedure is covered later.

6. Select **Web > Bookmarks** and then click **New Bookmark**.
7. Specify a name and description for the bookmark.

You must create bookmarks to enable the buttons that appear in the Pulse for iOS user interface. Typically, you create a bookmark for your company intranet and for Web e-mail.



NOTE: You must create an e-mail bookmark to enable the e-mail button within the Pulse interface on the iOS device, and that e-mail bookmark must be named **Mobile Webmail**.

8. In the URL box, specify the Web address for access to your organization's e-mail.

Figure 13: Creating the E-mail Bookmark for the Pulse Client

The screenshot shows the Juniper Central Manager interface for configuring a Web Bookmark. The left sidebar contains a navigation menu with categories like System, Authentication, Administrators, Users, Maintenance, and Troubleshooting. The main content area is titled 'Web Bookmark' and includes the following sections:

- Name:** A text field containing 'Mobile Webmail'.
- Description:** A text area containing 'special bookmark for Junos Pulse'.
- Bookmark to:** A section with a required field '* URL:' containing 'http://exchange3/owa'. An example URL is provided: 'Example: http://www.domain.com/'.
- Auto allow:** A section with a note about using auto-allow to add the bookmark to the Web access control policy. It includes a checked checkbox for 'Auto-allow Bookmark' and two radio button options: 'Only this URL' and 'Everything under this URL' (selected).
- Display options:** A section with three checkboxes: 'Open the bookmark in a new window' (checked), 'Do not display the Web browser's URL address bar' (unchecked), and 'Do not display the Web browser's menu and toolbar' (unchecked).
- Save changes?:** Two buttons: 'Save Changes' and 'Save as Copy'.

A note at the bottom states: '* indicates required field'.



NOTE: Alternatively, you can use Web resource policies to define the bookmarks.

9. Set the **Auto Allow** and **Display Options** as desired, and then click **Save Changes**.
10. On the VPN Tunneling tab, set the Split Tunneling Options by selecting the following options:
 - **Split Tunneling: Enable**
 - **Route Precedence: Endpoint routes**

These are the only split tunneling modes supported on iOS.
11. To change default session time-outs, select **General > Session Options**.
12. In the Session lifetime section, specify **Max. Session Length** in minutes. The remaining session time appears on the Pulse interface of the mobile device client in the format days hours:minutes:seconds. The other session settings are not applied to mobile clients.
13. Click **Save Changes**.
14. Select **Users > Resource Policies > VPN Tunneling > Connection Profiles**.

A resource policy is a system rule that specifies resources and actions for a particular access feature. .

15. Click **New Profile**.

16. Specify a name and description for the connection profile.

When you define the connection profile, note the following:

- *IP Address Assignment options*—When Pulse Secure Access Service receives a client request to start a session, it assigns an IP address to the client based on the IP address policies you define.
- *Connection Settings*—ESP is the default transport. The Pulse for iOS VPN client supports both ESP and SSL.
- *DNS Settings*—Searching IVE DNS first with split tunneling enabled is not supported. With split tunneling enabled, Junos Pulse uses the IVE DNS for queries for hosts in the IVE DNS search domains only. All other queries go to the client's DNS servers.
- *Proxy Server Settings*—The Pulse for iOS client software supports all of the proxy server settings except **Preserve client-side proxy settings**. That option is specific to the Windows client only. Automatically modifying the client proxy configuration when split tunneling is enabled is not supported.

17. In the Roles area, select **Policy applies to SELECTED roles**. Then add the role you created for iOS devices to the Selected roles list.

18. Click **Save Changes**.

19. Select **Users > User Realms > New User Realm**.

20. Specify a name and description. Then click **Save Changes** to create the realm and to display the realm option tabs.

21. In the Servers section, specify the authentication settings.

Authentication server configuration is described in Authentication Servers.

22. On the General tab for the realm, select the **Session Migration and Sharing** check box.

23. On the Role Mapping tab for the realm, create a new rule that maps all users to the iOS device role you created earlier in this procedure.

Related Documentation

- [Host Checker for Pulse iOS Clients on page 183](#)
- [Configuring Host Checker for Junos Pulse iOS Clients on page 184](#)
- [Allowing Junos Pulse for iOS Users to Save Webmail Password on page 183](#)
- [Creating VPN Tunneling Connection Profiles](#)
- [Resource Policies](#)

Allowing Junos Pulse for iOS Users to Save Webmail Password

A Web bookmark on the role for iOS users allows users to access e-mail through a Web link. You can allow users of the Pulse for iOS app to save their e-mail password when they login to the e-mail system. After you have created a Mobile Webmail bookmark for the role used by iOS users, enable password the option for user to save their e-mail password by doing the following.

1. Open the role you created for iOS users.
2. Click **General > Session Options**.
3. In the section labeled **Persistent Password Caching**, select **Enabled**.
4. Click **Save Changes**.

Related Documentation

- [Configuring a Role and Realm for Junos Pulse for Apple iOS on page 180](#)
- [Host Checker for Pulse iOS Clients on page 183](#)

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.



NOTE: A Host Checker policy that is configured for a VPN tunnel is not triggered if the VPN is launched automatically by VPN on Demand.

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.

Related Documentation

- [Configuring Host Checker for Junos Pulse iOS Clients on page 184](#)
- [Implementing Host Checker Policies for Junos Pulse for iOS Devices on page 186](#)
- Host Checker and Trusted Network Computing

Configuring Host Checker for Junos 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. Endpoint Defense includes complete information on configuring the certificate environment for the Pulse Secure Access Service.



NOTE: A Host Checker policy that is configured for a VPN tunnel is not triggered if the VPN is launched automatically by VPN on Demand on iOS.

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*.
 - 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 displays **A jailbroken device is not allowed to access the network. Please contact your network administrator.**

8. When you are finished, click **Save Changes**.

**Related
Documentation**

- [Host Checker for Pulse iOS Clients on page 183](#)
- [Implementing Host Checker Policies for Junos Pulse for iOS Devices on page 186](#)
- [Junos Pulse for Mobile Devices Overview on page 173](#)

Implementing Host Checker Policies for Junos 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 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.
5. Click **Save Changes**.

Related Documentation

- [Host Checker for Pulse iOS Clients on page 183](#)
- [Configuring Host Checker for Junos Pulse iOS Clients on page 184](#)
- Host Checker and Trusted Network Computing

Installing the Junos Pulse for Apple iOS App

Junos Pulse is available in the iTunes App Store. After installing the Pulse app, a user can manually configure it.

1. On the iOS device, launch Junos Pulse.

2. Tap the Configuration item on the main status page to display Pulse configurations.
3. Create a new configuration with the URL. The URL for the connection is the Pulse Secure Access Service sign-in URL that was created and defined for mobile devices. Then configure the certificate settings as required.



NOTE: When iPhone users launch Pulse for the first time, they see a security warning and a prompt for enabling Pulse SSL VPN functionality. This security precaution helps deter the silent installation of malicious VPN software. If the user declines the Pulse software, the Pulse splash screen appears until the user presses the Home button on the device. If the user accepts the Pulse software, the security warning no longer appears when Pulse is started.



NOTE: For certificate authentication, the Pulse Secure Access Service SSL certificate must be issued by a CA. It cannot be self-signed. If the CA is not one of the built-in trusted CAs on the iOS device, then the CA certificate must be imported into the iOS device. Also, the Pulse Secure Access Service must be accessed using a hostname (not an IP address), and the hostname must match the Common Name of the Pulse Secure Access Service SSL certificate.



NOTE: The Pulse iOS app also supports the Junos Pulse Mobile Security Suite (MSS) R3.0 and later. Using the Pulse Mobile Security Gateway, the security administrator can use mobile device management (MDM) features to define Pulse connections and other settings, and then those settings are downloaded to the device when it registers with the gateway. For more information, see the [Junos Pulse Mobile Security Gateway documentation](#).

Related Documentation

- Using Configuration Profiles for Junos Pulse for iOS
- [Junos Pulse for Apple iOS Overview on page 177](#)
- About Sign-In Policies

Using iPhone Configuration Utility Profiles for Junos Pulse for iOS

Instead of instructing users to create Pulse VPN configurations manually, you can use a Configuration Profile to define Pulse configurations for the iOS device, and then distribute the configuration profiles by e-mail or by posting them on a Web page. When users open the e-mail attachment or download the profile using Safari on their iOS device, they are prompted to begin the installation process.

You use the iPhone Configuration Utility to create configuration profiles and specify Juniper SSL as the Connection Type for the VPN Payload. You can download the iPhone Configuration Utility (3.0 or later) from the Apple support Web. For details about the

utility and how to create Configuration Profiles, see the *iPhone OS Enterprise Deployment Guide*, which is available at www.apple.com.



NOTE: The Pulse iOS app also supports the Junos Pulse Mobile Security Suite (MSS) R3.0 and later. Using the Pulse Mobile Security Gateway, the security administrator can use the mobile device management (MDM) features to define Pulse connections and other settings within a profile. Those settings are downloaded to the device when it registers with the gateway and updated when the device periodically checks in with the server after registration. For more information, see the [Junos Pulse Mobile Security Gateway documentation](#).

- Related Documentation**
- [Junos Pulse for Apple iOS Overview on page 177](#)
 - [Junos Pulse for Mobile Devices Overview on page 173](#)

Collecting Log Files from Junos Pulse for iOS

The iOS device user can use the following procedure to e-mail the Junos Pulse log files:

1. On the iOS device, start the Junos Pulse app.
2. Tap **Status**.
3. Tap **Logs > Send Logs**.
4. Enter an e-mail address and tap **Send**.

- Related Documentation**
- [Junos Pulse for Apple iOS Overview on page 177](#)
 - [Installing the Junos Pulse for Apple iOS App on page 187](#)

Junos Pulse for iOS Error Message Reference

The following error message summary for Junos Pulse for iOS describes possible issues and suggests resolution actions where possible.

Table 14: Junos Pulse for iOS Error Messages

Message	Possible Causes	Suggested Actions
Please provide values for all the fields	A required field was not provided.	Provide a value for all the required fields and then try the operation again. Contact your mobile security provider.
A configuration with the same name already exists. Please choose a different name.	Configuration names must be unique.	Choose a configuration name that is not in use by another configuration, and then try the operation again.

Table 14: Junos Pulse for iOS Error Messages (*continued*)

Message	Possible Causes	Suggested Actions
An internal error occurred while creating the configuration.	An undefined error occurred.	Verify all of the values you entered, and then try the operation again. If the error occurs again, contact the Pulse administrator.
Please contact your administrator.	Host Checker policy failed and the reason string is displayed for the failure.	Tap the Cancel button and then try again after performing the remediation actions.
Your device is running operating system version x.y.z.	The iOS version running on the device is not allowed to connect.	If prompted to continue, tap Continue to connect with limited connectivity or tap Cancel to cancel the connection and try again after upgrading iOS.
Junos Pulse Mobile Security Suite is not active on your device.	Pulse Mobile Security is not active.	If prompted to continue, tap Continue to connect with limited connectivity or tap Cancel to cancel the connection and try again after registering with Mobile Security Suite.
Your iOS device is jailbroken.	Jail broken iOS devices are not allowed to connect.	If prompted to continue, tap Continue to connect with limited connectivity or tap Cancel to cancel the connection.
Host Checker is not supported with this version of Junos Pulse. Please upgrade the Junos Pulse client or contact your administrator.	Unsupported Junos Pulse client - Junos Pulse Host Checker is supported on Pulse 3.2 and later.	Check for the update of Junos Pulse on the App store and upgrade the Junos Pulse client to 3.2 or later, and then try again.
Session disconnected due to invalid certificate.	The Pulse client downloads session information from the Pulse server and the certificate received from the server does not match the stored session certificate.	Click the Close button on the Alert dialog to return to home screen. User can retry the connection.
Failed to connect to the server.	Sign-in process failed.	Check the network connection (for example, Wi-Fi, 3G, etc.), and then retry the connection.
Compliance Check couldn't be completed.	Host checker compliance check couldn't be completed during sign-in process.	Try to connect again.

- Related Documentation**
- [Junos Pulse for Apple iOS Overview on page 177](#)
 - [Installing the Junos Pulse for Apple iOS App on page 187](#)

Junos Pulse for Google Android

- Junos Pulse for Android Overview on page 191
- Configuring a Role and Realm for Pulse for Android on page 192
- Allowing Junos Pulse for Android Users to Save Webmail Password on page 194
- Host Checker for Pulse Android Clients on page 194
- Configuring Host Checker for Junos Pulse Android Clients on page 195
- Implementing Host Checker Policies for Junos Pulse for Android Clients on page 197
- Junos Pulse for Android Error Message Reference on page 198
- Launching the Junos Pulse for Android App Using a Command on page 200

Junos Pulse for Android Overview

Junos Pulse can create an authenticated SSL session between a device running Google Android and Pulse Secure Access Service. Junos Pulse enables secure connectivity to Web-based applications and data based on identity, realm, and role. Junos Pulse is available for download from the Android Market. The *Junos Pulse Mobile Supported Platforms Guide*, which is available at <http://www.juniper.net/support/products/pulse/mobile/> lists the mobile device OS versions supported by Pulse and the security features supported on each mobile device OS.



NOTE: The Google Android OS has limitations in its support for certificate-based authentication. For successful certificate authentication, the user certificate and the private key must be separate files. If necessary, you can separate the private key from the certificate by using `openssl` commands before you install the certificate and the key on the Android device. The Juniper Networks Knowledgebase includes an article, [KB19692](#), that describes in detail how to create a certificate and key that enables successful certificate authentication for Junos Pulse on Android.



NOTE: To ensure that users see consistent bookmarks in the Pulse client UI no matter which server they are connected to, you should configure and enable user record synchronization, a feature of the Pulse Secure Access Service platform.

Related Documentation

- [About User Record Synchronization](#)

Configuring a Role and Realm for Pulse for Android

To enable access from an Android device to Pulse Secure Access Service the Pulse administrator must configure specific realm and role settings on the Pulse server.

To configure Pulse Secure Access Service for Android device access:

1. Log in to the Pulse server admin console.
2. Select **User Roles > New User Role**.
3. On the New Role page, specify a name for the role and, optionally, a description. Make note of the name because later in this procedure, you create a realm and map realm users to this role.
4. In the Access Features section, select **Web**.
5. Click **Save Changes** to create the role and to display the role configuration tabs.
6. Select **Web > Bookmarks** and then click **New Bookmark**.

You must create bookmarks to enable the buttons that appear in the Pulse for Android user interface. Typically, you create a bookmark for your company intranet and for Web e-mail. You must create an e-mail bookmark to enable the e-mail button within the Pulse interface on the Android, and that e-mail bookmark must be named **Mobile Webmail**.

Figure 14: Creating the E-mail Bookmark for the Pulse Client

JUNIPER
Central Manager

Help | Guidance | Sign Out

System > Roles > Pulse > **Web Bookmark**

Name: Mobile Webmail

Description: special bookmark for Junos Pulse

Bookmark to

* URL: http://exchange3/owa Example: http://www.domain.com/
We recommend that you use the fully qualified domain name when entering the bookmark URL.

Auto allow

Use auto-allow to automatically add this web bookmark for this role to the Web access control policy. In order for the auto-allow bookmark option to work properly, you must enter a fully qualified domain name in your bookmark URL.

☒ **Auto-allow Bookmark**

☐ Only this URL

☒ Everything under this URL

Display options

☒ **Open the bookmark in a new window**

☐ Do not display the Web browser's URL address bar

☐ Do not display the Web browser's menu and toolbar

Save changes?

* indicates required field



NOTE: Alternatively, you can use Web resource policies to define the bookmarks.

7. To change default session time-outs, select **General > Session Options**.
8. In the Session lifetime section, specify **Max. Session Length** in minutes. The remaining session time appears on the Pulse interface of the mobile device client in the format days hours:minutes:seconds. The other session settings are not applied to mobile clients.
9. Select **Users > User Realms > New User Realm**.
10. Specify a name and, optionally, a description and then click **Save Changes** to create the realm and to display the realm option tabs.
11. On the Authentication Policy tab for the realm, click **Host Checker** and enable the optional Pulse Mobile Security check to require that mobile device users have Pulse Mobile Security software installed and enabled. See [“Junos Pulse for Mobile Devices Overview” on page 173](#) for more information.
12. On the Role Mapping tab for the realm, create a new rule that maps all users to the Android role you created earlier in this procedure.

- Related Documentation**
- [Host Checker for Pulse Android Clients on page 194](#)
 - [Allowing Junos Pulse for Android Users to Save Webmail Password on page 194](#)
 - Resource Policies

Allowing Junos Pulse for Android Users to Save Webmail Password

A Web bookmark on the role for Android users allows users to access e-mail through a Web link. You can allow users of the Pulse for Android app to save their e-mail password when they login to the e-mail system. After you have created a Mobile Webmail bookmark for the role used by Android users, enable password the option for user to save their e-mail password by doing the following.

1. Open the role you created for Android users.
2. Click **General > Session Options**.
3. In the section labeled **Persistent Password Caching**, select **Enabled**.
4. Click **Save Changes**.

- Related Documentation**
- [Configuring a Role and Realm for Pulse for Android on page 192](#)
 - [Host Checker for Pulse Android Clients on page 194](#)

Host Checker for Pulse Android Clients

Host Checker is a component of Junos Pulse that reports the integrity of Android 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 Android 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.
- **Root Detection**—Rooting is a process that allows Android users to gain root access to the operating system and bypass usage and access limitations imposed by device manufacturers and carriers. With a rooted device, a user can install applications that are not available and have not been certified by the device manufacturer or by the app store process. Rooted devices expose the device to a greater risk of running malicious applications. Host Checker can detect rooted devices and then allows or deny network access based on the Host Checker enforcement policy.

- **Mobile Security Suite**—Pulse Mobile Security Suite (MSS) for Android supports antivirus, antispam, and features that help protect the device if it is lost or stolen: remote wipe, remote lock, and locate. Host Checker enables you to require that an Android device have the Pulse Mobile Security Suite installed and enabled. The Pulse MSS is detected by 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.



NOTE: Junos Pulse Secure Access Service software release 7.1 (IVE OS 7.1R1) introduced a different implementation of this feature, and that implementation is still available in subsequent releases of the software. In the earlier implementation, You can enable a Mobile Security Check as part of Host Checker component of a realm authentication policy. Although you can still use this earlier implementation of the Mobile Security Suite check, we recommend that you employ the Host Checker policy rather than the realm authentication method. The two methods are compatible so you can enable both. However, enabling both methods is not recommended because that would cause Pulse Secure Access Service to run two different checks to accomplish one task.

Related Documentation

- [Configuring Host Checker for Junos Pulse Android Clients on page 195](#)
- [Implementing Host Checker Policies for Junos Pulse for Android Clients on page 197](#)
- [Junos Pulse Mobile Security Overview on page 217](#)
- Host Checker and Trusted Network Computing

Configuring Host Checker for Junos Pulse Android Clients

Host Checker policies can be part of a larger Host Checker configuration that applies to many different types of clients or to Android devices only.

To create a Host Checker policy for Android 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 Android HC Policy.

4. Click the Mobile tab, and then click the Android 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-Android-2-2-or-higher. Rule names cannot include spaces.
 - b. Specify the criteria. For example, to enforce Android 2.2 or higher, create two conditions: Equal to 2.2 and Above 2.2.

Host Checker supports Android versions 1.6 through 3.1.
 - c. Click **Save Changes**.
 - **Rooting Detection**—Rooting is a process that allows Android users to gain root access to the operating system and bypass usage and access limitations imposed by manufacturers and service providers. With a rooted device, an Android user can install applications that have not been certified through the app store process. Rooted devices possess a greater risk of running malicious applications.
 - a. Specify a descriptive name for this rule. For example, No-Android-root.
 - b. The **Don't allow rooted devices** check box is enabled by default.
 - c. Click **Save Changes**.
 - **Mobile Security Suite**—Pulse Mobile Security Suite (MSS) for Android supports features that help protect the device from viruses and malware and can help protect the device if it is lost or stolen
 - a. Specify a descriptive name for this rule. For example, Android-MSS.
 - b. In the Criteria section, the **Enforce Mobile Security Suite on the device** check box is enabled by default.
 - c. Click the **Terminate the user session if a threat/virus is found** box to have the Pulse server end the VPN session if Host Checker finds a virus or malware on the device. The user should be instructed to run the Pulse Mobile Security Suite virus scan on their device and remove the threats to before attempted to establish a VPN connection. The Host Checker policy allows you to enable custom instructions and provide instructions to users that appear if Host Checker finds an issue on the device.
 - d. Click **Save Changes** to save the rule and open the Host Checker Policy page.
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 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 is returned by Host Checker or integrity measurement verifier (IMV) and explains why the client machine does not meet the Host Checker policy requirements. For example, if the rooting detection policy fails, Pulse displays, "A rooted device is not allowed to access the network. Please contact your network administrator."
8. When you are finished, click **Save Changes**.

Related Documentation

- [Host Checker for Pulse Android Clients on page 194](#)
- [Implementing Host Checker Policies for Junos Pulse for Android Clients on page 197](#)
- [Junos Pulse Mobile Security Overview on page 217](#)

Implementing Host Checker Policies for Junos Pulse for Android Clients

After you create one or more Host Checker policies for Android 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 Android 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 Android device and allows access.
 - **Require and Enforce**—Requires that the Android device be in compliance with the Host Checker policy. Pulse Secure Access Service downloads Host Checker to the Android 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 Android device is allowed access if it passes any of the Require and Enforce policies. The Cache Cleaner policy does not apply to Android 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 Android 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 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 Android device is allowed access if it passes any of the Require and Enforce policies. The Cache Cleaner policy does not apply to Android devices.
5. Click **Save Changes**.

Related Documentation

- [Host Checker for Pulse Android Clients on page 194](#)
- [Configuring Host Checker for Junos Pulse Android Clients on page 195](#)
- [Host Checker and Trusted Network Computing](#)

Junos Pulse for Android Error Message Reference

The following error message summary for Junos Pulse for Android describes possible issues and suggests resolution actions where possible.

Table 15: Junos Pulse for Android Error Messages

Message	Possible Causes	Suggested Actions
The certificate for this server is invalid. Tap Accept to connect to this server anyway.	The server certificate for the page received from the Pulse server is not valid.	<p>Tap View Certificate to examine the certificate.</p> <p>Tap Accept and open the URL.</p> <p>Tap Decline. The connection attempt is ended. Contact the Pulse administrator.</p>

Table 15: Junos Pulse for Android Error Messages (*continued*)

Message	Possible Causes	Suggested Actions
Session disconnected due to invalid certificate.	The Pulse client downloads session information from the Pulse server and the certificate received from the server does not match the stored session certificate. While accessing e-mail or intranet, the certificate received from Pulse server does not match the previously stored session certificate.	Click the Close button on the Alert dialog to return to home screen. Try the operation again. If the error occurs again, contact the Pulse administrator.
On the Pulse client status screen, the VPN status appears as Not Supported.	The device does not support VPN.	Click the Close button on the Alert dialog to return to home screen. Try the operation again.
Failed to connect to the server.	Sign-in Process failed.	Check the network connection (for example, Wi-Fi, 3G, etc.), and then try the operation again.
Failed to process the HTML information from the server.	Sign-in Process failed.	Try the operation again. If the error occurs again, contact the Pulse administrator.
Your session was terminated. Please connect again.	An invalid URL was used while accessing intranet and e-mail pages.	Reconnect to the Pulse server. If the error occurs again, contact the Pulse administrator.
Compliance Check couldn't be completed.	Host checker compliance check could not be completed during sign-in process.	Try the operation again. If the error occurs again, contact the Pulse administrator.

- Related Documentation**
- [Junos Pulse for Apple iOS Overview on page 177](#)
 - [Configuring a Role and Realm for Pulse for Android on page 192](#)

Launching the Junos Pulse for Android App Using a Command

The Junos Pulse for Android VPN API enables you to start (or stop) a Junos Pulse VPN connection from an external Android app. This feature requires Junos Pulse for Android R4.0 or higher. If you implement the API call so that it provides all necessary information, Pulse starts and establishes a VPN connection with no input from the user, and then passes a result code and corresponding data back to the external app. If the API call does not include all of the necessary information, for example, no password is specified, the Pulse login page appears and the user must provide the required information.

When Pulse is launched programmatically to initiate a VPN connection, the following connection behaviors occur.

- If Pulse is not already installed on the device, an error occurs. If Pulse is not already running, Pulse is launched. The next step depends on the current Pulse connection status and configuration. One of the following occurs:
- If Pulse does not already have an active connection to a Pulse Secure Access server, it uses an existing configuration to establish a VPN connection to the Pulse server.
- If Pulse does not already have an active connection, and it does not already have a configuration for the target Pulse server, Pulse opens the Add Configuration screen and populates the login fields that are included in the call. The user must specify any missing information.
- If the Pulse app is already connected to the Pulse server specified in the connection request, the API returns status that Pulse is already connected. It is the calling application's responsibility to maintain state of which Pulse server it is connected to in order to make the correct API call.

Usage notes:

- If the user has specified the username, realm, and role when creating the VPN configuration in the Junos Pulse app, those values are used to auto-fill the username, realm, and role for the login pages during login.
- Error messages related to authentication or Host Checker failure are not supported. In case of incorrect user credentials, the Pulse login screen appears and the user must manually provide credentials.
- The VPN notification icon appears on the Android device after the VPN connection is established and it is cleared when the VPN session is disconnected.

To launch Pulse and connect to the Pulse server from an external Android app, you use an explicit intent. The explicit intent names the component to be called by the Android system by using the Java class as the identifier. Pulse authenticates using the Android Webkit framework. It passes the result code and corresponding data back to the external app.

You use the VPN status command to determine run time status of the VPN connection. The status command allows you to handle the use case where the VPN connect command

results in a successful session connect with the Pulse server, but the VPN tunnel was not established.

To stop the VPN connection, the external app sends an explicit intent to Pulse to disconnect, and then Pulse disconnects the VPN connection and passes a result code back to the app.

Junos Pulse for Android VPN API Reference

Junos Pulse for Android VPN API enables the VPN connection as follows.

1. The external app sends an Android explicit intent to the Junos Pulse app to authenticate the user and start a VPN connection. The intent contains VPN commands and parameters.
2. Pulse checks if the device supports VPN. If not then it returns that information to the calling app.
3. For a VPN connect command, Pulse checks the user credentials passed through the intent. For a URL that is not already defined on the device, a new Pulse connection profile is created and shown to the user to save or update. The intent then authenticates using the Webkit framework and starts the VPN connection.
4. For a VPN status command, the status of a the VPN connection is returned. Status includes the Pulse server IP address, data sent, data received, and the connection start time.
5. For a VPN disconnect command, Pulse disconnects the user session and stops the VPN connection.
6. Pulse passes the result code and corresponding data in a call back to the external app. The external app must implement the callback function.

The VPN API will internally use the Android Intent API calls to add extended data to the intent. The name must include a package prefix.

```
public Intent putExtra (String name, int value)
```

```
public Intent putExtra(String name, String value)
```

Explicit Intent Target Component

Package name/Class

name—net.juniper.junos.pulse.android/net.juniper.junos.pulse.android.ui.ExplicitIntentActivity

Explicit Intent API — VPN Connect

Command Extra

Extra Name: "Junos Pulse Vpn Command"

Extra Value and Type: 1 [integer]

Required: Yes

Command Parameters Extra:

1. Extra Name: "Url"
Extra Value and Type: Valid SA Url [String]
Required: Yes
2. Extra Name: "Username"
Extra Value and Type: Valid Username [String]
Required: No
3. Extra Name: "Password"
Extra Value and Type: Valid Password [String]
Required: No
4. Extra Name: "Realm"
Extra Value and Type: Valid Realm [String]
Required: No
5. Extra Name: "Role"
Extra Value and Type: Valid Role [String]
Required: No
6. Extra Name: "Certpath"
Extra Value and Type: Valid certificate file path on device [String]
Required: No
7. Extra Name: "Keypath"
Extra Value and Type: Valid certificate key file path on device [String]
Required: No

Callback Return Code and Intent Parameters

1. JUNOS_PULSE_RETURN_CODE_SESSION_CONNECTED [Value = 6]
2. JUNOS_PULSE_RETURN_CODE_SESSION_DISCONNECTED [Value = 7]
Intent Params: None
Return code 7 indicates that VPN disconnect succeeded.
3. JUNOS_PULSE_RETURN_CODE_VPN_NOT_SUPPORTED [Value = 3]
Intent Params: None
Return code 3 indicates that VPN is not supported on this device. VPN using Junos Pulse is not supported on all devices. All pre-Android ICS, non-Samsung, non-Lenovo, non-plugin devices should return this status code. Junos Pulse for Android is supported on Android 2.1 and higher (API Level 7) devices. Devices that are running an earlier version of Android do not see Pulse on Google Play.

Explicit Intent API — VPN Disconnect**Command Extra**

Extra Name: "Junos Pulse Vpn Command"
Extra Value and Type: 2 [integer]
Required: Yes

Command Parameters Extra: None

Callback Return Code and Intent Parameters

1. JUNOS_PULSE_RETURN_CODE_SESSION_DISCONNECTED [Value = 7]
 Intent Params: None
 Return code 7 indicates that VPN disconnect succeeded.
2. JUNOS_PULSE_RETURN_CODE_VPN_NOT_SUPPORTED [Value = 3]
 Intent Params: None
 Return code 3 indicates that VPN is not supported on this device. VPN using Junos Pulse is not supported on all devices. All pre-Android ICS, non-Samsung, non-Lenovo, non-plugin devices should return this status code. Junos Pulse for Android is supported on Android 2.1 and higher (API Level 7) devices. Devices that are running an earlier version of Android do not see Pulse on Google Play.

Explicit Intent API — VPN Check Status

Command Extra
 Extra Name: "Junos Pulse Vpn Command"
 Extra Value and Type: 3 [integer]
 Required: Yes

Command Parameters Extra: None

Callback Return Code and Intent Parameters

1. JUNOS_PULSE_RETURN_CODE_VPN_CONNECTED [Value = 1]
 Intent Params:
 - a. Extra Name: "Ipaddr"
 Extra Value and Type: Valid Gateway Url [String]
 Required: Yes
 - b. Extra Name: "Starttime"
 Extra Value and Type: VPN Start Time [String]
 Required: Yes
 - c. Extra Name: "Tx"
 Extra Value and Type: Bytes Sent [integer]
 Required: Yes
 - d. Extra Name: "Rx"
 Extra Value and Type: Bytes Received [integer]
 Required: Yes
2. JUNOS_PULSE_RETURN_CODE_VPN_DISCONNECTED [Value = 2]
 Intent Params: None
3. JUNOS_PULSE_RETURN_CODE_VPN_NOT_SUPPORTED [Value = 3]
 Intent Params: None
 Return code 3 indicates that VPN is not supported on this device. VPN using Junos Pulse is not supported on all devices. All pre-Android ICS, non-Samsung, non-Lenovo, non-plugin devices should return this status code. Junos Pulse for Android is supported

on Android 2.1 and higher (API Level 7) devices. Devices that are running an earlier version of Android do not see Pulse on Google Play.

Pulse returns the following result code if any unsupported command is issued:

JUNOS_PULSE_RETURN_CODE_VPN_INVALID_COMMAND [Value = 5]

Intent Params: None

Return Code 5 indicates that the third-party app has called a VPN command value that is not supported.

Explicit Intent API — Example

```
Intent intent = new Intent();
intent.setComponent(ComponentName.unflattenFromString("net.juniper.junos.pulse.android/
net.juniper.junos.pulse.android.ui.ExplicitIntentActivity"));
//Set the intent with authentication parameters like username, password.
JunosPulseActivityIntent.putExtra("Junos Pulse Vpn Command", 1);
JunosPulseActivityIntent.putExtra("Url", "connect4.juniper.net");
JunosPulseActivityIntent.putExtra("Username", "test");
JunosPulseActivityIntent.putExtra("Password", "password");
JunosPulseActivityIntent.putExtra("Realm", "Users");
startActivity(JunosPulseActivityIntent);
```

Related Documentation

- [Junos Pulse for Android Overview on page 191](#)

Junos Pulse for Nokia Symbian Devices

- Junos Pulse for Symbian Overview on page 205

Junos Pulse for Symbian Overview

Junos Pulse can create an authenticated session between a device running Nokia Symbian and Pulse secure access service. Junos Pulse for Symbian devices uses IKEv2 (Internet Key Exchange) to set up a security association in the IPsec protocol suite. Junos Pulse enables secure connectivity to Web-based applications and data based on identity, realm, and role. Junos Pulse is available for download from the Nokia Ovi store.

The *Junos Pulse Mobile Supported Platforms Guide*, which is available at <http://www.juniper.net/support/products/pulse/mobile/> lists the mobile device OS versions supported by Pulse and the security features supported on each mobile device OS.

The Nokia Symbian relies on IKEv2 authentication and that requires a certificate. Before you begin, be sure you have completed the following certificate configuration steps:

- Import the valid Device Certificate to the Secure Access Server.

Configuration > Certificates > Device Certificate

- Import the Trusted Client CA certificate.

Configuration > Certificates > Trusted Client CAs

- Import the Trusted Server Certificate

Configuration > Certificates > Trusted Server CAs

- Configure a valid NC profile to work with IKEv2.

Configuring Pulse Secure Access Service for Junos Pulse on Symbian Devices

To enable access from a Symbian device to Pulse Secure Access Service, the device user must download and install the Junos Pulse app, and the Pulse administrator must configure specific realm and role settings on the Pulse server.

To configure Pulse Secure Access Service for Symbian device access:

1. Log in to the Pulse server admin console.
2. Select **User Roles > New User Role**.

3. On the New Role page, specify a name for the role and, optionally, a description. Make note of the name because later in this procedure, you create a realm and map realm users to this role.
4. In the Access Features section of the New Role page, select the **IKEv2** check box.
5. Click **Save Changes** to create the role and to display the role configuration tabs.
6. Select **Web > Bookmarks** and then click **New Bookmark**.

You must create bookmarks to enable the buttons that appear in the Pulse for Android user interface. Typically, you create a bookmark for your company intranet and for Web e-mail. You must create an e-mail bookmark to enable the e-mail button within the Pulse interface on the Android, and that e-mail bookmark must be named **Mobile Webmail**.

Figure 15: Creating the E-mail Bookmark for the Pulse Client

The screenshot shows the Juniper Central Manager interface for configuring a Web Bookmark. The left sidebar contains a navigation menu with categories like System, Authentication, Administrators, Users, Maintenance, and Troubleshooting. The main content area is titled 'Web Bookmark' and includes the following sections:

- Name:** A text field containing 'Mobile Webmail'.
- Description:** A text area containing 'special bookmark for Junos Pulse'.
- Bookmark to:** A section with a '* URL:' field containing 'http://exchange3/owa'. To the right, an example URL is provided: 'Example: http://www.domain.com/ We recommend that you use the fully qualified domain name when entering the bookmark URL.'
- Auto allow:** A section with a note: 'Use auto-allow to automatically add this web bookmark for this role to the Web access control policy. In order for the auto-allow bookmark option to work properly, you must enter a fully qualified domain name in your bookmark URL.' Below this are three radio buttons: 'Auto-allow Bookmark' (checked), 'Only this URL', and 'Everything under this URL'.
- Display options:** A section with a checkbox 'Open the bookmark in a new window' and two sub-checkboxes: 'Do not display the Web browser's URL address bar' and 'Do not display the Web browser's menu and toolbar'.
- Save changes?:** Two buttons: 'Save Changes' and 'Save as Copy'.

A footnote at the bottom states: '* indicates required field'.



NOTE: Alternatively, you can use Web resource policies to define the bookmarks.



NOTE: To ensure that users see consistent bookmarks in the Pulse client UI no matter which server they are connected to, you should configure and enable user record synchronization, a feature of the Pulse Secure Access Service platform.

7. To change default session time-outs, select **General > Session Options**.
8. In the Session lifetime section, specify **Max. Session Length** in minutes. The remaining session time appears on the Pulse interface of the mobile device client in the format days hours:minutes:seconds. The other session settings are not applied to mobile clients.
9. Select **Users > User Realms > New User Realm**.
10. Specify a name and, optionally, a description. Then click **Save Changes** to create the realm and to display the realm option tabs.
11. On the Authentication Policy tab for the realm, click **Host Checker** and make sure that all Host Checker policies are disabled except for the optional Pulse Mobile Security check.

You can require that mobile device users have Pulse Mobile Security software installed and enabled.
12. On the Role Mapping tab for the realm, create a new rule that maps all users to the Symbian device role you created earlier in this procedure.

**Related
Documentation**

- [Junos Pulse Mobile Security Overview on page 217](#)
- Resource Policies
- About User Record Synchronization
- About Using Certificates on Secure Access Service

CHAPTER 13

Junos Pulse for Windows Mobile Devices

- [Junos Pulse for Windows Mobile Overview on page 209](#)
- [Configuring Junos Pulse Secure Access Service for Windows Mobile Endpoints on page 211](#)
- [Configuring Host Checker for Junos Pulse for Windows Mobile Clients on page 215](#)
- [Junos Pulse Mobile Security Overview on page 217](#)

Junos Pulse for Windows Mobile Overview

Junos Pulse supports Secure Application Manager (SAM). SAM provides remote access using application names and destinations instead of network subnets. SAM does not require a virtual adapter or virtual IP address on the endpoint so SAM connectivity is secure. SAM provides access to client/server applications and thin client solutions without provisioning a VPN tunnel.

Junos Pulse can provide secure, application-level, remote access to enterprise servers from client applications on mobile endpoints that are running the Windows Mobile operating system. You can provide secure access to individual client/server applications, such as Lotus Notes, Microsoft Outlook, Citrix, and ActiveSync, as well as to application servers.



NOTE: Junos Pulse for Windows Mobile is available for download from the [Juniper Web](#).

Pulse Release 1.0, 2.0, and 3.0 and Pulse SAM Connectivity

The SAM client software has evolved to meet the needs of different environments. [Table 16 on page 210](#) describes the progression of Pulse/SAM client software.

Table 16: Pulse/SAM Client Version Summary

Pulse/SAM Version	Supported Platforms	Description	Notes
Pulse R1.0	Windows Mobile	WSAM client that is installed from the Pulse Secure Access server.	Supports Host Checker.
Included with SSL/VPN software R7.0 and R7.1	Windows XP		
	Windows Vista		
	Windows 7		
Pulse R2.0	Windows Mobile (6.0, 6.1, and 6.5) NOTE: Junos Pulse R2.0 is supported on touch-based Windows Mobile devices only.	Pulse for Windows Mobile; available for download from juniper.net .	<p>If you install the Pulse 2.0 mobile client on a Windows Mobile device that already has Pulse R1.0, the installation detects the presence of the old client and removes it prior to installing the new client. It also detects and removes Host Checker. Host Checker is not supported.</p> <p>If Pulse R2.0 for Windows Mobile is installed on a Windows Mobile device, the user should not use a browser to sign into a realm that has Pulse R1.0 enabled. Pulse R1.0 cannot detect if Pulse R2.0 for Windows Mobile is already installed, and so it prompts the user to install Pulse R1.0.</p> <p>NOTE: If Pulse R2.0 is installed on a Windows Mobile device, and the user connects to a role that has Host Checker enabled, the user is prompted to install Host Checker. However, if the user allows the installation, nothing happens. To avoid this scenario, you should create a separate role for Pulse R2.0 for Windows Mobile devices.</p> <p>Pulse 2.0 for Windows Mobile supports the optional Pulse Mobile Security Suite.</p>
Pulse R3.0	Windows XP	Pulse R3.0 incorporates SAM functionality as a native Pulse connection method.	Supports Host Checker.
Included with Pulse Secure Access Service software R7.2.	Windows Vista		
	Windows 7		

The *Junos Pulse Mobile Supported Platforms Guide*, which is available at <http://www.juniper.net/support/products/pulse/mobile/> lists the mobile device OS versions supported by Pulse and the Pulse Mobile Security Suite features supported on each mobile device OS.



NOTE: Pulse Secure Access Service also supports a Java-based SAM client (JSAM). The JSAM client can be deployed from Pulse Secure Access Service to any endpoint that supports Java.

- Related Documentation**
- [Configuring Junos Pulse Secure Access Service for Windows Mobile Endpoints on page 211](#)
 - [Secure Application Manager Overview](#)

Configuring Junos Pulse Secure Access Service for Windows Mobile Endpoints

This section describes how to configure Junos Pulse Secure Access Service to support Pulse for Windows Mobile endpoints.

To enable SAM and configure a role for Windows Mobile endpoints:

1. Log in to the Pulse Secure Access Service admin console.
2. Select **User Roles > New User Role**.
3. On the New Role page, specify a name for the role and, optionally, a description. Make note of the name because later in this procedure, you create a realm and map realm users to this role.
4. In the Access Features section of the New Role page, select the **Secure Application Manager** check box and then select **Windows version**.



NOTE: In the Options section, do not enable Junos Pulse. If you select Junos Pulse and Secure Application Manager, Windows version, you enable the Pulse/SAM access method, which is used for Windows XP, Vista, and Windows 7. The Junos Pulse check box must be left cleared to enable the role for Pulse for Windows Mobile clients.

5. Click **Save Changes** to create the role and to display the role configuration tabs.
6. Select **Web > Bookmarks** and then click **New Bookmark**.

You must create bookmarks to enable the buttons that appear in the Pulse for Windows Mobile user interface. Typically, you create a bookmark for your company intranet and for Web e-mail. You must create an e-mail bookmark to enable the e-mail button within the Pulse for Windows Mobile app, and that e-mail bookmark must be named **Mobile Webmail**.

Figure 16: Creating the E-mail Bookmark for the Pulse Client

Central Manager Help | Guidance | Sign Out

Roles > Pulse > Web Bookmark

Name: Mobile Webmail

Description: special bookmark for Junos Pulse

Bookmark to

*** URL:** http://exchange3/owa Example: http://www.domain.com/ We recommend that you use the fully qualified domain name when entering the bookmark URL.

Auto-allow

Use auto-allow to automatically add this web bookmark for this role to the Web access control policy. In order for the auto-allow bookmark option to work properly, you must enter a fully qualified domain name in your bookmark URL.

☒ **Auto-allow Bookmark**

☐ Only this URL

☒ Everything under this URL

Display options

☒ **Open the bookmark in a new window**

☐ Do not display the Web browser's URL address bar

☐ Do not display the Web browser's menu and toolbar

Save changes?

* indicates required field



NOTE: Alternatively, you can use Web resource policies to define the bookmarks.



NOTE: To ensure that users see consistent bookmarks in the Pulse app no matter which server they are connected to, you should configure and enable user record synchronization, a feature of the Pulse Secure Access Service platform.

Most of the General and SAM tab options apply to Pulse for Windows Mobile clients. The following describes the role options that you can employ to manage Windows Mobile sessions.

General > Restrictions

Source IP—Control from which IP addresses users can access the Web portal sign-in page, be mapped to a role, or access a resource.

Browser—Allow or deny access to the role based on the browser's user agent string.

Certificate—Allow all users or only users with a signed client-side certificate.

Host Checker—Check compliance with defined policies. You must first define appropriate Host Checker policies before you can assign them to the role.

General > VLAN/Source IP

VLAN and Select Source IP—To direct traffic to specific sites based on the role, you can define a source IP alias for each role, and then use the alias 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 the alias. 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.

Max. Session Length—A session can remain active for the number of minutes set in this option. The session ends when it reaches this limit. Idle Timeout, Reminder Time, and Enable Session Extension features are not applicable to Windows Mobile clients.

General > Session Options

Idle Timeout—The maximum time a session can remain idle (no traffic) before the server ends the session.

Max. Session Length—The maximum time for a session before the server ends the session.

Reminder Time—The number of minutes prior to a session end when the server notifies the user that the session will end soon.

Enable Session Extension—Not supported by the Pulse for Windows Mobile app.

General > UI Options

UI Options—The settings on this page define the Pulse Secure Access Service Web portal page.

SAM > Applications

Add Application—We recommend that you use resource profiles to specify the applications available to Pulse for Windows Mobile users, but you can use role and resource policy settings instead.

SAM > Options

Auto-uninstall Secure Application Manager—This feature is not applicable to the Windows Mobile client. Users must download and install Pulse for Windows Mobile before the Windows Mobile device can connect to the Pulse Secure Access Service.

Prompt for username and password for intranet sites—If you enable this option, the Pulse Secure Access Service requires users to enter sign-in credentials before connecting to sites on your internal network. This option changes Internet Explorer's intranet zone setting so that Internet Explorer always prompts the user for network sign-in credentials for an intranet site.

Auto-upgrade Secure Application Manager—This feature is not applicable to the Pulse for Windows Mobile app.

Resolve only host names with domain suffixes in the device DNS domains—If you enable this option, users can only browse to Web sites that are part of their login domain.

Session start script and Session end script—This feature is not applicable to the Pulse for Windows Mobile app.

To use resource profiles to specify the applications available to Junos Pulse for Windows Mobile users:

1. Create resource profiles that enable access to client applications and destinations and configure the appropriate settings. Select **Users > Resource Profiles > SAM > Client Applications**.
2. Click **New Profile**.
3. From the Type list, select **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, SAM verifies that the checksum value of the executable matches this value. If the values do not match, SAM notifies the user that the identity of the application could not be verified and does not forward connections from the application to the server.
 - **Lotus Notes**—Select this option to have SAM intermediate traffic from the Lotus Notes fat client application.
 - **Microsoft Outlook**—Select this option to have SAM intermediate traffic from the Microsoft Outlook application.
 - **NetBIOS file browsing**—Select this option to have SAM intercept NetBIOS name lookups in the TDI drivers on port 137.
 - **Citrix**—Select this option to have SAM intermediate traffic from 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 Pulse Secure Access Service in the WSAM Destination list so that LDAP and Kerberos traffic can be proxied and sent to the Pulse server.
 - Configure a WSAM Access Control Policy to allow access to all domain controllers.



NOTE: You can 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.

5. Enter a unique name and optionally a description for the resource profile.

6. In the **Autopolicy: SAM Access Control** section create supporting auto policies and assign the policies to the role:
 - a. If it is not already enabled, select the **Autopolicy: SAM Access Control** check box.
 - 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.
 - 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 server also automatically enables the SAM option in the roles General > Overview page for all of the roles you select.
9. Click **Save Changes**.
10. Select **Users > User Realms > New User Realm**.
11. Specify a name and, optionally, a description and then click **Save Changes** to create the realm and to display the realm option tabs.
12. On the Authentication Policy tab for the realm, click **Host Checker** and enable the optional Pulse Mobile Security check to require that mobile device users have Pulse Mobile Security software installed and enabled.
13. On the Role Mapping tab for the realm, create a new rule that maps all users to the Windows Mobile role you created earlier in this procedure.

Related Documentation

- [Configuring Host Checker for Junos Pulse for Windows Mobile Clients on page 215](#)
- About User Record Synchronization
- Resource Policies
- [Junos Pulse Mobile Security Overview on page 217](#)

Configuring Host Checker for Junos Pulse for Windows Mobile Clients

You can configure Host Checker to enforce policies for handheld devices, such as PDAs and smart phones, that run the Windows Mobile operating system. 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 Pulse server Web portal. 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 server. When the server upgrades to a newer version of Host Checker, the Windows Mobile device automatically updates the next time the user connects to the server. To remove Host Checker from the device, use the Remove Programs applet in the Settings panel of the device.

To create a Host Checker policy for Windows Mobile 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 WinMobile HC Policy.

4. Click the Mobile tab, and then click the Windows Mobile tab.
5. In the Rule Settings section, click **Select Rule Type**, select one of the following options, and then click **Add**:
 - **OS Checks**—To specify the Windows Mobile version that must be installed on the device. :
 - **Ports**—Allows you to specify the ports numbers that can be used to access the server.
 - **Process**—Allows you to specify a specific process that must be running on the endpoint.
 - **File**—Allows you to verify the existence of a particular file on the endpoint.
 - **Registry Setting**—Check for a specific value in a registry setting.
 - **Machine Certificate**—Allows you to verify that the endpoint has a specific machine certificate installed. When validating a client-side CA certificate, the Pulse server checks that the certificate is not expired or corrupt and that the certificate is signed by a CA that the Pulse server recognizes
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 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.
- **Kill processes**—Terminate specific processes on the endpoint.
- **Delete files**—Delete specific files on the endpoint.
- **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.

8. When you are finished, click **Save Changes**.
**Related
Documentation**

- [Host Checker for Pulse iOS Clients on page 183](#)
- [Host Checker for Pulse Android Clients on page 194](#)

Junos Pulse Mobile Security Overview

The Junos Pulse Mobile Security Suite is an optional feature of the Pulse application for mobile devices. It provides mobile security and device management. It protects mobile devices against viruses, spyware, Trojans and worms, and includes tools to mitigate the risks of lost and stolen devices.

The Junos Pulse Mobile Security Suite provides the following features:

- *Antivirus*—Protects mobile devices against viruses and malware delivered via e-mail, Short Message Service (SMS), Multimedia Messaging Service (MMS), direct download, Bluetooth, or infrared transmission.
- *Firewall*—Protects users from threats by filtering and blocking TCP/IP traffic. A bidirectional, port-based and IP-based packet filtering option protects the mobile device from harmful or questionable content and prevents malicious content from being transferred to the device. The firewall monitors cellular data and WI-FI traffic.
- *Antispam*—Provides call and message filtering. Users can prevent interruptions and disturbances by blocking voice and SMS spam by customizing contacts into groups of blacklisted (blocked) numbers.
- *Device monitoring and control*—Provides real time content monitoring of SMS, MMS, and e-mail messages. The administrator can access call logs, address books, and even photos stored on the device.
- *Loss and theft protection*—Loss and theft protection features include remote lock, remote wipe, GPS tracking, backup and restore, remote alarms, and SIM change

notification by means of commands run from the Pulse Mobile Security Gateway by the administrator.

- *Backup and restore*—Allows a user to back up the contacts and calendar PIM data stored on the device.

Device Management—The Pulse Mobile Security Gateway provides a management interface for managing and controlling mobile devices. The Pulse Mobile Security Gateway enables you to create user accounts and profiles, create rules and policies for devices, remotely execute features on the client, remove undesirable applications from devices, and generate reports related to malware detection and security levels. For more information, see the [Junos Pulse Mobile Security Gateway documentation](#).

**Related
Documentation**

- [Junos Pulse for Apple iOS Overview on page 177](#)
- [Junos Pulse for Android Overview on page 191](#)
- [Junos Pulse for Symbian Overview on page 205](#)
- [Junos Pulse for Windows Mobile Overview on page 209](#)

PART 4

Index

- [Index on page 221](#)

Index

Symbols

3G wireless.....	169
802.1x connections	
connection, Pulse Secure Access Service.....	89
Pulse - OAC comparison.....	163
Pulse Access Control Service.....	26
Remote Desktop Protocol and machine authentication.....	38
802.1x connection	
certificate.....	7
reboot on upgrade.....	10

A

acceleration	
client policies.....	129
client status.....	130
troubleshooting.....	126
Access Manager.....	122
ACE server.....	25, 88
ActiveX	
Web installation.....	148
adapter type.....	26, 89
address resolution	
IPv6.....	16
admin privileges.....	144
Advanced Connectivity license	
adding, Pulse Secure Access Service.....	115
advanced endpoint defense	
Pulse Access Control Service.....	57
Pulse Secure Access Service.....	108
AES.....	164
agentless	
sign-in notifications.....	66, 67
allow saving logon information	
Pulse Access Control Service.....	25
Pulse Secure Access Service.....	87
allow user connections	
Pulse Access Control Service.....	25
Pulse Secure Access Service.....	88

allow user to override connection policy	
App Acceleration connection option.....	27
connection option.....	27, 33, 90, 94
connection option, App Acceleration.....	90
connection option, SRX	27, 90
Android	
certificate authentication.....	191
antispyware	
Pulse Access Control Service.....	57
Pulse Secure Access Service.....	108
API	
Pulse for Android.....	200
App Acceleration connection option	
community string.....	27
Apple iPhone.....	180, 187
application acceleration	
deployment option.....	20
application-level remote access.....	81, 209
authentication	
SecurID.....	9
authentication methods.....	165
automatic updates.....	10
automatic upgrades.....	60, 112
autoscan lists.....	163
B	
binding server ID.....	148
BlackBerry.....	174
bound and unbound clients	
overview.....	9
software upgrades.....	61, 112
browser	
launching Pulse	149
browser session cookie.....	71

C

certificate	
certificate, Pulse Secure Access Service.....	22
roles, Pulse Secure Access Service.....	22
selection.....	25, 87
smart card.....	165
support.....	165
certificate authentication	
Android.....	191
Pulse Access Control Service.....	43
Pulse Secure Access Service.....	80
certificate store selection	
Pulse Access Control Service.....	43
Pulse Secure Access Service.....	80

CHAP inner authentication.....	164	connection set options.....	24
CIFS acceleration		adapter type.....	26, 89
client policies.....	129	allow saving logon information.....	25, 87
client status.....	130	allow user connections.....	25, 88
client errors.....	11	allow user to override connection	
OS X.....	11	policy.....	27, 33, 90, 94
clients, Junos Pulse		allow user to override connection policy, App	
configuring adjacencies.....	129	Acceleration.....	27
configuring policies.....	129	allow user to override connection policy,	
distributing through SMS or Pulse Secure		SRX.....	27
Access Service.....	131	community string.....	27, 90
download from a MAG Series or WXC		Connection Identity.....	26
gateway.....	127	display splash screen.....	25, 88
download from Pulse Secure Access		dynamic certificate trust.....	25, 88
Service.....	126	dynamic connections.....	25, 88
enable downloads	128	hiding or displaying.....	25, 88
loading a client image.....	130	non-broadcast.....	89
uninstall.....	128	outer username.....	26, 89
viewing status.....	130	Pulse Secure Access Service.....	87, 89
command line launcher.....	168	scan list.....	89
examples.....	158	server certificate DN.....	26, 89
commands		wireless suppression.....	26, 88
Pulse launcher for Android.....	200	connectivity	
community string.....	27, 90	wireless.....	16
component set options		cookie.....	71
Pulse Access Control Service.....	46	credential provider.....	165, 168
Pulse Secure Access Service.....	98	Access Control Service.....	39
component sets, configuring for Junos		Secure Access Service.....	76
Pulse.....	48, 99	customer support.....	xii
compression		contacting JTAC.....	xii
client policies.....	129	D	
client status.....	130	default deployment.....	143
config file.....	146	default installer.....	144
ConfigMgr.....	51, 103, 105	defaults, Pulse configuration.....	19
configuration, Junos Pulse client		deleting	
displaying	130	Pulse client log files.....	15
connection option		deployment options	
allow user to override connection policy, App		overview.....	19
Acceleration.....	90	diagnostics.....	166
allow user to override connection policy,		distributing Junos Pulse clients through SMS or	
firewall.....	90	Pulse Secure Access Service.....	131
connection properties.....	146	DNS lookups.....	46, 98
connection rules		DNS server search.....	169
configuring.....	44, 96	documentation	
connection set		comments on.....	xii
Pulse Access Control Service.....	30	related documentation.....	xi
server.....	94	download a Junos Pulse client	126, 127

- dynamic certificate trust
 - Pulse Access Control Service.....25
 - Pulse Secure Access Service.....88
- dynamic connections.....7, 19, 149
 - overview.....9
 - Pulse Access Control Service.....25
 - Pulse Secure Access Service.....88
- dynamic VPNs
 - configuration overview.....122
- E**
 - EAP methods.....164
 - EAP-GTC inner authentication.....164, 165
 - EAP-JUAC inner authentication.....164, 165
 - EAP-MD5 inner authentication.....164, 165
 - EAP-MSCHAPv2 inner authentication.....164
 - EAP-PEAP outer authentication.....164
 - EAP-TLS outer authentication.....164
 - EAP-TTLS outer authentication.....164
 - EES (Enhanced Endpoint Security)
 - Pulse Access Control Service.....57
 - Pulse Secure Access Service.....108
 - Enable Session Extension.....23
 - Pulse Access Control Service.....23
 - encryption methods
 - Pulse Access Control Service.....164
 - Enhanced Endpoint Security
 - Pulse Access Control Service component set option.....47
 - Enhanced Endpoint Security (EES)
 - Pulse Access Control Service.....57
 - Pulse Secure Access Service.....108
 - error messages.....11
 - OS X.....11
 - ESP transport mode.....168
 - Exchange acceleration
 - client policies.....129
 - client status.....130
 - explicit intent
 - API for Android.....200
 - exporting
 - Junos Pulse client software or configuration.....131
 - extend session.....167
- F**
 - FIPS.....165, 169
 - firewall access
 - configuring on SRX.....121
 - Forget Saved Settings.....25, 88
 - FTP servers, using
 - to load the Pulse client software.....130
- G**
 - GINA.....38, 76, 168
- H**
 - hard token.....9, 25, 88
 - hardware requirements.....10, 15
 - Heartbeat Interval.....22
 - and heartbeat interval.....22
 - Heartbeat Timeout.....22, 23
 - Host Checker
 - for Android clients.....194
 - for Android clients, configuring.....195
 - for Android clients, enabling.....197
 - for iOS clients, configuring.....184
 - for iOS clients, enabling.....186
 - for iOS clients, overview.....183
 - for Windows Mobile clients.....215
 - Pulse Secure Access service.....22
 - Shavlik on Pulse Access Control Service.....55
 - Shavlik on Pulse Secure Access Service.....107
 - Host Checker patch assessment policies.....8
 - Pulse Access Control Service.....49
 - Pulse Secure Access Service.....101
 - Host Enforcer.....166
 - hostname resolution.....16
- I**
 - server
 - component set option.....46
 - IF-MAP
 - configuring for session migration.....140
 - server and client.....140
 - IMCs and IMVs, overview.....50
 - Pulse Secure Access Service.....102
 - installation
 - Junos Pulse clients.....125
 - requirements.....10, 15, 16
 - installers
 - default.....144
 - preconfigured.....144, 150, 154
 - Web.....143, 148
 - Instant Virtual System.....66
 - integrity measurement collectors (IMCs) and verifiers (IMVs).....50
 - Pulse Secure Access Service.....102

iPass Enterprise Mobility Services.....	114
iPass integration.....	114
iPass Open Mobile.....	114
iPhone	
installing Pulse.....	187
SSL/VPN access.....	180
IPv6	
address resolution.....	16
IVS.....	66
J	
jail breaking detection	
for iOS clients.....	183
Java	
Web installation.....	148
Juniper Installer Service.....	144
Junos Pulse	
sign-in notifications.....	66, 67
Junos Pulse clients	
configuring adjacencies	129
configuring policies.....	129
configuring the Windows Firewall.....	126
distributing through SMS or Pulse Secure	
Access Service.....	131
download from a MAG Series or WXC	
gateway.....	127
download from Pulse Secure Access	
Service.....	126
enable downloads.....	128
loading a client image.....	130
uninstall.....	128
viewing status.....	130
Junos Pulse Collaboration Suite,	
enabling.....	90
overview.....	115
Junos Pulse installer, creating.....	150, 154
Junos Pulse Mobile Security Suite.....	xii
Junos Pulse, user experience.....	6
K	
Kaspersky.....	126
and application acceleration.....	32, 90
Kerberos SSO.....	167
L	
languages supported.....	11
Layer 2 credential provider	
Access Control Service.....	39
Layer 3 credential provider	
Access Control Service.....	39
learned user settings.....	25, 87
limit to subnet.....	23
loading software	
for Junos Pulse clients.....	130
Local Computer	
Pulse Access Control Service.....	43
Pulse Secure Access Service.....	80
localization.....	11
localized	
sign-in notifications.....	67
location awareness	
configuring.....	44, 96
location awareness rules.....	28, 92
overview.....	6
log files	
iOS devices.....	189
Pulse client, deleting.....	15
log viewer.....	166
logging in	
to download Junos Pulse client software	128
login notifications	
agentless.....	66, 67
Junos Pulse.....	66, 67
LZ compression	
client policies.....	129
client status.....	130
M	
MaAfee firewall.....	126
machine authentication.....	165
802.1X and Remote Desktop Protocol.....	38
certificate authentication.....	33, 75
configuration summary.....	33, 75
Pulse Access Control Service.....	33, 43
Pulse Secure Access Service.....	75, 80
machine settings.....	146
machine-only	
authentication.....	34
malware, Host Checker policy	
Pulse Access Control Service.....	57
Pulse Secure Access Service.....	108
manuals	
comments on.....	xii
MAPI acceleration	
client policies.....	129
client status.....	130
Max. Session Length.....	22

-
- MDM.....185, 188
 - messages.....11
 - OS X.....11
 - Microsoft System Center Configuration
 - Manager.....51, 103, 105
 - Mobile Device Management.....185
 - mobile device management.....188
 - Mobile Security detection
 - for Android clients.....195
 - for iOS clients.....183
 - MSCHAP inner authentication.....164
 - MSCHAPv2 inner authentication.....164
 - N**
 - NAT-T.....166
 - NetBIOS name lookups
 - SAM.....85
 - netmask.....23
 - Network Connect.....149
 - Network Sequence Caching
 - client policies.....129
 - client status130
 - Nokia Symbian
 - configuring access.....205
 - Norton firewall.....126
 - O**
 - OAC, feature comparison with Pulse.....163
 - Odyssey Access Client
 - compatible versions.....15
 - feature comparison with Pulse.....163
 - supported release.....15
 - Open Mobile.....114
 - OPSWAT IMV.....166, 168
 - OS detection
 - for Android clients.....194
 - for iOS clients.....183
 - outer username
 - 802.1X connection, Pulse Access Control
 - Service.....26
 - 802.1X connection, Pulse Secure Access
 - Service.....89
 - P**
 - PAP inner authentication.....164
 - password
 - saving web mail password for Android.....194
 - saving web mail password for iOS.....183
 - passwords
 - one-time.....25, 88
 - to download Junos Pulse client software.....128
 - patch assessment version monitoring.....8
 - patch assessment, in Host Checker policy.....8
 - Pulse Access Control Service.....49
 - Pulse Secure Access Service.....101
 - port 3578
 - and application acceleration.....32, 90
 - post-authentication sign-in notifications,
 - configuring.....67
 - pre-authentication sign-in notifications,
 - configuring.....67
 - preconfigured installer.....20, 144, 150, 154
 - privileges.....144
 - protecting against malware, spyware
 - Pulse Access Control Service.....57
 - Pulse Secure Access Service.....108
 - Proxy Automatic Configuration
 - iOS VPN.....179
 - proxy server settings
 - iOS connection profile.....182
 - Pulse and security certificates.....7
 - Pulse Collaboration Suite,
 - enabling.....90
 - overview.....115
 - Pulse Launcher
 - examples.....158
 - Pulse launcher
 - for Android.....200
 - Pulse Mobile Security Suite.....xii, 217
 - Pulse Secure Access Service, download a Junos
 - Pulse client.....126
 - command line launcher
 - examples.....158
 - push configuration.....59, 110
 - R**
 - Radius server.....25, 88
 - realm
 - Android devices.....193
 - iOS devices.....182
 - SAM.....86
 - Symbian devices.....207
 - Windows Mobile devices.....215
 - Remote Desktop Protocol
 - 802.1X and machine authentication.....38
 - resource profiles.....86
 - roaming.....23, 71

Roaming session.....	23
roles.....	174
Android devices.....	192
iOS devices.....	180
mobile device UI.....	174
Pulse Access Control Service.....	21
Pulse Secure Access Service.....	69
SAM.....	82
Symbian devices.....	205
troubleshooting display problems.....	174
Windows Mobile devices.....	211
rooting detection	
for Android clients.....	194
route monitor.....	168
RSA SecurID	
client software version.....	9
RSA SofToken.....	165
S	
scan list.....	7
802.1X connection, Pulse Access Control	
Service.....	26
802.1X connection, Pulse Secure Access	
Service.....	89
scan lists.....	163
SCCM.....	51, 103, 105
scripts.....	169
Pulse Access Control Service.....	24, 74
Pulse Secure Access Service.....	73, 74
SAM.....	85
Windows Mobile app.....	72, 214
Secure Meeting.....	90, 115
Secure Virtual Workspace.....	16
security	
EES.....	47
security certificates, with Pulse.....	7
Sequence Caching	
client policies.....	129
client status.....	130
server certificate DN	
802.1X connection, Pulse Access Control	
Service.....	26
802.1X connection, Pulse Secure Access	
Service.....	89
session cookie.....	71
session lifetime.....	22
session migration.....	135
and authentication server support.....	138
and IF-MAP.....	140
and session timeout.....	137
configuring.....	140
overview.....	6
task summary.....	139
session scripts.....	169
Pulse Access Control Service.....	24, 74
Pulse Secure Access Service.....	73, 74
SAM.....	85
Windows Mobile app.....	72, 214
session time-outs.....	169
session timeout	
Android.....	193
iOS.....	181
Symbian.....	207
Shavlik	
configuring on Pulse Access Control	
Service.....	55
configuring on Pulse Secure Access	
Service.....	107
Shavlik IMV.....	166, 169
sign-in notifications.....	23
agentless.....	66, 67
Junos Pulse.....	66, 67
localized.....	67
single sign-on.....	39, 76
smart card.....	9, 165
smartcard authentication.....	25, 88
SMS.....	51, 103, 105
SMS (System Management Server).....	54, 105
soft token.....	9, 25, 88
software package.....	61, 113
software requirements.....	10, 15, 16
software upgrades	
and bound clients.....	10
for Junos Pulse clients.....	130
overview.....	10
split tunneling	
iOS VPN.....	178, 179
split tunneling options.....	72
split tunnelling	
comparison of NC and Pulse.....	168
SRX Series gateways	
deployment option.....	21
SSL fallback.....	168
SSL optimization	
client policies.....	129
client status.....	130
supplicant.....	7
support, technical See technical support	

-
- suspend a connection.....27
 - SVW.....16
 - Symbian
 - configuring access.....205
 - System Center Configuration Manager.....51, 103, 105
 - System Center Configuration Manager with Host
 - Checker policy.....54, 105
 - system management server (SMS) with Host
 - Checker policy.....54, 105
- T**
- TCP acceleration
 - client policies.....129
 - client status.....130
 - technical support
 - contacting JTAC.....xii
 - third-party software.....114
 - time-to-live, DNS.....46, 98
 - TKIP.....164
 - token authentication.....9, 25, 88
 - Trend Micro firewall.....126
 - troubleshooting
 - application acceleration.....32, 90
- U**
- UDP port 3578
 - and application acceleration.....32, 90
 - unbound clients
 - overview.....9
 - uninstall the Junos Pulse client.....128
 - upgrade
 - client software.....61, 113, 130
 - user interface
 - Pulse client.....4
 - user roles
 - Pulse Access Control Service.....21
 - server.....69
 - user-after-desktop
 - authentication.....35
 - usernames and passwords
 - to download Junos Pulse client software128
- V**
- version monitoring virus signatures and firewall.....8
 - virus signature version monitoring.....8
 - VPN.....121
- W**
- Web install.....143, 148
 - Web launch.....149
 - Web-mail password
 - Android.....194
 - iOS.....183
 - WEP.....164
 - VPN on Demand
 - Android VPN.....191
 - bookmarks.....179, 191, 207, 212
 - iOS devices.....179
 - iOS VPN.....178, 179
 - Symbian VPN.....207
 - Windows Mobile app.....212
 - Windows Mobile.....209
 - configuring access.....85, 214
 - wireless supplicant.....7, 16
 - wireless suppression
 - Pulse Access Control Service.....26, 164
 - Pulse Secure Access Service.....88
 - WPA/WPA2.....164
 - WSAM destinations.....86
 - App Acceleration connection option
 - community string.....90

