Junos Pulse

Administration Guide

Release

2.0

Published: 2011-01-26

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

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

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

The information in this document is current as of the date listed in the revision history.

END USER LICENSE AGREEMENT

READ THIS END USER LICENSE AGREEMENT ("AGREEMENT") BEFORE DOWNLOADING, INSTALLING, OR USING THE SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE OR OTHERWISE EXPRESSING YOUR AGREEMENT TO THE TERMS CONTAINED HEREIN, YOU (AS CUSTOMER OR IF YOU ARE NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) CONSENT TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT OR CANNOT AGREE TO THE TERMS CONTAINED HEREIN, THEN (A) DO NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND (B) YOU MAY CONTACT JUNIPER NETWORKS REGARDING LICENSE TERMS.

1. **The Parties.** The parties to this Agreement are (i) Juniper Networks, Inc. (if the Customer's principal office is located in the Americas) or Juniper Networks (Cayman) Limited (if the Customer's principal office is located outside the Americas) (such applicable entity being referred to herein as "Juniper"), and (ii) the person or organization that originally purchased from Juniper or an authorized Juniper reseller the applicable license(s) for use of the Software ("Customer") (collectively, the "Parties").

2. **The Software.** In this Agreement, "Software" means the program modules and features of the Juniper or Juniper-supplied software, for which Customer has paid the applicable license or support fees to Juniper or an authorized Juniper reseller, or which was embedded by Juniper in equipment which Customer purchased from Juniper or an authorized Juniper reseller. "Software" also includes updates, upgrades and new releases of such software. "Embedded Software" means Software which Juniper has embedded in or loaded onto the Juniper equipment and any updates, upgrades, additions or replacements which are subsequently embedded in or loaded onto the equipment.

3. **License Grant.** Subject to payment of the applicable fees and the limitations and restrictions set forth herein, Juniper grants to Customer a non-exclusive and non-transferable license, without right to sublicense, to use the Software, in executable form only, subject to the following use restrictions:

a. Customer shall use Embedded Software solely as embedded in, and for execution on, Juniper equipment originally purchased by Customer from Juniper or an authorized Juniper reseller.

b. Customer shall use the Software on a single hardware chassis having a single processing unit, or as many chassis or processing units for which Customer has paid the applicable license fees; provided, however, with respect to the Steel-Belted Radius or Odyssey Access Client software only, Customer shall use such Software on a single computer containing a single physical random access memory space and containing any number of processors. Use of the Steel-Belted Radius or IMS AAA software on multiple computers or virtual machines (e.g., Solaris zones) requires multiple licenses, regardless of whether such computers or virtualizations are physically contained on a single chassis.

c. Product purchase documents, paper or electronic user documentation, and/or the particular licenses purchased by Customer may specify limits to Customer's use of the Software. Such limits may restrict use to a maximum number of seats, registered endpoints, concurrent users, sessions, calls, connections, subscribers, clusters, nodes, realms, devices, links, ports or transactions, or require the purchase of separate licenses to use particular features, functionalities, services, applications, operations, or capabilities, or provide throughput, performance, configuration, bandwidth, interface, processing, temporal, or geographical limits. In addition, such limits may restrict the use of the Software to managing certain kinds of networks or require the Software to be used only in conjunction with other specific Software. Customer's use of the Software shall be subject to all such limitations and purchase of all applicable licenses.

d. For any trial copy of the Software, Customer's right to use the Software expires 30 days after download, installation or use of the Software. Customer may operate the Software after the 30-day trial period only if Customer pays for a license to do so. Customer may not extend or create an additional trial period by re-installing the Software after the 30-day trial period.

e. The Global Enterprise Edition of the Steel-Belted Radius software may be used by Customer only to manage access to Customer's enterprise network. Specifically, service provider customers are expressly prohibited from using the Global Enterprise Edition of the Steel-Belted Radius software to support any commercial network access services.

The foregoing license is not transferable or assignable by Customer. No license is granted herein to any user who did not originally purchase the applicable license(s) for the Software from Juniper or an authorized Juniper reseller.

4. **Use Prohibitions.** Notwithstanding the foregoing, the license provided herein does not permit the Customer to, and Customer agrees not to and shall not: (a) modify, unbundle, reverse engineer, or create derivative works based on the Software; (b) make unauthorized copies of the Software (except as necessary for backup purposes); (c) rent, sell, transfer, or grant any rights in and to any copy of the Software, in any form, to any third party; (d) remove any proprietary notices, labels, or marks on or in any copy of the Software or any product in which the Software is embedded; (e) distribute any copy of the Software to any third party, including as may be embedded in Juniper equipment sold in the secondhand market; (f) use any 'locked' or key-restricted feature, function, service, application, operation, or capability without first purchasing the applicable license(s) and obtaining a valid key from Juniper, even if such feature, function, service, application, operation, or capability is enabled without a key; (g) distribute any key for the Software provided by Juniper to any third party; (h) use the

Software in any manner that extends or is broader than the uses purchased by Customer from Juniper or an authorized Juniper reseller; (i) use Embedded Software on non-Juniper equipment; (j) use Embedded Software (or make it available for use) on Juniper equipment that the Customer did not originally purchase from Juniper or an authorized Juniper reseller; (k) disclose the results of testing or benchmarking of the Software to any third party without the prior written consent of Juniper; or (l) use the Software in any manner other than as expressly provided herein.

5. **Audit.** Customer shall maintain accurate records as necessary to verify compliance with this Agreement. Upon request by Juniper, Customer shall furnish such records to Juniper and certify its compliance with this Agreement.

6. **Confidentiality.** The Parties agree that aspects of the Software and associated documentation are the confidential property of Juniper. As such, Customer shall exercise all reasonable commercial efforts to maintain the Software and associated documentation in confidence, which at a minimum includes restricting access to the Software to Customer employees and contractors having a need to use the Software for Customer's internal business purposes.

7. **Ownership.** Juniper and Juniper's licensors, respectively, retain ownership of all right, title, and interest (including copyright) in and to the Software, associated documentation, and all copies of the Software. Nothing in this Agreement constitutes a transfer or conveyance of any right, title, or interest in the Software or associated documentation, or a sale of the Software, associated documentation, or copies of the Software.

8. **Warranty, Limitation of Liability, Disclaimer of Warranty.** The warranty applicable to the Software shall be as set forth in the warranty statement that accompanies the Software (the "Warranty Statement"). Nothing in this Agreement shall give rise to any obligation to support the Software. Support services may be purchased separately. Any such support shall be governed by a separate, written support services agreement. TO THE MAXIMUM EXTENT PERMITTED BY LAW, JUNIPER SHALL NOT BE LIABLE FOR ANY LOST PROFITS, LOSS OF DATA, OR COSTS OR PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, OR FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THIS AGREEMENT, THE SOFTWARE, OR ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. IN NO EVENT SHALL JUNIPER BE LIABLE FOR DAMAGES ARISING FROM UNAUTHORIZED OR IMPROPER USE OF ANY JUNIPER OR JUNIPER-SUPPLIED SOFTWARE. EXCEPT AS EXPRESSLY PROVIDED IN THE WARRANTY STATEMENT TO THE EXTENT PERMITTED BY LAW, JUNIPER DISCLAIMS ANY AND ALL WARRANTIES IN AND TO THE SOFTWARE (WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE), INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT. IN NO EVENT DOES JUNIPER WARRANT THAT THE SOFTWARE, OR ANY EQUIPMENT OR NETWORK RUNNING THE SOFTWARE, WILL OPERATE WITHOUT ERROR OR INTERRUPTION, OR WILL BE FREE OF VULNERABILITY TO INTRUSION OR ATTACK. In no event shall Juniper's or its suppliers' or licensors' liability to Customer, whether in contract, tort (including negligence), breach of warranty, or otherwise, exceed the price paid by Customer for the Software that gave rise to the claim, or if the Software is embedded in another Juniper product, the price paid by Customer for such other product. Customer acknowledges and agrees that Juniper has set its prices and entered into this Agreement in reliance upon the disclaimers of warranty and the limitations of liability set forth herein, that the same reflect an allocation of risk between the Parties (including the risk that a contract remedy may fail of its essential purpose and cause consequential loss), and that the same form an essential basis of the bargain between the Parties.

9. **Termination.** Any breach of this Agreement or failure by Customer to pay any applicable fees due shall result in automatic termination of the license granted herein. Upon such termination, Customer shall destroy or return to Juniper all copies of the Software and related documentation in Customer's possession or control.

10. **Taxes.** All license fees payable under this agreement are exclusive of tax. Customer shall be responsible for paying Taxes arising from the purchase of the license, or importation or use of the Software. If applicable, valid exemption documentation for each taxing jurisdiction shall be provided to Juniper prior to invoicing, and Customer shall promptly notify Juniper if their exemption is revoked or modified. All payments made by Customer shall be net of any applicable withholding tax. Customer will provide reasonable assistance to Juniper in connection with such withholding taxes by promptly: providing Juniper with valid tax receipts and other required documentation showing Customer's payment of any withholding taxes; completing appropriate applications that would reduce the amount of withholding tax to be paid; and notifying and assisting Juniper in any audit or tax proceeding related to transactions hereunder. Customer shall comply with all applicable tax laws and regulations, and Customer will promptly pay or reimburse Juniper for all costs and damages related to any liability incurred by Juniper as a result of Customer's non-compliance or delay with its responsibilities herein. Customer's obligations under this Section shall survive termination or expiration of this Agreement.

11. **Export.** Customer agrees to comply with all applicable export laws and restrictions and regulations of any United States and any applicable foreign agency or authority, and not to export or re-export the Software or any direct product thereof in violation of any such restrictions, laws or regulations, or without all necessary approvals. Customer shall be liable for any such violations. The version of the Software supplied to Customer may contain encryption or other capabilities restricting Customer's ability to export the Software without an export license.

12. **Commercial Computer Software.** The Software is “commercial computer software” and is provided with restricted rights. Use, duplication, or disclosure by the United States government is subject to restrictions set forth in this Agreement and as provided in DFARS 227.7201 through 227.7202-4, FAR 12.212, FAR 27.405(b)(2), FAR 52.227-19, or FAR 52.227-14(ALT III) as applicable.

13. **Interface Information.** To the extent required by applicable law, and at Customer's written request, Juniper shall provide Customer with the interface information needed to achieve interoperability between the Software and another independently created program, on payment of applicable fee, if any. Customer shall observe strict obligations of confidentiality with respect to such information and shall use such information in compliance with any applicable terms and conditions upon which Juniper makes such information available.

14. **Third Party Software.** Any licensor of Juniper whose software is embedded in the Software and any supplier of Juniper whose products or technology are embedded in (or services are accessed by) the Software shall be a third party beneficiary with respect to this Agreement, and such licensor or vendor shall have the right to enforce this Agreement in its own name as if it were Juniper. In addition, certain third party software may be provided with the Software and is subject to the accompanying license(s), if any, of its respective owner(s). To the extent portions of the Software are distributed under and subject to open source licenses obligating Juniper to make the source code for such portions publicly available (such as the GNU General Public License (“GPL”) or the GNU Library General Public License (“LGPL”)), Juniper will make such source code portions (including Juniper modifications, as appropriate) available upon request for a period of up to three years from the date of distribution. Such request can be made in writing to Juniper Networks, Inc., 1194 N. Mathilda Ave., Sunnyvale, CA 94089, ATTN: General Counsel. You may obtain a copy of the GPL at http://www.gnu.org/licenses/gpl.html, and a copy of the LGPL at http://www.gnu.org/licenses/lgpl.html .

15. **Miscellaneous.** This Agreement shall be governed by the laws of the State of California without reference to its conflicts of laws principles. The provisions of the U.N. Convention for the International Sale of Goods shall not apply to this Agreement. For any disputes arising under this Agreement, the Parties hereby consent to the personal and exclusive jurisdiction of, and venue in, the state and federal courts within Santa Clara County, California. This Agreement constitutes the entire and sole agreement between Juniper and the Customer with respect to the Software, and supersedes all prior and contemporaneous agreements relating to the Software, whether oral or written (including any inconsistent terms contained in a purchase order), except that the terms of a separate written agreement executed by an authorized Juniper representative and Customer shall govern to the extent such terms are inconsistent or conflict with terms contained herein. No modification to this Agreement nor any waiver of any rights hereunder shall be effective unless expressly assented to in writing by the party to be charged. If any portion of this Agreement is held invalid, the Parties agree that such invalidity shall not affect the validity of the remainder of this Agreement. This Agreement and associated documentation has been written in the English language, and the Parties agree that the English version will govern. (For Canada: Les parties aux présentés confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattaché, soient redigés en langue anglaise. (Translation: The parties confirm that this Agreement and all related documentation is and will be in the English language)).

Table of Contents

About This Guide xiii

Objectives xiii
Audience xiii
Document Conventions xiii
Related Documentation xiv
Obtaining Documentation xiv
Documentation Feedback xiv
Requesting Technical Support xv
    Self-Help Online Tools and Resources xv
    Opening a Case with JTAC xv

Part 1 Junos Pulse

Chapter 1 Junos Pulse Overview 3

Introducing Junos Pulse 3
    Location Awareness 5
    Session Migration 5
    Centralized Control 6
    Security Certificates 6
    Compliance and Remediation 7
    Two-factor Authentication 7
    Bound and Unbound Clients 7
    SA Series and IC Series Gateway Deployment Options 8
    WXC Series Gateway Deployment Options 9
    SRX Series Gateway Deployment Options 9
    Automatic Software Updates 10
Supported Network Gateways 10
Junos Pulse Client Installation Requirements 11
Accessing Junos Pulse Client Error Messages 11
Migrating From Odyssey Access Client to Junos Pulse 13
    Wireless Connectivity, OAC, and Junos Pulse 14
Migrating From Network Connect to Junos Pulse 14

Chapter 2 Configuring Junos Pulse on IC Series Gateways 15

Before You Begin 15
Junos Pulse and IC Series Gateways Overview 16
Configuring a Role for Junos Pulse 16
Client Connection Set Options 19
Creating a Client Connection Set 23
Configuring Location Awareness Rules 24
Junos Pulse Component Set Options 27

Creating a Client Component Set 28
Endpoint Security Monitoring and Management 29
Remediation Options 31
Issuing a Remediation Message 34
Using SMS/SCCM Remediation 35
Using Shavlik Remediation 36
Enabling Enhanced Endpoint Security 38
Pushing Junos Pulse Configurations Between Gateways of the Same Type 40
Enabling or Disabling Automatic Pulse Upgrades 41
Upgrading Junos Pulse Software 42

Chapter 3 Configuring Junos Pulse on SA Series Appliances 45

Before You Begin 45
Junos Pulse and SA Series Appliances Overview 45
Junos Pulse and IVS 46
Configuring a Role for Junos Pulse 47
Configuring Role Options for Junos Pulse 47
Client Connection Set Options 49
Creating a Client Connection Set 53
Configuring Location Awareness Rules 55
Junos Pulse Component Set Options 58
Creating a Client Component Set 58
Endpoint Security Monitoring and Management 60
Remediation Options 61
Issuing a Remediation Message 64
Using SMS/SCCM Remediation 64
Using Shavlik Remediation 66
Enabling Enhanced Endpoint Security 67
Pushing Junos Pulse Configurations Between Gateways of the Same Type 69
Enabling or Disabling Automatic Pulse Upgrades 71
Upgrading Junos Pulse Software 71

Chapter 4 Configuring Junos Pulse on SRX Series Gateways 73

Junos Pulse and SRX Series Gateways 73
Dynamic VPN Configuration Overview 74

Chapter 5 Configuring Junos Pulse on WXC Series Gateways 77

Installing the Junos Pulse Client 77
Downloading the Junos Pulse Client from a WXC Series Gateway 77
Downloading the Junos Pulse Client from an SA Series Appliance 78
Uninstalling the Junos Pulse Client 79
Managing Software, Configurations, and Policies 79
Enabling Pulse Client Downloads from WXC Series Gateways 79
Enabling Pulse Client Adjacencies on WXC Series Gateways 80
Configuring Pulse Client Policies on WXC Series Gateways 80
Viewing the Status of Pulse Clients on WXC Series Gateways 80
Defining the Pulse Client Configuration on WXC Series Gateways 81
Viewing the Pulse Client Configuration on WXC Series Gateways 82

Uploading Pulse Client Software to WXC Series Gateways . . . 82
Distributing the Pulse Client from WXC Series Gateways . . . 82
Distributing the Pulse Client Through an SA Series Appliance . . . 83
Distributing the Pulse Client Through SMS/SCCM . . . 83
Chapter 6 Session Migration . . . 85
Session Migration Overview . . . 85
Session Migration and Session Timeout . . . 87
How Session Migration Works . . . 88
Session Migration and Session Lifetime . . . 88
Authentication Server Support . . . 88
Task Summary: Configuring Session Migration . . . 89
Configuring Session Migration for the Pulse Client . . . 90
Configuring an IF-MAP Federated Network for Session Migration . . . 90
Chapter 7 Deploying Junos Pulse Client Software . . . 93
Junos Pulse Client Installation Overview . . . 93
Installing the Junos Pulse Client from the Web . . . 94
Installing the Junos Pulse Client Using a Preconfiguration File . . . 95
Installing the Pulse Client Using Advanced Command Line Options . . . 96
Examples . . . 97
Part 2 Junos Pulse Compatibility
Chapter 8 Client Software Feature Comparison . . . 101
Feature Comparison: Odyssey Access Client and Junos Pulse . . . 101
Feature Comparison: Network Connect and Junos Pulse . . . 105
Pulse Split Tunneling . . . 107
Feature Comparison: WX Client and Junos Pulse . . . 107
Part 3 Junos Pulse for Mobile Devices
Chapter 9 Junos Pulse for Mobile Devices and Junos Pulse Mobile Security Suite . . . 111
Overview . . . 111
Junos Pulse Mobile Security Gateway . . . 112
Chapter 10 Junos Pulse for Apple iOS Devices . . . 113
Junos Pulse for Apple iOS Overview . . . 113
Before You Begin . . . 114
Configuring a Role and Realm for Pulse for Apple iOS . . . 114
Installing the Junos Pulse VPN App . . . 116
Using Configuration Profiles . . . 117
Collecting Log Files . . . 117
Chapter 11 Junos Pulse for Google Android Devices . . . 119
Junos Pulse for Android Overview . . . 119
Configuring a Role and Realm for Pulse for Android . . . 119
Chapter 12 Junos Pulse for Nokia Symbian Devices . . . 123
Junos Pulse for Symbian . . . 123
Configuring an SA Series Appliance for Junos Pulse on Symbian Devices . . 123

Chapter 13 **Junos Pulse for Windows Mobile Devices 127**

Junos Pulse for Windows Mobile 127
Pulse R1.0 and Pulse R2.0 for Mobile Devices Compatibility 127
Configuring an SA Series Appliance for Junos Pulse for Windows Mobile Endpoints 128
Defining Applications on the Windows Mobile Device 129

Chapter 14 **Junos Pulse Mobile Security Suite 131**

Junos Pulse Mobile Security Overview 131
Pulse Mobile Security Suite Features 132
Pulse Mobile Security Configuration Overview 133
Requiring Pulse Mobile Security for SA Series Appliance Access 133

Part 4 Index

Index 137

List of Tables

About This Guide xiii

Table 1: Notice Icons xiii
Table 2: Junos Pulse Documentation xiv

Part 1 Junos Pulse

Chapter 1 Junos Pulse Overview 3

Table 3: Junos Pulse Client Hardware and Software Requirements 11

Chapter 2 Configuring Junos Pulse on IC Series Gateways 15

Table 4: Configurable Options for Junos Pulse Connection Sets 20

Chapter 3 Configuring Junos Pulse on SA Series Appliances 45

Table 5: Configurable Parameters for Junos Pulse Connection Sets 50

Part 2 Junos Pulse Compatibility

Chapter 8 Client Software Feature Comparison 101

Table 6: Odyssey Access Client and Junos Pulse Feature Comparison 101
Table 7: Network Connect and Junos Pulse Feature Comparison 105
Table 8: Pulse Split Tunneling 107
Table 9: WX Client and Junos Pulse Feature Comparison 108

Part 3 Junos Pulse for Mobile Devices

Chapter 14 Junos Pulse Mobile Security Suite 131

Table 10: Pulse Mobile Security Suite Features 132

About This Guide

- Objectives on page xiii
- Audience on page xiii
- Document Conventions on page xiii
- Related Documentation on page xiv
- Obtaining Documentation on page xiv
- Documentation Feedback on page xiv
- Requesting Technical Support on page xv

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 through Juniper Networks gateways.

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 through Juniper Networks gateways. This guide describes the procedures for configuring Junos Pulse as the access client. Before using the procedures in the *Junos Pulse Administration Guide* be sure you already have configured the access gateway and that you are familiar with how to administer the gateways. This guide refers to the access gateway administration guides.

Document Conventions

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

Table 1: Notice Icons

Icon	Meaning	Description
ℹ	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 xiv describes related Junos Pulse documentation.

Table 2: Junos Pulse Documentation

Title	Description
Junos Pulse Mobile Security Administration Guide	Describes the Pulse Mobile Security Suite and includes procedures for network administrators who are responsible for setting up and managing security on mobile devices.
Junos Pulse Secure Access Service Administration Guide	Describes how to configure and maintain a Juniper Networks SA Series Appliance.
Junos Pulse Access Control Service Administration Guide	Describes how to configure and maintain the Unified Access Control solution and the IC Series 4500 and 6500 devices.
Application Acceleration Administration Guide	Describes how to use the JWOS Web interface to configure, monitor, and manage the Juniper Networks WXC Application Acceleration gateways and their remote Junos Pulse clients.
Junos Security Configuration Guide	Describes how to use and configure security features on SRX Series Services 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

This part introduces Junos Pulse, describes Junos Pulse features, and presents configuration concepts.

- Junos Pulse Overview on page 3
- Configuring Junos Pulse on IC Series Gateways on page 15
- Configuring Junos Pulse on SA Series Appliances on page 45
- Configuring Junos Pulse on SRX Series Gateways on page 73
- Configuring Junos Pulse on WXC Series Gateways on page 77
- Session Migration on page 85
- Deploying Junos Pulse Client Software on page 93

CHAPTER 1

Junos Pulse Overview

- Introducing Junos Pulse on page 3
- Supported Network Gateways on page 10
- Junos Pulse Client Installation Requirements on page 11
- Accessing Junos Pulse Client Error Messages on page 11
- Migrating From Odyssey Access Client to Junos Pulse on page 13
- Migrating From Network Connect to Junos Pulse on page 14

Introducing Junos Pulse

Junos Pulse is an extensible multi service network client that supports integrated connectivity, location-aware network access, acceleration, and security. 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.

NOTE: For information about Pulse on mobile devices, see "Junos Pulse for Mobile Devices" on page 109.

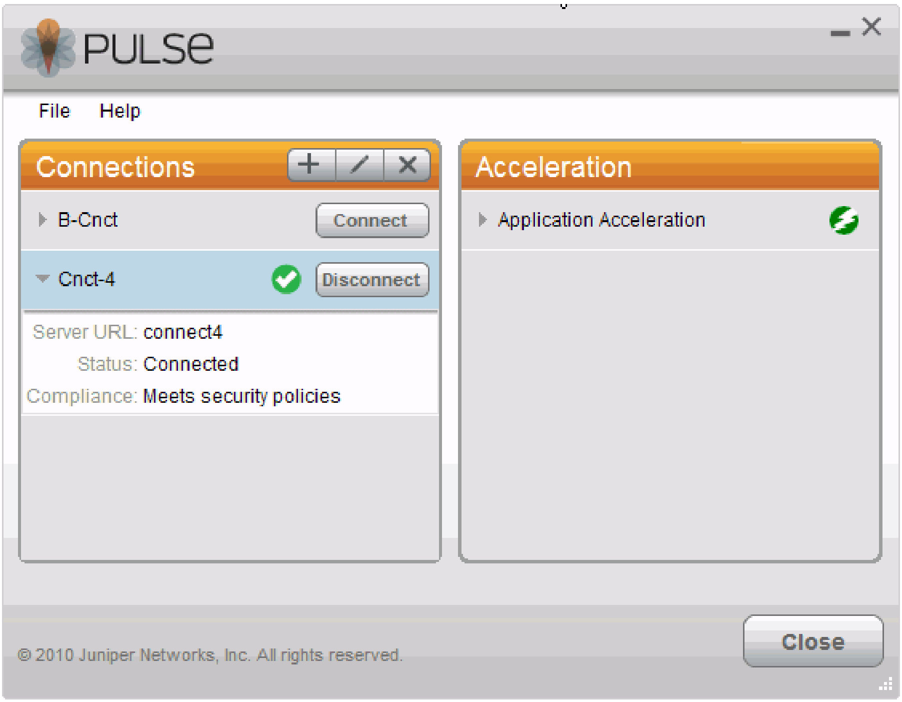
Junos Pulse comprises client and server software. The client enables secure authenticated network connections to protected resources and services over local and wide area networks. The server is integrated into the administrator interface of supported Juniper Networks gateways.

Pulse delivers remote access and connectivity to enterprise and service provider networks in conjunction with Juniper Networks SA Series SSL VPN Appliances. Pulse can provide application acceleration features when implemented with Juniper Networks Application Acceleration gateways (WXC). Pulse also delivers secure, identity-enabled NAC for LAN-based network and application access when deployed with Juniper Networks IC Series UAC Appliances. Pulse integrates third-party endpoint security applications such as anti spyware and anti malware applications.

The Junos Pulse client interface for the Pulse Windows client (see Figure 1 on page 4) includes three panels. The Connections panel lists the Pulse connections. Each connection is a set of properties that enables network access through a specific access gateway.

The Connections panel appears in every Pulse installation. The Security panel is visible only when optional security options are deployed, such as the Juniper Networks Enhanced Endpoint Security (EES) application. If an access gateway is licensed to provide EES, you can enable EES and deploy it as part of the Host Checker configuration. A user can expand items in the Connections and Security panels to see more information. The Acceleration panel appears only when the Pulse client has an adjacency with an Application Acceleration (WXC) gateway.

Figure 1: Junos Pulse Client Interface



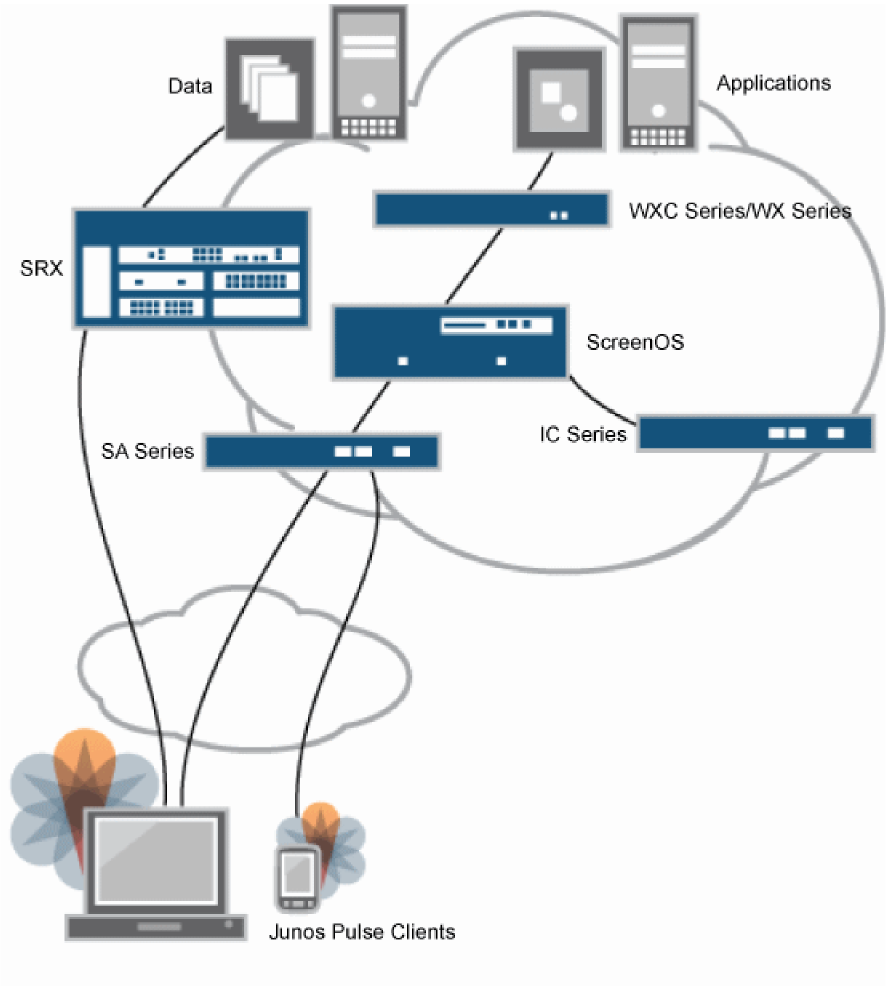
Server URL: connect4
Status: Connected
Compliance: Meets security policies

© 2010 Juniper Networks, Inc. All rights reserved.

Junos Pulse combines the features of Odyssey Access Client for LAN access, Network Connect or the SRX client software for WAN access, and WX client software for application acceleration services. Users of mobile devices (smartphones) can install the Pulse mobile device app from the respective app stores for secure connectivity to an SA Series Appliance. Mobile device users can also enable an optional security component.

Figure 2 on page 5 shows how the Junos Pulse client software provides access and application acceleration in a network that includes different gateways.

Figure 2: Junos Pulse in the Network



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 an SA Series Appliance when the user is at home, and to establish a UAC connection when the user is 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 gateway on the network, and then securely access additional gateways without needing reauthentication. For example, a user can connect from home through an SA Series Appliance, and then arrive at work and connect through an IC Series appliance without having to log in again. Session migration also enables users to access different resources within the network that are protected by Juniper

Networks gateways 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 one IC Series or SA Series Appliance to configure all of the connections that clients need, and then push those configurations (IC to IC or SA to SA) 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.

You can define Junos Pulse connections on the server. A connection includes all of the information that a Pulse client needs to connect to a specific access gateway. 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 create 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 gateway's Web portal. It is also installed as part of a Web install of Junos Pulse. Each supported access gateway includes one default connection set, and that default connection set includes a dynamic connection.
- 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 access device, 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 on endpoints. You configure rules in Host Checker policies on IC Series and SA Series gateways to specify the minimum criteria for the security compliance of endpoints that are allowed to enter the network. 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 IC Series and SA Series gateways.

- 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.

  IC Series and SA Series gateways 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.

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 higher) must already be installed on the client machine.

Bound and Unbound Clients

Another feature of Pulse configuration management is the ability to bind Pulse clients to a single gateway or to a specified set of gateways. Binding Junos Pulse clients ensures that the client does not receive different configurations when accessing other gateways.

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

- **Bound client**—A bound client is managed by a gateway or group of gateways. The gateway administrator defines the Junos Pulse connections and software components that are installed on the endpoint. When the client connects to the access gateway that is managing it, the access gateway automatically provisions configuration and software component updates. The gateway administrator can permit the user to add and remove connections and to modify connections received from the gateway. The gateway administrator can also allow dynamic connections, (connections added by gateways when the user logs into the gateway by way of a browser). A dynamic connection enables a bound client to add connections from gateways other than the one the client is bound to.

  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 software is installed without any connections. The user must add connections manually. Dynamic connections can be added by visiting the Web portals of supported gateways. An unbound client does not accept configuration updates from an access gateway even if client configurations are defined on that access gateway.

SA Series and IC Series Gateway Deployment Options

On the network side, the Junos Pulse configuration is integrated into the admin console of supported gateways. On SA Series and IC Series appliances, you can deploy all of the connections and components required for clients to connect to any supported gateway. SA Series and IC Series appliances support the following deployment options:

- **Web install**—Create all of the settings that an endpoint needs for connectivity and services, and install the software on endpoints that connect to the access gateway Web portal and successfully log in to the gateway. The IC Series and SA Series Appliances 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, install only the components required for the connection, and permit an automatic connection to the IC Series appliance or SA Series Appliance to which the endpoint connects.
- **Default installer**—A default Junos Pulse installer package (in both .msi and .exe formats) is included in the access gateway software. You can distribute this default installer to endpoints, install it, and then let users create their own connections. Or, after installing the default Junos Pulse package, users can automatically install dynamic connections by browsing to the user Web portal of an access gateway 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 a specific server. If the user is able to log in to the access gateway's user Web portal, the connection parameters are downloaded and installed on the Junos Pulse client.
- **Preconfigured installer**—Create the connections that an endpoint needs for connectivity and services, download the settings file (.jnprpreconfig), download default Pulse .msi

installation program, and then run the .msi installation program by using an msiexec command with the settings file as an option. You can use the msiexec command to deploy Pulse using a standard software distribution process, such as SMS/SCCM.

NOTE: Junos Pulse for mobile devices uses a different deployment model than Pulse for Windows endpoints. For information about Pulse on mobile devices, see "Junos Pulse for Mobile Devices" on page 109.

WXC Series Gateway Deployment Options

The Junos Pulse client accelerates traffic between the client system and a remote WXC Series gateway. The WXC Series gateways and Pulse clients discover each other automatically and begin accelerating traffic without user intervention. WXC Series gateways support the following deployment options:

- The WXC administrator can enable Pulse downloads and configure Pulse client configuration, and then users can download the Junos Pulse client from a WXC Series gateway running JWOS 6.1. When the license is present, a Junos Pulse selection appears in the task bar of the Web interface for the WXC Series gateway.
- The Junos Pulse client can be downloaded and installed automatically when users access an SA Series Appliance. On version 7.0 or later SA Series Appliances, you can configure a WX connection and install it along with the Pulse client software. You can also deploy a WX connection from an IC Series appliance to a client. Although an IC Series appliance is for LAN access where WAN application acceleration is not used, IC Series and SA Series Appliances 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. For information about Pulse on mobile devices, see "Junos Pulse for Mobile Devices" on page 109.

SRX Series Gateway Deployment Options

Although the ability to configure and deploy Junos Pulse client software from an SRX Series gateway is not yet available, 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 supported IC or SA Series devices.
- You can download the Junos Pulse installer from a supported gateway 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.

NOTE: Junos Pulse for mobile devices can access SA Series Appliances only. For information about Pulse on mobile devices, see "Junos Pulse for Mobile Devices" on page 109.

Automatic Software Updates

After you deploy Junos Pulse client software to endpoints, software updates occur automatically. If you upgrade the Junos Pulse software on your IC Series or SA Series Appliance, updated software components are pushed to a client the next time it connects. (You can disable this automatic upgrade feature.) SRX Series gateways and WXC Series gateways do not support automatic software upgrades.

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 access gateway, after which those configuration properties reside on the client computer.

Related Documentation

- Session Migration Overview on page 85
- Junos Pulse for Windows Mobile on page 127
- Enabling or Disabling Automatic Pulse Upgrades on page 41

Supported Network Gateways

The following Juniper Networks gateways support Junos Pulse:

- IC Series UAC Gateway Release 4.0 and later
- SA Series SSL VPN Appliance Release 7.0 and later
- WXC Series JWOS Release 6.1 and later
- SRX Series Release 10.2 and later

NOTE: Although the ability to configure and deploy Junos Pulse client software from an SRX Series gateway is not yet available, endpoints can use Junos Pulse client software to connect to SRX Series gateways that are running Junos OS Release 10.2 or later. You can create connections that use the connection type "Firewall" and deploy these connections from supported gateways. You can also download the Junos Pulse installer from a supported gateway or the Juniper Networks Web and install it using local distribution methods.

Related Documentation

- Junos Pulse Client Installation Requirements on page 11

Junos Pulse Client Installation Requirements

Table 3 on page 11 lists the minimum hardware and software requirements to support the Junos Pulse client software for Windows endpoints. For information about Pulse on mobile devices, see "Junos Pulse for Mobile Devices" on page 109. For expanded platform support information, see the *Junos Pulse Supported Platforms Guide*, which is available at http://www.juniper.net/support/products/pulse.

Table 3: Junos Pulse Client Hardware and Software Requirements

Component	Requirement
Operating System and browser	Windows 7 Enterprise 64 bit; Internet Explorer 8.0 (32 bit) and Firefox 3.5 Vista Enterprise SP2 32 bit; Internet Explorer 7.0, Internet Explorer 8.0, and Firefox 3.0. XP Professional SP3 32 bit; Internet Explorer 7.0, Internet Explorer 8.0, and Firefox 3.5.
CPU	500 MHz
Memory	512 MB of RAM
Available disk space	30 MB minimum free space 400 MB for WX connections

NOTE: For increased security, we recommend that you disable the Fast User Switching feature on Windows endpoints. The Fast User Switching feature allows more than one user to log on simultaneously at a single computer. The feature is enabled by default for Windows 7 and Windows Vista and for domain users on Windows XP. With the Fast User Switching feature enabled, all concurrent user sessions on a system can access the current desktop connections to networks and IC Series appliances. Thus, if one user has a current network connection, other users logged in on the same computer can access the same network connections, which creates a security risk.

Related Documentation

- Introducing Junos Pulse on page 3
- Supported Network Gateways on page 10

Accessing Junos Pulse Client Error Messages

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 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
- JA—Japanese
- KO—Korean
- ZH—Chinese (Traditional)
- ZH-CN—Chinese (Simplified)

A Junos Pulse endpoint can have the following message catalog files:

- \Program Files\Common Files\Juniper Networks\8021xAccessMethod\
  MessageCatalog8021xAM_DE.txt
  MessageCatalog8021xAM_EN.txt
  MessageCatalog8021xAM_ES.txt
  MessageCatalog8021xAM_FR.txt
  MessageCatalog8021xAM_JA.txt
  MessageCatalog8021xAM_KO.txt
  MessageCatalog8021xAM_ZH-CN.txt
  MessageCatalog8021xAM_ZH.txt
- \Program Files\Common Files\Juniper Networks\Connection Manager\
  MessageCatalog8021xAM_DE.txt
  MessageCatalogConnMgr_EN.txt
  MessageCatalogConnMgr_ES.txt
  MessageCatalogConnMgr_FR.txt
  MessageCatalogConnMgr_JA.txt
  MessageCatalogConnMgr_KO.txt
  MessageCatalogConnMgr_ZH-CN.txt
  MessageCatalogConnMgr_ZH.txt
- \Program Files\Common Files\Juniper Networks\eapService\
  MessageCatalogEapAM_DE.txt
  MessageCatalogEapAM_EN.txt
  MessageCatalogEapAM_ES.txt
  MessageCatalogEapAM_FR.txt
  MessageCatalogEapAM_JA.txt
  MessageCatalogEapAM_KO.txt
  MessageCatalogEapAM_ZH-CN.txt
  MessageCatalogEapAM_ZH.txt

- \Program Files\Common Files\Juniper Networks\iveConnMethod\
  MessageCatalogIveAM_DE.txt
  MessageCatalogIveAM_EN.txt
  MessageCatalogIveAM_ES.txt
  MessageCatalogIveAM_FR.txt
  MessageCatalogIveAM_JA.txt
  MessageCatalogIveAM_KO.txt
  MessageCatalogIveAM_ZH-CN.txt
  MessageCatalogIveAM_ZH.txt
- \Program Files\Common Files\Juniper Networks\JamUI\
  MessageCatalogPulseUI_DE.txt
  MessageCatalogPulseUI_EN.txt
  MessageCatalogPulseUI_ES.txt
  MessageCatalogPulseUI_FR.txt
  MessageCatalogPulseUI_JA.txt
  MessageCatalogPulseUI_KO.txt
  MessageCatalogPulseUI_ZH-CN.txt
  MessageCatalogPulseUI_ZH.txt
- \Program Files\Common Files\Juniper Networks\JUNS\
  MessageCatalogCommon_DE.txt
  MessageCatalogCommon_EN.txt
  MessageCatalogCommon_ES.txt
  MessageCatalogCommon_FR.txt
  MessageCatalogCommon_JA.txt
  MessageCatalogCommon_KO.txt
  MessageCatalogCommon_ZH-CN.txt
  MessageCatalogCommon_ZH.txt
- \Program Files\Common Files\Juniper Networks\WX Client\
  MessagecatalogWxAM_DE.txt
  MessagecatalogWxAM_EN.txt
  MessagecatalogWxAM_ES.txt
  MessagecatalogWxAM_FR.txt
  MessagecatalogWxAM_JA.txt
  MessagecatalogWxAM_KO.txt
  MessagecatalogWxAM_ZH-CN.txt
  MessagecatalogWxAM_ZH.txt

Related Documentation

- Introducing Junos Pulse on page 3

Migrating From Odyssey Access Client to Junos Pulse

An endpoint can have Junos Pulse and Odyssey Access Client (OAC) Release 5.2 or later installed at the same time. If the endpoint has an earlier 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 Release 5.2 or later, the Pulse installation proceeds. If the OAC is not at least Release 5.2, the Pulse installation displays a message advising the user to uninstall or upgrade OAC.

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 Junos 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

- OAC Features and Junos Pulse on page 101
- Supported Network Gateways on page 10

Migrating From Network Connect to Junos Pulse

Junos Pulse and Network Connect (NC) Release 6.3 or later can run at the same time on an endpoint. For example, you can use NC to establish connections to an SA Series Appliance that does not support Junos Pulse.

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.

On endpoints that connect through an SA Series Appliance, if Junos Pulse is running on the Windows main desktop, you cannot launch Junos Pulse within Secure Virtual Workspace (SVW). SVW is not supported with Pulse.

Related Documentation

- Network Connect Features and Junos Pulse on page 105
- Supported Network Gateways on page 10

CHAPTER 2

Configuring Junos Pulse on IC Series Gateways

- Before You Begin on page 15
- Junos Pulse and IC Series Gateways Overview on page 16
- Configuring a Role for Junos Pulse on page 16
- Client Connection Set Options on page 19
- Creating a Client Connection Set on page 23
- Configuring Location Awareness Rules on page 24
- Junos Pulse Component Set Options on page 27
- Creating a Client Component Set on page 28
- Endpoint Security Monitoring and Management on page 29
- Issuing a Remediation Message on page 34
- Using SMS/SCCM Remediation on page 35
- Using Shavlik Remediation on page 36
- Enabling Enhanced Endpoint Security on page 38
- Pushing Junos Pulse Configurations Between Gateways of the Same Type on page 40
- Enabling or Disabling Automatic Pulse Upgrades on page 41
- Upgrading Junos Pulse Software on page 42

Before You Begin

Before you begin configuring Junos Pulse, be sure you have already configured your IC Series appliance in your network. 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 Pulse installation because you can define the conditions that an endpoint must meet to be allowed access to protected resources. For complete information, see the *Junos Pulse Access Control Service Administration Guide*.

Related Documentation

- Introducing Junos Pulse on page 3

Junos Pulse and IC Series Gateways Overview

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

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

- Use the defaults or make changes to the Junos Pulse default component set and default connection set, and then download and distribute Pulse by having users log in to the gateway's user Web portal. 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), download default Pulse .msi installation program, and then run the .msi installation program by using an msiexec command with the settings file as an option. You can use the msiexec command to deploy Pulse using a standard software distribution process, such as SMS/SCCM.
- Distribute Junos Pulse with no preconfiguration. You can download the default Junos Pulse installation file in either .msi or .exe format from the IC Series appliance, and then distribute the file to endpoints using your organization's standard software distribution methods. Because the installer does not contain preconfigured connections, users must define network connections manually. Or you can create dynamic connections on each access gateway. These connections are automatically downloaded to the installed Pulse client when users provide their login credentials to the gateway's user Web portal.

Related Documentation

- Junos Pulse and SA Series Devices Overview on page 45
- Junos Pulse and SRX Series Gateways on page 73
- Enabling Pulse Client Downloads from WXC Series Gateways on page 79

Configuring a Role for Junos Pulse

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. For complete information about all role configuration options, see the *Junos Pulse Access Control Service Administration Guide*.

To configure a role for Junos 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. This name appears in the list of Roles on the Roles page.
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.
   - **Browser**—Browser options allow you to enforce the use of a particular type of browser for Web access to the IC Series appliance. Browser options apply only to operations that involve accessing the IC Series appliance 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 the IC Series appliance 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 installed the client-side certificate on the IC Series appliance on the Trusted Client CAs page of the admin console.
   - **Host Checker**—Host Checker options allow you to enable Host Checker polices, 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. See the *Junos Pulse Access Control Service Administration Guide* for information about configuring authentication and Host Checker policies.

   General > Session Options

   - **Session lifetime**—Session lifetime options allow you to set timeout values for user session. 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, the IC Series appliance 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 the IC Series appliance 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 the IC Series appliance should wait before terminating a session when the endpoint does not send a heartbeat response.

    - **Enable Session Extension**—This option applies to OAC sessions only. The Junos Pulse client does not prompt a user to extend a session that has exceeded a session interval.

  - **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 the IC Series appliance 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 Web page options that a user sees after a successful login by means of a browser. Be sure that you have already defined the authentication settings for this role. See the *Junos Pulse Access Control Service Administration Guide* for information on sign-in policies, sign-in pages, sign-in notifications, and authentication protocol sets.

5. Select the Agent tab. The “agent” is the client program for a user assigned to this role. Configure the following options.

   - Select **Install Agent for this role**.

   - Select **Install Junos Pulse**.

6. In the **Session scripts** area, optionally specify a location for the following:

   - **Windows: Session start script**—Specify a script to run for users assigned to the role after Pulse connects with the IC Series appliance. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources.

   - **Windows: Session end script**—Specify a script to run for users assigned to the role after Junos Pulse disconnects from the IC Series appliance. 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.

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**, if you are creating this role to distribute new or updated connections to existing Pulse users.
9. 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

- Endpoint Security Monitoring and Management on page 29

Client Connection Set Options

A Pulse client connection set contains network options and allows you to configure specific connection policies for client access to any access gateway that supports Junos Pulse. Table 4 on page 20 describes connection set options.

Table 4: Configurable Options for Junos Pulse Connection Sets

Options	**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.
	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 gateway. See the *Junos Pulse Access Control Service Administration Guide* or the *Junos Pulse Secure Access Service Administration Guide* for complete information about setting up certificate-based authentication.
	Dynamic connections—Allows new connections to be added automatically to a Junos Pulse client when it encounters new supported gateways through the Web browser.
	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: • 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.

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

When you create a connection for a connection set, you choose a connection type. The following options are available for each connection type.	
802.1X options	**Adapter type**—Specifies the type of adapter to use for authentication: wired or wireless.
	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.
	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.
Trusted Server List for 802.1X Connection	**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.
IC or SA options	**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.
	This server—Specifies whether the endpoint connects to this gateway.
	URL—Allows you to specify a URL for a different gateway as the default connection. Specify a different server's URL to create connections for other gateways in your network.
Firewall options (for Dynamic VPN)	**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.
	URL—Specifies the location of the firewall.
WX options	**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.
	Community string—The Junos Pulse client and the Application Acceleration (WXC) gateway can form an adjacency for WAN optimization only if they belong to the same community as identified by the community string. When you create a WX connection, be sure the community string for the connection matches the community string defined on the Application Acceleration (WXC) gateway.

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

If you create an IC or SA or a Firewall connection, you can also specify how the connection is established, including the rules that control the location awareness feature. 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 logs on—When the endpoint is started and the user has logged in to the endpoint, the Junos Pulse client software connects automatically.

NOTE: All connections on an endpoint that are configured to start automatically will attempt to connect to their target networks at startup time. To avoid multiple connections, configure location awareness rules.

According to location awareness rules—Location awareness rules enable an endpoint to connect conditionally. For example, the endpoint connects to an IC Series appliance if it is connected to the company intranet or it connects to an SA Series Appliance 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.

Related Documentation

- Endpoint Security Monitoring and Management on page 29

Creating a Client Connection Set

To create a 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**
   - **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:
   - **802.1X**
   - **IC or SA**
   - **Firewall**
   - **WX**
10. If you select **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.
11. Click **Save Changes**.
12. If you selected **IC or SA** for the type, select or clear the following check boxes:

- **Allow user to override connection policy**
- **Connect automatically**
- **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.

13. If you select **Firewall**, enter an IP address in the Address box.
14. From the Options list, select or clear the following check boxes:
    - **Allow user to override connection policy**
    - **Connect automatically**
    - **URL**—Enter the network address for the firewall.
15. (Optional) You can enable location awareness by creating location awareness rules. Location awareness can force a connection to a particular interface. See "Configuring Location Awareness Rules" on page 24 for more information.
16. If you select **WX**, select the **Connect Automatically** check box to permit the client to automatically form an adjacency to an Application Acceleration (WXC) gateway 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.

17. After you have created the client connection set, create a client component set and select this connection set.

Related Documentation

- Endpoint Security Monitoring and Management on page 29

Configuring Location Awareness Rules

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

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

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

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

The following location awareness example includes two connections. The first connection is an IC Series appliance connection that resolves to TRUE when the endpoint is connected to the corporate LAN. The second connection is an SA Series Appliance connection that resolves to TRUE when the endpoint is located in a remote location.

IC Series appliance 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.
```

SA Series Appliance 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 SA Series Appliance resolves to the external facing IP
address of the SA Series Appliance, 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 WX 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 the SA Series Appliance 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

- Session Migration Overview on page 85

Junos Pulse Component Set Options

A 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.

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 gateways 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 an IC or SA device. 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. The preconfigured installer always installs all components unless you specify the specific components you want using command line options.

Related Documentation

- Junos Pulse Client Installation Overview on page 93
- Installing the Junos Pulse Client Using a Preconfiguration File on page 95
- Creating a Client Component Set on page 28

Creating a Client Component Set

Client component options affect Web-based installations only. For a preconfigured installer, specify components as part of the MSIEXEC command. 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 an IC or SA Series Appliance.
4. Specify a name for the client component set.
5. (Optional) Enter a description for this client component set.
6. Select a connection set that you have created, or use the default connection set.
7. For Junos Pulse client components, select one of the following option buttons:
   - **All components**—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 an IC or SA device. 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. The preconfigured installer always installs all components unless you specify the specific components you want using command line options.

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 93
- Installing the Junos Pulse Client Using a Preconfiguration File on page 95
- Endpoint Security Monitoring and Management on page 29

Endpoint Security Monitoring and Management

On Windows systems, 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.

The IC Series device 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 the IC Series device and verify a particular aspect of a host's integrity. Each IMV on the IC Series device 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 IC Series device, 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 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 the IC Series device, 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 an IC Series device 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.

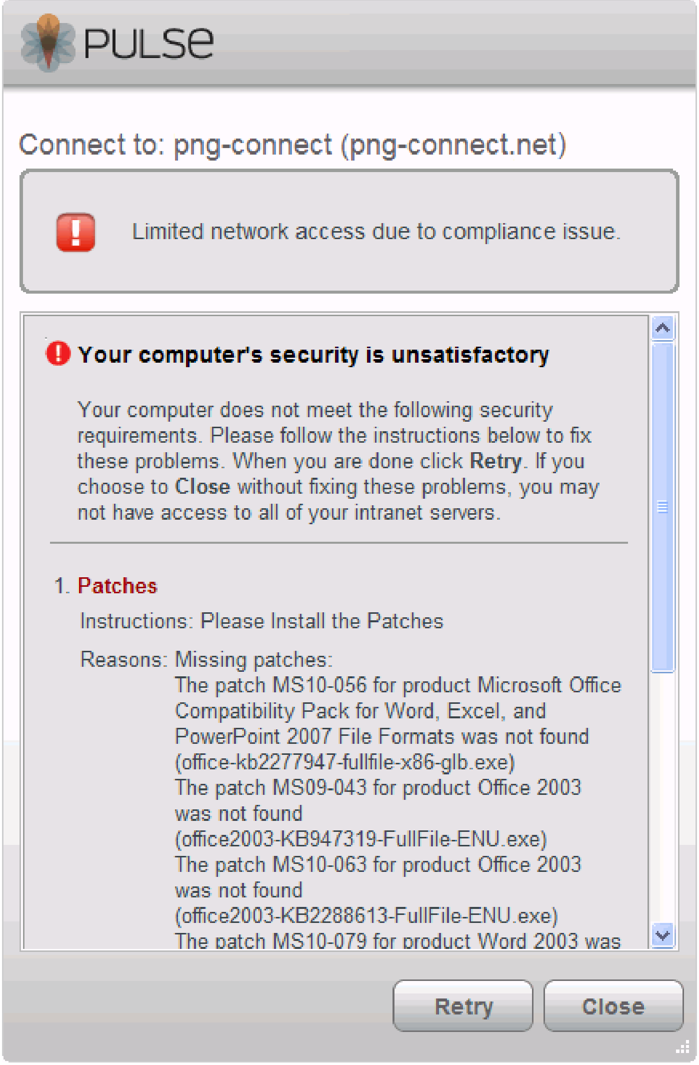
For complete information on configuring Host Checker policies, see the *Junos Pulse Access Control Service Administration Guide*.

Remediation Options

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

- **Instructions to the user**—The IC Series device 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 3 on page 31 shows a typical Pulse remediation message.

Figure 3: Pulse Remediation Instructions



Connect to: png-connect (png-connect.net)

Limited network access due to compliance issue.

Your computer's security is unsatisfactory

Your computer does not meet the following security requirements. Please follow the instructions below to fix these problems. When you are done click **Retry**. If you choose to **Close** without fixing these problems, you may not have access to all of your intranet servers.

1. Patches

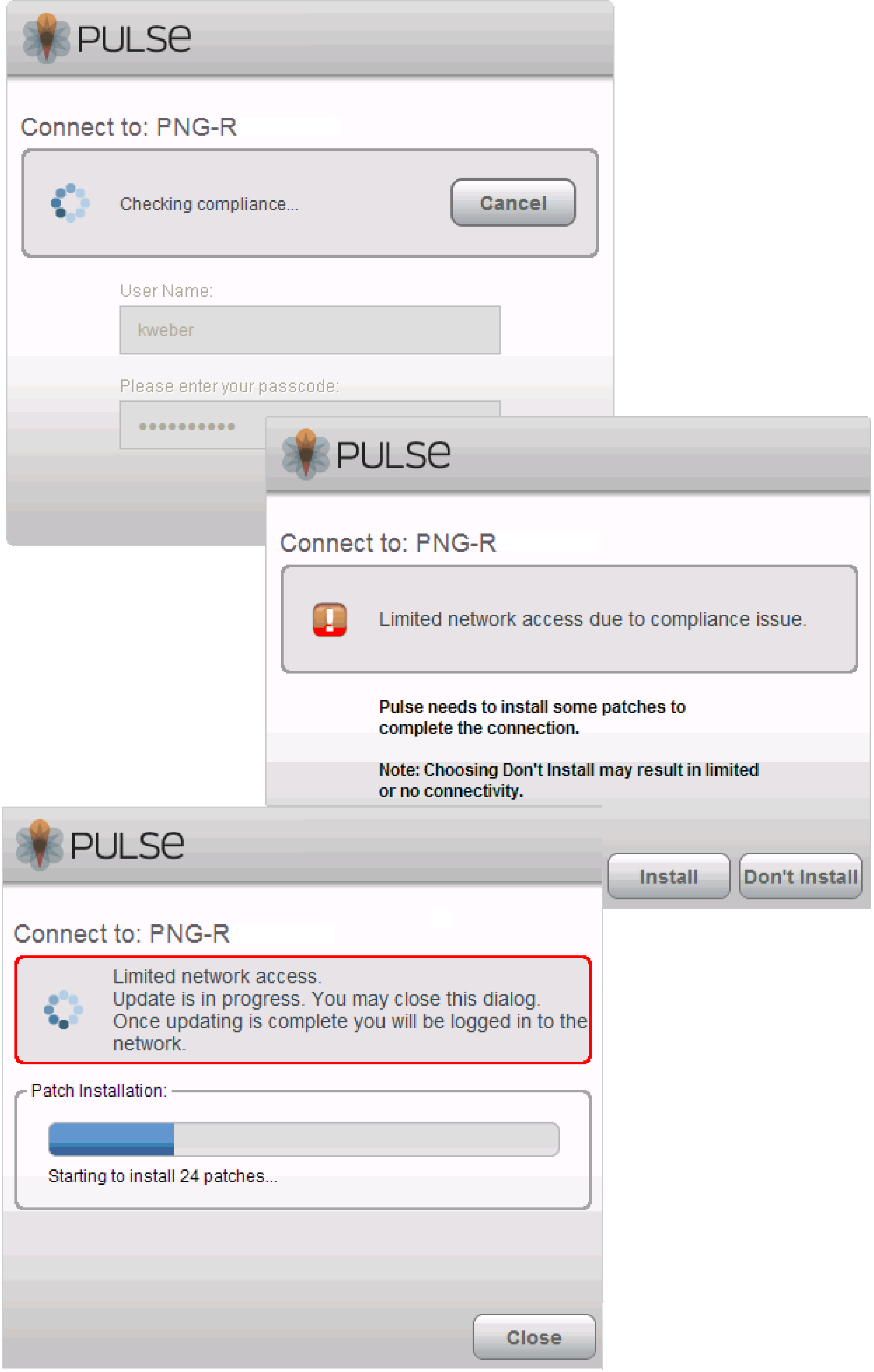
Instructions: Please Install the Patches

Reasons: Missing patches:
The patch MS10-056 for product Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats was not found (office-kb2277947-fullfile-x86-glb.exe)
The patch MS09-043 for product Office 2003 was not found (office2003-KB947319-FullFile-ENU.exe)
The patch MS10-063 for product Office 2003 was not found (office2003-KB2288613-FullFile-ENU.exe)
The patch MS10-079 for product Word 2003 was

- **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**—IC Series software R4.1 and higher 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 4 on page 33

Figure 4: Pulse Client Screens for Shavlik Patch Remediation



Connect to: PNG-R

Checking compliance...

User Name:

kweber

Please enter your passcode:

••••••••••

Connect to: PNG-R

Limited network access due to compliance issue.

Pulse needs to install some patches to complete the connection.

Note: Choosing Don't Install may result in limited or no connectivity.

Connect to: PNG-R

Limited network access.
Update is in progress. You may close this dialog.
Once updating is complete you will be logged in to the network.

Patch Installation:

Starting to install 24 patches...

Related Documentation

- Issuing a Remediation Message on page 34
- Using SMS/SCCM Remediation on page 35
- Using Shavlik Remediation on page 36

Issuing a Remediation Message

If a Host Checker policy finds that an endpoint is not in compliance, Host Checker can display a message through Pulse 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>, <b>, <br>, <font>, and <a href>. For example:

   You do not have the latest signature files.

   <a href=”www.company.com”>Click here to download the latest signature files.</a>
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 on page 29
- Using SMS/SCCM Remediation on page 35
- Using Shavlik Remediation on page 36

Using SMS/SCCM Remediation

Pulse supports the SMS/SCCM download method for patch deployment. If the IC Series device 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 IC Series device 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 IC Series or SA Series device, 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.

   For detailed information about configuring Host Checker rules, see the *Junos Pulse Access Control Service Administration Guide*.
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 on page 29
- Issuing a Remediation Message on page 34
- Using Shavlik Remediation on page 36

Using Shavlik Remediation

Endpoints with Pulse R2.0 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 on the IC Series device.

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 the IC Series device 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. For information on how to update ESAP files, see the *Junos Pulse Access Control Service Administration Guide*.

The IMC and IMV software for patch monitoring is backward compatible. Since this feature is available from Pulse R2.0 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 more than one IC Series or SA Series device, 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.

   For detailed information about configuring Host Checker rules, see the *Junos Pulse Access Control Service Administration Guide*.
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 on page 29
- Issuing a Remediation Message on page 34

- Using SMS/SCCM Remediation on page 35

Enabling Enhanced Endpoint Security

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 the IC Series device, and that you can restrict or quarantine these endpoints according to your Host Checker policy configuration. When EES is running on an endpoint, the Junos 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 IC Series device. 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 the IC Series device 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 the IC Series device, 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 the IC Series device. 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.

User Experience

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 antispyware:

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 on page 29
- Issuing a Remediation Message on page 34
- Using SMS/SCCM Remediation on page 35
- Using Shavlik Remediation on page 36

Pushing Junos Pulse Configurations Between Gateways of the Same Type

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

This section describes how to use the Push Configuration feature to centrally manage Junos Pulse. For complete details about using Push Configuration to centrally manage all of the settings of an gateway, see the appropriate administration guide.

The following notes apply to pushing configurations:

- You can push to a single gateway or to multiple gateways 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 gateway 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 gateway that is a member of a cluster as long as the target gateway is not a member of the same cluster as the source.
- Target gateways can refuse pushed configuration settings. The default is to accept.
- After an update, the target gateway 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 gateways do not display a warning message when they receive a pushed configuration.
- The target gateway automatically logs out administrators during the push process.
- The source and target gateways must have the same build version and number.
- The administrator account on the source gateway must sign in to the target gateway 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 gateway 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 gateway. 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 access gateway to other gateways of the same type:

1. If you have not already done so, define the targets by selecting **Maintenance > Push Config > Targets**. For detailed procedures on how to define targets, see the appropriate gateway administration guide.
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 gateway. 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 gateway.
6. Add the targets to the **Selected Targets** box.
7. Click **Push Configuration**.

Enabling or Disabling Automatic Pulse Upgrades

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

NOTE: A bound endpoint receives connection set options and connections from its binding server, but it can have its Pulse client software upgraded from any Pulse server that has the automatic upgrade option enabled. During a client software upgrade the client loses connectivity temporarily.

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

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

3. Click **Save Changes**.

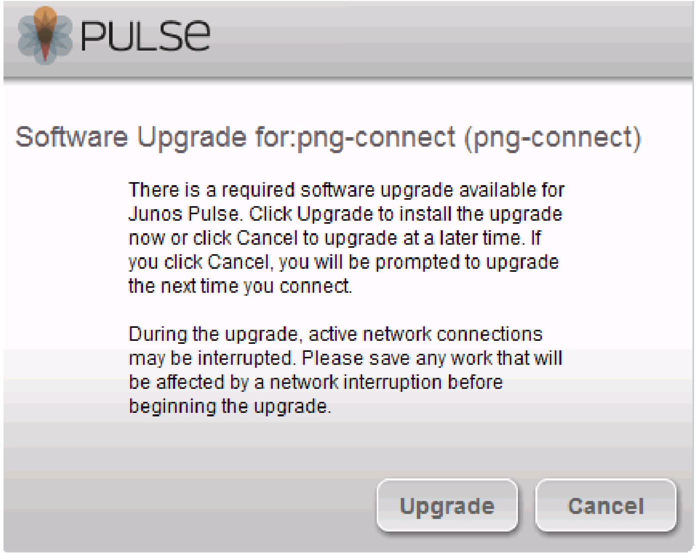
Related Documentation

- Upgrading Junos Pulse Software on page 42

Upgrading Junos Pulse Software

The software image for each supported gateway includes a Junos Pulse client software package. When a newer version of Pulse is available, you can upload the new software to the gateway. You can have more than one version of Pulse on a gateway but only one Pulse client package can be active. If you activate a new version of Pulse, and If the gateway'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 client loses connectivity temporarily.

Figure 5: Pulse Client Upgrade Message



Software Upgrade for:png-connect (png-connect)

There is a required software upgrade available for Junos Pulse. Click Upgrade to install the upgrade now or click Cancel to upgrade at a later time. If you click Cancel, you will be prompted to upgrade the next time you connect.

During the upgrade, active network connections may be interrupted. Please save any work that will be affected by a network interruption before beginning the upgrade.

After you have staged the new Pulse software package in a location accessible to the gateway, use the following procedure to upload the software to an IC Series or SA Series Appliance:

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 gateway 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

- Uploading Pulse Client Software to WXC Series Gateways on page 82
- Enabling or Disabling Automatic Pulse Upgrades on page 41

CHAPTER 3

Configuring Junos Pulse on SA Series Appliances

- Before You Begin on page 45
- Junos Pulse and SA Series Appliances Overview on page 45
- Configuring a Role for Junos Pulse on page 47
- Client Connection Set Options on page 49
- Creating a Client Connection Set on page 53
- Configuring Location Awareness Rules on page 55
- Junos Pulse Component Set Options on page 58
- Creating a Client Component Set on page 58
- Endpoint Security Monitoring and Management on page 60
- Issuing a Remediation Message on page 64
- Using SMS/SCCM Remediation on page 64
- Using Shavlik Remediation on page 66
- Enabling Enhanced Endpoint Security on page 67
- Pushing Junos Pulse Configurations Between Gateways of the Same Type on page 69
- Enabling or Disabling Automatic Pulse Upgrades on page 71
- Upgrading Junos Pulse Software on page 71

Before You Begin

Before you begin configuring Junos Pulse, be sure you have already configured the SA Series Appliance in your network. 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. For complete information, see the *Junos Pulse Secure Access Service Administration Guide*.

Junos Pulse and SA Series Appliances Overview

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

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

- Use the defaults or make changes to the Junos Pulse default component set and default connection set, and then download and distribute Pulse by having users log in to the gateway's user Web portal and be assigned to a role. After the installation is complete, users have all the connections they need to access network resources.
- Create connections that an endpoint needs for connectivity and services, download the Pulse settings file (.jnprpreconfig), download default Pulse .msi installation program, and then run the .msi installation program by using an msiexec command with the settings file as an option. You can use the msiexec command to deploy Pulse using a standard software distribution process, such as SMS/SCCM.
- Distribute Junos Pulse with no preconfiguration. You can download the default Junos Pulse installation file in either .msi or .exe format from the SA Series Appliance, and then distribute the file to endpoints using your organization's standard software distribution methods. Because the installer does not contain preconfigured connections, users must define network connections manually. Or you can create dynamic connections on each access gateway. These connections are automatically downloaded to the installed Pulse client when users provide their login credentials to the gateway's user Web portal.

The following tasks summarize how to configure Junos Pulse on an SA Series Appliance:

- 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. For more information on IVS, see the *Junos Pulse Secure Access Service Administration Guide*.

Related Documentation

- Configuring a Role for Junos Pulse on page 47
- Creating a Client Connection Set on page 23

Configuring a Role for Junos Pulse

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

The following procedure describes the role configuration options that apply to a role that employs Junos Pulse. For complete information about all role configuration options, see the *Junos Pulse Secure Access Service Administration Guide*.

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. Click **Save Changes**. Role configuration tabs appear.

Configuring Role Options for Junos Pulse

All of the options for role configuration tabs are described in the *Junos Pulse Secure Access Service Administration Guide*. The role options that are specific to Junos Pulse are located in the Network tab.

To configure a role for Junos Pulse endpoints:

1. From the admin console, select **Users > User Roles**.
2. Click the role you want to configure and then click the Network Connect tab.
3. Under Client Options, select **Junos Pulse**.
4. Under Split Tunneling Options, select your options:
   - **Split Tunneling**—Split tunneling options let you define how network traffic flows on the client.
     - **Enable**— Pulse modifies routes on the client so that traffic meant for the corporate intranet uses the virtual adapter created by Pulse (the Pulse tunnel) and all other traffic goes through the local physical adapter.

    - **Disable**—When the Pulse session is established, predefined local subnet and host-to-host routes that might cause split-tunneling behavior are removed, and all network traffic from the client goes through the Pulse tunnel. With split tunneling disabled, users cannot access local LAN resources during an active VPN session.

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

- **Route Override**—You can define which routing table takes precedence:
    - **Yes**—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.
    - **No**—Current IP routes take precedence.
- **Route Monitor**—Pulse can monitor the route tables and take appropriate action.
    - **Yes**—Pulse ends the connection if a change is made to the routing tables.
    - **No**—Route tables are allowed to change on the client endpoint.

5. Under **Auto Launch Options**, select the **Auto-launch** check box to activate Pulse automatically when the endpoint is started.
6. In the **Session scripts** area, optionally specify a location for the following:
    - **Windows: Session start script**—Specify a script to run for users assigned to the role after Junos Pulse connects with the SA Series appliance. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources.
    - **Windows: Session end script**—Specify a script to run for users assigned to the role after Junos Pulse disconnects from the SA series appliance. 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.
7. Click **Save Changes**.

Host Checker options allow you to enable Host Checker policies, to choose one or more policies for the role, and to specify whether the endpoint must meet all or just one of the selected Host Checker policies. See the *Junos Pulse Access Control Service Administration Guide* for complete information on configuring endpoint security settings.

To configure Host Checker for a selected role:

1. For a selected role, select **General > Restrictions > Host Checker**.
2. Select the check box **Allow users whose workstations meet the requirements specified by these Host Checker policies**.
3. Click **Add** to move Host Checker policies from the **Available Policies** list to the **Selected Policies** list.
4. Select the check box **Allow access to the role...** to grant access if the endpoint passes any of the selected Host Checker policies.
5. Click **Save Changes**.

Related Documentation

- Junos Pulse and SA Series Devices Overview on page 45

Client Connection Set Options

A Pulse client connection set contains network options and allows you to configure specific connection policies for client access to any access gateway that supports Junos Pulse. Table 5 on page 50 describes connection set options.

Table 5: Configurable Parameters for Junos Pulse Connection Sets

Options	**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.
	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 gateway. See the *Junos Pulse Access Control Service Administration Guide* or the *Junos Pulse Secure Access Service Administration Guide* for complete information about setting up certificate-based authentication.
	Dynamic connections—Allows new connections to be added automatically to a Junos Pulse client when it encounters new supported gateways through the web browser.

Table 5: Configurable Parameters for Junos Pulse Connection Sets *(continued)*

	Wireless suppression—Disables the endpoint's wireless access when a wired connection is available. 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.
When you create a connection for a connection set, you choose a connection type. The following lists the options available for each connection type.	
802.1X options	**Adapter type**—Specifies the type of adapter to use for authentication: wired or wireless.
	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.
	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.
Trusted Server List for 802.1X Connection	**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.
IC or SA options	**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.
	This server—Specifies whether you want the endpoint to connect to this gateway.
	URL—Allows you to specify a URL for a different gateway as the default connection. Specify a different server's URL to create connections for other gateways in your network.

Table 5: Configurable Parameters for Junos Pulse Connection Sets *(continued)*

Firewall options:	**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.
	URL—Specifies the location of the firewall.
WX options	**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. 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.
	Community string—The Junos Pulse client and the Application Acceleration (WXC) gateway can form an adjacency for WAN optimization only if they belong to the same community as identified by the community string. When you create a WX connection, be sure the community string for the connection matches the community string defined on the Application Acceleration (WXC) gateway.
If you create an IC or SA or a Firewall connection, you can also specify how the connection is established, including the rules that control the location awareness feature. 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 logs on—When the endpoint is started and the user has logged on to the endpoint, the Junos Pulse client software connects automatically. 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 connections, you should configure location awareness rules.

Table 5: Configurable Parameters for Junos Pulse Connection Sets *(continued)*

	According to location awareness rules—Location awareness rules enable an endpoint to connect conditionally. For example, the endpoint connects to an IC Series appliance if it is connected to the company intranet or it connects to an SA Series Appliance 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.

Related Documentation

- Junos Pulse and SA Series Devices Overview on page 45
- Creating a Client Connection Set on page 23

Creating a Client Connection Set

To create a 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**
- **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:
   - **802.1X**
   - **IC or SA**
   - **Firewall**
   - **WX**
10. If you select **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.
11. Click **Save Changes**.
12. If you selected **IC or SA** for the type, select or clear the following check boxes:
    - **Allow user to override connection policy**
    - **Connect automatically**
    - **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.
13. If you select **Firewall**, enter an IP address in the Address box.
14. From the Options list, select or clear the following check boxes:
    - **Allow user to override connection policy**
    - **Connect automatically**
    - **URL**—Enter the network address for the firewall.
15. (Optional) You can enable location awareness by creating location awareness rules. Location awareness can force a connection to a particular interface. See “Configuring Location Awareness Rules” on page 24 for more information.

16. If you select **WX**, select the **Connect Automatically** check box to permit the client to automatically form an adjacency to an Application Acceleration (WXC) gateway 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.

17. After you have created the client connection set, create a client component set and select this connection set.

Related Documentation

- Endpoint Security Monitoring and Management on page 29

Configuring Location Awareness Rules

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

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

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

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

The following location awareness example includes two connections. The first connection is an IC Series appliance connection that resolves to TRUE when the endpoint is connected to the corporate LAN. The second connection is an SA Series Appliance connection that resolves to TRUE when the endpoint is located in a remote location.

IC Series appliance 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.
```

SA Series Appliance 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 SA Series Appliance resolves to the external facing IP
address of the SA Series Appliance, 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 WX 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 the SA Series Appliance 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

- Session Migration Overview on page 85

Junos Pulse Component Set Options

A Junos Pulse component includes specific software components that provide Junos 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 gateways and to be able to use application acceleration. When you include the WX component, the disk space requirement for the Junos Pulse client installation increases to 300 MB.
- **No components**—Creates a Pulse preconfiguration settings file (.jnprpreconfig) that updates existing Pulse client configurations, for example, to add a new connection. 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 an IC or SA device. 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. The preconfigured installer always installs all components unless you specify the specific components you want using command line options.

Creating a Client Component Set

Client component options affect Web-based installations only. For a preconfigured installer, specify components as part of the MSIEXEC command. 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 an IC or SA Series Appliance.

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 an IC or SA device. 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. The preconfigured installer always installs all components unless you specify the specific components you want using command line options.

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.

Endpoint Security Monitoring and Management

On Windows systems, 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.

The SA Series device 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 the SA Series device and verify a particular aspect of a host's integrity. Each IMV on the SA Series device 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 device, 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 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 the SA Series device, 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 an SA Series device 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.

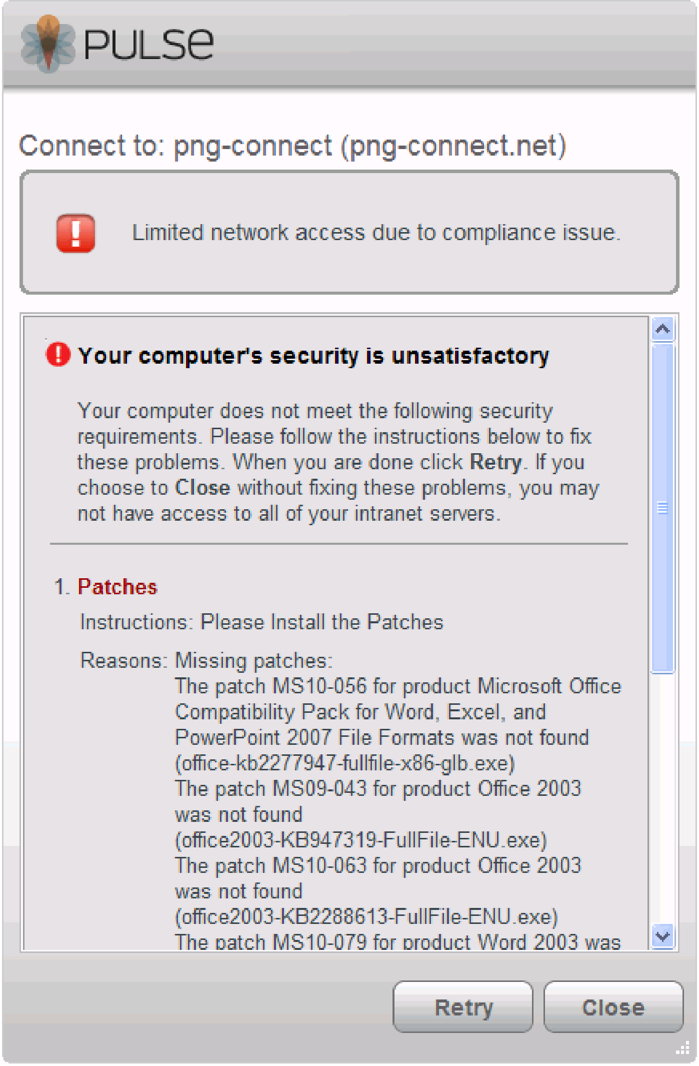
For complete information on configuring Host Checker policies, see the *Junos Pulse Secure Access Service Administration Guide*.

Remediation Options

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

- **Instructions to the user**—The SA Series device 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 6 on page 62 shows a typical Pulse remediation message.

Figure 6: Pulse Remediation Instructions



Connect to: png-connect (png-connect.net)

Limited network access due to compliance issue.

Your computer's security is unsatisfactory

Your computer does not meet the following security requirements. Please follow the instructions below to fix these problems. When you are done click **Retry**. If you choose to **Close** without fixing these problems, you may not have access to all of your intranet servers.

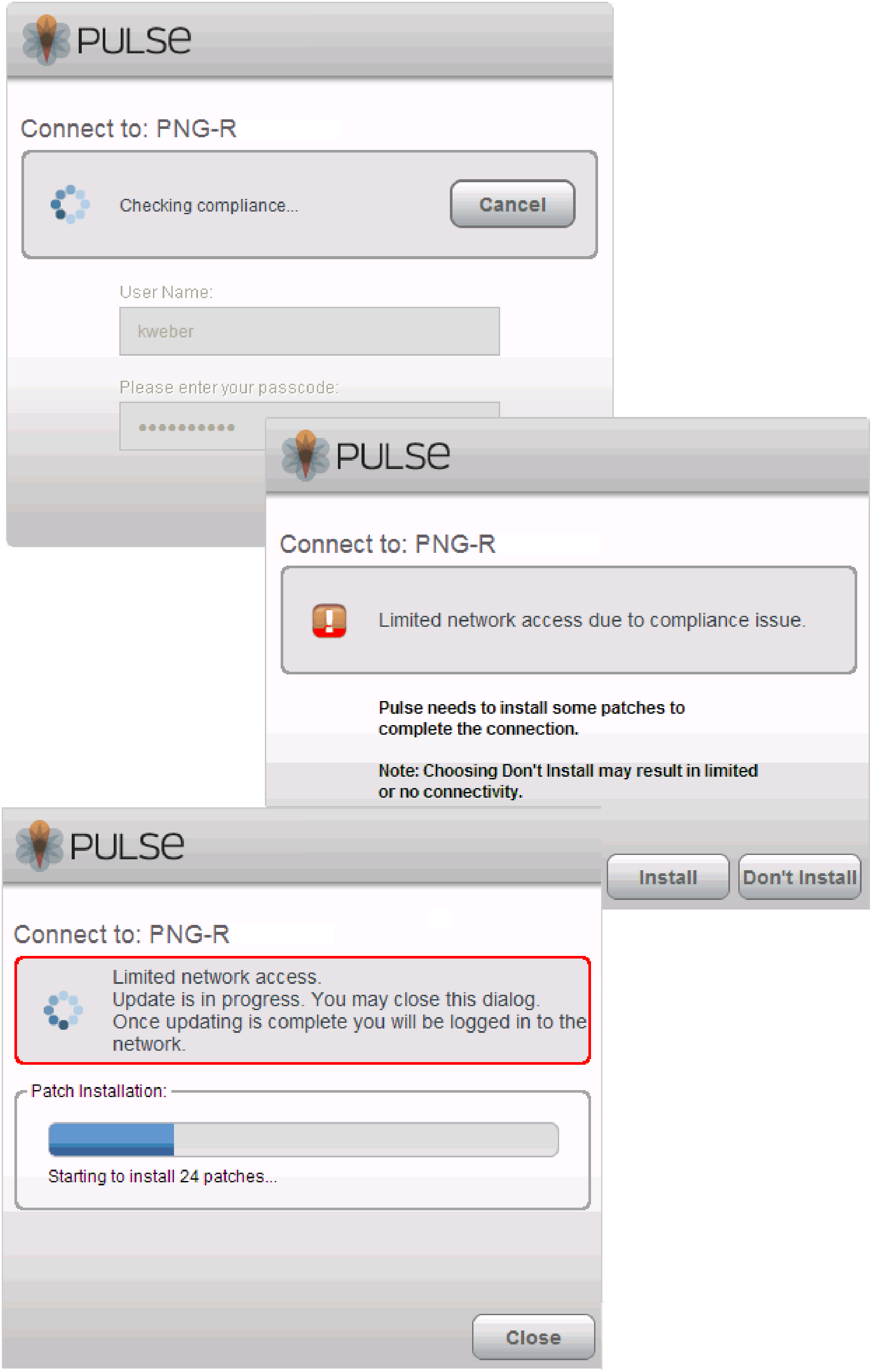
1. Patches

Instructions: Please Install the Patches

Reasons: Missing patches:
The patch MS10-056 for product Microsoft Office Compatibility Pack for Word, Excel, and PowerPoint 2007 File Formats was not found (office-kb2277947-fullfile-x86-glb.exe)
The patch MS09-043 for product Office 2003 was not found (office2003-KB947319-FullFile-ENU.exe)
The patch MS10-063 for product Office 2003 was not found (office2003-KB2288613-FullFile-ENU.exe)
The patch MS10-079 for product Word 2003 was

- **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 software R7.1 and higher 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 7 on page 63

Figure 7: Pulse Client Screens for Shavlik Patch Remediation



Connect to: PNG-R

Checking compliance...

User Name: kweber

Please enter your passcode: ••••••••••

Connect to: PNG-R

Limited network access due to compliance issue.

Pulse needs to install some patches to complete the connection.

Note: Choosing Don't Install may result in limited or no connectivity.

Connect to: PNG-R

Limited network access.
Update is in progress. You may close this dialog.
Once updating is complete you will be logged in to the network.

Patch Installation:

Starting to install 24 patches...

Related Documentation

- Issuing a Remediation Message on page 64
- Using SMS/SCCM Remediation on page 64
- Using Shavlik Remediation on page 66

Issuing a Remediation Message

If a Host Checker policy finds that an endpoint is not in compliance, Host Checker can display a message through Pulse 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 Secure Access 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>, <b>, <br>, <font>, and <a href>. For example:

   You do not have the latest signature files.

   <a href=”www.company.com”>Click here to download the latest signature files.</a>
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.

Using SMS/SCCM Remediation

Pulse supports the SMS/SCCM download method for patch deployment. If the SA Series device 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 IC Series device 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 IC Series or SA Series device, 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.

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

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.

Using Shavlik Remediation

Endpoints with 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 on the SA Series device.

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 the SA Series device 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 R7.1. The default ESAP package shipped with SA R4.1 contains the required patch deployment files. Any older ESAP packages fail to update on these devices. For information on how to update ESAP files, see the *Junos Pulse Secure Access Service Administration Guide*.

The IMC and IMV software for patch monitoring is backward compatible. Since this feature is available from Pulse R2.0 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 more than one IC Series or SA Series device, 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.

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

Enabling Enhanced Endpoint Security

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 the SA Series device, and that you can restrict or quarantine these endpoints according to your Host Checker policy configuration. When EES is running on an endpoint, the Junos 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 IC Series device. 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 the SA Series device 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 the SA Series device, 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 the SA Series device. 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.

User Experience

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 antispyware:

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 on page 64
- Using SMS/SCCM Remediation on page 64
- Using Shavlik Remediation on page 66

Pushing Junos Pulse Configurations Between Gateways of the Same Type

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

This section describes how to use the Push Configuration feature to centrally manage Junos Pulse. For complete details about using Push Configuration to centrally manage all of the settings of an gateway, see the appropriate administration guide.

The following notes apply to pushing configurations:

- You can push to a single gateway or to multiple gateways 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 gateway 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 gateway that is a member of a cluster as long as the target gateway is not a member of the same cluster as the source.

- Target gateways can refuse pushed configuration settings. The default is to accept.
- After an update, the target gateway 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 gateways do not display a warning message when they receive a pushed configuration.
- The target gateway automatically logs out administrators during the push process.
- The source and target gateways must have the same build version and number.
- The administrator account on the source gateway must sign in to the target gateway 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 gateway 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 gateway. 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 access gateway to other gateways of the same type:

1. If you have not already done so, define the targets by selecting **Maintenance > Push Config > Targets**. For detailed procedures on how to define targets, see the appropriate gateway administration guide.
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 gateway. 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 gateway.

6. Add the targets to the **Selected Targets** box.
7. Click **Push Configuration**.

Enabling or Disabling Automatic Pulse Upgrades

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

NOTE: A bound endpoint receives connection set options and connections from its binding server, but it can have its Pulse client software upgraded from any Pulse server that has the automatic upgrade option enabled. During a client software upgrade the client loses connectivity temporarily.

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

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

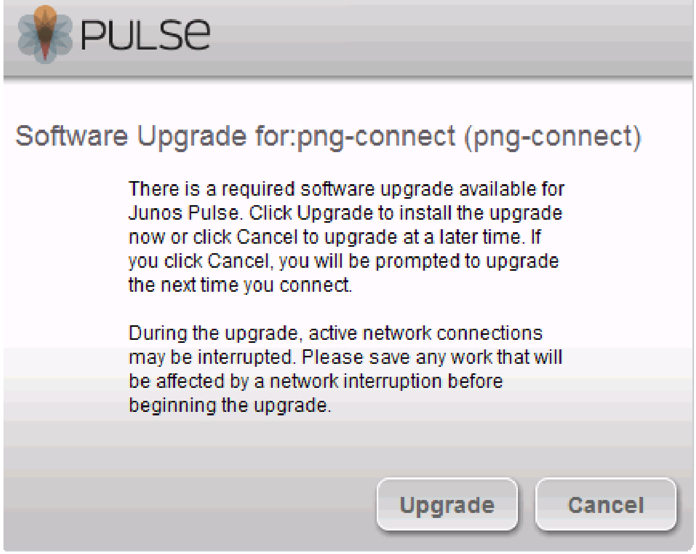
Related Documentation

- Upgrading Junos Pulse Software on page 42

Upgrading Junos Pulse Software

The software image for each supported gateway includes a Junos Pulse client software package. When a newer version of Pulse is available, you can upload the new software to the gateway. You can have more than one version of Pulse on a gateway but only one Pulse client package can be active. If you activate a new version of Pulse, and If the gateway'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 client loses connectivity temporarily.

Figure 8: Pulse Client Upgrade Message



Software Upgrade for:png-connect (png-connect)

There is a required software upgrade available for Junos Pulse. Click Upgrade to install the upgrade now or click Cancel to upgrade at a later time. If you click Cancel, you will be prompted to upgrade the next time you connect.

During the upgrade, active network connections may be interrupted. Please save any work that will be affected by a network interruption before beginning the upgrade.

After you have staged the new Pulse software package in a location accessible to the gateway, use the following procedure to upload the software to an IC Series or SA Series Appliance:

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 gateway 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

- Uploading Pulse Client Software to WXC Series Gateways on page 82
- Enabling or Disabling Automatic Pulse Upgrades on page 41

CHAPTER 4

Configuring Junos Pulse on SRX Series Gateways

- Junos Pulse and SRX Series Gateways on page 73
- Dynamic VPN Configuration Overview on page 74

Junos Pulse and SRX Series Gateways

Junos Pulse supports virtual private network (VPN) tunnel connectivity to SRX Series gateways that are running Junos OS Release 10.2 or later. To configure a firewall access environment for Junos Pulse clients, you must configure the VPN settings on the SRX Series gateway and create and deploy a firewall connection on the Junos Pulse client.

NOTE: Junos Pulse for mobile devices can access SA Series Appliances only. For information about Pulse on mobile devices, see "Junos Pulse for Mobile Devices" on page 109.

SRX Series gateways running Junos OS Release 10.x cannot deploy Junos Pulse client software. For configuration and deployment, you have the following options:

- In an environment that includes SA Series or IC Series appliances, create connections of the type Firewall with a target URL 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 IC Series or SA Series Appliance 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. You can download the Junos Pulse client software from:

  http://www.juniper.net/customers/csc/software/

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.

Dynamic VPN Configuration Overview

A dynamic VPN allows administrators to provide IPsec access to a gateway on a Juniper Networks device.

The following procedure lists the tasks for configuring a dynamic VPN. For detailed information on these topics, see the JUNOS© Software 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 send 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 93

CHAPTER 5

Configuring Junos Pulse on WXC Series Gateways

This chapter describes how to install and manage the Junos Pulse from a WXC Application Acceleration gateway.

- Installing the Junos Pulse Client on page 77
- Managing Software, Configurations, and Policies on page 79

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 WXC Series gateway. The WXC Series gateways and Pulse clients discover each other automatically and begin accelerating traffic without user intervention.

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:

- Downloading the Junos Pulse Client from a WXC Series Gateway on page 77
- Downloading the Junos Pulse Client from an SA Series Appliance on page 78
- Uninstalling the Junos Pulse Client on page 79

Downloading the Junos Pulse Client from a WXC Series Gateway

You can download the Junos Pulse client from any WXC Series gateway running JWOS 6.1 that has a client license. When the license is present, a **Junos Pulse** selection is shown in the taskbar of the Web interface for the WXC Series gateway.

Before users can download the Pulse client software, you must:

- Verify that Pulse client downloads are enabled (see “Enabling Pulse Client Downloads from WXC Series Gateways” on page 79).

- Specify the Pulse client configuration (see “Defining the Pulse Client Configuration on WXC Series Gateways” on page 81).

To download the Pulse client from a WXC Series gateway 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://*WXC 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 Junos Pulse client starts automatically, and the Junos Pulse icon is shown in the system tray in the lower-right corner of the Windows desktop. Application acceleration starts automatically when remote WXC gateways are discovered. No additional configuration is necessary.

Downloading the Junos Pulse Client from an SA Series Appliance

The Junos Pulse client can be downloaded and installed automatically when users access an SA Series Appliance. For version 6.5 or 6.3 SA Series Appliances, the Junos Pulse client must first be exported from a WXC Series gateway and uploaded to the SA Series Appliance. (See “Distributing the Pulse Client from WXC Series Gateways” on page 82.) Note that version 7.0 (or later) SA Series Appliances include the Junos Pulse client, so exporting the client from a WXC Series gateway is not necessary.

To download the Junos Pulse client from an SA Series Appliance:

1. On a computer running Windows 7, Windows Vista, or Windows XP, enter the URL of the SA Series Appliance in a supported Web browser. For example:

   https://wx-sa.juniper.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 to download and install 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 remote WXC Series gateways are discovered. 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 clients:

- Enabling Pulse Client Downloads from WXC Series Gateways on page 79
- Enabling Pulse Client Adjacencies on WXC Series Gateways on page 80
- Configuring Pulse Client Policies on WXC Series Gateways on page 80
- Viewing the Status of Pulse Clients on WXC Series Gateways on page 80
- Defining the Pulse Client Configuration on WXC Series Gateways on page 81
- Viewing the Pulse Client Configuration on WXC Series Gateways on page 82
- Uploading Pulse Client Software to WXC Series Gateways on page 82
- Distributing the Pulse Client from WXC Series Gateways on page 82

Enabling Pulse Client Downloads from WXC Series Gateways

Windows users can download and install the Junos Pulse client software from a WXC Series gateway running JWOS 6.1 or later 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 WXC Series gateway (see “Uploading Pulse Client Software to WXC Series Gateways” on page 82).
3. Select **Allow Pulse software download** to allow users to download the client software.
4. Select **Require user authentication** to require users to log in, and specify the required username and password.
5. Click **Submit** to activate the changes.
6. Click **Save** in the taskbar to retain your changes after the next reboot.

Enabling Pulse Client Adjacencies on WXC Series Gateways

By default, a WXC Series gateway running JWOS 6.1 (or later) 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: If Kaspersky software is installed on the Pulse endpoint, it must be configured to allow traffic on UDP port 3578.

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 WXC 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 on WXC Series Gateways

You can configure compression and acceleration services for each client that is currently adjacent (connected) or that has been adjacent at any time since the last time the WXC Series gateway was restarted. When an adjacency is established, the local application policies are applied to the traffic sent to that client.

To define the default configuration for a client, see “Defining the Pulse Client Configuration on WXC Series Gateways” on page 81.

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 on WXC Series Gateways

You can view the connection status of each Junos Pulse client and the status of each service between the local WXC Series gateway and each remote 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 WXC 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 WXC Series gateway. To enable the service, see “Configuring Pulse Client Policies on WXC Series Gateways” on page 80.
✗	A problem exists, or the service is enabled on the local WXC Series gateway, but disabled on the Pulse client.

Defining the Pulse Client Configuration on WXC Series Gateways

When users download the Junos Pulse client software, a client configuration is included. You must generate a client configuration from the current WXC configuration file (**startup.cfg**) or load a customized configuration file from a local disk, FTP server, or TFTP server.

To view the current client configuration, see “Viewing the Pulse Client Configuration on WXC Series Gateways” on page 82.

1. Select **Junos Pulse > Admin > Load Pulse Configuration**.

   The client configuration and its last update time are indicated at the top of the page. If a client configuration is not defined, **Not Available** is displayed.

2. Select one of the following:

Generate configuration file	Generates a client configuration based on the current WXC configuration saved in the **startup.cfg** file.
Local disk	Specify the path and filename on a machine in your network or click **Browse** and select the configuration file.
TFTP server	Enter a TFTP server’s IP address and the path and filename on the server, such as **/juniper/client_config.cfg**.
FTP server	Enter an FTP server’s IP address and the path and filename on the server, such as **/juniper/client_config.cfg**. 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.

3. Click **Load** to update the client configuration.

Viewing the Pulse Client Configuration on WXC Series Gateways

The default configuration that is downloaded to Junos Pulse clients can be viewed through the Web interface. Note that when you generate the Pulse client configuration from the WXC Series gateway, the client configuration contains a subset of the CLI commands from the gateway configuration.

To view the client configuration:

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

Uploading Pulse Client Software to WXC Series Gateways

When a new version of the Junos Pulse client software becomes available, you must upload it to the WXC Series 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	Enter a TFTP server's IP address and the path and filename on the server.
FTP server	Enter an FTP server's IP address and the path and filename on the server. 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 from WXC Series Gateways

In addition to allowing users to download the Junos Pulse client from a WXC Series 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 SA Series Appliance. For version 6.5 or 6.3 SA Series Appliances, you must export the Pulse client software package from a WXC Series gateway, and then upload the package to the SA Series Appliance. Version 7.0 or later SA Series Appliances include the Pulse client, so exporting the client from a WXC gateway is not necessary. Junos Pulse configuration information for the SA Series Appliance is included in both the *Junos Pulse Administration Guide* and the *Junos Pulse Secure Access Service Administration Guide*.

- **Microsoft System Management Server (SMS) or Microsoft System Center Configuration Manager (SCCM)**—You can distribute the Junos Pulse client through SMS/SCCM by exporting the client configuration for inclusion in the Windows installer file.

Distributing the Pulse Client Through an SA Series Appliance

Use the following procedure to distribute the Junos Pulse client through a version 6.5 or 6.3 SA Series Appliance. To distribute the Pulse client through a version 7.0 or later SA Series Appliance, 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 on WXC Series Gateways” on page 81).
2. Select **Junos Pulse > Admin > Export Pulse Software**.
3. Export the client software package to be installed on an SA Series Appliance:
   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 folder or file share.
4. Upload the exported software package to an SA Series Appliance:
   a. Log in as an administrator to the admin console of the SA Series Appliance 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 SMS/SCCM

To use SMS/SCCM to distribute the Junos Pulse client, you must export the client configuration from the WXC Series gateway and use it to replace the default client configuration in the Windows installer file.

To distribute the Junos Pulse client through SMS/SCCM:

1. Export the client configuration from the WXC Series 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 folder or file share.
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 **http://www.juniper.net/customers/support**.
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 on 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 WXC, 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

- Session Migration Overview on page 85
- Task Summary: Configuring Session Migration on page 89
- Configuring Session Migration for the Pulse Client on page 90
- Configuring an IF-MAP Federated Network for Session Migration on page 90

Session Migration Overview

When you enable session migration on two or more Juniper gateways (IC Series gateways and SA Series gateways), a Pulse endpoint can migrate from one location to another and connect to a different access gateway without providing additional authentication. For example, a user can be connected from home through an SA Series gateway, and then arrive at work and connect to an IC Series gateway 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 gateway.

Sessions can be migrated between IC Series gateways and SA Series gateways 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 gateways 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 IC Series gateway or SA Series gateway 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 gateway, the migrating gateway publishes new session information to the IF-MAP server. The session is associated with the migrating gateway. The IF-MAP server notifies the authenticating gateway, and information about the session that existed from the authenticating gateway is removed, leaving only session information from the migrating gateway on the IF-MAP server. The authenticating gateway removes information about the session from its local session table, and the user license count is decremented.

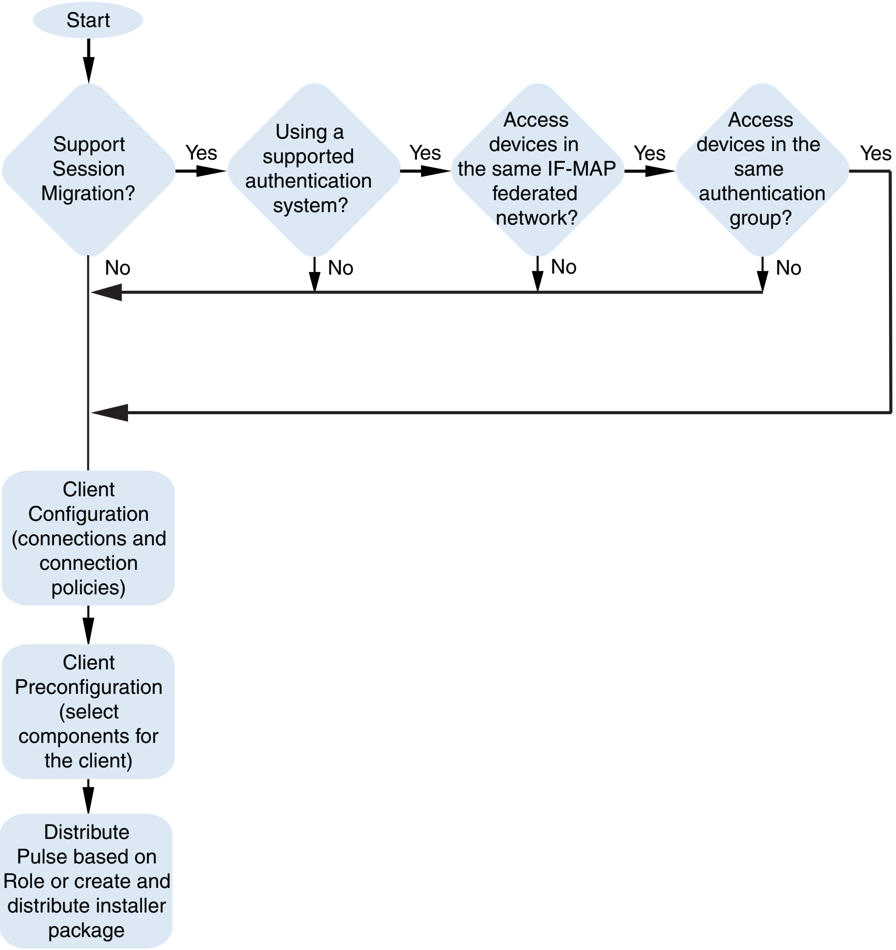
When a session is migrated, its attributes perform role-mappings according to the realm. Standard role-mapping rules determine user access capabilities. You can import user attributes when a session is migrated, or you can configure a dedicated directory server to look up attributes for migrated user 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 gateways should ensure that Host Checker policies are appropriately configured for endpoint compatibility.

The new session is displayed in the Active Users log of the migrating access gateway, and the license count is incremented for the duration of the session.

Figure 9 on page 87 illustrates the task flow for enabling session migration for Pulse.

Figure 9: Requirements for Pulse Session Migration


Start
Support Session Migration?
Yes
Using a supported authentication system?
Yes
Access devices in the same IF-MAP federated network?
Yes
Access devices in the same authentication group?
Yes
No
No
No
No
Client Configuration (connections and connection policies)
Client Preconfiguration (select components for the client)
Distribute Pulse based on Role or create and distribute installer package

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 IC Series gateway, sessions are retained until the heartbeat timeout expires. For SA Series gateway sessions, the idle timeout determines how long the session is retained.

If an endpoint that is connected to an IC Series or SA Series gateway 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 IC Series or SA Series gateway.

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.

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 Junos Pulse Client on page 90
- Task Summary: Configuring Session Migration on page 89

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 IC Series gateway connection and a SA Series gateway connection.
2. Configure an IF-MAP federated network, with the applicable IC Series gateways 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

- Session Migration Overview on page 85
- Configuring Session Migration for the Junos Pulse Client on page 90
- Configuring an IF-MAP Federated Network for Session Migration on page 90

Configuring Session Migration for the Pulse Client

NOTE: Ensure that all of the IC Series gateways and SA Series gateways 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

- Session Migration Overview on page 85
- Task Summary: Configuring Session Migration on page 89
- Configuring an IF-MAP Federated Network for Session Migration on page 90

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. An SA Series Appliance 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 specify how users request authentication. 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 SA Service Appliance 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

- Session Migration Overview on page 85
- Task Summary: Configuring Session Migration on page 89

CHAPTER 7

Deploying Junos Pulse Client Software

- Junos Pulse Client Installation Overview on page 93
- Installing the Junos Pulse Client from the Web on page 94
- Installing the Junos Pulse Client Using a Preconfiguration File on page 95

Junos Pulse Client Installation Overview

This section describes how to deploy Junos Pulse client software from SA Series and IC Series appliances. SRX Series Services gateways do not yet support Pulse deployment. Application Acceleration gateways (WXC) support deployment of WX connections only. See "Installing the Junos Pulse Client" on page 77 for information about how to deploy Pulse through an Application Acceleration (WXC) gateway.

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

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

You can deploy Junos Pulse to endpoints from SA Series and IC Series appliances in the following ways:

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

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

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

Installing the Junos Pulse Client from the Web

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

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

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

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

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 an access gateway, 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.

Installing the Junos Pulse Client Using a Preconfiguration File

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 .msi installer program using an msiexec (windows\system32\msiexec.exe) command.

NOTE: The preconfigured installer always installs all components unless you specify the specific components you want using the ADDLOCAL command line options. The components installed by a preconfigured installer are determined by the ADDLOCAL option and not by the component set you use to create the preconfiguration file.

To create a preconfigured Junos Pulse installer for distribution to 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**. You specify the components to install with a preconfigured installer in the msiexec command line.
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. 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 msi.
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.
7. Download the appropriate Junos Pulse installer for your Windows environment:
   - Junos Pulse Installer (32-bit)

- Junos Pulse Installer (64-bit)

To install Pulse using the preconfiguration file, run the Pulse installer program using an msiexec command and specify the CONFIGFILE property to specify the preconfiguration file. Command line properties (CONFIGFILE and ADDLOCAL) are case sensitive and must be all caps. The CONFIGFILE property must specify the full path to the configuration file. For example:

```
msiexec -i JunosPulse.msi CONFIGFILE=c:\temp\myconfiguration.jnprpreconfig
```

Installing the Pulse Client Using Advanced Command Line Options

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

- 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 property specifies which features and feature options (sub-features) to install. A feature comprises the core components required to support client connections from the specified platform. You can also specify optional sub-features. For example, if you want to support 802.1X connections, you must specify the Pulse8021x sub-feature.

  NOTE: To install all components, run the installer without using the ADDLOCAL option.

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

  ADDLOCAL features:

  - PulseNC—Pulse components required for SA Series SSL VPN Appliances.
  - PulseUAC—Pulse components required for IC Series Unified Access Control Appliances.
  - PulseSRX—Pulse components required for SRX Series Services Gateways.
  - PulseWX—Pulse components required for Application Acceleration Platforms.

    Optional sub-features:

    - Pulse8021x—Available with PulseUAC. Includes 802.1x connectivity components.
    - NCEES—Available with PulseNC. Includes Enhanced Endpoint Security components for connections to an SA Series Appliance.
    - NCTNCClientPlugin—Available with PulseNC. Includes Trusted Network Connect components for connections to an SA Series Appliance.

- UACEES—Available with PulseUAC. Includes Enhanced Endpoint Security components for connections to an IC Series Unified Access Control Appliance.
- UACTNCClientPlugin—Available with PulseUAC. Includes Trusted Network Connect components for connections to an IC Series Unified Access Control Appliance.
- UACNetshim—Available with PulseUAC.

Examples

To install PulseUAC with 802.1x and EES support, use the following command line:

```
msiexec -i JunosPulse.msi ADDLOCAL=PulseUAC,Pulse8021x,UACEES
```

To install PulseNC and PulseSRX, use the following command line:

```
msiexec -i JunosPulse.msi ADDLOCAL=PulseNC,PulseSRX
```

To install PulseNC with EES and TNC Client Plugin, use the following command line:

```
msiexec -i JunosPulse.msi ADDLOCAL=PulseNC,NCEES,NCTNCClientPlugin
```

To install PulseWX, use the following command line:

```
msiexec -i JunosPulse.msi ADDLOCAL=PulseWX
```

If you are installing a sub-feature that is targeted for both PulseNC and PulseUAC, you can specify the sub-feature just once. For example, to install the EES and TNC Client Plugin sub-features on PulseNC and PulseUAC, use any one of the following command lines:

```
msiexec.exe -i JunosPulse.msi ADDLOCAL=PulseUAC,PulseNC,UACEES
msiexec.exe -i JunosPulse.msi ADDLOCAL=PulseUAC,PulseNC,NCCEES
msiexec.exe -i JunosPulse.msi ADDLOCAL=PulseUAC,PulseNC,UACEES,NCCEES
```

Related Documentation

- Creating a Client Connection Set on page 23
- Creating a Client Component Set on page 28

PART 2

Junos Pulse Compatibility

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

- Client Software Feature Comparison on page 101

CHAPTER 8

Client Software Feature Comparison

- Feature Comparison: Odyssey Access Client and Junos Pulse on page 101
- Feature Comparison: Network Connect and Junos Pulse on page 105
- Feature Comparison: WX Client and Junos Pulse on page 107

Feature Comparison: Odyssey Access Client and Junos Pulse

Table 6 on page 101 compares the features in Odyssey Access Client (OAC) Release 5.2 and Junos Pulse.

Table 6: Odyssey Access Client and Junos Pulse Feature Comparison

Feature	Junos Pulse Release 1.0	Junos Pulse Release 2.0	OAC Release 5.2
Wired/Wireless 802.1X Features			
Wired 802.1X support	Yes (with Microsoft Windows supplicant)	Yes (with Microsoft Windows supplicant)	Yes
Auto scan lists	Yes (with Microsoft Windows supplicant)	Yes (with Microsoft Windows supplicant)	Yes
Wireless suppression	Yes (with Microsoft Windows supplicant)	Yes (with Microsoft Windows supplicant)	Yes
Support for Network Provider (scraping passwords, listing)			Yes
Association Mode and Encryption Methods			

Table 6: Odyssey Access Client and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Junos Pulse Release 2.0	OAC Release 5.2
Association mode support (for open, shared, WPA/WPA2)	Yes (with Microsoft Windows supplicant)	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 (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	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
• 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

Table 6: Odyssey Access Client and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Junos Pulse Release 2.0	OAC Release 5.2
Certificates from smart card reader		Yes	Yes
Soft token support		Yes	Yes
Machine login support			Yes
Machine authentication followed by user authentication			Yes
Credential provider on 32- and 64-bit Windows Vista and Windows 7			Yes
Pre-desktop login (to IC Series appliance)			Yes
Configurable UAC Layer 2 connection			Yes
Configurable connection association modes	Connection association modes cannot be configured from client; configuration dynamically downloaded from IC Series appliance		Yes
Certifications			
FIPS compliance			Yes
Common Criteria			
Installation and Upgrade Methods			
Auto-upgrade	Yes	Yes	Yes
Web-based installation	Yes	Yes	Yes
Standalone (MSI) installation	Yes	Yes	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	Yes

Table 6: Odyssey Access Client and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Junos Pulse Release 2.0	OAC Release 5.2
Host Enforcer			Yes
Log viewer			Yes
Logging and Diagnostics	Yes Debug level, file size limits	Yes Debug level, file size limits	Yes
Other Features			
OPSWAT IMV support	Yes	Yes	Yes
Shavlik IMV support (patch assessment)	Yes	Yes	Yes
Automatic patch remediation	Yes via SMS/SCCM	Yes via Shavlik or SMS/SCCM	Yes via SMS/SCCM
Host Checker support	Yes	Yes	Yes
Enhanced Endpoint Security support (Windows OS only)	Yes	Yes	Yes
IPsec tunneling to Policy Enforcement Points with NAT-T	Yes	Yes	Yes
Access service and plug-ins	Yes	Yes	Yes
Block 3rd party EAP messages			Yes
Layer 3 authentication	Yes	Yes	Yes
Server-based pre-configuration of realm/role	Yes	Yes	Yes
Extend session duration			Yes
IC cardinality (connect to IC Series appliances, status message, elapsed time, etc.)	Yes	Yes	Yes
Client-site management of clustered IC Series appliances	Yes	Yes	Yes
Kerberos SSO	Yes	Yes	Yes

Table 6: Odyssey Access Client and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Junos Pulse Release 2.0	OAC Release 5.2
Initial configuration (intervention-less client provisioning)	Yes	Yes	Yes
Dynamically configurable on IC Series appliances	Yes	Yes	Yes

Feature Comparison: Network Connect and Junos Pulse

Network Connect (NC) is a client program for SA Series remote access. Junos Pulse includes most of the functionality of NC. Table 7 on page 105 compares the features of NC and Junos Pulse.

Table 7: Network Connect and Junos Pulse Feature Comparison

Feature	Junos Pulse Release 1.0	Junos Pulse Release 2.0	Network Connect Release 6.3
Proxy Support			
Internet Explorer	Yes	Yes	Yes
Mozilla Firefox			Yes
Split Tunneling Options			
Disable split tunneling without route monitor	Yes	Yes	
Disable split tunneling with route monitor		Yes	Yes
Enable split tunneling with route monitors		Yes	Yes
Enable split tunneling without route monitors	Yes	Yes	Yes
Enable split tunneling with allowed access to local subnet		Yes	Yes
Disable split tunneling with allowed access to local subnet		Yes	Yes
Client Launch Options			

Table 7: Network Connect and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Junos Pulse Release 2.0	Network Connect Release 6.3
Command line launcher			Yes
Log off on connect			Yes
Launch as a standalone client	Yes	Yes	Yes
Launch from browser	Yes	Yes	Yes
GINA and Credential Provider support			Yes
Transport Mode			
SSL fallback mode	Yes	Yes	Yes
ESP			Yes
Other Features			
OPSWAT IMV support	Yes	Yes	Yes
Shavlik IMV support (patch assessment)	Yes	Yes	Yes
Patch automatic remediation	Yes via SMS/SCCM	Yes via Shavlik or SMS/SCCM	
Host Checker support	Yes	Yes	Yes
Enhanced Endpoint Security support (Windows OS only)	Yes	Yes	Yes
Run configured scripts when client connects/disconnects		Yes	Yes
Modify DNS server search order based on SA gateway configuration	Yes	Yes	Yes
Reconnect automatically if connection breaks	Yes	Yes	Yes

Table 7: Network Connect and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Junos Pulse Release 2.0	Network Connect Release 6.3
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 8 on page 107 lists the Network Connect split tunneling options and shows how they map to Pulse 2.0 and later split tunneling options.

Table 8: 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
Enable split tunnel	Enable	Yes	No
Enable split tunnel with route monitor	Enable	Yes	Yes
Enable split tunnel, allow local access	Enable	No	No

Feature Comparison: WX Client and Junos Pulse

Table 9 on page 108 compares the features of the WX Client and Junos Pulse.

Table 9: WX Client and Junos Pulse Feature Comparison

Feature	Junos Pulse Release 1.0	Junos Pulse Release 2.0	WX Client Release 1.0
Acceleration			
TCP acceleration	Yes	Yes	Yes
CIFS acceleration	Yes	Yes	Yes
Compression			
LZ Compression	Yes	Yes	
Caching			
NSC disk based caching			Yes
Adjacencies			
Max adjacencies	4	4	4

PART 3

Junos Pulse for Mobile Devices

- Junos Pulse for Mobile Devices and Junos Pulse Mobile Security Suite on page 111
- Junos Pulse for Apple iOS Devices on page 113
- Junos Pulse for Google Android Devices on page 119
- Junos Pulse for Nokia Symbian Devices on page 123
- Junos Pulse for Windows Mobile Devices on page 127
- Junos Pulse Mobile Security Suite on page 131

CHAPTER 9

Junos Pulse for Mobile Devices and Junos Pulse Mobile Security Suite

- Overview on page 111

Overview

Junos Pulse for mobile devices enables authenticated access from mobile (handheld) devices to corporate applications such as corporate e-mail and the corporate intranet through an SA Series Appliance. 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 Junos Pulse Mobile Security Suite provides 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 VPN client software for the particular device type. The Pulse mobile device software is available as a free download from the app stores of the supported mobile devices. Pulse for mobile devices and Pulse Mobile Security software cannot be deployed directly from an SA Series Appliance. The type of secure connectivity and the supported security features vary according to what is supported on each mobile operating system.

NOTE: For all devices, you should already have your authentication server configured and user accounts created for mobile device users.

Pulse is supported on the following mobile devices:

- Junos Pulse for Apple® iOS
- Junos Pulse for Google Android™
- Junos Pulse for BlackBerry

NOTE: The BlackBerry client does not support VPN connectivity to an SA Series Appliance.

Table 10 on page 132 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 SA 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. The Pulse Mobile Security Gateway is available as software-as-a-service. For more information, see the *Junos Pulse Mobile Security Gateway Administration Guide*.

CHAPTER 10

Junos Pulse for Apple iOS Devices

- Junos Pulse for Apple iOS Overview on page 113
- Configuring a Role and Realm for Pulse for Apple iOS on page 114
- Installing the Junos Pulse VPN App on page 116
- Using Configuration Profiles on page 117
- Collecting Log Files on page 117

Junos Pulse for Apple iOS Overview

Junos Pulse can create an authenticated Layer 3 SSL VPN session between an Apple iOS device (iPhone, iPad, iPod Touch) and an SA Series Appliance. Junos Pulse enables secure connectivity to corporate applications and data based on identity, realm, and role. Junos Pulse is available for download from the iTunes App Store.

SSL VPN access to a Juniper Networks SA Series Appliance requires the following software versions:

- Apple iOS 4.1 or later
- Juniper Networks SA Series Appliance Release 6.4 or later

The Junos Pulse VPN app supports the following features:

- Full Layer 3 tunneling of packets
- UDP/ESP and NCP/SSL modes
- All types of authentication, including client certificate authentication
- 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. For details about how to create a VPN on Demand configuration, see the *iPhone OS Enterprise Deployment Guide*, which is available at www.apple.com.

Before You Begin

Before you configure support for Apple iOS devices on your SA Series Appliance, 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.
- Connecting through proxies that require authentication is not supported.
- Static host mapping is not created for the SA/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 through the SA Series Appliance.
  - When split tunneling is set to Split tunneling enabled, DNS servers that are configured through the SA Series Appliance are used only for hostnames within SA domains.
- Session scripts are not supported.
- RADIUS accounting is not supported.
- Web-based installation from a Juniper gateway that supports Junos Pulse 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.

Configuring a Role and Realm for Pulse for Apple iOS

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

To configure an SA Series Appliance for Apple iOS device access:

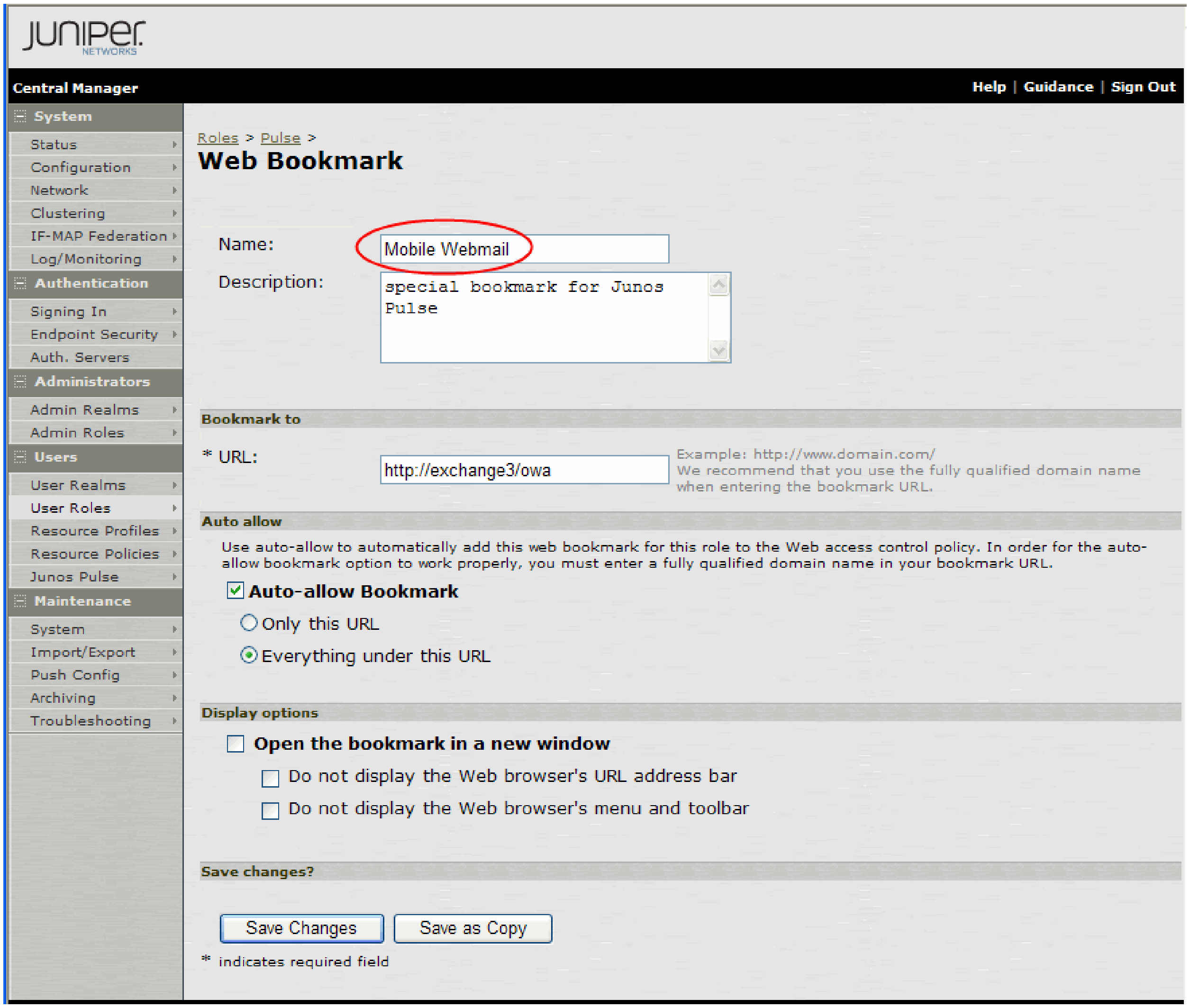
1. Log in to the SA Series Appliance admin console.
2. Select **User Roles > New User Role**.
3. On the New Role page, specify a name for the role and, optionally, a description. Make note of the name because later in this procedure, you create a realm and map realm users to this role.
4. In the Access Features section of the New Role page, select the **Network Connect** check box and the **Network Connect** option.

Although you are configuring access for a Junos Pulse client, you must select the **Network Connect** option.

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 10: Creating the E-mail Bookmark for the Pulse Client



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. See the *Junos Pulse Secure Access Service Administration Guide* for more information on resource policies.

7. To change default session timeouts, 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. On the Network Connect tab for the role, be sure that the **Split Tunneling Options** are set correctly and then click **Save Changes**.
10. Select **Users > Resource Policies > Network Connect > NC Connection Profiles**.
11. Click **New Profile**.

    When the SA Series Appliance receives a client request to start a session, it assigns an IP address to the client based on the IP address policies you define. When you define the connection profile, note the following:

    - Proxy Server Settings—Automatically modifying the client proxy configuration when split tunneling is enabled is not supported.
    - 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.
12. In the Roles area, select **Policy applies to SELECTED roles**. Then add the role you created for iOS devices to the Selected roles list.
13. Click **Save Changes**.
14. Select **Users > User Realms > New User Realm**.
15. Specify a name and description. Then click **Save Changes** to create the realm and to display the realm option tabs.
16. On the General tab for the realm, select the **Session Migration** check box.
17. On the Authentication Policy tab for the realm, click **Host Checker** and make sure that all Host Checker policies are disabled. iOS devices do not support Host Checker.
18. 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.

Installing the Junos Pulse VPN App

Perform the following configuration on each iOS device that is to connect to the SA Series Appliance.

1. Download the Junos Pulse app from the iTunes App Store.
2. On the iOS device, launch Junos Pulse.
3. Tap the Configuration item on the main status page to display Pulse configurations.
4. Create a new configuration with the URL that you defined as the sign-in URL 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 SA gateway 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 SA gateway must be accessed using a hostname (not an IP address), and the hostname must match the Common Name of the SA gateway's SSL certificate.

Using Configuration Profiles

Instead of instructing users to create Junos 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.

Collecting Log Files

The iOS device user can use the following procedure to e-mail the 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**.

CHAPTER 11

Junos Pulse for Google Android Devices

- Junos Pulse for Android Overview on page 119
- Configuring a Role and Realm for Pulse for Android on page 119

Junos Pulse for Android Overview

Junos Pulse can create an authenticated SSL session between a device running Google Android and an SA Series Appliance. 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. Table 10 on page 132 lists the mobile device OS versions supported by Pulse. Android device access is supported by SA Series Release 6.5 and later.

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.

Configuring a Role and Realm for Pulse for Android

To enable access from an Android device to an SA Series Appliance the SA administrator must configure specific realm and role settings on the SA Series Appliance.

To configure an SA Series Appliance for Android device access:

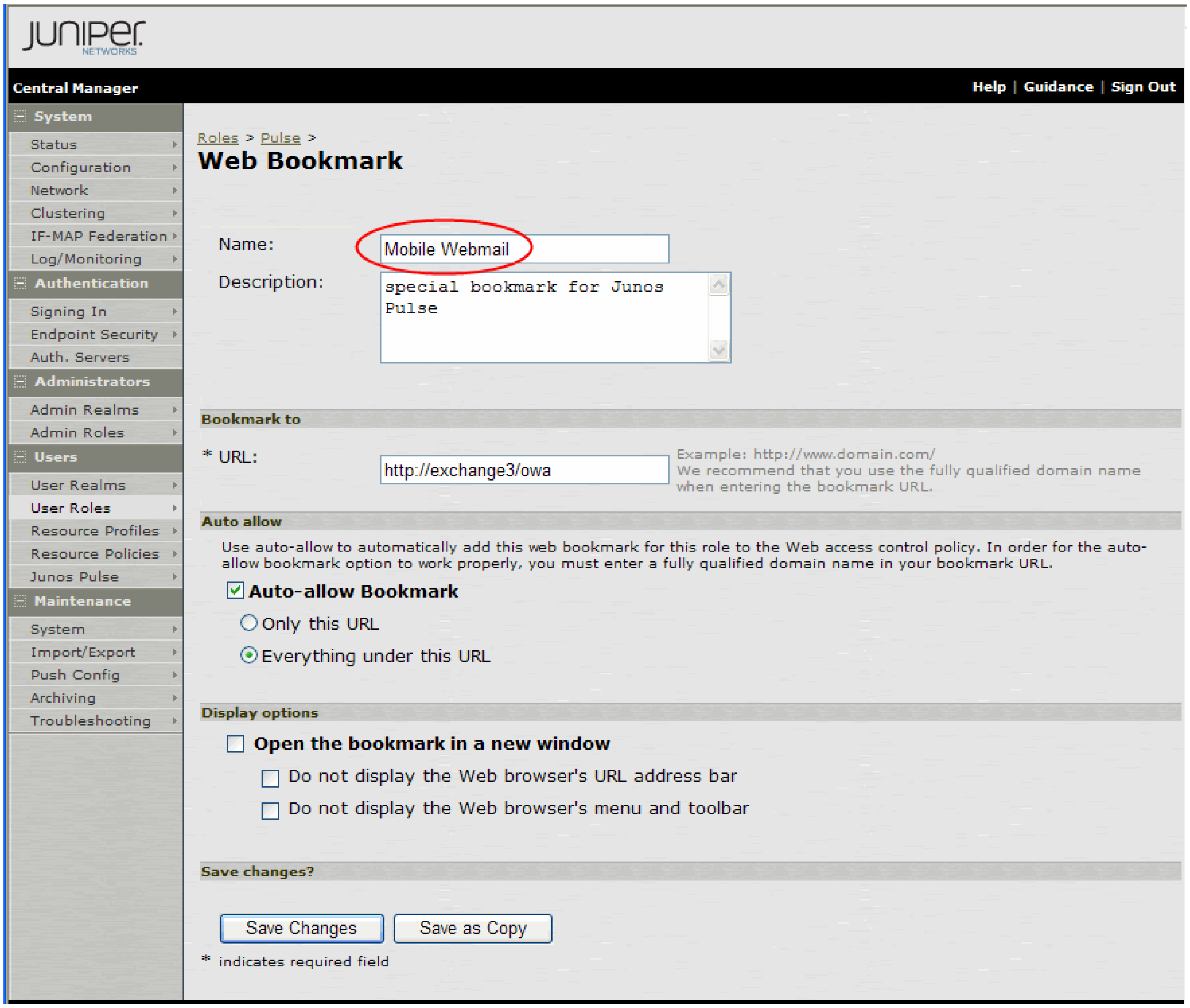
1. Log in to the SA Series Appliance admin console.
2. Select **User Roles > New User Role**.
3. On the New Role page, specify a name for the role and, optionally, a description. Make note of the name because later in this procedure, you create a realm and map realm users to this role.
4. In the Access 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 11: Creating the E-mail Bookmark for the Pulse Client



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. See the *Junos Pulse Secure Access Service Administration Guide* for more information on resource policies.

7. To change default session timeouts, 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 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. See "Junos Pulse Mobile Security Overview" on page 131 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

- Junos Pulse Mobile Security Overview on page 131

CHAPTER 12

Junos Pulse for Nokia Symbian Devices

- Junos Pulse for Symbian on page 123

Junos Pulse for Symbian

Junos Pulse can create an authenticated session between a device running Nokia Symbian and an SA Series Appliance. 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. Table 10 on page 132 lists the mobile device OS versions supported by Pulse. Mobile device access is supported by SA Series Release 7.0 and later.

Configuring an SA Series Appliance for Junos Pulse on Symbian Devices

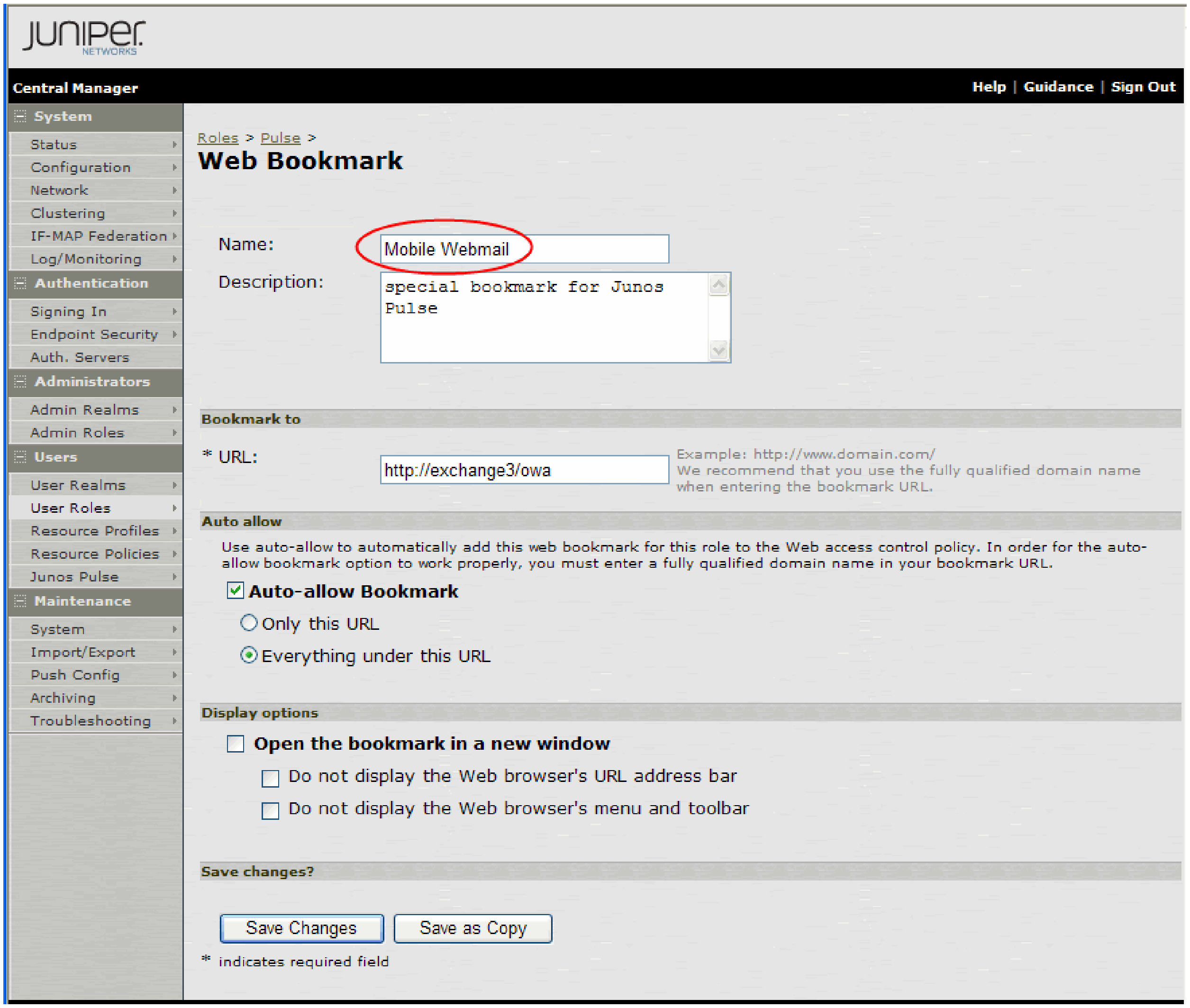
To enable access from a Symbian device to an SA Series Appliance, the device user must download and install the Junos Pulse app, and the SA administrator must configure specific realm and role settings on the SA Series Appliance.

To configure an SA Series Appliance for Symbian device access:

1. Log in to the SA Series Appliance 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 12: Creating the E-mail Bookmark for the Pulse Client



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. See the *Junos Pulse Secure Access Service Administration Guide* for more information on resource policies.

7. To change default session timeouts, 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. See “Junos Pulse Mobile Security Overview” on page 131 for more information.

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 131

CHAPTER 13

Junos Pulse for Windows Mobile Devices

- Junos Pulse for Windows Mobile on page 127

Junos Pulse for Windows Mobile

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. Junos Pulse is available for download from the Windows Marketplace for Mobile. Table 10 on page 132 lists the mobile device OS versions supported by Pulse. Mobile device access is supported by SA Series Release 6.5 and later.

NOTE: Junos Pulse 2.0 introduces new client software for Windows Mobile devices. The Pulse 2.0 client supports the optional Pulse Mobile Security Suite. The Pulse 2.0 client is available as a free download from the Windows Marketplace. If you install the Pulse 2.0 mobile client on a Windows Mobile device that already has the previous version of Pulse for Windows Mobile devices, which is installed directly from an SA Series appliance, the installation detects the presence of the old client and removes it prior to installing the new client.

Pulse R1.0 and Pulse R2.0 for Mobile Devices Compatibility

The Pulse R1.0 client software for Windows Mobile devices is based on Windows Secure Access Manager (WSAM). The Pulse R1.0 client software runs on Windows Mobile devices and on Windows XP, Windows Vista, and Windows 7 endpoints. Pulse R1.0 client software is downloaded and installed from the SA Series device. The Pulse R1.0 client software for Windows Mobile devices supports Host Checker.

Pulse R2.0 client software for Windows Mobile devices is also based on WSAM. However, Pulse R2.0 client software for Windows Mobile devices is new and different software. Instead of downloading and installing it directly from the SA Series device, you download and install it from the Windows Marketplace. Pulse R2.0 client software for Windows Mobile devices does not support Host Checker.

The following describes behaviors and best-use practices to follow in an environment where Pulse 1.0 is already present on Windows Mobile devices:

- If Pulse R1.0 is installed on the mobile device, the Pulse 2.0 installation program uninstalls Pulse R1.0. It also detects and removes Host Checker.
- If Pulse R2.0 is installed on a Windows Mobile device, the user should not use the browser to sign into a realm that has Pulse R1.0 (WSAM) enabled. Pulse R1.0 cannot detect if Pulse R2.0 is already installed, and so it prompts the user to install Pulse R1.0.
- If Pulse 2.0 is installed on a Windows Mobile device, and the user connects to a role on the SA Series device 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 2.0 for Windows Mobile device access.

Configuring an SA Series Appliance for Junos Pulse for Windows Mobile Endpoints

This section describes how to configure Junos Pulse for Windows Mobile endpoints. For more detailed procedures, see the *Junos Pulse Secure Access Service Administration Guide*, which also includes instructions for configuring application-level remote access to enterprise servers from client applications running on Windows, Linux, and Macintosh endpoints.

Before you configure Junos Pulse for Windows Mobile endpoints, be sure that you have completed all the procedures for configuring connectivity for the SA Series Appliance, such as specifying the network identity and adding user IDs.

To configure Junos Pulse for Windows Mobile endpoints on the SA Series Appliance:

1. Create resource profiles that enable access to client/server applications or destination networks and configure the appropriate settings (select **Users > Resource Profiles**).
2. Create supporting auto policies and assign the policies to existing user roles. (Select **Users > Resource Profiles> SAM**).

   We recommend that you use resource profiles, but you can use role and resource policy settings instead by following these steps in the admin console:

   a. Enable access at the role-level using settings (select **Users > User Roles > Role > General > Overview**).

   b. Specify client/server applications and servers (select **Users > User Roles > SAM > Applications**).

   c. Specify application servers (select **Users > Resource Policies > SAM > Access**).
3. After enabling access to client/server applications or destination networks using resource profiles or roles and resource policies, you can modify general role and resource options in the following pages of the admin console:

   a. (Optional) Configure role-level options, such as whether the server automatically launches and upgrades the client software (select **Users > User Roles > SAM > Options**).

b. (Optional) Control IP based hostname matching at the resource level (select **Users > Resource Policies > SAM > Options**).

4. Ensure that an appropriate version of Pulse for Windows Mobile endpoints is available to remote clients (select **Maintenance > System > Installers**).

Defining Applications on the Windows Mobile Device

When you define client/server applications to secure through Junos Pulse on a Windows Mobile device, define applications specific to mobile gateways through user roles.

To define applications:

1. Select **Users > User Roles > *Select Role* > SAM > Applications**.

The following are some mobile gateway-specific executable files that you can enable for mobile endpoints:

- tmail.exe—Specifies the Pocket Outlook application.

  Pulse supports the following modes through Pocket Outlook:

  - S-IMAP/S-POP and S-SMTP
  - ActiveSync—If the mobile endpoint to which you are providing Pocket Outlook access uses ActiveSync, ensure that the IP address of the Exchange Server appears in the list of destination hosts defined in the user role. Direct Push, a feature built into Exchange Server 2007, is supported, but you must set the value of HTTPServerTimeout to 20 minutes or less.
  - mstsc40.exe—Specifies the Windows Terminal Services application.
  - explore.exe—Specifies the Pocket Internet Explorer application.

Related Documentation

- Junos Pulse Mobile Security Overview on page 131

CHAPTER 14

Junos Pulse Mobile Security Suite

- Junos Pulse Mobile Security Overview on page 131
- Requiring Pulse Mobile Security for SA Series Appliance Access on page 133

Junos Pulse Mobile Security Overview

The Junos Pulse Mobile Security Suite is an optional feature of the Junos 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.

NOTE: The user can initiate a backup but the administrator must perform the restore.

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 Administration Guide*.

Pulse Mobile Security Suite Features

Table 10 on page 132 shows the Pulse Mobile Security Suite features that are supported on each mobile device. Connectivity and security features can operate independently from each other. The security features rely on the device's 3G, 4G, or Wi-Fi access. For example, virus definitions are updated without regard to the device's VPN status.

Table 10: Pulse Mobile Security Suite Features

Pulse Mobile Security Feature	Google Android (1.6, 2.0, 2.1, 2.2)	Apple iOS (4.1)	Windows Mobile (6.0, 6.1 and 6.5)	Symbian (Series 60 3rd and 5th editions)	BlackBerry (4.2 and later)
VPN	Access is through an authenticated SSL browser session.	✓	✓	✓	
Antivirus	✓		✓	✓	✓
Personal firewall			✓	✓	
Antispam			✓	✓	
Backup and restore NOTE: The user can initiate a backup. A restore operation must be performed by the administrator.	✓		✓	✓	✓
Monitor and Control	✓		✓	✓	✓
Antitheft NOTE: Antitheft features are controlled from the gateway.	✓		✓	✓	✓

- Android and Windows Mobile device access is supported by SA Series Release 6.5 and later.
- Symbian device access is supported by SA Series Release 7.0 and later.
- Apple iOS device access is supported by SA Series Release 6.4 and later.
- The Pulse Mobile security check feature is available on SA Series Release 7.0 Release 2 and later.

Pulse Mobile Security Configuration Overview

After users install the Junos Pulse app, which includes Pulse Mobile Security software, the user must register the security software to activate it. The software prompts the user for an optional username and password and for a license key. The Pulse Mobile Security administrator must provide the license key to each user via e-mail or SMS. A successful registration adds device information to the Pulse Mobile Security Gateway database.

NOTE: The optional username and password are reserved for future use.

Requiring Pulse Mobile Security for SA Series Appliance Access

Pulse Mobile Security is an optional licensed feature of the Pulse mobile device app. An SA administrator can configure the SA Series Appliance to perform a host check and require that Pulse Mobile Security be activated on mobile devices before granting access to the device through the SA Series Appliance. If you select security feature, a Pulse client is permitted to connect to the SA only if the following criteria are met:

- The mobile device user has registered Pulse Mobile Security Suite.
- The mobile device has been scanned and is free of viruses.

NOTE: The Pulse Mobile Security Check feature is available on SA Series Appliances Release 7.0 Release 2 or later. The Pulse Mobile Security Check feature is not supported on Apple iOS devices.

To require Pulse Mobile Security software on the device:

1. On the SA Series Appliance admin console, select **Users > User Realms**.
2. Select the realm you created for mobile devices. If necessary, create a new one now.
3. On the Authentication Policy tab, select **Host Checker**.
4. Select the **Enable Mobile Security Check** check box, and then click **Save Changes**.

   The Mobile Security Check is now applied to all realm users. If you have created more than one realm for mobile device access, enable this check box on each realm.

Mobile device users must perform the following tasks:

- Download and install the Pulse client software app for the particular device type. The Pulse Mobile Security client software is bundled with the VPN app.
- Start Pulse Mobile Security by tapping the Pulse icon.
- If the device is not registered, respond to the prompts for registration information, including a license key.

PART 4

Index

- Index on page 137

Index

Symbols

3G wireless.....107

802.1X
- connection, IC Series appliance.....21
- connection, SA Series Appliance.....51

A

acceleration
- client policies 80
- client status 80
- comparison of WX Client and Pulse.....108

Access Manager.....73

ACE server.....20, 50

ActiveSync.....129

ActiveX
- Web installation.....94

adapter type.....21, 51

adjacencies.....108

advanced endpoint defense
- IC.....38
- SA.....67

AES.....102

allow saving logon information
- IC Series Gateway.....20
- SA Series Appliance.....50

allow user connections
- IC Series appliance.....20
- SA Series Appliance.....50

allow user to override connection policy
- connection option, firewall 21, 52
- connection option, IC or SA.....21, 51
- connection option, WX.....52
- WX connection option.....21

Android
- certificate authentication.....119
- versions.....132

antispyware
- IC.....38
- SA.....67

Apple iOS
- versions.....132

Apple iPhone.....114, 116

application-level remote access.....127

authentication
- SecurID.....7

authentication methods.....102

automatic updates.....10

automatic upgrades.....41, 71

autoscan lists.....101

B

BlackBerry.....111
- versions.....132

bound and unbound clients
- overview.....7
- software upgrades.....41, 71

browser requirements.....11

C

certificate
- roles, IC Series appliances.....17
- selection.....20, 50
- smart card.....103
- support.....102

certificate authentication
- Android.....119

CHAP inner authentication.....102

CIFS acceleration
- client policies 80
- client status 80

client errors.....11

clients, Junos Pulse
- configuring adjacencies.....80
- configuring policies 80
- defining the client configuration 81
- distributing through SMS/SCCM or SA.....82
- download from a WXC gateway.....77
- download from SA Series Appliance.....78
- enable downloads 79
- loading a client image 82

uninstall....79
viewing status 80
command line launcher....106
community string....21, 52
component set options
IC Series appliance....27
SA Series Appliance....58
component sets, configuring for Junos Pulse....28, 58
compression 108
client policies 80
client status 80
ConfigMgr....31, 62
configuration, Junos Pulse client
defining....81
displaying 82
connection rules
configuring....24, 55
connection set
SA Series Appliance....23, 53
connection set options....19, 49
adapter type....21, 51
allow saving logon information....20, 50
allow user connections....20, 50
allow user to override connection policy, firewall....21, 52
allow user to override connection policy, IC or SA....21, 51
allow user to override connection policy, WX....21, 52
community string....21, 52
dynamic certificate trust....20, 50
dynamic connections....20, 50
outer username....21, 51
scan list....21, 51
server certificate DN....21, 51
wireless suppression....20, 51
connectivity
wireless....14
CPU requirements....11
credential provide....103
credential provider....106
customer support....xv
contacting JTAC....xv

D

default deployment....93
default installer....94
defaults, Pulse configuration....8
deployment options
overview....8
diagnostics....103
disk space requirements....11
distributing Junos Pulse clients through SMS/SCCM or SA....82
DNS lookups....26, 57
DNS server search....106
documentation
comments on....xiv
related documentation....xiv
download a Junos Pulse client 77, 78
dynamic certificate trust
IC Series appliance....20
SA Series Appliance....50
dynamic connections....6, 8
IC Series appliance....20
overview....8
SA Series Appliance....50
dynamic VPNs
configuration overview....74

E

EAP methods....102
EAP-GTC inner authentication....102
EAP-JUAC inner authentication....102
EAP-MD5 inner authentication....102
EAP-MSCHAPv2 inner authentication....102
EAP-PEAP outer authentication....102
EAP-TLS outer authentication....102
EAP-TTLS outer authentication....102
EES (Enhanced Endpoint Security
IC....38
SA....67
Enable Mobile Security Check....133
Enable Session Extension....18
encryption methods
IC Series appliance....101
Enhanced Endpoint Security
IC Series appliance component set option....27
Enhanced Endpoint Security (EES)
IC....38
SA....67
error messages....11
ESP transport mode....106
exporting
Junos Pulse client software or configuration....82
extend session....104

F

Fast User Switching, as security risk.................................11
features
    Pulse Mobile Security Suite....................................132
FIPS..103, 107
firewall access
    configuring on SRX..73
Forget Saved Settings...20, 50
FTP servers, using
    to load a client configuration file.............................81
    to load the Pulse client software............................82

G

GINA..106
Google Android
    versions...132

H

hard token...7, 20, 50
hardware requirements...11
Heartbeat Interval..17
Heartbeat Timeout...18
host check...133
Host Checker
    IC Series appliance...17
    Shavlik on IC..36
    Shavlik on SA...66
Host Checker patch assessment policies.......................7
    IC...29
    SA..60
Host Enforcer...104

I

IC Series appliance
    component set option...27
IF-MAP
    configuring for session migration...........................90
    server and client..90
IMCs and IMVs, overview...30
    SA..60
installation
    Junos Pulse clients...77
    requirements...11
installers
    default..94
    preconfigured...94, 95
    Web...93, 94
Instant Virtual System..46

integrity measurement collectors (IMCs) and
  verifiers (IMVs)..30
    SA...60
iOS
    versions...132
iPhone
    installing Pulse...116
    SSL/VPN access..114
IVS...46

J

Java
    Web installation..94
Junos Pulse clients
    configuring adjacencies 80
    configuring policies 80
    defining the client configuration 81
    distributing through SMS/SCCM or SA................82
    download from a WXC gateway..............................77
    download from SA Series Appliance......................78
    enable downloads..79
    loading a client image 82
    uninstall...79
    viewing status 80
Junos Pulse installer, creating...95
Junos Pulse Mobile Security Suite..................................xiv

K

Kaspersky
    and application acceleration..............24, 52, 55, 80
Kerberos SSO...104

L

languages supported...12
learned user settings...20, 50
limit to subnet..18
loading software
    for Junos Pulse clients 82
localization...12
location awareness
    configuring...24, 55
    location awareness rules....................................22, 52
    overview..5
log files
    iOS devices..117
log viewer...104
logging in
    to download Junos Pulse client software 79

LZ compression
    client policies 80
    client status 80

M
machine authentication....103
malware, Host Checker policy
    IC....38
    SA....67
manuals
    comments on....xiv
Max. Session Length....17
memory requirements....11
messages....11
Microsoft System Center Configuration
  Manager....31, 62
MSCHAP inner authentication....102
MSCHAPv2 inner authentication....102

N
NAT-T....104
netmask....18
Nokia Symbian
    configuring access....123
    versions....132

O
OAC, feature comparison with Pulse....101
Odyssey Access Client
    compatible versions....13
    feature comparison with Pulse....101
    supported release....13
operating systems support....11
OPSWAT IMV....104, 106
outer username
    802.1X connection, IC Series appliance....21
    802.1X connection, SA Series Appliance....51

P
PAP inner authentication....102
passwords
    one-time....20, 50
    to download Junos Pulse client software....79
patch assessment version monitoring....7
patch assessment, in Host Checker policy....7
    IC....29
    SA....60

platform support
    gateways....10
    Windows....11
port 3578
    and application acceleration....24, 52, 55, 80
preconfigured installer....8, 94, 95
protecting against malware, spyware
    IC....38
    SA....67
Pulse and security certificates....6
Pulse Mobile Security Suite....xiv, 131
    features....132
push configuration....40, 69

R
Radius server....20, 50
realm
    Android devices....121
    iOS devices....116
    Symbian devices....124
releases
    gateway support....10
roaming....18
Roaming session....18
roles
    Android devices....119
    IC Series appliance....17
    iOS devices....114
    SA Series Appliance....47
    Symbian devices....123
    Windows Mobile devices....128
route monitor....105
RSA SecurID
    client software version....7
RSA SofToken....103

S
S-IMAP/S-POP....129
S-SMTP....129
SA Series Appliance, download a Junos Pulse client
  from....78
scan list....6
    802.1X connection, IC Series appliance....21
    802.1X connection, SA Series Appliance....51
scan lists....101
SCCM....31, 62
scripts....106
    IC Series appliance....18
    SA Series....48

Secure Virtual Workspace....14
security
    EES....27
    risk....11
security certificates, with Pulse....6
server certificate DN
    802.1X connection, IC Series appliance....21
    802.1X connection, SA Series Appliance....51
Session lifetime....17
session migration....85
    and authentication server support....88
    and IF-MAP....90
    and session timeout....87
    configuring....90
    overview....5
    task summary....89
session scripts....106
    IC Series appliance....18
    SA Series....48
session time-outs....107
session timeout
    Android....121
    iOS....116
    Symbian....124
Shavlik
    configuring on IC....36
    configuring on SA....66
Shavlik IMV....104, 106
smart card....7, 103
smartcard authentication....20, 50
SMS....31, 62
SMS (System Management Server)....35, 64
soft token....7, 20, 50
SofToken....103
software package....42, 71
software requirements....11
software upgrades
    and bound clients....8
    for Junos Pulse clients 82
    overview....10
split tunneling
    iOS devices....113
split tunneling options....47
split tunnelling
    comparison of NC and Pulse....105
SRX Series gateways
    deployment option....9
SSL fallback....106
supplicant....6
support, technical *See* technical support
supported device versions....132
supported gateways....10
SVW....14
Symbian
    configuring access....123
    versions....132
System Center Configuration Manager....31, 62
System Center Configuration Manager with Host Checker policy....35, 64
system management server (SMS) with Host Checker policy....35, 64

T

TCP acceleration
    client policies 80
    client status 80
technical support
    contacting JTAC....xv
time-to-live, DNS....26, 57
TKIP....102
token authentication....7, 20, 50
troubleshooting
    application acceleration....24, 52, 55, 80

U

UDP port 3578
    and application acceleration....24, 52, 55, 80
unbound clients
    overview....7
uninstall the Junos Pulse client....79
upgrade
    client software....42, 71
upgrading
    client software 82
user interface....4
user roles
    IC Series appliance....17
    SA Series Appliance....47
usernames and passwords
    to download Junos Pulse client software 79

V

version monitoring virus signatures and firewall....7
versions
    gateway support....10
    Windows support....11
virus signature version monitoring....7
VPN....73

W

Web install..93, 94
WEP..102
Wi-Fi
    iOS devices..114
Windows
    supported versions..11
Windows Mobile..127
    configuring access..128
    versions..132
wireless supplicant..6, 14
wireless suppression
    IC Series appliance..20, 101
    SA Series Appliance..51
WPA/WPA2..102
WX Client, feature comparison with Pulse..107
WX connection option
    community string..21, 52
WXC Series gateways
    deployment option..9