JUNIPER NETWORKS

Junos Pulse

Administration Guide

Release

1.0

Published: 2010-09-01

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

Junos Pulse Administration Guide

Revision History
2010-06-09—Release 1.0
2010-09-01—Release 1.0 - updated for iOS device support

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

List of Tables

About This Guide

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
NOTE:	Informational note	Indicates important features or instructions.
CAUTION:	Caution	Indicates a situation that might result in loss of data or hardware damage.

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.

CHAPTER 1

Junos Pulse Overview

Introducing Junos Pulse

Junos Pulse is an integrated 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 Junos Pulse client software and the Junos Pulse connection configurations that reside on the endpoint.

NOTE: For information about Pulse on mobile devices, see "Junos Pulse for Mobile Devices" on page 83.

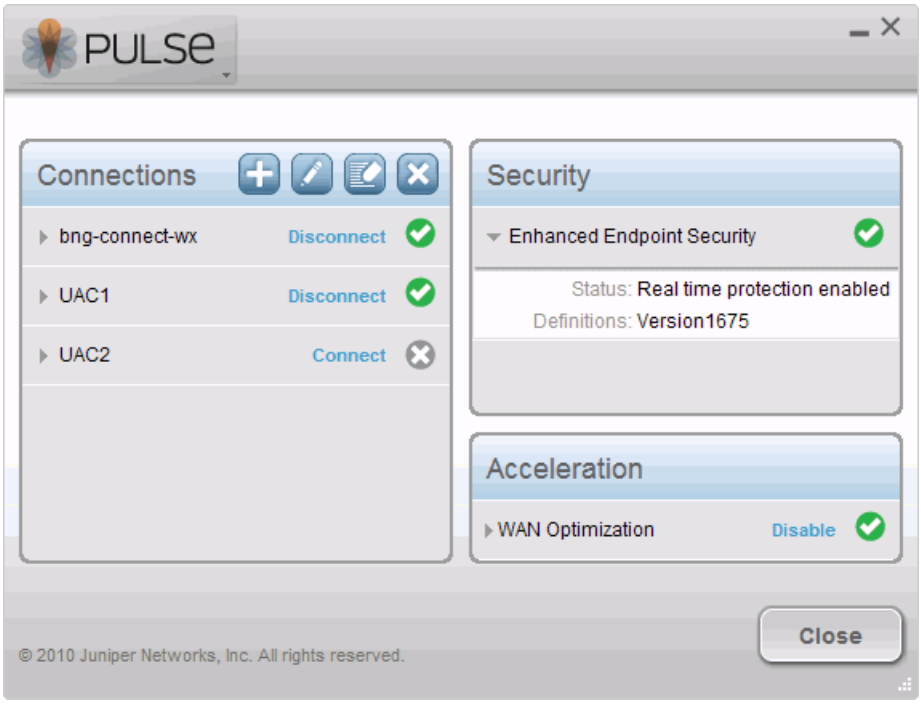
Junos Pulse comprises client and server software. The client enables secure authenticated network connections to protected resources and services over local and wide area networks. The server is integrated into the administrator interface of supported Juniper Networks gateways.

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 Unified Access Control (UAC). In addition, 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 licensed 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.

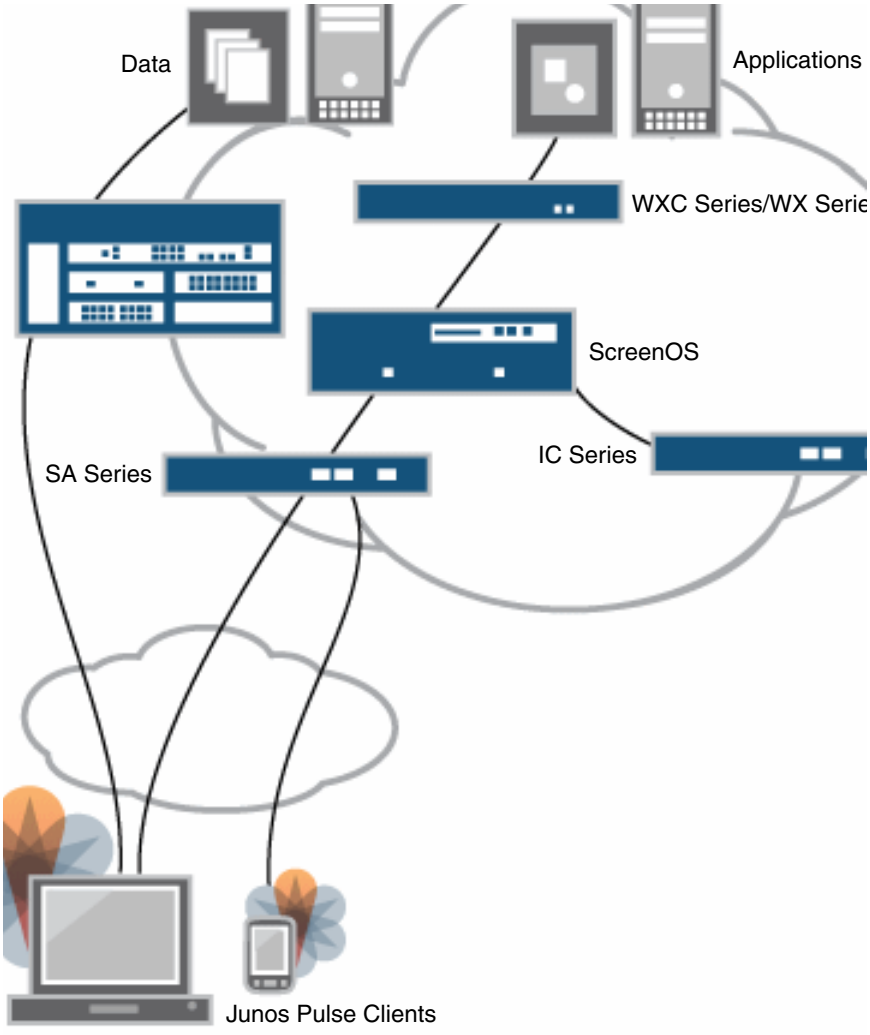
Figure 1: Junos Pulse Client Interface



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 WAN optimization (application acceleration) services. You can also deploy a component of Junos Pulse to provide secure, application-level remote access to enterprise servers from client applications running on mobile endpoints that are running the Windows Mobile operating system.

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 gateway 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 gateway, and then arrive at work and connect through an IC Series gateway 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 gateway to configure all of the connections that clients will need, and then push those configurations (IC to IC or SA to SA) to the other servers using the Push Configuration or the Export/Import XML 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 (except for login credentials) 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.

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 gateways, you can deploy all of the connections and components required for clients to connect to any supported gateway. SA Series and IC Series gateways 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 gateways 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 gateway or SA Series gateway to which the endpoint connects.
- **Preconfigured installer**—Create all of the settings that an endpoint needs for connectivity and services, create an installer package, (.MSI) and distribute the installer file to endpoints.
- **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.

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 gateway. On version 7.0 or later SA Series gateways, 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 gateway to a client. Although an IC Series gateway is for LAN access where WAN application acceleration is not used, IC Series and SA Series gateways can deploy any type of Pulse connection, which allows flexibility in how you deploy Pulse to users.

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 10.0, 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 gateways.
- 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. After installing Pulse, users create a connection to an SRX gateway.

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 gateway, 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 Topics

- Session Migration Overview on page 61
- Junos Pulse for Windows Mobile Endpoints on page 91

- Enabling or Disabling Automatic Pulse Upgrades on page 29

Supported Network Gateways

The following Juniper Networks gateways support Junos Pulse Release 1.0:

- IC Series UAC Gateway Release 4.0
- Secure Access Series Gateway Release 7.0
- WXC Series JWOS Release 6.1
- SRX Series Release 10.0

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 9.5. 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.

Junos Pulse Client Installation Requirements

The Junos Pulse Release 1.0 client software is supported on computers that run Microsoft Windows. Table 2 on page 9 lists the minimum hardware and software requirements to support the Junos Pulse client software. Table 3 on page 10 lists the supported Windows Mobile versions. For expanded platform support information, see the *Junos Pulse Supported Platforms Guide*, which is available at http://www.juniper.net/support/products/pulse.

Table 2: 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 Infranet Controllers. 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.

Table 3: Junos Pulse Client for Mobile Operating System Requirements

Component	Requirement
Mobile operation systems	Windows Mobile 6.5 Standard, Classic, and Professional
	Windows Mobile 6.1 Standard, Classic, and Professional
	Windows Mobile 6.0 Standard, Classic, and Professional

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

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. A user can view the version of OAC by selecting Help > About in the OAC menu bar.

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 Release 5.2 or later 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.

The procedure for enabling the Windows wireless supplicant on the endpoint varies according to the version of Windows. The following procedure describes how to enable the wireless supplicant on a Windows XP endpoint. For detailed information on enabling the wireless supplicant on Windows Vista and Windows 7 endpoints, see the Microsoft documentation on network setup for those operating systems.

To enable the wireless supplicant on a Windows XP endpoint:

1. Select **Start > Control Panel** and then double-click **Network Connections** to display the network connections list.
2. Under LAN and High-speed Internet, right-click **Wireless Network Connection** to display the pop-up menu, and then select **View Available Wireless Networks**.
3. Under Related Tasks, select **Change advanced settings**. The Wireless Network Connection Properties dialog box appears.
4. Click the Wireless Network tab.
5. Select the **Use Windows to configure my wireless network settings** check box, and then click **OK**.

You might also need to configure the properties for available wireless networks before you can connect.

Related Topics

- OAC Features and Junos Pulse on page 75
- Supported Network Gateways on page 9

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 gateway 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. A user can view the version of Network Connect by selecting Advanced View, and then clicking the Information tab.

On endpoints that connect through an SA Series gateway, 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 Topics

- Network Connect Features and Junos Pulse on page 79
- Supported Network Gateways on page 9
- Strong Host, Split Tunnel, Network Connect, and Junos Pulse on page 81

CHAPTER 2

Configuring Junos Pulse on IC Series Gateways

Before You Begin

Before you begin configuring Junos Pulse, be sure you have already configured your IC Series gateway 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 *Unified Access Control Administration Guide*.

Junos Pulse and IC Series Gateways Overview

You must configure the IC Series gateway and the Junos Pulse settings on the gateway so that when users authenticate to a realm, 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 a preconfigured Junos Pulse installer, and then use your organization's standard software distribution methods to deploy it. After the installation is complete, users have all the connections they need to access network resources.
- 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 gateway, and then distribute the file to endpoints using your organization's standard software distribution methods. Because the installer contains 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.

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 *Unified Access Control 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 gateway. Browser options apply only to operations that involve accessing the IC Series gateway 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 gateway 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 gateway 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 *Unified Access Control Administration Guid*e 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 Infranet Controller 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 Infranet Controller 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 Infranet Controller 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 Infranet Controller 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 *Unified Access Control 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 Junos Pulse connects with the Infranet Controller. 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 Infranet Controller. For example, you can specify a script that disconnects mapped network drives.
8. Click **Save Changes**, and then select **Agent > Junos Pulse**.
9. 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.
10. Select **Users > User Realms > Select Realm > Role Mapping > New Rule** to configure role mapping rules that map Junos Pulse users to the role you configured.

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 19 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. The user sees a username and token prompt and the Save settings check box is disabled. 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 *Unified Access Control Administration Guide* or the *Juniper Networks Secure Access 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 gateway if it is connected to the company intranet or it connects to an SA Series gateway 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.

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 23 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.
17. After you have created the client connection set, create a client component set and select this connection set.

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 gateway. But that same client automatically connects to an IC Series gateway 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.

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

IC Series gateway 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 gateway 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 gateway resolves to the external facing IP
address of the SA Series gateway, 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 gateway 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**.

Junos Pulse Component Set Options

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

Component set options include the following choices:

- **All components**—Includes the components listed in Table 5 on page 26. 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. When you include the WX component, the disk space requirement for the Junos Pulse client installation increases to 300 MB.
- **No components**—Creates an installer that updates existing Pulse client configurations, for example, to add a new connection. Do not use this option to create an installer to add Pulse to endpoints that do not already have Pulse installed.
- **Minimal components**—Includes only the components needed to support the selected connections. For example, if the connection set you create includes a connection to an IC Series gateway, the component set will include only the components required

to connect to IC Series gateways. The default is Minimal components, which provides all needed components and limits the size of the Junos Pulse installation file.

Table 5: Junos Pulse Components

Component	Function
Core functions	Allows the client to download a minimal component set and install on endpoints.
802.1X access	Includes the required components for 802.1X connections. Pulse supports 802.1X access for Infranet Controllers. A Pulse 802.1X connection provides configuration settings associated with 802.1X connections including the server certificates associated with the IC and wireless network scan lists. Pulse interacts with the native wired and wireless 802.1X supplicant on the endpoint.
IC or SA access	Provides basic functionality that allows Junos Pulse to interoperate with IC or SA Series or SA Series gateways.
Firewall access	Provides basic functionality that allows Junos Pulse to operate as a dynamic VPN client with Juniper Networks SRX Series firewalls.
WX functionality	Supports application acceleration with Application Acceleration gateways (WXC).
Host Checker	Includes the Trusted Network Computing (TNC) client that allows IC or SA connections to run and enforce Host Checker policies. This component provides support for all existing host checks on Windows machines.
Enhanced Endpoint Security	Allows IC and SA to use the integrated Enhanced Endpoint Security anti malware software.
IC IPsec	Allows the client to use IPsec as a communication method with the IC Series gateway when a Juniper Networks security gateway is employed.
SSL-VPN	Supports SSL connections with the SA Series gateways.

Creating a Client Component Set

To create a client component set:

1. From the admin console, select **Users > Junos Pulse > Components**.
2. Click **New** to create a new component set.
3. If you have not yet created a client connection set, select **Users > 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 gateway.

4. Specify a name for the client component set.
5. (Optional) Enter a description for this client component set.
6. Select a connection set that you have created, or use the default connection set.
7. For Junos Pulse client components, select one of the following option buttons:
   - **All components**—The installer contains all Junos Pulse components and supports all access methods and all features.
   - **No components**—The preconfigured installer is a configuration update only and works on endpoints that already have the Junos Pulse client installed.
   - **Minimal components**—The configuration is analyzed and only the access methods needed to support the connections in the configuration (along with Junos Pulse core components) are included in the installer. Additional components are downloaded as needed at runtime and are not part of the installer.
8. Click **Save Changes**.
9. After you create a component set, distribute the client to users through one of the following methods:
   a. Return to the main **Junos Pulse Client Components** page to download and install the preconfiguration utility and create an installer package.
   b. 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.

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 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.

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

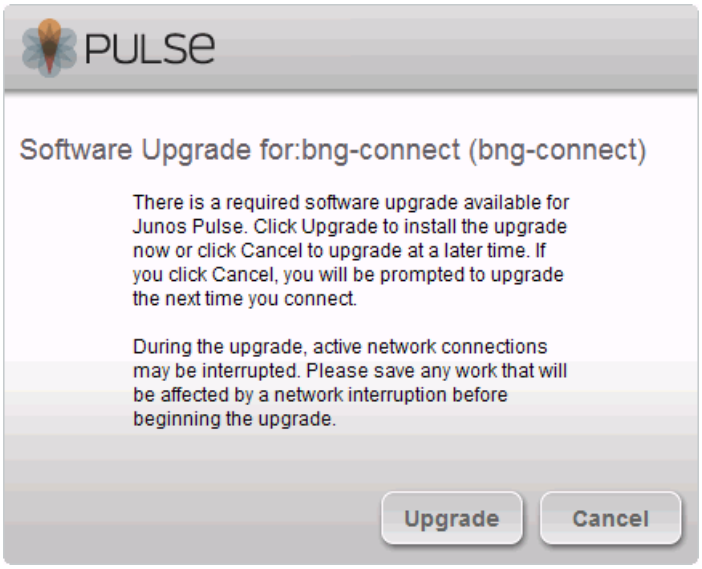
1. From the gateway admin console, select **Maintenance > System > Options**.
2. Set or clear the **Enable automatic upgrade of Junos Pulse Clients** check box.
3. Click **Save Changes**.

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.

Figure 3: Pulse Client Upgrade Message



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 gateway:

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 to select it, and then click **Activate**.

Related Topics

- Uploading Pulse Client Software to WXC Series Gateways on page 58
- Enabling or Disabling Automatic Pulse Upgrades on page 29

CHAPTER 3

Configuring Junos Pulse on SA Series Gateways

Before You Begin

Before you begin configuring Junos Pulse, be sure you have already configured the SA Series gateway 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 *Juniper Networks Secure Access Administration Guide*.

Junos Pulse and SA Series Gateways Overview

Configure the SA Series gateway and the Junos Pulse settings on the gateway so that when users authenticate to a realm, 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 a preconfigured Junos Pulse installer, and then use your organization's standard software distribution methods to deploy it. After the installation is complete, users have all the connections they need to access network resources.
- 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 gateway, and then distribute the file to endpoints using your organization's standard software distribution methods. Because the installer contains 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 gateway:

- 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

Junos Pulse is not compatible with the Instant Virtual System (IVS) feature of SA Series gateways. 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 *Juniper Networks Secure Access Administration Guide*.

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 *Juniper Networks Secure Access 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 *Juniper Networks Secure Access 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 a split tunneling option:
   - **Disable Split Tunneling**—All network traffic passes through the tunnel.
   - **Enable Split Tunneling**—Traffic for the intranet passes through the tunnel and all other traffic uses the local physical adapter.

NOTE: Split tunneling, when enabled, is controlled by split tunneling resource policies. Junos Pulse does not support the **Exclude access** option, which you can enable in a split tunneling resource policy. See the *Juniper Networks Secure Access Administration Guide* for more information about configuring resource policies.

5. Under **Auto Launch Options**, select the **Auto-launch** check box to activate Pulse automatically when the endpoint is started.
6. 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 *Unified Access Control 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**.

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 6 on page 35 describes connection set options.

Table 6: 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. The user sees a username and token prompt and the Save settings check box is disabled. 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 *Unified Access Control Administration Guide* or the *Juniper Networks Secure Access 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 6: 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.
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.

Table 6: Configurable Parameters for Junos Pulse Connection Sets *(continued)*

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.
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 6: 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 gateway if it is connected to the company intranet or it connects to an SA Series gateway 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.

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 23 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.
17. After you have created the client connection set, create a client component set and select this connection set.

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 gateway. But that same client automatically connects to an IC Series gateway 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.

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

IC Series gateway 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 gateway 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 gateway resolves to the external facing IP
address of the SA Series gateway, 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 gateway 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**.

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 the components listed in Table 7 on page 43. 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 an installer that updates existing Pulse client configurations, for example, to add a new connection. Do not use this option to create an installer to add Pulse to endpoints that do not already have Pulse installed.
- **Minimal components**—Includes only the components needed to support the selected connections. For example, if the connection set you create includes a connection to an IC Series gateway, the component set will include only the components required

to connect to IC Series gateways. The default is Minimal components, which provides all needed components and limits the size of the Junos Pulse installation file.

Table 7: Junos Pulse Components

Component	Function
Core functions	Allows the client to download a minimal component set and install on endpoints.
802.1X access	Includes the required components for 802.1X connections. The Pulse client interacts with the native wired and wireless 802.1X supplicant on the endpoint.
IC or SA access	Provides basic functionality that allows Junos Pulse to interoperate with IC or SA Series or SA Series gateways.
Firewall access	Provides basic functionality that allows Junos Pulse to operate as a dynamic VPN client with Juniper Networks SRX Series firewalls.
WX functionality	Supports application acceleration with Application Acceleration gateways (WXC).
Host Checker	Includes the Trusted Network Computing (TNC) client that allows IC or SA connections to run and enforce Host Checker policies. This component provides support for all existing host checks on Windows machines.
Enhanced Endpoint Security	Allows IC Series and SA Series gateways to use the integrated Enhanced Endpoint Security anti malware software.
IC IPsec	Allows the client to use IPsec as a communication method with an IC Series gateway when a Juniper Networks security gateway is employed.
SSL-VPN	Supports SSL connections with SA Series gateways.

Creating a Client Component Set

To create a client component set:

1. From the admin console, select **Users > Junos Pulse > Components**.
2. Click **New** to create a new component set.
3. If you have not yet created a client connection set, select **Users > Junos Pulse > Connections** and create a new connection set. Alternatively, 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 Series or SA Series gateway.
4. Specify a Name for the client component set.
5. (Optional) Enter a Description for this client component set.

6. Select a connection set that you have created, or use the default connection set.
7. For Junos Pulse client components, select one of the following option buttons:
   - **All components**—The installer contains all Junos Pulse components and supports all access methods and all features.
   - **No components**—The preconfigured installer is a configuration update only and works on endpoints that already have the Junos Pulse client installed.
   - **Minimal components**—The configuration is analyzed and only the access methods needed to support the connections in the configuration (along with Junos Pulse core components) are included in the installer. Additional components are downloaded as needed at runtime and are not part of the installer.
8. Click **Save Changes**.
9. After you create a component set, distribute the client to users by one of the following methods:
   a. Return to the main **Junos Pulse Client Components** page to download and install the preconfiguration utility and create an installer package.
   b. Distribute 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 is changed even though the list of components has not, the existing configuration on the endpoint is replaced either right away (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.

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 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.

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

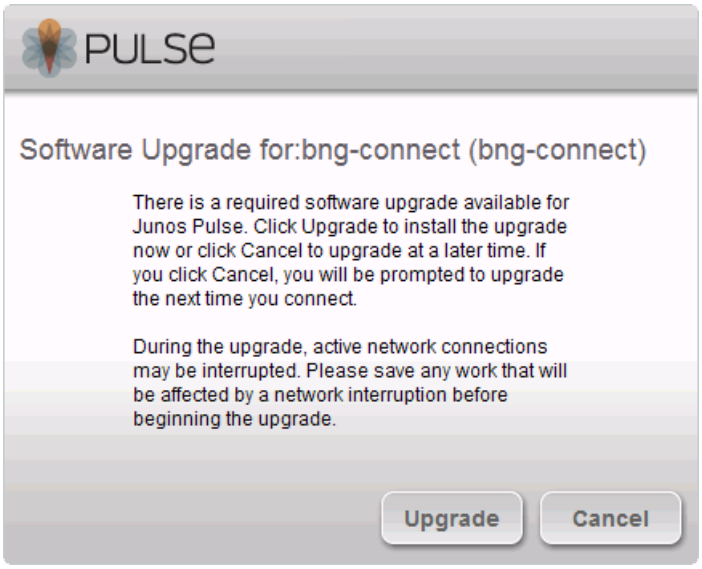
1. From the gateway admin console, select **Maintenance > System > Options**.
2. Set or clear the **Enable automatic upgrade of Junos Pulse Clients** check box.
3. Click **Save Changes**.

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.

Figure 4: Pulse Client Upgrade Message



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 gateway:

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 to select it, and then click **Activate**.

Related Topics

- Uploading Pulse Client Software to WXC Series Gateways on page 58
- Enabling or Disabling Automatic Pulse Upgrades on page 29

CHAPTER 4

Configuring Junos Pulse on SRX Series Gateways

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 10.0 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.

SRX Series gateways 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 gateways, 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 gateway 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 support an earlier access client called Juniper Networks Access Manager. You must uninstall Access Manager before you deploy Junos Pulse to endpoints.Access Manager was released on a limited basis for use with SRX Series Services gateways running Junos OS Release 9.5. 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.

Configuring a Dynamic VPN

The dynamic VPN feature secures traffic through your network by passing it through IPsec VPN tunnels. To configure an IPsec VPN tunnel, you must specify Phase 1 settings (which enable participants to establish a secure channel in which to negotiate the IPsec security association (SA)), and Phase 2 settings (which enable participants to negotiate the IPsec SA that authenticates traffic flowing through the tunnel). This section summarizes the tasks and lists other tasks you must complete in order to enable the tunnels on your network. See the JUNOS© Software documentation for detailed information on how to configure a VPN on an SRX Series gateway.

The dynamic VPN feature is disabled by default on the device. You must enable and configure it before you can use it. As part of the VPN configuration, you define the client configuration. The client and the settings are downloaded to your users' computers. The users must uninstall the VPN client before installing the Junos Pulse client.

To configure the dynamic VPN feature, you must do the following:

1. Define an outgoing interface to pass IKE security associations (SAs) through the device. For more information about interfaces, see the *JUNOS Software Interfaces and Routing Configuration Guide*.
2. Create security policies to define which traffic can pass through your network. For more information about security policies, see "Security Policies Overview" in the *Junos Software Security Configuration Guide*.
3. Create at least one access profile to control the authentication of users who want to establish dynamic VPN tunnels to your firewall. For more information about access profiles, see "Understanding Authentication Schemes" in the *Junos Software Security Configuration Guide*.
4. Create an IKE gateway to include in your VPN configuration:
   - Create one or more IKE Phase 1 proposals. For detailed instructions, see "Configuring an IKE Phase 1 Proposal (Standard and Dynamic VPNs)" and "Configuring an IKE Phase 1 Proposal—Quick Configuration (Dynamic VPNs)" in the *Junos Software Security Configuration Guide*.
   - Create one or more IKE policies. For detailed instructions, see "Configuring an IKE Policy (Standard and Dynamic VPNs)" and "Configuring an IKE Policy—Quick Configuration (Dynamic VPNs)" in the *Junos Software Security Configuration Guide*.
   - Create an IKE gateway configuration. For detailed instructions, see "Configuring an IKE Gateway (Standard and Dynamic VPNs)" and "Configuring an IKE Gateway—Quick Configuration (Dynamic VPNs)" in the *Junos Software Security Configuration Guide*.
5. Create an IPsec AutoKey to include in your VPN configuration:
   - Create one or more IPsec Phase 2 proposals. For detailed instructions, see "Configuring an IPsec Phase 2 Proposal (Standard and Dynamic VPNs)" and

Configuring an IPsec Phase 2 Proposal—Quick Configuration (Dynamic VPNs)" in the *Junos Software Security Configuration Guide*.

- Create one or more IPsec policies. For more detailed instructions, see "Configuring an IPsec Policy (Standard and Dynamic VPNs)" and "Configuring an IPsec Policy—Quick Configuration (Dynamic VPNs)" in the *Junos Software Security Configuration Guide*.

6. Create a client VPN configuration. For detailed configuration instructions, see "Creating a Client Configuration—Quick Configuration (Dynamic VPNs)" and "Creating a Client Configuration (Dynamic VPNs) in the *Junos Software Security Configuration Guide*.
7. Update your security policy (or policies) to include your client VPN configuration. For more information about policies, see "Security Policies Overview" in the *Junos Software Security Configuration Guide*.
8. Specify global settings for client downloads. For detailed configuration instructions, see "Configuring Global Client Download Settings—Quick Configuration (Dynamic VPNs)" and "Configuring Global Client Download Settings (Dynamic VPNs)" in the *Junos Software Security Configuration Guide*.

   The *Junos Software Security Configuration Guide* describes the client download settings that enable an endpoint to download the Access Manager client. This step is necessary to add the access profile that enables the Access Manager client or Junos Pulse to successfully establish a VPN tunnel. However, SRX Series gateways do not support Pulse client deployment, and users who install Access Manager must first uninstall it before they can install Pulse.

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

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

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 55).

- Specify the Pulse client configuration (see “Defining the Pulse Client Configuration on WXC Series Gateways” on page 57).

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 a SA Series Gateway

The Junos Pulse client can be downloaded and installed automatically when users access a SA Series gateway. For version 6.5 or 6.3 SA Series gateways, the Junos Pulse client must first be exported from a WXC Series gateway and uploaded to the SA Series gateway (see “Distributing the Pulse Client from WXC Series Gateways” on page 58). Note that version 7.0 (or higher) SA Series gateways include the Junos Pulse client, so exporting the client from a WXC Series gateway is not necessary.

To download the Junos Pulse client from a SA Series gateway:

1. On a computer running Windows 7, Windows Vista, or Windows XP, enter the URL of the SA Series gateway 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

Windows users can download and install the Junos Pulse client software from a WXC Series gateway running JWOS 6.1 or higher 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 58).
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 higher) can form an adjacency with any client that is running a supported version of the Junos Pulse client software. Traffic is accelerated after the adjacency is established. You can disable and enable client adjacencies at any time. After an adjacency is manually disabled (or disrupted for any reason), it takes about 30 seconds to reestablish the adjacency.

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 57.

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 56.
	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 58.

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. Click **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 gateway. For version 6.5 or 6.3 SA Series gateways, you must export the Pulse client software package from a WXC Series gateway, and then upload the package to the SA Series gateway. Version 7.0 or higher SA Series gateways include the Pulse client, so exporting the client from a WXC gateway is not necessary. Junos Pulse configuration information

for the SA Series gateway is included in both the *Junos Pulse Administration Guide* and the *Secure Access Administration Guide*.

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

Distributing the Pulse Client Through a SA Series Gateway

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

1. Load or generate a Junos Pulse client configuration (see "Defining the Pulse Client Configuration on WXC Series Gateways" on page 57).
2. Select **Junos Pulse > Admin > Export Pulse Software**.
3. Export the client software package to be installed on a SA Series gateway:
   a. Select **Create Host Checker package for use with SA** to have the Host Checker install and start the Junos Pulse client. If the client fails or is stopped manually, it is not restarted automatically.
   b. Click **Export**, click **OK**, and then save the **.zip** file to a local folder or file share.
4. Upload the exported software package to an SA Series gateway:
   a. Log in as an administrator to the admin console of the SA Series gateway and select **Authentication > Endpoint Security > Host Checker**.
   b. Verify that the **Perform check every X minutes** and **Client-side process, login inactivity timeout** are set to 10 minutes or more, and that the timeout interval is not greater than the check interval.
   c. Select **New 3rd Party Policy**, specify a policy name, and select the exported Junos Pulse client software package as the Policies File.
   d. Click **Save Changes**.
   e. Select **Users > User Realms > Select Realm > Authentication Policy > Host Checker**. Select both the **Evaluate Policies** and **Require and Enforce** check boxes for the displayed Junos Pulse client policy.
   f. Click **Save Changes** to save the Host Checker policy.

Distributing the Pulse Client Through SMS

To use SMS 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:

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 on 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

When you enable session migration on two or more Juniper Networks gateways (IC Series gateways and SA Series gateways), a Junos 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 reauthenticating. If session migration is not enabled, Junos Pulse users must reauthenticate 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: either using the same IF-MAP server, or using IF-MAP servers that are replicas of one another.

The gateways must also be in the same authentication group. Authentication groups are configured through authentication realms. An authentication group is simply a string that you define for common usage. You can use authentication groups to tie together realms with similar authentication methods. For example, 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 who have successfully authenticated.

When a user session is migrated to another gateway, the migrating gateway publishes new session information to the IF-MAP server. The session is thereby 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.

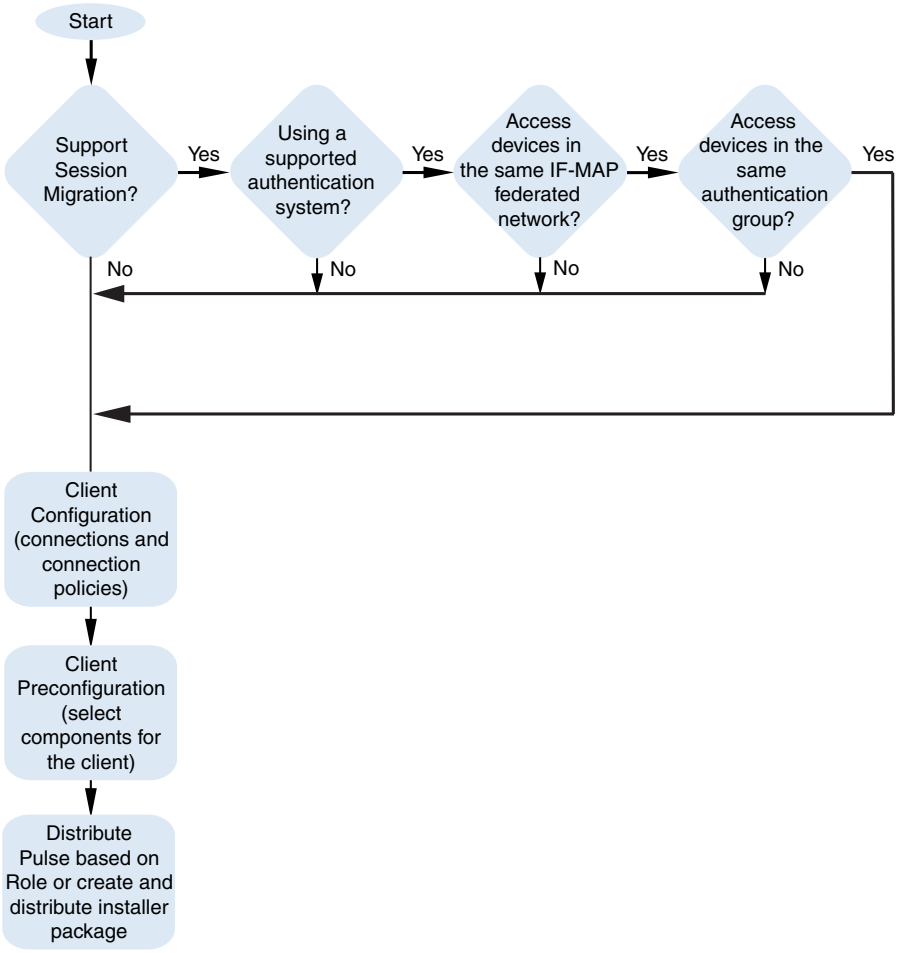
To ensure that session migration retains user sessions, you should configure a limited access remediation role that does not require a Host Checker policy. This is necessary because the Host Checker timeout may be exceeded if an endpoint is in hibernation or asleep. With the new remediation role, the 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 prior to 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 appears in the Active Users log of the migrating access gateway, and the license count is incremented for the duration of the session.

Figure 5 on page 63 illustrates the flow for enabling session migration.

Figure 5: Requirements for Junos Pulse Session Migration



Session Migration and Session Timeout

Session timeout on the authenticating server does not apply to a migrated session. The session start time on the authenticating server 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 has expired. For SA Series gateway sessions, the idle timeout determines how long the session is retained.

If an endpoint connected to an IC Series or SA Series gateway is rebooted and the user has not signed out, when the endpoint is restarted and the user attempts to connect to the same access gateway, Junos 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 for coordinating 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 Junos Pulse client.

When the Junos Pulse client connects to a migrating gateway in the same authentication group, the Junos 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 Junos 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 like online banking can come to work. Because of this flexibility, users might be away from their machines for a long period 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 user sessions do not time out while users are away from their machines. You adjust session lifetime on the gateway on the **Users > User Roles >** *Role Name* **> General > Session Options** page of 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 is 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 into 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, as 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 user name must reflect an existing account.

Related Topics

- Configuring Session Migration for the Junos Pulse Client on page 66
- Task Summary: Configuring Session Migration on page 65

Task Summary: Configuring Session Migration

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

1. Configure location awareness rules within a client connection set to specify locations that should be 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 hibernated.
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 Junos Pulse client to users.

Related Topics

- Session Migration Overview on page 61
- Configuring Session Migration for the Junos Pulse Client on page 66
- Configuring an IF-MAP Federated Network for Session Migration on page 66

Configuring Session Migration for the Junos 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, each of the gateways should be configured in accordance with the procedures outlined in this topic.

To configure session migration:

1. In the admin console, select **Users > User Realms** page.
2. Select an existing realm, or create a new realm.
3. From 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 end users. The authentication group is used as an identifier.
5. Select the option button for either **Use Attributes from IF-MAP** or **Lookup Attributes using Directory Server**.

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

Related Topics

- Session Migration Overview on page 61
- Task Summary: Configuring Session Migration on page 65
- Configuring an IF-MAP Federated Network for Session Migration on page 66

Configuring an IF-MAP Federated Network for Session Migration

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

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

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

You must identify the IF-MAP server to each IC Series device and SA Series device IF-MAP client. To add the server, you specify the IF-MAP URL of the server and how to authenticate to the server. Match the URL and security settings to equal those on the IF-MAP server to which the IF-MAP clients will connect.

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

1. From the admin console select **System > IF-MAP Federation > Overview**.
2. On the IC Series device, under Choose whether this IC Series device runs an IF-MAP Server, an IF-MAP client, or no IF-MAP, select the **IF-MAP Server** option button.
3. Click **Save Changes**.
4. From the admin console select **System > IF-MAP Federation > This Server > Clients**.
5. Under IF-MAP Client, enter a **Name** and an optional **Description** for this client.

   For example, enter the name SA-access1.corporate.com and the description Secure Access 1.
6. Type one or more IP addresses of the client. If the client is multi-homed, for best results list all of its physical network interfaces. If the client is an IC Series device or Secure Access cluster, list the internal and external network interfaces of all nodes. It is necessary to enter all of the IP addresses for all of the interfaces because equipment failures may cause traffic between the IF-MAP client and the IF-MAP server to be re-routed through a different network interface. Listing all of the IP addresses maximizes the probability that IF-MAP Federation still works in the event of a failure.

   For example, enter 172.16.100.105.
7. Under Authentication, select the Client Authentication Method: **Basic or Certificate**.
   a. If you select **Basic**, enter a Username and Password. The same information should be added to the IF-MAP server.
   b. If you select **Certificate**, choose which Certificate Authority (CA) to use to verify the certificate for this client. Optionally, specify certificate attributes or restrictions to require values for certain client certificate attributes.
8. Click **Save Changes** to save the IF-MAP Client instance on the IF-MAP server.

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

1. From the admin console select **System > IF-MAP Federation > Overview**.
2. In the IC Series device, under Choose whether this IC Series device runs an IF-MAP Server, an IF-MAP client, or no IF-MAP, select the **IF-MAP Client** option button. On the SA Series device, select **Enable IF-MAP Client** check box.
3. Type the server URL for IF-MAP Web service on the IF-MAP server. Append the server URL with **/dana-ws/soap/dsifmap** for all Juniper Networks IF-MAP servers.

   For example, https://access2.corporate.com/dana-ws/soap/dsifmap.

4. Select the client authentication method: **Basic** or **Certificate**.

   a. If you select **Basic**, enter a username and password. This is the same as the information that was entered on the IF-MAP server.

   b. If you select **Certificate**, select the device certificate to use.

      Ensure that the certificate of the CA that signed the IF-MAP server certificate is added from the System > Configuration > Certificates > Trusted Server CA page.

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

5. Click **Save Changes**.

Related Topics

- Session Migration Overview on page 61
- Task Summary: Configuring Session Migration on page 65

CHAPTER 7

Deploying Junos Pulse Client Software

Junos Pulse Client Installation Overview

This section describes how to deploy Junos Pulse client software from SA Series and IC Series gateways. 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 53 for information about how to deploy Pulse through an Application Acceleration (WXC) gateway.

The IC Series gateway and SA Series gateway 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 gateway or SA Series gateway 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 gateways 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.
- **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 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). 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.

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 (Users > Junos Pulse > 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 Preconfigured Installer

After you create a client connection set and include the settings within a client component set, you can create an installer package. To do this, you download and install a preconfiguration utility from a link on the IC or SA admin console and install the program on a PC. The preconfiguration utility is a Windows program. You use the utility to bundle your settings and components into an installer that you distribute to users.

NOTE: To distribute new connections to Pulse clients using an installer package, use these procedures and choose **No components** in the component set. In this case, the client receives the new connections but no new components are installed.

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

1. Create a client component set with a custom connection set.
2. From the admin console, select **Junos Pulse > Components**.
3. Click the **download and install pre-configuration utility** link. You are prompted to save the application preconfigurationBuilder.x86.exe.
4. Click **save** to download the application to your PC.
5. On your PC, double-click the downloaded file to install the preconfiguration utility.
6. From the admin console, select **Junos Pulse > Components**.
7. Select the check boxes next to the component sets for the preconfiguration installer that you want to create.
8. Click **Create Install Package**. You are prompted to save the preconfiguration. Make note of the file name and location where you put the file.
9. Save the preconfiguration to your PC.
10. On your PC, select **Juniper Networks > Preconfiguration Builder > Juniper Networks Preconfiguration Builder**. You are prompted to select a Juniper preconfiguration file.
11. Select the preconfiguration that you downloaded. After you specify a file name and location, the Preconfiguration Utility creates a .MSI program that you can distribute to users.

Installing the Junos Pulse Client Using the Default Installer

The Junos Pulse client software installer is included as part of the software image of the access gateway. The default installer includes the components needed for connecting to the access gateway. You can download the default installer from the gateway and distribute it for installation according to your local practices.

To download the Junos Pulse client software default installer:

1. Select **Maintenance > System > Installers**, and distribute the installer to users.
2. Click the Download link next to the Pulse installer format you want:
   - Junos Pulse Installer (.exe)
   - Junos Pulse Installer (.msi)

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.

CHAPTER 8

Client Software Feature Comparison

Feature Comparison: Odyssey Access Client and Junos Pulse

Table 8 on page 75 compares the features in Odyssey Access Client (OAC) Release 5.2 and Junos Pulse Release 1.0.

Table 8: Odyssey Access Client and Junos Pulse Feature Comparison

Feature	Junos Pulse Release 1.0	Odyssey Access Client Release 5.2
Wired/Wireless 802.1X Features		
Wired 802.1X support	Yes (with Microsoft Windows supplicant)	Yes
Auto scan lists	Yes (with Microsoft Windows supplicant)	Yes
Wireless suppression	Yes (with Microsoft Windows supplicant)	Yes
Support for Network Provider (scraping passwords, listing)		Yes
Association Mode and Encryption Methods		
Association mode support (for open, shared, WPA/WPA2)	Yes	Yes

Table 8: Odyssey Access Client and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Odyssey Access Client Release 5.2
Encryption (for WEP, TKIP, AES, WEP with preconfigured key, WPA/WPA2 with pre-shared key)	Yes	Yes
EAP Methods		
EAP-TLS outer authentication	Yes	Yes
EAP-TTLS outer authentication	Yes	Yes
With EAP-MSCHAPv2 inner authentication	Yes	Yes
• With EAP-GTC inner authentication	Yes	Yes
• With EAP-MD5 inner authentication	Yes	Yes
• With EAP-JUAC inner authentication	Yes	Yes
• With EAP-JSSO inner authentication	Yes	Yes
• With EAP-TNC inner authentication	Yes	Yes
• With PAP inner authentication	Yes	Yes
• With CHAP inner authentication	Yes	Yes
• With MSCHAP inner authentication	Yes	Yes
• With MSCHAPv2 inner authentication	Yes	Yes
EAP-PEAP outer authentication		Yes
EAP-GTC outer authentication		Yes
EAP-MD5 outer authenticationn		Yes
EAP-JUAC outer authentication	Yes	Yes
Authentication Methods		
Prompt for user name and password	Yes	Yes
Certificate support (automatic, specific)	Yes	Yes
Certificates from smart card reader		Yes

Table 8: Odyssey Access Client and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Odyssey Access Client Release 5.2
Soft token support		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)		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 gateway	Yes
Certifications		
FIPS compliance		Yes
Common Criteria		
Installation and Upgrade Methods		
Auto-upgrade	Yes	Yes
Web-based installation	Yes	Yes
Standalone (MSI) installation	Yes	Yes
Upgrade/coordinate with previous versions	Yes	Yes
Manual Uninstall	Yes	Yes
Browser based installation and upgrades	Yes	Yes
Diagnostics and Logging		
Server side control for enabling/disabling client logs		Yes
IPsec diagnostics and configuration	Yes	Yes

Table 8: Odyssey Access Client and Junos Pulse Feature Comparison *(continued)*

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

Table 8: Odyssey Access Client and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Odyssey Access Client Release 5.2
Dynamically configurable on IC Series gateways	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 9 on page 79 compares the features of NC and Junos Pulse.

Table 9: Network Connect and Junos Pulse Feature Comparison

Feature	Junos Pulse Release 1.0	Network Connect Release 6.3
Proxy Support		
Internet Explorer	Yes	Yes
Mozilla Firefox		Yes
Split Tunneling Options		
Disable split tunneling without route monitor	Yes	
Disable split tunneling with route monitor		Yes
Enable split tunneling with route monitors		Yes
Enable split tunneling without route monitors	Yes	Yes
Enable split tunneling with allowed access to local subnet		Yes
Disable split tunneling with allowed access to local subnet		Yes
Client Launch Options		
Command line launcher		Yes
Log off on connect		Yes
Launch as a standalone client	Yes	Yes

Table 9: Network Connect and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Network Connect Release 6.3
Launch from browser	Yes	Yes
GINA and Credential Provider support		Yes
Transport Mode		
SSL fallback mode	Yes	Yes
ESP		Yes
Other Features		
OPSWAT IMV support	Yes	Yes
Shavlik IMV support (patch assessment)	Yes	Yes
Patch automatic remediation	Yes via Shavlik or SMS	
Host Checker support	Yes	Yes
Enhanced Endpoint Security support (Windows OS only)	Yes	Yes
Run configured scripts when client connects/disconnects		Yes
Modify DNS server search order based on SA gateway configuration	Yes	Yes
Reconnect automatically if connection breaks	Yes	Yes
Dial-up adapter support	Yes	Yes
3G wireless adapter support	Yes	Yes
Max/Idle Session Time-outs	Yes	Yes
Logging		
Log to file	Yes	Yes
Upload log		Yes

Table 9: Network Connect and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Network Connect Release 6.3
Certifications		
FIPS		Yes

Strong Host, Split Tunnel, Network Connect, and Junos Pulse

Network Connect and Junos Pulse support different behaviors under the strong host model of a multihomed network interface. This behavior difference means that migrating an endpoint from Network Connect to Junos Pulse can result in differences in how network traffic is routed through the endpoint's interfaces.

Multihomed means multiple network interfaces. Each interface has its own IP configuration. When an endpoint has an active network connection through Network Connect or Junos Pulse, it has two connections, the physical connection and a virtual connection created by Network Connect or Junos Pulse.

The strong host and weak host models were defined by Microsoft to minimize security risks in a Windows environment. In a network configuration that uses the strong host model, an endpoint can send packets on an interface only if the interface is assigned the source IP address of the packet being sent, and it can receive packets only on the interface that is specified as the destination IP address of the packet. In a network configuration that uses the weak host model, packets with a destination address of any of the endpoint's interfaces can be received by any of that endpoint's interfaces and the endpoint can send packets on any of its interfaces without regard to the source IP address of the packet being sent. Windows XP uses weak host behavior for IPv4 interfaces and strong host behavior for IPv6 interfaces. Windows Vista and Windows 7 default to strong host behavior.

Network Connect and Junos Pulse exhibit different split tunnel behaviors in a strong host network environment:

- **Network Connect**—When creating a tunnel with split tunneling disabled, Network Connect removes existing default network, local subnet and host-to-host routes. (The local routes are restored when the Network Connect session is terminated.) This change forces all traffic through the tunnel. For example, if a user is connected to a home network and, while sending an FTP stream, the user initiates a Network Connect VPN connection, the FTP connection loses its connection to its destination host. The FTP stream continues only after the interface updates its IP configuration, which must come from the settings provided by the tunnel.
- **Junos Pulse**—When creating a tunnel with split tunneling disabled, Junos Pulse establishes the tunnel on a Junos Pulse virtual adapter and creates duplicate default network, local subnet, and host-to-host routes with lower metric values than the physical interfaces. Connections that exist prior to when Junos Pulse establishes a tunnel continue to operate and pass traffic outside of the tunnel. For example, if a user

is connected to a home network and, while sending an FTP stream, the user initiates a Junos Pulse VPN connection, the FTP stream continues uninterrupted along its original interface according to that interface's IP configuration. If a packet's source IP is the physical interface IP, then the packet is sent from that physical interface.

Feature Comparison: WX Client and Junos Pulse

Table 10 on page 82 compares the features of the WX Client and Junos Pulse.

Table 10: WX Client and Junos Pulse Feature Comparison

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

PART 3

Junos Pulse for Mobile Devices

CHAPTER 9

Junos Pulse for Apple iOS

Junos Pulse for Apple iPhone and Apple iPod Touch

Junos Pulse can create an authenticated Layer 3 SSL VPN session between an Apple iPhone or Apple iPod Touch and an SA Series gateway. 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 gateway requires the following software versions:

- Apple iOS 4.1 or higher
- Juniper Networks SA Series gateway Release 6.4 or higher

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

Before You Begin

Before you configure support for Apple iOS devices on your SA Series gateway, 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 some 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 gateway.
  - When split tunneling is set to Split tunneling enabled, DNS servers that are configured through the SA Series gateway 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 Apple iOS Device Access on SA Series Gateways

To enable SSL/VPN access from an Apple iOS device to an SA Series gateway, 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 gateway.

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

1. Log in to the SA Series gateway admin console.
2. Select **User Roles > New User Role**.
3. On the New Role page, specify a name for the role and an optional 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. On the General tab for the role, click the**Session Options** menu to open the Session Options page.
7. In the **Roaming Session** area, select **Enabled** and then click **Save Changes**.
8. On the Network Connect tab for the role, be sure that the **Split Tunneling Options** are set correctly and then click **Save Changes**. Junos Pulse supports the following split tunneling options:
   - Allow access to local subnet
   - Enable split tunneling
9. Select **Users > Resource Policies > Network Connect > NC Connection Profiles**.
10. Click **New Profile**.

    When the SA Series gateway 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.
11. In the Roles area, select **Policy applies to SELECTED roles**. Then add the role you created for iOS devices to the Selected roles list.
12. Click **Save Changes**.
13. Select **Users > User Realms > New User Realm**.
14. Specify a name and optional description and then click **Save Changes** to create the realm and to display the realm option tabs.
15. On the General tab for the realm, select the **Session Migration** check box.
16. On the Authentication Policy tab for the realm, click **Certificate** and select one of the following options:
    - **Allow all users**—Allow access without using client certificates for authentication.
    - **Only allow users with a client-side certificate signed by Trusted Client CAs to sign in**—A client-side certificate is required. To restrict access even further, you can define unique certificate attribute/value pairs. Note that the client certificate must have all the attributes you define. Users must import the client certificate into their iOS device before they can connect to the SA Series gateway. One method of importing a certificate is through an e-mail attachment. The Apple *Enterprise Deployment Guide* describes all of the methods for adding a certificate to an iOS device.

NOTE: 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.

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.
19. Install custom Web pages for Junos Pulse. See "Installing Custom Sign-in Pages for Apple iOS Device Users" on page 88.
20. Create a custom sign-in URL for the custom sign-in pages. See "Creating a Custom Sign-in URL for an iOS Device" on page 89.
21. Map this sign-in URL to the realm you created earlier in this procedure.

    Make note of the URL. You must communicate this URL to users so they can create the proper Junos Pulse configuration.

Related Topics

- Installing Custom Sign-in Pages for Apple iOS Device Users on page 88
- Creating a Custom Sign-in URL for an iOS Device on page 89

Installing Custom Sign-in Pages for Apple iOS Device Users

We recommend that you install a set of sign-in pages on your SA Series gateway that are properly formatted for a mobile device screen.

To download and install mobile device sign-in pages:

1. Go to http://kb.juniper.net/KB17749. A Juniper KnowledgeBase article includes a link to download a custom sign-in pages file, junos_pulse_custom_pages.zip. Put the file in a location where you can then upload it to the SA Series gateway.
2. On the SA Series gateway admin console, select **Authentication > Signing In > Sign-in Pages**.
3. Click **Upload Custom Pages**.
4. Specify a name that allows you to easily identify this set of pages.
5. For Page Type, select **Access**.
6. Click **Browse**, select the custom sign-in pages file, junos_pulse_custom_pages.zip, and then click **Open**.
7. Click **Upload Custom Pages**.

Creating a Custom Sign-in URL for an iOS Device

The following procedure describes how to specify the settings that are required for creating a mobile device sign-in policy. For complete information about sign-in policies, see the *Juniper Networks Secure Access Administration Guide*.

1. On the SA Series gateway admin console, select **Authentication > Signing In > Sign-in Policies**.
2. Click **New URL**.
3. In the **Sign-in URL** box, specify the URL using the format <*host*>/<*path*>. The path can be any string you want. For example, yourcompany.com/myvpn.
4. In the **Sign-in page** box, select the custom sign-in page you uploaded for iOS device access.
5. In the Authentication realm section, if you select **User picks from a list of authentication realms**, be sure to add to the **Selected realms** list the realm you created for iPhone access.

NOTE: Make note of the URL. You must communicate this URL to iPhone users so they can create the proper Junos Pulse configuration.

6. Click **Save Changes**.

Installing the Junos Pulse VPN App

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

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 Junos Pulse SSL VPN functionality. This security precaution helps deter the silent installation of malicious VPN software. If the user declines to accept the Junos Pulse software, the Junos Pulse splash screen appears until the user presses the Home button on the device. If the user accepts the Junos Pulse software, the security warning no longer appears when Pulse is started.

Collecting Log Files

To examine the Junos Pulse log files that reside on the iOS device, use the following procedure to e-mail the log files by means of the Pulse app:

1. On the iOS device, start the Junos Pulse app.
2. Tap **Status > Email Logs**.
3. Enter an e-mail address and tap **Send**.

CHAPTER 10

Junos Pulse for Windows Mobile

Junos Pulse for Windows Mobile

Junos Pulse can provide secure, application-level remote access to enterprise servers from client applications running 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 NetBIOS file browsing as well as application servers.

NOTE: Junos Pulse on a mobile endpoint requires a different configuration and deployment process than when you deploy Junos Pulse on Windows XP, Windows Vista, or Windows 7 endpoints.

The following describes some important considerations for deploying Junos Pulse on Windows Mobile endpoints:

- Junos Pulse for Windows Mobile endpoints does not support location awareness or session migration.
- Junos Pulse for Windows Mobile endpoints is not available on the SA 700 appliance.

To configure endpoint security on your mobile gateway, see the Host Checker chapter of the *Secure Access Administration Guide*.

Configuring Junos Pulse for Windows Mobile Endpoints

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

NOTE: The process of configuring Junos Pulse for Windows Mobile endpoints is different from the process of configuring Junos Pulse for Windows XP, Windows Vista and Windows 7 endpoints.

Before you configure Junos Pulse for Windows Mobile endpoints, you should make sure that you have completed all the procedures necessary to configure connectivity for the SA Series gateway such as specifying the network identity and adding user IDs.

To configure Junos Pulse for Windows Mobile endpoints:

1. Use the admin console of the SA Series gateway to create resource profiles that enable access to client/server applications or destination networks.
2. Create supporting autopolicies as necessary, and assign the policies to user roles using settings in Users > Resource Profiles> SAM.

   We recommend that you use resource profiles (as described above). However, if you do not want to use resource profiles, you can use role and resource policy settings in the following pages of the admin console instead:

   a. Enable access at the role-level using settings in the **Users > User Roles > Role > General > Overview** page of the admin console.

   b. Specify client/server applications and servers in the **Users > User Roles > SAM > Applications** page of the admin console.

   c. Specify application servers using settings in the **Users > Resource Policies > SAM > Access** page of the admin console.
3. After enabling access to client/server applications and/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 should automatically launch and upgrade the client software using settings in the **Users > User Roles > SAM > Options** page of the admin console.

   b. (Optional) Control IP based hostname matching at the resource level using settings in the **Users > Resource Policies > SAM > Options** page of the admin console.
4. Ensure that an appropriate version of Junos Pulse for Windows Mobile endpoints is available to remote clients using settings in the **Maintenance > System > Installers** page of the SA Series gateway admin console.
5. If you want to enable or disable client-side logging for Junos Pulse on the Windows Mobile endpoints, configure the appropriate options through the **System > Log/Monitoring > Client Logs > Settings** tab of the admin console.

Defining Applications on the Windows Mobile Endpoint

When defining client/server applications to secure through Junos Pulse on a Windows Mobile endpoint, you should define mobile gateway-specific applications through the Users > User Roles > *Select Role* > SAM > Applications page.

Listed below are some mobile gateway-specific executable files that you might want to enable for mobile endpoints:

- tmail.exe—Specifies the Pocket Outlook application

  Secure Access supports the following modes through Pocket Outlook:

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

Installing Junos Pulse on a Windows Mobile Endpoint

Junos Pulse for Windows Mobile endpoints is supported on the following versions of Windows Mobile:

- Windows Mobile 6.5 Standard, Classic, and Professional
- Windows Mobile 6.1 Standard, Classic, and Professional
- Windows Mobile 6.0 Standard, Classic, and Professional

A Windows Mobile endpoint user must first connect to the SA Series gateway through a web browser. The user can invoke Junos Pulse automatically or manually. If you configure the system to auto-launch, the user invokes Junos Pulse simply by signing into the SA Series gateway from the Windows Mobile endpoint. If you or the user disables the auto-launch option, the user can manually invoke Junos Pulse by clicking its link on the SA Series gateway home page. (If you enable auto-launch, users can override the setting through the Preferences > Applications page of the end-user console.) If Junos Pulse is not already installed on the user's Windows Mobile system, the SA Series gateway downloads it to the user's endpoint, and then installs it.

PART 4

Index

Index

D

E

F

G

H

I

S

T

U

V

W