JUNIPER NETWORKS

Junos Pulse

Migration Guide

Release

1.0

Published: 2010-06-09

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

Junos Pulse Migration Guide

Revision History
2010-06-09—Release 1.0

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

END USER LICENSE AGREEMENT

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Table of Contents

About This Guide ix

Audience ix
Document Conventions ix
Requesting Technical Support ix
Self-Help Online Tools and Resources x
Opening a Case with JTAC x

Part 1 Migrating to Junos Pulse

Chapter 1 **Migrating to Junos Pulse 3**

Supported Network Gateways 3
Junos Pulse Client Installation Requirements 4
Migrating From Odyssey Access Client to Junos Pulse 5
Wireless Connectivity, OAC, and Junos Pulse 5
Feature Comparison: Odyssey Access Client and Junos Pulse 6
Migrating From Network Connect to Junos Pulse 9
Feature Comparison: Network Connect and Junos Pulse 10
Strong Host, Split Tunnel, Network Connect, and Junos Pulse 12
Junos Pulse and SRX Series Gateways 13
Migrating from WX Client to Junos Pulse 13
Feature Comparison: WX Client and Junos Pulse 14

Part 2 Index

Index 17

About This Guide

- Audience on page ix
- Document Conventions on page ix
- Requesting Technical Support on page ix

Audience

The *Junos Pulse Migration Guide* is for network administrators who are responsible installing Junos Pulse in an environment that currently supports Odyssey Access Client, Network Connect, WX Client, or firewall VPN client software such as Juniper Networks Access Manager. See the *Junos Pulse Administration Guide* and the gateway administration guides for more information. This guide includes selected information from the *Junos Pulse Administration Guide*.

Document Conventions

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

Table 1: Notice Icons

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

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

Migrating to Junos Pulse

- Migrating to Junos Pulse on page 3

CHAPTER 1

Migrating to Junos Pulse

- Supported Network Gateways on page 3
- Junos Pulse Client Installation Requirements on page 4
- Migrating From Odyssey Access Client to Junos Pulse on page 5
- Feature Comparison: Odyssey Access Client and Junos Pulse on page 6
- Migrating From Network Connect to Junos Pulse on page 9
- Feature Comparison: Network Connect and Junos Pulse on page 10
- Strong Host, Split Tunnel, Network Connect, and Junos Pulse on page 12
- Junos Pulse and SRX Series Gateways on page 13
- Migrating from WX Client to Junos Pulse on page 13
- Feature Comparison: WX Client and Junos Pulse on page 14

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 4 lists the minimum hardware and software requirements to support the Junos Pulse client software. Table 3 on page 4 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

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 6
- Supported Network Gateways on page 3

Feature Comparison: Odyssey Access Client and Junos Pulse

Table 4 on page 6 compares the features in Odyssey Access Client (OAC) Release 5.2 and Junos Pulse Release 1.0.

Table 4: 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
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

Table 4: Odyssey Access Client and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Odyssey Access Client Release 5.2
• 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
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

Table 4: Odyssey Access Client and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Odyssey Access Client Release 5.2
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
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

Table 4: Odyssey Access Client and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Odyssey Access Client Release 5.2
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
Dynamically configurable on IC Series gateways	Yes	Yes

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 10
- Supported Network Gateways on page 3
- Strong Host, Split Tunnel, Network Connect, and Junos Pulse on page 12

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 5 on page 10 compares the features of NC and Junos Pulse.

Table 5: 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

Table 5: Network Connect and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Network Connect Release 6.3
Client Launch Options		
Command line launcher		Yes
Log off on connect		Yes
Launch as a standalone client	Yes	Yes
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

Table 5: Network Connect and Junos Pulse Feature Comparison *(continued)*

Feature	Junos Pulse Release 1.0	Network Connect Release 6.3
Max/Idle Session Time-outs	Yes	Yes
Logging		
Log to file	Yes	Yes
Upload log		Yes
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.

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.

Migrating from WX Client to Junos Pulse

Migrating endpoints from an existing WX Client environment to Junos Pulse requires that you uninstall the old client software from the endpoint and then install Pulse on the endpoint.

NOTE: To support Junos Pulse, WXC Series gateways must be running JWOS 6.1. The upgrade procedure to move from an earlier release to JWOS 6.1 is described in the JWOS 6.1 Release Notes document. See the Juniper Networks Web site at http://www.juniper.net/customers/csc/software. You must follow the upgrade procedure described in the release notes to successfully upgrade a WXC Series gateway to JWOS 6.1.

Feature Comparison: WX Client and Junos Pulse

Table 6 on page 14 compares the features of the WX Client and Junos Pulse.

Table 6: 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 2

Index

- Index on page 17

Index

Symbols

3G wireless....11

A

acceleration
    comparison of WX Client and Pulse....14
Access Manager....13
adjacencies....14
AES....6
authentication methods....7
autoscan lists....6

B

browser requirements....4

C

certificate
    smart card....7
    support....7
CHAP inner authentication....7
command line launcher....11
compression....14
connectivity
    wireless....5
CPU requirements....4
credential provide....7
credential provider....11
customer support....ix
    contacting JTAC....ix

D

diagnostics....8
disk space requirements....4
DNS server search....11

E

EAP methods....6
EAP-GTC inner authentication....6
EAP-GTC outer authentication....7
EAP-JUAC inner authentication....6
EAP-JUAC outer authentication....7
EAP-MD5 inner authentication....6
EAP-MD5 outer authentication....7
EAP-MSCHAPv2 inner authentication....6
EAP-PEAP outer authentication....7
EAP-TLS outer authentication....6
EAP-TNC inner authentication....7
EAP-TTLS outer authentication....6
encryption methods
    IC Series gateway....6
ESP transport mode....11
extend session....9

F

Fast User Switching, as security risk....4
FIPS....8, 12
firewall access
    configuring on SRX....13

G

GINA....11

H

hardware requirements....4

I

installation
    requirements....4

K

Kerberos SSO....9

L

log viewer....8

M

machine authentication....7
memory requirements....4
mobile OS....4
MSCHAP inner authentication....7
MSCHAPv2 inner authentication....7

multihomed network....12

N
NAT-T....9

O
OAC, feature comparison with Pulse....6
Odyssey Access Client
  compatible versions....5
  feature comparison with Pulse....6
  supported release....5
operating systems support....4
OPSWAT IMV....8, 11

P
PAP inner authentication....7
platform support
  gateways....3
  Windows....4

R
releases
  gateway support....3
route monitor....10
RSA SofToken....7

S
scan lists....6
scripts....11
Secure Virtual Workspace....10
security
  risk....4
session scripts....11
session time-outs....12
Shavlik IMV....8, 11
smart card....7
SofToken....7
software requirements....4
split tunneling
  strong host....12
split tunnelling
  comparison of NC and Pulse....10
SSL fallback....11
strong host model....12
support, technical *See* technical support
supported gateways....3
SVW....10

T
technical support
  contacting JTAC....ix
TKIP....6

V
versions
  gateway support....3
  Windows support....4
VPN....13

W
WEP....6
Windows
  strong host....12
  supported versions....4
wireless supplicant....5
wireless suppression
  IC Series gateway....6
With EAP-JSSO inner authentication....6
WPA/WPA2....6
WX Client, feature comparison with Pulse....14