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

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

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

About the Documentation ......................................................... xi
Documentation and Release Notes ........................................... xi
Supported Platforms ............................................................... xi
Documentation Conventions .................................................... xi
Documentation Feedback ....................................................... xiii
Requesting Technical Support ................................................ xiii
Self-Help Online Tools and Resources ................................... xiv
Opening a Case with JTAC ...................................................... xiv

### Part 1 Overview

#### Chapter 1 Junos Pulse .................................................. 3
Introducing Junos Pulse ......................................................... 3
Junos Pulse Client for Windows ............................................. 3
Pulse Client for Mac OS X ...................................................... 4
User Experience ................................................................. 6
Location Awareness ............................................................. 6
Session Migration ............................................................... 6
Centralized Pulse Configuration Management ...................... 6
Security Certificates ........................................................... 7
Compliance and Remediation ............................................... 8
Two Factor Authentication .................................................... 9
Junos Pulse Collaboration Suite Integration ...................... 9
Sign In Notifications ......................................................... 9
Automatic Software Updates .............................................. 9
Installation Requirements .................................................. 10
Junos Pulse Client Installation Overview ......................... 10
Application Acceleration Deployment Options .................. 13

#### Chapter 2 Client Software Feature Comparisons ................... 15
Comparing Odyssey Access Client and Junos Pulse ............ 15
Comparing Network Connect and Junos Pulse .................... 19
Pulse Split Tunneling .......................................................... 21

#### Chapter 3 Software Migration ........................................ 23
Migrating From Odyssey Access Client to Junos Pulse Client .... 23
Migrating From Network Connect to Junos Pulse ............... 25

#### Chapter 4 Session Migration ........................................... 27
Understanding Session Migration ....................................... 27
Session Migration Overview ............................................... 27
Session Migration and Session Timeout ......................... 29
<table>
<thead>
<tr>
<th>Page</th>
<th>Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>29</td>
<td>How Session Migration Works</td>
</tr>
<tr>
<td>30</td>
<td>Session Migration and Session Lifetime</td>
</tr>
<tr>
<td>30</td>
<td>Session Migration and Load Balancers</td>
</tr>
<tr>
<td>30</td>
<td>Authentication Server Support</td>
</tr>
<tr>
<td>31</td>
<td>Task Summary: Configuring Session Migration</td>
</tr>
<tr>
<td>33</td>
<td>Chapter 5 Junos Pulse Launcher</td>
</tr>
<tr>
<td>33</td>
<td>Junos Pulse Command-line Launcher</td>
</tr>
<tr>
<td>39</td>
<td>Part 2 Installation</td>
</tr>
<tr>
<td>39</td>
<td>Chapter 6 Junos Pulse Client</td>
</tr>
<tr>
<td>39</td>
<td>Installing Junos Pulse Client from the Web</td>
</tr>
<tr>
<td>40</td>
<td>Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File</td>
</tr>
<tr>
<td>41</td>
<td>Installing the Pulse Client Using Advanced Command-Line Options</td>
</tr>
<tr>
<td>41</td>
<td>Examples</td>
</tr>
<tr>
<td>43</td>
<td>Repairing a Pulse Installation on a Windows Endpoint</td>
</tr>
<tr>
<td>44</td>
<td>Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File</td>
</tr>
<tr>
<td>45</td>
<td>Installing the Pulse Client on OS X Endpoints Using Command-Line Options</td>
</tr>
<tr>
<td>49</td>
<td>Part 3 Configuration</td>
</tr>
<tr>
<td>49</td>
<td>Chapter 7 Junos Pulse</td>
</tr>
<tr>
<td>50</td>
<td>Adding a Pulse Configuration to a New Pulse Installation</td>
</tr>
<tr>
<td>55</td>
<td>Part 4 Administration</td>
</tr>
<tr>
<td>55</td>
<td>Chapter 8 Session Migration</td>
</tr>
<tr>
<td>55</td>
<td>Task Summary: Configuring Session Migration</td>
</tr>
<tr>
<td>56</td>
<td>Configuring Session Migration for the Pulse Client</td>
</tr>
<tr>
<td>56</td>
<td>Configuring an IF-MAP Federated Network for Session Migration</td>
</tr>
<tr>
<td>61</td>
<td>Part 5 Troubleshooting</td>
</tr>
<tr>
<td>61</td>
<td>Chapter 9 Junos Pulse Launcher</td>
</tr>
<tr>
<td>61</td>
<td>Launching Junos Pulse from the Pulse Server Web Portal</td>
</tr>
<tr>
<td>62</td>
<td>Usage Notes</td>
</tr>
<tr>
<td>63</td>
<td>Chapter 10 Junos Pulse Connections</td>
</tr>
<tr>
<td>63</td>
<td>Using jamCommand to Import Junos Pulse Connections</td>
</tr>
<tr>
<td>65</td>
<td>jamCommand Reference</td>
</tr>
<tr>
<td>69</td>
<td>Chapter 11 Junos Pulse Client Error Messages</td>
</tr>
<tr>
<td>69</td>
<td>Junos Pulse Client Error Messages Overview</td>
</tr>
<tr>
<td>70</td>
<td>Accessing Junos Pulse Client Error Messages on Mac OS X Endpoints</td>
</tr>
<tr>
<td>71</td>
<td>Chapter 12 Junos Pulse Client Log Files</td>
</tr>
<tr>
<td>71</td>
<td>Junos Pulse Client Log Files</td>
</tr>
<tr>
<td>74</td>
<td>Deleting the Junos Pulse Client Log Files</td>
</tr>
</tbody>
</table>
## Table of Contents

**Chapter 13**

- **Junos Pulse Client Interface** ........................................... 75
- **Junos Pulse Client Status Icons** ........................................ 75

**Part 6**

- **Index** ........................................................................... 79
# List of Figures

<table>
<thead>
<tr>
<th>Part</th>
<th>Chapter</th>
<th>Overview</th>
<th>Figure 1: Junos Pulse Client Interface</th>
<th>Figure 2: Junos Pulse for Mac Client Interface</th>
<th>Figure 3: Junos Pulse Client Interface (Windows Version)</th>
<th>Figure 4: Requirements for Pulse Session Migration</th>
<th>Figure 5: Junos Pulse Configuration Properties Defined on the Pulse Server</th>
<th>Figure 6: Junos Pulse Configuration Properties in a Preconfiguration File</th>
</tr>
</thead>
<tbody>
<tr>
<td>Part 1</td>
<td>Chapter 1</td>
<td>Junos Pulse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Part 3</td>
<td>Chapter 7</td>
<td>Junos Pulse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
List of Tables

About the Documentation ...................................................... xi
Table 1: Notice Icons ............................................................ xii
Table 2: Text and Syntax Conventions ................................. xii

Part 1 Overview

Chapter 2 Client Software Feature Comparisons ............................... 15
Table 3: Odyssey Access Client and Junos Pulse Feature Comparison .... 15
Table 4: Network Connect and Junos Pulse Feature Comparison ... 19
Table 5: Pulse Split Tunneling .................................................. 21

Chapter 5 Junos Pulse Launcher .................................................. 33
Table 6: Pulse Launcher Arguments ........................................... 34
Table 7: Pulse Launcher Return Codes ..................................... 35

Part 5 Troubleshooting

Chapter 12 Junos Pulse Client Log Files ....................................... 71
Table 8: Junos Pulse Event Log Messages ................................. 71

Chapter 13 Junos Pulse Client Interface ...................................... 75
Table 9: Pulse Icon States (Windows Tray and OS X Menu Bar) .......... 75
About the Documentation

- Documentation and Release Notes on page xi
- Supported Platforms on page xi
- Documentation Conventions on page xi
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiii

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at http://www.juniper.net/books.

Supported Platforms

For the features described in this document, the following platforms are supported:

- WXC Series
- SA Series
- MAG Series
- IC Series

Documentation Conventions

Table 1 on page xii defines notice icons used in this guide.
Table 1: Notice Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![info]</td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td>![caution]</td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td>![warning]</td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td>![laser]</td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
</tbody>
</table>

Table 2 on page xii defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold text like this</strong></td>
<td>Represents text that you type.</td>
<td>To enter configuration mode, type the <code>configure</code> command: user@host&gt; configure</td>
</tr>
<tr>
<td><strong>Fixed-width text like this</strong></td>
<td>Represents output that appears on the terminal screen.</td>
<td>user@host&gt; show chassis alarms No alarms currently active</td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>Introduces or emphasizes important new terms. Identifies guide names. Identifies RFC and Internet draft titles.</td>
<td>A policy term is a named structure that defines match conditions and actions. Junos OS CLI User Guide RFC 1997, BGP Communities Attribute</td>
</tr>
<tr>
<td><strong>Italic text like this</strong></td>
<td>Represents variables (options for which you substitute a value) in commands or configuration statements.</td>
<td>Configure the machine’s domain name: [edit] root@# set system domain-name domain-name</td>
</tr>
<tr>
<td><strong>Text like this</strong></td>
<td>Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.</td>
<td>To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level. The console port is labeled CONSOLE.</td>
</tr>
<tr>
<td><code>&lt; &gt;</code> (angle brackets)</td>
<td>Encloses optional keywords or variables.</td>
<td>stub &lt;default-metric metric&gt;;</td>
</tr>
</tbody>
</table>
Table 2: Text and Syntax Conventions (continued)

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
</table>
| | (pipe symbol)   | Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity. | broadcast | multicast  
|                  | (string1 | string2 | string3)                          | rsvp [ # Required for dynamic MPLS only  |
| # (pound sign)   | Indicates a comment specified on the same line as the configuration statement to which it applies. | community name members [ community-ids ]                                   |
| [ ] (square brackets) | Encloses a variable for which you can substitute one or more values. | [edit] routing-options { static { route default { nexthop address; retain;  
|                  |                                                           } } }                                                       |
| Indention and braces ( { } ) | Identifies a level in the configuration hierarchy. | [edit] routing-options { static { route default { nexthop address; retain;  
|                  |                                                           } } }                                                       |
| : (semicolon)    | Identifies a leaf statement at a configuration hierarchy level. | [edit] routing-options { static { route default { nexthop address; retain;  
|                  |                                                           } } }                                                       |
| GUI Conventions   |                                                                           |                                                                           |
| **Bold text like this** | Represents graphical user interface (GUI) items you click or select. | • In the Logical Interfaces box, select All Interfaces.  
|                  |                                                                           | • To cancel the configuration, click Cancel.  |
| > (bold right angle bracket) | Separates levels in a hierarchy of menu selections. | In the configuration editor hierarchy, select Protocols>Ospf. |

**Documentation Feedback**

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

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

**Requesting Technical Support**

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

- **Product warranties**—For product warranty information, visit [http://www.juniper.net/support/warranty/](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/](http://www.juniper.net/customers/support/)
- **Search for known bugs**: [http://www2.juniper.net/kb/](http://www2.juniper.net/kb/)
- **Find product documentation**: [http://www.juniper.net/techpubs/](http://www.juniper.net/techpubs/)
- **Find solutions and answer questions using our Knowledge Base**: [http://kb.juniper.net/](http://kb.juniper.net/)
- **Download the latest versions of software and review release notes**: [http://www.juniper.net/customers/csc/software/](http://www.juniper.net/customers/csc/software/)
- **Search technical bulletins for relevant hardware and software notifications**: [https://www.juniper.net/alerts/](https://www.juniper.net/alerts/)
- **Join and participate in the Juniper Networks Community Forum**: [http://www.juniper.net/company/communities/](http://www.juniper.net/company/communities/)
- **Open a case online in the CSC Case Management tool**: [http://www.juniper.net/cm/](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/](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/](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](http://www.juniper.net/support/requesting-support.html).
PART 1

Overview

- Junos Pulse on page 3
- Client Software Feature Comparisons on page 15
- Software Migration on page 23
- Session Migration on page 27
- Junos Pulse Launcher on page 33
CHAPTER 1

Junos Pulse

• Introducing Junos Pulse on page 3
• Installation Requirements on page 10
• Junos Pulse Client Installation Overview on page 10
• Application Acceleration Deployment Options on page 13

Introducing Junos Pulse

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

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

Users of mobile devices (smart phones) can install the Pulse mobile device app from the respective app stores for secure connectivity to Junos Pulse Secure Access Service. Mobile device users can also enable an optional security component, the Junos Pulse Mobile Security Suite. Windows 8.1 (Pro and RT) introduced a Junos Pulse VPN client as part of the operating system.

Junos Pulse Client for Windows

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

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

Figure 1: Junos Pulse Client Interface

Pulse Client for Mac OS X

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

- Connections to Junos Pulse Access Control Service
- Connections to Junos Pulse Secure Access Service
  
  Pulse clients connect to the Pulse Secure Access Service in SSL fallback mode.

- Host Checker

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

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

From the user perspective, Junos Pulse presents a clean, uncomplicated interface. The user can enter credentials, select a realm, save settings, and accept or reject the server certificate. When you configure the client, you can specify whether to permit end users to modify settings, such as by adding connections.

NOTE: If your Pulse environment uses Security Assertion Markup Language (SAML) for a Single Sign-on (SSO) authentication environment, the Pulse user sees a credential dialog box that is served (HTTPS) from the Pulse server instead of the local Pulse client credential dialog box. The sign-in page is defined as part of the sign-in policy on the Pulse server and the Pulse client embeds the sign-in page within a Pulse client dialog box.

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

Location Awareness

The location awareness feature enables you to define connections that are activated automatically based on the location of the endpoint. Pulse determines the location of the endpoint by evaluating rules that you define. For example, you can define rules to enable Junos Pulse to automatically establish a secure tunnel to the corporate network through Junos Pulse Secure Access Service when the user is at home, and to establish a Junos Pulse Access Control Service connection when the user is in the office and connected to the corporate network over the LAN. Location awareness rules are based on the client's IP address and network interface information. Split tunneling must be enabled for location awareness.

Session Migration

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

Centralized Pulse Configuration Management

Centralized configuration management is a key feature of Junos Pulse. Pulse connection sets (the configurations that define how and when a Pulse client connects), are bound to a particular Pulse server. The binding server is the one that provides the initial Pulse configuration to the Pulse client. For example, if you create a Pulse connection set on ServerA, and then distribute those connections to endpoints, those clients are bound to ServerA.
A bound client is managed by its particular Pulse server. The Pulse administrator defines the Junos Pulse connections and software components that are installed on the endpoint. When the Pulse client connects to the Pulse server that is managing it, the server automatically provisions configuration and software component updates. The administrator can permit the user to add, remove, and modify connections. The administrator can also allow dynamic connections (connections that are added by Pulse servers when the user logs into the server using a browser). A dynamic connection enables a bound client to add connections from Pulse servers other than the one the client is bound to. Dynamic connections are created as manual rather than automatic connections, which means that they are run only when the user initiates the connection or the user browses to a Pulse server and launches Pulse from the server’s Web interface. Dynamic connections create the connection with the minimum configuration required to make the connection, which means that the URL used to install or launch Pulse from the Pulse server’s Web interface is used as the Connection URL and connection name. Binding Junos Pulse clients to a particular server ensures that the client does not receive different configurations when it accesses other Pulse servers. 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 Secure Access or Pulse Access control server that has the automatic upgrade option enabled. (SRX gateways do not support Pulse software updates.)

**NOTE:** A Junos Pulse client can be bound to only one Pulse server connection set at a time. The Junos Pulse client can receive updates and changes to that bound connection set from other Pulse servers only if the connection set is exported from the Pulse server and then imported to another Pulse server.

A Pulse client does not need to be bound to a Pulse server. An unbound client is managed by its user. If the Junos Pulse client software is installed without any connections, the user must add connections manually. Dynamic connections can be added by visiting the Web portals of Pulse servers. An unbound client does not accept configuration updates from any Pulse server.

“Adding a Pulse Configuration to a New Pulse Installation” on page 50 explains the binding process in more detail.

**Security Certificates**

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

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

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

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

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

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

- Virus signature monitoring
  
  You can configure Host Checker to monitor and verify that the virus signatures, operating systems, software versions, and patches installed on client computers are up to date. You can configure automatic remediation for those endpoints that do not meet the specified criteria.

- Patch management information monitoring and patch deployment
  
  You can configure Host Checker policies that check for Windows endpoints’ operating system service pack, software version, or desktop application patch version compliance.

- Patch remediation options
  
  Pulse and Host Checker support endpoint remediation through Microsoft System Management Server or Microsoft System Center Configuration Manager (SMS/SCCM) or through the Shavlik patch deployment engine. With SMS/SCCM, Pulse triggers a preinstalled SMS/SCCM client to get patches from a pre-configured SMS/SCCM server. Shavlik uses a patch deployment engine that Pulse downloads to any endpoint that needs remediation. Shavlik provides patches directly from Microsoft and other vendors’ Web sites. (Internet connectivity is needed for Shavlik remediation.) Shavlik patch management is an optional feature. A separate license is required for Shavlik patch monitoring and deployment.

- Endpoint configuration
  
  You can configure custom rules to allow Host Checker to check for third-party applications, files, process, ports, registry keys, and custom DLLs.
Pulse mobile clients support a set of Host Checker functions that vary from one OS to the next. For complete information on Host Checker for mobile clients, see *Implementing Host Checker Policies for Junos Pulse for iOS Devices*, *Implementing Host Checker Policies for Junos Pulse for Android Clients*, and *Junos Pulse Mobile Security Overview*.

## Two Factor Authentication

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

## Junos Pulse Collaboration Suite Integration

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

## Sign In Notifications

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

## Automatic Software Updates

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

---

**NOTE:** The automatic update feature is supported on Pulse Secure Access and Pulse Access Control servers only. SRX gateways do not support automatic Pulse software updates.

---

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

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

This section describes how to deploy Pulse for Windows and Pulse for Mac OS X client software from Pulse Access Control Service and Pulse Secure Access Service platforms. Pulse Application Acceleration Service supports deployment of App Acceleration connections only.

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

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

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

- **Web install**—With a Web install (also called a server-based installation), users log in to the Pulse server’s Web portal and are assigned to a role that supports a Pulse installation. When a user clicks the link to run Junos Pulse, the default installation program adds Pulse to the endpoint and adds the default component set and the default connection set. If you do not make any changes to the defaults, the endpoint receives a Pulse installation in which a connection to the Pulse server is set to connect automatically. You can edit the default connection set to add connections of other Pulse servers and change the default options.
NOTE: A Web install requires that the user have Java installed and enabled for an installation through the Firefox browser or ActiveX enabled for an installation through Internet Explorer. If the browser does not meet this requirement, the user receives a descriptive message at the beginning of the installation process.

NOTE: A Web install is not compatible with the Pulse rebranding tool, BrandPackager.

- **Preconfigured installer**—Create the connections that an endpoint needs for connectivity and services, download the settings file (.jnprpreconfig), and download default Pulse installation program. For Windows endpoints you run the Pulse installation program by using an msiexec command with the settings file as an option. For OS X endpoints, you run the default installer and then import the .jnprpreconfig file using a separate command.

- **Default installer**—You can download the default Pulse installation program and distribute it to endpoints using your local organization’s standard software distribution method (such as Microsoft SMS/SCCM). The Junos Pulse client software is installed with all components and no connections. After users install a default Pulse installation, they can add new connections manually through the Pulse client user interface or by using a browser to access a Pulse server’s Web portal. For the latter, the Pulse server’s dynamic connection is downloaded automatically and the new connection is added to the Pulse client’s connections list. Dynamic connections are created as manual rather than automatic connections, which means that they are run only when the user initiates the connection or the user browses to a Pulse Server and launches Pulse from the server’s Web interface.

If the Windows endpoints in your environment do not have admin privileges, you can use the Juniper Installer Service program, which is available on the admin console System Maintenance Installers page. The Juniper Installer Service allows users to download, install, upgrade, and run client applications without administrator privileges. In order to perform tasks that require administrator privileges, the Juniper Installer Service runs under the client’s Local System account (a powerful account with full access to the system) and registers itself with Windows’ Service Control Manager (SCM). An Active-X control or a Java applet running inside the user’s Web browser communicates the details of the installation processes to be performed through a secure channel between the Pulse server and the client system.

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

- When installing a Juniper client application on a user’s Windows system, the Juniper Installer Service deploys two files on the client machine:
  - JuniperSetupSPIControl.ocx
  - AccessServiceComponent.exe
The device auto-starts this service when installing, and, then stops and removes it when uninstalling.

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

- You should ensure that the Microsoft Windows Installer exists on the client system prior to installing the Juniper Installer Service.

- Your end-users’ client systems must contain either a valid and enabled Java Runtime Engine (JRE) or a current SA Series Appliance ActiveX control. If the client systems do not contain either of these software components, the users will be unable to connect to the gateway. If there is no JRE on your end-users’ client systems, you should download an appropriate installer package from Maintenance > System > Installers. The service appears in the Windows Services (Local) list as Neoteris Setup Service. The service starts automatically on install and during client system start up.

Related Documentation:
- Adding a Pulse Configuration to a New Pulse Installation on page 50
- Installing Junos Pulse Client from the Web on page 39
- Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 40
- Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 44
### Application Acceleration Deployment Options

The Junos Pulse client (Windows and Mac) accelerates traffic between the client system and a network's Junos Pulse Application Acceleration Service. Pulse Application Acceleration Service and Pulse clients discover each other automatically and begin accelerating traffic without user intervention.

**NOTE:** Junos Pulse for Apple iOS and Junos Pulse for Google Android support application acceleration only when configured to operate with Riverbed Steelhead WAN optimization service.

Junos Pulse Application Acceleration Service supports the following deployment options:

- The administrator can enable Pulse downloads and configure Pulse client configuration, and then users can download the Junos Pulse client from JWOS 6.1 or higher. When the license is present, a Junos Pulse selection appears in the task bar of the Web interface for the Pulse server.

- The Junos Pulse client can be downloaded and installed automatically when users access Junos Pulse Secure Access Service. On SA Series SSL VPN systems running software Release 7.0 or later, you can configure an App Acceleration connection for Application Acceleration Service and install it along with the Pulse client software. You can also deploy an App Acceleration connection from Junos Pulse Access Control Service. Although Pulse Access Control Service is for LAN access where WAN application acceleration is not used, Pulse Access Control Service can deploy any type of Pulse connection, which allows flexibility in how you deploy Pulse to users.

**Related Documentation**

- [Junos Pulse for Mobile Devices Overview](#)
- [Understanding Session Migration on page 27](#)

---

Copyright © 2013, Juniper Networks, Inc.
Client Software Feature Comparisons

- Comparing Odyssey Access Client and Junos Pulse on page 15
- Comparing Network Connect and Junos Pulse on page 19

Comparing Odyssey Access Client and Junos Pulse

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

Table 3 on page 15 compares the features in Odyssey Access Client (OAC) and Junos Pulse to help you transition to Pulse. For detailed information about supported platforms and installation requirements, see the Junos Pulse Supported Platforms Guide, which is available at http://www.juniper.net/support/products/pulse.

Table 3: Odyssey Access Client and Junos Pulse Feature Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos Pulse Release 5.0 OSX</th>
<th>Junos Pulse Release 5.0 Win</th>
<th>Odyssey Access Client</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wired/Wireless 802.1X Features</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wired 802.1X support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>(with Microsoft Windows supplicant)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto scan lists</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>(with Microsoft Windows supplicant)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless suppression</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>(with Microsoft Windows supplicant)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 3: Odyssey Access Client and Junos Pulse Feature Comparison (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Odyssey Access Client</th>
<th>Junos Pulse Release 5.0 OSX</th>
<th>Junos Pulse Release 5.0 Win</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support for Network Provider (scraping passwords, listing)</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Association Mode and Encryption Methods</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Association mode support (for open, shared, WPA/WPA2)</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Encryption (for WEP, TKIP, AES, WEP with preconfigured key, WPA/WPA2 with pre-shared key)</td>
<td>Yes</td>
<td>(with Microsoft Windows supplicant)</td>
<td></td>
</tr>
<tr>
<td>EAP Methods</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EAP-TLS outer authentication</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>EAP-TTLS outer authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>• With EAP-JUAC inner authentication</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• With EAP-MSCHAPv2 inner authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• With EAP-GTC inner authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• With EAP-MD5 inner authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• With PAP inner authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• With CHAP inner authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• With MSCHAP inner authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• With MSCHAPv2 inner authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EAP-PEAP outer authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• With EAP-JUAC inner authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• With EAP-DD5 inner authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• With EAP-GTC inner authentication</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication Methods</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prompt for user name and password</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>Odyssey Access Client</td>
<td>Junos Pulse Release 5.0 OSX</td>
<td>Junos Pulse Release 5.0 Win</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------------------------</td>
<td>-----------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Certificate support (automatic, specific)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Certificates from smart card reader</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Soft token support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Machine login support</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Machine authentication followed by user authentication</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Credential provider on 32- and 64-bit Windows</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Pre-desktop login</td>
<td>N/A</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable UAC Layer 2 connection</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configurable connection association modes</td>
<td>Yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIPS compliance</td>
<td></td>
<td>Pulse SSL-VPN mode of SA connection is fully FIPS compliant.</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pulse server certificate verification and private key signing is FIPS compliant.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pulse IPSec is FIPS compatible.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pulse wireless is FIPS compatible. (WPA encryption is controlled by Windows.)</td>
<td></td>
</tr>
<tr>
<td>Installation and Upgrade Methods</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto-upgrade</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Web-based installation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Standalone installation</td>
<td>Yes (.dmg)</td>
<td>Yes (.msi)</td>
<td>Yes</td>
</tr>
<tr>
<td>Upgrade/coordinate with previous versions</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manual Uninstall</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 3: Odyssey Access Client and Junos Pulse Feature Comparison (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Odyssey Access Client</th>
<th>Junos Pulse Release 5.0 OSX</th>
<th>Junos Pulse Release 5.0 Win</th>
<th>Junos Pulse Release 5.0 Win</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser based installation and upgrades</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Diagnostics and Logging</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPsec diagnostics and configuration</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Host Enforcer</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Log viewer</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Logging and Diagnostics</td>
<td>Yes</td>
<td>Yes</td>
<td>Set debug level</td>
<td>Set debug level, set file size limits</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>In addition to the Pulse log files, Pulse writes events to the Windows application event log. (Windows Vista and Windows 7 systems only.)</td>
<td></td>
</tr>
<tr>
<td>Other Features</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OPSWAT IMV support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Shavlik IMV support (patch assessment)</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Automatic patch remediation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>via SMS/SCCM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>via Shavlik or SMS/SCCM</td>
</tr>
<tr>
<td>Host Checker support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Enhanced Endpoint Security support (Windows OS only)</td>
<td>N/A</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>IPsec tunneling to Policy Enforcement Points with NAT-T</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Access service and plug-ins</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Block 3rd party EAP messages</td>
<td>N/A</td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Layer 3 authentication</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Server-based pre-configuration of realm/role</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Extend session duration</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>IC cardinality</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 3: Odyssey Access Client and Junos Pulse Feature Comparison (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Odyssey Access Client</th>
<th>Junos Pulse Release 5.0 OSX</th>
<th>Junos Pulse Release 5.0 Win</th>
<th>Related Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client-site management of clustered Pulse servers</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Comparing Network Connect and Junos Pulse on page 19</td>
</tr>
<tr>
<td>Kerberos SSO</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Initial configuration (intervention-less client provisioning)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Dynamically configurable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

Comparing Network Connect and Junos Pulse

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

Table 4 on page 19 compares the features of NC and Pulse to help you transition from NC to Junos Pulse. For detailed information about supported platforms and installation requirements, see the Junos Pulse Supported Platforms Guide, which is available at http://www.juniper.net/support/products/pulse.

Table 4: Network Connect and Junos Pulse Feature Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>Network Connect Release 6.3</th>
<th>Junos Pulse Release 5.0 Mac</th>
<th>Junos Pulse Release 5.0 Win</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Support</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internet Explorer</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Apple Safari</td>
<td></td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Google Chrome</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Split Tunneling Options

| Disable split tunneling without route monitor | Yes | Yes |
| Disable split tunneling with route monitor     | Yes | Yes |
Table 4: Network Connect and Junos Pulse Feature Comparison (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Junos Pulse Release 5.0 Mac</th>
<th>Junos Pulse Release 5.0 Win</th>
<th>Network Connect Release 6.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable split tunneling but allow directly connected local subnet access</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Enable split tunneling with route monitors</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable split tunneling without route monitors</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable split tunneling with allowed access to local subnet</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Disable split tunneling with allowed access to local subnet</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Client Launch Options</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Command line launcher</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Log out on connect</td>
<td>n/a</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Launch as a standalone client</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Launch from browser</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>GINA and Credential Provider support</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Transport Mode</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SSL fallback mode</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**NOTE:** If ESP is not available, the connection uses SSL. Once a connection switches to SSL, it does not go back to ESP until the connection is restarted.

| ESP | Yes | Yes | Yes |
| Other Features | | | |
| OPSWAT IMV support | Yes | Yes | Yes |
| Shavlik IMV support (patch assessment) | Yes | | Yes |
| Patch automatic remediation | Yes | | via Shavlik or SMS/SCCM |
| Host Checker support | Yes | Yes | Yes |
### Table 4: Network Connect and Junos Pulse Feature Comparison (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Network Connect Release 6.3</th>
<th>Junos Pulse Release 5.0 Mac</th>
<th>Junos Pulse Release 5.0 Win</th>
<th>Feature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced Endpoint Security support (Windows OS only)</td>
<td>Yes</td>
<td>Yes</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Run configured scripts when client connects/disconnects</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Modify DNS server search order based on server configuration</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Reconnect automatically if connection breaks</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Dial-up adapter support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>3G wireless adapter support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Max/Idle Session Time-outs</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Logging</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log to file</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>Upload log</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Certifications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FIPS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pulse SSL-VPN mode of SA connection is fully FIPS compliant.</td>
<td></td>
<td></td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Pulse server certificate verification and private key signing is FIPS compliant.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pulse IPSec is FIPS compatible.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pulse wireless is FIPS compatible. (WPA encryption is controlled by Windows.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Pulse Split Tunneling

Table 5 on page 21 lists the Network Connect split tunneling options and shows how they map to Pulse split tunneling options.

### Table 5: Pulse Split Tunneling

<table>
<thead>
<tr>
<th>NC Split Tunnel Option</th>
<th>Pulse Split Tunnel Setting</th>
<th>Route Override State</th>
<th>Route Monitor State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable split tunnel</td>
<td>Disabled</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Table 5: Pulse Split Tunneling (continued)

<table>
<thead>
<tr>
<th>NC Split Tunnel Option</th>
<th>Pulse Split Tunnel Setting</th>
<th>Route Override State</th>
<th>Route Monitor State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable split tunneling but allow local access</td>
<td>Disabled</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Enable split tunnel</td>
<td>Enable</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Enable split tunnel with route monitor</td>
<td>Enable</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Enable split tunnel, allow local access</td>
<td>Enable</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

Related Documentation
- Comparing Odyssey Access Client and Junos Pulse on page 15
CHAPTER 3
Software Migration

- Migrating From Odyssey Access Client to Junos Pulse Client on page 23
- Migrating From Network Connect to Junos Pulse on page 25

Migrating From Odyssey Access Client to Junos Pulse Client

Odyssey Access Client® (OAC) is 802.1X network access client software that supports the Extensible Authentication Protocol (EAP) for secure wireless LAN access. Together with an 802.1X-compatible authentication server, OAC secures WLAN communications. OAC also serves as a client for enterprises that are deploying identity-based (wired 802.1X) networking. OAC provides wireless access to enterprise networks, home Wi-Fi networks, and public hotspots.

Junos® Pulse is an extensible multiservice network client that supports integrated connectivity, location-aware network access, application acceleration, security, and selected third-party services. Junos Pulse simplifies the user experience by letting the network administrator configure, deploy, and control the Pulse client software and the Pulse connection configurations that reside on the endpoint. In addition to 802.1X authentication, Pulse can provide Layer 3 access and other services.

Like OAC, Pulse client software is bundled with Junos Pulse Access Control Service software. However, there are significant differences between OAC and Pulse and you should be aware of these differences when you plan a migration from OAC to Pulse. The following list includes planning considerations and best-practices for a migration project. See the related topics list for details about the Pulse configuration tasks.

- The 802.1X communication protocol that you use with OAC might need to be changed to support Pulse. OAC supports the full range of 802.1X protocols; Pulse supports only EAP-TTLS/EAP-JUAC. See “Comparing Odyssey Access Client and Junos Pulse” on page 15, which lists the 802.1X protocols supported by OAC and Pulse.
- One common migration practice is to create new sign-in policies, user realms, and user roles for Junos Pulse, and then control the cut-over to Pulse by enabling Pulse sign-in policies and disabling OAC sign-in policies. The new policies, realms, and roles can be clones of the existing OAC policies, realms, and roles as a starting point. However, Pulse has more robust connection decision capabilities so you will probably want to edit your Pulse roles to take advantage of the Pulse capabilities. For example, you can replace both OAC and Network Connect with Pulse and use one client for authenticated LAN access and secure SSL VPN access. Location awareness rules allow Pulse to
detect the network environment and choose a network connection based on current location.

- How many OAC configuration do you use? You need a pulse configuration for each of the OAC configurations you currently use. A Pulse access configuration is called a connection. It comprises properties that define how, when, and where a connection is established with a Pulse gateway. When you create the Pulse connections that you distribute to Pulse clients, you configure how the connection can be established. Pulse connections support machine authentication and credential provider authentication. Figure 3 on page 24 shows a Pulse Windows client that includes multiple connections.

Figure 3: Junos Pulse Client Interface (Windows Version)

- Odyssey Access Client is a wireless supplicant. Pulse, by design, is not a wireless supplicant. Pulse uses the underlying wireless supplicant on the endpoint, which is typically provided by the endpoint’s OS X or Windows operating system. When you migrate to Pulse and uninstall OAC, you remove the OAC wireless supplicant and the endpoint falls back to using wireless connectivity provided by the OS. You define 802.1X authentication connections for the Pulse client to enable authenticated 802.1X connectivity in the enterprise network. Any custom network configurations that users added to their local OAC configuration are lost when OAC is removed. For example, if a user added connection information to connect to a home wireless network, the user will need to redefine that connection in the endpoint’s wireless supplicant. A best practice is to mention this needed configuration to users as part of the Pulse roll-out. In OAC, network auto-scan lists are defined on the client. With Pulse, you can define an auto-scan list as part of an 802.1X connection that is pushed to the Pulse client.

- Do you use wireless suppression in your OAC environment? Wireless suppression disables wireless connections as long as the client has a wired network connection.
You enable wireless suppression as part of a Pulse connection set. Pulse connection set properties define the decision process that Pulse uses to establish network connections.

- If you are using OAC FIPS Edition, you need to deploy Pulse 5.0 or later to support the same level of FIPS compliance that is supported by OAC.

- Do you allow users to modify configuration settings after you deploy them in your OAC environment? When you create a Pulse connection, you can define whether users can override the connection decision that has been defined by the Pulse administrator as part of the Pulse connection. You can also disable the user’s ability to create new connections. Connections created by users are manual connections, that is, the connection is not tried unless the user opens Pulse and selects it.

- Do you allow OAC users to add, remove, or modify trusted servers and certificates? Pulse does not expose this functionality to users. Pulse handles certificates in the same fashion as a browser. When you define a Pulse connection you can allow users to choose to accept an unverified certificate, which allows users to connect to servers that use a self-signed certificate.

### Related Documentation

- Comparing Odyssey Access Client and Junos Pulse on page 15
- Client Connection Set Options for Junos Pulse Access Control Service
- Machine Authentication for Pulse Access Control Service Overview
- Configuring Location Awareness Rules for Junos Pulse
- Machine and User Authentication Through a Pulse Connection for Pulse Access Control Service
- Remote Desktop Protocol Compatibility with Junos Pulse 802.1X Machine Authentication Connection
- Junos Pulse Client Installation Overview on page 10

### Migrating From Network Connect to Junos Pulse

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

**NOTE:** The Pulse installation program checks for NC. If the installation program finds NC Release 6.3 or later, the Pulse installation proceeds. If NC is not at least Release 6.3, the program displays a message telling the user to upgrade NC. For detailed information about supported platforms and installation requirements, see the Junos Pulse Supported Platforms Guide, which is available at [http://www.juniper.net/support/products/pulse](http://www.juniper.net/support/products/pulse)

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

- Comparing Odyssey Access Client and Junos Pulse on page 15
- Comparing Network Connect and Junos Pulse on page 19
CHAPTER 4

Session Migration

- Understanding Session Migration on page 27
- Task Summary: Configuring Session Migration on page 31

Understanding Session Migration

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

- Session Migration Overview on page 27
- Session Migration and Session Timeout on page 29
- How Session Migration Works on page 29
- Session Migration and Session Lifetime on page 30
- Session Migration and Load Balancers on page 30
- Authentication Server Support on page 30

Session Migration Overview

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

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

The servers must be in the same authentication group. Authentication groups are configured through authentication realms. An authentication group is a string that you define for common usage. You can use authentication groups to group together realms with similar authentication methods. Such as, one authentication group for SecurID authentication, another authentication group for AD. A single gateway can belong to more than one authentication group, with a different authentication group per realm.
The Pulse server to which a user authenticates publishes session information to the IF-MAP server. Other IF-MAP clients in the federated network can use the information to permit access without additional authentication to users.

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

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

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

“Session Migration” on page 27 illustrates the task flow for enabling session migration for Pulse.
Figure 4: Requirements for Pulse Session Migration

Session Migration and Session Timeout

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

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

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

How Session Migration Works

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

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

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

Session Migration and Session Lifetime

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

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

Session Migration and Load Balancers

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

Authentication Server Support

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

The following list provides a summary of authentication server support:

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

Siteminder—No support for migrating sessions because Siteminder SSO is used instead.

Certificate—No support for migrating sessions because sessions are authenticated using certificates.

SAML—No support for migrating sessions because SAML SSO is used instead.

---

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

---

**Related Documentation**
- Configuring Session Migration for the Pulse Client on page 56
- Task Summary: Configuring Session Migration on page 31

---

**Task Summary: Configuring Session Migration**

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

1. Configure location awareness rules within a client connection set to specify locations included in the scope of session migration for users. For example, configure location awareness rules for a corporate Pulse Access Control server connection and a Pulse Secure Access server connection.

2. Configure an IF-MAP federated network, with the applicable Pulse Access Control servers and SA Series appliances as IF-MAP Federation clients of the same IF-MAP Federation server.

3. Ensure that user entries are configured on the authentication server for each gateway.

4. Ensure that user roles are configured for all users on each gateway.

5. Define a remediation role with no Host Checker policies to allow user sessions to be maintained when an endpoint is sleeping or hibernating.

6. Configure role-mapping rules that permit users to access resources on each gateway.

7. Enable and configure session migration from the User Realms page of the admin console.

8. Distribute the Pulse client to users.

---

**Related Documentation**
- Understanding Session Migration on page 27
- Configuring Session Migration for the Pulse Client on page 56
- Understanding Federated Deployments
CHAPTER 5

Junos Pulse Launcher

- Junos Pulse Command-line Launcher on page 33

Junos Pulse Command-line Launcher

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

Pulse Launcher Usage Notes:

- Pulse Launcher runs on Windows 32-bit and 64-bit endpoints.
- The Pulse Launcher program, pulselauncher.exe, is installed as part of a Pulse client installation in Program Files\Common Files\Juniper Networks\Integration or Program Files (x86)\Common Files\Juniper Networks\Integration.
- Pulse Launcher works only for the SSL VPN or UAC connection type. Pulse Launcher does not support the SRX or UAC (802.1X) connection types.
- The Pulse Launcher program does not support the role mapping option that prompts a user to select from a list of assigned roles. If you use the Pulse Launcher and more than one role can be assigned to a user, you must configure the role mapping settings for the realm to merge settings for all assigned roles. If the realm settings require the user to select a role, the Pulse Launcher command fails and exits with return code 2.
- Pulse Launcher does not support secondary authentication.

To use the Pulse Launcher program:

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

Table 7 on page 35 lists the Pulse Launcher return codes.
The following command shows the complete pulselauncher.exe command syntax:

```
```

### Table 6: Pulse Launcher Arguments

<table>
<thead>
<tr>
<th>Argument</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>-version</td>
<td>Display the Pulse Launcher version information, then exit.</td>
</tr>
<tr>
<td>-help</td>
<td>Display available arguments information.</td>
</tr>
<tr>
<td>-stop</td>
<td>Stop Pulse and disconnect all active connections.</td>
</tr>
<tr>
<td>-url &lt;url&gt;</td>
<td>Specify the Pulse server URL.</td>
</tr>
<tr>
<td>-u &lt;user&gt;</td>
<td>Specify the username.</td>
</tr>
<tr>
<td>-p &lt;password&gt;</td>
<td>Specify the password for authentication.</td>
</tr>
<tr>
<td>-r &lt;realm&gt;</td>
<td>Specify the realm on the Pulse server.</td>
</tr>
<tr>
<td>-d &lt;DSID&gt;</td>
<td>Passes a cookie to Pulse Launcher for a specified Pulse server from another authentication mechanism when Pulse Launcher starts. When you use the -d argument, you must also specify the -url argument to specify the Pulse server.</td>
</tr>
<tr>
<td>-cert &lt;client certificate&gt;</td>
<td>Specify the certificate to use for user authentication. For &lt;client certificate&gt; use the string specified in the Issued To field of the certificate. When using the -cert argument, you must also specify the -url and -r &lt;realm&gt; arguments.</td>
</tr>
<tr>
<td></td>
<td>To use certificate authentication with the Pulse Launcher program, you must first configure the Pulse server to allow the user to sign in via user certificate authentication. You must also configure a trusted client CA on the Pulse server and install the corresponding client-side certificate in the Web browsers of end-users before running the Pulse Launcher. If the certificate is invalid, the Pulse Launcher displays an error message on the command line and logs a message in the log file.</td>
</tr>
<tr>
<td></td>
<td><strong>NOTE:</strong> If Pulse is launched through a browser, the browser handles certificate verification. If Pulse is launched through an application on Windows, the application handles certificate verification. If Pulse is launched through the Pulse Launcher on Windows, Pulse Launcher handles the expired or revoked client certificates.</td>
</tr>
<tr>
<td>-signout &lt;url&gt;</td>
<td>Signout disconnects and signs out from a specific server. Suspend puts an active connection in the suspend state without removing the session information from the server. Resume restores a suspended connection. Pulse can have multiple simultaneous connections so the -url argument is required when you use -signout, -suspend, or -resume.</td>
</tr>
<tr>
<td>-suspend &lt;url&gt;</td>
<td>The amount of time allowed for the connection to take place before the attempt fails. Min = 45 (default), Max = 600.</td>
</tr>
</tbody>
</table>
The following table lists the possible return codes pulselauncher.exe returns when it exits.

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-1</td>
<td>Pulse is not running.</td>
</tr>
<tr>
<td>0</td>
<td>Success.</td>
</tr>
<tr>
<td>1</td>
<td>A parameter is invalid.</td>
</tr>
<tr>
<td>2</td>
<td>Connection has failed or Pulse is unable to connect to the specified gateway.</td>
</tr>
<tr>
<td>3</td>
<td>Connection established with error.</td>
</tr>
<tr>
<td>4</td>
<td>Connection does not exist. Example: the command attempts to sign out from a server that has not been added on the Pulse UI.</td>
</tr>
<tr>
<td>5</td>
<td>User cancelled connection.</td>
</tr>
<tr>
<td>6</td>
<td>Client certificate error.</td>
</tr>
<tr>
<td>7</td>
<td>Timeout error.</td>
</tr>
<tr>
<td>8</td>
<td>No user connection allowed from Pulse UI.</td>
</tr>
<tr>
<td>9</td>
<td>No policy override from Pulse UI.</td>
</tr>
<tr>
<td>25</td>
<td>Invalid action for current connection state. This error code would occur if you tried to suspend or resume a connection that was disconnected.</td>
</tr>
<tr>
<td>100</td>
<td>General error.</td>
</tr>
</tbody>
</table>

Examples

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

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

The following Pulse Launcher example shows a certificate authentication:

```
tpulselauncher return code: 0
```

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

```
```
pulselauncher return code: 0

Related Documentation

• Using jamCommand to Import Junos Pulse Connections on page 63
• jamCommand Reference on page 65
PART 2

Installation

- Junos Pulse Client on page 39
CHAPTER 6

Junos Pulse Client

- Installing Junos Pulse Client from the Web on page 39
- Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 40
- Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 44

Installing Junos Pulse Client from the Web

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

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

The default Junos Pulse installation settings include minimal components, which includes the Host Checker component, and a connection to the Pulse server. If you want a Web install that has customized settings, you can do any of the following:

- Edit the default connection set and add new connections. The default installer uses the default component set which includes the default connection set.
- Create a new connection set and edit the default component set to include the new connection set.
- Edit the role to specify a component set that includes the connections you want for the default installation.
NOTE: A Pulse installation causes a restart of active network connections on a Windows endpoint. When a user initiates a Pulse installation through a WAN connection to the Web interface of a Pulse server, the user might need to log in to their service provider again to reestablish network connectivity. Users need to be aware of this issue before they begin the installation.

Related Documentation
- Junos Pulse Client Installation Overview on page 10
- Launching Junos Pulse from the Pulse Server Web Portal on page 61

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

The following procedures apply to Windows installations only.

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

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

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

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

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

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

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

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

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

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

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

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

---

### Installing the Pulse Client Using Advanced Command-Line Options

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

**Usage Notes:**

- The preconfigured installer installs all Pulse components unless you specify the specific components you want using ADDLOCAL options. If you use one or more ADDLOCAL options, the preconfigured installer installs only the components specified by ADDLOCAL. A preconfigured installer ignores the component set you select when you create the preconfiguration file.

- When you use ADDLOCAL options, be sure that your msiexec command specifies all the components required for your connections. For example, if the connection requires 802.1X connectivity for a connection to Pulse Access Control Service, be sure to include both the 802.1X component and the Pulse Access Control Service component (ADDLOCAL=PulseUAC,Pulse8021x).

- When you run msiexec, you should append /qn or /qb (msiexec options) to the command line to suppress the installation program user interface. For example, the user interface lets the user choose a complete installation or a custom installation,
which can override the components you specify with ADDLOCAL options. If the user selects Complete, the msiexec program ignores the ADDLOCAL options in the command line and installs all components. The /qn option specifies a silent install, so no user interface appears. The /qb option also hides the user interface but it displays a progress bar.

- The procedures in this topic are valid with Windows installations only. For information about installing Pulse on OS X endpoints, see “Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File” on page 44.

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

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

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

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

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

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

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

The ADDLOCAL property has the following features:

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

The ADDLOCAL property has the following optional subfeatures:

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

• **UACEndpointDefense**—Available with PulseUAC. Includes EES components for connections to Pulse Access Control Service.

• **UACHostChecker**—Available with PulseUAC. Includes Host Checker components for connections to Pulse Access Control Service.

• **UACIPSec**—Available with PulseUAC. Includes components required to connect to Pulse Access Control Service using IPSec from 32-bit Windows endpoints. This feature is available in the 32-bit MSI only.

• **UACIPSec64**—Available with PulseUAC. Includes components required to connect to Pulse Access Control Service using IPSec from 64-bit Windows endpoints. This feature is available in the 64-bit MSI only.

### Examples

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

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

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

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

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

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

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

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

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

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

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

### Repairing a Pulse Installation on a Windows Endpoint

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

To repair a Pulse installation on a Windows endpoint:

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

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

Related Documentation
- Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 44

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

The following procedures apply to OS X installations only.

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

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

1. Select Users > Junos Pulse > Connections and create a connection set with the connections that you want to distribute.
2. Select Users > Junos Pulse > Components.
3. If necessary, create a new component set with the connection sets you want to distribute.
   
   It does not matter which component option you select, All components, No components, or Minimal components. The Pulse installation program for OS X always installs all components.

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

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

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

7. Download the Junos Pulse installer, Junos Pulse Installer (Macintosh).
Installing the Pulse Client on OS X Endpoints Using Command-Line Options

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

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

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

1. Run the Pulse installation program:
   ```bash
   sudo /usr/sbin/installer -pkg <full-path-to-the-pulse-install-package> -target /
   ```
2. Import the settings from the .jnprpreconfig file:
   ```bash
   /Applications/Junos\ Pulse.app/Contents/Plugins/JamUI/jamCommand –importFile
   <full-path-to-the-jnprpreconfig-file>
   ```

Related Documentation
- Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 40
- jamCommand Reference on page 65
PART 3

Configuration

- Junos Pulse on page 49
- Session Migration on page 55
CHAPTER 7

Junos Pulse

- Adding a Pulse Configuration to a New Pulse Installation on page 50
Adding a Pulse Configuration to a New Pulse Installation

When you install the Junos Pulse for Windows or Junos Pulse for Mac OS X client on an endpoint using the default Pulse installation program, the endpoint has all the Pulse components it needs to connect to Pulse servers. However, the Pulse client needs a configuration that identifies the Pulse servers it can connect to, that is, the connections. Connection properties also define how the connections are to be started, manually, automatically, or according to location awareness rules, and how Pulse connections receive updates. These connection set properties are also called machine settings. Figure 5 on page 50 shows the default Pulse connection set properties (machine settings) that are passed to the Pulse client as its configuration. Figure 6 on page 52 shows the connection set properties as they appear in a Pulse preconfiguration file, which you can use to add the Pulse configuration when you install Pulse. The preconfiguration file also includes Pulse connections.

Figure 5: Junos Pulse Configuration Properties Defined on the Pulse Server

There are two methods for installing an initial configuration on a new Pulse client:

- Use a Pulse preconfiguration file (.jnprpreconfig) when you install Pulse on endpoints using the default Pulse installer.
- Instruct users to open a browser and login to a Pulse server Web portal where the Pulse configuration has been defined. After successful login, the user should start Junos Pulse from the Web page. Or you can enable Auto-launch as a role option to have the Pulse installation begin automatically after login.

The first time a Pulse client connects to a server that offers a Pulse configuration, the configuration settings are installed on the client, and the client is bound to that server,
which means that only that server can update the client’s configuration. Any Pulse server can update the Pulse client software version if that feature is enabled, and any Pulse server can add a connection to an existing Pulse client configuration if Dynamic connections is enabled as part of the connection set on the binding server. Only the binding server can update the Pulse client’s configuration.

If the Pulse configuration has Dynamic connections enabled, then connections from other Pulse servers are automatically added to the Pulse client’s connections list when the user connects to the other Pulse server through that server’s Web portal. For example, a user has a Pulse configuration from PulseServerA (the binding server) and the Pulse configuration allows dynamic connections. If the user browses to PulseServerB and successfully authenticates through that server’s Web portal, the server adds a PulseServerB connection to the Pulse client configuration, and it appears in the Pulse client’s connection list. This new connection is set to start manually so that it does not attempt to connect when the endpoint is restarted or conflict with the connections from the binding server. A dynamic connection is added to the Pulse client’s connections list. However, the connection’s target URL is Pulse Web server URL; it does not use the URL that is defined for the connection in the server’s Pulse connection properties. In most cases, these URLs will be the same.

You can see a Pulse configuration by creating and viewing a .jnprpreconfig file. (To create the file, go to the Pulse Component screen, select a component set, and then click the Download Pulse Configuration button.) The .jnprpreconfig file contains a section that defines the machine settings and separate sections for each Pulse connection deployed to the client, as shown in Figure 6 on page 52.
The machine settings and each centrally configured connection (as opposed to connections created by users or added as dynamic connections) include the server ID (server-id) of the binding server. When a user browses to a Pulse server, and the server offers a new configuration, (that is, updates to the machine settings), the client ignores it unless the server ID in the new configuration matches the server ID of the Pulse client's configuration.

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

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

Related Documentation

• Junos Pulse Client Installation Overview on page 10
• Introducing Junos Pulse on page 3
CHAPTER 8

Session Migration

- Task Summary: Configuring Session Migration on page 55
- Configuring Session Migration for the Pulse Client on page 56
- Configuring an IF-MAP Federated Network for Session Migration on page 56

Task Summary: Configuring Session Migration

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

1. Configure location awareness rules within a client connection set to specify locations included in the scope of session migration for users. For example, configure location awareness rules for a corporate Pulse Access Control server connection and a Pulse Secure Access server connection.

2. Configure an IF-MAP federated network, with the applicable Pulse Access Control servers and SA Series appliances as IF-MAP Federation clients of the same IF-MAP Federation server.

3. Ensure that user entries are configured on the authentication server for each gateway.

4. Ensure that user roles are configured for all users on each gateway.

5. Define a remediation role with no Host Checker policies to allow user sessions to be maintained when an endpoint is sleeping or hibernating.

6. Configure role-mapping rules that permit users to access resources on each gateway.

7. Enable and configure session migration from the User Realms page of the admin console.

8. Distribute the Pulse client to users.

Related Documentation

- Understanding Session Migration on page 27
- Configuring Session Migration for the Pulse Client on page 56
- Understanding Federated Deployments
Configuring Session Migration for the Pulse Client

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

To configure session migration:

1. In the admin console, select Users > User Realms.
2. Select an existing realm, or create a new realm.
4. In the Authentication Group box, enter a string that is common to all of the gateways that provision session migration for users. The authentication group is used as an identifier.
5. Select for either the Use Attributes from IF-MAP option button or the Lookup Attributes using Directory Server option.

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

Related Documentation
- Understanding Session Migration on page 27
- Task Summary: Configuring Session Migration on page 31
- Understanding Federated Deployments

Configuring an IF-MAP Federated Network for Session Migration

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

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

An IF-MAP server certificate must be installed on the IF-MAP server. The client verifies the server certificate when it connects to the server. The server certificate must be signed by a Certificate Authority (CA), the client must be configured to trust certificates signed by that CA, and the hostname in the server certificate must match the hostname in the IF-MAP URL on the client.
You must identify the IF-MAP server to each IC Series device and SA Series device IF-MAP client. To add the server, you specify the IF-MAP URL of the server and how to authenticate to the server. Match the URL and security settings to equal those on the IF-MAP server to which the IF-MAP clients will connect.

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

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

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

1. From the admin console select System > IF-MAP Federation > Overview.
2. In the IC Series device, under Choose whether this IC Series device runs an IF-MAP Server, an IF-MAP client, or no IF-MAP, select the IF-MAP Client option button. On the SA Series device, select Enable IF-MAP Client check box.
3. Type the server URL for IF-MAP Web service on the IF-MAP server. Append the server URL with /dana-ws/soap/dsifmap for all Juniper Networks IF-MAP servers.
   For example, https://access2.corporate.com/dana-ws/soap/dsifmap.
4. Select the client authentication method: Basic or Certificate.
   
a. If you select Basic, enter a username and password. This is the same as the information that was entered on the IF-MAP server.

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

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

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

5. Click Save Changes.

Related Documentation

- Understanding Session Migration on page 27
- Task Summary: Configuring Session Migration on page 31
PART 4

Administration

- Junos Pulse Launcher on page 61
- Junos Pulse Connections on page 63
CHAPTER 9

Junos Pulse Launcher

- Launching Junos Pulse from the Pulse Server Web Portal on page 61

Launching Junos Pulse from the Pulse Server Web Portal

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

The following items describe the Pulse connection behaviors:

- The Pulse client has been installed on the endpoint by using the default Pulse installer. The installed Pulse client does not yet have any connections. The user browses to the Pulse server, logs into the server, and then clicks the Pulse button on the Web portal page. The following action occurs:
  1. The default Pulse connection set is automatically deployed to the client.
  2. The connection that has a URL that matches the server URL is launched.

- The Pulse client has been installed on the endpoint and it has a connection from the Pulse server. The user browses to the Pulse server, logs into the server, and then clicks the Pulse button on the Web portal page. The following action occurs:
  1. The connection that has a URL that matches the server URL is launched.

- Pulse has been installed on the endpoint and it has a connection from two different Pulse servers. The user browses to one of these Pulse servers, logs into the server, and then clicks the Pulse button on the Web portal page. The following action occurs:
  1. Only the connection that has a URL that matches the server URL is launched.

- Pulse has been installed on the endpoint. It has a connection for one Pulse server but the user browses to a different Pulse server, logs into the server, and then clicks the Pulse button on the Web portal page. The following action occurs:
  1. A new dynamic connection is created on the Pulse client for this Pulse server. (Note that the default connection on the server must be configured as a dynamic connection.) This new connection is a manual connection, that is, it does not start automatically when Pulse starts.
  2. The new connection for this Pulse server is started based on matching URLs.
Usage Notes

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

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

Related Documentation

- Adding a Pulse Configuration to a New Pulse Installation on page 50
- Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 40
- Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 44
CHAPTER 10

Junos Pulse Connections

- Using jamCommand to Import Junos Pulse Connections on page 63

Using jamCommand to Import Junos Pulse Connections

The jamCommand.exe program is a command line program that imports a .jnprpreconfig file into the Pulse client. The jamCommand program is available for Windows (XP, Vista, Windows 7, and Windows 8) and Mac OSX.

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

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

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

To install Pulse connections using jamCommand:

1. Create a .jnprpreconfig file on the Pulse server.
   In the Pulse server admin console, click Users > Junos Pulse > Components.
2. Select the component sets you want, and then click Download Installer Configuration.
3. Distribute the .jnprpreconfig file to the Pulse endpoints.
4. Run jamCommand with the .jnprpreconfig file as an option. For example:
   - On Windows:
     \Program Files\Common Files\Juniper Networks\Jam\jamcommand -importfile myfile.jnprpreconfig
   - On Mac OSX:
/Applications/Junos Pulse/Contents/Plugins/JamUI/jamCommand -importfile myfile.jnprpreconfig

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

Related Documentation
- Junos Pulse Command-line Launcher on page 33
- Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 40
- Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 44
- jamCommand Reference on page 65
jamCommand Reference

**Syntax**
jamCommand [-import [script]] [-tray] [-log[level]]

- /import
- /importFile <script>
- /tray
- /log <level>
- /stop
- /suspend <GUIDS>
- /resume <GUIDS>
- /resume
- /brand <brandfile>
- /unbrand
- /norestart

**Release Information**
Introduced with Pulse R1.0. Pulse R3.1 introduced the suspend and resume options.
Pulse R4.0.3 introduced new options to support the Junos Pulse Client Customization tool.

**Description**
The jamCommand.exe program is a command line program that imports a .jnprpreconfig or a Branding.PulseBrandingPackage file into the Pulse client. The jamCommand program is available for Windows and Mac OSX.

**Options**
- import—Import script from the default memory-mapped file.
- importFile <script>—Import script from the specified file.
- tray—Launch the tray notify application.
- log—Set the global log level.
- stop—Stop the Pulse UI.
- suspend <GUIDS>—Suspend the Pulse UI.
- resume <GUIDS>—Resume a suspended Pulse UI.
brand <brandfile>—Install the Pulse user interface changes defined in the Pulse branding file.

unbrand—Remove the changes applied by the Pulse branding file.

norestart—Do not restart Pulse after applying the Pulse branding file.

Required Privilege Level

 administrator

Related Documentation

• Installing the Junos Pulse Client on Windows Endpoints Using a Preconfiguration File on page 40
• Installing the Junos Pulse Client on OS X Endpoints Using a Preconfiguration File on page 44
• Customizing Junos Pulse Overview
PART 5

Troubleshooting

- Junos Pulse Client Error Messages on page 69
- Junos Pulse Client Log Files on page 71
- Junos Pulse Client Interface on page 75
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 the user can take to resolve the issue. Some of the message catalog files are part of a Junos Pulse component and are installed on an endpoint only if that component is installed on the endpoint.

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

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

Related Documentation

- Introducing Junos Pulse on page 3
Accessing Junos Pulse Client Error Messages on Mac OS X Endpoints

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

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

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

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

Related Documentation

- Introducing Junos Pulse on page 3
- Junos Pulse Client Log Files on page 71
CHAPTER 12

Junos Pulse Client Log Files

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

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

Pulse maintains its own log files on all supported platforms. On Windows 7 and Windows Vista, the Pulse client also logs its major operational events into Windows Event Log. Network administrators can review the Pulse event log to help troubleshoot problems. Table 8 on page 71 lists the Pulse messages that can appear in the Windows event log.

To view the Pulse messages:

1. Open the Windows Event Viewer.
2. Click Applications and Services > Junos Pulse > Operational.

Table 8: Junos Pulse Event Log Messages

<table>
<thead>
<tr>
<th>ID</th>
<th>Level</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>600</td>
<td>error</td>
<td>The connection &lt;ID&gt; failed authentication: Error &lt;ID&gt;.</td>
<td>802.1X EAP authentication failure.</td>
</tr>
<tr>
<td>601</td>
<td>informational</td>
<td>User has canceled authentication of the connection &lt;ID&gt;.</td>
<td>The user canceled 802.1X EAP authentication.</td>
</tr>
<tr>
<td>602</td>
<td>error</td>
<td>Failure writing wireless LAN profile for connection &lt;ID&gt; Error &lt;ID&gt;: Reason &lt;ID&gt;: Profile: &lt;ID&gt;.</td>
<td>A failure occurred while a wireless LAN profile was being created or modified.</td>
</tr>
</tbody>
</table>
Table 8: Junos Pulse Event Log Messages (continued)

<table>
<thead>
<tr>
<th>ID</th>
<th>Level</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>603</td>
<td>error</td>
<td>Failure writing wireless LAN profile for connection &lt;ID&gt; Error &lt;ID&gt;.</td>
<td>A failure occurred while a wireless LAN profile was being deleted.</td>
</tr>
<tr>
<td>604</td>
<td>error</td>
<td>Failure writing wired LAN profile for connection &lt;ID&gt; Error &lt;ID&gt;; Profile: &lt;ID&gt;.</td>
<td>A failure occurred while a wired LAN profile was being created or modified.</td>
</tr>
<tr>
<td>605</td>
<td>error</td>
<td>Failure writing wired LAN profile for connection &lt;ID&gt; Error &lt;ID&gt;.</td>
<td>A failure while a wired LAN profile was being deleted.</td>
</tr>
<tr>
<td>500</td>
<td>informational</td>
<td>Pulse servicing has completed successfully. All components are up to date.</td>
<td>Pulse servicing was successful.</td>
</tr>
<tr>
<td>501</td>
<td>informational</td>
<td>Pulse servicing has completed successfully. All components are up to date.</td>
<td>Servicing was requested but all components were up to date.</td>
</tr>
<tr>
<td>502</td>
<td>error</td>
<td>Pulse servicing has failed. Failure summary:</td>
<td>Pulse servicing failed.</td>
</tr>
<tr>
<td>100</td>
<td>informational</td>
<td>User requested connection &lt;ID&gt; to start.</td>
<td>The user initiated a connect request.</td>
</tr>
<tr>
<td>101</td>
<td>informational</td>
<td>User requested connection &lt;ID&gt; to stop.</td>
<td>The user initiated a disconnect request.</td>
</tr>
<tr>
<td>102</td>
<td>informational</td>
<td>Connection &lt;ID&gt; is starting because its policy requirements have been met. Connection Policy: &lt;ID&gt;.</td>
<td>A connection was started because of a policy evaluation.</td>
</tr>
<tr>
<td>103</td>
<td>informational</td>
<td>Connection &lt;ID&gt; is stopping because of its policy requirements. Connection Policy: &lt;ID&gt;.</td>
<td>A connection was stopped because of a policy evaluation.</td>
</tr>
<tr>
<td>104</td>
<td>informational</td>
<td>Connection &lt;ID&gt; is stopping because of transition to context &lt;ID&gt;.</td>
<td>The machine-to-user connection was disconnected to transition to another identity.</td>
</tr>
<tr>
<td>105</td>
<td>informational</td>
<td>Connection &lt;ID&gt; is starting because of transition to context &lt;ID&gt;.</td>
<td>The machine-to-user connection was connected as part of the transition to another identity.</td>
</tr>
<tr>
<td>106</td>
<td>informational</td>
<td>Connection &lt;ID&gt; is disconnected due to computer suspend.</td>
<td>The connection to Pulse Secure Access Service was disconnected because the computer is being suspended.</td>
</tr>
<tr>
<td>107</td>
<td>informational</td>
<td>Connection &lt;ID&gt; is disconnected due to login error.</td>
<td>A credential provider connection was disconnected because of a login error.</td>
</tr>
<tr>
<td>108</td>
<td>informational</td>
<td>Connection &lt;ID&gt; is disconnected because it was modified.</td>
<td>A connection was disconnected because it was modified.</td>
</tr>
</tbody>
</table>
### Table 8: Junos Pulse Event Log Messages (continued)

<table>
<thead>
<tr>
<th>ID</th>
<th>Level</th>
<th>Message</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>109</td>
<td>informational</td>
<td>User requested connection <code>&lt;ID&gt;</code> to suspend.</td>
<td>The user initiated a suspend request.</td>
</tr>
<tr>
<td>110</td>
<td>informational</td>
<td>User requested connection <code>&lt;ID&gt;</code> to resume.</td>
<td>The user initiated a resume request.</td>
</tr>
<tr>
<td>1</td>
<td>informational</td>
<td>The Junos Pulse service version <code>&lt;ID&gt;</code> has successfully started.</td>
<td>The Pulse service started.</td>
</tr>
<tr>
<td>2</td>
<td>informational</td>
<td>The Junos Pulse service has stopped.</td>
<td>The Pulse service stopped.</td>
</tr>
<tr>
<td>200</td>
<td>error</td>
<td>No connections matching URL <code>&lt;ID&gt;</code> were found in Pulse database. Request to start a connection from the browser has failed.</td>
<td>Pulse failed to resume a connection from the browser.</td>
</tr>
<tr>
<td>400</td>
<td>error</td>
<td>The host check for connection <code>&lt;ID&gt;</code> has failed. Failed policies: <code>&lt;ID&gt;</code>.</td>
<td>Host Checker failed one or more policies.</td>
</tr>
<tr>
<td>300</td>
<td>informational</td>
<td>The connection <code>&lt;ID&gt;</code> was established successfully through web-proxy <code>&lt;ID&gt;</code>.</td>
<td>Pulse established a connection to Pulse Secure Access Service or Pulse Access Control Service through a Web proxy.</td>
</tr>
<tr>
<td>301</td>
<td>informational</td>
<td>The connection <code>&lt;ID&gt;</code> was established successfully to address <code>&lt;ID&gt;</code>.</td>
<td>Pulse established a direct (nonproxy) connection to Pulse Secure Access Service or Pulse Access Control Service.</td>
</tr>
<tr>
<td>302</td>
<td>informational</td>
<td>The connection <code>&lt;ID&gt;</code> was disconnected.</td>
<td>The Pulse connection was disconnected from the Pulse server.</td>
</tr>
<tr>
<td>303</td>
<td>error</td>
<td>The connection <code>&lt;ID&gt;</code> encountered an error: <code>&lt;ID&gt;</code> Peer address: <code>&lt;ID&gt;</code>.</td>
<td>A connection encountered an error.</td>
</tr>
<tr>
<td>304</td>
<td>error</td>
<td>The connection <code>&lt;ID&gt;</code> was disconnected due to change in routing table. Interface address changed from <code>&lt;ID&gt;</code> to <code>&lt;ID&gt;</code>.</td>
<td>Pulse detected a change in the route to the Pulse server.</td>
</tr>
<tr>
<td>305</td>
<td>informational</td>
<td>VPN tunnel transport for connection <code>&lt;ID&gt;</code> switched from ESP to SSL mode due to missing ESP heartbeat.</td>
<td>ESP to SSL fallback occurred because of missing ESP heartbeats.</td>
</tr>
<tr>
<td>306</td>
<td>informational</td>
<td>VPN tunnel for connection <code>&lt;ID&gt;</code> is switched to ESP mode.</td>
<td>Tunnel transport switched to ESP mode.</td>
</tr>
<tr>
<td>307</td>
<td>error</td>
<td>The connection <code>&lt;ID&gt;</code> encountered an error: System error: <code>&lt;ID&gt;</code> Peer address: <code>&lt;ID&gt;</code>.</td>
<td>The Pulse connection failed because of a system error.</td>
</tr>
<tr>
<td>308</td>
<td>error</td>
<td>The server disconnected connection <code>&lt;ID&gt;</code> Reason <code>&lt;ID&gt;</code> Peer address: <code>&lt;ID&gt;</code>.</td>
<td>The server disconnected a connection.</td>
</tr>
</tbody>
</table>
Deleting the Junos Pulse Client Log Files

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

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

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

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

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

2. Empty the Recycle Bin.

   Alternatively, you could first rename debuglog.log and then delete it. After you delete the log file, the Pulse client creates a new one. However, that operation might take some time depending on the activities of the Pulse client.
CHAPTER 13

Junos Pulse Client Interface

- Junos Pulse Client Status Icons on page 75

Junos Pulse Client Status Icons

The Junos Pulse client interface (Windows and OS X) displays a system tray icon (Windows) or a menu bar icon (OS X) that indicates connection status, provides access to menu items that let the user connect and disconnect from networks and meetings, and enables quick access to the program interface. Only one icon is visible even when there are multiple connections. One icon provides the status for all connections by indicating the most important connection state information. Table 9 on page 75

Table 9: Pulse Icon States (Windows Tray and OS X Menu Bar)

<table>
<thead>
<tr>
<th>Icon</th>
<th>State Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Icon]</td>
<td>Connection failed.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Connected with issues. For example, Host Checker found an issue that must be fixed before full access is available.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>Connected.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>The user has suspended the connection.</td>
</tr>
<tr>
<td>![Icon]</td>
<td>No active connections.</td>
</tr>
</tbody>
</table>

Related Documentation
- Installation Requirements on page 10
- Introducing Junos Pulse on page 3
PART 6

Index

• Index on page 79
Index

Symbols

#, comments in configuration statements..........................xiii
( ), in syntax descriptions..................................................xiii
.inprrpconfig
  example.............................................................................50
3G wireless...........................................................................21
802.1X
  Pulse - OAC comparison..................................................15
802.1x connections
  certificate.............................................................................7
  reboot on upgrade..........................................................9
< >, in syntax descriptions.................................................xii
[ ], in configuration statements..........................................xiii
{ }, in configuration statements........................................xiii
| (pipe), in syntax descriptions........................................xiii

A

ActiveX
  Web installation..............................................................39
admin privileges.....................................................................11
AES......................................................................................16
application acceleration
  deployment option..........................................................13
authentication
  SecurID.............................................................................9
authentication methods.......................................................16
automatic updates..................................................................9
autoscan lists.......................................................................15

B

binding server ID.................................................................53
braces, in configuration statements....................................xiii
brackets
  angle, in syntax descriptions.............................................xii
  square, in configuration statements...................................xiii
browser
  launching Pulse ..............................................................61

certificate
  smart card.........................................................................17
  support..............................................................................17
CHAP inner authentication................................................16
client errors...........................................................................69
  OS X.................................................................................70
command line launcher......................................................20
examples..............................................................................35
command-line launcher......................................................33
comments, in configuration statements.............................xiii
config file............................................................................50
connection properties.......................................................50
credentials
  provider.............................................................................17, 20
contacting JTAC.................................................................xiii

default deployment............................................................10
default installer.......................................................................11
deleting
  Pulse client log files......................................................74
diagnostics............................................................................18
DNS server search..............................................................21
documentation
  comments on....................................................................xiii
dynamic connections..........................................................50, 61
  overview.............................................................................7

e

EAP methods.......................................................................16
EAP-GTC inner authentication............................................16
EAP-JUAC inner authentication...........................................16
EAP-MD5 inner authentication............................................16
EAP-MSCHAPv2 inner authentication................................16
EAP-PEAP outer authentication.........................................16
EAP-TLS outer authentication.............................................16
EAP-TTLS outer authentication...........................................16
encryption methods
  Pulse Access Control Service..........................................16
error codes
  pulselauncher...................................................................33
error messages......................................................................69
  OS X.................................................................................70
ESP transport mode............................................................20

Copyright © 2013, Juniper Networks, Inc.