

# Junos Pulse Release 1.0

Junos Pulse Build# 6541

Secure Access Build# 16007

Unified Access Control Build# 14913

JWOS Build# 6.1R1.13



Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
408 745 2000 or 888 JUNIPER  
[www.juniper.net](http://www.juniper.net)  
June, 2010

## Contents

Junos Pulse Release 1.0.....	1
<b>Important Notes</b> .....	3
Installing and Deploying Junos Pulse .....	3
New Features in this Release .....	3
Interoperability and Supported Platforms.....	3
Junos Pulse Client Availability.....	3
Known Issues and Limitations.....	3
Junos Pulse 1.0 .....	3
Installation and Configuration .....	4
Unified Access Control .....	4
Secure Access.....	5
Endpoint Security .....	6
SRX .....	6
802.1x.....	6
Application Acceleration .....	6
Communicating Issues .....	7

For information about supported minimum requirements for Network and Security Manager (NSM), please refer to the *Juniper Networks Network and Security Manager Installation Guide*.

## Important Notes

There are several important steps you must follow before using this version of Pulse:

- Please uninstall any previous versions of Pulse (including Pulse Beta).
- Please uninstall any versions of Odyssey Access Client prior to version 5.2
- Please uninstall any instances of WX Client on the client.
- Please uninstall the Juniper Access Manager Web Client.

## Installing and Deploying Junos Pulse

There are several ways to deploy Junos Pulse to endpoints:

- Create a custom configuration on the IC Series or SA Series device, and direct users to navigate to the access device for an automatic download through a role. This is the simplest way to deploy Pulse!
- Create a custom configuration, download an installer package, and distribute to users through a System Management Server (SMS).
- Download the default installer from the Maintenance > System > Installers page and distribute to users.

With the default installer, all components and connections needed for connecting to an access device are included in the client.

For custom configurations, you create component sets and connection sets on the Intranet Controller or Secure Access device, and then download an installer package. See the Junos Pulse User Guide for complete instructions.

- Download the default installer from the Client Download page on the WXC device running JWOS 6.1.

## New Features in this Release

- Please refer to the What's New document for details about new features available in this release: <http://www.juniper.net/support/products/pulse>

## Interoperability and Supported Platforms

- Please refer to the *Pulse Supported Platforms* document for supported versions of Screen OS, JUNOS, browsers, and operating systems in this release: <http://www.juniper.net/support/products/pulse>

## Junos Pulse Client Availability

- Pulse packages are available for download from the following URL: <http://www.juniper.net/support/products>
- Log in with your Juniper support account to download any Pulse packages.

## Known Issues and Limitations

The following lists known issues which are still outstanding in this release:

### Junos Pulse 1.0

- Infranet Enforcer "deny" messages are currently not displayed in the Junos Pulse user interface. (488619)
- Pulse UI does not display correctly in High Contrast graphics settings. (490249)
- The F1 key does not display the Table of contents help window. (484222)
- Disabling "Allow user to override connection policy" will result in a user not being able to connect if the connection policy indicates a connection should not be connected. (498065)

- Disabling Junos Pulse Split Tunneling on a Secure Access device may impact the ability for Pulse to evaluate Location Policies associated with the physical interface on the endpoint. (506100)
- When using a packet capture / monitor tool like Wireshark or NetMon (on XP), certain IP packets sent may appear to be sent 'twice'. This is most often observed when the network capture mechanism enables "Promiscuous Mode" on the network adapter. (514609)
- Please ensure that all IC Series and SA Series devices are upgraded to this release if they are running previous beta versions. You should not attempt to run beta versions simultaneously with the release version on different devices. (514865)
- Trailing white space is not pruned when entering user credentials within Pulse. (513433)
- If Junos Pulse is uninstalling while connected to an IC or SA device, the Pulse user session on the IC or SA device may not be deleted immediately. The session will be removed from the device when the user session's Heart Beat interval on the IC or Idle Timeout on the SA expires. (488572)
- If Pulse UI displays "Connect Requested" connection status for an extended period of time and no progress is shown in establishing the connection, clicking disconnect followed by connect should allow the connection to proceed. (514890)
- Pulse UI may not display correctly on screen resolutions of 800 x 600 or less. (524205)
- Pulse does not support certificate based authentication with certificates created or imported with "enable strong private key protection" feature. (518468)
- Pulse may take 2-3 minutes to reconnect to an active node after a manual vip-failover occurs. (518027)

## Installation and Configuration

- Canceling the Junos Pulse client installation is currently not supported. (492565)
- Pulse deployed via dynamic deployment from an SA or IC device cannot be upgraded using the full installer package. (513007)
- Some users may experience extended install times for Juniper's network driver component. (494736)
- Some versions of Windows XP contain a known issue that causes extended install times for Pulse. Please refer to MS Incident KB949900 for a patch that should resolve the issue (<http://support.microsoft.com/default.aspx/kb/949900>). (519639)
- Pulse installation on Vista x64 may not pre-install Juniper Networks Virtual Adapter instances. The first time a Pulse connection is established that requires a Juniper Networks Virtual Adapter instance the adapter will be installed resulting in a slight delay during the first connection. (521929)
- If the user receives the error message "error provisioning access method connection" when attempting to establish a connection, it is possible that a third party USB device is interfering with the Juniper Networks Virtual Adapter. (527406)
- When attempting to establish connections, Pulse may prompt you multiple times to upgrade 'missing components'. (529409)
- Configuration changes to SA or IC devices that result in deploying new Firewall, 802.1x, or WX connections may require end users to re-login to the device via the web browser. (523193)
- The SA or IC administrator must associate a connection set with Pulse enabled user roles in order for Pulse to be properly deployed to endpoints. Pulse will not be installed or upgraded if the Pulse role references an empty connection set. (525667)
- Pulse pre-configured installers can not re-bind the endpoint when it is already bound to a server. (524357)
- If Junos Pulse and Kaspersky AntiVirus are installed and you attempt to uninstall Pulse, the popup message "Error!Can't initialize pulg-ins directory.please try again later.." maybe displayed. If this occurs, try uninstalling Pulse again. (528694)

## Unified Access Control

- If you are using UAC IPSec Enforcement using Junos Pulse, applications might experience a slight delay in being able to establish network connections. (491848)

- When you configure Junos Pulse to make 802.1x based connections, a reboot may be required on Windows XP the next time Junos Pulse is upgraded. (492843)
- When you create a preconfigured installer, you download and run the pre-configuration utility on a Windows machine. The operating system (32- or 64-bit) on which you generate a preconfigured installer determines the machines on which the installed Pulse client will run. If you generate the preconfigured installer on a 64-bit machine, the Pulse client installed by that installer will run only on 64-bit machines. If you generate the preconfigured installer on a 32-bit machine, the Pulse client installed by that installer will run only on 32-bit machines. (498503)
- Establishing a connection to an IC Series device via the Pulse client is not supported when there is an existing active connection to the IC Series device with Odyssey Access Client. (509095)
- NAP Host Checker Policies will not work with Pulse if Odyssey Access Client is installed and also evaluating NAP Host Checker Policies. (512884)
- Certain client firewalls may make the Pulse connection on the IC appear as if it is located behind a NAT device when it is not. (519630)
- If connected to a SA Series device and an IC Series device, then disconnect from the SA Series device, other Pulse clients may receive the error "Too many connections from the same endpoint" error while attempting to connect to the IC Series device. (528650)
- When both Pulse and the Odyssey Access Client are installed on the same machine, it is advisable that only one client be used when establishing connections to the same IC Series device. (526333)
- While Pulse is connected to an IC Series device and the user initiates a connection to a Firewall, the IC Series device connection may get disconnected. (524075)
- When Pulse has connections to both an IC Series and SA Series Access and the user disconnects from the IC Series device, the Active Users page may show that the user session is still active. (523750).

## Secure Access

- Multiple simultaneously connected SA Series device connections are not supported in Junos Pulse.
- Changes made to Junos Pulse configuration on SSL-VPN and UAC Devices are not showing up in the Admin Access Logs. (475507)
- It is currently not possible to provide Junos Pulse access for the delegated admin role on SA/IC Series devices. (477822)
- When running Junos Pulse within Secure Virtual Workspace, the Pulse user interface will not launch correctly if it is also running on the base desktop. (483290)
- When using the Firefox browser to deploy Pulse from a SA Series or IC Series device, please be sure that "Enable the next generation Java Plugin" is enabled in the Java console. (498586)
- Please be sure to install 32-bit version of Java runtime on 64-bit windows versions when deploying pulse via the Firefox browser. (502486)
- SAML OAAM authentication is not supported with the Pulse client. (505578)
- XML Export of the Pulse Configuration from a SA Series or IC Series device is exporting connection type as 802.1x for WX connection in Junos Pulse connection sets. (513816)
- Junos Pulse may not be able to connect correctly to an SA Series device configured for secondary authentication when certificate authentication and local authentication are configured as primary/secondary authentication servers. (489989)
- When client proxy or server proxy is configured, if user click on Sign out from the browser while Pulse NC is connected or if the Pulse NC user is timed out, Pulse may go into infinite reconnect loop. This is because the proxy PAC file set by NC AM is not reverted in this situation, thus blocking Pulse from reconnecting. To come out of this situation, end user needs to click on disconnect on Pulse UI and try to connect again. (521906)

## Endpoint Security

- Activating EES on an SA Series or IC Series device does not immediately deploy this feature to currently connected Pulse clients. Re-connecting the connection to the device in the Pulse client is necessary to deploy EES to the endpoint. (513926)
- When the Host Checker Policy Monitoring feature is enabled on an SA Series or IC Series device, policy monitoring may continue to be functional on the endpoint after disconnecting the corresponding connection in the Pulse UI. (482978)
- Pulse endpoints that sign-in to a sign-in URL mapped to multiple realms with and without host checker restrictions may display Host Checker failure message even when compliant with the Host Checker policy. The message can be ignored and dismissed by clicking the continue button or disconnecting and connecting again. (520291)
- When EES is enabled and Pulse is connecting to an SA Series or IC Series device that doesn't have an adequate number of licenses available, Pulse does not display the correct reason for the failure in the Pulse UI. (523683)
- When ESS is enabled and Pulse is upgraded or installing missing components, EES may be disabled after the installation has finished. (529318)
- When Endpoint Security is downloaded and installed over a slow network connection, Pulse may remain in the connecting state indefinitely. (528511)
- When Pulse with Enhanced Endpoint Security (EES) and the Juniper Networks Host Checker are installed, EES may become disabled if you uninstall Host Checker. (528117)

## SRX

- Installing Junos Pulse 1.0 after installing JAM 1.0 is not supported.
- Save credentials in the Junos Pulse credential dialog is not working correctly for SRX connections. (490482)
- For firewall connections, the "Forget saved settings" option may not clear all saved data. (492880)

## 802.1x

- Junos Pulse doesn't show authentication failure when using 802.1x connections and an expired client certificate is used. (487727)
- When using Junos Pulse 802.1x connections on Windows XP with Odyssey Access Client installed, you will have to check the checkbox, "use windows to configure my wireless network settings", manually after you uncheck "use Odyssey to operate this adapter" in Odyssey Access Client. (504701)
- Pre-configuration of 802.1x settings is required in order for the 802.1x feature to work correctly if users cannot log-in to the IC via the web browser to dynamically deploy the configuration. (526341)

## Application Acceleration

- The Junos Pulse Application Acceleration component may cause disruptions with some types of network connections on systems with multiple network interfaces that are connected simultaneously. (504692)
- Deploying the Junos Pulse WAN Application Acceleration package via Host Checker is not supported when logging in via the Junos Pulse client. This is only applicable to browser based initial deployments. (504952)
- Firewalls like Kaspersky software that are known to block Pulse Application Acceleration control packets. UDP port 3578 will have to be provisioned to open ports at the endpoint. (505817)
- If Junos Pulse software requires the Application Acceleration capability to be deployed from an SA Series device, 'All' components should be selected at the SA Series device. (505944)
- Multiple simultaneous PPP connections are not supported when the Application Acceleration component is installed. This might occur if both a dial-up, PPPOE, or WWAN/PPP connection is active and a PPTP or LP2TP VPN is also used. Multiple dial-up or multiple PPTP/L2TP connections running simultaneously are also unsupported. (515531)

- Pulse may disrupt Internet Connection Sharing via Windows Virtual Wifi on Windows 7 Endpoints when Application Acceleration is installed. (507628)
- Pulse Application Acceleration feature may disrupt network traffic to VMWare Virtual Machines running in "bridged mode" on the same endpoint. (522313)
- Application Acceleration may not get enabled correctly when changing the configured community string after deploying Pulse via Host Checker. (527411)
- An Application Acceleration adjacency can still be established between Pulse and WXC server when the community string that was deployed to the Pulse client from an SA or IC device is removed from the Administrator UI of the SA or IC device. (527660)
- When creating a WX Connection in the SA Series or IC Series device Administrator UI, do not use a blank value for the Community String property. (527732)

## Communicating Issues

To open a case or to obtain support information, please visit the Juniper Networks Support Site:

<http://www.juniper.net/support>.