Junos Pulse Release 2.0

Junos Pulse Build# 8491

Secure Access Build# 17675

Unified Access Control Build# 17057

JWOS Build# 6.1R2
Contents

Junos Pulse Release 2.0................................................................................................................................................. 1
Juniper Networks Junos Pulse 2.0 – New Features ....................................................................................................... 3
  Additional Split Tunneling Options .......................................................................................................................... 3
  Ability to Run Administrator-Configured Scripts ...................................................................................................... 3
  Authentication Using Smart Cards .......................................................................................................................... 4
  MSI Installer ............................................................................................................................................................. 4
  RSA SoftToken Support .......................................................................................................................................... 5
  Junos Pulse 2.0 Support for SA Series SSL VPN and IC Series UAC Gateways .................................................. 5
Installing and Deploying Junos Pulse 2.0 ....................................................................................................................... 5
New Features in this Release ......................................................................................................................................... 6
Interoperability and Supported Platforms ........................................................................................................................ 6
Junos Pulse Client Availability ......................................................................................................................................... 6
Known Issues and Limitations ......................................................................................................................................... 6
  Junos Pulse 2.0 ....................................................................................................................................................... 6
  Installation and Configuration .................................................................................................................................. 6
  Unified Access Control ........................................................................................................................................... 7
  Secure Access ......................................................................................................................................................... 8
  Endpoint Security .................................................................................................................................................... 8
  SRX ......................................................................................................................................................................... 9
  802.1x ...................................................................................................................................................................... 9
  Application Acceleration .......................................................................................................................................... 9
  Communicating Issues ............................................................................................................................................ 10

For information about supported minimum requirements for Network and Security Manager (NSM), please refer to the Juniper Networks Network and Security Manager Installation Guide.
Juniper Networks Junos Pulse 2.0 – New Features

Additional Split Tunneling Options

Junos Pulse 2.0 (for Microsoft Windows) introduces additional split tunneling options, allowing customers to set policies controlling the traffic behavior from the remote user’s Microsoft Windows PC to the SA Series SSL VPN. The additional split tunneling options in Junos Pulse 2.0 for Windows enable customers to apply the same breadth of split tunneling options available in Network Connect to Junos Pulse.

The enhanced split tunneling options in Junos Pulse 2.0 include the following configuration options:

- **Enable or Disable Split Tunneling**: This option allows the administrator to either enable or disable split tunneling.

- **Overriding Routes**: This option allows the administrator to override any conflicting routes in the system routing table. When this option is enabled, Junos Pulse will check the system routing table for any routes that conflict with the routes set up for the Junos Pulse virtual adapter. If there are any conflicting routes, those routes are removed until the Junos Pulse SSL VPN session is up and running. When the SSL VPN session is terminated, Junos Pulse restores the conflicting system routes.

- **Monitoring Routes**: This option allows the administrator to regularly monitor the system routing table for conflicts and to ensure that the split tunneling configuration enabled in Junos Pulse is adhered to throughout the duration of the SSL VPN session. When this option is enabled, Junos Pulse monitors the system routing table in real-time and takes action when newly installed applications or programs modify the system routes, potentially creating conflicts.

Junos Pulse 2.0 delivers split tunneling option parity with Network Connect, allowing Enterprises and Service Providers to customize split tunneling behavior for end users, connecting to their SA Series SSL VPN gateways.

**Compatible with:**

SA Series SSL VPN 7.1

Ability to Run Administrator-Configured Scripts

Junos Pulse 2.0 (for Microsoft Windows) introduces the ability for an administrator to run custom scripts either at the time when a user session is established or torn down. The administrator could configure such scripts to run either for a VPN session to the SA Series SSL VPN gateway, or for a UAC session to the IC Series UAC gateway.

When this feature is configured, Junos Pulse copies over the script file to the local file system and executes the script either at the time of establishing a user session or when the session is terminated.

The benefits of administrator-configured scripts include allowing an administrator to execute custom settings on a user’s desktop either when the SA Series SSL VPN or UAC session is established; or when the SA Series SSL VPN or UAC session is torn down. Examples of administrator-configured script options include the configuration of a default printer, or of other local settings.

**Compatible with:**

SA Series SSL VPN 7.1

IC Series UAC 4.1
**Authentication Using Smart Cards**

Junos Pulse 2.0 supports the authentication of users using smart cards. Administrators can deploy Junos Pulse for remote user authentication using smart cards, as well as for managing PIN and password policy management. Junos Pulse supports smart card authentication to a local Microsoft Windows computer as well as in RDP environments, authenticating the user to a remote machine from a locally available smart card.

Smart card authentication is also made intuitive to remote users by indicating the smart card certificate in the user interface prompts using a different icon from that used for locally installed certificates.

Junos Pulse 2.0 allows remote user authentication using smart cards to both the SA Series SSL VPN gateways, as well as the IC Series UAC gateways.

Smart cards that have been tested on Junos Pulse 2.0 include (to date):

- RSA SID800 USB tokens.
- SafeNet iKey 1000/ 2032/4000/eToken-PRO USB tokens.
- Gemalto .Net cards.
- DoD (ActivIdentity) CAC cards.

**Compatible with:**

<table>
<thead>
<tr>
<th>SA Series SSL VPN 7.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC Series UAC 4.1</td>
</tr>
</tbody>
</table>

**MSI Installer**

Junos Pulse 2.0 now supports a new, redesigned installer that uses the Microsoft Windows Installer (MSI) technology. This allows for the seamless deployment of Junos Pulse by customers through software management systems (SMS) that are widely used for deploying MSI based applications.

The new MSI installer provides several key benefits to customers, including:

- **Seamless Rollback:** As the installation proceeds, a list of all actions is maintained and, if there is a failure at any point, the changes are cleanly reverted. Also, during an upgrade if any files are being replaced (overwritten), backup copies of the original files are maintained so that they can be reverted to in the case of an upgrade failure.

- **System Repair:** Windows Repair, which can repair improperly installed applications, is now supported. Windows Repair can reinstall the application to repair any corrupted or missing data, including files, registry keys, services, etc.

- **Smother Upgrades:** The MSI installer allows for smoother upgrades since the new version is installed on top of the older version. Also, in the unlikely case that an upgrade fails, a backup copy of the original installation is maintained, allowing for a simple rollback to the original version.

- **Improved Logging and Troubleshooting:** MSI installers allow for more detailed logging of system actions taken during installations and upgrades. This allows for easier troubleshooting and debugging in the unlikely event that anything goes wrong.

**Compatible with:**

<table>
<thead>
<tr>
<th>SA Series SSL VPN 7.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC Series UAC 4.1</td>
</tr>
</tbody>
</table>
RSA SoftToken Support

Junos Pulse 2.0 for the Microsoft Windows operating system supports integration with RSA SoftID, allowing automatic access to the user’s RSA passcodes using the PIN entered by the user. When Junos Pulse detects RSA SoftID installed on the same Microsoft Windows system, it prompts the user for the RSA PIN number and programmatically retrieves the passcodes for successful authentication.

This feature allows for seamless and easy access for users to both the SA Series SSL VPN gateways, as well as the IC Series UAC gateways.

Both the SA Series and IC Series gateways can authenticate users against RSA ACE servers using EAP-GTC protocol. When Junos Pulse 2.0 is used to authenticate users over EAP-GTC against an RSA ACE server, the integration with RSA SoftID is activated.

Compatible with:

<table>
<thead>
<tr>
<th>SA Series SSL VPN 7.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>IC Series UAC 4.1</td>
</tr>
</tbody>
</table>

Junos Pulse 2.0 Support for SA Series SSL VPN and IC Series UAC Gateways

Junos Pulse 2.0 (for Windows) successfully interoperates with both the SA Series 7.0 and IC Series 4.0 software releases. The features enabled in Junos Pulse are the features available in the appropriate server-side releases. Junos Pulse 2.0 can be used to support the same set of features that were used with version 1.0 of the Junos Pulse software against SA Series 7.0 and IC Series 4.0.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Remote Access with SA Series SSL VPN</th>
<th>LAN Access Control with UAC (IC Series)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows XP, Windows Vista, Windows 7 (32- and 64-bit systems)</td>
<td>SA Series 7.0 Sa Series 7.1</td>
<td>IC Series 4.0 IC Series 4.1</td>
</tr>
</tbody>
</table>

Installing and Deploying Junos Pulse 2.0

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 IC Series or SA Series device, and then download an installer package. See the Junos Pulse Administration Guide for complete instructions.
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 2.0

- When using a Smartcard, the user is prompted by either the Smartcard provider or Microsoft Base Smartcard Crypto Provider CSP for the PIN/Password. This prompt is not managed by Pulse and may remain displayed after a Pulse connection is disconnected or the Pulse process has exited. (549408)
- When Custom SSL Cipher Selection is chosen on the IC Series device and AES alone is selected, Pulse connections from XP clients will not work. This is a limitation due to the cryptography available from the Windows XP operating system. (516592,555704)
- 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" results in a user not being able to connect if the connection policy indicates a connection should not be made. (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)
- 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 Series device or Idle Timeout on the SA expires. (488572)
- If the 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)
- The 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

- The Junos Pulse configuration file cannot be downloaded from an IC or SA Series device when used with
Internet Explorer’s default security settings. The workaround is to add the IC or SA Series device IP address to the trusted site list under Tools->Internet Options->Security->Trusted Sites. (581648)

- Once Junos Pulse 2.0 is installed, it is not advisable to use the standalone Pulse 1.0 installer. This may result in failures to uninstall any Junos Pulse 1.0 components. (575731)

- When upgrading to Junos Pulse 2.0 using the MSI installer package, it may take several minutes to remove the previous version of Junos Pulse and appear hung. This issue is caused by the Windows Installer doing verbose logging. The issue is documented and discussed in Microsoft KB article http://support.microsoft.com/kb/971133. (559861)

- If the RSA Soft Token application (RSA 4.1.0.458) is installed after the Junos Pulse 2.0 is installed, you must reboot the system in order for Junos Pulse to detect the presence of the soft token application. (543379)

- Canceling the Junos Pulse client installation is currently not supported. (492565)

- Pulse deployed via dynamic deployment from an SA or IC Series 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 Series 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 plug-ins directory:please try again later..." may be displayed. If this occurs, try uninstalling Pulse again. (528694)

**Unified Access Control**

- Junos Pulse 1.0 should not be installed with the Odyssey Access Client 5.3. (545524)

- After changing an IPSec Policy on an IC Series device to 'force VA', Pulse may not configure the IPSec Virtual Adapter for the active user. (492887)

- 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 shows that the user session is still active. (523750).

Secure Access
• When using a USB EVDO modem to connect to a SA Series device, Junos Pulse 2.0 may not provide network access after connecting successfully. (583893)
• Junos Pulse connections may toggle between connecting and connected when Kaspersky Internet Security is active on the endpoint and Route Monitoring is enabled at the role-level. To workaround this issue, disable Route Monitoring on the SA Series device. (562789)
• To connect to a SA series device with Junos Pulse and Kaspersky anti-virus installed, split tunneling must be enabled. (557069)
• Multiple simultaneously connected SA Series device connections are not supported in Junos Pulse.
• Changes made to Junos Pulse configuration on SA Series and IC Series 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 a user clicks on Sign out from the browser while Pulse NC is connected or if the Pulse NC user is timed out, Pulse may go into an 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, the end user must click disconnect on the Pulse UI and try to connect again. (521906)

Endpoint Security
• Shavlik Remediation may fail on endpoints running Kaspersky Antivirus 6.0 for Windows workstations. The
patch remediation may succeed if the Kaspersky Antivirus software is turned off. (573973)

- When using Patch Remediation, the patch installation count may exceed the missing patch count. This may occur when the same patch is attempted to be installed twice. The result will be a failure during the second attempt, which should be ignored. Two known patches that can exhibit this issue, WindowsXP-KB954459.exe on Windows XP and msxml6-KB954459.exe. (561392)
- During patch remediation after auto remediation complete, the user may be prompted to reboot the system. If the user attempts to connect prior to rebooting, the connection may pass the compliance check. An example of such a patch is the WindowsXP-KB953155.exe. (575714)
- When a Shavlik policy is configured and a browser is used to login and launch Junos Pulse, high CPU utilization may be observed. To avoid this issue, the user should login directly using Junos Pulse. (565692)
- During patch installation, some anti-malware solutions may report a risk warning on stdeploy.exe. To avoid the warning, add Hostcheckpluginhost.exe to the anti-malware exceptions list; otherwise user's can safely ignore the warning to continue. (573970)
- When Enhanced Endpoint Security (EES) is enabled and the user installs Junos Pulse via a browser, the upgrade prompt may be shown immediately after connecting to the Junos Secure Access Gateway. (574762)
- When using Shavlik Remediation with proxy credentials, Junos Pulse may stay in the connecting state. To workaround this issue, wait a few seconds before entering the proxy credentials (523146).
- In the Junos Pulse 2.0, the Shavlik remediation dialog prompt may flash when transitioning from the certificate to credentials dialog. (544665).
- For testing Patch Remediation feature for restricted user account, the machine should be rebooted after Pulse installation in admin account. If user switches to restricted user without rebooting then Patch Installation Progress dialog does not appear. (560962)

SRX

- Installing Junos Pulse 1.0 after installing JAM 1.0 is not supported.
- When using SecurID to authenticate, Junos Pulse 2.0 does not request a new passcode when reconnecting. (570033)
- When using SecurID to authenticate, Junos Pulse 2.0 requests user to enter the password instead of token information. (570037)
- When using Dynamic-VPN with the SRX-240 configured to use xauth authentication through the radius server, the IPSec tunnel may not get established when the virtual adapter is created. (576246)
- 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 check box, "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

- When Junos Pulse Application Acceleration is enabled while connected to a Local Area Network, network access may slow down. (523789)
- 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)
- Pulse may disrupt Internet Connection Sharing via Windows Virtual Wifi on Windows 7 Endpoints when Application Acceleration is installed. (507628)
- 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.