Pulse Connect Secure
Release Notes
PCS 8.2R8.2 Build 58717
ESAP version 3.0.3
<table>
<thead>
<tr>
<th>Contents</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>4</td>
</tr>
<tr>
<td>Hardware Platforms</td>
<td>4</td>
</tr>
<tr>
<td>Virtual Appliance Editions</td>
<td>4</td>
</tr>
<tr>
<td>Upgrade Paths</td>
<td>4</td>
</tr>
<tr>
<td>General Notes</td>
<td>5</td>
</tr>
<tr>
<td>Fixed Issues in Current 8.2R8.2 Release</td>
<td>5</td>
</tr>
<tr>
<td>Fixed Issues in Current 8.2R8.1 Release</td>
<td>6</td>
</tr>
<tr>
<td>Known Issues in Current 8.2R8.1 Release</td>
<td>6</td>
</tr>
<tr>
<td>New Features in 8.2R8 Release</td>
<td>6</td>
</tr>
<tr>
<td>Fixed Issues in Current 8.2R8 Release</td>
<td>7</td>
</tr>
<tr>
<td>Known Issues in Current 8.2R8 Release</td>
<td>9</td>
</tr>
<tr>
<td>Fixed Issues in 8.2R.7.2 Release</td>
<td>9</td>
</tr>
<tr>
<td>Fixed Issues in 8.2R7.1 Release</td>
<td>9</td>
</tr>
<tr>
<td>Fixed Issues in 8.2R7 Release</td>
<td>10</td>
</tr>
<tr>
<td>New Features in 8.2R6 Release</td>
<td>12</td>
</tr>
<tr>
<td>Fixed Issues in 8.2R6 Release</td>
<td>12</td>
</tr>
<tr>
<td>Known Issues in 8.2R6 Release</td>
<td>15</td>
</tr>
<tr>
<td>Fixed Issues in 8.2R5.1 Release</td>
<td>16</td>
</tr>
<tr>
<td>Known Issues in 8.2R5.1 Release</td>
<td>16</td>
</tr>
<tr>
<td>New Features in 8.2R5 Release</td>
<td>16</td>
</tr>
<tr>
<td>Noteworthy Changes in 8.2R5</td>
<td>18</td>
</tr>
<tr>
<td>Fixed Issues in 8.2R5 Release</td>
<td>18</td>
</tr>
<tr>
<td>Known Issues in 8.2R5 Release</td>
<td>19</td>
</tr>
<tr>
<td>New Features in 8.2R4 Release</td>
<td>23</td>
</tr>
<tr>
<td>Fixed Issues in 8.2R4 Release</td>
<td>23</td>
</tr>
<tr>
<td>Known Issues in 8.2R4 Release</td>
<td>24</td>
</tr>
<tr>
<td>New Features in 8.2R3 Release</td>
<td>24</td>
</tr>
<tr>
<td>Fixed Issues in 8.2R3 Release</td>
<td>26</td>
</tr>
<tr>
<td>Known Issues in 8.2R3 Release</td>
<td>27</td>
</tr>
<tr>
<td>New Features in 8.2R2 Release</td>
<td>30</td>
</tr>
<tr>
<td>Fixed Issues in 8.2R2 Release</td>
<td>31</td>
</tr>
<tr>
<td>Known Issues in 8.2R2 Release</td>
<td>32</td>
</tr>
<tr>
<td>Fixed Issues in 8.2R1.1 Release</td>
<td>34</td>
</tr>
<tr>
<td>New Features in 8.2R1 Release</td>
<td>35</td>
</tr>
<tr>
<td>Known Issues in 8.2R1 Release</td>
<td>37</td>
</tr>
<tr>
<td>Fixed Issues in 8.2R1 Release</td>
<td>41</td>
</tr>
<tr>
<td>Documentation</td>
<td>42</td>
</tr>
<tr>
<td>Documentation Feedback</td>
<td>42</td>
</tr>
</tbody>
</table>
Technical Support ................................................................................................................................. 42
Revision History ...................................................................................................................................... 42
Introduction

This document is the release notes for Pulse Connect Secure Release 8.2R8.2. This document contains information about what is included in this software release: supported features, feature changes, unsupported features, known issues, and resolved issues. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

Hardware Platforms

You can install and use this software version on the following hardware platforms:

- MAG2600, MAG4610, MAG6610, MAG6611, MAG SM160, MAG SM360
- PSA300, PSA3000, PSA5000, PSA7000F, PSA7000C

To download software for these hardware platforms, go to: https://www.pulsesecure.net/support/.

Virtual Appliance Editions

This software version is available for the following virtual appliance editions:

- Demonstration and Training Edition (DTE)
- Service Provider Edition (SPE)

The following table lists the virtual appliance systems qualified with this release.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Qualified System</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware</td>
<td>HP ProLiant DL380 G5 with Intel(R) Xeon(R) CPU</td>
</tr>
<tr>
<td></td>
<td>ESXi 6.0, 5.5U3, 5.5</td>
</tr>
<tr>
<td>KVM</td>
<td>CentOS 6.6 with Kernel cst-kvm 2.6.32-504.el6.x86_64</td>
</tr>
<tr>
<td></td>
<td>QEMU/KVM v1.4.0</td>
</tr>
<tr>
<td></td>
<td>Linux Server Release 6.4 on an Intel Xeon CPU L5640 @ 2.27GHz</td>
</tr>
<tr>
<td></td>
<td>24GB memory in host</td>
</tr>
<tr>
<td></td>
<td>Allocation for virtual appliance: 4vCPU, 4GB memory and 20GB disk space</td>
</tr>
<tr>
<td>Hyper-V</td>
<td>Microsoft Hyper-V Server 2012 R2</td>
</tr>
</tbody>
</table>

To download the virtual appliance software, go to: https://www.pulsesecure.net/support/.

Upgrade Paths

The following table describes the tested upgrade paths.

<table>
<thead>
<tr>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2Rx</td>
<td>You can upgrade to 8.2R8.2.</td>
</tr>
<tr>
<td>8.0Rx or 8.1Rx</td>
<td>You can upgrade directly to 8.2Rx simply by installing the 8.2Rx update.</td>
</tr>
<tr>
<td>Earlier than 8.0Rx or 8.1Rx</td>
<td>First upgrade to release 8.0Rx or 8.1Rx; then upgrade to 8.2Rx.</td>
</tr>
<tr>
<td>Pulse Secure Desktop 5.2Rx Client Software Upgrade</td>
<td>Refer to the Pulse Secure Desktop Client 5.2 release notes.</td>
</tr>
</tbody>
</table>
## General Notes

1. For policy reasons security issues are not normally mentioned in release notes. To find more information about our security advisories, please see our [security advisory page](https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40771).

2. In 8.2R1.1 and above, all PCS client access binaries (Network Connect, WSAM, Host Checker, JSAM, Windows Terminal Services, Citrix Terminal Services) are signed with a SHA-2 code signing certificate to improve security and ensure compatibility with Microsoft OS's 2016 restrictions on SHA-1 code signing. This certificate will expire on Jan 13, 2019.

3. Important note: Windows 7 machines must contain a March 10, 2015 Windows 7 Update in order to be able to accept and verify SHA-2-signed binaries properly. This Windows 7 update is described [here](https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40771) and [here](https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40771). If this update is not installed (in other words if a Windows 7 machine has not received an OS update since March 10, 2015), then PCS 8.2R1.1 and later will have reduced functionality (see PRS-337311 below). (As a general rule, Pulse Secure, LLC recommends that client machines be kept current with the latest OS updates to maximize security and stability).

4. In 8.2R1 and 8.2R1.1, the Pulse Linux client packages will not be available under the Admin installer’s page. However, the 8.1R7 Pulse Linux client is compatible with PCS 8.2R1 and 8.2R1.1. The previously downloaded/installed Pulse Linux clients will also work with 8.2R1 PCS.

5. In 8.2R2, the 8.1R8 Pulse Linux client package (both RPM and Debian packages) are available under the Admin installer's page.

6. You can also download the Pulse Linux client packages from the [Pulse Secure Licensing and Download Center](https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40771), under the download section for PCS 8.1R7 and 8.1R8.

7. When custom ciphers are selected, there is a possibility that some ciphers are not supported by the web browser. If any of ECDH/ECDSA ciphers are selected, they require ECC certificate to be mapped to the internal/external interface. If an ECC certificate is not installed, the admin may not be able to login to the appliance. The only way to recover from this situation is to connect to the system console and select option 8 to reset the SSL settings from the console menu. Option 8 resets the inbound SSL settings to the default settings. Any custom SSL settings are lost. This is applicable only to Inbound SSL settings.

8. Pre-5.0 Android and pre-9.1 iOS devices don't support Suite B ciphers. So, if Suite B is enabled, Pulse client on pre-5.0 Android and pre-9.1 iOS devices will not be able to connect to PCS device.

## Fixed Issues in Current 8.2R8.2 Release

Please refer to SA40771 for issues fixed in this release.

[https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40771](https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40771)
Fixed Issues in Current 8.2R8.1 Release

The following table lists issues that have been fixed and are resolved by upgrading to this 8.2R8.1 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-347074</td>
<td>Communication may be interrupted (IO_TIMEOUT) when using the Active Directory server type via DNS in large infrastructures.</td>
</tr>
<tr>
<td>PRS-353700</td>
<td>Unable to modify HC policy in the admin UI.</td>
</tr>
<tr>
<td>PRS-353804</td>
<td>Role based VLAN with source IP is not working.</td>
</tr>
<tr>
<td>PRS-352820</td>
<td>With high logging rates AD domain join failures might be seen.</td>
</tr>
<tr>
<td>PRS-353549</td>
<td>Admin user may get logged off with the encryption strength setting as PFS and enabling the packet capture.</td>
</tr>
</tbody>
</table>

Known Issues in Current 8.2R8.1 Release

The following table lists known issues in 8.2R8.1 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-354067</td>
<td>Admin user may get logged off if the ECC device certificate is not present and enable Encryption Strength as 'Suite B - Accept only Suite B ciphers'. <strong>Work around:</strong> Using CLI console, select option number 8 - ‘Reset allowed encryption strength for SSL’. This option will reset to the default security settings then admin login will be success.</td>
</tr>
</tbody>
</table>

New Features in 8.2R8 Release

The following table describes the major features that are introduced in 8.2R8 release.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FIPS 140-2 Level 1 compliance</td>
<td>Pulse Connect Secure on the PSA series appliances are now validated for FIPS 140-2 Level 1 compliance. Federal agencies protecting sensitive government data using cryptographic modules are mandated to use FIPS 140-2 validated technology. Pulse Secure MAG series appliances are already validated. For details, refer: <a href="http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2017.htm#2896">http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2017.htm#2896</a></td>
</tr>
<tr>
<td>SOH Host Checker Policy</td>
<td>Support for Custom Host Checker rule using Statement of Health via clientless Host Checker.</td>
</tr>
</tbody>
</table>
### Turkey time zone changes
Support for Turkey time zone changes. It is now marked as UTC +3.

### Fixed Issues in Current 8.2R8 Release
The following table lists issues that have been fixed and are resolved by upgrading to this 8.2R8 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Release Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-338370</td>
<td>Multiple VDI sessions cannot be launched through a browser using Pulse Secure Application Launcher.</td>
</tr>
<tr>
<td>PRS-349620</td>
<td>The html5acc-server daemon may generate a process snapshot (crash) if an invalid DNS entry is defined in an HTML5 bookmark.</td>
</tr>
<tr>
<td>PRS-340522</td>
<td>Host Checker policy/rule that has the customer Statement of Health (SoH) check fails from the web browser.</td>
</tr>
<tr>
<td>PRS-341933</td>
<td>Attempting to join a meeting using a dynamically generated URL from an external server may display an access forbidden message if the dynamic URL has a trailing slash in the reference host definition.</td>
</tr>
<tr>
<td>PRS-342154</td>
<td>SSH bookmarks may prompt to confirm the fingerprint of the SSH server being accessed.</td>
</tr>
<tr>
<td>PRS-345645</td>
<td>When using RADIUS authentication with challenge/token responses and an invalid passcode response is given, Pulse does not show initial login request.</td>
</tr>
<tr>
<td>PRS-346477</td>
<td>IKEv2 connections are dropped when using a Directory/Attribute server on the realm.</td>
</tr>
<tr>
<td>PRS-346515</td>
<td>Installed packages are set as the rollback version rather than the current version.</td>
</tr>
<tr>
<td>PRS-346565</td>
<td>Turkey time zone was not set correctly.</td>
</tr>
<tr>
<td>PRS-346863</td>
<td>SSL acceleration being enabled may cause the web server and cluster services to destabilize and fail to recover.</td>
</tr>
<tr>
<td>PRS-347025</td>
<td>Log archiving with SCP enabled may fail.</td>
</tr>
<tr>
<td>PRS-347421</td>
<td>XML import with periodic snapshot settings configured for a stop date may fail.</td>
</tr>
<tr>
<td>PRS-347479</td>
<td>The Pulse Connect Secure admin UI incorrectly reports the status of the PSA7000 power supply as “unknown”.</td>
</tr>
<tr>
<td>PRS-347583</td>
<td>IKEv2 tunnels get disconnected and users are unable to connect when tunnel setup rate is high.</td>
</tr>
<tr>
<td>Problem Report Number</td>
<td>Release Note</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>PRS-347729</td>
<td>Changing user passwords may not complete and cause users to fail connection establishment.</td>
</tr>
<tr>
<td>PRS-347787</td>
<td>Unable to delete resource profile bookmark from role.</td>
</tr>
<tr>
<td>PRS-347854</td>
<td>AD Domain join is successful but creation of key tab failed.</td>
</tr>
<tr>
<td>PRS-347945</td>
<td>Users may need to login and reauthenticate to continue using web browsing functionality after a cluster failover.</td>
</tr>
<tr>
<td>PRS-348281</td>
<td>GINA authentication fails for Network Connection when Host Checker is required.</td>
</tr>
<tr>
<td>PRS-349003</td>
<td>Executing SNMP commands was causing logs to be written to disk, thereby causing alerts for high disk usage.</td>
</tr>
<tr>
<td>PRS-349121</td>
<td>Using SNMP may cause disk usage warnings.</td>
</tr>
<tr>
<td>PRS-349373</td>
<td>Unable to do group search using Active Directory mode.</td>
</tr>
<tr>
<td>PRS-349450</td>
<td>The message regarding using Pulse Workspace could not be dismissed. This is now possible.</td>
</tr>
<tr>
<td>PRS-349453</td>
<td>The message regarding using Pulse One could not be dismissed. This is now possible.</td>
</tr>
<tr>
<td>PRS-349490</td>
<td>When user's logout, there is no recommendation to close the browser.</td>
</tr>
<tr>
<td>PRS-349666</td>
<td>License expiration may be reached sooner than expected in a cluster after a cluster split.</td>
</tr>
<tr>
<td>PRS-349684</td>
<td>The message for using Profiler cannot be dismissed; it can now be dismissed until the next upgrade.</td>
</tr>
<tr>
<td>PRS-349880</td>
<td>JSAM fails to be launched from Firefox.</td>
</tr>
<tr>
<td>PRS-350026</td>
<td>mailto links are rewriting incorrectly.</td>
</tr>
<tr>
<td>PRS-350169</td>
<td>When using the new UI, the logging disk utilization is erroneously labelled as disk utilization.</td>
</tr>
<tr>
<td>PRS-350225</td>
<td>Changing the OPSWAT version from V3 to V4 erroneously adjusts the name of the Mac OS Firewall policy.</td>
</tr>
<tr>
<td>PRS-350480</td>
<td>The virtual appliance is unable to switch console type between serial and VT.</td>
</tr>
<tr>
<td>PRS-350588</td>
<td>Unable to add IPv6 entry on Security-&gt;Health Check options page.</td>
</tr>
<tr>
<td>PRS-352820</td>
<td>With high logging rates AD domain join failures might be seen.</td>
</tr>
</tbody>
</table>
### Known Issues in Current 8.2R8 Release

The following table lists known issues in 8.2R8 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-347074</td>
<td>Communication may be interrupted (IO_TIMEOUT) when using the Active Directory server type via DNS in large infrastructures.</td>
</tr>
<tr>
<td>PRS-352890</td>
<td>Popup window does not close after Network Connect auto-launch. <strong>Symptom:</strong> Browser pop-up windows does not close after auto-launch. <strong>Statement:</strong> After auto-launch of NC, pop-windows does not close automatically. With this window, there is no functionality affected.</td>
</tr>
</tbody>
</table>

### Fixed Issues in 8.2R7.2 Release

The following table lists issues that have been fixed and are resolved by upgrading to this release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Release Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-351573</td>
<td>Resource access through Network Connect will fail after 90 seconds and will recover automatically.</td>
</tr>
</tbody>
</table>

### Fixed Issues in 8.2R7.1 Release

The following table lists issues that have been fixed and are resolved by upgrading to 8.2R7.1 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Release Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-350585</td>
<td>Administrators cannot download dsrecord trace files with an invalid access parameter message after stopping the recording.</td>
</tr>
</tbody>
</table>
## Fixed Issues in 8.2R7 Release

The following table lists issues that have been fixed and are resolved by upgrading to this release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Release Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-308251</td>
<td>Pulse does not support downgrade of ESAP version.</td>
</tr>
<tr>
<td>PRS-336990</td>
<td>Pulse iOS client does not reconnect correctly when the device wakes from sleep.</td>
</tr>
<tr>
<td>PRS-341063</td>
<td>Scheduled log archive may cause cluster splits.</td>
</tr>
<tr>
<td>PRS-341356</td>
<td>Pulse Collaboration Outlook plug-in fails to run on Outlook 2013 and 2016 with a runtime error.</td>
</tr>
<tr>
<td>PRS-342180</td>
<td>Network Connect unable to start in Mac OS 10.8 Japanese OS.</td>
</tr>
<tr>
<td>PRS-342408</td>
<td>HTML5 bookmarks are not synchronized between appliances when utilizing User Record Sync (URS) transaction.</td>
</tr>
<tr>
<td>PRS-342491</td>
<td>Citrix Listed Applications launches the ICA session using the profile credentials rather than the bookmark SSO credentials.</td>
</tr>
<tr>
<td>PRS-342887</td>
<td>Smart card authentication using WTS fails with &quot;The logon attempted failed&quot; error from non-domain windows machines due to NLA being enabled.</td>
</tr>
<tr>
<td>PRS-342731</td>
<td>VPN Tunneling daemon (dsagentd) may crash when using DHCP for IP assignment.</td>
</tr>
<tr>
<td>PRS-342896</td>
<td>Host Checker may fail to launch when the browser proxy configuration contains wildcards.</td>
</tr>
<tr>
<td>PRS-342992</td>
<td>Files with spaces in the name that are saved through Firefox using the file browsing feature are truncated to the space.</td>
</tr>
<tr>
<td>PRS-343826</td>
<td>XML export does not include “Windows 10” and “Windows 10 64-bit” for Host Checker predefined rule policies.</td>
</tr>
<tr>
<td>PRS-344340</td>
<td>Adding roles to a resource profile may cause previously added roles to be removed from the profile.</td>
</tr>
<tr>
<td>PRS-344457</td>
<td>Hyperlinks inside JIRA are rewritten incorrectly and cannot be clicked.</td>
</tr>
<tr>
<td>PRS-345223</td>
<td>User-created HTML5 bookmarks configured with &lt;PASSWORD&gt; fail to send the user password.</td>
</tr>
<tr>
<td>PRS-345415</td>
<td>Host Checker AV compliance check fails for McAfee Endpoint Security 10.1.</td>
</tr>
<tr>
<td>PRS-346051</td>
<td>RDP bookmarks configured for auto-launch are triggered multiple times when accessed through Edge.</td>
</tr>
<tr>
<td>Problem Report Number</td>
<td>Release Note</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>PRS-346124</td>
<td>LDAP Server Name/Address field does not allow hyphens.</td>
</tr>
<tr>
<td>PRS-346144</td>
<td>Seamless window and RemoteApp bookmarks fail to open when accessed through Chrome.</td>
</tr>
<tr>
<td>PRS-346153</td>
<td>Auto-launching Network Connect though Chrome does not work as expected (“Detected incorrect data from server” is displayed).</td>
</tr>
<tr>
<td>PRS-346204</td>
<td>Pulse One registration may require multiple attempts to complete.</td>
</tr>
<tr>
<td>PRS-346391</td>
<td>Pulse Mobile client for iOS does not connect correctly after sleep.</td>
</tr>
<tr>
<td>PRS-346524</td>
<td>DHCP release packets may not include the DHCP OPTION configured on the VPN Tunneling connection profile.</td>
</tr>
<tr>
<td>PRS-346796</td>
<td>RDP bookmarks configured for a seamless window may fail to launch from IE.</td>
</tr>
<tr>
<td>PRS-346821</td>
<td>HTML5 does not honor role-based VLAN/Source IP settings.</td>
</tr>
<tr>
<td>PRS-346836</td>
<td>HTML5 does not connect when NLA is configured and &quot;Warn on certificate problems&quot; is unchecked.</td>
</tr>
<tr>
<td>PRS-346924</td>
<td>Pulse Secure Application Launcher fails to complete auto-launch correctly with Chrome (“Detected incorrect data” warning).</td>
</tr>
<tr>
<td>PRS-346965</td>
<td>If a role is configured for only HTML5 access, the Pulse Secure ActiveX client is prompted for installation in the browser.</td>
</tr>
<tr>
<td>PRS-347037</td>
<td>Pulse Secure Application Launcher may fail to launch correctly on macOS machines.</td>
</tr>
<tr>
<td>PRS-347221</td>
<td>An HTTP500 error is presented to users if the resource configured for authorization only access is not enabled on the web ACL.</td>
</tr>
<tr>
<td>PRS-347276</td>
<td>Changing SSL options may cause the web process to fail.</td>
</tr>
<tr>
<td>PRS-347279</td>
<td>Adding a resource profile-based web bookmark to a role fails to save.</td>
</tr>
<tr>
<td>PRS-347333</td>
<td>If the UDP packet is fragmented, resource access may fail over Pulse or Network Connect.</td>
</tr>
<tr>
<td>PRS-347457</td>
<td>The option to save a resource profile-based web bookmark is not available when adding the bookmark on the role.</td>
</tr>
<tr>
<td>PRS-347489</td>
<td>Host Checker State of health policy is failing when automatic update is enabled.</td>
</tr>
<tr>
<td>PRS-347692</td>
<td>Protected resources are not accessible from Pulse or Network Connect if a negative cache is saved by the client OS.</td>
</tr>
<tr>
<td>Problem Report Number</td>
<td>Release Note</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------</td>
</tr>
<tr>
<td>PRS-347971</td>
<td>LDAP Server Name/IP Address field does not allow domain name with fourth level subdomain or greater.</td>
</tr>
<tr>
<td>PRS-348012</td>
<td>Swap memory graph may not display on the System&gt; Status &gt; Overview page.</td>
</tr>
<tr>
<td>PRS-348176</td>
<td>WSAM may crash when application bypass is configured.</td>
</tr>
<tr>
<td>PRS-348327</td>
<td>Adding a resource profile-based web bookmark to a role may cause an internal server error.</td>
</tr>
<tr>
<td>PRS-348329</td>
<td>After adding a web resource profile-based bookmark to a role, an array value may be displayed.</td>
</tr>
<tr>
<td>PRS-348744</td>
<td>Session database snapshot may not be saved.</td>
</tr>
<tr>
<td>PRS-349333</td>
<td>Admin user may not be able to login to a cluster with an invalid session warning.</td>
</tr>
<tr>
<td>PRS-349902</td>
<td>rewrite-server may crash during sustained heavy load.</td>
</tr>
</tbody>
</table>

**New Features in 8.2R6 Release**

The following table describes the major features that are introduced in 8.2R6 release.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| NLA feature           | Windows Terminal Service custom URLs can now be configured to enable or disable NLA by adding the following parameter at the end of the TS bookmark.  
"disablenla=yes" reverts to pre 8.1R7 behavior that disables NLA.  
"disablenla=no" enables NLA. (Introduced in 8.1R7)  
(Note that the above parameter should be added without double quotes.) |
| WSAM support on Redstone | On Windows 10 Redstone machine with UEFI and Secure Boot, WSAM client installs but does not work. User sees error message "A digitally signed driver is required". |
| HSTS support          | HTTP Strict Transport Security (HSTS) is now supported on PCS device.  
This is a web security policy mechanism which helps to protect websites against protocol downgrade attacks and cookie hijacking.  
If a user was able to access PPS with HSTS and later failed to access the I user may clear the browser cache before accessing the PPS again. |

**Fixed Issues in 8.2R6 Release**

The following table lists issues that have been fixed and are resolved by upgrading to this release.
<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Release Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-331942</td>
<td>Cloud Management menu item should not be seen in License Server Mode.</td>
</tr>
<tr>
<td>PRS-340377</td>
<td>Excessive cache events corresponding to batch device record deletions due to device records limit introduced with onboarding feature causing event server restarts.</td>
</tr>
<tr>
<td>PRS-340573</td>
<td>Validation of allowed servers (and ports) configuration in admin-UI for &quot;Role</td>
</tr>
<tr>
<td>PRS-340753</td>
<td>NC Bandwidth management in 8.1R8 has significant decrease in throughput as compared to 8.0R9.</td>
</tr>
<tr>
<td>PRS-340892</td>
<td>Cannot check out MS Office files on SharePoint 2013.</td>
</tr>
<tr>
<td>PRS-341801</td>
<td>Windows 10 Redstone Preview 10.0.14291 standalone WSAM not working (non-Pulse).</td>
</tr>
<tr>
<td>PRS-342017</td>
<td>WSAM does not work as expected with Bypass Application setting when specified Path for the executable.</td>
</tr>
<tr>
<td>PRS-342171</td>
<td>DMI restore RPC with mode=full does not configure IP settings.</td>
</tr>
<tr>
<td>PRS-343397</td>
<td>Pulse may fail to install after uninstalling when using Pulse WSAM.</td>
</tr>
<tr>
<td>PRS-343882</td>
<td>AAA &amp; WSAM: RADIUS accounting does not send consistent data for per-app/WSAM connections.</td>
</tr>
<tr>
<td>PRS-343915</td>
<td>Host Checker fails to load with 3rd Party Policy Check.</td>
</tr>
<tr>
<td>PRS-344196</td>
<td>Publisher name for PSIS is displayed incompletely in Control Panel.</td>
</tr>
<tr>
<td>PRS-344323</td>
<td>JSAM is popping up in two different windows after upgrading to 8.2RX.</td>
</tr>
<tr>
<td>PRS-344390</td>
<td>Toggling &quot;Dynamic Policy Evaluation&quot; option under Realm resets &quot;Maximum number of concurrent users&quot; under Realm &gt; Authentication Policy &gt; Limits.</td>
</tr>
<tr>
<td>PRS-344513</td>
<td>TNCS crash might with special characters in HC policy.</td>
</tr>
<tr>
<td>PRS-344520</td>
<td>Downloading Japanese and Chinese language files shows garbled characters in the filename.</td>
</tr>
<tr>
<td>PRS-344534</td>
<td>Unexpected failure with Host Checker policy for Machine Certificate validation due to expired certificate.</td>
</tr>
<tr>
<td>PRS-344583</td>
<td>WSAM Bypass Application does not work with Wildcard * specified in Filename.</td>
</tr>
<tr>
<td>Problem Report Number</td>
<td>Release Note</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>PRS-344771</td>
<td>Under certain situations, user is unable to disconnect a WSAM session using the signout command. User will see “unable to stop the Secure Application Manager” error.</td>
</tr>
<tr>
<td>PRS-344788</td>
<td>Support for Windows 10 Redstone.</td>
</tr>
<tr>
<td>PRS-344849</td>
<td>Windows Terminal Service custom URLs can now be configured to enable or disable NLA by adding the following parameter at the end of the TS bookmark.</td>
</tr>
<tr>
<td>PRS-344919</td>
<td>Specific traffic can cause high throughput, high CPU and multiple web crashes on the active node of an A/P cluster.</td>
</tr>
<tr>
<td>PRS-344992</td>
<td>Users are getting disconnected from their Session with “System process detected a Host Checker time out on host” logged in the user Access log</td>
</tr>
<tr>
<td>PRS-345052</td>
<td>HTML5 user created bookmark is not considered persistent data.</td>
</tr>
<tr>
<td>PRS-345081</td>
<td>HTML5 RDP sessions getting disconnected randomly.</td>
</tr>
<tr>
<td>PRS-345117</td>
<td>When PulseUI is launched by standard user in Linux, Host Checker does not check for process run in root account.</td>
</tr>
<tr>
<td>PRS-345193</td>
<td>8.2R5 checks for ive version in xml file breaking manageability via NSM.</td>
</tr>
<tr>
<td>PRS-345379</td>
<td>Windows 10/8 - DNS/Split Tunnel behavior needs to be added to Admin Guides and other related documents.</td>
</tr>
<tr>
<td>PRS-345466</td>
<td>Pulse One menu should be available in License Server Mode.</td>
</tr>
<tr>
<td>PRS-345516</td>
<td>Config downloader does not tolerate network faults; Pulse One is left spinning.</td>
</tr>
<tr>
<td>PRS-345529</td>
<td>Import of Root IVS Cluster Config using Option except IP Address on PSA displays IVS Menu.</td>
</tr>
<tr>
<td>PRS-345865</td>
<td>Import of configuration from Pulse One returned an Error: Failed to get top-level element name.</td>
</tr>
<tr>
<td>PRS-345890</td>
<td>When both auto-launch and custom start page are enabled, user is not redirected to custom start page after client launches when using Chrome browser.</td>
</tr>
<tr>
<td>PRS-345921</td>
<td>Need to correct hardware platforms supporting mgmt port.</td>
</tr>
<tr>
<td>PRS-345936</td>
<td>HTML5 RDP Guacamole Home Button should be configurable.</td>
</tr>
<tr>
<td>PRS-346591</td>
<td>Displaying Profiler banner in PCS.</td>
</tr>
<tr>
<td>Problem Report Number</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>PRS-346632</td>
<td>Program dsunity recently failed, continuously, after upgrade to 8.2R5HF4.</td>
</tr>
<tr>
<td>PRS-347316</td>
<td>Duplicate Terminal services profile may result in Internal error.</td>
</tr>
</tbody>
</table>

**Known Issues in 8.2R6 Release**

The following table lists Known issues in 8.2R6 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
</table>
| PRS-346749            | Redstone WSAM: Error seen while upgrading & WSAM in disconnected state.  
**Symptom:**  
Error seen while upgrading & WSAM in disconnected state.  
As part of uninstallation it is not able to stop samproxy which is the root cause.  
**Conditions:**  
If WSAM is upgraded from Pre-8.2R6 onwards to 8.2R6, we see this issue.  
This issue is not seen when upgraded from 8.2R6 to later release's.  
**Work Around:**  
Kill the Pre-8.2R6 WSAM process from task manager and upgrade to 8.2R6. |
| PRS-333669            | When connecting to connect6 using PSAL, certificate warning message is displayed even when certificate is valid.  
Following KB was published:  
https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB40171/?q=KB40171&l=en_US&fs=Search&pn=1&atype |
Fixed Issues in 8.2R5.1 Release
The following table lists issues that have been fixed and are resolved by upgrading to 8.2R5.1 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Release Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-342397</td>
<td>After upgrading, users are unable to connect – logs show error failed to set ACLs for users with NCIP x.x.x.x.</td>
</tr>
<tr>
<td>PRS-345212</td>
<td>Users are unable to login. They immediately receive message “Sorry your session has expired”.</td>
</tr>
<tr>
<td>PRS-345533</td>
<td>Make default ESAP version 3.0.3 on PPS and PCS.</td>
</tr>
<tr>
<td>PRS-346124</td>
<td>AAA: LDAP server name / address field does not allow hyphens in 8.2R5.</td>
</tr>
</tbody>
</table>

Known Issues in 8.2R5.1 Release
The following table lists Known issues in 8.2R5.1 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-341063</td>
<td>Occasionally, under heavy load condition, cluster split is observed after scheduled archiving is over. Cluster recovers immediately after split occurs.</td>
</tr>
<tr>
<td>PRS-346678</td>
<td>Pulse installation via browser installs Pulse but shows as Pulse service not running.</td>
</tr>
</tbody>
</table>

New Features in 8.2R5 Release
The following table describes the major features that are introduced in 8.2R5 release.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv6 support for DNS</td>
<td>DNS resolution for hostname with IPv6 addresses is supported from this release.</td>
</tr>
<tr>
<td></td>
<td>• Enables admin to configure DNS servers with IPv6 addresses.</td>
</tr>
<tr>
<td></td>
<td>• Allows applications to resolve IPv6 resources using DNS server.</td>
</tr>
<tr>
<td>IPv6 Support for Active Directory Server</td>
<td>Active Directory Standard mode authentication server is extended to support IPv6 based backend servers from this release. Authentication and Authorization features supported with IPv4 will work with IPv6. Dual mode, IPv4 only and IPv6 only based interfaces are supported with this feature.</td>
</tr>
<tr>
<td>IPv6 support for RADIUS</td>
<td>RADIUS authentication server is extended to support IPv6 backend server deployments. Authentication and Authorization features supported with IPv4 will work with IPv6.</td>
</tr>
</tbody>
</table>
### Feature

<table>
<thead>
<tr>
<th>Cloud Secure</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Pulse Cloud Secure technology provides seamless and secure access to cloud-based applications. With this PCS release, end users with iOS, Android mobile or Windows, and Mac desktops can now connect to enterprise cloud/SaaS applications through Single Sign-on. The following capabilities are available as a part of the Cloud Secure technologies:</td>
<td></td>
</tr>
<tr>
<td>• Single Sign-On to Cloud Applications like Salesforce, Dropbox with PCS as IDP through SAML assertion</td>
<td></td>
</tr>
<tr>
<td>• Office 365 Single Sign-On with PCS as IDP</td>
<td></td>
</tr>
<tr>
<td>• Compliance check and failure notification support with Pulse Workspace as MDM server for mobile devices and Pulse Client for desktop users.</td>
<td></td>
</tr>
<tr>
<td>• Role Based Access Control for the Cloud applications</td>
<td></td>
</tr>
<tr>
<td>• Dashboard support for cross platform visibility</td>
<td></td>
</tr>
</tbody>
</table>

| Google Authenticator 2FA Integration | This release supports TOTP authentication by using the Google Authenticator algorithm for generating shared secret keys and tokens. User can deploy Google Authenticator as a multi-factor authenticator within PCS. |
| • Google Authenticator works as an additional authentication mechanism. |
| • A new user can register in the following ways: |
| o Using single barcode: Click on “Scan Barcode” and then point your camera at the QR code on your computer screen. |
| o Using manual entry: Click on “Manual Entry” and enter the email address of your Google Account. Then, enter the secret key on your computer screen into the box next to the key and select "Done". |
| Currently, this feature is supported with-in a cluster boundary and cannot work with standalone that works behind load balancer. |

| Fault-tolerance for TCP and TLS Syslog Servers | PCS and PPS support sending admin-access, user-access, events and sensors logs to admin-configured syslog servers. Currently, if a TCP | TLS syslog server becomes unreachable (due to a network outage or due to a syslog server outage), the logs getting logged in PCS/PPS during this time are not sent to the syslog server. This feature helps the syslog server to recover the logs lost during a disconnect. The administrator can configure fault-tolerance on syslog serves by enabling this option from the admin UI. PPS/PCS reads the lost pending logs during a disconnect from the log disk and transports them to the syslog server on a reconnect. |

<p>| Mobility Support for IKEv2 authentication with EAP-TLS | IKEv2 EAP-TLS is a mutual authentication method that uses certificate based authentication mechanism. This release extends current IKEv2 EAP authentication framework to support EAP-TLS authentication method. Adding this feature support allows mobile devices supporting IKEv2 EAP-TLS to authenticate and securely connect to VPN. |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pulse Application Launcher for Firefox</td>
<td>The “Pulse Application Launcher” (PAL), which launches and installs Pulse Secure desktop clients via browsers without relying on Java or ActiveX technologies, has been enhanced to support the Firefox browser (release 45.0).</td>
</tr>
<tr>
<td>Integration with new OPSWAT SDK v4</td>
<td>Pulse Policy Secure leverages OPSWAT integration for endpoint desktop compliance evaluation. With this release the newer version of OPSWAT v4 will be used as the earlier version will be EOL by end of 2016. Note: Kindly ensure that all the servers and clients are upgraded prior to switching on the OPSWAT v4</td>
</tr>
</tbody>
</table>

**Noteworthy Changes in 8.2R5**

With OPSWAT v4 SDK new product support list is being worked upon and updated by OPSWAT periodically, which is delivered as part of ESAP. In case any issue observed related to compliance evaluation or remediation for any specific product, then do ensure that latest ESAP is applied or switch to OPSWAT v3 SDK.

**Fixed Issues in 8.2R5 Release**

The following table lists issues that have been fixed and are resolved by upgrading to 8.2R5 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Release Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCS-3384</td>
<td>Admin Log not updated when multiple monitor option is enabled/disabled.</td>
</tr>
<tr>
<td>PRS-340765</td>
<td>While using the floating toolbar for HTML5 access feature, you may notice a small black strip on the extreme right side of the browser. Moving the floating toolbar to the left will render it properly.</td>
</tr>
<tr>
<td>PRS-339514</td>
<td>Chrome browser does not go to home page automatically after user clicks on Terminal Service bookmarks. As a workaround, user need to manually click the link provided to go to home page.</td>
</tr>
<tr>
<td>PRS-339296</td>
<td>PCS does not send syslog traffic through internal port, if mgmt port is disabled.</td>
</tr>
<tr>
<td>PRS-341030</td>
<td>Cache cleaner doesn't clean up the Recycle bin and the folder data when we sign in and sign out from IE browsers.</td>
</tr>
<tr>
<td>PRS-340481</td>
<td>Watchdog restart webserver on setting encryption strength as Suite B and RSA cert is configured for internal port.</td>
</tr>
<tr>
<td>PRS-339052</td>
<td>PPS granular cipher: 8021.x is not honoring SSL settings configured in admin UI.</td>
</tr>
<tr>
<td>PRS-339434</td>
<td>XML Import of User Realm fails, if User-agent-pattern contains starting or trailing whitespaces.</td>
</tr>
</tbody>
</table>
### Problem Report Number

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Release Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-340387</td>
<td>Pulse and other clients cannot be launched from chrome browser when PFS or SuitB ciphers are being used on the 8.2R3 SA and end users already have older version of Pulse application launcher installed on their machines.</td>
</tr>
<tr>
<td>PRS-341306</td>
<td>In the situation that &quot;weak ciphers not allowed&quot; option is disabled before upgrading to 8.2R3, configuration is exported before any update to the ciphers, this exported configuration would fail to be imported again later.</td>
</tr>
<tr>
<td>PCS-4045</td>
<td>HTML5 Error messages which get displayed after session disconnect are not localized.</td>
</tr>
<tr>
<td>PRS-341379</td>
<td>End-user cannot install host checker component and Pulse Client using Firefox ESR 45.</td>
</tr>
<tr>
<td>PRS-330382</td>
<td>Intermittent false positive SNMP alert as ifAdminStatus down.</td>
</tr>
<tr>
<td>PRS-341268</td>
<td>&quot;Disable external interface when internal interface fails&quot; option is not working.</td>
</tr>
</tbody>
</table>

### Known Issues in 8.2R5 Release

The following table lists Known issues in 8.2R5 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-343499</td>
<td>Warning or Error message may not be seen while disabling IPv6 on management port or disabling port from Admin UI or through XML import. This happens when AAA traffic over management port is configured for Administrative network.</td>
</tr>
<tr>
<td>PRS-342734</td>
<td>Configuration Mismatch happens when HTML5 Access is selected in User Role (upgrade bug).</td>
</tr>
<tr>
<td>PRS-342551</td>
<td>Import of security/ssl-options XML from older (7.x/8.1) version on to 8.2R5 causes &quot;Custom cipher does not match the available selection&quot; error.</td>
</tr>
<tr>
<td>PRS-339873</td>
<td>When the login to Node A is not followed by a clean logout and closure of the browser, a login of the same user to Node B does not reflect recently deleted bookmarks in the user session. Instead, the bookmarks from Node B get synced back to Node A. This happens whenever there is a warning that 'User Record Synchronization' is in progress.</td>
</tr>
<tr>
<td>PCS-4584</td>
<td>With Legacy NC client, QR code will not be shown in TOTP registration page. As workaround users need to enter secret key manually.</td>
</tr>
<tr>
<td>PCS-4579</td>
<td>Syslog FT: Need to provide drop-down box for configuring FT settings for all the cluster members.</td>
</tr>
<tr>
<td>Problem Report Number</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>PRS-342154</td>
<td>SSH rewriting prompts to accept fingerprints of SSH server. There is no functional impact and the workaround is to accept the prompt and proceed with the connection.</td>
</tr>
<tr>
<td>PRS-343579</td>
<td>During reboot, sequence of timing may lead to pareventd process crash, but there is no user impact.</td>
</tr>
<tr>
<td>PRS-345028</td>
<td>After importing binary user config, the device might be unreachable. This is an intermittent issue and admin will need to restart services to bring the device back up.</td>
</tr>
<tr>
<td>PCS-4583</td>
<td>When TOTP auto-unlock feature is enabled, the locked out TOTP users will be automatically unlocked only upon their next login attempt after lock period expires.</td>
</tr>
<tr>
<td>PCS-4584</td>
<td>With Legacy NC client, QR code will not be shown in TOTP registration page. As workaround users need to enter secret key manually.</td>
</tr>
<tr>
<td>PRS-344821</td>
<td>When accounting is enabled for PCS then for WSAM users accounting stop message may not be sent for WSAM session.</td>
</tr>
</tbody>
</table>
|                       | **Symptom:**<br>Host-Checker fails to launch on Mac OS.  
**Conditions:**<br>If custom sign-in pages from pre-8.2R5 is used, and the pulse connect secure is upgraded to 8.2R5 or later.  
**Work Around:**<br>After upgrading to 8.2R5 or later, if Custom sign-in pages are used, it is required for the Admins to download the new sample.zip file from Authentication->Sign in->Sign-in-Page, merge your changes in new custom sign-in page, and upload the modified file. |
| PRS-341802           | User may not be able to use WSAM on Windows Redstone.  
This is the restriction of driver signing imposed by operating system.  
Workaround is there but since it is risky for system it is not recommended. |
<p>| PRS-338371           | Whenever two VDI terminals are opened in chrome/Firefox/Edge one after the other, the second VDI terminal shuts the first one. This means, we can access only the second VDI terminal but not the first one. Note that this issue will occur when working on chrome/Firefox/Edge which is using the PSAL component for launching clients. There is no problem in opening two VDI terminals in IE. |
| PRS-336184           | Whenever PCS’s end user configuration is set to Chinese simplified, and PSAL is opened through Chrome browser on a Chinese PC, the characters on the PSAL dialog box appear in Chinese traditional but not Chinese simplified. |
| PRS-343838           | Certificate authentication configuration for Linux client is not supported and might result in a crash on cent OS 6.4. |</p>
<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-344167</td>
<td>Auto uninstall of NC might fail due a timing issue. Workaround is to try the sign-out operation second time.</td>
</tr>
<tr>
<td>PRS-343759</td>
<td>For Cloud Secure, in case for a single PWS user with more than 5 devices are registered, then for that specific user the authentication token may not get pushed to the mobile device resulting to failure in o365 access.</td>
</tr>
<tr>
<td>PRS-342249</td>
<td>For Cloud Secure, on Windows 10 desktop the PSAL has to be pre-installed for seamless SSO access of the thick applications.</td>
</tr>
<tr>
<td>PRS-344470</td>
<td>In the Cloud Secure dashboard, the statistical chart data represents the cloud applications specific information and not the ECP flow data of o365 access on mobile devices.</td>
</tr>
<tr>
<td>PRS-303232</td>
<td>Live upgrade of IF-MAP server is not supported and will cause downtime. An upgrade should be scheduled for off hours, a time when the minimum number of users will be affected.</td>
</tr>
<tr>
<td>PRS-324568</td>
<td>Guest user sessions are reported as &quot;802.1x Auth&quot; in &quot;Auth Mechanism&quot; chart on dashboard.</td>
</tr>
</tbody>
</table>
| PRS-342658            | **Symptom:** Some of the syslogs are not received in the TCP | TLS syslog server after a reconnect.  
**Conditions:**  
- Fault Tolerance feature is enabled for the TCP | TLS syslog server  
- TCP | TLS syslog server is down, and comes back after a while  
- PCS/PPS retransmits the syslogs generated during the syslog server downtime  
- New logs are generated when the PCS/PPS is retransmitting the pending logs |
| PRS-342845            | IOS user when tries to join secure meeting it fails. They see an error "Exceeds license for number of users".                              |
| PRS-343655            | Samba diagnostic log to troubleshoot Active Directory Server will log "NT_STATUS_INTERNAL_ERROR" when using Kerberos only Authentication protocol.  
It will not harm the functionality of Active Directory Server features with this error logging. |
<p>| PRS-344139            | Configuration distribution of 'Pulse Collaboration' using Pulse One may fail with an error &quot;Please specify a Room for the Meeting Name&quot;. A workaround is to not include 'Pulse Collaboration' in the configuration settings used for the group by editing the appliance group from the Pulse One console, and try configuration distribution again. |
| PRS-342944            | Configuring DNS servers with IPv6 addresses for Layer 3 VPN tunneling is not supported.                                                |</p>
<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-309431</td>
<td>With OPSWAT Patch Management Host Checker policy, the missing patches will be detected only with admin privileges for SCCM 2012 and SCCM 2007.</td>
</tr>
<tr>
<td>PRS-318679</td>
<td>For Host Checker with BitLocker Encryption software, the encrypted drives will be reported as encrypted only when these drives are in Unlocked state.</td>
</tr>
<tr>
<td>PRS-339456</td>
<td>In some Windows machines it takes around 20 minutes for detecting missing patches, which is the Microsoft OS behavior. The same will be observed with Host Checker Patch Management policy evaluation as well.</td>
</tr>
<tr>
<td>PRS-344555</td>
<td>When the same Pulse Client is connected to multiple PPS/PCS servers with different OPSWAT versions 3 and 4, then the compliance evaluation would be done using the server configured OPSWAT version. The compliance evaluation will be conducted in sequence as for each server connection respective server specific version will be downloaded. It's recommended to switch on the OPSWAT v4 SDK post all the servers are upgraded.</td>
</tr>
<tr>
<td>PRS-343928</td>
<td>With V3 and V4 SDK, we require admin privileges to turn on the MAC In Built firewall as part of remediation.</td>
</tr>
<tr>
<td>PRS-343232</td>
<td>BitLocker Encryption status won't get detected if we run with restricted user privileges on Windows machine.</td>
</tr>
</tbody>
</table>
| PRS-345193            | **Symptom:** Unable to manage PCS config through NSM. PCS returns 'No IVE data Version' rpc error.  
**Conditions:**  
PC is running 8.2R5 and later  
NSM Admin trying to change PCS config and trying to update device through the NSM Client.  
**Workaround:** None |
| PRS-344807            | With Google Chrome browser, Host Checker failures does not change the role on PPS until Host Checker times out. |
| PRS-341063            | Cluster may split during archiving. In the situation when cluster did split, it recovers within a minute. The probability of cluster split is higher in the situation where additional Pulse package is uploaded to PCS, and User Record is scheduled to be archived at the same time as one or more items in the archive configuration page. To work around this issue, the following is recommended: 1. Remove unnecessary Pulse client package from PCS. The Pulse client package can be downloaded from Pulse Secure support site whenever it is needed; 2. Schedule archiving in a way that each selectable item in the archive configuration page is archived at different time – either different hour of the day, or different day of the week. Resolution for this issue is been worked on and will be released soon. |
| PRS-342396            | In 8.2, if there is one or more role configured with 2000+ ACLs, after users from the role with 2000+ ACLs establish VPN connection, users from the next role unable to establish VPN tunnel. Resolution for this issue is been worked on and will be released soon. |
New Features in 8.2R4 Release

The following table describes the major features that are introduced in this release.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Changes made to be compliant with NDcPP certification | 1. When NDcPP option is enabled, only NDcPP allowed crypto algorithms are allowed.  
2. Device certification 3072 bit key length support  
3. Device certification revocation check  
5. Note: NDcPP certification in progress. |
| Pulse Linux client UI | The Pulse Linux client now supports the following operations to be done through the UI.  
1. Connection management (add/edit/delete connections)  
2. Connect/disconnect to VPN  
3. Check VPN status and statistics  
4. Upload logs to PCS  
5. Configure the client log level |
| Support for multifactor authentication with Pulse Linux client | Pulse Linux client has been qualified for the following MFA mechanisms.  
1. RSA (software token and hardware token)  
2. Duo Security  
3. Safenet  
4. But the Pulse Linux should be able to support other MFA methods too as the client uses web based UI to authenticate into the PCS |
| Support for system proxy in command line mode | Pulse Linux client supports the system proxy in the following modes.  
1. Manual configuration  
2. Auth proxy  
3. Pac file configuration  
In this release, there are some limitations in running the Pulse Linux client in UI mode with system proxy configured. Command line mode of the client does not have those limitations and it works. |

Fixed Issues in 8.2R4 Release

The following table lists issues that have been fixed and are resolved by upgrading to this release.
Problem Report Number | Release Note
--- | ---
PRS-337187 | Dsserver tasks issues seen and they are having timeout/disconnect issues for Pulse Mobile

PRS-340595 | PCS reports it cannot verify Pulse One certificate despite correct certificate was loaded.

PRS-339030 | Some Pulse users are unable to access resources intermittently.

PRS-342088 | After 8.2R3 ran a few days without user access, there is a bug causes admin and user unable to login.

### Known Issues in 8.2R4 Release

The following table lists Known issues in 8.2R4 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-341792</td>
<td>When CA Certificate Policy is set to fail that causes the certificate authentication through other CAs to fail.</td>
</tr>
<tr>
<td>PRS-341773</td>
<td>Adding a connection with duplicate name closes the connection creation window after the warning in Pulse Linux client.</td>
</tr>
<tr>
<td>PRS-341921</td>
<td>Pulse Linux client does not automatically reconnect during the network outages.</td>
</tr>
</tbody>
</table>

### New Features in 8.2R3 Release

The following table describes the major features that are introduced in 8.2R3 release.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Support proxy Authentication for JSAM when using NTLM</td>
<td>Previously JSAM component is unable to establish a connection with a backend server when a proxy server is present in the middle. With this feature, this limitation will be removed and JSAM will be able to handle the proxy authentication challenge from the proxy server successfully.</td>
</tr>
<tr>
<td>Secure Access - Support for Dual monitor configuration when using Windows Terminal Services</td>
<td>User should be able to stretch the display into multiple monitors. Admin will be able to configure the option as part of RDP profile selection.</td>
</tr>
<tr>
<td>RSA Risk Based Authentication(RBA) support with PCS Cluster</td>
<td>RSA SecurID Risk-Based Authentication is a token less, multi-factor enterprise authentication solution that uses risk scoring to determine that users are who they say they are while preserving the username and password login experience. Provides a token alternative – token less authentication is a convenient way for your users to authenticate securely, via a web interface, without the need for a token.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>Secure Access - Support for Hyper-V hypervisor</td>
<td>Hyper-V is another hypervisor that we must support as part of extended platform support for virtual appliances. Note: Kernel Watchdog is not supported on Hyper-V platforms. In PCS/PPS, on Maintenance-&gt;system-&gt;options page kernel watchdog checkbox is grayed out. Transition or first step to provide Azure support.</td>
</tr>
</tbody>
</table>
| Cloud Secure – Solution Tech Preview | Pulse Cloud Secure technology provides secure access to the cloud, while offering additional benefits. With this PCS release, we are delivering Cloud Secure tech preview. End user with iOS devices can now connect to enterprise cloud/SaaS application in a seamless and secure fashion. Following capabilities are available as part of Cloud Secure technologies:  
- Single Sign On of Cloud Applications like Salesforce, Dropbox with PCS as IDP through SAML assertion  
- Office 365 Single Sign On with PCS as IDP (through SAML ECP support)  
- PulseOne as MDM server integration with PCS to provide compliance check of iOS device during authentication |
| Cloud Secure - SAML changes for Secure Access | 1. SA Admin, can configure SA as IdP for SAML SSO easily.  
2. End users can do SSO in the application without being prompted for passwords.  
3. End user can login to end application behind rewriter/PTP on being redirected from Enterprise Landing Page. |
| Granular Cipher Configuration | This feature provides ability to select specific ciphers and order the ciphers with preference orders. There is an Inbound SSL option tab as well as an Outbound SSL option tab. The Inbound SSL tab controls all incoming SSL traffic; the Outbound SSL option controls the outbound SSL connections from PCS: connection to SCEP server, Syslog server, and rewriter and ActiveSync connections. |
| HTML5 RDP – End User can create HTML5 access bookmarks | This feature allows the end user to create and edit bookmarks and access them over RDP via HTML5. When an admin enables this feature, the end user can perform the following:  
- Create/Update bookmarks  
- Enable/Disable SSO based Authentication  
- Enable/Disable accessing resource operation like file transfer, printing etc.  
- Select the Encryption type  
- Set the remote program options.  
Note that creating HTML5 based user bookmarks for Terminal services sessions is not supported on mobile devices, however end users can create these from a Windows or Mac machine and access the bookmarks from your mobile device. |
| Third Party Applications Support | Currently support of following applications:  
- Policy Server 12.5 SP3/SP4 |
Enhance UX - Fail open if certificate used for signing jar files has expired.

User will be able to launch PCS jar files even if the certificate expired but were signed when the certificate had a valid timestamp.

Fixed Issues in 8.2R3 Release

The following table lists issues that have been fixed and are resolved by upgrading to 8.2R3 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Release Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-338476</td>
<td>In the admin UI, longer role names are not completely visible under available roles on resource policy page.</td>
</tr>
<tr>
<td>PRS-339141, PRS-338701, PRS-339321, PRS-339405, PRS-339133, PRS-339161</td>
<td>Enabling Suite B or PFS option causes some clients fail to connect to PCS. Known clients that fail to connect include but not limited to the following: Network Connect client, Pulse Collaboration client, WSM client, VDI client, Host Checker, WTS client and Pulse Mobile Android version 4.4.4. A warning will be added in the future on the configuration page to alert admin of the potential.</td>
</tr>
<tr>
<td>PRS-339254</td>
<td>3072 bit is shown erroneously as one of the possible key length for certificate.</td>
</tr>
<tr>
<td>PRS-339328</td>
<td>FIPS ON Mode allows RC4 Ciphers in TLS1.1 and TLS1.2 Custom Settings.</td>
</tr>
<tr>
<td>PRS-339024</td>
<td>On Windows 10, unable to launch previous component (prior to 8.2) when 8.2 Installer Service is installed.</td>
</tr>
<tr>
<td>PRS-336902</td>
<td>If you download Pulse 5.2 package from the my.pulsesecure.net site, then upload it to your PCS, then make it your active version, then browse to: Maintenance &gt; System &gt; Installers and attempt to download either the Windows or Mac Pulse installer, you will see a blank white page and no client installer will be downloaded.</td>
</tr>
<tr>
<td>PRS-340498</td>
<td>Citrix listed Apps are not launching with IE and FF.</td>
</tr>
<tr>
<td>PRS-340349</td>
<td>CTS custom ICA bookmark with SSO does not work.</td>
</tr>
<tr>
<td>PRS-340253</td>
<td>NC service not starting after upgrading from 7.1R2.</td>
</tr>
<tr>
<td>PRS-339600</td>
<td>Domain name parameter is not passed for WTS after upgrading to 8.2R1.1.</td>
</tr>
<tr>
<td>PRS-337893</td>
<td>Remote App is not launching when the &quot;Launch seamless window&quot; option is set on WTS bookmark.</td>
</tr>
</tbody>
</table>
### Problem Report Number

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-337999</td>
<td>Support for configuring RDP with custom port.</td>
</tr>
<tr>
<td>PRS-336856</td>
<td>Suppressing the certificate warning for the WTS.</td>
</tr>
<tr>
<td>PRS-338691</td>
<td>Non-authenticated users were unable to join meeting with &quot;Edge&quot; and &quot;Chrome&quot; browser in absence of Pulse Secure Application Launcher already installed on the PC. <strong>Workaround:</strong> User can manually download and install Pulse Application Launcher from the meeting-join page.</td>
</tr>
<tr>
<td>PRS-337378</td>
<td><strong>Problem:</strong> Pulse Connect Secure gateways version 8.2 and later are unable to web-deploy version 5.1 and earlier Pulse Secure desktop clients. <strong>Symptoms:</strong> When attempting to web-deploy a pre-5.2 Pulse desktop client from an 8.2 PCS gateway, the end user's web browser will hang on &quot;Launching Pulse Secure&quot;. <strong>Workaround:</strong> There are a number of recommended workarounds: 1. Install the Pulse Secure 5.1RX client using the MSI file, then connect to 8.2R1. This could be done either by manually invoking the MSI file, or, by leveraging a software distribution system like SMS. 2. Connect to a 8.1RX PCS gateway and get Pulse 5.1RX web deployed, then connect to an 8.2R1 gateway after deployment.</td>
</tr>
</tbody>
</table>

### Known Issues in 8.2R3 Release

The following table lists Known issues in 8.2R3 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-340573</td>
<td>In admin UI, &quot;Allowed servers (and ports)&quot; configuration from &quot;Role</td>
</tr>
<tr>
<td>PCS-3384</td>
<td>Admin Log not updated when multiple monitor option is enabled/disabled.</td>
</tr>
<tr>
<td>PRS-340760</td>
<td>HTML5 RDP If you have switched your primary and secondary mouse clicks of the mouse, HTML5 access feature does not recognize these changes.</td>
</tr>
<tr>
<td>Problem Report Number</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>PRS-340765</td>
<td>While using the floating toolbar for HTML5 access feature, you may notice a small black strip on the extreme right side of the browser. Moving the floating toolbar to the left will render it properly.</td>
</tr>
<tr>
<td>PRS-339514</td>
<td>Chrome browser does not go to home page automatically after user clicks on Terminal Service bookmarks. As a workaround, user need to manually click the link provided to go to home page.</td>
</tr>
</tbody>
</table>
| PRS-339296            | **Symptom:**
PCS does not send syslogs to remote syslog server.

**Conditions:**
1) Management port is enabled on the PCS.
2) PCS connects to Remote Syslog Server through management port.
3) Admin disables management port.
4) PCs is expected to send traffic through internal port. However, it does not.

**Workaround:**
Make changes in any of the syslog server entries (eg. change facility or connection type). This should trigger the PCS to re-establish the connection with the Syslog Server, and start sending syslogs. |
| PRS-341030            | **Symptom:** Cache cleaner doesn't clean up the Recycle bin and the folder data when we sign in and sign out from IE browsers.

**Conditions:**
1) Create a cache cleaner policy to empty the recycle bin and custom folders.
2) From the endpoint, connect to PCS from IE browser and then sign out.
3) Cache cleaner doesn't clean up the Recycle bin and the custom folders |
| PRS-334398            | **Symptom:**
Guest OS name shows as Other Linux(32bit) for VA-SPEs deployed on VMware ESXi

**Conditions:**
PCS running pre-8.2 and deployed on VMware ESXi, and upgraded to 8.2.

**Workaround:**
It is only a display issue. Kernel would be upgraded to 64-bit after upgrade to 8.2.
Freshly deployed VA-SPE using 8.2 OVF will not exhibit this issue. |
| PRS-339295            | **Symptom:**
PCS does not send syslogs to remote syslog server

**Conditions:**
1) Management port is enabled on the PCS. |
<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
</table>
| PRS-340481            | 2) PCS connects to Remote Syslog Server through management port.  
3) Admin disables management port.  
4) PCs is expected to send traffic through internal port. However, it does not.  
**Workaround:**  
Make changes in any of the syslog server entries (e.g. change facility or connection type). This should trigger the PCS to re-establish the connection with the Syslog Server, and start sending syslogs. |
| PRS-341029            | When Suite B is enabled, only ECC ciphers were enabled. At this point, ECC certificate must be configured for all ports, including internal ports. If RSA certificate is configured for internal port by mistake, this prevents any connections to PCS, including watchdog connection. Because Watchdog fails to connect to webserver, it thinks webserver is unresponsive thus restarts webserver. |
| PRS-338642            | Cache cleaner does not perform the cleaning when user signs out from IE browser. If user connects and signs out from PCS again, then the cleaning is performed. |
| PRS-339052            | When CC Proxy with NTLM authentication is configured with domain\user, user will not be able to access resources via JSAM. |
| PM-1972               | Pre-5.0 Android and pre-9.1 iOS devices don't support Suite B ciphers. So, if Suite B is enabled, Pulse client on pre-5.0 Android and pre-9.1 iOS devices will not be able to connect to PCS device. |
| PRS-339434            | PPS granular cipher: 8021.x is not honoring SSL settings configured in admin UI.  
**Symptom:** XML Import of User Realm fails, if User-agent-pattern contains starting or trailing whitespaces  
**Workaround:**  
1. If user agent has a trailing space, add a leading space also.  
2. If user agent has a leading space, add a trailing space also.  
This will ensure the XML import goes through.  
This will not be seen if the user-agent-pattern does not have any trailing/leading spaces also. |
| PRS-340387            | The PSAL client installed in previous release (before 8.2R3) doesn't support Suite B or PFS ciphers, thus auto-upgrade to 8.2R3 doesn't work. If user had PSAL clients installed, there are two options:  
1. Do not enable PFS or Suite B ciphers until all users upgraded PSAL to 8.2R3 version.  
2. User must download PSAL from a 8.2R4 PCS device and install manually. |
### Problem Report

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-341306</td>
<td>In the situation that “weak ciphers not allowed” option is disabled before upgrading to 8.2R3, configuration is exported before any update to the ciphers, this exported configuration would fail to be imported again later. To work around this issue, 1) make a modification on the cipher selection page; or 2) manually update the value of “weak ciphers not allowed” in XML file to be enabled.</td>
</tr>
<tr>
<td>PRS-339683</td>
<td>Cloud Secure dashboard is not displaying failed App details.</td>
</tr>
<tr>
<td>PCS-4045</td>
<td>HTML5 Error messages which get displayed after session disconnect are not localized.</td>
</tr>
<tr>
<td>PRS-341427</td>
<td>When launching HC on MAC using the safari browser, at times if PSAL download prompt is looping then kill the PSAL process and launch the HC again.</td>
</tr>
<tr>
<td>PRS-341379</td>
<td>End users logging in from Firefox ESR browser using java delivery (Firefox version 45 and above + Java 8 Update 91) will see prompt to save Setup Client Installer if Host Checker is configured. They can save and cancel the installer file and click on the link “Once java is installed and enabled, please Click here to continue” for continuing the login.</td>
</tr>
<tr>
<td>PRS-340749</td>
<td>If a user with restricted permissions creates a Secure Meeting and attempts to allow a remote user to control a window associated with privileged process (the “Grant Control” function), the remote user will not be able to manipulate that privileged window.</td>
</tr>
</tbody>
</table>

### New Features in 8.2R2 Release

The following table describes the major features that are introduced in 8.2R2 release.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux command line client Host Checker</td>
<td>This Pulse Secure Linux Client feature is to support java-free host checking functionality on Linux. Pulse Secure Linux Client checks endpoint properties for file, process and port rule types to allow access to protected resources. Pulse Secure Linux Client. Host Checker functionality complies with the standards produced by the Trusted Network Connect (TNC) subgroup of Trusted Computing Group.</td>
</tr>
<tr>
<td>Custom Sign-in Page</td>
<td>The 8.2R2 Pulse Connect Secure gateway now supports custom sign-in pages for the Pulse Secure desktop client. (Previously, custom-sign-in pages were supported only for the Network Connect client.) Custom sign-in pages allow for the creation of HTML authentication and password-management screens to provide customized localization, online help, error messages, server redirection, and page styles using CSS (cascading style sheets). This new support for the Pulse desktop client is identical</td>
</tr>
</tbody>
</table>
### Feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>to that of the custom-sign-in-page support in the Network Connect client.</td>
<td></td>
</tr>
<tr>
<td>VMWare Horizon view client 2.x and 3.x support</td>
<td>In this release, user can launch virtual desktop using Horizon view client 2.x or 3.x</td>
</tr>
</tbody>
</table>

### Fixed Issues in 8.2R2 Release

The following table lists issues that have been fixed and are resolved by upgrading to 8.2R2 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Release Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-322363</td>
<td>Webserver process restarts under heavy load.</td>
</tr>
<tr>
<td>PRS-329411</td>
<td>The user access log may show a mismatched logged in username between ActiveSync user and PCS username.</td>
</tr>
<tr>
<td>PRS-331805</td>
<td>Online help for Network Connect on MAC OSX is missing.</td>
</tr>
<tr>
<td>PRS-332212</td>
<td>For Network Connect and Pulse VPN users, if a user session ends during a DHCP renew transaction, a process crash may occur causing IP addresses to not be provisioned from the DHCP server.</td>
</tr>
<tr>
<td>PRS-333721</td>
<td>The Network Connect GINA tile is not present on Windows 10 clients.</td>
</tr>
<tr>
<td>PRS-334156</td>
<td>Improved Pulse One related error messages in the event log.</td>
</tr>
</tbody>
</table>
| PRS-334161            | When using the following rewriter settings, a POST request results in an Internal Server Error:  
|                       |   - Unrewritten pages open in new window  
|                       |   - Action = Don't rewrite (with redirect)                                   |
| PRS-335285            | While connecting from Pulse client after session resumption, realm information is missing from user access logs. |
| PRS-335517            | System snapshot failing intermittently from serial console, whereas it works fine through the admin UI. |
| PRS-336161            | The configuration XML that is uploaded to Pulse One is not consistent, causing Pulse One to see configuration changes or conflicts which do not actually exist. |
| PRS-336255            | Internal error seen when saving changes under User Roles --> Files --> Options page for Roles with Files options disabled |
| PRS-336378            | When using the rewriter, uploading attachments in Lotus Notes 9 fails when using Internet Explorer. |
## Problem Report Number

### Release Note

**PRS-336944**  
XML Import of LDAP Server duplicates the user-attributes. This issue can cause issues with Pulse One being out of sync with the master appliance.

**PRS-337120**  
When VLAN/source IP is set on the role, accessing protected resources fails.

**PRS-337315**  
XML import fails when Pulse One tries to distribute a SAML authentication server.

**PRS-337334**  
User attributes in the hostname/IP field for HTML5 RDP bookmarks is not supported.

**PRS-337496**  
Registering with Pulse One may result in slow memory leak.

**PRS-337742**  
Options in user role and XML schema for HTML5 Access are missing.

**PRS-337752**  
Unable to connect with Windows Terminal Services (WTS) using a custom port (other than port 3389).

**PRS-337870**  
Google font style (Oxygen) used in the new admin interface requires the device to have access to the Internet.

**PRS-337911**  
Pre-authentication sign-in notification appears twice when custom sign-in page is used.

**PRS-337924**  
VPN users that are mapped to roles which are configured with ACLs containing IP ranges are unable to establish a VPN tunnel.

**PRS-338062**  
PCS shows a blank page with "Content-type: text/html" during login.

## Known Issues in 8.2R2 Release

The following table lists Known issues in 8.2R2 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-339822</td>
<td>If a system configuration file that does not contain Pulse One registration data is imported into a PCS appliance that is registered with Pulse One then the resulting appliance will not be registered with Pulse One but will have Pulse One related processes running. These extraneous processes can impact performance on the device. We therefore recommend that you Clear Configuration on the Pulse One Settings page in the admin console before importing the system configuration file.</td>
</tr>
<tr>
<td>PRS-338204</td>
<td>Active VDI sessions are not listed in SA admin &quot;Active Virtual Desktop Sessions&quot; if end user connects with Horizon view client 2.x or 3.x</td>
</tr>
<tr>
<td>Problem Report Number</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>PRS-338370</td>
<td>Users are unable to connect to multiple VDI or Terminal Service bookmarks when logged in using the Chrome browser.</td>
</tr>
<tr>
<td>PRS-338646</td>
<td>With View 3.x client users are not able to enter valid credentials if SSO fails.</td>
</tr>
<tr>
<td>PRS-338270</td>
<td>View client 3.x fails to launch virtual desktop if proxy is configured in client machine. This is a VMWare Limitation. Here is the KB from VMWare: <a href="https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&amp;cmd=displayKC&amp;externalId=2089969">https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&amp;cmd=displayKC&amp;externalId=2089969</a></td>
</tr>
<tr>
<td>PRS-338277</td>
<td>User access log records the connection broker IP rather than the desktop IP in the successful connection message.</td>
</tr>
<tr>
<td>PRS-331861</td>
<td>The Pulse desktop client does not honor the idle-session timeout in ESP mode when the idle-session timeout is greater than 16 minutes.</td>
</tr>
<tr>
<td>PRS-338197</td>
<td>The VMware View client fails to be installed when the following is true: Firefox or Edge browser is used AND the delivery option is configured as “Access the URL through the Pulse Connect Secure”.</td>
</tr>
<tr>
<td>PRS-338362</td>
<td>An SSL error may be seen after clicking on a VDI bookmark when using VMware View 3.x.</td>
</tr>
<tr>
<td>PRS-335995</td>
<td>A PCS or PPS with the IVS license installed is unable to connect to Pulse One. The license cache may need to be reset by importing a system.cfg without an IVS license in order to successfully register the appliance with Pulse One.</td>
</tr>
<tr>
<td>PRS-337815</td>
<td>The Pulse Secure client for Linux does not support periodic Host Checker updates.</td>
</tr>
<tr>
<td>PRS-335901</td>
<td>Pulse Linux client does not support Multi-Factor Authentication (MFA).</td>
</tr>
<tr>
<td>PRS-338860</td>
<td>Pulse Linux client does not support client certificate authentication.</td>
</tr>
<tr>
<td>PRS-337981</td>
<td>Pulse Linux: Pulse Client does not print any error when user attempts to establish duplicate tunnels.</td>
</tr>
<tr>
<td>PRS-336407</td>
<td>The VPN clients on Linux, both the 64-bit Pulse Linux client and the 32-bit Network Connect client, do not support configurations where the proxy is placed between PCS and protected resource.</td>
</tr>
<tr>
<td>PSD-1177</td>
<td>Pulse Secure client for Linux does not utilize the system proxy settings.</td>
</tr>
<tr>
<td>PRS-337937</td>
<td>Pulse Secure client for Linux shows does not disconnect after uploading logs to the PCS gateway.</td>
</tr>
<tr>
<td>Problem Report Number</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>PRS-337741</td>
<td>The Pulse service used by the Pulse Secure client for Linux does not stop automatically if the tunnel is destroyed due to network connectivity failure.</td>
</tr>
<tr>
<td>PRS-336136</td>
<td>The Pulse One configuration settings were part of user settings until 8.1R6 of PCS; and from 8.1R7 of PCS these settings are part of the system settings. The Pulse One configuration settings will be overwritten when a user settings configuration from 8.1R6 or lesser version, is imported to 8.1R7 or higher. XML import of Pulse One configuration settings are not affected by this change.</td>
</tr>
</tbody>
</table>

### Fixed Issues in 8.2R1.1 Release

The following table lists issues that have been fixed and are resolved by upgrading to 8.2R1.1 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Release Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-337308</td>
<td>When using the new admin UI and there is more than one page of role mapping rules, clicking &quot;Save Changes&quot; causes some rules to be removed without log messages.</td>
</tr>
<tr>
<td>PRS-337010</td>
<td>On 32-bit Windows machine, users received &quot;An authentication error has occurred&quot; error message when launching Windows Terminal Services bookmark if admin enabled Windows Terminal Services client logging.</td>
</tr>
<tr>
<td>PRS-336843</td>
<td>Source IP Restrictions do not activate as expected.</td>
</tr>
<tr>
<td>PRS-335501</td>
<td>A new feature in 8.2r1 shows a warning in the Admin UI if the insecure RC4 cipher is enabled. This new feature does not properly detect when RC4 is enabled when hardware acceleration is turned on. If hardware acceleration is not enabled, or the device does not have the hardware accelerator installed, the feature works as expected.</td>
</tr>
<tr>
<td>PRS-336158</td>
<td>PCS (part of A/A cluster) that is registered, connected with Pulse One, may cause a cluster split (possibly after a long run).</td>
</tr>
<tr>
<td>PRS-331800</td>
<td>On the Admin login page with multiple realm selection option, the first realm selection is not reflected on UI but it does login to the selected realm. User can clean the browser history to overcome this UI behavior.</td>
</tr>
<tr>
<td>PRS-337032</td>
<td>Remote desktop protocol (RDP) client restriction bypass issue. Please see</td>
</tr>
</tbody>
</table>
## New Features in 8.2R1 Release

The following table describes the major features that are introduced in 8.2R1 release.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pulse Secure Application Launcher (replacement for NPAPI)</td>
<td>Due to the end of ActiveX and Java support on many browsers, an alternate solution is provided in this release for the proper launching of client applications such as Pulse Desktop Client. This release uses a custom URL, pulsesecure://, to deliver and launch client applications. When invoked, the custom URL will automatically trigger new application – Pulse Application Launcher. The Pulse Application Launcher has the ability to accept the parameters from the user’s browser and launch the client application. This solution currently works on Chrome on Windows OS and Safari on Mac OS X.</td>
</tr>
<tr>
<td>iOS Support for accessing RDP/Telnet/SSH sessions using a HTML5 browser</td>
<td>In this release, users can access remote sessions using iOS.</td>
</tr>
<tr>
<td>IPv6 SNMP Support</td>
<td>PCS can send and receive SNMP alerts via IPv6 interface configured at the trap server.</td>
</tr>
<tr>
<td>Update “Last VPN Connect” time attribute in LDAP</td>
<td>The “Last VPN Connect” attribute in LDAP is updated when a user logs in. Admins can then run “reaper” scripts against their Active Directory and remove users that may not have logged in since “X” number of days.</td>
</tr>
<tr>
<td>Windows 2012 R2 Support</td>
<td>Windows 2012 R2 is now qualified with Pulse Connect Secure 8.2 software (auth only).</td>
</tr>
<tr>
<td>RSA Auth Manager 8.1</td>
<td>RSA Auth Manager is now qualified with Pulse Connect Secure 8.2 software.</td>
</tr>
<tr>
<td>Network level authentication support for WTS</td>
<td>Windows Terminal Services (WTS) now supports Microsoft’s Network Level Authentication.</td>
</tr>
<tr>
<td>Support for accessing RDP/Telnet/SSH sessions using HTML5-compliant browsers</td>
<td>- Users can launch RDP, Telnet, and SSH sessions via admin-created bookmarks. - Single sign on and NLA (Network Level Authentication) is supported by default. - Admin can configure screen resolution, color depth, DPI and additional settings as outlined in the admin guide</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>when creating the bookmarks.</td>
</tr>
<tr>
<td></td>
<td>• Users can transfer files from local machine to the remote machine and vice versa.</td>
</tr>
<tr>
<td></td>
<td>o If the admin has enabled it, a special G:\ drive is available in the remote machine. This drive contains a folder called “Download”. Any files dropped in these folders are automatically transferred between local and remote machines.</td>
</tr>
<tr>
<td></td>
<td>• Users can copy and paste text from local machine to remote machine and vice versa.</td>
</tr>
<tr>
<td></td>
<td>o Users can bring the clipboard access screen to the foreground by clicking on Ctrl + Alt + Shift. This will automatically include clipboard data that exists in the remote machine...to be transferred to the local machine.</td>
</tr>
<tr>
<td>Supported Operating Systems</td>
<td>The solution works on all supported browsers (Internet Explorer, Safari, Chrome) that run on desktop operating systems such as Windows, OS X and Linux.</td>
</tr>
<tr>
<td></td>
<td>• The solution works on Android OS and iOS.</td>
</tr>
<tr>
<td>UX admin revamp</td>
<td>The PCS administration web UI look and feel has been redesigned to improve the user interface experience. In PCS 8.2 release, user will have option to choose new user interface or switch to the classic user interface. The default UI is the new user interface. To use this new web UI, the PCS device must be connected to the external network. If the PCS device does not have connectivity to the external network, then the new user interface cannot be used and the classic user interface must be used.</td>
</tr>
<tr>
<td>Citrix Xen 7.6, StoreFront 2.6 &amp; 3.0</td>
<td>Citrix XenApp 7.6 and StoreFront 2.6 &amp; 3.0 is now qualified with Pulse Connect Secure 8.2 software.</td>
</tr>
<tr>
<td>VMWare Horizon View 6.0.1, 6.1 &amp; 6.2 HTML5 access.</td>
<td>VMware Horizon View 6.0.1, 6.1 &amp; 6.2 HTML 5 access is qualified with Pulse Connect Secure 8.2 software.</td>
</tr>
<tr>
<td>Certificate expiration warning</td>
<td>When a certificate has expired, or is about to expire, there is currently no notification available to the admin to take corrective or preventive action to renew certificates. The “Certificate Expiration Warning” feature provides the admin with a warning at the time of login. Also, the admin can query the certificates about to expire in a configured number of days for the type of certificates that are of interest.</td>
</tr>
<tr>
<td>Windows 10 support</td>
<td>Microsoft's latest Windows release, Windows 10, is qualified with Pulse Connect Secure (Only IE 11 browser).</td>
</tr>
<tr>
<td>OCSP logging</td>
<td>With the Online Certificate Status Protocol (OCSP) Logging Enhancement feature, the admin will be able to see the username, OCSP responder IP address and certificate serial number in the OCSP logs. With this information, the admin will be able to debug any OCSP related issues by correlating Connect Secure user access.</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>logs and logs from OCSP responders. In addition to that, admin will be able to filter all the OCSP related logs for a user for debugging OCSP related issue related to that user.</td>
<td></td>
</tr>
<tr>
<td>AES is preferred over RC4</td>
<td>AES is a preferred cipher over RC4. I.e. If a client that supports both AES and RC4 connects to PCS, AES is used.</td>
</tr>
<tr>
<td>A new feature in 8.2r1 shows a warning in the Admin UI if the insecure RC4 cipher is enabled. This new feature does not properly detect when RC4 is enabled when hardware acceleration is turned on. If hardware acceleration is not enabled, or the device does not have the hardware accelerator installed, the feature works as expected.</td>
<td></td>
</tr>
</tbody>
</table>

### Known Issues in 8.2R1 Release

The following table lists Known issues in 8.2R1 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
</table>
| PRS-339416            | When a two node SM-360 cluster is subjected to high load (approximately 17,000 users), the clustering process on one of the nodes is unable to communicate to the other leading to a cluster split and rejoin.  
In such situations, our recommendation is to reduce the load against the cluster by splitting the cluster into individual standalone devices or by distributing the load across multiple clusters. |
<p>| PRS-328634            | In Chrome browser, User is presented with ‘Application launcher not installed’ page twice when Host Checker is enabled along with auto launch of applications such as pulse desktop client or WSAM, This is due to Chrome issue <a href="https://code.google.com/p/chromium/issues/detail?id=468698">https://code.google.com/p/chromium/issues/detail?id=468698</a> |
| PRS-330443            | Custom Statement-of-Health policies will not function properly on Windows 10 because of Microsoft's phasing-out of support for the NAP (Network Access Protection) plugin. As such, if you have such a policy enabled (to verify, go to the PCS/PPS admin console and look under Authentication-&gt;Endpoint Security-&gt;Host Checker Policy-&gt;Windows-&gt;Rule Settings-&gt;&quot;Custom: Statement of Health&quot;), then you must disable it for all Windows 10 users. |</p>
<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-335517</td>
<td>System snapshot failing intermittently from serial console. Taking snapshot from admin UI works fine.</td>
</tr>
<tr>
<td>PRS-318679</td>
<td>For Host Checker with Bit Locker Encryption software, the encrypted drives will be reported as encrypted only when these drives are in Unlocked state.</td>
</tr>
<tr>
<td>PRS-309431</td>
<td>With OPSWAT Prebootatch Management Host Checker policy, the missing patches will be detected only with admin privileges for SCCM 2012 and SCCM 2007.</td>
</tr>
<tr>
<td>PRS-336183</td>
<td>The Pulse Application Launcher, which assists in the launching of Pulse clients from web browsers, displays text in Traditional Chinese when run a Simplified Chinese locale. There is no workaround at this time to get Simplified Chinese displayed by the Pulse Application Launcher.</td>
</tr>
<tr>
<td>PRS-336129</td>
<td>In order to make localization work properly for pulse client side applications on Windows platforms, end user needs to set correct language for non-Unicode programs under &quot;Control Panel&quot;-&gt;&quot;Clock, Language and Region&quot;-&gt;&quot;Region&quot;.</td>
</tr>
<tr>
<td>PRS-333621</td>
<td>On a fresh Windows 10 machine, Network Connect might fail to establish a tunnel for the first time. An error message is shown (&quot;timeout&quot; error message). Subsequent tries work fine.</td>
</tr>
</tbody>
</table>

**PRS-335317**

Symptom: Restricted users cannot upgrade the Pulse Secure desktop client.

Conditions: On a Windows machine, if an end user who has restricted permissions (as opposed to administrative permissions) attempts upgrade the Pulse Secure desktop client from a pre-5.2 version to a 5.2-or-later version using a web browser, the upgrade will fail with the message "You do not have the proper privileges to install the application."

Workaround: There are a number of ways to avoid this issue. The best way is to initiate the upgrade of the client by launching the client and connecting to the upgraded Pulse Secure gateway (as opposed to launching a web browser and connecting the web browser to the gateway). This client-initiated upgrade will complete as expected - it is only web-based upgrades that will not function. An alternative workaround would be to give the end user administrative privileges before attempting the web-based upgrade.

**PRS-334329**

During the uninstall of the Network Connect (NC) client under certain circumstances on Windows machines, end users may be presented with a User Access Control (UAC) prompt.

**PCS-2785**

On OS X, logging out of the user UI may display "Stopping components..." in the browser. Refresh the page to log in again.
<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PCS-2787</td>
<td>On OS X, file transfer, when using the new HTML5/RDP feature, does not work when using Safari. The workaround is to use Chrome instead.</td>
</tr>
<tr>
<td>PCS-2789</td>
<td>File transfer (using the new HTML5/RDP feature) does not work if &quot;Disable Audio&quot; option is un-checked.</td>
</tr>
<tr>
<td>PCS-2790</td>
<td>RDP session through IE11 doesn't play audio since audio codec is not supported.</td>
</tr>
<tr>
<td>PCS-2791</td>
<td>If printing is enabled, it may allow users to transfer some file types (when using HTML5/RDP feature), even if file transfer is disabled.</td>
</tr>
<tr>
<td>PCS-2792</td>
<td>When encryption is configured for &quot;Standard RDP Encryption&quot; or &quot;TLS Encryption&quot; then Username should be configured as &lt;DOMAIN Name&gt;&lt;Username&gt; and not just &lt;Username&gt;. This is mainly applicable for servers that are joined to a domain.</td>
</tr>
<tr>
<td>PCS-2850</td>
<td>On iOS File transfer to/from RDP machine through the Safari Browser does not work. The workaround is to use the Chrome browser.</td>
</tr>
<tr>
<td>PCS-2851</td>
<td>On iOS, the remote sessions using HTML5/RDP do not include sound.</td>
</tr>
<tr>
<td>PCS-2883</td>
<td>Cannot use a variable in the Host Name entry for HTML5/RDP feature.</td>
</tr>
<tr>
<td>PRS-332326</td>
<td>Client certificate based authentication using ECC Certificate doesn't work in Safari Browser.</td>
</tr>
<tr>
<td>PRS-332372</td>
<td>Client certificate authentication doesn't work in Safari Browser when LDAP Server is configured as Authentication server along with Certificate based Realm Restriction.</td>
</tr>
<tr>
<td>PRS-335105</td>
<td>The Certificate Expiration Warning feature will automatically start reporting certificates about to expire 7 days after installing (or upgrading to) this version. If you need to find out the expiration status immediately after an install (or upgrade) click on the &quot;Check Now&quot; button.</td>
</tr>
<tr>
<td>PRS-335115</td>
<td>Broadcast IP packet through a tunnel from an external client is not forwarded to the backend network.</td>
</tr>
<tr>
<td>PRS-331687</td>
<td>IPSEC Compression is not available for tunnels formed with 8.2 PCS gateway. IPSEC Compression checkbox is removed from the Connection Profiles Web UI page. Customers who has existing configs with IPSEC Compression will find that tunnels are negotiated with no compression in 8.2.</td>
</tr>
<tr>
<td>PRS-335501</td>
<td>A new feature in 8.2r1 shows a warning in the Admin UI if the insecure RC4 cipher is enabled. This new feature does not properly detect when RC4 is enabled when hardware acceleration is turned on.</td>
</tr>
<tr>
<td>Problem Report Number</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>PRS-336255</td>
<td>A &quot;500 internal error&quot; is seen when saving changes under User Roles --&gt; Files --&gt; Options page (only for Roles with Files options disabled). Issue is seen with new roles created and not with default Users Roles.</td>
</tr>
<tr>
<td>PRS-331800</td>
<td>On the Admin login page with multiple realm selection option, with chrome browser the first realm selection is not reflected on UI but it does login to the selected realm. User can clean the browser history to overcome this UI behavior.</td>
</tr>
<tr>
<td>PRS-336684</td>
<td>On end-user Mac machine, for browser base connections the debug log file is not created if the pulse client is not installed on the Mac machine. For troubleshooting purpose the pulse client would need to be installed on the mac machine.</td>
</tr>
<tr>
<td>PRS-336333</td>
<td>If multiple realms along with host checker policies are configured for sign-in url, “Endpoint Security Status” on Active Users page is shown as “Not Applicable”.</td>
</tr>
<tr>
<td>PRS-316786</td>
<td>Console Protection authenticates with users created in Default Network even when IVE is functioning in Administrative Network.</td>
</tr>
<tr>
<td>PRS-336159</td>
<td>SA (part of A/A cluster) that is registered, connected with Pulse One, may cause a cluster split (possibly after a long run).</td>
</tr>
<tr>
<td>PRS-331122</td>
<td>The OCSP Responder URL gets updated in Root CA rather than in Sub CA when Client is Authenticated using Certificate Issued from Sub CA which is configured for &quot;Inherit from Root CA&quot; mode.</td>
</tr>
<tr>
<td>PRS-337120</td>
<td>When VLAN/source IP is set on the role, access intranet resources fails.</td>
</tr>
<tr>
<td>PRS-337425</td>
<td>When launching clients from the browser, a blank page might be seen with “Content-type: text/html” before the launch of the client. This blank page will disappear and the client will launch successfully.</td>
</tr>
<tr>
<td>PRS-337686</td>
<td>Zero downtime for end users during an upgrade of an Active-Active or Active-Passive cluster is not available when upgrading from an older release to either 8.2R1 or 8.2R1.1. Post upgrade, the end users that were connected prior to the upgrade will have to re-authenticate to the PCS device.</td>
</tr>
<tr>
<td>PRS-337311</td>
<td>As described in the “General Notes” section of this document (search for “SHA-2”), PCS client access binaries in 8.2R1.1 and later are code-signed with SHA-2 certificates in order to meet new restrictions enforced by Microsoft operating systems in 2016. This new code-signing feature causes certain issues with older versions of Windows 7. Specifically, versions of Windows 7 that have not been patched since March 10, 2015 will not be able to load certain...</td>
</tr>
</tbody>
</table>
fixed issues in 8.2R1 release

The following table lists issues that have been fixed and are resolved by upgrading to 8.2R1 release.

<table>
<thead>
<tr>
<th>Problem Report Number</th>
<th>Release Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRS-316902</td>
<td>Wi-Fi profile with EAP-TTLS can't be configured on Windows 7 client.</td>
</tr>
<tr>
<td>PRS-296395</td>
<td>Pulse collaboration is not working correctly with native Mac Book Air 11&quot; resolution 1366x768.</td>
</tr>
<tr>
<td>PRS-316775</td>
<td>After Windows client onboarded, modifying the Pulse connection set on SA is not reflected on Windows client. Re-onboard on Windows client doesn't refresh Pulse connection set either. -- add more detail about how to get the new Pulse connection set onto Windows client.</td>
</tr>
<tr>
<td>PRS-319000</td>
<td>License client pulls license count from license server, the client's event log mistakenly shows the license count as its user count. The actual user count in system is correct.</td>
</tr>
<tr>
<td>PRS-318766</td>
<td>In a 2 node cluster, delete all licenses from both nodes, re-import a previously exported config into one node, parevntd crash was observed, but import completes successfully, parevntd restarts automatically and continues without an issue. If only deletes all the licenses for one of the node, dparevntd didn't crash. The crash was because the cache was not in sync.</td>
</tr>
<tr>
<td>PRS-331722</td>
<td>Problem: Accessing VMWare Horizon View HTML5 Access 6.0.1, 6.1 and 6.2 via PCS Rewriter throws blank Screen.</td>
</tr>
<tr>
<td>PRS-331732</td>
<td>Going through the huge list of Trusted server CAs to identify expired certificates is tedious so a new filter is added in trusted server CA page to show only the expired certificates.</td>
</tr>
</tbody>
</table>
Documentation

Pulse documentation is available at https://www.pulsesecure.net/techpubs/.

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@pulsesecure.net.

Technical Support

When you need additional information or assistance, you can contact “Pulse Secure Global Support Center (PSGSC):

- https://www.pulsesecure.net/support
- support@pulsesecure.net
- Call us at 1-844-751-7629 (toll-free USA)

For more technical support resources, browse the support (website https://www.pulsesecure.net/support).

Revision History

The following table lists the revision history for this document.

<table>
<thead>
<tr>
<th>Revision</th>
<th>Published Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.2</td>
<td>August 2017</td>
<td>8.2R8.2 update</td>
</tr>
<tr>
<td>9.1</td>
<td>July 2017</td>
<td>8.2R8.1 update</td>
</tr>
<tr>
<td>9.0</td>
<td>June 2017</td>
<td>8.2R8 update</td>
</tr>
<tr>
<td>8.2</td>
<td>April 2017</td>
<td>8.2R7.2 update</td>
</tr>
<tr>
<td>8.1</td>
<td>March 2017</td>
<td>8.2R7.1 update</td>
</tr>
<tr>
<td>8.0</td>
<td>February 2017</td>
<td>8.2R7 update</td>
</tr>
<tr>
<td>7.1</td>
<td>December 2016</td>
<td>Added HSTS support in New features of 8.2R6</td>
</tr>
<tr>
<td>7.0</td>
<td>December 2016</td>
<td>8.2R6 update</td>
</tr>
<tr>
<td>6.0</td>
<td>September 2016</td>
<td>8.2R5 update</td>
</tr>
<tr>
<td>5.0</td>
<td>June 2016</td>
<td>8.2R4 update</td>
</tr>
<tr>
<td>4.0</td>
<td>May 2016</td>
<td>8.2R3 update</td>
</tr>
<tr>
<td>3.1</td>
<td>April 11, 2016</td>
<td>Added PRS-339416 under known issues of 8.2R1</td>
</tr>
<tr>
<td>3.0</td>
<td>April 1, 2016</td>
<td>8.2R2 update</td>
</tr>
<tr>
<td>Version</td>
<td>Date</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>2.0</td>
<td>February 2016</td>
<td>8.2R1.1 update</td>
</tr>
<tr>
<td>1.0</td>
<td>January 7, 2016</td>
<td>Initial publication – 8.2R1</td>
</tr>
</tbody>
</table>