



Pulse Policy Secure

Release Notes

PPS 9.1R2 Build 1705

Pulse Profiler Version 1.6 (FPDB Version 40)

PDC 9.1R2 Build 901

Default ESAP Version: ESAP 3.3.5

Release Build	9.1R2, 1705
Published	July 2019
Document Version	1.2

Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134
<https://www.pulsesecure.net>

© 2019 by Pulse Secure, LLC. All rights reserved

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at <https://www.pulsesecure.net/support/eula>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Revision History

The following table lists the revision history for this document.

Revision		Description
2.0	July	Updated for 9.1R2
1.2	June	Added "Session Bridging for Linux Platform" under New Features in 9.1R1 Release.
1.1	May	Added PRS 371536, PRS 373619 under Fixed Issues in 9.1R1 Release.
1.0	April	Updated for 9.1R1

Contents

Revision History.....	3
Introduction	5
Hardware Platforms.....	5
Virtual Appliance Editions	5
Upgrade Paths	6
Upgrade Scenario Specific to Virtual Appliances	7
General Notes	7
New Features in 9.1R2 Release.....	8
Fixed Issues in 9.1R2 Release.....	8
Known Issues in 9.1R2 Release	9
New Features in 9.1R1 Release.....	10
Noteworthy Changes in 9.1R1 Release	11
Fixed Issues in 9.1R1 Release.....	11
Known Issues in 9.1R1 Release	11
Documentation	14
Technical Support.....	14

Introduction

This document is the release notes for Pulse Policy Secure. 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:

- 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:

- Virtual Pulse Secure Appliance (PSA-V)

Note:

- From 9.1R1, VA-DTE will not be supported.
- From 9.0R1 release, Pulse Secure has begun the End-of-Life (EOL) process for the VA-SPE virtual appliance. In its place, Pulse Secure is launching the new PSA-V series of virtual appliances designed for use in the data center

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

Platform	Qualified System
VMware	<ul style="list-style-type: none"> • HP ProLiant DL380 G5 with Intel(R) Xeon(R) CPU • ESXi 6.7
KVM	<ul style="list-style-type: none"> • CentOS 6.6 with Kernel cst-kvm 2.6.32-504.el6.x86_64 • QEMU/KVM v1.4.0 • Linux Server Release 6.4 on an Intel Xeon CPU L5640 @ 2.27GHz • 24GB memory in host • Allocation for virtual appliance: 4vCPU, 4GB memory and 40GB disk space
Hyper-V	<ul style="list-style-type: none"> • Microsoft Hyper-V Server 2016 and 2019

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

Upgrade Paths

The following table describes the tested upgrade paths. Please note that here x and y refer to the following:

x: Latest maintenance release version

y: Any release version

Upgrade From	Qualified	Compatible
9.1R1	Yes	
9.0Rx	Yes	
9.0Ry		Yes
5.4Rx	Yes	
5.4Ry		Yes

For versions, earlier than 5.3:

- First upgrade to release 5.4R3 | 5.4Ry and then upgrade to 9.1Rx.



Note

- Beginning with PPS 5.4R3 release, access to Profiler functionality on Pulse Secure Appliance (PSA) platforms will require a Profiler license installed.
- To continue using Profiler, the license should be procured and installed prior to upgrade.
- If your system is running beta software, roll back to the previously installed official software release before upgrading. This practice ensures the rollback version is a release suitable for production.

Upgrade Scenario Specific to Virtual Appliances

PSA-V cannot be upgraded to 9.1R2 without core license. Follow these steps to upgrade to 9.1R2:

1. If PSA-V is running 5.3Rx:
 - a. Upgrade to 5.4R3 or later.
 - b. Install Core license through Authcode.
 - c. Upgrade to 9.1R2.
2. If PSA-V is running 5.4R1:
 - a. Upgrade to 5.4R3 or later.
 - b. Install Core license through Authcode.
 - c. Upgrade to 9.1R2.
3. If PSA-V is running 5.4R3 or later:
 - a. Install Core License through Authcode.
 - b. Upgrade to 9.1R2.



Note:

- If your system is running beta software, roll back to your previously installed official software release before you upgrade to 9.1R2. This practice ensures the rollback version is a release suitable for production.
- On a PPS virtual appliance, we highly recommend to freshly deploy a PSA-V from 5.4Rx-based OVF, when any of the following conditions are met:
 - If the disk utilization goes beyond 85% or if an admin receives iveDiskNearlyFull SNMP Trap.
 - If the factory reset version on the PSA-V is 4.x or <= 5.3Rx.

General Notes

1. PPS license clients, running 5.1R1 and above, will not be able to lease licenses from License Servers running on PCS 8.0R1 to PCS 8.0R4. If you plan to upgrade PPS License clients to 5.1R1 and above versions, the license servers need to be upgraded to 8.0R5 and above. See [KB40095](#) for more information.
2. 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](#).
3. When custom ciphers are selected, there is a possibility that some ciphers are not supported by the browser currently being used by the PPS administrator.
4. If any ECDH/ECDSA ciphers are selected, they require ECC certificate to be mapped to the internal/external interface. If an ECDH/ECDSA cipher is selected, an ECC certificate is required to be installed on the internal/external interface. The only way to recover from this is to connect to the serial console and select option 8 to reset the SSL settings. This option, 8, resets the SSL setting to factory default. Any customization done is lost. This applies only to Inbound SSL settings.
5. Minimum ESAP version supported on 9.1R2 is 3.3.5.
6. With OPSWAT v4 SDK, the new product support list is being worked upon and updated by OPSWAT periodically, which is delivered as part of ESAP.

New Features in 9.1R2 Release

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

Feature	Description
EasiSMS Gateway Support	PPS supports EasiSMS gateway through the SMTP server. EasiSMS uses an email format to send SMS to end user mobile phones.
Migration of Cisco ACS RADIUS/TACACS+ client configuration to PPS	Migrating RADIUS/TACACS+ client configuration configured on the Cisco ACS device.
V3 to V4 Opswat SDK migration	PPS supports the migration of servers and clients to Opswat v4 to take advantage of latest updates.
Alert based integration with Nozomi Networks	PPS along with Nozomi Networks provides threat detection and threat response in ICS/OT environment.
VA Partition	<p>PCS/PPS supports upgrading from PCS 8.2Rx/ PPS 5.3Rx to 9.1R2 for the following supported platforms:</p> <ul style="list-style-type: none"> • VMWare ESXi • KVM • Hyper-V <p>When upgrading a VA-SPE running PCS 8.2R5.1/PPS 5.3Rx or below that was deployed with an OVF template to a higher version, the upgrade was failing. This feature solves the upgrade problem for VMWare, KVM and Hyper-V. Refer KB41049 for more details.</p>
Report Max Used Licenses to HLS VLS	The licensing client reports maximum used sessions count instead of the maximum leased licenses count. For MSP customers, this change helps in billing the tenants based on maximum sessions used.
Flag Duplicate Machine ID in access logs	<p>Pulse client expects the machine ID is unique on each machine. If multiple endpoints have the same machine ID, for security reasons, the existing sessions with the same machine id are closed.</p> <p>A new access log message is added to flag the detection of a duplicate Machine ID in the following format: Message: Duplicate machine ID "<Machine_ID>" detected. Ending user session from IP address <IP_address>. Refer document KB25581 for details.</p>
Backup configs and archived logs on AWS S3/Azure Storage	<p>Two new methods of archiving the configurations and archived logs are available apart from SCP and FTP methods: PPS/PCS supports pushing configurations and archived logs to the S3 bucket in the Amazon AWS deployment and to the Azure storage in the Microsoft Azure deployment.</p>
Profiler	
Windows defender and Microsoft Security Essentials support	Agentless Host Checker with Profiler supports Windows defender and Microsoft Security Essentials.
Profiler dashboard update	Profiler dashboard supports chart for Profile Groups. This chart is also part of downloaded PDF report.

Fixed Issues in 9.1R2 Release

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

Problem Report Number	Release Note
PRS- 376312	Summary: Factory reset from VMware VA console does not load the factory reset version and loads the current version.
PRS-376265	Summary: Invalid character error seen while adding Radius Return attribute value which contains "<" and ">" characters.
PRS-376465	Summary: Host Checker service in Pulse is crashing while performing policy monitoring when pulse client is retrying.
PRS-372699	Summary: NMAP scan profiling is inaccurate
PRS-372499	Summary: Session from Exported session list get purged on cluster if the passive node is disabled, rebooted and rejoined.

Problem Report Number	Release Note
PRS-372440	Summary: Post Failover, Delayed session resumption with Pulse Client.

Known Issues in 9.1R2 Release

The following table lists Known issues in this release.

Problem Report Number	Release Note
PRS- 376980	<p>Symptom: Clear config on PPS set the default 'Account Lockout' values to zero for 'Guest Authentication' server and this value cannot be modified or saved.</p> <p>Condition: If the 'Account Lockout' values are set to zero, it always display an error while saving 'Guest Authentication' server changes as zero is not an accepted value for 'Account lockout' parameter.</p> <p>Workaround: Exporting XML\binaries before PPS Upgrade and then Importing to 9.1R2 after Upgrade can help to set the correct 'Account Lockout' values under Authentication->Auth Servers</p>
PRS-378002	<p>Symptom: Cache server is continuously crashing in Longevity setup. Unable to open admin UI, crash messages display.</p> <p>Condition: When cache memory is hitting more than 512mb this crash has been observed.</p> <p>Workaround: NA, rollback and upgrade to latest version to start the test again.</p>
PRS-378052	<p>Symptom: SMTP Port 465 is not working for PPS guest user.</p> <p>Condition: Under SMTP settings, port 465 should also supported for Guest user.</p> <p>Workaround: SMTP port 587 with selecting SSL works in case of guest.</p>
PRS 379003	<p>Symptom: End user always gets the remediation role even after endpoint meets all the End Point Security Policies.</p> <p>Condition: This issue persists in macOS Catalina Version 10.15 Beta.</p> <p>Workaround: NA</p>
PRS-379012	<p>Symptom: Radius Disconnect message (DM) is not working after importing user.cfg configuration from the previous release.</p> <p>Condition: When previous configuration (from 9.0R1) is loaded onto the box, overwrites the default radius.dct. "Funk-Dest-IPv6-Address" attribute is missing in the old dictionary.</p> <p>Workaround: After restoring the dictionary to factory default, DM is sent to the switch and session is disconnected.</p>
PRS-379063	<p>Symptom: While performing L3 followed by L2 and frequently enable/disable migration option some time SDKs are replacing next periodic host check</p> <p>Conditions: On Windows Platform using Pulse performing L2 authentication with Host Check enabled on Role/Realm with Migration feature enabled.</p> <p>Workaround: For replacing expected SDKs wait for next periodic Handshake or Disconnect and again connect to server using Pulse.</p>
PRS - 377549	<p>Symptom: PSIS is not upgrading to the 9.1R2 version.</p> <p>Condition: When CTS, WTS and VDI gets upgraded to 9.1R2 in Win10RS5+.</p> <p>Workaround: NA</p>
Profiler	
PRS-378960	<p>Symptom: Selected profiler name not retained in profiler dashboard.</p> <p>Condition: In dashboard, Profiler name not retained when revisiting the same page after moving to another page.</p> <p>Workaround: NA</p>
PRS-378956	<p>Symptom: Linkdown Trap is not updating device link status in Device Discovery Report when profiler processes for the first time.</p> <p>Condition: Profiler not processing Linkdown Trap without Linkup trap update in Device Discovery page for the device.</p> <p>Workaround: NA</p>

Problem Report Number	Release Note
PRS-377534	<p>Symptom: Profiler report downloaded from Admin UI always captures the charts in default styles even though admin has changed some of the chart styles on the Dashboard page</p> <p>Condition: Administrator downloading of profiler report from Profiler Dashboard page</p> <p>Workaround: NA. Currently, profiler report is always generated with the default chart types.</p>

New Features in 9.1R1 Release

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

Feature	Description
SNMP Enforcement using ACL (Cisco, HP, Juniper)	SNMP enforcement using ACL is supported for Cisco, Juniper and HP switches.
Meraki 802.1x and Guest Access support	802.1X and Guest Access support is qualified with Cisco Meraki WLC.
Google Auth Multi Factor Authentication	TOTP server can be added as a secondary auth server in PPS.
Session bridging for Linux Platform	PPS supports bridging the Layer 2 Native Supplicant 802.1X session with Layer3 Agentless (Browser based) Session on Linux platform.
RADIUS server capability on External port	802.1X authentication is now supported on external port.
SAML Auth Server support	PPS can be configured as SAML service provider (SP) for all industry standard SAML IdP's.
Session Migration using Cert authentication	Session migration in an IF-MAP federated network supports Cert Auth and SAML auth
Machine certificate check on MacOS	Machine certificate check on Mac OS is now supported for PPS.
TACACS+ Enhancements – DB sync, pass back attributes to devices such as F5 and Juniper	TACACS+ authorization support for Administrators using custom attributes for Juniper and F5 devices. TACACS+ configuration synchronization across WAN cluster
DNS traffic on any physical interface	Prior to 9.1R1 release, DNS traffic was sent over the Internal interface. Starting with 9.1R1 release, an administrator can modify the DNS setting to any physical interface namely Internal Port, External Port or Management Port.
Profiler	
Distributed Profiler Enhancements	The Administrators can sync the profiled data from one Profiler to another from the profiler auth server configuration page. Multiple branch offices can sync their profiled data to central office. Admin can view the Device Discovery Report to view and control the multiple offices.
Profiler Device Age Out	Profiler device age-out interval configuration allows admin to automatically delete the devices from the database. Admin can define the age-out interval for a group of devices also using Profile Groups
Profile Windows devices using SNMP(HOST)	SNMP-HOST Collector is a collection method that receives endpoint information where the endpoints are monitored through SNMP. Admin can configure subnets to scan and community strings in profiler auth server configuration page.
Approval for Profile Groups	Administrator can select “needs approval” for selected Profiler group.
Key-value based search in DDR	Administrator can search in DDR with key value-based query. Query syntax is similar to that of profile groups.

Feature	Description
Publishing IP address from Profiler to Active User Session	Admin can add IP address from Profiler to active session for L3 enforcement when RADIUS accounting is not enabled. This is supported only for MAC auth and dot1X.
Huawei switches added in supported list for Network Infrastructure Device	Admin can select Huawei switch from supported list in network infrastructure device page.

Noteworthy Changes in 9.1R1 Release

None

Fixed Issues in 9.1R1 Release

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

Problem Report Number	Release Note
PRS-374583	Summary: Behavior of "re-authentication" and "termination" options in radius Return Attribute policy page is interchanged.
PRS-371733	Summary: Assigned VLAN is not updated if fetched on the next poll and always shows default configured VLAN.
PRS-370902	Summary: Behavioral Analytics dashboard is not displaying charts for potential malware and anomalous traffic from IoT devices for more than 4 device categories intermittently.
PRS-370903	Summary: MAC address is not updated in the user session details.
PRS-374582	Summary: Behavior of "re-authentication" and "termination" options in radius Return Attribute policy page is interchanged.
PRS-374368	Summary: PSAL launch failed when proxy browser is configured.
PRS-374477	Summary: Fortinet admission control feature will not work with domain users (AD).
PRS-371536	Summary: Host Checker: Virus Definition Check for updates fails for K7 Virus Security ZERO (14.x),
PRS-373619	Summary: Host Checker: Virus Definition Check for updates fails for AVG Free Antivirus (19.2.x).

Known Issues in 9.1R1 Release

The following table lists Known issues in this release.

Problem Report Number	Release Note
PRS-372687	<p>Symptom: RADIUS CoA disconnect for Splash sign on page in Meraki WLC does not acknowledge the session disconnect message sent by PPS.</p> <p>Conditions: Guest session will be deleted from PPS, but the session will be active on WLC for the default timeout period of the guest session on Meraki WLC.</p> <p>Workaround: Admin can login to Meraki dashboard and de-authorize the guest manually from Wireless > Splash logins page. In addition to that, we have raised an enhancement request to Meraki to support COA disconnect on splash sign on page with radius authentication.</p>
PRS-372794	<p>Symptom: RADIUS Accounting stop message is not sent by Meraki when guest logs out or gets disconnected from Guest SSID</p> <p>Conditions: The Guest session will remain active on PPS for the duration of Maximum Session Length (default=725 mins).</p> <p>Workaround: Admin can login to Meraki dashboard and de-authorize the guest manually from Wireless > Splash logins page which will immediately send the Accounting stop message from Meraki to PPS.</p>
PRS-373861	<p>Symptom: TACACS+ Accounting start and stop messages are not sent by BIG IP F5 device</p> <p>Condition: PPS may have stale sessions as it does not receive stop accounting packets. However, these</p>

Problem Report Number	Release Note
	<p>sessions are deleted from PPS when Maximum Session Timeout expires.</p> <p>Workaround: NA. If there is any stale TACACS+ session on PPS, it does not cause any security risk as any TACACS+ login is controlled by the BIG IP F5 device.</p>
PRS-372849	<p>Symptom: Session migration fails for secondary auth server. User is prompted with secondary auth server password.</p> <p>Condition: If secondary auth server is configured for session migration.</p> <p>Workaround: NA</p>
PRS-376312	<p>Symptom: Factory reset from VMware VA console does not load the factory reset version and loads the current version.</p> <p>Conditions: When trying to do factory reset to 9.1R1 from higher version in VMware-VA</p> <p>Workaround: Factory reset is possible by manual intervention. After successful 'Factory reset' command given from console, Virtual Appliance will reboot and will display three options in LILO menu:</p> <ul style="list-style-type: none"> -Current version -Rollback version -Factory reset version <p>Admin need to manually select the Factory reset version for the factory reset to happen successfully on VMware VA.</p>
PRS-372250	<p>Symptom: Session migration fails for 802.1X authentication.</p> <p>Condition: When the user tries to migrate the 802.1X sessions from PPS to PCS.</p> <p>Workaround: NA</p>
PRS-374476	<p>Symptom: Firewall SOH policy evaluation fails for domain user when Private and Public Networks profiles in Windows Firewall are not turned ON.</p> <p>Condition: When Private and Public network profile for domain user is not turned ON for Windows firewall.</p> <p>Workaround: NA</p>
PRS-374820	<p>Symptom: Profiler SNMP polling messages might be shown twice in event logs with in few seconds. even sometimes 'Switch poll error: Failure in send to.' in logs.</p> <p>Condition: If network infrastructure devices config imported using binary/xml</p> <p>Workaround: NA. This might happen once.</p>
PRS-374663	<p>Symptom: L3 session is established with Internal IP while performing L3 followed by L2 using Pulse with PPS External VIP address.</p> <p>Conditions: When PPS nodes are in cluster and external port is used for RADIUS authentication.</p> <p>Workaround: NA</p>
PRS-360616	<p>Symptom: SAML authentication failed with error "Missing/Invalid sign-in URL" despite correct credentials while using PDC embedded browser version 9.0.1.</p> <p>Condition: Using PDC browser version 9.0.1 with PPS version 9.1R1.</p> <p>Workaround: Use latest PDC version with Release 9.1R1.</p>
PRS-366966	<p>Symptom: Juniper Connector UI provides option to select TCP ports for communicating with PPS. However, PPS connector always use port 443, making the selected TCP port ineffective.</p> <p>Conditions: Configuring PPS as connector in Juniper PE.</p> <p>Workaround: Ensure that the Port number is always set to 443.</p>
PRS-367195	<p>Symptom: While configuring the Pulse Policy Secure connector in Juniper PE, administrator need to enter the system-local administrator credentials as PPS admin and AD user account cannot be used for generating REST API key for PPS-Juniper PE communication.</p> <p>Conditions: Configuring PPS as Connector in Juniper PE.</p> <p>Workaround: Juniper SDSN integration with PPS requires creating a local Admin user on PPS.</p>
PRS-367291	<p>Symptom: Certificate Authentication fails due to configuration of "Skip Revocation when OSCP/CDP server is not available" for HC policy enforced at realm level.</p> <p>Condition: When admin enables Skip Revocation check and OSCP server is not reachable.</p> <p>Workaround: Set the OSCP timeout to less than 5 seconds.</p>
PRS-368055	<p>Symptom: Admin is allowed to create anomaly role mapping rules based on custom expressions when UEBA license is not installed.</p> <p>Condition: Configuring anomaly role mapping rules based on custom expressions when Behavioral Analytics license is not installed</p> <p>Workaround: Install Behavioral Analytics License.</p>
PRS-366296 PRS-369738	<p>Symptom: Authentication to PPS fails as Duo custom sign-in pages are not displayed.</p>

Problem Report Number	Release Note
	<p>Condition: User authenticates to PPS and assigned realm is configured with Duo as secondary authentication server.</p> <p>Workaround: Use passcode-based Duo authentication.</p>
PRS-367024	<p>Symptom: Authentication fails for browser-based login for Duo and LDAP combination with predefined user as <USER> in secondary authentication server.</p> <p>Condition: User authenticates to PPS and assigned realm is configured with Duo as primary and LDAP as secondary auth server</p> <p>Workaround: Use passcode-based Duo authentication.</p>
PRS-368136	<p>Symptom: VIP failover fails in A/P cluster when the Active node becomes unreachable with SPAN configured on external port.</p> <p>Condition: Active node becomes unreachable in A/P Cluster with Local SPAN enabled on cluster nodes' external port.</p> <p>Workaround: Configure Remote SPAN.</p>
PRS-368689	<p>Symptom: OS Check rule is not supported when trying to connect from 9.0R3 Pulse client to old PPS (9.0R2\9.0R1) server on MAC OS platform.</p> <p>Condition: When OS check Host checker rule is evaluated with new Pulse client connecting to pre-9.0R3 PPS server.</p> <p>Workaround: Pulse client on MAC platform and PPS server need to be 9.0R3 for OS Check host checker policy to work as expected.</p>
PRS-368967	<p>Symptom: Host checker fails on Mac OS 10.14 Mojave endpoint when Activate Older OPSWAT SDK in ESAP is enabled.</p> <p>Condition: When ESAP with V3 SDK is activated on the server.</p> <p>Workaround: Administrator should activate ESAP with V4 SDK on PPS for Host check to work as expected.</p>
PRS-376265	<p>Symptom: Invalid character error seen while adding Radius Return attribute value which contains "<" and ">" characters.</p> <p>Condition: While creating new Radius Return attribute value or editing existing Radius Return attribute value which contains "<" and ">" characters.</p> <p>Workaround:</p> <ol style="list-style-type: none"> 1) Upgrade case: It would work fine, if Radius Return attributes are not modified. To edit or create new Radius Return attribute value, please follow step 2. 2) Fresh Deployment: To add Radius Return attribute value which contains "<" and ">" characters, export XML file from Maintenance >Import\Export >Export XML and add\modify the Radius Return Attribute value in Exported XML and then import the same XML from Maintenance >Import\Export->Import XML.
Profiler	
PRS-369079	<p>Symptom: For Agentless Host Checker with Profiler, Antivirus Rule with "virus definition age" check may fail.</p> <p>Conditions: Windows registry does not maintain the timestamp, when last virus definition was installed. Time is taken as midnight time (00:00:00) of the date, when the last definition was installed.</p> <p>Workaround: Create the rule with (expected number of definition age + 1) days.</p>
PRS-367687	<p>Symptom: Remote profiler is unable to communicate with Profiler; hence the remote endpoints are not profiled.</p> <p>Conditions: If self-signed certificate is used on Profiler Authentication server.</p> <p>Workaround: Using a CA signed certificate on Profiler server.</p>
PRS-361246	<p>Symptom: Endpoint session status is not updated in DDR table if the same endpoint is imported through Binary configuration.</p> <p>Conditions: Importing profiler data using Binary configuration.</p> <p>Workaround: Reconnect the existing user session.</p>
Cloud Application Visibility	
PRS-370268	<p>Symptom: CAV fails to configure proxy on endpoint, when Juniper SRX is configured as an Infranet Enforcer for a resource.</p> <p>Condition: Juniper SRX is configured as Infranet Enforcer.</p> <p>Workaround: N/A</p>
PRS-370249	<p>Symptom: CAV policies are not applied when endpoints establish dot1x connection with a switch/access point.</p> <p>Condition: Authenticator is a third-party device and is configured to use PPS as authenticating server.</p> <p>Workaround: N/A</p>

Problem Report Number	Release Note
PRS-370237	<p>Symptom: CAV policy updates are not sent to PPS if CAV Database is updated with PCS IP address.</p> <p>Condition: If CAV database at client side is updated with PCS IP address and the user establishes L2/L3 connection.</p> <p>Workaround: N/A</p>
PRS-370123	<p>Symptom: DNS resolution fails after CAV is re-enabled at user role level.</p> <p>Conditions: If already added user role is deleted from the CAV policies.</p> <p>Work Around: - N/A</p>
PRS-369277	<p>Symptom: CAV feature does not work when Pulse SAM is enabled on client.</p> <p>Conditions: Pulse SAM and CAV enabled for the same role.</p> <p>Work Around: - N/A</p>
PRS-369891	<p>Symptom: Authentication token fetching is failing under NATed environment on Pulse client for CAV policies update.</p> <p>Conditions: PCS configured behind a NAT device.</p> <p>Work Around: N/A</p>
PRS-369279	<p>Symptom: Lockdown is not working properly if CAV policies are configured.</p> <p>Conditions: Enabling CAV with lock down.</p> <p>Work Around: N/A</p>

Documentation

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

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>.