Pulse Policy Secure

Release Notes
PPS 9.0R2.1 Build 51569
Pulse Profiler Version 1.4 (FPDB Version 33)
PDC 9.0R2.1 Build 1421
Default ESAP Version: ESAP 3.2.7

Release, Build	**9.0R2.1, 51569**
Published	**September 2018**
Document Version	**2.3**

Pulse Secure, LLC

2700 Zanker Road, Suite 200

San Jose, CA 95134

https://www.pulsesecure.net

Contents

Introduction

This document is the release notes for Pulse Policy Secure Release 9.0R2.1. 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:

- Demonstration and Training Edition (DTE)
- Virtual Pulse Secure Appliance (PSA-V)

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

Platform	Qualified System
VMware	• HP ProLiant DL380 G5 with Intel(R) Xeon(R) CPU • ESXi 6.0, 5.5U3, 5.5
KVM	• 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 o 24GB memory in host • Allocation for virtual appliance: 4vCPU, 4GB memory and 40GB disk space
Hyper-V	• Microsoft Hyper-V Server 2012 R2

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
9.0R1	Yes	
5.4Rx	Yes	
5.4Ry		Yes
5.3Rx	Yes	-
5.3Ry	-	Yes

For versions, earlier than 5.3:

First upgrade to release 5.3Rx|5.3Ry, 5.4Rx|5.4Ry and then upgrade to 9.0Rx.

Note:

- Beginning with PPS 5.4R3 release, access to Profiler functionality on Pulse Secure Appliance (PSA) platforms will require a Profiler License to unlock Profiler feature.
- Please make sure to procure and install the Profiler license prior to upgrading. If you upgrade without having the Profiler license, you will no longer have access to Profiler features.
- 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.
- On a PCS/PPS virtual appliance, we highly recommend to freshly deploy a PSA-V from 5.4-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 5.0.

Upgrade Scenario Specific to Virtual Appliances

PSA-V cannot be upgraded to 9.0R2.1 without core license. Follow these steps to upgrade to 9.0R2.1:

1. If PSA-V is running 5.3Rx:
    a. Upgrade to 5.4R3 or later.
    b. Install Core license through Authcode.
    c. Upgrade to 9.0R2.1.
2. If PSA-V is running 5.4R1:
    a. Upgrade to 5.4R3 or later.
    b. Install Core license through Authcode.
    c. Upgrade to 9.0R2.1.
3. If PSA-V is running 5.4R3 or later:
    a. Install Core License through Authcode.
    b. Upgrade to 9.0R2.1.

Note: VM images crash when tried to upgrade to 9.0R2.1 when the reset version is 5.4 and below.

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 C5.1R1 and above versions, the license servers needs 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 web browser. If any ECDH/ECDSA ciphers are selected, they require ECC certificate to be mapped to the internal/external interface. If an ECC certificate is not installed, administrators may not be able to login to the appliance. 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.
4. Pre-5.0 Android and pre-9.1 iOS devices don't support Suite B ciphers. If Suite B is enabled, Pulse client on pre-5.0 Android and pre-9.1 iOS devices will not be able to connect.
5. 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. In case of any issue related to compliance evaluation or remediation for any specific product, then ensure that latest ESAP is used or roll back to OPSWAT v3 SDK.

Fixed Issues in 9.0R2.1 Release

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

Problem Report Number	Release Note
PRS-357112	Summary: Web server crashes with ECDH cert load.

New Features in 9.0R2 Release

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

Feature	Description
Secure Access for IoT/IIoT	PPS enables secure access to IoT devices through PPS/Profiler and SRX firewall integration. It allows the Admin to configure an IoT Access policy so that only authorized users can access the IoT devices. It also enables automatic access control for the newly discovered devices.
Cloud Application Visibility (CAV)	Cloud Application Visibility feature enables administrators to secure and manage cloud applications. It also provides visibility of the cloud applications used by the user and allows the administrator to set granular access and use policies to monitor the Cloud Application usage in real time. Note: • This is a licensed feature and requires the Cloud Secure license to be installed. • CAV feature is not supported in a cluster configuration in this release.
Provisioning PCS sessions to Check Point Firewall using IF-Map through PPS.	Pulse Policy Secure (PPS) integrates with Check Point Firewall to provision user's identity information (user name, roles and IP address) to Check Point firewall using shared secret. You can provision Pulse Connect Secure (PCS) user's identity information to Check Point firewall using IF-Map so that access control can be provided for PCS users accessing resources protected by Check Point Firewall.

Noteworthy changes in 9.0R2 Release

- Layer 2 session bridging for Agentless Login: Session bridging feature is now enhanced to support bridging of consecutive layer 2 sessions.
- Host Check for 64-bit MacOS applications: Host Check support is added for the 64-bit Mac OS applications.

Fixed Issues in 9.0R2 Release

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

Problem Report Number	Release Note
PRS-358212	Summary: MacOS patch management compliance checks fail if the product is not updated to Software Update (2.x) when using OPSWAT V4.
PRS-366343	Summary: Authentication server types may repeat in the authentication server type drop-down when creating a new authentication server
PRS-364495	Summary: MAC auth (802.1x) and guest access cannot use the same switch.
PRS-365105	Summary: When using XML export, HTML escape codes are shown rather than the rendered value.
PRS-364215	Summary: Delegated Admin may receive an HTTP 500 Internal Server Error when logging in.
PRS-364691	Summary: Universal XML file may fail to import.
PRS-364122	Summary: Machine certificate Host Checker validation fails on Trusted Platform Module (TPM)-enabled machines.
PRS-364535	Summary: "Smart Dishwasher" appliance may not be profiled correctly.

Problem Report Number	Release Note
PRS-364468	Summary: Pulse connection may fail compliance checks with OPSWAT v3 SDK as active.
PRS-364462	Summary: Checkpoint firewalls may be available as an enforcer option on the resource access policy configuration page.
PRS-364438	Summary: Location Group may display escape characters rather than the character when adding a network infrastructure device.
PRS-362428	Summary: Host Checker file checks may fail if the user profile contains special characters.
PRS-363732	Summary: CDP/LLDP is not updated properly when IP Phone IP address contains single digits in an octet (e.g. 10.1.1.1).
PRS-362553	Summary: NMAP scan may not be done again if a user disconnects and connects again quickly.
PRS-358373	Summary: Bridging multiple L2 sessions is not supported.
PRS-362660	Summary: Avaya 9133 WAP wrongly classified as Linux by DHCP.
PRS-359561	Summary: PPS is accepting invalid PCLS certificates.
PRS-366275	Summary: The PPS platforms now use a fully 64-bit kernel.
PRS-364497	Summary: Current version is showing as 9.0R1:HF1 after upgrading to 9.0R1:HF2(50039) build.

Unsupported Features in 9.0R2 Release

None.

Known Issues in 9.0R2 Release

The following table lists Known issues in 9.0R2 release.

Problem Report Number	Release Note
PRS-366184	Symptom: Resource Access Policy failed with errors "Unable to load Manufacturer" and "Failed to Save due to resource limit exceeds 32768 characters. Conditions: If the Admin tries to create a resource policy, which exceeds 32768 characters. Workaround: Create multiple policies for a set of Device Category and Manufacturer if resources exceed 32768 characters.
PRS-365725	Symptom: IoT Access Policy changes do not get saved. Conditions: When a policy is opened for editing from 'Resource access policy' page and in if a new policy is added from 'Resource access Policy' page from another tab. Workaround: Open the IoT Access policy page again for editing and save the changes.
PRS-359313	Symptom: Endpoint compliance fails when Host Checker policy is saved on the policy page immediately after modifying the rule. Conditions: If Host Checker policy is immediately saved after modifying the rule. Workaround: The user will need to login again.
PRS-361154	Symptom: When an active node is disabled and enabled back in an active/passive cluster, endpoint table is deleted from both cluster nodes. Conditions: Disabling and enabling an active node in an active/passive cluster.

Problem Report Number	Release Note
	Workaround Users must re-login.
PRS-356373	**Symptom:** Import of malformed XML file for named user account records is allowed. **Conditions**: Importing an invalid XML. **Workaround:** Validate the XML is correct prior to import.
PRS-355333	**Symptom:** Named User tab does not load (cannot be viewed) when user count is greater than 150K. **Conditions:** Administrators will not be able to view or delete any named users if they more than 150,000 (150K) named users are registered. **Workaround:** Split the deployment into multiple stand alone and/or cluster deployments each with a smaller group of users.
PRS- 362479	**Symptom:** PPS communicates to Checkpoint over physical IP of VIP holder interface rather than using VIP itself. **Conditions:** PPS communicates to Checkpoint over physical IP of VIP holder interface. **Work-Around:** All PPS cluster node's IP need to be configured in checkpoint as "host" for Checkpoint integration to work with PPS cluster.
PRS-352129	**Symptom:** Custom SOH AntiSpyware policy doesn't take Group policy configuration into consideration while evaluating in windows 10 OS. **Condition:** Group policy setting are not considered while evaluating the policy Windows 10 OS. **Workaround:** None
PRS-356794	**Symptom**: Users logging in from Windows Server OS clients are reported as Windows 7 clients on the Active Users page. **Conditions**: Users logging in through browser for Windows 2008, 2012, and 2016. Are shown as windows 7 clients on the active users page. **Workaround**: None
PRS-352127	**Symptom:** Custom SOH Antivirus policy doesn't take Group policy configuration into consideration while evaluating in windows 10 OS. **Conditions:** Group policy setting are not considered while evaluating the policy Windows 10 OS. **Workaround:** None
PRS-354907	**Symptom:** user-identity information provisioned by Pulse Policy Secure removed from Checkpoint Firewall post reboot. **Conditions:** Only after Checkpoint Firewall reboot **Workaround:** Delete the Checkpoint Firewall configuration from PPS and then reconfigure.
PRS-344807	**Symptom:** On Google Chrome browser, periodic host checking is not supported and can result in session termination if periodic checking is configured. It is recommended to use other browsers for agentless access with Host Checker and periodic checking enabled. **Conditions:** Agentless login with Host Checker Compliance enforced using Google Chrome **Workaround:** Use an alternative browser.
PRS-347062	**Symptom:** With Fortinet integration, only one use case/authentication mechanism (Agentless or Pulse) is supported at a time. This is because of the limitation with Forti Authenticator which supports configuration of only one Event ID per auth type indicator **Conditions:** User login from both Pulse and Browser **Workaround:** Users should login using either Pulse Client or Browser.
PRS-347512	**Symptom:** With Fortinet integration, for MDM and dot1x use cases, user access is provided only if accounting is enabled on WLC /Switches and WLC/Switch sends the end user IP in interim updates. Otherwise user access will be denied in Forti Authenticator **Conditions:** User authenticates via 802.1X or MDM. **Workaround:** Radius Accounting should have been enabled on Switches/WLC.
PRS-360918	**Symptom:** SNMP scan does not happen after importing 2000 switches via xml import. **Conditions**: Import xml with SNMP switch config having 2000 switches. **Workaround**: PPS restart is needed for SNMP to poll all switches after importing 2000 switches.
PRS-351666	**Symptom**: Traps processing will not stop, when Switch user modified from snmpv3 trap supported user to unsupported user in PPS SNMP device. **Conditions**: Switch delete and re-add in SNMP device list without reboot. **Workaround**: After rebooting the PPS device, PPS will not process v3 traps. Restart the PPS services on endpoint.

Problem Report Number	Release Note
PRS-349430	Symptom: MAC authentication login rate is slow with high rate of logins on PSA5000. Conditions: Login rate for MAC authentication is lower when the number of sessions on the same machine reaches 30k+. Workaround: If the login rate is high, authentication may be performed multiple times.
PRS-366544	Symptom: Pulse Client and browser connection fails when CVE check rule is configured with ESAP 3.2.5 onwards. Conditions: Compliance check passes for the first time but fails at every periodic check until CVE rule is removed or lower ESAP versions are activated. Workaround: Admin should activate ESAP 3.2.4 or lower versions to evaluate CVE checks.
Cloud Application Visibility	
PRS-365349	Symptom: The user can disable CAV proxy setting in Firefox browser. Condition: When the user tries to modify CAV proxy settings in Firefox browser. Workaround: The Administrator must block users to modify proxy settings in Firefox browser.
PRS-366171	Symptom: CAV proxy exceptions list is not set based on the connecting server when connection is transferred from PPS to PCS Condition: When the user connection changes from PPS to PCS with CAV enabled role. Workaround: Use "Preserve Client Side" proxy option, in VPN connection profile.
PRS-366210	Symptom: Pulse SAM stops sending traffic to PCS when CAV is enabled for a user role. Conditions: When user logs in to PPS/PCS using Pulse Client with user role enabled on Pulse SAM and CAV. Workaround: CAV role should not be enabled for Pulse SAM enabled user role.
PRS-365717	Symptom: The Cloud Application Visibility is not supported when Client/Server proxy is configured. Conditions: If the admin configures VPN Connection Profile with Client/Server proxy then Pulse Client creates a PAC file with the proxy servers and the CAV proxy is bypassed. Workaround: NA Conditions: If PAC file is configured in user's Windows machine then CAV cannot perform proxy chaining. Workaround: NA Conditions: If user's Windows machine has a proxy configured (not configured using VPN Connection Profile), then CAV performs proxy chaining and intercepts the traffic. Workaround: Admin must configure "preserve client proxy settings" option in PCS VPN Connection Profile.
PRS-365513	Symptom: Cloud Application Visibility does not update the application visits to server for all Windows user accounts on same Windows machine. Conditions: When multiple users on same Windows machine access applications. Workaround: Each user in Windows should login to PCS/PPS using Pulse Client to update CAV application visits to server.
PRS-366325	Symptom: Active user session shows endpoint behind NAT when the connection is transferred from PCS to PPS for the first time. Condition: User has connected to PCS first and then established a connection with PPS. Workaround: User has to disconnect the session and reconnect while moving from PCS to PPS for the first time.

New Features in 9.0R1 Release

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

Feature	Description
Provisioning PCS sessions to PAN firewall using IF-MAP through PPS.	Pulse Policy Secure (PPS) integrates with Palo Alto Network's (PAN) Firewall to provision user's identity information (user name, roles and IP address) to PAN firewall using REST API. You can provision Pulse Connect Secure (PCS) user's identity information to PAN firewall using IF-Map so that access control can be provided for PCS users accessing resources protected by PAN Firewall.

Feature	Description
Host Checker Enhancements	• Support for Patch Management rule configuration on Mac OS platform. • Support for OS check type rule configuration on Mac OS platform. • Support for configuring Common Vulnerability and Exposure (CVE) Check Rules on Windows platform. • Host Checker supports the caching of previous HC evaluation and performs the HC evaluation after a defined amount of time (For example, 1 week) instead of every time the user connects.
Guest Access Compliance	PPS supports compliance check enforcement for Guest User login (for WLC and Cisco Wired Switch).
RFC (6218) Cisco Key Wrap support	PPS supports Advanced Encryption Standard (AES) key wrap for RADIUS.
Admission Control based on PAN firewall alerts	PPS receives the threat alert information from Palo Alto Networks firewall and takes the appropriate action on the PPS user session based on the admission control policies configured in PPS.
REST API support	PPS supports REST API based configuration.
TACACS+ support	PPS supports network device administration using TACACS+.
Clustering Support	PPS supports clustering on Hyper-V and KVM platforms.
Default VLAN for all untagged traffic	VLANs can now be added to all the interfaces – Internal, External, and Management. A default VLAN can be specified to tag all the egress packets on that interface.
JITC Certification	• Password Strengthening. • Re-Authentication of Admin Users • Configuration Change Notification for Admin Users. • Notification for Unsuccessful Admin Login Attempts.
NDcPP Certification	• When NDcPP option is enabled, only NDcPP allowed crypto algorithms are allowed. • Device/Client Auth certificate 3072-bit key length support. • Not allowing Import of Device/Client Auth Certificate if Respective CAs are not in Trusted Stores. • Not allowing Importing of Device Certificate without Server Authentication EKU (Extended Key Usage). • Device/Client Auth/CA certificate revocation check during Certificate Import · Syslog/Pulse one server certificate revocation check during TLS connection establishment. • Not Allowing 1024-bit Public Key Length Server Certificate from Syslog/Pulse one server during TLS connection. • Many other NDcPP Compliant Support mentioned in https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10785 for PPS.
Distributed Profiler	Pulse Secure Profiler now supports profiling endpoints when the endpoints are connected to the PPS through a WAN. This is often the case in distributed networks where several “branch” offices connect to a central datacenter. By installing a “Profiler Forwarder” in each of the branches, you can ensure all profiling happens locally in the LAN, and the results are sent to the “remote” Profiler running in the datacenter.
Profile Management	Pulse Secure Profiler now supports browsing and searching through profiles that ship with Profiler, so you can know how a device gets profiled when it attaches itself to the network. Also, using edit capability, you can modify the profile, so the updated profile is instantly applied to all existing endpoints, as well as to new devices that have the same fingerprint.
SSH Collector	In previous releases, the OSX devices were fingerprinted mainly through the DHCP collector. In this release, fingerprinting the OSX endpoints is improved by using the SSH collector.
Export/Import CSV	You can now import data into the DDR report by using a CSV (comma-separated) file. In addition to just importing the data, you can also define an additional “custom” field that can be used for role-mapping as well.
Export/Import Profiler database	You can now export or import the full binary of Profiler database for archival purposes.

Fixed Issues in 9.0R1 Release

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

Problem Report Number	Release Note
PRS-360032	Summary: On the IF-MAP server the VIP failover is not working in Active/Passive cluster mode with PAN firewall.
PRS-353358	Summary: User Login Session not removed from PPS when Option "Policy applies to all roles OTHER THAN those selected below" chosen in Fortinet admission control policy.
PRS-355796	Summary: After upgrading the IF-MAP server, the existing IF-Map clients connected to the IF-MAP server gets disconnected. The UI wrongly shows GREEN status as connected, but all export request gets rejected as un-recognized client.
PRS-359636	Summary: After enabling/disabling the Active node the Passive node in IF-MAP server is not getting synchronized with the Active node and you might see some wrong entries.
PRS-356704	Summary: VA-SPE/PSA-V cluster cannot be created if the management port is not enabled on the nodes.
PRS-347064	Summary: With Fortinet integration, user access is given only in case the user is assigned single role on PPS. If user is assigned more than one role, access is not given by FortiGate Firewall. This is because of the limitation with Forti Authenticator which supports parsing of only role in the log messages.

Unsupported Features in 9.0R1 Release

None.

Known Issues in 9.0R1 Release

The following table lists Known issues in 9.0R1 release.

Problem Report Number	Release Note
PRS-359313	Symptom: Endpoint compliance fails when host checker policy is saved on the Policy page immediately after modifying the rule. Conditions: If Host checker policy is immediately saved after modifying the rule. Workaround: The user need to re-try the Pulse connection and compliance check will pass.
PRS-358212	Symptom: The compliance check will fail if the Patch management product is not changed to "Software Update (2.x)" after toggling from V3 SDK to V4 SDK on MAC OS. Conditions: When Patch Management policy is enabled with Product as "Software Update (10.11/10.12/10.13)" under V3 SDK and Admin toggles to V4 SDK, the Product mapping need to be modified by explicitly changing the Product name as "Software Update (2.x)" and save the policy for host checking to pass. Workaround: Admin has to explicitly change the Selected product as "Software Update (2.x)" under the Patch management rule and save it.

Problem Report Number	Release Note
PRS-361154	Symptom: When an active node is disabled and enabled back in AP cluster, endpoint table is deleted from both the cluster nodes. Conditions: Disabling and enabling an active node in AP cluster. Workaround Users must re-login.
PRS-362328	Symptom: A-SPE cluster VIP-Failover happens automatically. Conditions: Cluster VIP fail over. Workaround: None
PRS-362267	Symptom: Fed client not removing exported sessions though fed server is not reachable for more than 200 seconds. Conditions: Exported session not getting deleted after client loses connectivity. Workaround: None
PRS-356373	Symptom: XML Import of named users does not validate if XML file is valid. Conditions: Importing an invalid XML. Workaround: Export an existing named user table. modify it before importing it. Ensure XML information is correct.
PRS-355333	Symptom: Named users tab not loading with 150k unique named users on the system. Conditions: Admin will not be able to view or delete any named users if they have 150k or more named users on their system. Workaround: Split the deployment into multiple stand alone and cluster deployments and have a smaller group of users go to each gateway.
PRS- 362479	Symptom: PPS communicates to Checkpoint over physical IP of VIP holder interface rather than using VIP itself. Conditions: PPS communicates to Checkpoint over physical IP of VIP holder interface. Work-Around: All PPS cluster node's IP need to be configured in checkpoint as "host" for Checkpoint integration to work with PPS cluster.
PRS-352129	Symptom: Custom SOH AntiSpyware policy doesn't take Group policy configuration into consideration while evaluating in windows 10 OS. Condition: Group policy setting are not considered while evaluating the policy Windows 10 OS. Workaround: None
PRS-356794	Symptom: Users logging in from Windows Server OS clients are reported as Windows 7 clients on the Active Users page. Conditions: Users logging in through browser for Windows 2008, 2012, and 2016. Are shown as windows 7 clients on the active users' page. Workaround: None
PRS-352127	Symptom: Custom SOH Antivirus policy doesn't take Group policy configuration into consideration while evaluating in windows 10 OS. Conditions: Group policy setting are not considered while evaluating the policy Windows 10 OS. Workaround: None
PRS-354907	Symptom: user-identity information provisioned by Pulse Policy Secure removed from Checkpoint Firewall post reboot. Conditions: Only after Checkpoint Firewall reboot Workaround: Delete the Checkpoint Firewall configuration from PPS and then reconfigure.
PRS-344807	Symptom: On Google Chrome browser, periodic host checking is not supported and can result in session termination if periodic host checking is configured. Hence it is recommended to use other browsers for agentless access with host checker. Conditions: Agentless login with Host Checker Compliance enforced using Google Chrome Workaround: Use Mozilla Firefox browser.

Problem Report Number	Release Note
PRS-347062	**Symptom:** With Fortinet integration, only one use case/authentication mechanism (Agentless or Pulse) is supported at a time. This is because of the limitation with Forti Authenticator which supports configuration of only one Event ID per auth type indicator **Conditions:** User login from both Pulse and Browser **Workaround:** Users should login using either Pulse Client or Browser.
PRS-347512	**Symptom:** With Fortinet integration, for MDM and dot1x use cases, user access is provided only if accounting is enabled on WLC /Switches and WLC/Switch sends the end user IP in interim updates. Otherwise user access will be denied in Forti Authenticator **Conditions:** User authenticates via 802.1X or MDM. **Workaround:** Radius Accounting should have been enabled on Switches/WLC.
PRS-360918	**Symptom:** SNMP scan is not happening after importing 2000 switches config using xml import. **Conditions**: Import xml with SNMP switch config having 2000 switches. **Workaround**: PPS restart is needed for SNMP to poll all switches after importing 2000 switches config using xml import
PRS-351666	**Symptom**: Traps processing will not stop, when Switch user modified from snmpv3 trap supported user to unsupported user in PPS SNMP device. **Conditions**: Switch delete and re-add in SNMP device list without reboot. **Workaround**: After rebooting the PPS device, PPS will not process v3 traps. Restart the PPS services on endpoint.
PRS-349430	**Symptom**: MAC auth login rate is slow with high rate on PSA5000 only. On PSA7000 there is no impact. **Conditions**: Login rate for MAC auth is lower when the number of sessions on the same machine reaches 30k+. **Workaround**: If the login rate is too high for low end devices, authentication may be performed multiple times.

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.

Revision		Description
2.3	September 2018	Updated to Release 9.0R2.1
2.2	August 2018	Updated the cluster configuration limitation for CAV.
2.1	August 2018	Updated CAV, IoT, session bridging, and Mac OS 64-bit HC support for Release 9.0R2.
1.0	April 2018	Updated for Release 9.0R1