![Pulse Secure]

Pulse Policy Secure

Release Notes
PPS 9.0R5 Build 51971
Pulse Profiler Version 1.5 (FPDB Version 39)
PDC 9.0R5 Build 1907.1
Default ESAP Version: ESAP 3.3.5

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

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
4.3	September	9.0R5 Updates
4.2	July 2019	9.0R4.1 Updates
4.1	May 2019	Added PRS 371536, PRS 373619 as Known Issues in 9.0R4.
4.0	April 2019	Updated for 9.0R4
3.4	January 2019	Virtual Pulse Secure Appliance (PSA-V) term is updated under VA editions.
3.3	December 2018	Updated for Release 9.0R3.1. Only the build number has been updated.
3.2	December 2018	Updated for Release 9.0R3.
2.0	July 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

Contents

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

Note: From 9.0R1, Pulse Secure has begun the End-of-Life (EOL) process for the VA-SPE virtual appliance. In its place, Pulse Secure has launched 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	- HP ProLiant DL380 G5 with Intel(R) Xeon(R) CPU - ESXi 6.5
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 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
9.0R4.1	Yes	
9.0R3	Yes	
9.0R2	Yes	
9.0R1	Yes	
5.4Rx	Yes	
5.4Ry		Yes

Upgrade From	Qualified	Compatible
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 installed.
- To continue use of 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.
- On a 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 9.0R5 without core license. Follow these steps to upgrade:
1. If PSA-V is running 5.3Rx:
   a. Upgrade to 5.4R3 or later.
   b. Install Core license through Authcode.
   c. Upgrade to 9.0R5.
2. If PSA-V is running 5.4R1:
   a. Upgrade to 5.4R3 or later.
   b. Install Core license through Authcode.
   c. Upgrade to 9.0R5.
3. If PSA-V is running 5.4R3 or later:
   a. Install Core License through Authcode.
   b. Upgrade to 9.0R5.

Note: Upgrading from 5.4R2 or below to 9.0R5 is not supported for VM images.

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 9.0R5 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: Release 9.0R5

Feature	Description
Report Max Used Licenses to HLS|VLS	From 9.0R5 release, the licensing client starts reporting 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.

Fixed Issues: Release 9.0R5

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

Problem Report Number	Release Note
PRS-374583	**Symptom**: Behavior of "re-authentication" and "termination" options in radius Return Attribute policy page is interchanged.
PRS-379855	**Summary**: Host checker did not get installed properly" error appears on browser after the machine reboot.
PRS-377798	**Summary:** ACE server "node verification file" and SDCONF.rec being overwritten or cleared when "Auth Server" is included in Group settings.
PRS-377437	**Summary**: Event logs show "License server low-level protocol error Code = [47]" error on licensing client.
PRS-374641	**Summary**: Post upgrade to PPS 9.0R3.1, we observe "License server low-level protocol error Code = [47]" error on licensing client every 10 minutes.
PRS-374603	**Summary**: Syslog missing event logging info when upgrading.
PRS-374367	**Summary**: PSAL launch failed when browser Proxy is configured.
PRS-375060	**Summary:** PPS sends multiple Profiler WMI Scan message with in 1 minute.
PRS-372750	**Summary**: Sponsor GUAM: PPS is not deleting the desired user account from Sponsor portal.
PRS-376765	**Summary:** Guest sponsor wouldn't see guest entries that are due for approval upon logging on to PPS.

Known Issues: Release 9.0R5

The following table lists Known issues in this release.

Problem Report Number	Release Note
PRS-371733	**Symptom**: Assigned VLAN is not updated if fetched on the next poll and always shows default configured VLAN. **Conditions**: Assigned VLAN will not update in DDR on next switch poll, When VLAN Changed for the connected port due to Radius return VLAN attribute **Workaround**: NA

New Features: Release 9.0R4.1

There are no new features for this release.

Noteworthy changes: Release 9.0R4.1

None

Fixed Issues: Release 9.0R4.1

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

release.

Problem Report Number	Release Note
PRS-372999	**Summary**: Host Checker is failing for Host Checker(OS-Check only) for Chrome OS 71.0.3578.127 with Pulse Connect Secure 9.0R1 firmware version.
PRS-374597	**Summary**: Anti-Virus Definition check (number of updates) has been fixed by upgrading the **Opswat UpdateVerify** SDK from 2.3.15.208.
PRS-374702	**Summary**: Configuring PPS with Initial setup wizard fails with 500 Internal error, when Host Checker policy type is Process.
PPS-5674	**Summary**: Anti-Virus Signature evaluation has been optimized by changing server-side and client-side capabilities.
PRS-376889	**Summary**: Consider the drives for evaluation and ignore the drives only if API output says the drive is not capable of encryption explicitly.
PRS-374974	**Summary**: Fed client leaves L2 sessions as a stale entry in Fedwide sessions (IFMap Server) while removing the bridged sessions in the Fed client. Hence, it results in Fed server database full.

Known Issues: 9.0R4.1 Release

There are no new known issues for this release.

New Features: 9.0R4 Release

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

Feature	Description
Host Checker enhancement	• System Integrity Protection (SIP) can now be checked by Host Checker on macOS endpoints running macOS El Capitan (10.11) and higher • Command rule enables administrators to check for specific versions of the installed applications on macOS endpoints.
Backup administrator account for LDAP	PPS supports two LDAP administrator accounts. Adding the backup account, PPS now has the option to fallback from one account to other in case of authentication failure.
Remove and refresh expired Root CAs	Upgrading to 9.0R4 refreshes the system with latest set of Trusted Server CAs and removes any expired certificates from default Trusted Server CA store.
Support for snmpget	This release supports snmpget for the following: • SNMP monitoring of last day to connect to Pulse cloud or similar. • SNMP get max number of licensed users displayed under the licensing summary.
Send service traffic via any physical interface	Prior to this release, the NTP, SNMP, Syslog, and Log archiving services were set to send the traffic through Management port by default. In case the Management port was not available, the traffic was routed through Internal port. Starting with this release, Administrators can modify the settings of NTP and other services to any physical interface.
VA Partition for VMWare	VA Partition for VMWare to increase disk space.

Noteworthy changes: Release 9.0R4

None

Fixed Issues: Release 9.0R4

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

Problem Report Number	Release Note
PRS-365367	**Summary**: Profiler: Complete endpoint profiler data may not register on Pulse One properly.
PRS-365809	**Summary**: Profiler: SNMP polling may freeze and require a restart of services.

Problem Report Number	Release Note
PRS-372237	**Summary: Profiler:** Classifier crashes if Nmap smb_os_results are None.
PRS-368044	**Summary**: Host Checker: Cisco Malware protection fails to be detected properly.
PRS-370090	**Summary**: Host Checker: Virus Definition check for updates for Palo Alto Traps may fail.
PRS-370205	**Summary**: Pulse Client with Host Checker takes too long for 802.1X authentication and may time out for end users with many virtual adapters.
PRS-370606	**Summary**: Monitoring: There is now an option to refresh the dashboard every 24 hours.
PRS-371035	**Summary**: Host Checker/Logging: Certificate hash may be recorded in the user access log when doing machine cert authentication.
PRS-371747	**Summary**: Host Checker: Unsupported products may be displayed in the selection list.
PRS-371973	**Summary**: Host Checker: McAfee AV state may not be correctly identified.
PRS-372031	**Summary**: Cannot delete notes in the Device Discovery Report.
PRS-370785	**Summary:** Host Checker: Virus Definition Check for updates for Avast Internet Security 18.x doesn't with V4 SDK.
PRS-372386	**Summary**: Cisco VoIP phone Model CP-7960G was not profiled properly.
PRS-372355	**Summary**: "BEAM video conference robot" is missing in the profiler database.
PRS-371733	**Symptom**: Assigned VLAN is not updated if fetched on the next poll and always shows default configured VLAN.

Known Issues: Release 9.0R4

The following table lists Known issues in 9.0R3 release.

Problem Report Number	Release Note
PRS 371536	**Symptom:** Host Checker: Virus Definition Check for updates fails for K7 Virus Security ZERO (14.x). **Condition:** When Admin configures the policy with Virus Definition update for K7 Virus Security Zero (14.x). **Workaround:** NA
PRS 373619	**Symptom:** Host Checker: Virus Definition Check for updates fails for AVG Free Antivirus (19.2.x). **Condition:** When Admin configures the policy with Virus Definition update for AVG Free Antivirus (19.2.x). **Workaround:** NA

Fixed Issues: Release 9.0R3.1

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

Problem Report Number	Release Note
PRS-371257	**Summary:** Ensure all the Installer components are available on a fresh installation using Virtual Appliance (VA) image.

New Features: Release 9.0R3

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

Feature	Description
Behavioral Analytics	Behavioral Analytics is a controlled feature and it provides enhanced security for managed and unmanaged devices including IoT with any anomaly detected based on user/device traffic patterns. • Anomaly detection of devices based on traffic for IoT devices • Adaptive authentication using secondary authentication server • Potential Malware detection - DGA attacks ℹ️ Note: • Behavioral Analytics (Anomaly Detection, Potential Malware Detection) is a controlled feature and used for only evaluation purposes for this release. • Adaptive Authentication feature is part of PPS license. Anomalous traffic detection for IoT devices and Potential Malware detection requires Behavioral Analytics license to be installed on PPS.
IoT Auto Provisioning using PAN firewall	PPS enables secure access to IoT devices through PPS/Profiler and PAN 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.
RADIUS dictionary updates	802.1x port-based security is enhanced with updated RADIUS dictionary attributes.
Juniper SDSN Integration (Alert-based Integration)	PPS enhances the security by isolating or taking action at the endpoint level based on threat alerts receives from Juniper SDSN.
Host Checker – NETBIOS and Mac address check for MacOS	Improve security on Mac OS platform.
L2 Simplification	Simplification of L2 configuration using RADIUS return attribute policy (ACL name and ACL rule).
Secondary Authentication Server	PPS supports authentication using a Secondary Authentication Server.
802.1X support for Huawei Switch	PPS supports integration with Huawei Switch/WLC for 802.1X support.
Support default VLAN tagging in PSA-V clusters	Default VLAN ID is supported in the clustered environment.
Decoupling of AAA Servers from Internal Interface	Allows the administrator to choose the communicating interface or the network for each authentication server independently.
Upgrade to OpenSSL 1.0.2n	This feature automatically upgrades PPS to OpenSSL version 1.0.2n when the system software is upgraded.
Support TLS V1/2 LDAPS	This feature provides Outbound OpenSSL options apply to LDAPS and Start TLS.
RSA support in TACACS+	PPS supports RSA server authentication in TACACS+.
Custom HTTP response headers for security	This feature provides option to the administrator to enter a new custom HTTP header that is added to the responses. The user should be able to specify: 1. HTTP Header Name 2. HTTP Header Value If the header is already present, the system does not overwrite it.
REST API Enhancements	Enhancements include: • Export, import full configuration via REST • API to pull license state from server • API to fetch all groups available in a configured LDAP or AD authentication server • APIs to get active sessions, system information, leased client counts, configure device certificates • APIs to configure certificates based on CSR workflow • APIs to perform cluster operations Realm-based admin login for REST APIs
Profiler	
Agentless Mode with Profiler	Agentless Host Checker with Profiler allows user authorization based on the user device attributes without the need to install agents on their machines.
Profile Groups	The devices can be grouped based on device attributes and rules for easy access and identification. Group names can be used in role mapping rules, resource policies, filtering etc.

Feature	Description
Profiler Report Scheduling	The Profiler reports (PDF) can be scheduled, and the reports can be delivered in the e-mail notifications to the specified addresses.
On-Demand subnet scan	On demand subnet scan allows administrator to manually trigger active collector (NMAP, WMI and SSH) scan and discover devices in a network. The discovered devices are added to the Profiler database.
DDR enhancements	Device Discovery Reports table is enhanced with switch port view and sort with Profiler authentication server options.

Noteworthy changes: Release 9.0R3

None

Fixed Issues: Release 9.0R3

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

Problem Report Number	Release Note
PRS-366184	**Summary**: Resource Access Policy failed with errors "Unable to load Manufacturer" and "Failed to Save due to resource limit exceeds 32768 characters.
PRS-366813	**Summary:** Pulse Host check failure message will not be displayed in Embedded browser with custom sign-in pages using Pulse client.
PRS-368009	**Summary:** Resources list not updated in IoT policy when all devices deleted at same time from Device Discovery page.
PRS-356373	**Summary**: Import of malformed XML file for named user account records is allowed.
PRS-366544	**Summary**: Pulse Client and browser connection fails when CVE check rule is configured with ESAP 3.2.5 onwards.
PRS-368072	**Summary:** Profiler: Manually add device profiler name is not updating in DDR.

Known Issues: Release 9.0R3

The following table lists Known issues in 9.0R3 release.

Problem Report Number	Release Note
PRS-366966	**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. **Conditions**: Configuring PPS as connector in Juniper PE. **Workaround**: Ensure that the Port number is always set to 443.
PRS-367195	**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. **Conditions**: Configuring PPS as Connector in Juniper PE. **Workaround**: Juniper SDSN integration with PPS requires creating a local Admin user on PPS.
PRS-367291	**Symptom:** Certificate Authentication fails due to configuration of "Skip Revocation when OCSP/CDP server is not available" for HC policy enforced at realm level. **Condition:** When admin enables Skip Revocation check and OSCP server is not reachable. **Workaround:** Set the OSCP timeout to less than 5 seconds.
PRS-367349	**Symptom**: Anomaly attribute based role mapping rules accept any random string **Condition**: Configuring anomaly role mapping rules based on custom expressions on user realm or MAC Address realm. **Workaround**: Configure anomaly role mapping rules based on custom expressions with only supported strings , 'dga_detected' or 'unknown_server' or 'unknown_domain'.
PRS-368055	**Symptom:** Admin is allowed to create anomaly role mapping rules based on custom expressions when UEBA license is not installed. **Condition**: Configuring anomaly role mapping rules based on custom expressions when Behavioral Analytics license is not installed **Workaround:** Install Behavioral Analytics License.
PRS-366296 PRS-369738	**Symptom:** Authentication to PPS fails as Duo custom sign-in pages are not displayed. **Condition**: User authenticates to PPS and assigned realm is configured with Duo as secondary authentication server. **Workaround:** Use passcode based Duo authentication.
PRS-367024	**Symptom:** Authentication fails for browser based login for Duo and LDAP combination with predefined user as <USER> in secondary authentication server. **Condition:** User authenticates to PPS and assigned realm is configured with Duo as primary and LDAP as secondary auth server **Workaround:** Use passcode based Duo authentication.
PRS-370902	**Symptom:** Behavioral Analytics dashboard is not displaying charts for potential malware and anomalous traffic from IoT devices for more than 4 device categories intermittently. **Condition**: Device anomalies are reported for more than 4 different unmanaged device categories. **Workaround**: Use custom filters to display the dashboard data.
PRS-368136	**Symptom**: VIP failover fails in A/P cluster when the Active node becomes unreachable with SPAN configured on external port. **Condition**: Active node becomes unreachable in A/P Cluster with Local SPAN enabled on cluster nodes' external port. **Workaround**: Configure Remote SPAN.
PRS-368689	**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. **Condition:** When OS check Host checker rule is evaluated with new Pulse client connecting to pre-9.0R3 PPS server. **Workaround:** Pulse client on MAC platform and PPS server need to be 9.0R3 for OS Check host checker policy to work as expected.
PRS-368967	**Symptom:** Host checker fails on Mac OS 10.14 Mojave endpoint when Activate Older OPSWAT SDK in ESAP is enabled. **Condition:** When ESAP with V3 SDK is activated on the server. **Workaround**: Administrator should activate ESAP with V4 SDK on PPS for Host check to work as expected.

Problem Report Number	Release Note
PRS-370903	**Symptom**: MAC address is not updated in the user session details. **Condition**: Custom sign-in pages are configured on PPS and user is presented with Embedded browser while authenticating to PPS using Pulse Client. **Workaround**: Do not use custom sign-in pages.
Profiler	
PRS-369079	**Symptom**: For Agentless Host Checker with Profiler, Antivirus Rule with "virus definition age" check may fail. **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. **Workaround**: Create the rule with (expected number of definition age + 1) days.
PRS-367687	**Symptom**: Remote profiler is unable to communicate with Profiler; hence the remote endpoints are not profiled. **Conditions**: If self-signed certificate is used on Profiler Authentication server. **Workaround**: Using a CA signed certificate on Profiler server.
PRS-361246	**Symptom:** Endpoint session status is not updated in DDR table if the same endpoint is imported through Binary configuration. **Conditions:** Importing profiler data using Binary configuration. **Workaround:** Reconnect the existing user session.
Cloud Application Visibility	
PRS-370268	**Symptom**: CAV fails to configure proxy on endpoint, when Juniper SRX is configured as an Infranet Enforcer for a resource. **Condition**: Juniper SRX is configured as Infranet Enforcer. **Workaround**: N/A
PRS-370249	**Symptom**: CAV policies are not applied when endpoints establish dot1x connection with a switch/access point. **Condition**: Authenticator is a third-party device and is configured to use PPS as authenticating server. **Workaround:** N/A
PRS-370237	**Symptom**: CAV policy updates are not sent to PPS if CAV Database is updated with PCS IP address. **Condition**: If CAV database at client side is updated with PCS IP address and the user establishes L2/L3 connection. **Workaround:** N/A
PRS-370123	**Symptom**: DNS resolution fails after CAV is re-enabled at user role level. **Conditions**: If already added user role is deleted from the CAV policies. **Work Around**: - N/A
PRS-369277	**Symptom**: CAV feature does not work when Pulse SAM is enabled on client. **Conditions**: Pulse SAM and CAV enabled for the same role. **Work Around**: - N/A
PRS-369891	**Symptom:** Authentication token fetching is failing under NATed environment on Pulse client for CAV policies update. **Conditions:** PCS configured behind a NAT device. **Work Around:** N/A
PRS-369279	**Symptom:** Lockdown is not working properly if CAV policies are configured. **Conditions:** Enabling CAV with lock down. **Work Around:** N/A

New Features: Release 9.0R2

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.
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: Release 9.0R2

- **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: Release 9.0R2

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.
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.

Problem Report Number	Release Note
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: Release 9.0R2

None.

Known Issues: Release 9.0R2

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-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.

Problem Report Number	Release Note
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: Release 9.0R1

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.
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: Release 9.0R1

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**: 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: Release 9.0R1

None.

Known Issues: Release 9.0R1

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**: Changes done in Host checker policy will be evaluated at next periodic hand shake time configured on PPS.
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.
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.

Problem Report Number	Release Note
PRS-362328	**Symptom:** A-PSA-V 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.
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

Problem Report Number	Release Note
	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.**