Pulse Policy Secure: Release Notes

PPS 9.1R7 Build 3265

Pulse Profiler Version (FPDB Version 44)

PDC 9.1R7 Build 2525

Default ESAP Version: ESAP 3.4.8

ublished June 2020

Document Version 1.3

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

Pulse Policy Secure: Release Notes

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 http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Introduction

This document is the release notes for Pulse Policy Secure. It contains information about what is included in this software release: New features, known issues, fixed issues, product compatibility, and upgrade instructions.

Product Compatibility

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 Virtual Pulse Secure Appliance (PSA-V) editions.

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 6.7
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 2016 and 2019
Azure-V	• Standard DS2 V2 (2 Core, 2 NICs) • Standard DS3 V2 (4 Core, 3 NICs) • Standard DS4 V2 (8 Core, 3 NICs)
Amazon Web Services (AWS)-V	• T2.Medium (2 Core, 2 NICs) • T2.Large (4 Core, 3 NICs and 2 NICs) • T2.Xlarge (8 Core, 3 NICs and 2 NICs)

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

Note:

- From 9.1R1, VA-DTE is not 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

New Features

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

Features	Description
Release 9.1R6	
Show Serial Number under Licensing Tab	The PPS Licensing tab (System > Configuration > Licensing) now displays the Serial Number.
Hardware ID is available on System Maintenance Tab	The Hardware ID is now included in System Maintenance > Platform tab.
Host Checker policies hyperlinked to policies page	Host Checker policies is now clickable (hyperlink) in User Realms page.
Release 9.1R5	
Pulse Policy Secure on Amazon Web Services (AWS)	Provides NAC services (802.1x, MAC Auth, L3 Firewall Enforcement) to multiple on-premise networks using PPS deployed on Amazon Web Services (AWS) cloud.
SNMP policy enforcement (Alcatel-Lucent, Huawei, Arista)	SNMP policy enforcement is now supported on Alcatel-Lucent, Huawei and Arista switches.
McAfee ePolicy Orchestrator (ePO) integration	Pulse Policy Secure (PPS) integration with the McAfee ePolicy Orchestrator (ePO) provides complete visibility of network endpoints and provide end to end network security. The PPS integration with McAfee ePO allows Admin to perform user access control based on alerts received from the McAfee ePO.
Splunk syslog add-on and Dashboard app	Splunk application for PPS uses the indexed data to render various charts and to show useful information on dashboard. The Pulse Secure App for Splunk allows you to view PPS data in a dedicated, customizable Splunk dashboard. This bidirectional interaction with Splunk allows security managers to quickly monitor the current operational/security posture.
IPv6 Support for Syslog, NTP and Log Archive	PPS now supports sending syslog messages to a syslog server using IPv6 address. Time synchronization using NTP server is now supported with IPv6 address. PPS also supports transferring archived PPS logs using FTP and SCP over IPv6 network.
SBR to PPS migration	SBR configurations (802.1x and Mac Address Authentication) can be migrated to PPS using XML import.
ECC certificate support for Juniper SRX firewall connection	PPS now supports Elliptic Curve Cryptography (ECC) certificate for SRX firewall connections.
Host Checker policy to detect hard disk Encryption in progress	Host Checker policy to allow detection of hard drive encryption in progress.

Features	Description
MSSQL support on PPS with external DB	PPS supports MSSQL as external Auth server for 802.1x and Layer 3 authentication.
PDF report capability	This feature in PPS allows the user to download the reports (User Summary Report, Single User Activities, Device Summary, Device Discovery, Single Device Activities, Authentication, Compliance, Infected Devices) in PDF format. Apart from the CSV, Tab Limited option, there is an option called PDF provided in PPS Reports.
Profiler	
Backup and Recovery, and Disaster management	Profiler deployments provides backup mechanism for enhanced disaster management (Profiler Forwarder, Remote Profiler, Centralized Standalone Profiler).
Viptela Switch Support	Viptela Switch support is added for SNMP Visibility.
Release 9.1R4	
Pulse Policy Secure on Azure platform	Provides NAC services (802.1x, MAC Auth, L3 Firewall Enforcement) to multiple on-premise networks using PPS deployed on Microsoft Azure cloud.
Huawei - Guest Access	Supports guest access use cases with Huawei WLC.
Mist Juniper WLC	Supports 802.1x and guest access with Juniper Mist WLC.
TACACS+ support for Arista Switch	Support Administrator access control for Arista.
Common Access Card (CAC) support with TACACS+	Supports TACACS+ authorization using Pulse Policy Secure. Authentication is performed by the third-party authentication server.
Provisioning only User-ID information to PAN firewall	Provides an option to admin in Auth table mapping policy to push only IP-User mapping to Palo Alto Networks firewall.
System Local user attribute support (Framed-IP-Address)	Allows to define user Attributes for system local server and associate those attributes to user names, including Framed-IP address. Values of those attributes to be defined for each user name.
Strong Hash	Supports protecting passwords stored in local authentication server using strong hash.
Release 9.1R3	
VSYS Support in PAN	Pulse Policy Secure supports provisioning user identity and resource access/IoT policies to multiple VSYS or specific VSYS (other than vsys1) on PAN firewall.
IBM QRadar Integration	Pulse Policy Secure along with IBM QRadar provides user access control based on threats/events received from IBM QRadar.

Features	Description
Splunk Integration	Splunk alert based integration supports sending alert information from Splunk to Pulse Policy Secure. PPS uses its existing functionality of admission control, L2/L3 enforcement and provides role based access control to secure the network.
Fortinet Identity management using RADIUS accounting messages	Pulse Policy Secure supports integration with FortiGate firewall using RADIUS accounting messages.
Mysql support	Pulse Policy Secure supports MYSQL as external Authentication server.
Local user account import through CSV in System local DB	Allows importing user accounts via CSV file in System local auth server. The local authentication server is an authentication database that is built in to PPS.
SNMP Enforcement using ACL for 3Com, DELL	SNMP ACL enforcement support is now expanded for 3Com and Dell switches.
SNMP Enforcement using VLAN for 3Com, Juniper and DELL	SNMP VLAN enforcement support is now expanded for 3Com, Juniper and Dell switches.
One-to-One NAT support	PPS allows auth table provisioning for the endpoints behind NAT (One-to One NAT mapping).
vTM and PPS Integration for Load Balancing	The Platform Limit, Maximum Licensed User Count and Cluster Name attribute values are available for optimal load balancing.
Release 9.1 R2	
Alert based integration with Nozomi Networks	PPS along with Nozomi Networks provides threat detection and threat response in ICS/OT environ-ment.
Backup configs and archived logs on AWS S3/Azure Storage	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.
EasiSMS Gateway Support	PPS supports EasiSMS gateway through the SMTP server. EasiSMS uses an email format to send SMS to end user mobile phones.
Flag Duplicate Machine ID in access logs	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. 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.
Migration of Cisco ACS RADIUS/TACACS+ client configuration to PPS	Migrating RADIUS/TACACS+ client configuration configured on the Cisco ACS device.

Features	Description
Report Max Used Licens-es 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.
V3 to V4 Opswat SDK mi-gration	PPS supports the migration of servers and clients to Opswat v4 to take advantage of latest updates.
VA Partition	PCS/PPS supports upgrading from PCS 8.2Rx/ PPS 5.3Rx to 9.1R2 for the following supported plat-forms: • VMWare ESXi • KVM • Hyper-V 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.
Profiler	
Profiler dashboard update	Profiler dashboard supports chart for Profile Groups. This chart is also part of downloaded PDF re-port.
Windows defender and Microsoft Security Essen-tials support	Agentless Host Checker with Profiler supports Windows defender and Microsoft Security Essentials.
Release 9.1 R1	
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.
Google Auth Multi Factor Authentication	TOTP server can be added as a secondary auth server in PPS.
Machine certificate check on MacOS	Machine certificate check on Mac OS is now supported for PPS.
Meraki 802.1x and Guest Access support	802.1X and Guest Access support is qualified with Cisco Meraki WLC.
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 bridging for Linux Platform	PPS supports bridging the Layer 2 Native Supplicant 802.1X session with Layer3 Agentless (Browser based) Session on Linux platform.
Session Migration using Cert authentication	Session migration in an IF-MAP federated network supports Cert Auth and SAML auth
SNMP Enforcement using ACL (Cisco, HP, Juniper)	SNMP enforcement using ACL is supported for Cisco, Juniper and HP switches.

Features	Description
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	
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. Ad-min 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 end-points 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 pro-file groups.
Publishing IP address from Profiler to Active User Session	Admin can add IP address from Profiler to active session for L3 enforcement when RADIUS account-ing 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

The following table describes the major feature changes that are introduced in the corresponding release.

Feature	Description
Release 9.1R3	
OAC Client Removal	OAC client is deprecated beginning with Release 9.1R3.
Profiler	
Note: For release 9.1R3, the minimum version of the fingerprints package supported is 41.	
NMAP Upgrade	Upgraded NMAP database and Binary for improving the detection and classification of new devices.
SNMP Performance improvements	Improved endpoint devices detection using SNMP.

Fixed Issues

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

Problem Report Number	Summary
Release 9.1R7	
PRS-390665	The equal to (=) character is now supported in the Custom Attributes of TACACS+ Shell Policy.
PRS-388455	If epupdate_hist.xml is hosted internally with no authentication and if "Use Proxy Server" (With/without auth) is enabled with FQDN or IP Address, the first 3 characters are ignored thus causing it to fail. For example, proxy.domain.net is taken as xy.domain.net. This issue is now fixed for both PCS and PPS.
PRS-389209	With PCS 9.0R2-9.1R6 and Pulse 9.0R2-9.1R3, the client continues to send thae CAV traffic to PCS every 300 seconds even when Cloud Secure license is not installed. From PCS 9.1R7 onwards, the PDC client (Pulse 9.0R2-9.1R3) will contact the PCS server only once per user session - KB44410.
Release 9.1R6	
PRS-390130	PPS now sends the appropriate status code for authentication failure in Cisco Switch.
PRS-388996	CSV export of Profiler Device Discovery Report with large number of entries (>50,000) can now be performed without any failure.
PRS- 388645	After upgrading PPS to 9.1R3-9.1R5, slow Host Checker response is observed due to a very frequent re-evaluation of Cybereason Active Probe product.
PRS-389276	The corruption of blob during the epupdate results in Host Checker scan failure for users till next successful epupdate.
Release 9.1R5	
PRS- 387688	Inappropriate error displayed for 'Test Intune Connection is fixed. Appropriate error message is displayed.
PRS-381678	Cluster Enhancement: Improve VIP unreachable time during cluster upgrade. This works for cluster with version running release 9.1R5 and later.
PRS-380303	ECC device certificate support on PPS is now added for SRX connection. Juniper added ECC device certificate support from Junos Release 15.X.
PRS-382340	Dashboard was reporting incorrect Session based OS count in graphs. This issue has been fixed.
PRS-384845	Host Checker policy to detect Hard Disk encryption in progress is now added in this release.
PRS-385491	TLS handshake failed error messages observed after PPS upgrade is now fixed.
PRS-387624	When replica (IF-MAP) is not reachable, CombinedChangeLog files keep accumulating and consumes space on HDD partition till it reaches 95%. This issue is now fixed.

Problem Report Number	Summary
Profiler	
PRS-388101	Canon printer was misclassified on PPS Profiler. This issue is fixed in the latest fingerprint database.
PRS-387423	PPS Profiler was not detecting the next-gen Edge OS from IGEL devices. This issue is now fixed.
PRS-388953	Finger Print database was not loaded properly into the memory during initial loading of fingerprint file. This issue is now fixed.
PRS-387461	PPS Profiler full synchronization issue with Pulse One is now fixed.
PRS-387638	PPS Profiler Finger print database is now updated to detect ASUSTek COMPUTER INC" as Manufacturer.
PRS-388117	Full Sync start time used to be a default time, i.e., 01 Jan 1970 rather Current Time.
PRS-387717	The "View all 'Unapproved Devices'" link in E-mail received by admin for Device Approval was not getting redirect ed to Device Discovery Report. This issue is now fixed.
Release 9.1R4.2	
PRS-387461	While forwarder full-sync is in progress and new devices are getting discovered full-sync was aborted and restarted.
Release 9.1R4.1	
PRS-385491	TLS handshake failed error message observed due to state variable in RADIUS access request is fixed.
Release 9.1R4	
PRS-382021	Dismiss until next upgrade option is not working for banner related to perpetual licensing.
PRS-380327	Devices in Network Infrastructure Device are in Undiscovered state after importing Devices
PRS-380855	Profiler is polling deleted switches once after deletion.
Release 9.1R3.1	
PRS-382319	Port Bounce issue for SNMP VLAN enforcement with Cisco switch is now fixed.
PRS-382287	TNCS process fails randomly on the server while evaluating the Host Checker policies.
PRS-385089	Duplicate machine ID feature is reverted as part of this PR.
Profiler	
PRS-384666	PPS web interface is running extremely slow.
PRS- 384736	trap-collector process restarting due to high memory usage.

Problem Report Number	Summary
PRS-385372	"trap-collector" consuming high CPU during startup.
Release 9.1 R3	
PRS- 376979	Clear config on PPS set the default 'Account Lockout' values to zero for 'Guest Authentica-tion' server and this value cannot be modified or saved.
PRS 379003	End user always gets the remediation role even after endpoint meets all the End Point Security Policies.
PRS-377371	New device anomaly is not detected when connecting to Pulse via embedded browser
PRS-377957	PPS not sending auth table entry to correct vsys in PAN firewall
Profiler	
PRS-378960	In dashboard, Profiler name not retained when revisiting the same page after moving to another page.
Release 9.1 R2	
PRS- 376312	Factory reset from VMware VA console does not load the factory reset version and loads the current version.
PRS-376265	Invalid character error seen while adding Radius Return attribute value which contains "<" and ">" characters.
PRS-376465	Host Checker service in Pulse is crashing while performing policy monitoring when pulse client is retrying.
PRS-372699	NMAP scan profiling is inaccurate
PRS-372499	Session from Exported session list get purged on cluster if the passive node is disabled, re-booted and rejoined.
PRS-372440	Post Failover, Delayed session resumption with Pulse Client.
Release 9.1 R1	
PRS-374583	Behavior of "re-authentication" and "termination" options in radius Return Attribute policy page is interchanged.
PRS-371733	Assigned VLAN is not updated if fetched on the next poll and always shows default config-ured. VLAN.
PRS-370902	Behavioral Analytics dashboard is not displaying charts for potential malware and anoma-lous traffic from IoT devices for more than 4 device categories intermittently.
PRS-370903	MAC address is not updated in the user session details.
PRS-374582	Behavior of "re-authentication" and "termination" options in radius Return Attribute policy page is interchanged.
PRS-374368	PSAL launch failed when proxy browser is configured.
PRS-374477	Fortinet admission control feature will not work with domain users (AD).

Problem Report Number	Summary
PRS-371536	Host Checker: Virus Definition Check for updates fails for K7 Virus Security ZERO (14.x),
PRS-373619	Host Checker: Virus Definition Check for updates fails for AVG Free Antivirus (19.2.x).

Known Issues

The following table lists the Known issues in the current release.

Problem Report Number	Description
Release 9.1R7	
PRS-389837	Symptom: For Cisco WLC, the Authentication is working fine, authorization is failing. In the Debug log, "Bad service type" error message is displayed and resulting in authorization failure. TCP Dump shows authorization is failing. Condition: During ACS to PPS migration with Cisco WLC. Workaround: Not Available
Release 9.1R5	
PRS-389553	Symptom: uacHostChecker process application exits unexpectedly Condition: Pulse Client with latest component tries to connect to lower server version, for example: 5.4R7.1 through Internet Explorer/Chrome/Firefox. Workaround: This issue is seen only on Windows 10 (1909) version whereas Windows RS5 (1809) and Windows7 Enterprise there is no issue.
PRS-389409	Symptoms: User sessions will not be synced for the session logged in at the time of second node upgrade in Active Passive cluster. Condition: During Active Passive cluster upgrade, when the first node comes up after upgrading newer version, it informs the other node to upgrade. During this time if any new user logs in then all those sessions will not be synced after second node upgrade. Workaround: Users needs to re-login
PRS-389234	Symptom: ECC device certificate is not supported with SRX firewall below Junos version 15.x. Condition: If the server uses ECC device certificate then the connection to SRX is established only with releases later than Junos 15.x version. Workaround: ECC certificate support is introduced in releases later than 15.x Junos version. If the server uses ECC device certificate, then the connection to SRX is established only with releases later than Junos 15.x version. If the server has both the ECC and RSA device certificate installed, then Restart Services (System Maintenance > Platform > Restart Services) is required to switch from ECC to RSA or vice versa).
PRS-389642	Symptom: XML import is failing if configuration file has syslog IPv6 settings. Condition: If IPv6 syslog server on log settings is configured then the XML import fails. Workaround: Export the binary system configuration and import on another device.

Problem Report Number	Description
PRS-389078	Symptom: When the end-user changes his password, login with the changed password fails. Condition: User won't be able to login with the changed password. Workaround: Admin can change the password for the end-user and that password can be used to login.
PRS-389763	Symptom: When SNMP Device is discovered using SNMP (v2/v3 version), Location Group and Default VLAN configured for the discovered device is not applied after clicking "Add Device". Condition: Discover a Switch using SNMP (v2/v3 version). Configure Location Group and Default VLAN, and then click on "Add Device". Added device will not have the Location Group and Default VLAN configuration. Workaround: Configuration has to be manually changed under Endpoint Policy > Network Access > Network Infrastructure Device.
PRS-385553	Symptom: Connection error displayed while installing Host Check component. The issue is seen while performing agentless connection (Host Check enabled) after cleaning all the previously installed Host Check components. Conditions: "UAC Host Checker" process running in the background. Workaround: Kill the process or reboot the system and perform agentless connection.
PRS-389865	Symptom: Session termination action from admission control policy is not triggered post AP cluster failover for existing user sessions. Condition: Users connected to Active Node in AP cluster will move to Passive Node on Cluster failover. If any Admission control event/alert is received for these users, action set in the Admission control policy will not be triggered. Workaround: As this issue is only for those sessions available before failover, new session should be created post failover to resolve the issue.
PRS-390106	Symptom: Inconsistent upgrade issues seen while upgrading Hyper-V images in clustering and single node. Condition: Upgrading a Hyper-V image to 9.1R5. Workaround: If cluster upgrade fails, reboot the node which is not upgraded. If the issue persists, try upgrading the nodes individually and then form cluster.
PRS-390303	Symptom: The event Agent_session_bridge is not included in Login Type Dashboard chart formation in splunk App. Condition: It gets impacted only when a user forming L2 followed by L3 session from the PDC client. The reason is, this event is not been added in parsing regexp in backend , hence bridged session will not be appeared in Login_Type Dashboard chart in Pulse policy Secure App. Workaround: The event 'Agent_session_bridge' should be added in backend with applying regexp for the field to be extracted for further use.

Problem Report Number	Description
PRS-390300	Symptom: The current splunk session displayed on Dashboard will not be retained when clicking on Pulse Policy Secure App. Condition: Splunk limitation Workaround: Not Available
Profiler	
PRS-389626	Symptom: Full sync happens more than once in Forwarder A/P Cluster. Condition: This issue is observed only after upgrading Forwarder A/P Cluster. Workaround: None
PRS-389305	Symptom: During "edit all similar devices" in DDR, the response message is displayed successful. However, devices are still getting classified in the background. Admin does not know when the re-classification is done for all the devices. Condition: This occurs when there is large number(~50K) of devices classified. Workaround: Refresh the DDR page after few minutes.
PRS- 389161	Symptom: If endpoints entries are deleted from DC, these endpoints are not deleted from DR and vice versa. Condition: This issue is only seen when full sync is in progress. If endpoints entries are deleted after full sync done, sync happens properly. Workaround: Delete the endpoints from DC/DR separately.
PRS-388961	Symptom: In the Switch View Bridge Interfaces are not showing up, all other interfaces are coming. Condition: Fetching the IFMIB doesn't gives the bridge interfaces. Workaround: None.
Release 9.1R4	
PRS-386989	Symptom: Mist is not sending class attribute and hence PPS unable to map session for incoming accounting request due to which the accounting stop will not remove the session from the PPS after Guest disconnects from SSID Condition: When SSID is disconnected from the endpoint by the Guest without logging out from the active session Workaround: Manually remove the active session from Mist controller Or Provide lower session timeout value for Guest users in PPS.
PRS- 387494	Symptom: Mist is not sending class attribute and hence PPS unable to map session for incoming accounting request and hence IP is not getting updated in the Active Users page in PPS Condition: When active Guest session is formed Workaround: NA

Problem Report Number	Description
PRS-384976	Symptom: Host Checker error found intermittently while installing Pulse Client using Chromium Edge browser with Host Checker configured. Condition: Host Checker configured. Workaround: Click on Ignore button.
Profiler PRS-387717	Symptom: The "View all 'Unapproved Devices'" link in E-mail received by admin for Device Approval does not redirect to Device Discovery Report. Condition: If Admin has configured Profiler to get email for any specific device types. (This setting is in 'Device Sponsoring' section of Profiler Configuration and in Profile Groups also) Workaround: Instead of using link from Email, admin can login to PPS and filter for "Unapproved Devices" in Device Discovery Report.
Release 9.1R3	
PRS-381239	Symptom: CSV import to System local database will fail with error message as "Invalid User Name. Only ASCII characters are allowed on PPS UI. Condition: When username in the CSV file to be imported to System local database involves charac-ters apart from ASCII Workaround: None
PRS-382287	Symptom: TNCS on the server crashes intermittently during the HC policy evaluations. Condition: With Opswat policies configured on the server, TNCS on the server crashes intermittently during the Opswat policies evaluation. Workaround: If Opswat policy evaluation fails for a specific end user, he/she may need to re-authenticate for getting the required access.
PRS-381394	Symptom: Microsoft Excel is changing the format of CSV file while saving. Condition: User tries to edit the CSV file using MS Excel. Workaround: User should make sure that CSV file fulfil all condition of CSV file format. Open file in simple editor like: notepad++, vim.
PRS-381554	Symptom: Policy evaluation failed on macOS 10.14x or any higher versions for a file rule configured to validate a file location with System default Directories <%HOME%> Condition: Hostcheck policy with File Rule for macOS 10.14.x or higher versions for a file located at System Directories <%HOME%> Workaround: Need to add permissions for "Pulse Client" under "Accessibility" and "Full Disk Access" and which can be accessed from System Preferences > Security & Privacy > Privacy Or without providing permission /tmp location can be used for File validation.

Problem Report Number	Description
PRS-380471	Symptom: PPS upgrade to 9.1R3 will not update the connection set and component set of the user role configured with Odyssey Access client settings. Condition: Fresh installation of Pulse client or migrating from OAC to Pulse client Workaround: OAC migration guide will help the administrators to configure the connection set and component set and map the same to appropriate roles.
PRS-382021	Symptom: Dismiss until next upgrade option is not working for banner related to perpetual licensing. Condition: Admin clicks on Dismiss until next upgrade. Workaround: For every new Admin login use the close button as a workaround.
PRS-380327	Symptom: Devices in Network Infrastructure Device are in Undiscovered state after importing Devices configuration using XML. Condition: Devices in Network Infrastructure Device are imported using XML. Workaround: Restart Services or enable all Switches manually.
PRS-380855	Symptom: Profiler is polling deleted switches once after deletion. Condition: Devices are deleted from Network Infrastructure Device list. Workaround: NA
Release 9.1 R2	
PRS-378002	Symptom: Cache server is continuously crashing in Longevity setup. Unable to open admin UI, crash messages display. Condition: When cache memory is hitting more than 512mb this crash has been observed. Workaround: NA, rollback and upgrade to latest version to start the test again.
PRS-378052	Symptom: SMTP Port 465 is not working for PPS guest user. Condition: Under SMTP settings, port 465 should also supported for Guest user. Workaround: SMTP port 587 with selecting SSL works in case of guest.
PRS-379012	Symptom: Radius Disconnect message (DM) is not working after importing user.cfg configuration from the previous release. Condition: When previous configuration (from 9.0R1) is loaded onto the box, overwrites the de-fault radius.dct. "Funk-Dest-IPv6-Address" attribute is missing in the old dictionary. Workaround: After restoring the dictionary to factory default, DM is sent to the switch and session is disconnected.
PRS-379063	Symptom: While performing L3 followed by L2 and frequently enable/disable migration option some time SDKs are replacing next periodic host check Conditions: On Windows Platform using Pulse performing L2 authentication with Host Check enabled on Role/Realm with Migration feature enabled. Workaround: For replacing expected SDKs wait for next periodic Handshake or Disconnect and again connect to server using Pulse.

Problem Report Number	Description
PRS - 377549	Symptom: PSIS is not upgrading to the 9.1R2 version. Condition: When CTS, WTS and VDI gets upgraded to 9.1R2 in Win10RS5+. Workaround: NA
Profiler	
PRS-378960	Symptom: Selected profiler name not retained in profiler dashboard. Condition: In dashboard, Profiler name not retained when revisiting the same page after moving to another page. Workaround: NA
PRS-378956	Symptom: Linkdown Trap is not updating device link status in Device Discovery Report when profiler processes for the first time. Condition: Profiler not processing Linkdown Trap without Linkup trap update in Device Discovery page for the device. Workaround: NA
PRS-377534	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 Condition: Administrator downloading of profiler report from Profiler Dashboard page Workaround: NA. Currently, profiler report is always generated with the default chart types.
Release 9.1 R1	
PRS-372687	Symptom: RADIUS CoA disconnect for Splash sign on page in Meraki WLC does not acknowledge the session disconnect message sent by PPS. 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. Workaround: Admin can login to Meraki dashboard and de-authorize the guest manually from Wire-less > 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.
PRS-372794	Symptom: RADIUS Accounting stop message is not sent by Meraki when guest logs out or gets discon-nected from Guest SSID Conditions: The Guest session will remain active on PPS for the duration of Maximum Session Length (default=725 mins). Workaround: Admin can login to Meraki dashboard and de-authorize the guest manually from Wire-less >Splash logins page which will immediately send the Accounting stop message from Meraki to PPS.
PRS-373861	Symptom: TACACS+ Accounting start and stop messages are not sent by BIG IP F5 device Condition: PPS may have stale sessions as it does not receive stop accounting packets. However, these sessions are deleted from PPS when Maximum Session Timeout expires. 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.

Problem Report Number	Description
PRS-372849	Symptom: Session migration fails for secondary auth server. User is prompted with secondary auth server password. Condition: If secondary auth server is configured for session migration. Workaround: NA
PRS-376312	Symptom: Factory reset from VMware VA console does not load the factory reset version and loads the current version. Conditions: When trying to do factory reset to 9.1R1 from higher version in VMware-VA Workaround: Factory reset is possible by manual intervention. After successful 'Factory reset' com-mand given from console, Virtual Appliance will reboot and will display three options in LILO menu: • Current version • Rollback version • Factory reset version Admin need to manually select the Factory reset version for the factory reset to happen successfully on VMware VA.
PRS-372250	Symptom: Session migration fails for 802.1X authentication. Condition: When the user tries to migrate the 802.1X sessions from PPS to PCS. Workaround: NA
PRS-374476	Symptom: Firewall SOH policy evaluation fails for domain user when Private and Public Net-works profiles in Windows Firewall are not turned ON. Condition: When Private and Public network profile for domain user is not turned ON for Windows firewall. Workaround: NA
PRS-374820	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. Condition: If network infrastructure devices config imported using binary/xml Workaround: NA. This might happen once.
PRS-374663	Symptom: L3 session is established with Internal IP while performing L3 followed by L2 using Pulse with PPS External VIP address. Conditions: When PPS nodes are in cluster and external port is used for RADIUS authentication. Workaround: NA
PRS-360616	Symptom: SAML authentication failed with error "Missing/Invalid sign-in URL" despite correct credentials while using PDC embedded browser version 9.0.1. Condition: Using PDC browser version 9.0.1 with PPS version 9.1R1. Workaround: Use latest PDC version with Release 9.1R1.

Problem Report Number	Description
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-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-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.

Problem Report Number	Description
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 ex-pected.
PRS-376265	Symptom: Invalid character error seen while adding Radius Return attribute value which contains "<" and ">" characters. Condition: While creating new Radius Return attribute value or editing existing Radius Return attrib-ute value which contains "<" and ">" characters. Workaround: • 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. • Fresh Deployment: To add Radius Return attribute value which contains "<" and ">" characters, ex-port XML file from Maintenance >Import\Export >Export XML and add\modify the Radius Return Attrib-ute value in Exported XML and then import the same XML from Maintenance >Import\Export->Import XML.
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 in-stalled. 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

Problem Report Number	Description
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

Upgrade Instructions

Upgrade Paths

The following table describes the tested upgrade paths.

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

Note: 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 current release without core license.

Follow these steps to upgrade to the current release:

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

General Notes

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.

Documentation

Pulse Secure 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://support.pulsesecure.net
- support@pulsesecure.net

Call us at 1- 844-751-7629 (toll-free USA)

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