Pulse Policy Secure

Release Notes
PPS 9.1R1 Build 1231
Pulse Profiler Version 1.6 (FPDB Version 39)
PDC 9.1R1 Build 607
Default ESAP Version: ESAP 3.3.5

Release Build	**9.1R1, 1231**
Published	**January 24, 2020**
Document Version	**1.3**

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

END USER LICENSE AGREEMENT

Revision History

The following table lists the revision history for this document.

Revision		Description
1.3	Jan	RADIUS server capability on External port feature description is updated.
1.2	June	Added “Session Bridging for Linux Platform” under New Features in 9.1R1 Release.
1.1	May	Added PRS 371536, PRS 373619 under Fixed Issues in 9.1R1 Release.
1.0	April	Updated for 9.1R1

Contents

Introduction

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

Hardware Platforms

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

- PSA300, PSA3000, PSA5000, PSA7000F, PSA7000C

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

Virtual Appliance Editions

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

- Virtual Pulse Secure Appliance (PSA-V)

Note:

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

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

Platform	Qualified System
VMware	• 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 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
9.0R4	Yes	
9.0R3	Yes	
9.0R2	Yes	
9.0R1	Yes	
5.4Rx	Yes	
5.4Ry		Yes

For versions, earlier than 5.3:

- First upgrade to release 5.3Rx|5.3Ry, 5.4Rx|5.4Ry and then upgrade to 9.1Rx.

Note

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

Upgrade Scenario Specific to Virtual Appliances

PSA-V cannot be upgraded to 9.1R1 without core license. Follow these steps to upgrade to 9.1R1:

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

Note:

- Direct Upgrade from Release 5.4R2 or below to Release 9.1R1 is not supported for KVM and HyperV VM images.
- On a PPS virtual appliance, we highly recommend to freshly deploy a PSA-V from 5.4Rx-based OVF, when any of the following conditions are met:
    - If the disk utilization goes beyond 85% or if an admin receives iveDiskNearlyFull SNMP Trap.
    - If the factory reset version on the PSA-V is 4.x or <= 5.3Rx.
- VA Partitioning (LVM) feature is added for VMware-VA starting from 9.1R1, which will decrease the OVF size of VMWare-VA image.

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 9.1R1 is 3.3.5.
6. With OPSWAT v4 SDK, the new product support list is being worked upon and updated by OPSWAT periodically, which is delivered as part of ESAP.

New Features in 9.1R1 Release

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

Feature	Description
SNMP Enforcement using ACL (Cisco, HP, Juniper)	SNMP enforcement using ACL is supported for Cisco, Juniper and HP switches.
Meraki 802.1x and Guest Access support	802.1X and Guest Access support is qualified with Cisco Meraki WLC.
Google Auth Multi Factor Authentication	TOTP server can be added as a secondary auth server in PPS.
Session bridging for Linux Platform	PPS supports bridging the Layer 2 Native Supplicant 802.1X session with Layer3 Agentless (Browser based) Session on Linux platform.
RADIUS server capability on External port	PPS supports RADIUS server authentication and 802.1X authentication using external port. Activate "Enable Auth Traffic Control" under Authentication servers to enable sending RADIUS traffic or receiving RADIUS traffic to PPS (as a RADIUS server) through external interface.
SAML Auth Server support	PPS can be configured as SAML service provider (SP) for all industry standard SAML IdP's.
Session Migration using Cert authentication	Session migration in an IF-MAP federated network supports Cert Auth and SAML auth
Machine certificate check on MacOS	Machine certificate check on Mac OS is now supported for PPS.
TACACS+ Enhancements – DB sync, pass back attributes to devices such as F5 and Juniper	TACACS+ authorization support for Administrators using custom attributes for Juniper and F5 devices. TACACS+ configuration synchronization across WAN cluster
DNS traffic on any physical interface	Prior to 9.1R1 release, DNS traffic was sent over the Internal interface. Starting with 9.1R1 release, an administrator can modify the DNS setting to any physical interface namely Internal Port, External Port or Management Port.
Profiler	
Distributed Profiler Enhancements	The Administrators can sync the profiled data from one Profiler to another from the profiler auth server configuration page. Multiple branch offices can sync their profiled data to central office. Admin can view the Device Discovery Report to view and control the multiple offices.
Profiler Device Age Out	Profiler device age-out interval configuration allows admin to automatically delete the devices from the database. Admin can define the age-out interval for a group of devices also using Profile Groups
Profile Windows devices using SNMP(HOST)	SNMP-HOST Collector is a collection method that receives endpoint information where the endpoints are monitored through SNMP. Admin can configure subnets to scan and community strings in profiler auth server configuration page.
Approval for Profile Groups	Administrator can select "needs approval" for selected Profiler group.
Key-value based search in DDR	Administrator can search in DDR with key value-based query. Query syntax is similar to that of profile groups.
Publishing IP address from Profiler to Active User Session	Admin can add IP address from Profiler to active session for L3 enforcement when RADIUS accounting is not enabled. This is supported only for MAC auth and dot1X.
Huawei switches added in supported list for Network Infrastructure Device	Admin can select Huawei switch from supported list in network infrastructure device page.

Noteworthy Changes in 9.1R1 Release

None

Fixed Issues in 9.1R1 Release

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

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

Known Issues in 9.1R1 Release

The following table lists Known issues in this release.

Problem Report Number	Release Note
PRS-372687	**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 Wireless > Splash logins page. In addition to that, we have raised an enhancement request to Meraki to support COA disconnect on splash sign on page with radius authentication.
PRS-372794	**Symptom**: RADIUS Accounting stop message is not sent by Meraki when guest logs out or gets disconnected 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 Wireless >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.
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:**

Problem Report Number	Release Note
	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' command 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 Networks 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.
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.

Problem Report Number	Release Note
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.
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 attribute value which contains "<" and ">" characters. **Workaround:** 1) Upgrade case: It would work fine, if Radius Return attributes are not modified. To edit or create new Radius Return attribute value, please follow step 2. 2) Fresh Deployment: To add Radius Return attribute value which contains "<" and ">" characters, export XML file from Maintenance >Import\Export >Export XML and add\modify the Radius Return Attribute value in Exported XML and then import the same XML from Maintenance >Import\Export->Import XML.
Profiler	
PRS-369079	**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.

Problem Report Number	Release Note
	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

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.**