Pulse Policy Secure

Release Notes
PPS 9.0R1Build 49495
Pulse Profiler Version 1.4 (FPDB Version 31)
Pulse Client Version 9.0.1Build 571
OAC version 5.60.41795 (5.6R20)
Default ESAP Version: ESAP 3.2.3

Release, Build	**9.0R1, 49495**
Published	**May 2018**
Document Version	**2.0**

Pulse Secure, LLC

2700 Zanker Road, Suite 200

San Jose, CA 95134

https://www.pulsesecure.net

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

END USER LICENSE AGREEMENT

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

Contents

Introduction

This document is the release notes for Pulse Policy Secure Release 9.0R1. This document contains information about what is included in this software release: supported features, feature changes, unsupported features, known issues, and resolved issues. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

Hardware Platforms

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

- PSA300, PSA3000, PSA5000, PSA7000F, PSA7000C

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

Virtual Appliance Editions

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

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

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

Table 1 Virtual Appliance Editions

Platform	Qualified System
VMware	• HP ProLiant DL380 G5 with Intel(R) Xeon(R) CPU • ESXi 6.0, 5.5U3, 5.5
KVM	• CentOS 6.6 with Kernel cst-kvm 2.6.32-504.el6.x86_64 • QEMU/KVM v1.4.0 • Linux Server Release 6.4 on an Intel Xeon CPU L5640 @ 2.27GHz o 24GB memory in host • Allocation for virtual appliance: 4vCPU, 4GB memory and 40GB disk space
Hyper-V	• Microsoft Hyper-V Server 2012 R2

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

Upgrade Paths

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

x: Latest maintenance release version

y: Any release version

Upgrade From	Qualified	Compatible
5.4Rx	Yes	
5.4Ry		Yes
5.3Rx	Yes	-
5.3Ry	-	Yes

For versions, earlier than 5.3:

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

Note:

- Beginning with PPS 5.4R3 release, access to profiler functionality on Pulse Secure Appliance (PSA) platforms will require a Profiler License to unlock Profiler feature. MAG Platforms do not support profiler functionality.
- Please make sure to procure the required Profiler license before you upgrade to PPS 5.4R4 or later. If you upgrade without having the Profiler license, you will no longer have access to the Profiler features.
- If your system is running Beta software, roll back to your previously installed official software release before you upgrade to 9.0R1 This practice ensures the rollback version is a release suitable for production.
- On a PCS/PPS virtual appliance, we highly recommend to freshly deploy a PSA-V from 5.4-based OVF, when any of the following conditions are met:
  - If the disk utilization goes beyond 85% or if an admin receives iveDiskNearlyFull SNMP Trap.
  - If the factory reset version on the PSA-V is 4.x or 5.0.

Upgrade Scenario Specific to Virtual Appliances

PSA-V cannot be upgraded to 9.0R1 without core license. Follow these steps to upgrade to 9.0R1:

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

General Notes

1. PPS acting as License clients, running 5.1R1 and above will not be able to lease licenses from License Servers running on PCS 8.0R1 to PCS 8.0R4. If you plan to upgrade PPS License clients to C5.1R1 and above versions, you would have to upgrade your License Servers to 8.0R5 and above. See KB40095 for more information.
2. For policy reasons security issues are not normally mentioned in release notes. To find more information about our security advisories, please see our **security advisory page.**
3. When custom ciphers are selected, there is a possibility that some ciphers are not supported by the web browser. Also, if any of ECDH/ECDSA ciphers are selected, they require ECC certificate to be mapped to the internal/external interface. If ECC certificate is not installed, admin may not be able to login to the box. The only way to recover from this situation is to connect to the system console and select option 8 to reset the SSL settings from the console menu. Option 8 resets the SSL setting to its default. So, the previously set SSL settings are lost. This is applicable only to Inbound SSL settings.
4. Pre-5.0 Android and pre-9.1 iOS devices don't support Suite B ciphers. So, if Suite B is enabled, Pulse client on pre-5.0 Android and pre-9.1 iOS devices will not be able to connect to PPS device.
5. With OPSWAT v4 SDK, the new product support list is being worked upon and updated by OPSWAT periodically, which is delivered as part of ESAP. In case of any issue related to compliance evaluation or remediation for any specific product, then ensure that latest ESAP is used or roll back to OPSWAT v3 SDK.

New Features in 9.0R1Release

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 in 9.0R1 Release

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

Problem Report Number	Release Note
PRS-360032	On the IF-MAP server the VIP failover is not working in Active/Passive cluster mode with PAN firewall.
PRS-353358	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	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	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	VA-SPE/PSA-V cluster cannot be created if the management port is not enabled on the nodes.
PRS-347064	With Fortinet integration, user access is given only in case the user is assigned single role on PPS. If user is assigned more than one role, access is not given by FortiGate Firewall. This is because of the limitation with Forti Authenticator which supports parsing of only role in the log messages.

Unsupported Features in 9.0R1 Release

None.

Known Issues in 9.0R1 Release

The following table lists Known issues in 9.0R1 release.

Problem Report Number	Release Note
PRS-359313	**Symptom:** Endpoint compliance fails when host checker policy is saved on the Policy page immediately after modifying the rule. **Conditions**: If Host checker policy is immediately saved after modifying the rule. **Workaround**: The user need to re-try the Pulse connection and compliance check will pass.
PRS-358212	**Symptom:** The compliance check will fail if the Patch management product is not changed to "Software Update (2.x)" after toggling from V3 SDK to V4 SDK on MAC OS. **Conditions**: When Patch Management policy is enabled with Product as "Software Update (10.11/10.12/10.13)" under V3 SDK and Admin toggles to V4 SDK, the Product mapping need to be modified by explicitly changing the Product name as "Software Update (2.x)" and save the policy for host checking to pass. **Workaround**: Admin has to explicitly change the Selected product as "Software Update (2.x)" under the Patch management rule and save it.
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-SPE cluster VIP-Failover happens automatically. **Conditions:** Cluster VIP fail over. **Workaround:** None
PRS-362267	**Symptom:** Fed client not removing exported sessions though fed server is not reachable for more than 200 seconds. **Conditions**: Exported session not getting deleted after client loses connectivity. **Workaround:** None
PRS-356373	**Symptom:** XML Import of named users does not validate if XML file is valid. **Conditions**: Importing an invalid XML. **Workaround:** Export an existing named user table. modify it before importing it. Ensure XML information is correct.
PRS-355333	**Symptom:** Named users tab not loading with 150k unique named users on the system. **Conditions:** Admin will not be able to view or delete any named users if they have 150k or more named users on their system. **Workaround:** Split the deployment into multiple stand alone and cluster deployments and have a smaller group of users go to each gateway.
PRS- 362479	**Symptom:** PPS communicates to Checkpoint over physical IP of VIP holder interface rather than using VIP itself. **Conditions:** PPS communicates to Checkpoint over physical IP of VIP holder interface. **Work-Around:** All PPS cluster node's IP need to be configured in checkpoint as "host" for Checkpoint integration to work with PPS cluster.
PRS-352129	**Symptom:** Custom SOH AntiSpyware policy doesn't take Group policy configuration into consideration while evaluating in windows 10 OS. **Condition:** Group policy setting are not considered while evaluating the policy Windows 10 OS. **Workaround:** None
PRS-356794	**Symptom**: Users logging in from Windows Server OS clients are reported as Windows 7 clients on the Active Users page. **Conditions**: Users logging in through browser for Windows 2008, 2012, and 2016. Are shown as windows 7 clients on the active users page. **Workaround**: None
PRS-352127	**Symptom:** Custom SOH Antivirus policy doesn't take Group policy configuration into consideration while evaluating in windows 10 OS. **Conditions:** Group policy setting are not considered while evaluating the policy Windows 10 OS. **Workaround:** None
PRS-354907	**Symptom:** user-identity information provisioned by Pulse Policy Secure removed from Checkpoint Firewall post reboot. **Conditions:** Only after Checkpoint Firewall reboot **Workaround:** Delete the Checkpoint Firewall configuration from PPS and then reconfigure.
PRS-344807	**Symptom:** On Google Chrome browser, periodic host checking is not supported and can result in session termination if periodic host checking is configured. Hence it is recommended to use other browsers for agentless access with host checker. **Conditions:** Agentless login with Host Checker Compliance enforced using Google Chrome **Workaround:** Use Mozilla Firefox browser.
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-360868	**Symptom:** Binary Profiler endpoint data importing is not working in cluster setup **Conditions:** If both nodes are Active in Active/Passive cluster then importing profiler endpoint data binary format will cause cluster data mismatch. **Workaround**: Import Profiler endpoint binary data in primary node before the passive node joins the cluster.
PRS-360918	**Symptom:** SNMP scan is not happening after importing 2000 switches config using xml import. **Conditions**: Import xml with SNMP switch config having 2000 switches. **Workaround**: PPS restart is needed for SNMP to poll all switches after importing 2000 switches config using xml import
PRS-351666	**Symptom**: Traps processing will not stop, when Switch user modified from snmpv3 trap supported user to unsupported user in PPS SNMP device. **Conditions**: Switch delete and re-add in SNMP device list without reboot. **Workaround**: After rebooting the PPS device, PPS will not process v3 traps. Restart the PPS services on endpoint.
PRS-349430	**Symptom**: MAC auth login rate is slow with high rate on PSA5000 only. On PSA7000 there is no impact. **Conditions**: Login rate for MAC auth is lower when the number of sessions on the same machine reaches 30k+. **Workaround**: If the login rate is too high for low end devices, authentication may be performed multiple times.

Documentation

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

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@pulsesecure.net.**

Technical Support

When you need additional information or assistance, you can contact "Pulse Secure Global Support Center (PSGSC):

- **https://www.pulsesecure.net/support**
- **support@pulsesecure.net**
- Call us at 1- 844-751-7629 (toll-free USA)

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

Revision History

The following table lists the revision history for this document.

Table 6 Revision History

Revision		Description
2.0	April 2018	Updated for Release 9.0R1
1.1	December 2017	Updated for Release 5.4R4
1.0	August 2017	Updated for Release 5.4R3