Pulse Policy Secure 5.3R1

Release Notes

Pulse Policy Secure version 5.3 R1 Build 32853

Pulse Client version 5.2 R1 Build 227

Odyssey Access Client version 5.60.30789

Product Release 5.3

Document Revision 1.0

Published: 2015-12-17

Table of Contents

List of Tables

Introduction

These release notes contain information about new features, software issues that have been resolved and new issues. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

This is an incremental release note document that describes the changes made from 5.2R3 release to 5.3R1. The 5.2R3 release notes still apply except for the changes mentioned in this document.

Hardware Platform

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

- MAG2600, MAG4610, MAG6610, MAG6611, MAG SM160, MAG SM360, PSA-300, PSA-3000, PSA-5000, PSA-7000c/f

Virtual Appliance Editions

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

- Demonstration and Training Edition (DTE)
- Service Provider Edition (SPE)

Table 1: Virtual Appliance Qualified Systems

Platform	Qualified System
VMware	• IBM BladeServer H chassis • BladeCenter HS blade server • vSphere 5.1, 5.0, and 4.1

KVM	• QEMU/KVM v1.4.0
	• Linux Server Release 6.4 on an Intel Xeon CPU L5640 @ 2.27GHz
	  ○ NFS storage mounted in host
	  ○ 24GB memory in host
	  ○ Allocation for virtual appliance: 4vCPU, 4GB memory and 20GB disk space

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

Interoperability and Supported Platforms

- Refer to the *Supported Platforms* document on the software download site for details about supported versions of the Cisco and Aruba WLC, PAN firewall & Screen OS Enforcer, the Junos Enforcer, client browsers, client smart phones, and client operating systems. Go to: http://www.pulsesecure.net/support/

Upgrading to Pulse Policy Secure 5.3R1

Table 2 Upgrade Paths

Release	Description
Pulse Policy Secure Software Upgrade	• Automatic updates to this release are supported for all PPS releases after and including PPS 5.1 R1. • This release does not support IC4500 and IC6500 devices. These hardware models have reached end-of-life (EOL).
Pulse Secure Desktop 5.2R1 Client Software Upgrade	Refer to the Pulse Secure Desktop Client 5.2 release notes.
Odyssey Access Client Upgrade	In this release same version of Odyssey client is retained.
PPS Agent (OAC)	PPS can handle 1500 concurrent endpoint upgrades.
Standalone OAC Client	This release supports the standalone, non-PPS version of Odyssey Access Client. Instructions for installing OAC on standalone clients are contained in the help guide under the section Getting Started > Initial Configuration.
Endpoint Security Assessment Plug-in (ESAP) Compatibility	ESAP package version 2.8.8 is the minimum version to be compatible with Pulse Policy Secure version 5.3R1. The default version for ESAP is 2.8.8
Network and Security Manager (NSM) Compatibility	NSM is not supported.

New Features

Table 3 describes the major features introduced in this release.

Table 3 List of New Features

Feature	Description
Palo Alto Networks (PAN) Firewall Integration	Provides advanced NAC/BYOD solution in a PAN Firewall deployment with the ability to auto-provision User Identity, IP address and role information on PAN firewall so that access policies can be enforced on the firewall based on the compliance status of user/device.
Compliance check for Mac Users	Compliance check and Role based Access Control for Apple Mac Users using native supplicant with certificate authentication
Support for Radius CoA	Provides expanded interoperability with Cisco, HP and Aruba network infrastructure. Without starting entire process of authentication, Radius CoA allows devices to change the VLAN/ACL for the endpoint based on roles.
Refreshed UX (Admin UI)	The PPS administration web UI, look and feel has been redesigned to improve user interface experience. In PPS 5.3 Release, user will have option to choose new user interface or switch to classic user interface. The default UI is the new user interface.
Simplifying PPS Deployment and Administration	Introduced UI wizards that make it simpler to configure common workflows such as realm, 802.1x, and IF-MAP configurations.
AES is preferred over RC4	AES is a preferred cipher over RC4. Ie. If a client that supports both AES and RC4 connects to SA, AES is used.
RC4 Warning	In PPS 5.3 release, a warning is shown in the Admin UI if the insecure RC4 cipher is enabled. This new feature does not properly detect when RC4 is enabled when hardware acceleration is turned on. If hardware acceleration is not enabled, or the device does not have the hardware accelerator installed, the feature works as expected.
Pulse Secure Application Launcher (replacement for NPAPI)	Due to the end of ActiveX and Java support on many browsers, an alternate solution is provided in this release for the proper launching of client applications such as Pulse Client. This release uses custom URL, pulsesecure://, to deliver and launch client applications. The custom URL when invoked, will automatically trigger new application – Pulse Application Launcher. The Pulse Application Launcher has the ability to accept the parameters from the user's browser and launch the client application. For more browser details refer to "Pulse Secure Desktop Client Supported Platform Guide for 5.2R1".

Noteworthy changes

Pulse Policy Server (PPS) acting as License clients, running C5.1R1 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.

Fixed Issues

Table 4 lists issues that are fixed and resolved by upgrading to this release.

Table 4 List of Issues Fixed in this Release

PR Number	Release Note
PRS-324342	With PPS in Active/Passive cluster mode, deleting the user from active user page doesn't disconnect user from Cisco WLC.
PRS-324854	User telnet session is disconnected when active node of Federation Client2 in Active/Passive cluster is powered off from CMC console.
PRS-328574	Error message seen on the VA-SPE console after upgrading during the first reboot (POST-INSTALL).
PRS-324694	Using Email2SMS setting for clickatell under SMS settings, gives SMS text with %0D%0A signs.
PRS-324524	Guest user session times out after reaching "Heartbeat Timeout" value configured in Guest Role.
PRS-326508	During kernel upgrade process the VA-SPE event logs frequently generated "Starting services: client access server".

Open Issues

Table 5 lists open issues in this release.

Table 5 List of Open Issues in this release

PR Number	Release Note
PRS-329095	If the client is connected via mac-auth, and when the session in PPS is deleted manually, PPS does not send disconnect message to WLC. So the session exists in the WLC till session times out.
PRS-318679	For Host Checker with Bit Locker Encryption software, the encrypted drives will be reported as encrypted only when these drives are in Unlocked state.
PRS-334875	Clients that imported truncated configurations (configs for certs that had DN values containing double-quote characters) before the fix was released, will not be able to establish 802.1x connections. The workaround is for the client to connect to a fixed (5.3 or 5.2r4, or later) PPS/PCS device via non-802.1x. This connection will cause a new configuration file to be downloaded to the client. Once this is done, the client should be able to connect again via 802.1x.

PRS-309431	With OPSWAT Patch Management Host Checker policy, the missing patches will be detected only with admin privileges for SCCM 2012 and SCCM 2007.
PRS-293992	As part of Radius CoA if the client IP Address and VLAN id is changed then pulse client is not able to reach the server new IP. In this case the client needs to reconnect.
PRS-317090	IPSec use-cases will not work if Fed client-1(Authentication PPS) is upgraded, due to change in public key. The new public key needs to be re-published to Fed client-2(Enforcer PPS). Workaround is to reboot the Fed client-2 so it can fetch new public key from Fed client-1.
PRS-335251	Merging of RADIUS return attribute policies is supported with CoA only, not with RADIUS authentication or after a RADIUS disconnect. The first return attribute policy that gets matched from the role mapping rules is the one that gets applied to the session.
PRS-335194	If native supplicant is used for 802.1x and Pulse client is used for host checking, bridging of those 2 sessions is not supported if the session lifetime for the L2 role is less than 10 minutes. For best results, there needs to be sufficient time given for remediation; so 30 minutes would be a good minimum value for the 'max session lifetime' for a role.
PRS-321071	Deleting user from Pulse Policy Secure active user page doesn't disconnect the Cisco 2500/5500/7500/8500 WLC wireless user.
PRS-335738	PPS takes more than 2 minutes to process first CoA-ACK received after A/P cluster failover. Due to this Admin User Access Logs show that RADIUS Attribute Change of Authorization timed out. But the CoA is successfully applied to the user session.
PRS-330443	Custom Statement-of-Health policies will not function properly on Windows 10 because of Microsoft's phasing-out of support for the NAP (Network Access Protection) plugin. As such, if you have such a policy enabled (to verify, go to the PCS/PPS admin console and look under Authentication->Endpoint Security->Host Checker Policy->Windows->Rule Settings->"Custom: Statement of Health"), then you must disable it for all Windows 10 users.
PRS-332137	Validation of data entered while creating an Infranet enforcer connection via Wizard happens when we click on Finish Button.
PRS-271433	In an Active-Active cluster operating as an IF-MAP client, you should ensure that the [x] Synchronize User Sessions" is checked to ensure cluster wide sessions are published to the IF-MAP server. Failure to enable this option will result in ONLY local authentications being published to the IF-MAP server.
PRS-327799	In the new refreshed Admin UX compared to old Admin UX the navigation menu options for admin roles are removed, as those are not applicable.
PRS-322455	Guest user session will not display Agent Type in Active Users page in. Wireless LAN Controllers deployment.
PRS-335111	Using Windows 10 TH2 or an Android's native supplicant for 802.1x connections fails to authenticate a user against a PPS device.
PRS-324891	In a cluster failure scenario when host checker is initiated through L2 then its not able to communicate host check message with Pulse client.
PRS-328109	Post DMI import of configuration, if there is a failure to bring up users then one needs to restart services after importing users.
PRS-328027	In Compliance report page, the MAC address is not displayed in the correct format for L2 authentication
PRS-336056	Re-connecting IF-MAP client with Fed server will take time after disconnect IF-MAP client with large number of imported session, hence auth table provisioning will be delayed in to SRX for new logged-in users.
PRS-331800	On the Admin login page with multiple realm selection options, with chrome browser the first realm selection is not reflected on UI but it does login to the selected realm. User can clean the browser history to overcome this UI behavior.
PRS-336684	On end-user Mac machine, for browser base connections the debug log file is not created if the pulse client is not installed on the Mac machine. For troubleshooting purpose the pulse client would need to be installed on the mac machine.

PRS-336333	If multiple realms along with host checker policies are configured for sign-in URL, “Endpoint Security Status” on Active Users page is shown as “Not Applicable”

Documentation

Table 6 describes the documentation set. The documentation is available at http://www.pulsesecure.net/support

Table 6 Documentation

Title	Description
Getting Started	
Release Notes	A release summary, including lists of new features, changed features, known issues, and fixed issues.
Supported Platforms	List of client environments, third-party servers, and third-party applications that have been tested and are compatible with the software release.
Getting Started Guide	How to complete a basic configuration to get started using the solution.
Licensing Guide	How to install any licenses that might be required.
Virtual Appliance Deployment Guide	How to install, configure, and use the virtual appliance edition.
IC Series to MAG Series Migration Guide	How to migrate the system configuration and user data to the newer platform.
Administration Guides	
Complete Software Guide	The complete collection of user documentation for this release in PDF format.
Administration Guide	How to complete the network and host configuration and how to use certificate security administration, configuration file management, and system maintenance features.
Feature Guides	
Guest Access Solution Configuration Guide	A complete guide to guest access solution, which enables self-registration of guest over WLC and enables administrator to manage guest user access privileges.
Solutions	
Endpoint Security Feature Guide	Describes Host Checker and Cache Cleaner settings.
Developer Reference Guide	

Custom Sign-In Pages Developer Reference	A reference on customization sign in pages.

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

Technical product support is available through the Pulse Secure Global Support Center (PSGSC).

- http://www.pulsesecure.net/support/
- Call 1-844-751-7629 (toll-free in the USA).
  If outside US or Canada, use a country number listed from one of the regional tabs

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

Requesting Technical Support

To open a case or to obtain support information, please visit the Pulse Secure Support Site: http://www.pulsesecure.net/support/

Revision History

Table 7 lists the revision history for this document.

Table 7: Revision History

Revision	Description
17 December 2015	Initial publication.