Pulse Policy Secure 5.1R1 Release Notes

Pulse Policy Secure version 5.1 R1 Build 27261

Pulse Client version 5.1 R1 Build 51831

Odyssey Access Client version 5.60.27023

Product Release 8.1/5.1

Document Revision 1.0

Published: 2014-12-15

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

END USER LICENSE AGREEMENT

Table of Contents

Introduction 5

Hardware Platform 5

Virtual Appliance Editions 5

Interoperability and Supported Platforms 5

Upgrading to Access Control Service 5.0R1 6

Pulse Secure Rebranding 6

New Features 7

Fixed Issues 8

Open Issues 8

Documentation 11

Documentation Feedback 12

Technical Support 12

Requesting Technical Support 12

Revision History 12

List of Tables

Table 1: Virtual Appliance Qualified Systems **5**
Table 2 Upgrade Paths **6**
Table 3 List of New Features **7**
Table 4 List of Issues Fixed in this Release **8**
Table 5 List of Open Issues in this release **8**
Table 6 Documentation **11**
Table 7: Revision History **12**

Introduction

This document is the release notes for Pulse Policy Secure Release 5.1. 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 Platform

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

- IC4500, IC6500, IC6500 FIPS, MAG2600, MAG4610, MAG6610, MAG6611, MAG SM160, MAG SM360

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 Screen OS Enforcer, the Junos Enforcer, client browsers, client smart phones, and client operating systems. Go to: http://www.pulsesecure.net/support/

Upgrading to Access Control Service 5.0R1

Table 2 Upgrade Paths

Release	Description
Access Control Service Software Upgrade	• Automatic updates to this release are supported for all UAC releases after and including UAC 4.4 R1. • This release does not support IC4000 and IC6000 devices. These hardware models have reached end-of-life (EOL).
Pulse Secure Desktop 5.1R1 Client Software Upgrade	Refer to the Pulse Secure Desktop Client 5.1 release notes.
Odyssey Access Client Upgrade	
UAC Agent (OAC)	An IC Series device can handle 1500 concurrent endpoint upgrades.
Standalone OAC Client	This release supports the standalone, non-UAC 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 2.6.6 is the minimum version to be compatible with Access Control Service version 5.0. The default version for ESAP is 2.6.6
Network and Security Manager (NSM) Compatibility	NSM is not supported

Pulse Secure Rebranding

Pulse Policy Secure 5.1 have been re-branded with the new Pulse Secure logo. The Pulse Secure logo has replaced Juniper logo. You will see certain changes on the admin console that indicate this re-brand. Pulse clients on desktop, mobile and Pulse Workspace have also been re-branded with the new corporate logo.
When you upgrade to 8.1/5.1, please be aware of these user-visible changes. There are no specific changes to the upgrade experience or to the overall behavior tied to re-branding. Several internal aspects such as filenames, location of install directories, registry keys and so on will remain the same, for now, with 8.1r1/5.1r1.

New Features

Table 3 describes the major features that are introduced in this release.

Table 3 List of New Features

Feature	Description
Hard Disk Encryption	This feature allows Admins to enforce hard disk based encryption checks as part of host checker posture assessment. This feature can be used to detect if a selected encryption software product is installed on the endpoint and if the drive to be checked is encrypted or not. By ensuring that a device has disk encryption enabled, administrator can indicate that the device is more secure for an enterprise.
Replacement of Shavlik Patch Assessment Solution by OPSWAT	We announced EOL for Shavlik as of Nov 2013. With this feature Pulse PCS and PPS product line offer a patch assessment solution for Windows devices by using OPSWAT technology for detection of Patch Management software installed on the endpoint.
GUAM SMS Notification for Guest User	This features add ability to notify guest with credentials over SMS
BYOD	Device Onboarding for iOS, Android, Windows and Mac Endpoints: This feature provides an end to end solution for users and devices to get on-boarded.
BYOD	MDM Phase 2 – Visibility: For devices that's already registered with the MDM servers(MobileIron, Airwatch or GreatBay) if the device link is clicked under active users page IC renders the attributes of the authenticated devices locally instead of redirecting them to the MDM site.
BYOD	MDM Phase 2 - Redirect to MDM: Provide ability to redirect to MDM server of Choice for enrollment.
PushConfig Enhancements	Enhancements of push configuration options such as scheduling and reliant config transfer.
A/P Cluster	Active Node Selection Algorithm Improvement: Improving the active node selection algorithm for A/P clusters to be a bit more deterministic and converge more rapidly.
AD Performance Improvements	Includes SAMBA Upgrade for Improved performance
User Auth performance improvement	User authentication rate for PEAP, EAP-TLS, EAP-TTLS auth protocols has been improved.
IF-MAP performance Improvements	This release improves the performance and stability if both IF-MAP Client and IF-MAP server

Fixed Issues

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

Table 4 List of Issues Fixed in this Release

PR Number	Release Note
PRS 285245	Fed Server in A/P cluster config not sharing Fed Wide Session with newly added passive node
PRS 299034	EPS: Failed to read AV Update Data from cache error seen on event logs when enabling Virus signature version monitoring for first time
PRS 299328	Activate buttons in IF-MAP Federation > Active Users > Imported don't work
PRS 296940	User mapped with multiple roles (100 roles) is unable to login from the client (OAC and PULSE)

PRS- 317569	• Users can change their own password using a web browser, if:
	  • The realm is configured for agentless (brower-based) sign-in
	  • The realm uses a local authentication server
	  • In the Local Authentication Server Settings panel, you have selected [x] Allow users to change their passwords
	  • In the associated realm's Authentication Policy panel, you have selected [x] Enable password management
	After signing in with a web browser, the user clicks the Preferences icon. A password changing panel appears.

Open Issues

Table 5 lists open issues in this release.

Table 5 List of Open Issues in this release

PR Number	Release Note
PRS-316827	Help guide does not have contents for new features introduced in this release. Help for new features can be downloaded offline from the following location: http://www.pulsesecure.net/support/
PRS-309692	With Screen OS firewalls there could be few obsolete imported entries on IF-MAP client even when auth table time out has already expired. The obsolete entries go away when the users log out.
PRS-315937	Pulse Secure recommends that certificates use a hash algorithm other than MD5. This recommendation applies to all certificates, including server certificates installed on a Pulse Policy Secure or Pulse Connect Secure appliance. Certificates that use MD5 are prone to a signature-collision attack.

PRS-313891	While importing a huge user's session config which takes more than five minutes to complete the import, may give an timeout error message. This is observed in different versions Firefox > 29. This is not seen in IE and chrome browser. In such cases, admin may get an error message stating that "The server is not reachable" or Page not found", and may not get the upgrade successful message. The workaround for this is to change the 'network.http.response.timeout' value to something higher like 3000 instead of 300 in about:config.
PRS-316273	Host Checker periodic interval can't be set to 0. If it is already set to 0 before upgrading to C5.1R1, changing other options under HostChecker->Options section requires periodic interval to be set to greater than zero.
PRS-289428	For dot1x session from OAC, Single user report under System > Reports doesn't show the IP address of the machine.
PRS-317469	When we try to change the license in the box, sometimes, the Radius process will not come up because of which dot1x authentication may not happen. The workaround for this problem is to 'restart services' under maintenance > system > platform.
PRS-269300	• Symptom: 802.1x authentication takes a very long time to complete. • Conditions: On early versions of the Pulse Desktop client, if the Certificate Authority (CA) certificate was not present in the endpoint's machine store, then any reconnecting after the max-session timeout expired would be delayed. • Solution: Ensure that the root certificate (and as necessary, certs of any intermediate CAs) of the endpoint device's certificate chain is installed in the client's user store. Once configured as such, reconnection attempts after the max-session timeout expires should take no longer than 5 seconds.
PRS-318066	Auto remediation for downloading signatures of Windows Bit defender AV with Pulse L2 is looping even though the signatures are updated automatically as part of auto remediation.
PRS-301108	When OAC is upgraded from earlier versions to the latest version it might ask for reboot on Windows 7, Windows 8 and Windows 8.1.
PRS-320628	Syslog msg NOT received in full, if no licenses are installed on IC **Short Desc-1**: Syslog message not received in full (only syslog header is received) on the Remote Syslog Server after upgrade of IC from 4.4R10 to 5.0R1 Conditions: o IP address is used for specifying UDP Syslog Server in 4.4Rx o No user licenses installed on IC o Workaround: o Install User License on the IVE o Delete and Re-add the Syslog server entries in all the log types (events/access/admin) **Short Desc-2**: Syslog message NOT sent by IVE to Remote Syslog Server after upgrade of IC from 4.4R10 to 5.0R1. Conditions:

- hostname is used for specifying the UDP Syslog Server in 4.4Rx
- no user licenses installed on IC
- Workaround:
- Install User License on the IVE
- Delete and Re-add the Syslog server entries in all the log types(events/access/admin)

Documentation

Table 6 describes the documentation set for the present release. 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	
User Access Management Framework Feature Guide	An overview of the framework and configuration steps for AAA servers, roles, realms, and sign-in features.
Solutions	

Endpoint Security Feature Guide	Describes Host Checker, Cache Cleaner and Secure Virtual Workspace 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 1-888-314-5822 (toll-free in the USA, Canada, and Mexico).
  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 6Table2 lists the revision history for this document.

Table 7: Revision History

Revision	Description
15 Dec 2014	Initial publication.