Pulse Connect Secure Release Notes

8.1 R1 build 33493

Product Release 8.1/5.1

Document Revision 1.1
Published: 2015-01-05

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

END USER LICENSE AGREEMENT

Table of Contents

List of Tables

Introduction

This document is the release notes for Pulse Connect Secure Release 8.1. 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 Platforms

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

- SA2500, SA4500, SA4500 FIPS, SA6500, SA6500 FIPS
- MAG2600, MAG4610, MAG6610, MAG6611, MAG SM160, MAG SM360

To download software for these hardware platforms, go to:

https://www.juniper.net/support/downloads/group/?f=sa

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 lists the virtual appliance systems qualified with this release.

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:
https://www.juniper.net/support/downloads/group/?f=sa

Upgrade Paths

Table 2 describes the tested upgrade paths.

Table 2 Upgrade Paths

Release	Description
7.1R19 to 8.1R1	You can upgrade directly to 8.1R1 simply by installing the 8.1R1 update. The upgrade path is tested.
Earlier than 7.1R19	First upgrade to release 7.1R19 or later; then upgrade to 8.1R1.

Note: If your system is running Beta software, roll back to your previously installed official software release before you upgrade to 8.1R1. This practice ensures the rollback version is a release suitable for production.

Pulse Secure Rebranding

Pulse Connect Secure 8.1 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
Replacement of Shavlik Patch Assessment Solution	In prior releases the patch assessment and patch remediation solution had limitation of using only the Shavlik patch management software. This feature replaces the Shavlik solution with Opswat solution and provides support for verifying patch management status on the client machine by using Opswat solution.
AD Improvements	Support multiple connections per domain for improved performance. Changes the default mode of AD auth server to “Active Directory” instead of “Active Directory Legacy”.
Troubleshooting for New AD	For New AD mode, provides a troubleshooting tab in Auth server page.

Support OWA Push Notification	Support Exchange OWA 2013 and OWA 2010 long lived connections through rewriter. To improve scaling and performance for OWA use cases.
Improve A/P Cluster VIP Ownership Improvement	Improving the active node selection algorithm for A/P clusters to be a bit more deterministic and converge more rapidly.
A/A Cluster Scalability Improvement	Introduce options to selectively share session details in A/A Cluster for Scalability Improvements.
Support for Citrix StoreFront Resource Profile for HTML5 Access	Supports HTML5 delivery of Citrix Apps.
Option Regarding Pulse Connect Secure Action When Max 'SAME ID' Session Limit is reached	Pulse Connect Secure can be configured to allow the same user ID to connect to the PCS multiple times concurrently.
Radius – Properly Use Session-Timeout Attribute received Attribute	While the Pulse Connect Secure is usually configured with default Idle-Timeout and Session-Timeout values, some use case requires that permit allow customers to adjust these timers. The values are returned in RADIUS Access-Accept in the Idle-Timeout and Session-Timeout attributes to the vSA.
AAA Port Troubleshooting	AAA Port Troubleshooting between Customer and Admin Config
PushConfig Enhancements	Enhancements of push configuration options such as scheduling and reliant config transfer.
BYOD – Device Onboarding	This feature provides an end to end solution for users and devices to get on-boarded.
BYOD – MDM – 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 – Redirect to MDM	Provide ability to redirect to MDM server of Choice for enrollment.
BYOD – Windows Onboarding Support	This feature provides an end to end solution for users and devices to get on-boarded.
Browser Cache Refresh	Ensure correct files are downloaded by Browser after Pulse Connect Secure is upgraded.
File Integrity Checks during Boot Up	Ensure no corruption to system's vital files.
Java SHA2 support	Support Java signing with SHA 256 Algorithm.
Support for SharePoint 2013	Support for SharePoint 2013 is added.
Address Sign-In URL Violates configured sign-in policies	For Pulse Connect Secure, this feature ensures that the hostname of the current URL matches the one that is associated with the internal id embedded in URL.
OPSWAT Hard Disk Encryption	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.

General notes

The code signing certificate expiration date is Jan 22, 2017.

Open Issues

Table 4 lists open issues in this release.

Table 4 List of Open Issues in this release

PR Number	Release Note
PRS-315938	In order to support clients with TLS 1.1 and TLS 1.2 enabled, the server cert installed on Pulse Secure should be compatible with TLS 1.2.
PRS-318942	Network connect Linux client sometimes exit when laptop is suspended.
PRS-310541	Basic verification logs in Troubleshooting tab does not show enough information about the failure in case of invalid container name configured in Active Directory authentication server
PRS-317468	Certificate profile with keysize of 4096 fails to install on Android 4.3 on Samsung Galaxy. Installation on Android 4.4 succeeds.
PRS-318721	In the case that SA has two different device certs, one for external and one for internal interface, if an iOS device onboarded via one of the interfaces, and later when the same device attempts to connect to SA via a different interface, a "profile installation failed" message is shown on the device.
PRS-316902	Wi-Fi profile with EAP-TTLS cannot be configured on Windows 7 client.
PRS-316775	After Windows client onboarded, modifying the Pulse connection set on SA is not reflected on Windows client. Re-onboard on Windows client does not refresh Pulse connection set either. -- add more detail about how to get the new Pulse connection set onto Windows client.
PRS-312321	If a device record was created on one of the AA cluster nodes prior to this node goes off line, when the node comes back up and rejoin the cluster, update to the device record before rejoin was wiped out. The device record shows the information before the cluster node went off line.
PRS-312623	After Wi-Fi profile is installed on iOS through on-boarding, admin updates Wi-Fi profile, iOS device has to onboard two times update to appear on the device. This is specific with iOS. Similar behavior was observed with other MDM services.
PRS-307473	Sometimes Wi-Fi profile installation fails on Mac client when security type with ?wep? and ?Auto Connect? Enabled. This is also observed with ipcu configuration utility.
PRS-307761	URI value is empty in the generated cert even though there is value defined for SAN type URI. This is specific to iOS. Test with other MDM showed the same issue.

PRS-311135	Occasionally, profile installation fails on Mac OS if CSR is configured with Email field as blank. Retry fixes this issue. This seems to be Mac OS specific.
PRS-319000	License client pulls license count from license server, the client's event log mistakenly shows the license count as its user count. The actual user count in system is correct.
PRS-314542	After CONSEC/POLSEC license is added to SA/UAC, if this system is upgraded to a release that CONSEC/POLSEC is not supported, the license is shown as temporary.
PRS-314540	After CONSEC/POLSEC license is added to SA/UAC, if this system is upgraded to a release that CONSEC/POLSEC is not supported, the license is shown as temporary.
PRS-318766	In a 2 node cluster, delete all licenses from both nodes, re-import a previously exported config into one node, parevntd crash was observed, but import completes successfully, parevntd restarts automatically and continues without an issue. If only deletes all the licenses for one of the node, dsparevent did not crash. The crash was because the cache was not in sync.
PRS-192228	On Windows 7 (and Vista) when a Pulse VPN connection is active, Windows Network Connection Status Indicator icon in the taskbar will erroneously report that the network adapter has 'No Internet Access'. Furthermore, Windows Network Location Awareness (NLA) infrastructure will erroneously report a lack of internet connectivity. Certain apps, like Office365, use NLA to determine whether there is Internet connectivity, and may fail as the result of this false report from NLA. This is a Microsoft issue; Microsoft currently claims that the fix will be available in the July 2014 updates to Windows 7 (released on "Patch Tuesday", the second Tuesday of the month). Previously, Microsoft claimed that this issue was fixed in a hotfix for Windows 7 and included in a roll-up update: Hotfix: http://support.microsoft.com/kb/2524478/en-us Rollup: http://support.microsoft.com/kb/2775511/en-us Update in MSFT catalog: http://catalog.update.microsoft.com/v7/site/Search.aspx?q=2775511 Unfortunately, testing has indicated that the Microsoft fix does not work. More information can be found at the following KB: http://kb.juniper.net/KB19201
PRS-303898	With Firefox, For applications such as SharePoint and Novell Filr, office documents residing in server cannot be opened or edited from within the Microsoft Office client, when SA core access is used. This is because the rewriter technology relies on the passing of cookies and Microsoft Office apps do not have access to the Firefox cookie store, which is needed for successful authentication through the SA."

PRS-313892	During an import operation, the import page may timeout if the browser's timeout setting is small. In such a case, please check logs to see the result of import
PRS-317624	Automatic rescheduling of the event does not happen for suspended pushes on process restart
PRS-315824	HC custom checks: custom check with wildcard entry for NetBIOS name rule is not working properly.
PRS-310409	Restart and Shutdown Guest Ops are NOT working with 8.1R1 on ESXi 4.1 U3 and ESXi 5.5.
PRS-309350	EPS: Patches are still shown as missing if we install the missing patches manually and not via Software Center.
PRS-309348	EPS: Remediation is not happening successfully with SCCM 2012 or SCM2007 server though the remediation is triggered by HC.
PRS-308930	BYOD: On HTC device the user need to enter certificate name during cert provisioning.
PRS-308155	BYOD: Importing User config with Certificate profile (Global Cert and CA Cert) creates the profile without any Cert.
PRS-304422	AP-Cluster-new-algorithm - Pulse is taking more time to reconnect during failover scenario when connected using external IPv6 VIP.
PRS-301930	Secure Mail: Facing issue while on-boarding IOS device using Smart Card.
PRS-289876	End user should get error message window if he try to onboard the device using Virtual hostname of Secure mail profile.
PRS-318720	When SA configured different signing cert for external and internal ports, the same iOS devices cannot onboard from a port if it onboarded once from a different port. This is by design.
PRS-321299	Pulse Secure WTS is failing launch if the host is Windows 2012 server.
PRS-320378	Certificate status checking using OCSP with proxy setting enabled will not work.
PRS-321590	Onboarding feature is not visible on VA-DTE.

PRS-312761	VMWare Tool status will show Running (Unsupported) because VMWare supports "Running unsupported" when guest OS is selected as Other and no specific OS is selected. IVE is always configured Guest OS as Other.

Fixed Issues

Table 5 lists issues that have been fixed and are resolved by upgrading to this release.

Table 5 List of Issues Fixed in this Release

PR Number	Release Note
PRS-301120	Help Page is not available under Maintenance-> System -> help in SA 8.0R1(build 27742)+ IC 5.0R1 (build 23274)[Context_Sensitive_help_adminPages:4]
PRS-300425	Meeting: Unable to launch Meeting client using Proxy, installation went through but client did not gets connected.
PRS-300360	Web Rewriter: OWA2013 - Error uploading user profile picture.
PRS-300058	Auto-uninstall of NC failed with Windows-7 64 bit PC.
PRS-299926	Two user sessions exported to fed-server in session migration scenario with AD as auth server; a leaked session also observed.
PRS-299903	JSAM: MAC:JSAM window displays status as "EXPIRED" when user login through new window option from JSAM window.
PRS-299618	8.0R1-27467-JSAM - In Windows user is able to see the upload log button on JSAM applet when "Enable upload logs" option is disabled, but not seen in MAC.
PRS-298778	[Dashboard]: Legends not visible for Top Roles chart on Win 7 + IE11 during first login.
PRS-298773	IE11: Under Role Session options under Roaming session "Limit to subnet" is not showing correct behavior with IE11 browser.
PRS-298759	IE11: For Citrix client download Page under terminal services options section traversing between 'Enable Remote desktop launcher' radio button is not showing correct behavior with IE11 browser.

PRS-298570	SNMPv3 Engine Id not displayed on Node 2 part of A/P - Cluster Upgrade Triggered from Node 1.
PRS-298100	New AD server traffic always go through internal port even if AAA traffic over management port is enabled.
PRS-297581	Dashboard data for different chart time period lost on System Operations when 300K limit crossed.
PRS-296700	AP Cluster External Port IPv6 VIPs are no longer pingable after disabling IPv6 on Internal port.
PRS-295512	[Logging]: Dynamic Filter on Date field not working.
PRS-294375	Syslog over TLS not working with STRM syslog server.
PRS-291794	Single Pulse Client Throughput numbers for SSL show degradation for 8.0 and 8.1.
PRS-291788	Enabling 'Back to my mac' through iCloud is causing a utun0 conflict.
PRS-290732	TS HOB: With client proxy enabled end user is not able to connect to backend resources through TS HOB applet.
PRS-287942	Secure Mail: On iPad Onboard button is disabled always after user onboarded first time and on IPhone Status button shows always Active even if user record is quarantined-deleted and mail profile is removed.

Documentation

Table 6 describes the documentation set for the present release. Related 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.
SA Series to MAG Series Migration Guide	How to migrate the system configuration and user data to the newer platform.

Administration Guides

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.
Content Intermediate Engine Developer Reference	A reference on content intermediation engine support for Web content.
Client-Side Changes Installation Reference	List of the files added or settings modified on the client desktop environment after the Pulse desktop client has been installed.
Endpoint Security Feature Guide	Describes Host Checker, Cache Cleaner and Secure Virtual Workspace settings.

Solutions

IF-MAP Feature Guide	An overview of the feature and configuration steps.

Developer Reference Guide	
Custom Sign-In Pages Developer Reference	A reference on customization sign in pages
DMI Developer Reference	A reference on using DMI to manage system configuration

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).

- http://www.pulsesecure.net/support/
- 1-888-314-5822 within the United States
- 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/.

Revision History

Table 7 lists the revision history for this document.

Table 7 Revision History

Revision	Description
15 Dec 2014	Initial publication.