



Pulse Connect Secure

Release Notes

PCS 9.1R1 Build 1505

PDC 9.1R1 Build 607

Default ESAP Version: ESAP 3.3.5

Release, Build	9.1R1, 1505
Published	Jun 2020
Document Version	1.1

Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134

<https://www.pulsesecure.net>

© 2020 by Pulse Secure, LLC. All rights reserved

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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.

Revision History

The following table lists the revision history for this document.

Revision	Date	Description
1.1	Jun 2020	Updated Fixed Issues with PRS-368927
1.0	May 2019	Initial Publication 9.1R1

Contents

Revision History.....	3
Introduction.....	5
Hardware Platforms.....	5
Virtual Appliance Editions.....	5
VMware Applications.....	5
Upgrade Paths.....	6
Upgrade Scenario Specific to Virtual Appliances.....	6
General notes.....	6
New Features in 9.1R1 Release.....	7
Fixed Issues in 9.1R1 Release.....	7
Known Issues in 9.1R1 Release.....	9
Documentation.....	11
DocumentationFeedback.....	11
Technical Support.....	11

Introduction

This document is the release notes for Pulse Connect Secure Release 9.1R1. This document contains information about what is included in this software release: supported features, feature changes, unsupported features, and known 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 release onwards, VA-DTE will not be supported.

 **Note:** 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 or with cloud services such as Microsoft Azure and AWS.

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

Platform	Qualified System
VMware	<ul style="list-style-type: none"> • HP ProLiant DL380 G5 with Intel(R) Xeon(R) CPU • ESXi 6.7
KVM	<ul style="list-style-type: none"> • CentOS 6.6 with Kernel <code>cst-kvm 2.6.32-504.el6.x86_64</code> • QEMU/KVM v1.4.0 • Linux Server Release 6.4 on an Intel Xeon CPU L5640 @ 2.27GHz • 24GB memory in host • Allocation for virtual appliance: 4vCPU, 4GB memory and 40GB disk space
Hyper-V	<ul style="list-style-type: none"> • Microsoft Hyper-V Server 2016 and 2019
Azure-V	<ul style="list-style-type: none"> • Standard DS2 V2 (2 Core, 2 NICs) • Standard DS3 V2 (4 Core, 3 NICs) • Standard DS4 V2 (8 Core, 3 NICs)
AWS-V	<ul style="list-style-type: none"> • T2.Medium (2 Core, 3 NICs and 2 NICs) • T2.Xlarge (4 Core, 3 NICs) • T2.2Xlarge (8 Core, 3 NICs)

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

VMware Applications

The following table lists the VMware applications qualified.

Platform	Qualified
VMware Horizon View HTML Access, version 7.5, 7.4	<ul style="list-style-type: none"> • Rewriter
VMware Horizon View Server version 7.6, 7.7	<ul style="list-style-type: none"> • VDI Profiles

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
9.0Rx	Yes	-
8.3Rx	Yes	-
8.3Ry	-	Yes

For versions prior to 8.2, first upgrade to release 8.2Rx | 8.2Ry or 8.3Rx | 8.3Ry, and then upgrade to 9.1R1.

Note: If your system is running beta software, roll back to your previously installed official software release before you upgrade to 9.1R1. This practice ensures the rollback version is a release suitable for production.

Note: On a PCS/PPS virtual appliance, we highly recommend to freshly deploy a PSA-V from 8.3Rx based OVF, when any of the following conditions are met:

- If the disk utilization goes beyond 85%.
- If an admin receives iveDiskNearlyFull SNMP Trap.
- If the factory reset version on the PSA-V is 7.x | 8.0.

Upgrade Scenario Specific to Virtual Appliances

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

1. If PSA-V is running 8.2Rx:
 - a. Upgrade to 8.3R3 or later.
 - b. Install Core license through Authcode.
 - c. Upgrade to 9.1R1.
2. If PSA-V is running 8.3R1:
 - a. Upgrade to 8.3R3 or later.
 - b. Install Core license through Authcode.
 - c. Upgrade to 9.1R1.
3. If PSA-V is running 8.3R3 or later:
 - a. Install Core License through Authcode.
 - b. Upgrade to 9.1R1.

General notes

1. 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](#).
2. In 8.2R1.1 and above, all PCS client access binaries (Network Connect, WSAM, Host Checker, JSAM, Windows Terminal Services, Citrix Terminal Services) are signed with a SHA2 code signing certificate to improve security and ensure compatibility with Microsoft OS's 2016 restrictions on SHA1 code signing. This certificate will expire on April 12, 2021. For details, refer to KB articles [KB14058](#) and [KB43834](#).
3. Important note: Windows 7 machines must contain a March 10, 2015 Windows 7 Update in order to be able to accept and verify SHA2-signed binaries properly. This Windows 7 update is described [here](#) and [here](#). If this update is not installed, PCS 8.2R1.1 and later will have reduced functionality (see PRS-337311 below). (As a general rule, Pulse Secure, LLC recommends that client machines be kept current with the latest OS updates to maximize security and stability).
4. When custom ciphers are selected, there is a possibility that some ciphers are not supported by the web

browser. If any ECDH/ECDSA ciphers are selected, they require ECC certificate to be mapped to the internal/external interface. If an ECC certificate is not installed and mapped to the internal and external ports (if enabled), administrators may not be able to login to the appliance. The only way to recover from this situation is to connect to the system console and select option 8 to reset the SSL settings. Option 8 resets the SSL setting to factory default. Any customization is lost and will need to be reconfigured. This is applicable only to Inbound SSL settings.

5. Pre-5.0 Android and pre-9.1 iOS devices don't support Suite B ciphers. 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 PCS device.
6. Minimum ESAP version supported on 9.1R1 is 3.2.7 and later.

Note: From 9.1R2 release onwards, Network Connect (NC) client and Windows Secure Application Manager (WSAM) client will not be supported.

Note: From 9.1R1 release onwards, Active Directory Legacy Mode configuration will not be supported. If you have an existing Active Directory authentication server using Legacy Mode, first migrate to Standard Mode and then upgrade PCS. For the detailed migration procedure, refer [KB40430](#).

New Features in 9.1R1 Release

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

Feature	Description
Software Defined Perimeter	Pulse Secure SDP uses PCS appliances which individually act as either an SDP controller or an SDP gateway. Mobile users of the Pulse Secure Client perform authentication on an SDP controller which runs an Authentication, Authorization and Accounting (AAA) Service. The SDP controller then enables direct communication between the user and the SDP gateways that protect the user's authorized resources and enables requested encryption.
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.
Authentication failure management	Account Lockout option is provided to manage user authentication failures for admin users of local authentication server. The admin user account will be locked after specified number of consecutive wrong password attempts. The account will be unlocked after the specified lockout period or by using the Unlock option.
Support for "client-name" parameter in HTML5 Access	User can pass "client-name" in HTML5 rdp using launcher method. The %clientname% variable is matched with a workstation ID and normally that variable is unique and dedicated remote desktop computer name.
Deploying PSA-V in KVM	User can deploy PSA-V in KVM using a template.
User access to internet resources PCS	AWS VPC GW and Azure VNet GW drop packets if the source IP is the endpoint tunnel IP. This feature NATs endpoint tunnel IP to Internal interface IP. The NAT allows user to access internet resources when connected to a VPN tunnel on an Azure or AWS-based PCS.
REST API enhancements	Enhancements include: <ul style="list-style-type: none"> - Getting Config without Pulse packages such as ESAP package and Pulse Client package - Backing up and restoring binary configuration

Fixed Issues in 9.1R1 Release

The following table lists Fixed issues in this release.

Problem Report Number	Summary
Pulse Connect Secure	
PCS-5064	Summary: Remove legacy mode from Active Directory auth. server.
PRS-375534	Summary: JSAM Stats value (Bytes count) is not getting displayed in IE - Activex.

PRS-375067	Summary: DNS resolution not working for alternate VPN connections.
PRS-374597	Summary: The definition update is not listed for Sentinelone product in "epupdate_hist.xml" file.
PRS-374057	Summary: Unable to add the resource <userAttr.Framed-Route> in IPV4 address under Split tunneling policy for PCS version 9.0Rx.
PRS-374037	Summary: Rewrite: PSAL launching Citrix app multiple times in an infinite loop on all the browsers.
PRS-373948	Summary: Web Rewrite :: Contents of a web response are not getting compressed as content encoding header is missing in the response from PCS.
PRS-373769	Summary: Host Checker IMC detects the Antivirus Change in the client PC and report it to IMV even when Perform Check every min is set to 0.
PRS-373696	Summary: Split tunneling FQDN policy with special character, fails to save.
PRS-370953	Summary: PTP: Unable to edit word documents hosted on SharePoint 2013 via PTP using MS Edge.
PRS-371023	Summary: Resource access dropped (RDP, SSH etc.) intermittently on SAW environment.
PRS-373102	Summary: Core Access: E-mail web page getting stuck on "login processing".
PRS-373076	Summary: Core Access:Web page shows horizontal scrollbars at the bottom of screen.
PRS-372181	Summary: DanaLoc fails in case of old window object reference from a new window object.
PRS-372834	Summary: PSAM:Pulse SAM takes at least 40 seconds to open custom start up page in UI Options compared to WSAM.
PRS-372677	Summary: AAA/Security/Pulse: SAML AuthnRequest leaks data across users with "Reuse NC/Pulse session" enabled.
PRS-372595	Summary: User getting same IP address assigned from IP pool in few hours.
PRS-372489	Summary: Pulse browser Toolbar is flickering when accessing OWA 2016 resource on iOS device through webrewrite.
PRS-372285	Summary: PSA 7000f Frequently reports one of the power supplies is back up.
PRS-372055	Summary: Unable to save Citrix listed application using Hostname with port number.
PRS-371973	Summary: HC: Compliance fails using Pulse Desktop client 9.0.2 build 1151.
PRS-371970	Summary: Users with username in UPN format in System Local Authserver are unable to log in using TOTP after upgrading to 9.0R3.
PRS-371944	Summary: Killed user session admin log "ADM23534" does not display admin user but the actual user being terminated.
PRS-371800	Summary: PCS device is unable to get the enrolled mobile device attribute from MDM server.
PRS-371394	Summary: Setting the hash property of location object causes problem in IE, Edge and Firefox browsers because the URL is appended with fragment identifier. In chrome and Safari browsers things work fine.
PRS-371602	Summary: Post upgrade to PCS 9.0R3, "License server low-level protocol error Code = [47]" error is triggered on license client.
PRS-371513	Summary: Page does not load via IE browser.
PRS-371406	Summary: "Auto populate domain information" behavior when unchecked: blank first then if wrong password, auto populates domain.
PRS-371357	Summary: HTML5 RDP logging do not show realm and shows ().
PRS-371342	Summary: Add iOS Check 12.1.1.
PRS-371266	Summary: Menu is not loading when accessing the application through web-rewrite.
PRS-371231	Summary: PCS 9.0 VA-DTE :: Nodes in cluster gets disabled automatically.
PRS-371205	Summary: Multicast Traffic not working intermittently in the VPN Tunnel in 8.3R6 / 5.3R6 version and after restarting services, works fine for all users.
PRS-371154	Summary: Wrong information in the log messages for Authorization Only Access when source ip restriction is configured on role.
PRS-371114	Summary: Add support for adding parameters "client-name" for HTML5 Access.
PRS-369351	Summary: LDAP authorization does not work when using ikev2 tunnel (handle 10K tunnels+few hundred ikev2 clients).
PRS-370138	Summary: Read-only admin sessions see an option as disabled that is actually enabled on user roles.
PRS-369960	Summary: Page displayed while PSAL downloads to a Mac client shows instruction for Mac; but then references Windows System Tray.

PRS-369200	Summary: Logs are not fully displayed if select the date as filter.
PRS-369142	Summary: File browsing SSO is not working with user details are given in variable form as well when configured to use system credentials.
PRS-369031	Summary: When a configuration object is renamed, not all of the resulting configuration changes are uploaded to Pulse One.
PRS-368927	Summary: Web process crashes and logs "ERR31093: Program web recently failed." in the event logs.
PRS-367879	Summary: Core Access: Unable to import or download the image using PTP.
PRS-367789	Summary: DMI agent not responding to netconf commands as expected.
PRS-367285	Summary: System Active/Passive cluster responding to ICMP request even after shutdown.
PRS-366634	Summary: Pulse IPv6 :: Randomly users are not able to access IPv6 resources through VPN device via VPN tunneling.
PRS-364219	Summary: PSA7000f interface status in Network Settings not working.

Known Issues in 9.1R1 Release

The following table lists known issues in this release.

Problem Report Number	Release Note
Pulse Connect Secure	
PRS-362240	<p>Symptom: User sees detect receiver window rather than PSAL download page upon clicking the apps.</p> <p>Conditions: Users are unable to launch Citrix Apps/Desktop that are published in storefront.</p> <p>Workaround:</p> <ul style="list-style-type: none"> Forward the Cookie: CtxsClientDetectionDone=true as name value pair in SSO form or using custom header policies. Re-click the bookmark by returning to home page and access the SF application again.
PRS-373014	<p>Symptom: Virtual Appliance platform license activated message seen every 10 mins in Admin logs.</p> <p>Conditions:</p> <ul style="list-style-type: none"> Admin has installed Virtual Appliance platform license through authorization codes. Admin has also leased cores from a license server. <p>Workaround: Delete the installed Virtual Appliance platform license (as the cores are provided by license server).</p>
PRS-373762	<p>Symptom: Named User Remote Repo (NURR) mode does not work when MSSP unlimited license is installed on the License server.</p> <p>Condition: MSSP Unlimited License installed on License server.</p> <p>Workaround: Pulse Secure advises MSSP customers with MSSP SKU to not use NURR mode.</p>
PRS-374091	<p>Symptom: All client installations fail when using auth proxy in MAC OS.</p> <p>Condition: Client installations in MAC OS using auth proxy.</p> <p>Workaround: None</p>
PRS-374458	<p>Symptom: Fresh deployment of Azure image on PCS is not available.</p> <p>Condition: Fresh deployment of Azure image on PCS.</p> <p>Workaround: Upgrade the server. A new image will be posted soon.</p>
PRS-374790	<p>Symptom: Unable to edit Power Point files within any browser from Share Point 2016 server.</p> <p>Condition: In Rewriter mode of browsing Share Point 2016 server.</p> <p>Workaround: Create Custom Header Allow policy for the Share Point URL.</p>
PRS-375051	<p>Symptom: Unable to edit existing client to increase or decrease the number of cores leased via REST/XML.</p> <p>Condition: Observed in REST PUT request and XML import.</p> <p>Workaround: Use the UI to make changes.</p>
PRS-375138	<p>Symptom: Client upload logs fails for Network Connect and JSAM.</p> <p>Condition: After launching Network Connect and JSAM on Windows 10, client upload log fails.</p> <p>Workaround: None</p>

Problem Report Number	Release Note
PRS-375329	<p>Symptom: HOB failed to launch through Java in IE.</p> <p>Condition: HOB launch fails with IE and JAVA combination on Windows 10 endpoint.</p> <p>Workaround: Launch through ActiveX.</p>
PRS-375886	<p>Symptom: JSAM launch failing for IE - JAVA.</p> <p>Condition: JSAM launch fails with IE and JAVA combination on Windows 10 endpoint.</p> <p>Workaround: Launch through ActiveX.</p>
PRS-376021	<p>Symptom: Intermittently end-user gets "Detected an Internal error" while logging into a browser-based session.</p> <p>Condition: When end-user tries to log in to Pulse Connect Secure through Safari browser on Mac.</p> <p>Workaround: Reboot the Mac laptop</p>
PRS-376245	<p>Symptom: HOB and JSAM not working in Linux.</p> <p>Condition: When end user tries to launch HOB and JSAM on Linux platform.</p> <p>Workaround: None</p>
PRS-376312	<p>Symptom: Factory reset from VMware VA console does not load the factory reset version and loads the current version.</p> <p>Condition: When trying to do factory reset to C9.1R1 from higher version in VMware-VA.</p> <p>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:</p> <ul style="list-style-type: none"> • Current version • Rollback version • Factory reset version <p>Admin need to manually select the Factory reset version for the factory reset to happen successfully on VMware VA.</p>
PCS-11922	<p>Symptom: DNS Port selection will not take any effect. DNS traffic will go through Internal Port only.</p> <p>Condition: On a PCS Virtual Appliance, when Administrative Network is enabled under Traffic Segregation. This issue is not applicable for PSA Hardware Devices.</p> <p>Workaround: None</p>
PCS-12383	<p>Symptom: SNAT functionality failed to work even when it is enabled post the fresh deployment.</p> <p>Condition: In cloud instance (Azure/AWS), admin enables the NAT behavior from its initial disabled state and sees the NAT functionality failed to work.</p> <p>Workaround: PCS needs to be rebooted from the portal post the deployment.</p>
Cloud Secure	
PRS-371781	<p>Symptom: Blocked ECP users will not be updated if Generic is selected under LDAP server Type.</p> <p>Condition: LDAP server type selected is Generic.</p> <p>Workaround: Select the LDAP server type as Active Directory.</p>
PRS-372846	<p>Symptom: Blocked ECP users will have a "Blocked till time" of 5 minutes.</p> <p>Condition: Request count for a particular user is less than 3.</p> <p>Workaround: None</p>
PRS-372861	<p>Symptom: Blocked ECP users will not be removed from the ECP reports page based on "Blocked till time".</p> <p>Condition: When a user entry is present in the ECP reports page.</p> <p>Workaround: None</p>

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>.