



# Pulse Connect Secure

Release Notes

PCS 9.0R6 Build 64143.2

PDC 9.0R6 Build 1971

Default ESAP Version: ESAP 3.3.5

Release, Build	<b>9.0R6, 64143.2</b>
Published	<b>May 2020</b>
Document Version	<b>6.3.1</b>

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://support.pulsesecure.net/product-service-policies/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
6.3.1	May 2020	Updated the 9.0R3 New Features section
6.3	December 2019	Initial Publication 9.0R6
6.2	September 2019	Initial Publication 9.0R5
6.1	July 2019	Initial Publication 9.0R4.1
6.0	April 2019	Initial Publication 9.0R4
5.3.1	March 2019	Updated the 9.0R3 Known Issues section
5.3	February 2019	Initial Publication 9.0R3.2
5.2	February 2019	Updated the TOTP feature in 9.0R3 New Features section
5.1	December 2018	Initial Publication 9.0R3.1
5.0	December 2018	Initial Publication 9.0R3
4.0	September 2018	Initial Publication - 9.0R3 Beta
3.0	August 2018	Initial Publication 9.0R2
2.0	April 2018	Initial Publication 9.0R1
1.0	February 2018	Initial Publication - 9.0R1 Beta

## Contents

Revision History.....	3
Introduction.....	5
Hardware Platforms.....	5
Virtual Appliance Editions.....	5
Upgrade Paths.....	5
Upgrade Scenario Specific to Virtual Appliances.....	6
General notes.....	6
Fixed Issues in 9.0R6 Release.....	7
New Features in 9.0R5 Release.....	7
Fixed Issues in 9.0R5 Release.....	8
Known Issues in 9.0R5 Release.....	9
Fixed Issues in 9.0R4.1 Release.....	9
Known Issues in 9.0R4.1 Release.....	10
New Features in 9.0R4 Release.....	10
Fixed Issues in 9.0R4 Release.....	11
Known Issues in 9.0R4 Release.....	12
Fixed Issues in 9.0R3.2 Release.....	12
Fixed Issues in 9.0R3.1 Release.....	13
New Features in 9.0R3 Release.....	13
Fixed Issues in 9.0R3 Release.....	14
Known Issues in 9.0R3 Release.....	16
New Features in 9.0R2 Release.....	22
Noteworthy Changes.....	23
Fixed Issues in 9.0R2 Release.....	23
Known Issues in 9.0R2 Release.....	25
New Features in 9.0R1 Release.....	26
Fixed Issues in 9.0R1 Release.....	28
Known Issues in 9.0R1 Release.....	29
Documentation.....	34
Technical Support.....	34

## Introduction

This document is the release notes for Pulse Connect Secure Release 9.0R6. 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://support.pulsesecure.net/>

## Virtual Appliance Editions

**Note:** From 9.0R1, 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"> <li>• HP ProLiant DL380 G5 with Intel(R) Xeon(R) CPU</li> <li>• ESXi 6.7</li> </ul>
VMWare	
VMWare Horizon View HTML Access, version 7.5, 7.4	<ul style="list-style-type: none"> <li>• Rewriter</li> </ul>
VMWare Horizon View Server version 7.6, 7.7	<ul style="list-style-type: none"> <li>• VDI Profiles</li> </ul>
KVM	<ul style="list-style-type: none"> <li>• CentOS 6.6 with Kernel cst-kvm 2.6.32-504.el6.x86_64</li> <li>• QEMU/KVM v1.4.0</li> <li>• Linux Server Release 6.4 on an Intel Xeon CPU L5640 @ 2.27GHz               <ul style="list-style-type: none"> <li>◦ 24GB memory in host</li> </ul> </li> <li>• Allocation for virtual appliance: 4vCPU, 4GB memory and 40GB disk space</li> </ul>
Hyper-V	<ul style="list-style-type: none"> <li>• Microsoft Hyper-V Server 2016 and 2019</li> </ul>
Azure-V	<ul style="list-style-type: none"> <li>• Standard DS2 V2 (2 Core, 2 NICs)</li> <li>• Standard DS3 V2 (4 Core, 3 NICs)</li> <li>• Standard DS4 V2 (8 Core, 3 NICs)</li> </ul>
AWS-V	<ul style="list-style-type: none"> <li>• T2.Medium (2 Core, 3 NICs and 2 NICs)</li> <li>• T2.Xlarge (4 Core, 3 NICs)</li> <li>• T2.2Xlarge (8 Core, 3 NICs)</li> </ul>

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

## 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
9.0R5	Yes	-

Upgrade From	Qualified	Compatible
9.0R4.1	Yes	-
9.0R3.2	Yes	-
9.0R2	Yes	-
9.0R1	Yes	-
8.3Rx	Yes	-
8.3Ry	-	Yes
8.2Rx	Yes	-
8.2Ry	-	Yes

For versions prior to 8.2, first upgrade to release 8.2Rx|8.2Ry or 8.3Rx|8.3Ry, and then upgrade to 9.0Rx.

**Note:** If your system is running beta software, roll back to your previously installed official software release before you upgrade to 9.0R6. 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 9.0R6 without a core license installed. Follow these steps to upgrade to 9.0R6:

1. If PSA-V is running 8.2Rx:
  - a. Upgrade to 8.3R3 or later.
  - b. Install Core license through Authcode.
  - c. Upgrade to 9.0R6.
2. If PSA-V is running 8.3R1:
  - a. Upgrade to 8.3R3 or later.
  - b. Install Core license through Authcode.
  - c. Upgrade to 9.0R6.
3. If PSA-V is running 8.3R3 or later:
  - a. Install Core License through Authcode.
  - b. Upgrade to 9.0R6.

## 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 the 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 9.0R6 is 3.2.7 and later.

## Fixed Issues in 9.0R6 Release

The following table lists Fixed issues in this release.

Problem Report Number	Summary
<b>Pulse Connect Secure</b>	
PRS-382840	<b>Summary:</b> adding process trace info in system snapshot.
PRS-381942	<b>Summary:</b> Users are accessing Citrix Storefront using HTML5 Receiver via Core Access.
PRS-381621	<b>Summary:</b> 9.0R4 and 9.0R5 SPE (PSA-V) do not show the User Record Sync column in Admin UI > Auth Server page.
PRS-381366	<b>Summary:</b> Multiple users getting disconnected from Pulse Client.
PRS-381266	<b>Summary:</b> Failure to launch Host Checker if the username contains non-English characters.
PRS-379801	<b>Summary:</b> Active Sync stopped working after upgrading the device to 9.0R4.
PRS-379125	<b>Summary:</b> Pulse One 2.0.1901: With PCS 9.0R5 (EA) having failure in target importing SAML using Artifact - empty "Source Artifact Resolution Service URL".
PRS-377681	<b>Summary:</b> PSA7000f reports HDDs missing and inactive after upgrade to 9.1R1.
PRS-377489	<b>Summary:</b> JSAM is not working when Do not include session cookie in URL (maximize security) is enabled.
PRS-377160	<b>Summary:</b> HTML-5 -RDP requires additional authentication.
PRS-375181	<b>Summary:</b> VLS does not throw any error if there is no response for Heartbeats sent to PCLS.
PRS-374146	<b>Summary:</b> UNC path is not handled properly by HOB Applet.
PRS-373941	<b>Summary:</b> Test Connection is not working with Airwatch and Mobile Iron as MDM server in PCS.
PRS-371699	<b>Summary:</b> Users unable to login as well as dropping users - LMDB full.
PRS-371351	<b>Summary:</b> 9.0 issue with Citrix port 2598 via JSAM, it is not working but works in 8.,2R8 so Citrix sessions drop regularly causing various issues.

## New Features in 9.0R5 Release

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

Feature	Description
Report Max Used Licenses to HLS VLS	From 9.0R5 release, the licensing client (PCS) starts reporting maximum used sessions count instead of the maximum leased licenses count. For MSP customers, this change helps in billing the tenants based on maximum sessions used.
Managing active user sessions	From 9.0R5 release, an administrator is provided with an option to delete selected active user sessions or all the active user sessions.

# Fixed Issues in 9.0R5 Release

The following table lists Fixed issues in 9.0R5 release.

Problem Report Number	Summary
<b>Pulse Connect Secure</b>	
PRS-379962	<b>Summary:</b> SAML authentication fails.
PRS-379855	<b>Summary:</b> Host checker did not get installed properly" error appears on browser after the machine reboot.
PRS-379058	<b>Summary:</b> Destination node is always showing the same error message with specific admin roles, user roles while trying to sync config.
PRS-377979	<b>Summary:</b> When accessing the resources via bookmark, the displayed content is incorrect.
PRS-377798	<b>Summary:</b> ACE server "node verification file" and SDCONF.rec being overwritten or cleared when "Auth Server" is included in Group settings.
PRS-377505	<b>Summary:</b> Config uploader fails to upload configuration to Pulse One.
PRS-377022	<b>Summary:</b> File Share accessing issue in 9.0R4.
PRS-377437	<b>Summary:</b> Event logs show "License server low-level protocol error Code = [47]" error on licensing client.
PRS-376872	<b>Summary:</b> Redirection to Custom Start Page takes more than 60 seconds in IE browser.
PRS-376869	<b>Summary:</b> Dns_cache process snapshots persist after upgrading to 9.0R4HF6.
PRS-376859	<b>Summary:</b> Premier Java Applet for Terminal Service failed to download .jar file.
PRS-376249	<b>Summary:</b> Logon page of SAP fiori portal displayed as blank in IE11 only via rewrite.
PRS-376036	<b>Summary:</b> PCS evaluation of the custom expression "time.dayOfYear" is not working as expected.
PRS-375880	<b>Summary:</b> Web Rewrite :: None of the contents in the Azure web portal are loading through rewrite.
PRS-375079	<b>Summary:</b> RCA: CORE.fqdncl crashes continues to occur even after 9.0R2.1HF6 (with fix).
PRS-375013	<b>Summary:</b> Radius OTP (Secondary authentication server) authentication fails for the Pulse Client users, however works fine through Browser.
PRS-374894	<b>Summary:</b> Invalid resource when trying to add "*.com" in split tunneling resource.
PRS-374831	<b>Summary:</b> Login page is not rendering properly for a web resource configured through rewrite.
PRS-374641	<b>Summary:</b> Post upgrade to PPS 9.0R3.1, we observe "License server low-level protocol error Code = [47]" error on licensing client every 10 minutes.
PRS-374603	<b>Summary:</b> Syslog missing event logging info when upgrading.
PRS-374367	<b>Summary:</b> PSAL launch failed when browser Proxy is configured.
PRS-374344	<b>Summary:</b> Last core dumps being generated at customer after applying 9.0R2.1HF6 with fixes. Need an RCA.
PRS-374138	<b>Summary:</b> Platform field incorrectly populated as Virtual Appliance for PSA License Client on License Server.
PRS-374057	<b>Summary:</b> Unable to add the resource <userAttr.Framed-Route> in IPV4 address under Split tunneling policy for PCS version 9.0Rx.
PRS-374037	<b>Summary:</b> PSAL launching Citrix app multiple times in an infinite loop on all the browsers.
PRS-373948	<b>Summary:</b> Contents of a web response are not getting compressed as Content-Encoding header is missing in the response from PCS.
PRS-373102	<b>Summary:</b> E-mail web page getting stuck on "login processing".
PRS-372834	<b>Summary:</b> PSAM:Pulse SAM takes more time to open custom start up page in UI Options compared to WSAM.
PRS-372805	<b>Summary:</b> Pulse Embedded Browser:: Realm level certificate restriction skipped with SAML authentication.
PRS-372595	<b>Summary:</b> User getting same IP address assigned from IP pool in few hours.
PRS-372055	<b>Summary:</b> Unable to save Citrix listed application using Hostname with port number.
PRS-371944	<b>Summary:</b> When user session is killed, admin log displays user instead admin user who performed the operation.



PRS-371406	<b>Summary:</b> "auto populate flag" check fails when the new page is loaded after giving a wrong login and password.
PRS-371357	<b>Summary:</b> HTML5 RDP logging does not show realm and shows ().
PRS-371154	<b>Summary:</b> Wrong information in the log messages for Authorization Only Access when source IP restriction is configured on role.
PRS-370953	<b>Summary:</b> PTP: Unable to edit word documents hosted on SharePoint 2013 via PTP using MS Edge.
PRS-370210	<b>Summary:</b> Clear config on PSA 300 fails with unable to mount /webserver partition.
PRS-368799	<b>Summary:</b> DFS: PCS sends periodic renewal to License Server through Internal Port, even if configured as Management.
PRS-368234	<b>Summary:</b> 8.3R3 Web Crashes requesting RCA as it disconnected many VPN tunnels and failover did not occur.
PRS-366643	<b>Summary:</b> Outlook (OWA) loading issue in IE11 via rewrite.

## Known Issues in 9.0R5 Release

The following table lists known issues in 9.0R5 release.

Problem Report Number	Release Note
<b>Pulse Connect Secure</b>	
PRS- 380017	<p><b>Symptom:</b> Cluster: PCS queries the license server for two times when a user clicks on "pull state from server" button.</p> <p><b>Conditions:</b> When user clicks on "pull state from server" button.</p> <p><b>Workaround:</b> None</p>
PRS- 379998	<p><b>Symptom:</b> On a cluster setup, dszserverd process fails.</p> <p><b>Conditions:</b> When license server is unreachable from internal port.</p> <p><b>Workaround:</b> None</p>
PRS- 379969	<p><b>Symptom:</b> Communication to License server happens through Internal port even though preferred network is configured as Management port.</p> <p><b>Conditions:</b> When default Vlanid is configured.</p> <p><b>Workaround:</b> None</p>

## Fixed Issues in 9.0R4.1 Release

The following table lists Fixed issues in 9.0R4.1 release.

Problem Report Number	Summary
<b>Pulse Connect Secure</b>	
PPS-5674	<b>Summary:</b> Anti-Virus Signature evaluation has been optimized by changing server-side and client-side capabilities.
PRS-372999	<b>Summary:</b> Host Checker is failing for Host Checker(OS-Check only) for Chrome OS 71.0.3578.127 with Pulse Connect Secure 9.0R1 firmware version.
PRS-374367	<b>Summary:</b> PSAL launch is failing when browser proxy is configured.
PRS-374597	<b>Summary:</b> Anti-Virus Definition check (number of updates) has been fixed by upgrading the Opswat UpdateVerify SDK from 2.3.15.208.
PRS-376034	<b>Summary:</b> For machine only stealth mode connection, "Use Desktop Credentials" shouldn't be enabled.
PRS-376429	<b>Summary:</b> When using Java and IE (without Active X), JSAM is failing to launch.
PRS-376652	<b>Summary:</b> Host Checker is getting stuck in checking compliance when manual proxy is configured on the browser.

PRS-376889	<b>Summary:</b> Consider the drives for evaluation and ignore the drives only if API output says the drive is not capable of encryption explicitly.
PRS-377489	<b>Summary:</b> Using PSAL, Java applets like Hob, JSAM, WTS fail to launch when "Do not include session cookie in URL (maximize security)" is enabled.
PRS-377945	<b>Summary:</b> After updating a role-mapping rule within a realm on master appliance, and then publishing that realm to a target appliance causes the following side-effects: <ul style="list-style-type: none"> <li>• Many log messages are logged in the target's Admin Access Log.</li> <li>• Causes all user sessions to be terminated on the target.</li> </ul>

## Known Issues in 9.0R4.1 Release

The following table lists known issues in 9.0R4.1 release.

Problem Report Number	Release Note
<b>Pulse Connect Secure</b>	
PRS-378012	<p><b>Symptom:</b> JSAM Stats (Bytes count) does not get displayed in IE.</p> <p><b>Conditions:</b> When the "Do not include session cookie in URL (maximize security)" option is enabled.</p> <p><b>Workaround:</b> None</p>

## New Features in 9.0R4 Release

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

Feature	Description
User Records Synchronization (URS) enhancement	In this release, this feature is available for Virtual Appliances i.e., VMware, Hyper-V, KVM, AWS & Azure. For more details about URS feature, see the "Synchronizing User Records" section in <i>Pulse Connect Secure 9.0R4 Administration Guide</i> .
Send service traffic via any physical interface	Prior to 9.0R4 release, the NTP, SNMP, Syslog, and Log archiving services were set to send the traffic through management port by default. In case the management port was not available, the traffic was routed through internal port. From 9.0R4 release, an administrator can modify the settings of NTP and other services to any physical interface.
Backup administrator account for LDAP	In this release, PCS supports two LDAP administrator accounts. By adding the backup account, PCS now has the option to fallback from one to other if one account fails authentication.
Remove and refresh expired Root CAs	When the system software is upgraded to 9.0R4, the latest set of Trusted Server CAs are uploaded. Any expired certificates in the default Trusted Server CA store are removed from the system.
Host Checker enhancement	<ul style="list-style-type: none"> <li>• Detection of System Integrity Protection (SIP) is available for macOS versions 10.11 and later.</li> <li>• Command rule enables administrators to check for the versions of the installed applications on the macOS endpoints.</li> </ul>
Support for snmpget	This release supports snmpget for the following: <ul style="list-style-type: none"> <li>• SNMP monitoring of last day to connect to Pulse cloud or similar.</li> <li>• SNMP get max number of licensed users displayed under the licensing summary.</li> </ul>
PSAL enhancement	When client log upload is enabled at System > Log/Monitoring > Client Logs > Settings, endpoints utilizing the Pulse Secure Application Launcher (PSAL) can upload client logs.
VA Partition for VMWare	This feature uses volume-based grouping of the disk partitions so that the administrator can flexibly define the size or rearrange the layout based on the requirement of the installed image.
Support for MOBIKE protocol	IKEv2 Mobility and Multihoming protocol provides better handling of clients that change IP addresses.

## Fixed Issues in 9.0R4 Release

The following table lists Fixed issues in 9.0R4 release.

Problem Report Number	Summary
<b>Pulse Connect Secure</b>	
PCS-11023	<b>Summary:</b> Link MAX_LICENSED_USERS_REACHED to Max count.
PRS-372285	<b>Summary:</b> PSA 7000f frequently reports one of the power supplies is back up.
PRS-368980	<b>Summary:</b> Process snapshots are getting generated on "Program dns_cache recently failed".
PRS-371325	<b>Summary:</b> Radius authentication fails with non-standard port when Auth Traffic Control is configured for external port.
PRS-364219	<b>Summary:</b> Interface statistics at System>Network>Overview may be incorrectly reported as -1 packets.
PRS-366634	<b>Summary:</b> IPv6 resource access may fail over a mixed mode L3 connection.
PRS-367285	<b>Summary:</b> Active/Passive cluster nodes may respond to ICMP (ping) requests after triggering shutdown from the Maintenance>Platform page.
PRS-367471	<b>Summary:</b> Pulse clients may fail to complete authentication and tunnel setup after a PCS cluster has been the target of a push config event.
PRS-367750	<b>Summary:</b> HOB-based RDP fails to launch when using Pulse Secure Application Launcher (PSAL).
PRS-367789	<b>Summary:</b> DMI agent fails to respond if the netconf request includes the xmlns parameter.
PRS-368044	<b>Summary:</b> Host Checker: Cisco Malware protection fails to be detected properly.
PRS-368158	<b>Summary:</b> WinTermSvc: Launching a terminal service session using RDP launcher or the PCS-based browser may fail when Pulse Secure Application launcher is required (e.g. using Firefox, Chrome, or Safari).
PRS-368255	<b>Summary:</b> Pulse: Captive portal authentication window will load and close without time to enter login details.
PRS-369031	<b>Summary:</b> Pulse One: Changing object names (e.g. realm or role) may not properly propagate to Pulse One, causing publish failure.
PRS-371325	<b>Summary:</b> File browsing: Non-static credential configuration fails SSO access to defined resource.
PRS-369200	<b>Summary:</b> Logging: Date range in the log viewer may exclude messages near the delta points.
PRS-370090	<b>Summary:</b> Host Checker: Virus Definition check for updates for Palo Alto Traps may fail.
PRS-370138	<b>Summary:</b> Admin: Read-only admin sessions may see a role option erroneously disabled.
PRS-370839	<b>Summary:</b> System: Cloud-based PCS appliances may fail to download XML configuration data when configured using hostname.
PRS-370893	<b>Summary:</b> Pulse: Proxy credentials are prompted when proxy exception is defined for the PCS URL using wildcard.
PRS-371012	<b>Summary:</b> Pulse: Lockdown is disabled after being enabled with always-on VPN.
PRS-371035	<b>Summary:</b> Host Checker/Logging: Certificate hash may be recorded in the user access log when doing machine cert authentication.
PRS-371095	<b>Summary:</b> System: Core license is not activated properly.
PRS-371205	<b>Summary:</b> Pulse: Multicast traffic may not work as expected with mixed multicast configuration across roles.
PRS-371257	<b>Summary:</b> System: Virtual appliances may not have the client installers available for download.
PRS-371266	<b>Summary:</b> Web: Javascript files that contain non-breaking space (ACSCII 160) may not rewrite properly.
PRS-371348	<b>Summary:</b> Host Checker: Hard drive encryption (FileVault) state may not be detected properly.
PRS-371539	<b>Summary:</b> Pulse: Instantproxy.pac may create an erroneous merge statement when the PCS is accessed through a proxy.
PRS-371754	<b>Summary:</b> AAA: Users registered with TOTP may not be able to login successfully after enabling registration on external port.

PRS-371789	<b>Summary:</b> System/Monitoring: SNMP queries may cause system failure and procsd process snapshots when more than 64 VPN tunnels are established.
PRS-371973	<b>Summary:</b> Host Checker: McAfee AV state may not be correctly identified.
PRS-372417	<b>Summary:</b> AAA: Custom sign-in page upload may fail when using a valid zip file.

## Known Issues in 9.0R4 Release

The following table lists known issues in 9.0R4 release.

Problem Report Number	Release Note
<b>Pulse Connect Secure</b>	
PCS-11701	<p><b>Symptom:</b> End-users are unable to log in to PCS.</p> <p><b>Conditions:</b></p> <ul style="list-style-type: none"> <li>- PCS is unable to lease more licenses from license server, since license server does not have enough licenses to lease.</li> <li>- Requests are redirected by an external load balancer to PCS, since MAX_LICENSED_USERS_REACHED is set to NO by PCS.</li> </ul> <p><b>Workaround:</b> Add more licenses on the license server.</p>
PRS-11893	<p><b>Symptom:</b> PCS downgrade fails when downgrading from 9.0R4 to pre-9.0R3 build.</p> <p><b>Condition:</b> Downgrading to pre-9.0R3 build directly from PCS 9.0R4.</p> <p><b>Workaround:</b> Downgrade first to 9.0R3 and then downgrade to the required pre-9.0R3 build.</p>
PRS-371095	<p><b>Symptom:</b> Server upgrade fails when tried to upgrade from pre-9.0R4 release to 9.0R4 when the ICE license is installed.</p> <p><b>Condition:</b> ICE license is pre-installed on the server.</p> <p><b>Workaround:</b> Delete the ICE license, upgrade the server and install the ICE license.</p>
PRS-375138	<p><b>Symptom:</b> Client upload logs fails for Network Connect and JSAM.</p> <p><b>Condition:</b> After launching Network Connect and JSAM on Windows 10, client upload log fails.</p> <p><b>Workaround:</b> None</p>
PRS-375329	<p><b>Symptom:</b> HOB failed to launch through Java in IE.</p> <p><b>Condition:</b> HOB launch fails with IE and JAVA combination on Windows 10 endpoint.</p> <p><b>Workaround:</b> Launch through ActiveX.</p>
PRS-375534	<p><b>Symptom:</b> JSAM Stats value (Bytes count) is not getting displayed in IE - Activex.</p> <p><b>Condition:</b> After launching JSAM on Windows 10 endpoint.</p> <p><b>Workaround:</b> None</p>
PRS-375886	<p><b>Symptom:</b> JSAM launch failing for IE - JAVA.</p> <p><b>Condition:</b> JSAM launch fails with IE and JAVA combination on Windows 10 endpoint.</p> <p><b>Workaround:</b> Launch through ActiveX.</p>

## Fixed Issues in 9.0R3.2 Release

The following table lists Fixed issues in 9.0R3.2 release.

Problem Report Number	Summary
<b>Pulse Connect Secure</b>	
PRS- 371754	<b>Summary:</b> Existing TOTP users who have registered through the internal port are not able to log in from external port after upgrading to 9.0R3.
PRS- 371789	<b>Summary:</b> Program <i>procsd</i> recently failed event occurring continuously in 9.0R3 version after upgrading from 8.3R6.


## Fixed Issues in 9.0R3.1 Release

The following table lists Fixed issues in 9.0R3.1 release.

Problem Report Number	Summary
<b>Pulse Connect Secure</b>	
PRS-371258	<b>Summary:</b> Ensure all the Installer components are available on a fresh installation using Virtual Appliance (VA) image.

## New Features in 9.0R3 Release

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

Feature	Description
TOTP Enhancement	<p>This feature provides the following enhancements to the existing TOTP Server implementation.</p> <ul style="list-style-type: none"> <li>End-users will now have only one TOTP account to maintain, regardless of the number of auth. servers configured in PCS.</li> <li>Admins can now configure one PCS to contact another PCS for validating TOTP Secrets, thereby eliminating the need to sync the TOTP secrets across multiple devices.</li> <li>Admins can now export the TOTP user accounts from a TOTP Auth. Server Users Page and import onto to desired PCS devices.</li> <li>Admins can now automate the export of TOTP user accounts from one PCS and import onto another PCS through REST API.</li> </ul> <p> <b>CAUTION:</b> Pre-9.0R3 users with more than one TOTP account will get reset when the system software is upgraded to PCS 9.0R3 or later. In such case, users have to re-register with TOTP.</p>
MTU calculation enhancement through PMTU	By default, Pulse Desktop Client uses MTU 576 in case of missing TCP MSS value; this is as per the RFC guidelines. For customers who do not want the default behavior and would like to use 1400 MTU, Pulse Desktop Client provides an option to configure the same on Gateway. When this option is set, Pulse Desktop Client uses 1400 MTU when TCP MSS is missing.
Core License distribution from License Server	This feature introduces leasing of CORE licenses from the license server in order to ease the restriction on each PSA-V appliance requiring it to contact PCLS to install CORE license.
Named User License enhancement	This feature provides a named user licensing solution across clusters, sites and products.
Adaptive Authentication	This feature supports adaptive authentication based on the dynamic analysis over user device type and location.
Custom HTTP response headers for security	<p>This feature provides option to the administrator to enter a new custom HTTP header that will be added to the responses. The user should be able to specify:</p> <ol style="list-style-type: none"> <li>HTTP Header Name</li> <li>HTTP Header Value</li> </ol> <p>If the header is already present, the system does not overwrite it.</p>
HTML5 Enhancements	<p>The following enhancements are made to HTML5 Access feature:</p> <ol style="list-style-type: none"> <li>Support HMAC-SHA-256 with SSH</li> <li>Specify HTML5 session values using URL query-parameters</li> <li>Support for custom pages</li> <li>Open the bookmark in new window</li> <li>New page for prompting user credentials</li> <li>Keyboard is set to "Text Input" by default for mobile devices.</li> <li>Support for HTML5 Access session for TLSv1.1 and TLSv1.2 enabled backend devices.</li> </ol>
Decoupling of AAA Servers from Internal Interface	This feature allows user to choose communicating interface/ network for each authentication server independently.

Feature	Description
Launching HOB and JSAM using PSAL.	This feature provides PSAL support for launching the HOB applet and JSAM on Java 9 & 10.
Toggle for Smartcard + NLA	This feature allows to enable smart cards and NLA simultaneously.
Support default VLAN tagging in PSA-V clusters	Default VLAN ID is supported in the clustered environment.
REST API enhancements	Enhancements include: <ul style="list-style-type: none"> <li>• Export, import full configuration via REST</li> <li>• API to pull license state from server</li> <li>• API to fetch all groups available in a configured LDAP or AD authentication server</li> <li>• APIs to get active sessions, system information, leased client counts, configure device certificates</li> <li>• APIs to configure certificates based on CSR workflow</li> <li>• APIs to perform cluster operations</li> <li>• Realm-based admin login for REST APIs</li> </ul>
Option to accept cert revocation	This feature instructs Pulse Connect Secure to skip revocation check and accept end user certificates when either OCSP server or CDP server is not accessible over the network.
Upgrade to OpenSSL 1.0.2n	This feature automatically upgrades Pulse Connect Secure to OpenSSL version 1.0.2n when the system software is upgraded.
Prevent multiple session using DSID	PCS/PPS devices currently use the DSID as the session handler cookie, which is set in the browser in clientless mode or used by the clients to identify the sessions. Since DSID cookie cannot be moved to httponly cookie, a new cookie is created such DSDID and set with httponly attribute for that cookie along with the regular DSID cookie.
Support TLS V1/2 LDAPS	This feature provides both TLS V1/2 and Outbound SSL options Support for LDAP Authentication Server.
<b>Cloud Secure</b>	
Dashboard Drill-Down support	The Cloud Secure Reports feature provides details on Application Access, Device Compliance details, Device details and Role assignments. The Cloud Secure dashboard have option to drill down to the report page.
Multiple SP support with ADFS Federation & Bookmark with re-writer	This feature allows users to access multiple cloud services using bookmarks in ADFS deployments with re-writer functionality enabled.

## Fixed Issues in 9.0R3 Release

The following table lists Fixed issues in 9.0R3 release.

Problem Report Number	Summary
<b>Pulse Connect Secure</b>	
PRS-350416	<b>Summary:</b> WTS icon gets disappear from taskbar when the user minimizes the session while it is opened in full screen mode.
PRS-356762	<b>Summary:</b> After cluster split and rejoin, joining node takes leader ownership and updates the existing user session data.
PRS-359525	<b>Summary:</b> RCA for Virtual Appliance 8.3R2 frozen intermittently on KVM platform.
PRS-359677	<b>Summary:</b> System/Log-Monitoring: SNMP trap sent messages are not recorded in the events log for process crashes.
PRS-361192	<b>Summary:</b> Allow authentication bypass via incorrect XML canonicalization and DOM traversal (CVE-2018-0489).
PRS-361471	<b>Summary:</b> HTML5 Citrix resource session closed (due to inactivity) even though user active.
PRS-361576	<b>Summary:</b> TNCS Crash can be induced via OpenConnect.

PRS-361770 PRS-367109	<b>Summary:</b> Activesync fails when German Umlaut character present in username in email client.
PRS-362177	<b>Summary:</b> Need to remove "Admission Control Events/Messages" option from Log settings in PCS UI.
PRS-362305	<b>Summary:</b> Unable to add AV listed all products from 8.3RX.
PRS-362409	<b>Summary:</b> Error connecting to Windows 10 Terminal service from MacOS using HOB when Windows 10 has KB4088776 installed.
PRS-362578	<b>Summary:</b> SNMP counter value is giving wrong output for iveVPNTunnels:::0 count.
PRS-362958	<b>Summary:</b> HOB: Mac users cannot launch HOB bookmarks if Target server is configured with NLA Auth.
PRS-363070	<b>Summary:</b> Reverse Proxy: VPN server is not forwarding the HTTP OPTIONS reply/content data back to the client application.
PRS-363191	<b>Summary:</b> Navigation toolbar not working in IE in SAP NetWeaver (Kernel 749_Rel Patch 425).
PRS-363796	<b>Summary:</b> Add iOS 11.3.1 to OS Check.
PRS-364611	<b>Summary:</b> Add iOS 11.4 to OS Check.
PRS-366163	<b>Summary:</b> Add iOS 11.4.1 for OS Check.
PRS-368506	<b>Summary:</b> Add iOS 12 to OS Check.
PRS-364000	<b>Summary:</b> OpenSSL RSA Key generation algorithm is vulnerable to a cache timing side channel attack.
PRS-364153	<b>Summary:</b> User image is not loading while accessing the resource using Web rewrite.
PRS-364443	<b>Summary:</b> Core Access: Unable to view the articles in an Internal Web resource via Core Access.
PRS-368205	<b>Summary:</b> Core Access: Web page is not rendering completely.
PRS-368583	<b>Summary:</b> Core Access: Unable to navigate to the tabs in using rewrite.
PRS-369467	<b>Summary:</b> Core Access: Search Option does not show results via Core access.
PRS-369743	<b>Summary:</b> Core Access: Barcode option does not work via Core Access.
PRS-364454	<b>Summary:</b> RCA for the DHCP proxy process snapshot getting generated in PCS and users are impacted on the device in 8.3R4 version.
PRS-364699	<b>Summary:</b> File share access is not working with Virtual port-based source IP configured on the user role in 9.0R1 version.
PRS-364721 PRS-369102	<b>Summary:</b> Rewrite: partial rendering of HOME page and error thrown while accessing LOGIN page.
PRS-367219	<b>Summary:</b> Rewrite: Text editor in the website is not working via rewrite in IE11 browser only.
PRS-367739	<b>Summary:</b> Rewrite: Standard Browser Toolbar do not show up on backend application home page using Safari browser.
PRS-364726	<b>Summary:</b> JSAM is not able to launch when Citrix resource is created with web-interface template.
PRS-364921	<b>Summary:</b> High CPU usage and frequent fqdnac1 process failure after upgrading from 8.3R5 to 9.0R1.
PRS-365198	<b>Summary:</b> Host Checker failed connecting to 8.2Rx and 8.3R4, if 9.0R1 HC components installed.
PRS-365232	<b>Summary:</b> PSA 7000f Frequently reports power supplies have failed.
PRS-365388	<b>Summary:</b> Users are unable to sync mails on phone after upgrade to 8.3R4.
PRS-365813	<b>Summary:</b> Core file browsing "modified date" remains the same as "create date" after modifying the file.
PRS-365822	<b>Summary:</b> File share bookmark not working in 9.0R1 version.
PRS-366015	<b>Summary:</b> HTML5 connection not established when the backend accepts only TLSv1.1 or TLS 1.2.
PRS-366134	<b>Summary:</b> Machine tunnel does not re-establish until ethernet cable removed and reconnected after user log off.
PRS-366690	<b>Summary:</b> AAA: Enabling assertion encryption causes login failure (SHA1 only is supported for OAEP) when using SHA1 encryption.
PRS-366889	<b>Summary:</b> Inconsistent behavior with "Bookmark opens new window... / Open the bookmark in a new window" option for Web Bookmarks.
PRS-366928	<b>Summary:</b> High CPU, fqdnac1 process snapshot generated with user disconnection.
PRS-367626	<b>Summary:</b> Ghostscript remote code execution vulnerability.
PRS-368273	<b>Summary:</b> Double VLAN tags for VLAN virtual ports configured.

PRS-368607	<b>Summary:</b> Remote code execution vulnerability in ghostscript.
PRS-370136	<b>Summary:</b> Username and password are visible in URL field when you try to login resource page.
PRS-370309	<b>Summary:</b> Incremental leasing not occurring with MAX_LICENSED_USERS_REACHED.
<b>Cloud Secure</b>	
PAND-2305	<b>Summary:</b> Cloud Secure SSO doesn't work with Android Clients when FQDN based split tunneling is configured in PCS.
PRS-360958	<b>Summary:</b> IdP-initiated SSO to Cloud Services via rewriter will not work in AD FS federation deployments when bookmarks are configured to override RelayState, Subject Name Format and Subject Name.
PRS-361492	<b>Summary:</b> Redesigned end user pages are not shown with secondary authentication server.
PRS-362059	<b>Summary:</b> Editing of bookmarks is not supported with Cloud Secure Admin UX.
PRS-362334	<b>Summary:</b> In Cloud Secure UX, on adding the Bookmark with just name keeping other fields blank, the other details will be picked up from the peer SP.
PRS-366545	<b>Summary:</b> Pulse client and browser connection fails when CVE check rule is configured with ESAP 3.2.5 onwards.

## Known Issues in 9.0R3 Release

The following table lists known issues in 9.0R3 release.

Problem Report Number	Release Note
<b>Pulse Connect Secure</b>	
PRS-370210	<p><b>Symptom:</b> PSA300 crashes with Unable to mount /webserver partition</p> <p><b>Condition:</b> On performing Clear Config on PSA300 using serial console,</p> <p><b>Workaround:</b> None. Do not perform Clear Config after upgrade to 9.0R3 build.</p>
PCS-7857	<p><b>Symptom:</b> During End User LDAP Authentication, PCS does not send newly Configured SSL Ciphers in the Outbound Settings Page for some period of time.</p> <p><b>Condition:</b> When End User is authenticated using LDAP immediately after the Change of Security Mode or Encryption Strength in Outbound Settings page.</p> <p><b>Workaround:</b> This issue will not occur if End User is authenticated two minutes after the change of Outbound SSL Settings.</p>
PCS-8844	<p><b>Symptom:</b> Device anomaly not supported for the user logging in from mobile device.</p> <p><b>Condition:</b> User log in from mobile through PCS-Client.</p> <p><b>Workaround:</b> None</p>
PCS-9046	<p><b>Symptom:</b> Adaptive authentication will not kick-in even when there is change in location/IP due to session roaming.</p> <p><b>Conditions:</b> Currently session roaming is taking precedence when both Adaptive Authentication and Session Roaming is enabled.</p> <p><b>Workarounds:</b> None</p>
PCS-9532	<p><b>Symptom:</b> Location based anomaly not supported on AA cluster with LB configured in non-transparent mode.</p> <p><b>Condition:</b> When user logs into PCS deployed in AA cluster with load-balancer operating in non-transparent mode.</p> <p><b>Workaround:</b> None</p>
PCS-9565	<p><b>Symptom:</b> User logging in for the first time will be prompted for secondary authentication and this will not be considered as anomaly.</p> <p><b>Condition:</b> When user logs in from either browser or Pulse client, secondary authentication will be prompted.</p> <p><b>Workaround:</b> None. In subsequent login attempts from the browser or Pulse client, secondary authentication will be prompted only when an anomaly is detected.</p>



Problem Report Number	Release Note
PCS-9870	<p><b>Symptom:</b> Adaptive Authentication does not work for users logging in using their private IPs.</p> <p><b>Condition:</b> Adaptive Authentication is not applicable for users logging in using their private IPs.</p> <p><b>Workaround:</b> None</p>
PCS-10486	<p><b>Symptoms:</b></p> <ul style="list-style-type: none"> <li>- Admin might not be able to fetch the exact location i.e. city of the anomaly for some users.</li> <li>- Admin might notice anomaly type as null i.e. Anomaly () when system failed to detect location for user IPs. This results in secondary authentication for end user.</li> </ul> <p><b>Condition:</b> User login from some countries where the location may not be traced.</p> <p><b>Workaround:</b> None</p>
PCS-10517	<p><b>Symptom:</b> User prompted for secondary authentication every time even when the Adaptive Authentication is enabled whenever users log into PCS from public IPv6 address.</p> <p><b>Condition:</b> Users login to PCS from public IPv6 address.</p> <p><b>Workaround:</b> IPv4 based login.</p>
PRS-370825	<p><b>Symptom:</b> Secondary authentication will be skipped even when the user logs in from different mobile device.</p> <p><b>Conditions:</b> User logs in from same location but using another mobile device.</p> <p><b>Workaround:</b> None</p>
PRS-370829	<p><b>Symptom:</b></p> <ul style="list-style-type: none"> <li>- User prompted for secondary authentication even when the user logs in from same location or same device on PCS cluster.</li> <li>- Anomaly type anomaly() seen in user access log.</li> </ul> <p><b>Conditions:</b> User logs in to PCS cluster from public IP when the cluster is in the transition state and entering into stable state.</p> <p><b>Workaround:</b> User needs to enter secondary credentials.</p>
PRS-371123	<p><b>Symptom:</b> Adaptive authentication does not work for admin users.</p> <p><b>Conditions:</b> Secondary authentication will be prompted every time when Secondary Authentication is enabled along with Adaptive Authentication option on admin-realm.</p> <p><b>Workaround:</b> None</p>
PCS-8930	<p><b>Symptom:</b> End user will not be able to login on PCS which has authentication from AD.</p> <p><b>Condition:</b> While adding Active Directory groups</p> <p><b>Workaround:</b> None</p>
PCS-9043	<p><b>Symptom:</b> Cluster is not supported on PCS.</p> <p><b>Conditions:</b></p> <ul style="list-style-type: none"> <li>- Both the nodes are configured with default VLAN ID.</li> <li>- Internal port of both the nodes are in different subnets</li> </ul> <p><b>Workarounds:</b></p> <ul style="list-style-type: none"> <li>- Remove default VLAN ID if possible, and then re-create cluster or</li> <li>- Configure same default VLAN ID on both the nodes and form a cluster.</li> </ul>
PCS-9157	<p><b>Symptom:</b> Enabling Skip Revocation does not allow Cert Auth login when CRL download fail in NDcPP/JITC Security Mode.</p> <p><b>Condition:</b> In NDcPP/JITC Security Mode when a CA Certificate is enabled with Option 'Skip Revocation check when OCSP/CDP server is not available' and configured to use 'CRL with CDP(s) Specified in the Trusted Client CA' the Client Cert Auth will fail.</p> <p><b>Workaround:</b> In NDcPP/JITC Security Mode, for the skip revocation to work the CDP Responder Method should be one of the following:</p> <ol style="list-style-type: none"> <li>a) CDP(s) specified in client certificates or</li> <li>b) Manually configured CDP</li> </ol>

Problem Report Number	Release Note
PRS-366717	<p><b>Symptom:</b> Not able to change Client Revocation Status Checking Settings and Existing CRL Configuration is getting overwritten on Root CA if Auto Import Option is enabled and Sub CA's are imported automatically during Client Cert Authentication in NDcPP/JITC Mode.</p> <p><b>Condition:</b> In NDcPP/JITC Mode when following condition occur, Existing CRL Configuration is getting overwritten and 'Client Revocation Status Checking' Configuration cannot be changed to any settings only for Root CA.</p> <ul style="list-style-type: none"> <li>- Enable Auto Import Options for Trusted Client CAs</li> <li>- Import Root CA under Trusted Client CAs configured for to use CRL with Manual method</li> <li>- Do a certificate authentication using client certificate issued by a SUB CA</li> <li>- Root CA client revocation status checking configuration will be changed from Manual Method to 'CDP(s) specified in client certificates' automatically</li> <li>- Changing Revocation Status Checking Settings from CRL to OCSP will fail</li> </ul> <p><b>Workaround:</b> Follow the below steps to solve this issue:</p> <ol style="list-style-type: none"> <li>1) Delete all the CA Chain manually</li> <li>2) Import all the CA Chain manually</li> <li>3) Reconfigure the CAs with required Revocation and Responder Method</li> </ol>
PRS-366797	<p><b>Symptom:</b> In NDcPP/JITC Mode, the Auto Import Option Configuration under Trusted Client CAs doesn't apply on automatically Imported Sub CAs during Client Certificate authentication.</p> <p><b>Condition:</b> In NDcPP/JITC Mode when following condition occur, Automatically Imported Sub CA will not be configured with the configuration specified in Auto Import Option Page.</p> <ul style="list-style-type: none"> <li>- Enable Auto Import Options for Trusted Client CAs to Use OCSP Client certificate status checking.</li> <li>- Import Root CA under Trusted Client CAs configured for to use None.</li> <li>- Do a certificate authentication using client certificate issued by a SUB CA.</li> <li>- The client revocation status checking configuration for automatically imported Sub CAs will be configured to 'CDP(s) specified in client certificates' rather than what is configured in Auto Import Options.</li> </ul> <p><b>Workaround:</b> Following are some workarounds to solve this issue:</p> <ul style="list-style-type: none"> <li>• If auto import feature is needed during Client Cert Auth, Best Option is to Use FIPS OFF or FIPS ON Mode</li> <li>• If auto import feature configuration is needed during Client Cert Auth in NDcPP/JITC Mode then for all the CA Chain which is getting automatically imported during Client Cert Auth, Admin have to manually reconfigure the Revocation Settings that is required.</li> <li>• In NDcPP/JITC Mode If auto import feature is not a must then Admin can Manually Import the CA Chain and reconfigure automatic CRL Configuration to the required Revocation Method as needed.</li> </ul>
PCS-9550	<p><b>Symptom:</b> License Server Admin UI show up Virtual CPUs cores leasable to PSA and other hardware platform groups. Core Licenses are leasable only to PSA-V.</p> <p><b>Condition:</b> Installing Limited and Unlimited Core license on license server for leasing.</p> <p><b>Workaround:</b> None</p>
PCS-9606	<p><b>Symptom:</b> PCS pages may not render properly.</p> <p><b>Condition:</b> If CSP header is configured with 'src' related directives like script-src,style-src etc.</p> <p><b>Workaround:</b> Do not configure CSP with 'src' directives.</p>
PCS-10031	<p><b>Symptom:</b> In Authentication Servers page, Global setting of interface to use to contact authservers get reset to Internal Port.</p> <p><b>Condition:</b></p> <ul style="list-style-type: none"> <li>• PCS is a standalone node and the Global setting to reach authserver is set to External or Management port.</li> <li>• PCS tries to join a cluster.</li> </ul> <p><b>Workaround:</b> Reset the Global setting of interface to the desired Interface (Internal, External, or Management) after the node joins the cluster.</p>

Problem Report Number	Release Note
PCS-10568	<p><b>Symptom:</b> AAA decouple traffic for AD Server / Radius Server via IPv6 VLAN fails.</p> <p><b>Condition:</b></p> <ul style="list-style-type: none"> <li>• PCS is configured with IPv6 VLANs for Internal, External and Management Interfaces.</li> <li>• AAA decouple feature is enabled.</li> </ul> <p><b>Workaround:</b> None</p>
PRS-350976	<p><b>Symptom:</b> Random core dumps are generated for the webprocess.</p> <p><b>Condition:</b> For NC/WTS/CTS/JSAM/WSAM users, the session gets disconnected.</p> <p><b>Workaround:</b> Reconnect manually.</p>
PRS-355046	<p><b>Symptom:</b> New UI changes for the feature, HTML5 Access Enhancements, does not have localization for the languages such as Italian and Polish, resulting in the variable name being displayed instead.</p> <p><b>Condition:</b> If we have HTML5 access enabled for a user role, and the user browser selected is Italian/Polish in the language setting, then the user bookmark page does not appear correctly, and we see "I18N_HTML5_ACCESS_*" instead of corresponding localized strings.</p> <p><b>Workaround:</b> None</p>
PRS-356373	<p><b>Symptom:</b> XML file is not validated properly for named users while importing.</p> <p><b>Condition:</b> Named user table is removed if an attempt is made to import a malformed XML</p> <p><b>Workaround:</b> Export an existing named user table. Modify it before importing it. Ensure XML information is correct.</p>
PRS-357329	<p><b>Symptom:</b> From troubleshooting UI, ping6 to external resource fails if VLAN or external interface is selected as egress interface. The same works for non VLAN interface.</p> <p><b>Condition:</b> Right network interface is not chosen when VLAN is selected.</p> <p><b>Workaround:</b> None</p>
PRS-361501	<p><b>Symptom:</b> PCS uses Internal port IP instead of the assigned VLAN Virtual Port IP, after a VIP failover.</p> <p><b>Condition:</b> None</p> <p><b>Workaround:</b> None</p>
PRS-361989	<p><b>Symptom:</b> After upgrading from 8.3R3 to 9.0R1, Named User database gets cleared.</p> <p><b>Workaround:</b> The database auto-builds as users log in. So, it does not have to be upgraded release to release.</p>
PRS-365256	<p><b>Symptom:</b> DNS query for Active Directory Authentication Server will flow through selected Interface instead of Internal Port.</p> <p><b>Condition:</b> AAA decouple feature is enabled and other than Internal Interface is selected for Active Directory Authentication Server.</p> <p><b>Workaround:</b> None</p>
PRS-366813	<p><b>Symptom:</b> Pulse Host check failure message will not be displayed in Embedded browser with custom sign-in pages using Pulse client.</p> <p><b>Condition:</b> When host checker is enabled on role\realm with Pulse Embedded browser using custom sign-in pages.</p> <p><b>Workaround:</b> Administrator can access the host checker in the 'User Access Logs' page on the server.</p>
PRS-367024	<p><b>Symptom:</b> Authentication fails.</p> <p><b>Condition:</b> User authenticates to PCS and assigned realm is configured with Duo as primary and LDAP as secondary authentication server.</p> <p><b>Workaround:</b> None</p>
PRS-367628	<p><b>Symptom:</b> Unable to launch HOB or JSAM when a PSAL process runs at background or simultaneously on MAC.</p> <p><b>Condition:</b> When PSAL process is running, the behavior of macOS is to redirect subsequent custom URLs to this process and not launch new process.</p> <p><b>Workaround:</b> Close HOB before launching JSAM.</p>
PRS-368392	<p><b>Symptom:</b> Duo custom sign-in pages are not displayed.</p> <p><b>Condition:</b> User authenticates to PCS and assigned realm is configured with AD as primary and Duo as secondary authentication server.</p> <p><b>Workaround:</b> Use passcode-based Duo authentication.</p>

Problem Report Number	Release Note
PRS-368641	<p><b>Symptom:</b> Multiple bookmarks do not work after upgrading from 9.0R1 to 9.0R3 with blank relay state configured under multiple bookmarks.</p> <p><b>Condition:</b> 9.0R1 is configured without relay state under Third-Party IDP configurations.</p> <p><b>Workaround:</b> After upgrading to 9.0R3, add the relay state under Third-Party IDP configurations page.</p>
PRS-368689	<p><b>Symptom:</b> OS Check rule is not supported when trying to connect from 9.0R3 Pulse client to old PPS / PCS (9.0R2 / 9.0R3) server on macOS platform.</p> <p><b>Condition:</b> When OS check Host checker rule is evaluated with new Pulse client connecting to pre-9.0R3 PPS\PCS server.</p> <p><b>Workaround:</b> Pulse client (on MAC platform) and PPS server need to be of the same version for OS Check host checker policy to work as expected.</p>
PRS-368712	<p><b>Symptom:</b> Data displayed is inaccurate when custom filter is selected in Behavioral Analytics dashboard.</p> <p><b>Condition:</b> Selecting custom filters in Behavioral Analytics dashboard.</p> <p><b>Workaround:</b> Select 'To' date to be a day ahead than the desired date.</p>
PRS-368733	<p><b>Symptom:</b> Unable to resolve backend resources through hostname. Ping command throws Invalid IPv4 address/Hostname resolution failed.</p> <p><b>Condition:</b> PCS is configured with default VLAN on Internal Port. Administrator changes the internal IP of the PCS through Serial Console.</p> <p><b>Workaround:</b> Reset the VLAN ID through Serial Console and reconfigure VLAN ID.</p>
PRS-368967	<p><b>Symptom:</b> Host checker fails on Mac OS 10.14 Mojave endpoint when V3 SDK is selected.</p> <p><b>Condition:</b> When ESAP with V3 SDK is activated on the server.</p> <p><b>Workaround:</b> Administrator should activate ESAP with V4 SDK on PPS\PCS for Host check to work as expected.</p>
PRS-369319	<p><b>Symptom:</b> Meeting application does not launch automatically in Safari Mac platform.</p> <p><b>Condition:</b> When PSAL is removed by deleting the application directory and then re-installed.</p> <p><b>Workaround:</b> User has to click the "Join Meeting" button manually to launch the Meeting application.</p>
PRS-369445	<p><b>Symptom:</b> 64-bit PSAL invocation fails for the scenario where 64-bit JRE just got installed in the machine and there is old PSAL zombie process despite customer exiting all old HOB/JSAM sessions.</p> <p><b>Condition:</b> 64-bit PSAL is launched for supporting JRE-64.</p> <p><b>Workaround:</b> Open TaskManager. kill PSAL process "PulseApplicationLauncher" and try PSAL invocation again.</p>
PRS-369563	<p><b>Symptom:</b> On RS5 client, WSAM behavior is not consistent, i.e. at times when WSAM is launched, the traffic for the configured resources is not SAMized.</p> <p><b>Condition:</b> Resource access with WSAM on a RS5 Client.</p> <p><b>Workaround:</b> None, use Pulse SAM.</p>
PRS-370181	<p><b>Symptom:</b> Logins do not work immediately after upgrade.</p> <p><b>Condition:</b> An issue in syncing the session database during upgrade results in some sessions not resuming properly.</p> <p><b>Workaround:</b> Use console option 21 to remove all sessions or reboot the cluster.</p>
PRS-370222	<p><b>Symptom:</b> PCLS analytics reporting needs to be enabled from the active node of the cluster.</p> <p><b>Conditions:</b> The license key for which the authentication code is issued is on the active node.</p> <ul style="list-style-type: none"> <li>If the registration is successful from the active, the analytics cannot resume from passive.</li> </ul> <p><b>Workaround:</b> None.</p>
PRS-370413	<p><b>Symptom:</b> The Device Certificate mapping of Internal/External VIP for AP Cluster should be removed on deleting and recreating the cluster using default VLANs.</p> <p><b>Conditions:</b> When Existing Cluster having Device Certificate mapped to VIP IP is deleted and Recreated by enabling default VLAN, the Cluster External/Internal VIP Mapping still shows in Device Certificate.</p> <p><b>Workaround:</b> Remove the Cluster VIP Mapping from Device Certificate before deleting and recreating the Cluster with default VLAN.</p>

Problem Report Number	Release Note
PRS-370433	<p><b>Symptom:</b> PCS does not prompt for optional parameters (VLAN ID, Secondary DNS, WINS Server).</p> <p><b>Conditions:</b> On a fresh deploy of PSA-V from OVF.</p> <ul style="list-style-type: none"> <li>After performing a clear config.</li> </ul> <p><b>Workaround:</b> Configure using Admin UI.</p>
PRS-370479	<p><b>Symptom:</b> Rewriter page response time degradation was observed in 9.0R3 on PSA7000.</p> <p><b>Conditions:</b> When the number of SSL connections handled by PCS is very high.</p> <p><b>Workaround:</b> None. The performance degradation will occur only during SSL connection establishment and there will be no impact to data throughput.</p>
PRS-370612	<p><b>Symptom:</b> Support for new Java version 11 is not provided in PSAL.</p> <p><b>Workaround:</b> None</p>
PRS-370662	<p><b>Symptom:</b> PCS fails to connect to CDP Server using HTTPS CRL URL via Proxy.</p> <p><b>Conditions:</b> When Trusted Client CAs are configured to send CRL traffic via Proxy with HTTPS URL, Client Cert Auth will fail if Skip Revocation check in CA is not enabled.</p> <p><b>Workaround:</b> Instead of using HTTPS OCSP URL, Configure HTTP OCSP URL which will not show this issue.</p>
PRS-370668	<p><b>Symptom:</b> PCS takes 4-5 seconds more than the Configured OCSP Timeout to detect OCSP Responder failure and perform Skip Revocation if OCSP URL is HTTPS.</p> <p><b>Conditions:</b> When CA is Configured for OCSP Client Revocation Status Checking with HTTPS URL then PCS takes 4-5 seconds more time than the Configured OCSP Timeout to detect OCSP Responder failure and perform Skip Revocation.</p> <p><b>Workaround:</b> Instead of using HTTPS OCSP URL, Configure HTTP OCSP URL which will not show this issue.</p>
PRS-370987	<p><b>Symptom:</b> IKEv2 fails to connect to Cluster VIP interface if default VLAN is enabled.</p> <p><b>Conditions:</b> In AP Cluster enabled with default VLAN, IKEv2 Client will fail to connect.</p> <p><b>Workaround:</b> Do not enable default VLAN for AP Cluster to connect using IKEv2 VPN.</p> <ul style="list-style-type: none"> <li>Use AA Cluster.</li> </ul>
<b>Cloud Secure</b>	
PRS-368086	<p><b>Symptom:</b> Device ID is not displayed for not-assessed devices in Cloud Secure report.</p> <p><b>Condition:</b> When accessing applications from devices without compliance checks.</p> <p><b>Workaround:</b> Enable compliance check when accessing applications.</p>
PRS-368628	<p><b>Symptom:</b> Upgrading from older builds to 9.0R3 builds with ECP data displays the Username as Unknown in Cloud Secure reports.</p> <p><b>Condition:</b> ECP data is captured in Cloud Secure dashboard in older release and then upgraded.</p> <p><b>Workaround:</b> None</p>
PRS-368816	<p><b>Symptom:</b> Cloud Secure dashboard does not capture data when ADFS is configured as Third-Party IDP with re-writer enabled.</p> <p><b>Condition:</b> ADFS configured as Third-Party IDP with re-writer enabled.</p> <p><b>Workaround:</b> None</p>
PRS-368915	<p><b>Symptom:</b> Redesigned Cloud Secure End User Page is not shown when accessing Outlook Application from Windows.</p> <p><b>Condition:</b> When accessing Outlook Applications from Windows machine.</p> <p><b>Workaround:</b> None</p>
<b>Cloud Application Visibility (CAV)</b>	
PRS-369277	<p><b>Symptom:</b> CAV will not work with PSAM.</p> <p><b>Condition:</b> When both PSAM and CAV are enabled for the same role.</p> <p><b>Workaround:</b> None</p>
PRS-369279	<p><b>Symptom:</b> Lockdown is not working properly if CAV policies are configured.</p> <p><b>Condition:</b> Intermittently we observed that enabling CAV+ lockdown is causing issue at Pulse Client.</p> <p><b>Workaround:</b> None</p>

Problem Report Number	Release Note
PRS-369891	<p><b>Symptom:</b> Authentication token fetching is failing under NATted environment on Pulse Client for CAV policies update.</p> <p><b>Condition:</b> When PCS has configured behind NAT device.</p> <p><b>Workaround:</b> None</p>
PRS-370123	<p><b>Symptom:</b> DNS resolution keeps failing after CAV is re-enabled at user role level.</p> <p><b>Condition:</b> If added user role has been deleted from the CAV policies.</p> <p><b>Workaround:</b> None</p>
PRS-370237	<p><b>Symptom:</b> CAV policy updates are not sending to PPS if CAV DB is updated with PCS IP, even if a new session to PPS has established.</p> <p><b>Condition:</b> If CAV DB at client side is updated with PCS IP and then the end-user establishes L2/UAC L3 connection with CAV enabled PPS.</p> <p><b>Workaround:</b> None</p>
PRS-370249	<p><b>Symptom:</b> CAV policies are not applied when endpoints establish dot1x connection with a switch/access point.</p> <p><b>Condition:</b> Authenticator is a third-party device and is configured to use PPS as authenticating server.</p> <p><b>Workaround:</b> None</p>
PRS-370268	<p><b>Symptom:</b> CAV fails to configure proxy on endpoint, when Juniper SRX is configured as Infranet Enforcer for a resource.</p> <p><b>Condition:</b> Juniper SRX is configured as Infranet Enforcer.</p> <p><b>Workaround:</b> None</p>

## New Features in 9.0R2 Release

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

Feature	Description
REST API enhancement	REST API access for an administrator user can be enabled during initial configuration and while creating a new administrator user in admin console.
UPN, domain\user formats with LDAP Cred. Provider	Credential Provider with LDAP(S) now supports both UPN and domain\user (pre-windows 2000 login) formats.
Option to toggle auto populate domain information	A new option is provided to prevent the rewriter from pre-populating the domain name in the intermediation page when using NTLM authentication. Useful in multi-domain environments for the user to provide domain information themselves, when it is different from the target server domain.
Third Party Applications: (New versions)	<p>VMWare 7.4 / 7.5</p> <p>Lotus iNotes 9.0 (using filters. See <a href="#">KB43863 - Supportability of Lotus Notes 9.0 through Rewrite</a>)</p> <p>RSA Authentication Manager 8.3</p> <p>Windows RS4</p>
Cloud Application Visibility (CAV)	<p>Cloud Application Visibility enables you to secure and manage cloud applications. It also provides visibility of the cloud application used by the user and allows administrators to set granular access and use policies to monitor the Cloud Application usage in real time.</p> <p>This is a licensed feature and it requires Cloud Secure license to be enabled.</p>
Host Checker MacOS 64-bit support	Added HC support for Mac OS 64-bit applications.
Location Awareness for On-premise users on Android	This feature allows suppressing of VPN connections based on the user location. Location awareness rules are pushed along with the Wi-Fi profile when the user connects to the SSID. This enables On-Premise users to get access to cloud applications without establishing a VPN connection.
SHA256 support	With the implementation of SHA256 algorithm support in PCS, the SAML responses can be signed with both SHA1 or SHA256-based on the service provider configurations.
Licensing	Subscription based licenses are added to existing Cloud Secure Licensing.

# Noteworthy Changes

SHA1 FIPS support is provided in this release. SHA1 is only used for digital signature generation, which is specifically allowed by NIST protocol-specific guidance.

## Fixed Issues in 9.0R2 Release

The following table lists Fixed issues in 9.0R2 release.

Problem Report Number	Summary
PRS-366677	<b>Summary:</b> Web cores found in both nodes of A-A cluster that went down and they occurred somewhat earlier than the incident.
PRS-366275	<b>Summary:</b> The PCS platforms now use a fully 64-bit kernel.
PRS-366259	<b>Summary:</b> Cloud Secure configuration is available while using the Classic UI.
PRS-364920	<b>Summary:</b> High CPU usage and frequent fqdncl process failure occur when using hostname-based configuration for VPN Tunneling.
PRS-366027	<b>Summary:</b> P-O-P:Policy trace is not able to filter the logs for Browser based logs since we are not printing the username for Auth request and response.
PRS-365970	<b>Summary:</b> DNS lookup may not fallback to secondary if the primary DNS server does not respond.
PRS-365791	<b>Summary:</b> Exception list rule for Always-on VPN may not save properly when using the configuration wizard.
PRS-365622	<b>Summary:</b> dsunity process crash may be observed on the PCS/PPS when connecting to a Pulse One cluster and the active Pulse One appliance fails over to the passive node.
PRS-365347	<b>Summary:</b> Clicking on any option from Cloud Secure > Cloud Secure Configuration > Basic > SAML Settings, while inside any of the Basic settings tab lands the user to application page.
PRS-365336	<b>Summary:</b> When upgrading from 9.0R1 build to 9.0R2, Cloud Secure dashboard displays dummy dashboard and not the original one with license warning.
PRS-365105	<b>Summary:</b> When using XML export, HTML escape codes are shown rather than the rendered value.
PRS-365076	<b>Summary:</b> Cloud Secure configuration is visible on license servers (and it should not be present).
PRS-364957	<b>Summary:</b> PUT/POST Operation to the IVE through REST API fails with "Internal server error" message.
PRS-364863	<b>Summary:</b> The Always-on configuration wizard may fail to create lockdown exception rules.
PRS-364848	<b>Summary:</b> The exported pre-configuration file may not contain all the lockdown exception rules.
PRS-360592	<b>Summary:</b> Duplicating multiple roles is not supported.
PRS-361991	<b>Summary:</b> Frequent invalid write in rewrite-server will cause crash with a segmentation fault.
PRS-364716	<b>Summary:</b> PCS-based remote profiler may not properly update the PPS/stand-alone profiler.
PRS-364691	<b>Summary:</b> Universal XML export may fail to import.
PRS-364122	<b>Summary:</b> Machine certificate Host Checker validation fails on TPM-enabled machines.
PRS-364501	<b>Summary:</b> Change default authentication method to public key for SSH configuration.
PRS-364470	<b>Summary:</b> After editing the Signature Algorithm option via Cloud Secure UX, changes are not getting into effect.
PRS-364440	<b>Summary:</b> Username may be shown as "System" in the user access log when using SAML-based authentication.
PRS-364345	<b>Summary:</b> Legacy virtual appliances (pre-8.2 OVF deployments) may fail to boot after increasing RAM or CPU (see KB40898 for more details).
PRS-357094	<b>Summary:</b> Provide SHA-1 FIPS support in 9.0R2.
PRS-364022	<b>Summary:</b> Error message is adding multiple caret ^ symbol in it.
PRS-363694	<b>Summary:</b> Pulse client login may fail on new realms.
PRS-362640	<b>Summary:</b> parent.location.href may fail to be rewritten correctly.



PRS-363413	<b>Summary:</b> Importing an XML file containing VPN Tunneling IPv4 ACL resources may fail if the port list contains a range (-) or comma-separated list.
PRS-363869	<b>Summary:</b> Browsing a file share root (\\server\ ) file bookmark fails when SSO is configured.
PRS-362957	<b>Summary:</b> Premier Java RDP (HOB) bookmarks fail to launch when NLA is enabled on the target system.
PRS-362394	<b>Summary:</b> DNS services may fail when Pulse and CrowdStrike are installed on the same system.
PRS-359021	<b>Summary:</b> Custom start page may not load when using the auto-launch option for Pulse.
PRS-358714	<b>Summary:</b> A PCS with multiple VLANs and virtual ports on each VLAN may become unreachable under heavy VPN tunnel usage.
PRS-363736	<b>Summary:</b> Cloud Secure configuration pages may be available without the Cloud Secure license installed.
PRS-363069	<b>Summary:</b> Authorization only URL does not keep HTTP OPTIONS method in reply to external users.
PRS-359676	<b>Summary:</b> System/Log-Monitoring: SNMP trap sent messages are not recorded in the events log for process crashes.
PRS-356761	<b>Summary:</b> IF-MAP session data/IP address is not updated properly for VPN Tunneling users during cluster failover and recovery.
PRS-361470	<b>Summary:</b> Users sessions may be closed due to inactivity incorrectly when using the HTML5 Citrix client.
PRS-362304	<b>Summary:</b> A Host Checker policy configured for specific products AND then choosing all products from the vendor will not save. Instead an error message is displayed "Please select one of the products or uncheck "Require specific product"".
PRS-362280	<b>Summary:</b> Critical "ERR20645" Msg="Watchdog: process /sbin/64/iptables-restore has exceeded number of file descriptors."
PRS-360268	<b>Summary:</b> AAAA requests are sent when IPv6 is not enabled. If the DNS server does not support AAAA records, the resource cannot be reached.
PRS-361769	<b>Summary:</b> Activesync fails when German Umlaut character present in username.
PRS-361673	<b>Summary:</b> The PCS may become disconnected from the domain when using standard mode AD/NT server instances under heavy load.
PRS-359407	<b>Summary:</b> When wireless suppression and location awareness are enabled, DNS settings may not be restored properly when switching from ethernet to Wi-Fi.
PRS-350415	<b>Summary:</b> Windows Terminal Service icon disappears from the taskbar when the window is minimized from full screen.
PRS-363544	<b>Summary:</b> Users may not be able to access resources through IE when a proxy is configured in association with the Pulse VPN tunnel.
PRS-363398	<b>Summary:</b> NDcPP restrictions are improperly applied when enabling FIPS mode (causing appliance to become unreachable).
PRS-362577	<b>Summary:</b> SNMP response for iveVPNTunnels query contains invalid data.
PRS-357377	<b>Summary:</b> NLASVC does not restart on Windows 10, causing mapped drives to not load when using Credential Provider-based connections.
PRS-362159	<b>Summary:</b> DNS client service fails to restart when launching Pulse on Windows 10 Redstone 3 and later.
PRS-361912	<b>Summary:</b> DNS client service fails to restart when launching Network Connect on Windows 10 Redstone 3 and later.
PRS-363019	<b>Summary:</b> Message for not allowing any attempt to remove a good disk HDD1 when disk HDD2 has gone bad is not printed.
PRS-362386	<b>Summary:</b> Importing a user.cfg may result in an invalid warning related to cluster IPs. Please note, no changes are made to appliance IPs when importing user.cfg.
PRS-361311	<b>Summary:</b> PSA7000-V registered to Pulse One is incorrectly reported as a VA-SPE.
PRS-360860	<b>Summary:</b> User sessions may not be deleted at session timeout if a user session was created during cluster failover.
PRS-358581	<b>Summary:</b> Policy trace may show login data for users on other realms when SAML authentication is enabled.
PRS-357051	<b>Summary:</b> Pulse Secure Application Launcher is inconsistently used in application launch dialogs.
PRS-362176	<b>Summary:</b> "Admission Control Messages" under "event and user access" log settings are removed.



# Known Issues in 9.0R2 Release

The following table lists known issues in 9.0R2 release.

Problem Report Number	Release Note
<b>Cloud Secure</b>	
PRS-366406	<p><b>Symptom:</b> Location awareness with On-demand VPN does not work in Android 8.0 Oreo devices.</p> <p><b>Conditions:</b> The android device used is running on 8.0 Oreo OS.</p> <p><b>Workaround:</b> None.</p>
PRS-366451	<p><b>Symptom:</b> On upgrade from 9.0r1 (having cloud secure license) to 9.0r2, other licenses do not work.</p> <p><b>Conditions:</b> 9.0r1 build has cloud secure license (such as PS-CS-LIC installed).</p> <p><b>Workaround:</b> Delete the CS license after upgrade to 9.0r2 and add again.</p>
<b>Cloud Application Visibility (CAV)</b>	
PRS-365350	<p><b>Symptom:</b> The user can disable CAV proxy setting in Firefox browser.</p> <p><b>Condition:</b> When the user tries to modify CAV proxy settings in Firefox browser.</p> <p><b>Workaround:</b> The Administrator must block users to modify proxy settings in Firefox browser.</p>
PRS-366171	<p><b>Symptom:</b> CAV proxy exceptions list is not set based on the connecting server when connection is transferred from PPS to PCS.</p> <p><b>Condition:</b> When the user connection changes from PPS to PCS with CAV enabled role.</p> <p><b>Workaround:</b> By default, when connection is transferred from PPS to PCS with default proxy options configured in VPN Connection Profile (No Proxy), then Pulse Client creates a Proxy Auto Config (PAC) file with old exclusions (that is, PPS). To avoid this use "Preserve Client Side" proxy option, in VPN connection profile.</p>
PRS-366210	<p><b>Symptom:</b> Pulse SAM stops sending traffic to PCS when CAV is enabled for a user role.</p> <p><b>Condition:</b> When user logs in to PPS/PCS using Pulse Client with user role enabled on Pulse SAM and CAV.</p> <p><b>Workaround:</b> CAV role should not be enabled for Pulse SAM enabled user role.</p>
PRS-365717	<p><b>Symptom:</b> Cloud Application Visibility is not supported when Client/Server proxy is configured.</p> <p><b>Condition:</b> If the admin configures a VPN Tunneling Connection profile with a proxy, the Pulse Desktop Client creates a PAC file with the proxy server(s) defined in the profile (bypassing the CAV proxy).</p> <p><b>Workaround:</b> NA</p>
	<p><b>Condition:</b> If PAC file is configured on the user's Windows machine, then CAV cannot perform proxy chaining.</p> <p><b>Workaround:</b> NA</p>
PRS-365513	<p><b>Condition:</b> If a user's Windows machine has a proxy configured (not configured using VPN Connection Profile), then CAV performs proxy chaining and intercepts the traffic.</p> <p><b>Workaround:</b> Administrators must configure "preserve client proxy settings" option in PCS VPN Connection Profile.</p>
	<p><b>Symptom:</b> Cloud Application Visibility is enabled for all users rather than a per-user basis when there are multiple accounts on the endpoint.</p> <p><b>Condition:</b> When multiple users on same Windows machine access applications.</p> <p><b>Workaround:</b> Users need to login individually to CAV using the Pulse client to force a new entry for tracking.</p>
PRS-367403	<p><b>Symptom:</b> With Java 10, Pulse Collaboration fails to launch in MAC OS High Sierra with version conflict error.</p> <p><b>Condition:</b> Trying to launch Pulse Collaboration on Mac OS with Java 10.</p> <p><b>Workaround:</b> Use Java 8</p>

Problem Report Number	Release Note
PRS-366325	<p><b>Symptom:</b> Active user session shows endpoint behind NAT when the connection is transferred from PCS to PPS for the first time.</p> <p><b>Condition:</b> User has connected to PCS first and then established a connection with PPS.</p> <p><b>Workaround:</b> User must disconnect the session and reconnect while moving from PCS to PPS for the first time.</p>

## New Features in 9.0R1 Release

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

Feature	Description
License Server HA	High Availability Support for License Server on PSA, VMware ESXi Hyper-V and KVM (Only Active/Passive Cluster supported)
VA Platform licensing and VA Platform Clustering (Part 2)	With Cluster support on Hyper-V and KVM, High availability and scalability is achieved with AA and AP cluster.
SMB v2/v3 with File Browsing	The file browsing module has been enhanced to support the SMB v2 and v3 protocols. Microsoft has deprecated SMB v1 and has been urging the community to move to v2/v3.
JAVA	<ol style="list-style-type: none"> <li>In this release support to launch clients using JAVA 9 (64-Bit) has been added. Now clients like JSAM, Hob Applets, STA, etc can run on using JAVA 9.</li> <li>In this release JAVA compiler has been modified from 1.1 to 1.6 and changed the Obfuscator from RetroGuard to ProGuard.</li> </ol> <p><b>Note:</b> On IE, the <b>Enable 64-bit processes for Enhanced Protection Mode</b> must be enabled to support 64-Bit.</p>
PCS hosted in AWS	<p>Amazon Web Service (AWS) is a cloud computing platform and infrastructure, created by Amazon, for building, deploying and managing applications and services through a global network of Amazon-managed data centers. It provides both PaaS and IaaS services.</p> <p>As part of this release we will support deploying Pulse Connect Secure in Amazon's AWS Cloud.</p>
Support for VDI 7.2 and 7.3.1	<p>Qualified support for VDI Profiles on VMWare Horizon Agent</p> <ol style="list-style-type: none"> <li>VMWare Horizon Agent 7.2</li> <li>VMWare Horizon Agent 7.3.1</li> </ol>
Embedded Browser (Captive Portal, Host Check & SAML flows)	Pulse desktop Client will use the embedded browser for SAML authentication, instead of external browser.
Minimum Client Version Enforcement - Server side.	<p>Pulse Desktop Client will now send an error message to the end user and will not prompt the user to upgrade their client.</p> <p>The Pulse Secure Client will not support Minimum Client Enforcement for Linux and PPS.</p>
Rewriter enhancements	<p>Earlier, the URL Rewriting technology (clientless access) sometimes struggled with modern applications that generate URLs dynamically on the client side using new JavaScript frameworks or constructs. JavaScript has also received a new version ECMA 6 that had new constructs for URL generation that were not being handled. Due to these issues, some modern applications would either not be compatible with the rewriter or require a significant number of custom filters. These issues have been addressed with the rewriter enhancements in this release.</p> <p><b>Note:</b> Please review <a href="http://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB43742">http://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB43742</a> before upgrading to 9.0R1 without fail.</p>
Proxy for PCLS Communication	This feature provides communication between VA-SPEs with Pulse Cloud Licensing Server (PCLS) and Pulse One through a configured proxy server. A new tab called Proxy Server has been added in the Network Settings to configure the proxy.

Feature	Description
JITC Certification	<ul style="list-style-type: none"> <li>• Log Support for detection and prevention of SMURF/SYN Flood/SSL Replay Attack.</li> <li>• Disable ICMPv6 echo response for multicast echo request.</li> <li>• Disable ICMPv6 destination unreachable response.</li> <li>• DSCP Support.</li> <li>• Password Strengthening.</li> <li>• Notification for unsuccessful admin login attempts.</li> <li>• Re-authentication of admin users.</li> <li>• Notification on admin status change</li> </ul>
NDcPP Certification	<ul style="list-style-type: none"> <li>• When NDcPP option is enabled, only NDcPP allowed crypto algorithms are allowed.</li> <li>• Device/Client Auth certificate 3072 bit key length support.</li> <li>• Not allowing Import of Device/Client Auth Certificate if Respective CAs are not in Trusted Stores.</li> <li>• Not allowing Importing of Device Certificate without Server Authentication EKU (Extended Key Usage).</li> <li>• Device/Client Auth/CA certificate revocation check during Certificate Import</li> <li>• Syslog/Pulse one server certificate revocation check during TLS connection establishment.</li> <li>• Not Allowing 1024 bit Public Key Length Server Certificate from Syslog/Pulse one server during TLS connection.</li> <li>• Many other NDcPP Compliant Support mentioned in <a href="https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10821">https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10821</a> for PCS and <a href="https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10785">https://www.niap-ccevs.org/Product/Compliant.cfm?PID=10785</a> for PPS</li> </ul>
PCS Azure 2vCPUs and 8vCPUs Support	Support PCS deployment in Azure with 2 CPUs and 8 CPUs. Qualified "standard_ds2_v2" for 2 CPUs and "standard_ds4_v2" for 8 CPUs.
PCS Azure 2 NIC Support	Support PCS deployment in Azure with 2 Interface (Internal and External). Qualified "standard_d2_v2" for 2 NIC PCS model.
FQDN based split tunneling Resources	PCS administrator will be able to specify the resources as FQDNs along with IPv4 and IPv6 resources.
HTML5 ClearType font smoothing support	ClearType is font-smoothing technology built into Windows to help make text more readable on LCD monitors. It is designed to smooth the fonts on the screen with subpixel rendering so that they are more readable on LCD displays. Prior to this release, HTML5 access did not support ClearType and font smoothing.
WAN Clustering	Active-Active Config Only Cluster Support for WAN Networks.
Clustering over high latency networks	Configuration sync over high latency networks has been added to the clustering framework, supporting up to 100 ms latencies. Session sync and Connection Profile using Global Static IP Pool are not supported over high latency networks.
Host Checker Enhancements	<ul style="list-style-type: none"> <li>• Support for Patch Management rule configuration on Mac OS platform.</li> <li>• Support for OS check type rule configuration on Mac OS platform.</li> <li>• Support for configuring Common Vulnerability and Exposure (CVE) Check Rules on Windows platform.</li> <li>• Host Checker supports the caching of previous HC evaluation and performs the HC evaluation only after a defined amount of time (For example, 1 week) instead of every time the user connects.</li> </ul>

Feature	Description
Cloud Secure	<p>The Pulse Cloud Secure technology provides seamless and secure access to cloud-based applications. With this PCS release, the following capabilities are available as part of the Cloud Secure:</p> <ul style="list-style-type: none"> <li>Redesigned End User Experience- End user pages are redesigned to enhance the overall login experience when accessing cloud services either through browser or native applications. This feature currently redesigns widely used pages like Login, Host Checker pages, Host Checker instructions and SAML Error pages.</li> <li>Licensing support for Cloud Secure- Cloud Secure requires license-based activation starting with Release 9.0R1. New license SKUs are added for enabling Cloud Secure features.</li> <li>Simplified Cloud Secure configurations for existing users- New option is added on Cloud Secure configuration page to re-use the existing PCS configuration. User's needs to provide the required SAML settings (if not configured already) for enabling Cloud Secure functionality.</li> <li>AD FS Impersonation-support for SP Initiated Access- Allows remote users to access Office 365 services using PCS as Identity Provider instead of authenticating to On-Premise AD FS server.</li> <li>Multiple SP support with AD FS Federation and Bookmark- Allows users to access multiple cloud services using bookmarks in ADFS deployments.</li> <li>Location Awareness for On-premise users on iOS- Allows suppressing of VPN connections based on the user location. Location awareness rules are pushed along with the Wi-Fi profile when the user connects to the SSID. This enables On-Premise users to get access to cloud applications without establishing a VPN connection.</li> <li>Cloud Secure Single Sign-On (SSO) with On-Demand VPN on Android platform- Allows VPN connection to be triggered dynamically on accessing applications managed by Pulse Workspace (PWS). Cloud Secure re-uses the VPN session information for providing SSO access to applications.</li> </ul>

## Fixed Issues in 9.0R1 Release

The following table lists Fixed issues in 9.0R1 release.

Problem Report Number	Release Note
PRS-351673	<b>Summary:</b> VDI: Connection server is not updated on Windows 7 machines with VMware horizon view client 4.1.0
PRS-351574	<b>Summary:</b> NC: After 90 seconds of tunnel launch, resource access fail for about 60 seconds and recover automatically.
PRS-347333	<b>Summary:</b> UDP resource is not accessible if the UDP packets get fragmented.
PRS-351193	<b>Summary:</b> Seeing dsagentd process restart in a VA-SPE after ikev2 eap-tls client connection and sending ping traffic for some time.
PRS-349783	<b>Summary:</b> Package upload fails on VA due to 100% space utilized in rootfs
PRS-345418	<b>Summary:</b> VA-SPE(VMWare) running 8.2R4 fails during boot-up after adding 2GB memory and adding CPU cores.
PRS-349140	<b>Summary:</b> When iOS user clicks the attendee URL present in the meeting invite mail, the PC client application comes in front end for few seconds and then gets invisible.
PRS-350525	<b>Summary:</b> Inaccurate statistics sent to accounting server when layer 3 VPN is formed with Pulse client.
PRS-356068	<b>Summary:</b> Enabling FIPS Mode Selects SSLv3 Option in Outbound Settings Page in one Particular Scenario.
PRS-356307	<b>Summary:</b> MD5 & SHA256 checksum evaluation fails intermittently for 64-bit custom: process policy.
PCS-5094	<b>Summary:</b> Pulse is prompting for password during session failover in AP Cluster with ESP mode.
PRS-356476	<b>Summary:</b> Max concurrent users is restricted to 2, even after leasing licenses from license server.
PCS-6479	<b>Summary:</b> VA-SPE: Max Concurrent Users should be based on no of allocated cores.
PRS-355916	<b>Summary:</b> PCS login page redirects to download Activex Plugin when no pulse components are installed on the PC.

Problem Report Number	Release Note
PRS-355058	<b>Summary:</b> Certificate Authentication doesn't work with Pulse Client available in App store.
PRS-352949	<b>Summary:</b> Office365 page is not loading properly after being rewritten by rewriter.
PRS-356722	<b>Summary:</b> While configuring Cloud Secure with New UX, you might encounter some UI issues / validation errors.

## Known Issues in 9.0R1 Release

The following table lists Known issues in 9.0R1 release.

Problem Report Number	Release Note
PRS-359356	<b>Symptom:</b> Upgrading PCS on Microsoft Azure or Amazon AWS Cloud will take 90-120 minutes. <b>Condition:</b> PCS has to deploy on Microsoft Azure or Amazon AWS Cloud. <b>Workaround:</b> None
PRS-363413	<b>Symptom:</b> XML import, REST API, selected pushconfig, Pulse One config distribution and DMI might fail. <b>Condition:</b> The issue arises when L3 ACLs are configured with IPv4 or IPv6 resources. <b>Workaround:</b> Use binary import for importing the configurations.
PCS-7391	<b>Symptom:</b> DFS share will not be listed when the user of current DFS is different from the linked one. <b>Condition:</b> Try to list/access the DFS share that do not have access with the given user. <b>Workaround:</b> Ask the admin to create the bookmark for actual share which linked via DFS bookmark.
PRS-355047	<b>Symptom:</b> The new fields "Performance Flags" in HTML5 Access bookmark doesn't support localization in the end user page. <b>Condition:</b> If the user selects any language other than English then instead of the local language being displayed, it displays i18N. <b>Workaround:</b> To get rid of this issue, the user must set the language of the client machine English and access the PCS end user page.
PCS-7398	<b>Symptom:</b> Unable to access the root shares with pre-defined credentials given in the SSO of auto-policy. <b>Condition:</b> Try to access the root shares with SSO configured with the resources. <b>Workaround:</b> Create the bookmark for the sub-folders with SSO credentials instead of the root share.
PCS-7403	<b>Symptom:</b> Domain detail is not auto populating when SMB1 is disabled on backend servers. <b>Condition:</b> SMB1 is disabled on backend server. <b>Workaround:</b> Enable SMB1 on the back-end server to auto-populate the domain details.
PRS-362240	<b>Symptom:</b> Applications are not launching via PSAL from Citrix Storefront. <b>Condition:</b> When client detects citrix receiver. <b>Workaround:</b> Pass the Cookie: CtxsClientDetectionDone=true by adding the header like below in the resource profile.
PRS-362214	<b>Symptom:</b> Swap Memory Utilization in the cockpit graph increases then remain constant and never comes down in cluster. <b>Condition:</b> Unknown <b>Workaround:</b> None
PCS-7048	<b>Symptom:</b> On adding a Cluster Wide Network Route when Cluster is in Particular State on Active-Active Config-Only WAN Cluster, any of the Node might lose cluster connectivity and web connectivity. <b>Condition:</b> When Network Route is added in Active-Active Config-Only WAN Cluster when Cluster is in Particular State. <b>Workaround:</b> Restart/Reboot of the node that is not working.
PRS-359811	<b>Symptom:</b> dsagentd process crashes when more than 1024 Connections are opened at the same time between PCS and LDAP Backend Server. <b>Condition:</b> Connect multiple users using LDAP Authentication such that 1024 Connection are opened at the same time between PCS and LDAP Backend Server. <b>Workaround:</b> None.

Problem Report Number	Release Note
PRS-361265	<p><b>Symptom:</b> Toggling back and forth between user session sync and config only cluster mode may result in user session sync mode not working.</p> <p><b>Condition:</b> Toggling back and forth between user session sync and config only cluster mode</p> <p><b>Workaround:</b> Cluster nodes will have to be warm restarted to start syncing sessions.</p>
PRS-362386	<p><b>Symptom:</b> Seeing Global Static IP Pool Incorrect Warning when Binary User Config is Imported on a Standalone Device</p> <p><b>Conditions: When PCS admin does following steps:</b></p> <ol style="list-style-type: none"> <li>Export Binary User Config from any of the older release or 9.0r1 release from Standalone Device</li> <li>Import the Binary User Config to same Standalone Device or a different Standalone Device</li> </ol> <p><b>Workaround:</b> None</p>
PRS-362525	<p><b>Symptom:</b> Pulse client connection does not use caching results, when launched via browser session with Auth\Non-auth proxy enabled.</p> <p><b>Condition:</b> Pulse client is launched via proxy from browser connection with HC caching enabled</p> <p><b>Workaround:</b> Connect again with browser\Pulse client and host checker results will be cached.</p>
PRS-362508	<p><b>Symptom:</b></p> <ol style="list-style-type: none"> <li>All the licenses get disabled on the PSA-V</li> <li>Virtual License Server is no longer able to lease licenses to the license clients</li> </ol> <p><b>Conditions:</b> Admin has set the Preferred Network to management port under Licensing --&gt; Download Licenses page.</p> <p><b>Workaround:</b></p> <ol style="list-style-type: none"> <li>Set preferred network to internal or external in Licensing --&gt; Download Licenses Page</li> <li>Re-download the licenses using a previously applied authcode to re-enable the licenses</li> </ol>
PRS-360931	<p><b>Symptom:</b> Cluster node remains in disabled state, even after re-installing core license on PSA-V.</p> <p><b>Conditions:</b></p> <ol style="list-style-type: none"> <li>PSA-V is part of a cluster and is installed with core license.</li> <li>Core license got expired/removed. As a result, node gets disabled in the cluster.</li> <li>Admin re-installs core license. Node remains in disabled state.</li> </ol> <p><b>Workaround:</b> Re-enable cluster node from the clustering page.</p>
PRS-360935	<p><b>Symptom:</b> PSA-V gets disabled after re-joining the cluster.</p> <p><b>Conditions:</b></p> <ol style="list-style-type: none"> <li>PSA-V Cluster (NODE-1 and NODE-2) installed with core licenses.</li> <li>Core license on NODE-2 gets expired. As a result, NODE-2 gets disabled in the cluster</li> <li>Admin download renewal core license. Admin now re-enables NODE-2 from NODE-1 clustering page.</li> <li>NODE-2 joins cluster, but all licenses on NODE-2 get overwritten by NODE-1.</li> <li>As a result, NODE-2 loses the core license, and gets disabled again.</li> </ol> <p><b>Workaround:</b></p> <ol style="list-style-type: none"> <li>Remove NODE-2 from cluster from NODE-1 Admin UI.</li> <li>Install core license on NODE-2.</li> <li>Re-add NODE-2 in NODE-1 as cluster member.</li> <li>Join the cluster from NODE-1 Admin UI.</li> </ol>
PRS-360054	<p><b>Symptom:</b> No error message is displayed when PDC version is lesser than minimum client version enforcement.</p> <p><b>Conditions:</b> The issue is observed in PDC 5.2R10 and 5.3R2 on Windows &amp; MAC</p> <p><b>Work Around:</b> None</p>
PRS-360369	<p><b>Symptom:</b> The minimum client version enforcement feature is not applicable for Linux desktop clients.</p> <p><b>Conditions:</b> Enforcement will not be applicable when Linux Pulse desktop client connects to PCS which has minimum client version enforcement enabled.</p> <p><b>Work Around:</b> None</p>
PRS-360349	<p><b>Symptom:</b> The minimum client version enforcement feature is not supported by PPS.</p> <p><b>Conditions:</b> Minimum client version enforcement does not take effect when clients connect to PPS which has this enforcement enabled.</p> <p><b>Work Around:</b> None</p>

Problem Report Number	Release Note
PRS-360616	<p><b>Symptom:</b> PCS side user logs shows an error message even when the SAML authentication is successful.</p> <p><b>Conditions:</b> "Missing/Invalid sign-in URL" error message seen in PCS user log even in successful SAML authentication.</p> <p><b>Workaround:</b> None</p>
PCS-7263	<p><b>Symptom:</b> Cluster are getting created on Hyper-V PCS even though nodes are enabled with different cores.</p> <p><b>Conditions:</b> Issues occurring while forming a cluster with dissimilar number of cores on PSA are not supported.</p> <p><b>Workaround:</b> None</p>
PCS-7046	<p><b>Symptom:</b> Cluster are getting created on KVM PCS even though nodes are enabled with different cores.</p> <p><b>Conditions:</b> Issues occurring while forming a cluster with dissimilar number of cores on PSA are not supported.</p> <p><b>Workaround:</b> None</p>
PCS-7224	<p><b>Symptom:</b> PCS may not come up if user try to reboot from AWS console</p> <p><b>Conditions:</b> Rebooting PCS from AWS console</p> <p><b>Workaround:</b> Do Stop and Start operation from AWS console</p>
PCS-6656	<p><b>Symptom:</b> AWS – end user will not be able to establish a tunnel if admin configure "DHCP" option under IPv4 address assignment.</p> <p><b>Condition:</b> In VPN configuration profile if admin selects DHCP option for IPv4 address assignment.</p> <p><b>Workaround:</b> In VPN configuration profile select IPv4 address pools option.</p>
PCS-7006	<p><b>Symptom:</b> AP Clustering does not work in AWS/Azure.</p> <p><b>Condition:</b> Active passive clustering is not supported in cloud.</p> <p><b>Workaround:</b> NA</p>
PCS-7038	<p><b>Symptom:</b> Currently VPN tunneling feature doesn't function correctly if we have configured VPN connection profile in cluster wide. The reason being is from AWS point of view, we cannot configure the routes specific to the cluster.</p> <p><b>Condition:</b> VPN connection profile as a cluster wide</p> <p><b>Workaround:</b> We have to have VPN resource profiles configured on all the nodes of cluster and configure the routes in AWS with next hop pointing to internal interface of the respective nodes.</p>
PCS-6599	<p><b>Symptom:</b> PCS acting as Pulse One Client, in NDcPP/JITC Mode will fail to connect to Pulse One SaaS</p> <p><b>Conditions:</b> If PCS admin does following steps:</p> <ol style="list-style-type: none"> <li>1. Enable NDcPP/JITC Mode in Inbound SSL Security Option</li> <li>2. Configure Pulse One in PCS to connect to Pulse One SaaS</li> </ol> <p><b>Workaround:</b> Use FIPS ON/OFF Mode in Inbound SSL Security Option</p>
PRS-352127	<p><b>Symptom:</b> Custom SOH Antivirus policy doesn't take Group policy configuration into consideration while evaluating in windows 10 OS.</p> <p><b>Condition:</b> Group policy setting are not considered while evaluating the policy Windows 10 OS.</p> <p><b>Workaround:</b> None</p>
PRS-344807	<p><b>Symptom:</b> 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.</p> <p><b>Conditions:</b> Agentless login with Host Checker Compliance enforced using Google Chrome</p> <p><b>Workaround:</b> Use Mozilla Firefox browser.</p>

Problem Report Number	Release Note
PRS-357865	<p><b>Symptom:</b> PCS in NDcPP/JITC Mode will allow end user login using both valid/revoked certificate when configured CRL server is unreachable or unresolvable</p> <p><b>Conditions:</b> If PCS admin does following steps:</p> <ol style="list-style-type: none"> <li>1. Enable NDcPP/JITC Mode in Inbound SSL Security Option</li> <li>2. Configure Auth Server, Realm and Signin Policy to Support Certificate Based Authentication</li> <li>3. Import CA into Trusted Client CA Store and Configure CRL               <ol style="list-style-type: none"> <li>a. Make the Configured CRL Server down</li> <li style="text-align: center;">OR</li> <li>b. Make the DNS Server which resolves CRL Server hostname unreachable</li> </ol> </li> <li>4. Login as end user using Valid or Revoked Certificate</li> </ol> <p><b>Workaround:</b> Use FIPS ON/OFF Mode in Inbound SSL Security Option</p>
PRS-352129	<p><b>Symptom:</b> Custom SOH AntiSpyware policy doesn't take Group policy configuration into consideration while evaluating in windows 10 OS.</p> <p><b>Condition:</b> Group policy setting are not considered while evaluating the policy Windows 10 OS.</p> <p><b>Workaround:</b> None</p>
PRS-358212	<p><b>Symptom:</b> 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</p> <p><b>Condition:</b> 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.</p> <p><b>Workaround:</b> Admin has to explicitly change the Selected product as "Software Update (2.x)" under the Patch management rule and save it</p>
PRS-360797	<p><b>Symptom:</b> Automatic configuration of PCS Initial IP Configuration is not working</p> <p><b>Conditions:</b> When deploying a PSA-V using create-va.pl script</p> <p><b>Workaround:</b> Manually configure the IP address using the PSA-V Virtual Console.</p>
PRS-362900	<p><b>Symptom:</b> Host Checker will not launch when accessing Microsoft O365 apps from Mac.</p> <p><b>Conditions:</b> Host Checker is enabled on PCS.</p> <p><b>Workaround:</b> Disable the Host Checker on PCS.</p>
PRS-362851	<p><b>Symptom:</b> End user is not redirected to home page Intermittently, post host checking in A/A cluster.</p> <p><b>Conditions:</b> Host checker is enabled with active-active PCS cluster deployment.</p> <p><b>Workaround:</b> Disable the Host Checker on PCS cluster.</p>
PRS-362336	<p><b>Symptom:</b> Error seen while adding O365 as Service Provider via New Cloud Secure Admin UX</p> <p><b>Conditions:</b> Configuring O365 as Service Provider in PCS</p> <p><b>Workaround:</b> Administrator have to retry adding the application again.</p>
PRS-362154	<p><b>Symptom:</b> Cloud Secure Admin UX alignment changes when resizing the browser</p> <p><b>Conditions:</b> Configuring Cloud Secure with New UX</p> <p><b>Workaround:</b> None</p>
PRS-362152	<p><b>Symptom:</b> Cloud Secure Dashboard settings page will be shown in expanded mode when the page is opened</p> <p><b>Conditions:</b> When admin access Cloud Secure Dashboard page</p> <p><b>Workaround:</b> None</p>
PRS-361867	<p><b>Symptom:</b> PCS devices upgraded to 9.0R1 does not show redesigned end user pages while accessing cloud applications.</p> <p><b>Conditions:</b> Upgrade is done to 9.0R1 from an older release.</p> <p><b>Workaround:</b> Enable the redesign end user pages manually from Cloud Secure Admin UX after upgrade.</p>
PRS-361066	<p><b>Symptom:</b> SSO will not work with gmail active sync profile in android.</p> <p><b>Conditions:</b> Active sync profile is pushed as part of managed Gmail app via PWS server.</p> <p><b>Workaround:</b> Enter the password field while logging.</p>
PRS-361494	<p><b>Symptom:</b> Redesigned end user pages will not appear after logout from cloud SAAS applications.</p> <p><b>Conditions:</b> Redesigned cloud secure pages are enabled via Cloud Secure New UX.</p> <p><b>Workaround:</b> None.</p>



Problem Report Number	Release Note
PRS-363184	<b>Symptom:</b> Device Attribute fetch fails from PWS while using External PKI Server in Pulse Workspace <b>Conditions:</b> PWS server is configured to use External PKI Server <b>Workaround:</b> Disable External PKI Server and use the in-built PWS CA server
PRS-362545	<b>Symptom:</b> SAML 1.1 version is not working with embedded browser. <b>Conditions:</b> When embedded browser is enabled and customer is using SAML 1.1, authentication may not work <b>Workaround:</b> Do not enable embedded browser.
PRS-363203	<b>Symptom:</b> VPN traffic will not go through tunnel when IPv4 stack is disabled on client machine and Split tunneling is enabled on the PCS server. <b>Conditions:</b> Client crashes when FQDN is enabled and IPV4 stack is disabled. <b>Workaround:</b> Enable IPv4 stack on client machine.

## Documentation

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

## Technical Support

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

- <https://support.pulsesecure.net/>
- [support@pulsesecure.net](mailto:support@pulsesecure.net)
- Call us at 1- 844-751-7629 (toll-free USA)

For more technical support resources, browse the support website <https://support.pulsesecure.net/>.