Pulse Connect Secure: Release Notes

PCS 9.1R8 Build 7453

PDC 9.1R8 Build 3143.1

Default ESAP Version: ESAP 3.4.8

Product Release	9.1R8
Published	August 2020
Document Version	8.2

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

www.pulsesecure.net

Pulse Connect Secure: Release Notes

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 http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Revision History

Table 1 lists the revision history for this document.

Date	Revision	Description
8.2	August 2020	Updated the Known Issues section.
8.1	July 2020	Updated the Fixed Issues section > 9.1R7 and 9.1R8 list.
8.0	July 2020	Initial Publication 9.1R8
7.0	June 2020	Initial Publication 9.1R7 Updated Fixed Issues > 9.1R1 Release with PRS-368927
6.0	May 2020	Initial Publication 9.1R6
5.3	April 2020	Updated Known Issues section for 9.1R5
5.2	April 2020	Cosmetic change for 9.1R5
5.1	April 2020	Updated New Features section for 9.1R5
5.0	April 2020	Initial Publication 9.1R5
4.3	April 2020	Initial Publication 9.1R4.3
4.2	March 2020	Initial Publication 9.1R4.2
4.1	February 2020	Initial Publication 9.1R4.1
4.0	January 2020	Initial Publication 9.1R4
3.1	October 2019	Updated Known Issues section for 9.1R3
3.0	October 2019	Initial Publication 9.1R3
2.0	July 2019	Initial Publication 9.1R2
1.0	May 2019	Initial Publication 9.1R1

Contents

Introduction

This document is the release notes for Pulse Connect Secure Release 9.1R8. This document contains information about what is included in this software release: supported features, feature changes, unsupported features, and known issues. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

Hardware Platforms

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

- PSA300, PSA3000, PSA5000, PSA7000f, PSA7000c

To download software for these hardware platforms, go to: https://support.pulsesecure.net/

Virtual Appliance Editions

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

- Virtual Pulse Secure Appliance (PSA-V)

Note: From 9.1R1 release onwards, VA-DTE is not supported.

Note: From 9.0R1 release, Pulse Secure has begun the End-of-Life (EOL) process for the VA-SPE virtual appliance. In its place, Pulse Secure has launched the new PSA-V series of virtual appliances designed for use in the data center or with cloud services such as Microsoft Azure, Amazon AWS, OpenStack Fabric and Alibaba Cloud.

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

Platform	Qualified System
VMware	• HP ProLiant DL380 G5 with Intel(R) Xeon(R) CPU • ESXi 6.7 Update 2c
KVM	• CentOS 6.6 with Kernel cst-kvm 2.6.32-504.el6.x86_64 • QEMU/KVM v1.4.0 • Linux Server Release 6.4 on an Intel Xeon CPU L5640 @ 2.27GHz • 24GB memory in host • Allocation for virtual appliance: 4vCPU, 4GB memory and 40GB disk space
Hyper-V	• Microsoft Hyper-V Server 2016 and 2019
Azure-V	• Standard DS2 V2 (2 Core, 2 NICs) • Standard DS3 V2 (4 Core, 3 NICs) • Standard DS4 V2 (8 Core, 3 NICs)

Platform	Qualified System
AWS-V	• T2.Medium (2 Core, 3 NICs and 2 NICs) • T2.Xlarge (4 Core, 3 NICs) • T2.2Xlarge (8 Core, 3 NICs)
Alibaba Cloud	• ecs.g6.2xlarge (8 vCPU, 32GB, 2 NICs)

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

VMware Applications

The following table lists the VMware applications qualified.

Platform	Qualified
VMware	
VMware Horizon View HTML Access, version 7.9, 7.10	• Rewriter
VMware Horizon View Server version 7.9, 7.10	• VDI Profiles

Upgrade Paths

The following table describes the tested upgrade paths. Please note that here x and y refer to the following:

x: Latest maintenance release version

Upgrade From	Qualified	Compatible
9.1Rx	Yes	-
9.1Ry	-	Yes
9.0Rx	Yes	-
9.0Ry	-	Yes
8.3Rx	Yes	-
8.3Ry	-	Yes

For versions prior to 8.3, first upgrade to release 8.3Rx|8.3Ry, then to 9.0Rx|9.0Ry, and then upgrade to 9.1R8.

Note: If your system is running beta software, roll back to your previously installed official software release before you upgrade to 9.1R8. 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 9.1R8 without a core license installed. Follow these steps to upgrade to 9.1R8:

1. If PSA-V is running 8.3Rx:
   a. Upgrade to 9.0Rx.
   b. Install Core license through Authcode.
   c. Upgrade to 9.1R8.
2. If PSA-V is running 9.0Rx or later:
   d. Install Core license through Authcode.
   e. Upgrade to 9.1R8.

For more details, see the ""Noteworthy Information in 9.1R4.3 Release"" section.

General notes

1. For policy reasons security issues are not normally mentioned in release notes. To find more information about our security advisories, please see our security advisory page.
2. In 8.2R1.1 and above, all PCS client access binaries (Network Connect, WSAM, Host Checker, JSAM, Windows Terminal Services, Citrix Terminal Services) are signed with a SHA2 code signing certificate to improve security and ensure compatibility with Microsoft OS's 2016 restrictions on SHA1 code signing. This certificate will expire on April 12, 2021. For details, refer to KB articles KB14058 and KB43834.
3. Important note: Windows 7 machines must contain a March 10, 2015 Windows 7 Update in order to be able to accept and verify SHA2-signed binaries properly. This Windows 7 update is described here and here. If this update is not installed, PCS 8.2R1.1 and later will have reduced functionality (see PRS-337311 below). (As a general rule, Pulse Secure, LLC recommends that client machines be kept current with the latest OS updates to maximize security and stability).
4. When custom ciphers are selected, there is a possibility that some ciphers are not supported by the web browser. If any ECDH/ECDSA ciphers are selected, they require ECC certificate to be mapped to the internal/external interface. If an ECC certificate is not installed and mapped to the internal and external ports (if enabled), administrators may not be able to login to the appliance. The only way to recover from this situation is to connect to the system console and select option 8 to reset the SSL settings. Option 8 resets the SSL setting to factory default. Any customization is lost and will need to be reconfigured. This is applicable only to Inbound SSL settings.
5. Pre-5.0 Android and pre-9.1 iOS devices don't support Suite B ciphers. If Suite B is enabled, Pulse client on pre-5.0 Android and pre-9.1 iOS devices will not be able to connect to PCS device.
6. Minimum ESAP version supported on 9.1R6 is 3.2.8 and later.

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

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

Noteworthy Information in 9.1R8 Release

For 9.1R8, Pulse Collaboration Client is packaged using PCS 9.1R7 build.

Noteworthy Information in 9.1R4.3 Release

1. In 9.1Rx OVF a critical issue was observed. The 9.1R4.3 release addresses this issue.
2. On some of the installations, it was observed that a few read-only files were being overwritten. Customers are experiencing HTTP 500 response for some of the admin requests. The 9.1R4.3 release addresses this issue.
3. Upgrade works only if VA is deployed with 8.3 OVF onwards. If VA is deployed with pre 8.3 OVF, upgrade to this image will not work.
4. Refer to KB44408 **for the recommendations / best practices to deploy Virtual Appliance and the logs needed for analysis/troubleshooting**.

New Features

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

Feature	Description
Release 9.1R8 Features	
UEBA package for fresh installation of PCS/PPS	In case you have a fresh installation of PCS/PPS, you may download latest UEBA package from Pulse Secure Support Site (my.pulsesecure.net) and add the package at Behavior Analysis page before using Adaptive Authentication or Geolocation based Conditional Access.
Show users by access type	Apart from showing the number of concurrent user sessions, PCS Dashboard now shows the L4 access type (PSAM) and Clientless access type (Browser) logins as non-tunnel users.
PCS Protection from Overload	This feature disallows user login, user login via Pulse Desktop, HTML5 connection or connection to a web resource when the CPU load is above a certain threshold. By default, this option is disabled for PCS upgrades and enabled for new installation.
Reset/Unlock TOTP user through REST API	This release provides REST API to Reset/Unlock a user under a TOTP server.
New license SKUs for PCS/PPS	In this release, added around 120 new license SKUs for PCS/PPS.
Support for pool of NTP servers and NTP status check	PCS now supports pool of NTP servers up to 4 NTP servers to sync date and time.
Release 9.1R7 Features	
Automatic enable/ disable ICE license	This release provides automatic management of ICE license. PCS enables ICE license when the logged in users count crosses the maximum licensed users count and disables ICE license when the logged in users count drops below the maximum licensed users count. As an example, If you installed 100 licensed user counts, when the 101th user logs in, ICE license gets automatically enabled.
Show current HTML5 RDP sessions in Dashboard	This release provides HTML5 sessions information in the dashboard and the trend graph that helps admin to view the CPU usage and take necessary action to provide better remote access experience for the users.
Support for srcset attribute in HTML	PCS provides support for the responsive images (in web applications) via rewriter by rewriting the srcset attribute value. The corresponding images would be fetched on client application based on screen size, resolutions and other features.
Enable/Disable FQDN ACL	FQDN ACL feature was enabled by default earlier even though there are no policies configured. A new admin configurable option to enable or disable FQDN ACL feature is added in 9.1R7 at System > Configuration > VPN tunneling.
Release 9.1R6 Features	

Feature	Description
Hyperlink to Host Checker Policies	In the User Realms > Authentication Policy > Host Checker page, the policy names now have hyperlinks. Click the link to view the policy configuration.
Hardware ID in the System Maintenance page	The System > Maintenance > Platform page displays Hardware ID along with the other platform details.
Serial number in the Licensing screen	The System > Configuration > Licensing page, displays Hardware Id and Serial number.
Enable/Disable option for ICE license	This release provides REST API to do the following on a Standalone/Cluster: • enable/disable ICE license • get the current status of ICE license.
Release 9.1R5 Features	
Terraform template support for AWS and Azure	PCS can be deployed using Terraform templates on supported hypervisors and cloud platforms.
Location based Conditional Access	Conditional Access feature for Cloud Secure now provides a mechanism to enforce access control policies based on location parameters by defining policies for applications.
Password management for Open LDAP	LDAP based password management works with generic LDAP servers such as OpenLDAP.
Microsoft Intune MDM integration	In this release, the Pulse Secure device access management framework supports integration with Microsoft Intune.
HTML5 Sessions report	Active number of HTML5 sessions on PCS can be obtained using a REST API call to api/v1/stats/active-html5-sessions.
MSSP Reporting enhancements	It is now possible to extract any particular license client/cluster report through REST API. Enhancements include: • Cluster-wise view in the license report. • License report in JSON format through REST. • Options to get cluster/client/period sub-section of the granular report through REST.
SSLDump for VLAN	In this release, SSLDump utility supports VLAN. Admins can use this tool for debugging / data collection purpose.
Edit default gateway configuration	In PCS hosted on a cloud environment, it is now possible to edit default gateway configuration from UI.
Host Checker feature enhancement	Host Checker policy to detect and allow hard disk in which encryption is in progress.
License server with Active-Active cluster	Administrators can: • create license server with Active Active cluster on virtual/cloud and hardware platforms. • lease all different type of licenses to license clients from any node of active-active cluster. • surrender/recall licenses from any node of active-active cluster.
Release 9.1R4.3 Features	

Feature	Description
No new features added for this release	
Release 9.1R4.2 Features	
No new features added for this release	
Release 9.1R4.1 Features	
No new features added for this release	
Release 9.1R4 Features	
PCS VA on Alibaba Cloud	PCS now supports VA deployment on Alibaba Cloud.
Conditional Access	Conditional Access feature for Cloud Secure provides a mechanism to enforce access control policies based on user and device parameters by defining policies for applications. Conditional Access policies are evaluated during application access time while roles are mapped to the session during the session creation time.
REST API enhancements	Enhancements include: • Update to "Getting Active Sessions" • Update to "Getting System Information" • Added "Fetching the User Login Statistics" • Added "Health Check Status" • Added "VIP Failover" • Added "Applying License" • Added "Deleting License" • Added "Getting License Clients" • Added "Getting License Report from License Server" • Added Profiler REST APIs
vTM and PCS Integration for Load Balancing	The Platform Limit, Maximum Licensed User Count and Cluster Name attribute values are available for optimal load balancing.
Support for Windows Redstone 6	In 9.1R4 release, Windows Redstone 6 - version 1909 is qualified.
Support for SharePoint 2019	In 9.1R4 release, SharePoint 2019 is qualified.
Support for VMware VDI 7.9, and 7.10	In 9.1R4 release, VMware VDI versions 7.9 and 7.10 are qualified.
Support for Citrix Virtual Apps and Desktops 7 1909	In 9.1R4 release, Citrix Virtual Apps and Desktops 7 1909 is qualified.

Feature	Description
Protect passwords stored in local auth server using stronger hash	When a new local authentication server is created, now admin has a choice to store the password with strong hashing using pbkdf2.
Support license reporting per license client	Licensing report is enhanced with usage statistics for each PCS instance - maximum user count per month per PCS/per MSSP. MSSPs can now: • generate accurate usage reports of their customers. • make the structured report in XML format to enable for parsing and usage for dashboard.
Release 9.1R3 Features	
Consolidated system and troubleshooting logs	The various system logs and troubleshooting logs that help in investigating user access issues and system issues can be configured and accessed using the Log Selection page.
Connect to nearest available DC	The LDAP authentication configuration is enhanced in 9.1R3 to locate the nearest Microsoft domain controllers, which are spread across the globe, by resolving DNS SRV records.
Zero touch provisioning	From 9.1R3 release, PCS can detect and assign DHCP networking settings automatically at the PCS VM boot up. In the script included in the PSA-V package, the PCS parameters should be set to null in order to fetch the networking configuration automatically from the DHCP server. **Note:** This feature is not supported on PSA hardware.
PCS hosted in OpenStack cloud	OpenStack is an open source cloud computing platform that allows deploying and managing a cloud infrastructure as an IaaS service. As part of this release, Pulse Secure supports deploying PCS KVM in OpenStack cloud.
VMware tools support	From 9.1R3 release, VMware support is qualified for VMware 10.3.10, ESXi 6.7 Update 2c.
Debug Log storage expansion	From 9.1R3 release, the maximum debug log size is increased to 1024 MB on hardware platforms.
Periodic iostat data collection	From 9.1R3 release, the “iostat” information is gathered periodically and made available as part of node monitoring in system snapshot.
Control copy/paste option for a user from an HTML5 session	9.1R3 release provides option to the administrators as well as end-user to enable/disable copy/paste from HTML5 RDP sessions. This option will be available under User Roles as well as Admin Created Bookmarks”.
Enhancements to Local Authentication Server default password	From 9.1R3 release, for a fresh installation, the valid password range defined is 0-999. Minimum length 10 and maximum length 128 are set as default values.
Restricting access to default resource policies	From 9.1R3 release, for a fresh installation, the following predefined resource policies are set to “Deny” state by default. • Web Access Resource Policy “Initial Policy for Local Resources” • Windows File Access Resource Policy “Initial File Browsing Policy” **Note:** The predefined policy for VPN Tunneling is not provided.

Feature	Description
IKEv2 Fragmentation	IKEv2 packets can be larger than the MTU especially the IKE_AUTH packets which include the certificate chain. These larger IKE packets get fragmented in the intermediate devices. This feature implements fragmentation at IKE level and avoids IP fragmentation.
MSS value for TCP connections on Tun devices	Due to larger IPv6 header as compared to IPv4, if the MSS of the PCS external interface is not set appropriately, the packets would be dropped on the external interface. This feature enables to set MSS to a lower value so that TCP connections are not dropped for 6-in-4 cases or when there is NAT translation somewhere in the network before reaching PCS.
Release 9.1R2 Features	
SP-Initiated SAML SSO	Pulse Secure supports SP-initiated SAML SSO when PCS is configured as IdP in gateway mode. PCS uses the existing user session in generating SAML assertion for the user for SSO.
IDP initiated SAML Single Logout	This feature provides a single logout functionality wherein if a user gets logged out of a session from one application, PCS (configured as IdP) notifies all other connected applications of that user with Single Logout.
Flag Duplicate Machine ID in access logs	Pulse client expects the machine ID is unique on each machine. If multiple endpoints have the same machine ID, for security reasons, the existing sessions with the same machine id are closed. A new access log message is added to flag the detection of a duplicate Machine ID in the following format: *Message: Duplicate machine ID "<Machine_ID>" detected. Ending user session from IP address <IP_address>. Refer document KB25581 for details.*
Microsoft RDWeb HTML5 Access	The newly introduced Microsoft RDWeb resource profile controls access to the published desktops and applications based on HTML5. The Microsoft RDWeb templates significantly reduce the configuration time by consolidating configuration settings into one place and by pre-populating a variety of resource policy settings. **Note:** In the 9.1R2 release, Microsoft RDWeb HTML5 access does not support Single Sign On. SSO will be made available in the future release.
Backup configs and archived logs on AWS S3/Azure Storage	Two new methods of archiving the configurations and archived logs are available now apart from SCP and FTP methods: Pulse Connect Secure now supports pushing configurations and archived logs to the S3 bucket in the Amazon AWS deployment and to the Azure storage in the Microsoft Azure deployment.
V3 to V4 OPSWAT SDK migration	PCS supports the migration of servers and clients to OPSWAT v4 to take advantage of latest updates.
Report Max Used Licenses to HLS|VLS	From 9.1R2 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.

Feature	Description
VA Partition Expansion	PCS/PPS supports upgrading from 8.2Rx to 9.1R2 for the following supported platforms: • VMWare ESXi • KVM • Hyper-V When upgrading a VA-SPE running 8.2R5.1 or below that was deployed with an OVF template to a higher version, the upgrade was failing. This feature solves the upgrade problem for VMWare, KVM and Hyper-V. Refer KB41049 for more details.
Release 9.1R1 Features	
Software Defined Perimeter	Pulse Secure SDP uses PCS appliances which individually act as either an SDP controller or an SDP gateway. Mobile users of the Pulse Secure Client perform authentication on an SDP controller which runs an Authentication, Authorization and Accounting (AAA) Service. The SDP controller then enables direct communication between the user and the SDP gateways that protect the user's authorized resources and enables requested encryption.
DNS traffic on any physical interface	Prior to 9.1R1 release, DNS traffic was sent over the Internal interface. Starting with 9.1R1 release, an administrator can modify the DNS setting to any physical interface namely Internal Port, External Port or Management Port.
Authentication failure management	Account Lockout option is provided to manage user authentication failures for admin users of local authentication server. The admin user account will be locked after specified number of consecutive wrong password attempts. The account will be unlocked after the specified lockout period or by using the Unlock option.
Support for "client-name" parameter in HTML5 Access	User can pass "client-name" in HTML5 rdp using launcher method. The %clientname% variable is matched with a workstation ID and normally that variable is unique and dedicated remote desktop computer name.
Deploying PSA-V in KVM	User can deploy PSA-V in KVM using a template.
User access to internet resources on an Azure-based or AWS-based PCS	AWS VPC GW and Azure VNet GW drop packets if the source IP is the endpoint tunnel IP. This feature NATs endpoint tunnel IP to Internal interface IP. The NAT allows user to access internet resources when connected to a VPN tunnel on an Azure or AWS-based PCS.
REST API enhancements	Enhancements include: Getting Config without Pulse packages such as ESAP package and Pulse Client package Backing up and restoring binary configuration

Fixed Issues

Problem Report Number	Summary
Release 9.1R8 PRs	
PRS-392702 PRS-391725	Additional logging to debug web crashes.
PRS-392244 PRS-388907	Active users were not able to sync to the newly added node on a 3 node Active/Active cluster. This is addressed in 9.1R8.
PRS-392040 PRS-388907	User sessions are not synced across the nodes in an Active/Passive cluster. This is addressed in 9.1R8.
PRS-391902	Invalid packet processing in kernel is addressed in 9.1R8.
PRS-391879	Intermittent audio disconnect issue with HTML5 RDP session is addressed in 9.1R8.
PRS-391837 PRS-380638	tncs process crash with Host Checker caching enabled is addressed in 9.1R8.
PRS-391004	The dsunitysamlhandler process crash is addressed in 9.1R8.
PRS-390937	In 9.1R4 to 9.1R7, when multi monitor option is selected under the Terminal Services session/ bookmark page as well as under Terminal Services Options page, XML config data shows incorrect value. This is addressed in 9.1R8.
PRS-390916	Kernel panic during upgrade on PSA5000-V running 9.1R3 on Hyper-V. This is addressed in 9.1R8.
PRS-390907	Log rollover is implemented for postgresd so that it does not cause the Disk to get full.
PRS-390831	SAML authentication is now successful when signing is enabled for SAML requests/responses using certificates.
PRS-390828	As dshealthstatsunity process was getting exited due to exceeding process size, data was not being sent to Pulse One for that particular interval and thus calculated cumulative count at Pulse One was incorrect. This issue is addressed in 9.1R8.
PRS-390769	Kernel logging options are added by default for better debuggability.
PRS-390426	As process was getting exited due to exceeding process size, data was not being sent to Pulse One for that particular interval. This issue is addressed in 9.1R8.
PRS-390274	For config elements with unicode characters and having length exceeding 4096 bytes, the config import fails on Pulse One client. This issue is addressed in 9.1R8.
PRS-390217	Tunnels get dropped during connection resumption due to a server error. This is addressed in 9.1R8.

Problem Report Number	Summary
PRS-389927	The TCPDump filter expression can now contain characters from the set "<>|;()[]?#$^&*=\'`"" .
PRS-389897	Kernel Panic hrtimer_interrupt issue is fixed.
PRS-389771	Multiple VIP fail over was seen on Virtual A/P cluster due to the time drift between system clock and hardware clock. This is addressed in 9.1R7 (KB44457).
PRS-389756	The dsagentd process crash during assignment of IP address from DHCP server is addressed in 9.1R8.
PRS-388630	With current OPSWAT library code, the verification of update functionality was not working. OPSWAT has fixed the issue and provided a new library.
PRS-388104	The top-roles section displayed on dashboard was not showing the roles name in Japanese and other languages. This issue is fixed for both Classic UI and New UI in 9.1R8.
PRS-385646	Whenever a user tries to access the VDI resource, a wrong error code for timeout was written in the logfile. The user sees the message "Missing host name/IP, Invalid host name/IP: " To address the issue: 1. Timeout error ID is passed to write in logfile. 2. A proper validation has been done for the wrong false alarm.
PRS-364693	Bandwidth Management policy not getting enforced for VPN tunneling users is fixed in 9.1R8 - https://kb.pulsesecure.net/articles/Pulse_Secure_Article/KB44402/?kA13Z000000L3Dc.
PCS-20480	PCS was returning "Incorrect ICE action" error message when trying to execute api/v1license/ice REST API to fetch the current status of ICE. This is addressed in 9.1R8.
Release 9.1R7 PRs	
PRS-391296	Application access using Citrix Terminal Services through IE browser fails in 9.1R5-9.1R6 PCS versions. This is addressed in 9.1R7.
PRS-390778	Host Checker support for OS version check is added for iOS versions 13.4 and 13.4.1.
PRS-390775	PCS syslog forwarder does not work if connection to syslog server fails during startup of the syslog forwarder process. This is addressed in 9.1R7.
PRS-390530	Enterprise user onboarding fails in Mac OS Catalina as the filename extension was not populated as '.mobileconfig'. This extension is added in 9.1R7.
PRS-390475	Noticeable slowness was seen in several applications including Citrix HTML5 video rendering in 9.1R3-9.1R6 PCS versions. This is addressed in 9.1R7.
PRS-390401	SNMP functionality was not working after cache sync. This is addressed in 9.1R7.
PRS-390234	User access log now shows real-time active HTML5 sessions count.
PRS-390118	In PCS A/P cluster split and joined scenario, lease license IDs are validated to reset the stale ID and license client will be able to lease licenses successfully.
PRS-389481	Cloud Platforms: Improved SNAT performance by tuning kernel module parameters based on the memory available in the device.

Problem Report Number	Summary
PRS-389209	With PCS 9.0R2-9.1R6 and Pulse 9.0R2-9.1R3, the client continues to send the CAV traffic to PCS every 300 seconds even when Cloud Secure license is not installed. From PCS 9.1R7 onwards, the PDC client (Pulse 9.0R2-9.1R3) will contact the PCS server only once per user session - KB44410.
PRS-388932	From PCS 9.1R7, the "Synchronization of last access time in user sessions" option in A/A Cluster mode will be auto-enabled and grayed out when the "Synchronize user sessions" option is enabled (otherwise, it can affect session migration). Existing cluster configuration is not modified during upgrade, so we recommend admins to enable this option for existing configurations as well.
PRS-388455	If epupdate_hist.xml is hosted internally with no authentication and if "Use Proxy Server" (With/without auth) is enabled with FQDN or IP Address, the first 3 characters are ignored thus causing it to fail. For example, proxy.domain.net is taken as xy.domain.net. This issue is now fixed for both PCS and PPS.
PRS-382777	Client's original Source IP was not logged if Load Balancer is used. Client's Source IP is now retrieved from 'X-Forwarded-For' header and logged in user access logs.
Release 9.1R6 PRs	
PRS-390370 PRS-390145	Java Script is displayed after the user scans the QR code only during the TOTP user registration.
PRS-390352	Hostname resolution for an FQDN with up to 255 characters was not supported through the L3 tunnel in PCS 9.1R5.
PRS-390198	Admin cannot download reports in PDF format for PCS.
PRS-389973	HTML5 connections cause memory leak in Guacamole server and result in high memory usage and swap memory usage
PRS-389811	CPU Allocation issue on PSA-7000 (all flavors/varieties) appliances in case of Single-Arm mode VA deployments is now resolved on PSA-7000 HW and ESXi (VMWare) solutions. Refer KB44446 for more details.
PRS-389744	Process snapshot for "dsserver-tasks" is generated while deleting meeting objects for corresponding users.
PRS-389544	Some of the examples listed under "Split Tunneling Networks" policies are not supported.
PRS-389523	External backend resource access using HTTP GET request with username in the URL for the file login.cgi fails through Rewriter.
PRS-389517	Web server crashes and results in User disconnections due to webSocket upgrade related messages during Auth Only URL access.
PRS-389440	User Accounts under TOTP Auth server Users section cannot be exported.
PRS-389406	Delayed or no response from PCS for SNMP queries under load condition.
PRS-389276	The corruption of blob during the epupdate results in Host Checker scan failure for users until the next successful epupdate.

Problem Report Number	Summary
PRS-389262	Web process snapshot is generated while sending POST request by REST API with an empty body.
PRS-389127	Garbled text in Citrix VDI profiles page when accessed using bookmark with the Japanese language.
PRS-388796	The dsagentd process (client server process) crashes and frequently disconnects in 9.1R4 when there are more than 1024 tunnels including MobIKE IKEv2 tunnels.
PRS-388645	After upgrading PCS/PPS to 9.1R3-9.1R5, slow Host Checker response is observed due to a very frequent re-evaluation of Cybereason Active Probe product.
PRS-388542	Garbled text in file share page when accessed using bookmark with the Japanese language.
PRS-374603	During system downtime activities such as an upgrade, Event IDs such as 20412/20413 are missing in the Syslog server.
Release 9.1R5 PRs	
PRS-389938	9.1R4.3 Radius crashing, unable to authenticate Pulse.
PRS-389550	Intermittently, the system throughput falls drastically and user connections fail.
PRS-389246	"500 Internal Error" is displayed when opening Authentication related pages.
PRS-389212	Intuitive Customer friendly ways and relevant logs to avoid customers configuring single core.
PRS-388958	Idle timeout session is not working, OWA 2016 keepalives not ignored through web-rewrite.
PRS-388885	License Surrendering not happening due to the heartbeat not sent.
PRS-388743	Host Checker :: OS Checks :: MAC :: Add support to configure Minimum Service Pack/Version for MAC Catalina(10.15).
PRS-388734	PSA7000 at 30% total CPU due to two guacd processes at 100% CPU, planning pandemic and wanted to know root cause.
PRS-388536	One node in Cluster is surrendering the licenses to the License server. However, the increment of the surrendered time is not happening.
PRS-388479	PSA5000 : 9.1R4 : A/P Cluster : REST API calls are failing intermittently when they are executed in a loop continuously.
PRS-388429	Text corrected under Log/Monitoring > Admin Access > Settings.
PRS-388421	PCS 9.1R4 incorrectly reporting duplicate machine ID.
PRS-388409	Unable to upload config to Pulse One: Configuration changed while preparing configuration to upload.
PRS-388331	After upgrade VA-DTE & PSA-V to 9.1R4, nfqueue unable to create IPTables when VM is configured with 1 CPU core only.
PRS-388244	FileShare:: Customer unable to download direct file from FileShare on 9.1R4 PCS version.
PRS-387954	Rewrite: Web page of the maps web applications fails to load via rewrite.

Problem Report Number	Summary
PRS-387780	Registered PCS Appliance failing with Pulse one communication after importing user config and shows registration expired error message.
PRS-387641	"Sign Out message" does not properly display unicode text (Japanese, Korean, Chinese, etc.) with Sign-In Pages via browser.
PRS-387359	Unable to authenticate user using certificate. Reason: Wrong Certificate::unsupported name constraint type.
PRS-387349	System: Built-in Trusted Server CAs cannot be removed if they have subCAs.
PRS-387062	PSAM sending unintended traffic via tunnel to VPN in 9.1R3.
PRS-386875	User Sessions get disconnected after upgrading to 9.1R3HF1.
PRS-385747	Program dsdashsummary failing continuously on PCS running on 9.0R4.1.
PRS-385466	Sharepoint 2019 is not loading properly through web-rewrite.
PRS-385027	VDI Bookmark would not establish connection to the VDI resource without host entry on the client machine.
PRS-384955	XML Import of trusted server CAs generates a spurious admin log message for each unchanged CA.
PRS-382364	System: Device does not boot up when upgrading from 8.3R7.1 to 9.0R5 with option DELETES all system and user configuration data before installing the service package is selected.
PRS-381972	System : Licensing : "License server low-level protocol error, server=, Code = [6] :Could not resolve host name" populated in event logs of license server.
PRS-381905	After upgrading to iOS 13, HTML5 Access users seems to have broken the on-screen mouse pointer.
PRS-381716	AAA::Issues with host checker when user logs in to a different realm with TOTP auth server enabled.
PRS-381699	Pulse One 2.0.1902: Certificate > Trusted Server CA changes not being distributed (deleted expired CA).
PRS-381678	VIP became unreachable from enforcer when upgrading from 5.4R7 to 9.1R2.
PRS-381046	Rewrite: Dynamic365 menu tabs do not render when on 9.1R1.
PRS-380298	User access log indicates Login failed using auth server LDAP Server (Failed::unable to verify the first certificate) for wrong password.
PRS-380225	"Program fqdnacl recently failed" event failure on PCS 9.0R4.
PRS-379752	Reboot failed on PSA7000f.
PRS-379137	Gliffy Plugin in Confluence does not work via Web Rewrite.
PRS-376852	IPV4 Settings change in External or Internal port keeping Default VLAN ID same does not reflect under VLAN tab..
PRS-365669	SNMP: ifAdEntAddr mapped to wrong ifAdEntIndex values.

Problem Report Number	Summary
Release 9.1R4.3 PRs	
PRS-389246	"500 Internal Error" is displayed when opening Authentication related pages.
Release 9.1R4.2 PRs	
PRS-380298	User Access log indicates "Login failed using Auth. server LDAP server (Failed: unable to verify the first certificate)" for wrong password.
PRS-387780	Registered PCS Appliance fails with Pulse One communication after importing user config and shows "Registration Expired" error message.
Release 9.1R4.1 PRs	
PRS-382268	PDC throws Authentication rejected by server [Error : 1319] when using global PCS url.
PRS-387062	PSAM sending unintended traffic via tunnel to VPN in 9.1R3.
Release 9.1R4 PRs	
PRS-365669	SNMP: ifAdEntAddr mapped to wrong ifAdEntIndex values.
PRS-367786	Device locked up and dropped all connections due to Web process consuming CPU.
PRS-375181	VLS does not throw any error if there is no response for Heartbeats sent to PCLS.
PRS-377456	EasyPrint feature using the Premier Java RDP Applet not working.
PRS-379345	Program dsagentd failed.
PRS-379411	PCS not sending any Syslog traffic to configured Syslog servers.
PRS-379801	Active Sync stopped working after upgrading the device to 9.0R4.
PRS-380136	Cluster communication and state storage problems on A/A cluster.
PRS-380765	Program dsagentd recently failed after upgrading PCS from 9.0R3.2 to 9.0R4.
PRS-380796	PCS-VA sending critical SNMP alerts while leasing license.
PRS-380993	DFS: process snapshot generated by snmptrap process.
PRS-381100	Program dsagentd recently failed while running Mixed [V4 and V6] 60K VPN Tunneling ACL's throughput test on PSA5k for secure cache build-3164.
PRS-381366	Multiple users getting disconnected from Pulse Client.
PRS-381403	Sharing Feature is not working in macOS Catalina.
PRS-381579	Sometimes empty logs are seen under "Log/Monitoring".
PRS-381621	9.0R4 and 9.0R5 SPE (PSA-V) do not show the User Record Sync column in Admin UI > Auth Server page.
PRS-381633	Host Checker checking for virus definition file based on Number of updates fails for Sophos Endpoint Security and Control 10.8.4.
PRS-381736	After Upgrade from 8.3R7.1 to 9.1R1, error encountered while upgrading cache (in Host Checker).

Problem Report Number	Summary
PRS-381795	[FQDN ACL / NFQUEUE] Request DEV help in determining why thousand of VPN Tunnels dropped traffic within.
PRS-381960	Facing slowness when accessing web application through Authorization-only access post upgrading to PCS OS 9.0R5.
PRS-381963	Group Names in the role mapping rule will get added with &, # and; special character if more than 5 groups are selected with AD as the auth server.
PRS-381984	The cookie setting should be included in the resource profile.
PRS-382001	UI: Description incorrect on default deny in 9.1R3 initial deployment.
PRS-382021	Button to dismiss the banner on PPS/PCS Dashboard for not accepting Perpetual license is not working.
PRS-382031	Need to replace VA-SPE|PSA-V in "Only EVAL licenses are allowed for manual installation in VA-SPE|PSA-V".
PRS-382035	Proper logging for NFQUEUE full and drops needed, also consider this situation for cluster A/P failover or add to healthcheck.
PRS-382191	Unable to ping the IPv6 VLAN-Gateway from the PCS device after changing the Gateway address.
PRS-382240	User dropped from the VPN tunnel connection ##g_dhcp_proxy_wbuf is maxed!.
PRS-382350	Unknown RAID status in PSA7000f due to no space left on device.
PRS-382804	Active node went unresponsive in A/P cluster and generated multiple Watchdog snapshots.
PRS-384939	“Invalid EKU text” error found while configuring "E-mail protection" under EKU text.
PRS-384963	Host checker: After upgrading to 9.1R3, HC "Successfully loaded" message is garbled when it is initiated in browser with Japanese language.
PRS-384967	healthcheck.api showing incorrect MAXIMUM-LICENSED-USER-COUNT in AA cluster.
PRS-385144	Web Rewrite: Images not loading on the web page for a web resource configured via rewrite.
PRS-385150	Access via SSH port forwarding fails.
PRS-385159	Home page of eTime (Timesheet) Web application is not rendering properly via Rewrite in all web browsers.
PRS-385203	Add iOS check for 13.2, 13.2.1, 13.2.2.
PRS-385496	Adding default policy for Citrix resources.
PRS-385500	VLS should use only MSP Authcode for registering with PCLS.
PRS-385526	Add iOS Check for 13.2.3.
PRS-385550	Users cannot see full display of shared screen, if the size of text, app and other items in the "Scale & layout" in Display settings is set to 150% (Recommended) on the client's machine.
PRS-385721	Unable to restore Local User Accounts Backup on PCS 9.0R5.

Problem Report Number	Summary
PRS-387517	DanaLoc appears to be missing when using IE11.
PRS-387541	Web Rewrite: Drop-down menu, Refresh button, Change Password option and Login button not working on the login page.
Release 9.1R3 PRs	
PRS-366490	System| Temperature status value on SNMP server displaying wrong value.
PRS-371351	Citrix sessions drop regularly causing various issues. These issues are observed in PCS 9.0 with Citrix port 2598 via JSAM. This issue is not found in 8.2R8.
PRS-371699	Users unable to login as well as dropping users - LMDB full.
PRS-372805	Realm level certificate restriction skipped with SAML Auth.
PRS-372999	Host checker is failing for Host Checker (OS-Check only) for Chrome OS 71.0.3578.127 with PCS 9.0R1 firmware version.
PRS-373160	Dropdown option misses internal menu while accessing via web rewrite.
PRS-374124	VDI Session are not showing under Virtual Desktop Sessions.
PRS-374146	UNC path is not handled properly by HOB Applet.
PRS-374318	PCS deployed on the AWS Cloud showing speed 10 Mbps.
PRS-374344	Last core dumps being generated at customer after 9.0R2.1HF6 with fixes.
PRS-374603	Syslog missing event logging info when upgrading.
PRS-374765	PSA7000f RAID failed after upgrading.
PRS-374831	Login page is not rendering properly for a web resource configured through rewrite.
PRS-374992	PCS using DUO as secondary authentication fails the first authentication attempt after installation.
.PRS-375079	CORE.fqdnacl crashes continues to occur even after 9.0R2.1HF6 (with fix).
PRS-375880	None of the contents in the Azure web portal are loading through rewrite.
PRS-375906	Unable to load a sign-in page getting stuck in loading the web page while accessing a web resource configured through the rewrite.
PRS-376036	PCS evaluation of the custom expression "time.dayOfYear" is not working as expected.
PRS-376247	Factory-reset does not work in 9.1R1 instead it boot up PCS with current image.
PRS-376249	Logon page of SAP fiori portal displayed as blank in IE11 only via rewrite.
PRS-376343	Mails are not getting synced in Native Email Client in iOS when using SA as ActiveSync Proxy due to stale records present and crash is happening in aseproxy-server service.
PRS-376357	When extending Pulse Client sessions, it causes network drop.
PRS-376429	JSAM stuck on loading forever on IE - Java.
PRS-376458	HOB stuck on loading forever on IE - Java.

Problem Report Number	Summary
PRS-376500	Azure 9.0R3.1 - postgresd service restarts constantly after deployment.
PRS-376520	Host checker fails to detect FireEye Endpoint Agent 29.7.0.
PRS-376840	Running Add command when the Disk is missing will cause a minor error message which requires a reboot.
PRS-376869	Dns_cache process snapshots persist after upgrading to 9.0R4HF6.
PRS-376953	Unable to view PDF files in the myDocuments application.
PRS-377022	File Share accessing issue in 9.0R4.
PRS-377160	HTML-5 -RDP requires additional authentication.
PRS-377482	After upgrading to 9.1R1, host checker word is garbled when it is initiated in browser with Japanese language.
PRS-377681	PSA7000f reports HDDs missing and inactive after upgrade to 9.1R1.
PRS-377825	After upgrading to 9.1R1, the name of the user role displayed in submenu is broken if the language is in Korean.
PRS-377979	When accessing the resources via bookmark, contents are not displayed correctly.
PRS-378049	Failed filesystem integrity check message seen on PSA5K console after upgrading from 9.1R1 to 9.1R2-2119.
PRS-378882	Periodic Snapshot settings via REST fails with error "Modification of Attribute not Allowed".
PRS-378964	When the admin clicks on 'Agent', they receive an error "the page you requested could not be found".
PRS-379125	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-379336	Chat option not working on the Medical application.
PRS-379773	Syslog - If an appliance is rebooted, it cannot successfully reconnect to a P1 syslog server.
PRS-379974	Critical Events do not get displayed in System > Overview Page.
PRS-380009	REST API calls failing for RDWeb Profiles in PCS.
PRS-380148	When syslog server's FQDN resolves to two IP addresses, one of which is reachable, PCS/PPS may fail to connect.
PRS-380762	Delay during session failover of PCS in Active/Active cluster in AWS.
PRS-381014	Japanese words are garbled when we click on the File share bookmark.
PRS-381318	DMI get-config of RDWeb resource profile returns badly formed XML.
Release 9.1R2 PRs	
PRS-367907	FQDNST denied IP is going via tunnel.
PRS-370210	Clear config on PSA 300 fails with unable to mount /webserver partition.

Problem Report Number	Summary
PRS-372439	Post failover, session resumption delayed with Pulse Client.
PRS-373290	Clear config on PSA 300 fails with unable to mount /webserver partition.
PRS-375013	Radius OTP as Secondary authentication fails for the Pulse Client.
PRS-375329	HOB failed to launch through Java in IE.
PRS-375886	JSAM launch failing for IE -JAVA.
PRS-376312	Factory reset from VMware VA console does not load the factory reset version and loads the current version.
PRS-376348	VMWare View 5.1 client does not connect after upgrade.
PRS-376859	Premier Java Applet for Terminal Service failed to download .jar file.
PRS-377945	Publishing for certain block types causes many log messages and other side effects.
Release 9.1R1 PRs	
PCS-5064	Remove legacy mode from Active Directory auth. server.
PRS-375534	JSAM Stats value (Bytes count) is not getting displayed in IE - Activex.
PRS-375067	DNS resolution not working for alternate VPN connections.
PRS-374597	The definition update is not listed for Sentinelone product in "epupdate_hist.xml" file.
PRS-374057	Unable to add the resource <userAttr.Framed-Route> in IPV4 address under Split tunneling policy for PCS version 9.0Rx.
PRS-374037	Rewrite: PSAL launching Citrix app multiple times in an infinite loop on all the browsers.
PRS-373948	Contents of a web response are not getting compressed as content encoding header is missing in the response from PCS.
PRS-373769	Host Checker IMC detects the Antivirus Change in the client PC and report it to IMV even when Perform Check every min is set to 0.
PRS-373696	Split tunneling FQDN policy with special character, fails to save.
PRS-370953	Unable to edit word documents hosted on SharePoint 2013 via PTP using MS Edge.
PRS-371023	Resource access dropped (RDP, SSH etc.) intermittently on SAW environment.
PRS-373102	Core Access: E-mail web page getting stuck on "login processing".
PRS-373076	Core Access:Web page shows horizontal scrollbars at the bottom of screen.
PRS-372181	DanaLoc fails in case of old window object reference from a new window object.
PRS-372834	PSAM:Pulse SAM takes at least 40 seconds to open custom start up page in UI Options compared to WSAM.
PRS-372677	AAA/Security/Pulse: SAML AuthnRequest leaks data across users with "Reuse NC/Pulse session" enabled.
PRS-372595	User getting same IP address assigned from IP pool in few hours.

Problem Report Number	Summary
PRS-372489	Pulse browser Toolbar is flickering when accessing OWA 2016 resource on iOS device through webrewrite.
PRS-372285	PSA 7000f Frequently reports one of the power supplies is back up.
PRS-372055	Unable to save Citrix listed application using Hostname with port number.
PRS-371973	HC: Compliance fails using Pulse Desktop client 9.0.2 build 1151.
PRS-371970	Users with username in UPN format in System Local Authserver are unable to log in using TOTP after upgrading to 9.0R3.
PRS-371944	Killed user session admin log "ADM23534" does not display admin user but the actual user being terminated.
PRS-371800	PCS device is unable to get the enrolled mobile device attribute from MDM server.
PRS-371394	Setting the hash property of location object causes problem in IE, Edge and Firefox browsers because the URL is appended with fragment identifier. In chrome and Safari browsers things work fine.
PRS-371602	Post upgrade to PCS 9.0R3, "License server low-level protocol error Code = [47]" error is triggered on license client.
PRS-371513	Page does not load via IE browser.
PRS-371406	"Auto populate domain information" behavior when unchecked: blank first then if wrong password, auto populates domain.
PRS-371357	HTML5 RDP logging do not show realm and shows ().
PRS-371342	Add iOS Check 12.1.1.
PRS-371266	Menu is not loading when accessing the application through web-rewrite.
PRS-371231	PCS 9.0 VA-DTE :: Nodes in cluster gets disabled automatically.
PRS-371205	Multicast Traffic not working intermittently in the VPN Tunnel in 8.3R6 / 5.3R6 version and after restarting services, works fine for all users.
PRS-371154	Wrong information in the log messages for Authorization Only Access when source ip restriction is configured on role.
PRS-371114	Add support for adding parameters “client-name’ for HTML5 Access.
PRS-369351	LDAP authorization does not work when using ikev2 tunnel (handle 10K tunnels+few hundred ikev2 clients).
PRS-370138	Read-only admin sessions see an option as disabled that is actually enabled on user roles.
PRS-369960	Page displayed while PSAL downloads to a Mac client shows instruction for Mac; but then references Windows System Tray.
PRS-369200	Logs are not fully displayed if select the date as filter.
PRS-369142	File browsing SSO is not working with user details are given in variable form as well when configured to use system credentials.

Problem Report Number	Summary
PRS-369031	When a configuration object is renamed, not all of the resulting configuration changes are uploaded to Pulse One.
PRS-368927	Web process crashes and logs "ERR31093: Program web recently failed." in the event logs.
PRS-367879	Core Access: Unable to import or download the image using PTP.
PRS-367789	DMI agent not responding to netconf commands as expected.
PRS-367285	System| Active/Passive cluster responding to ICMP request even after shutdown.
PRS-366634	Randomly users are not able to access IPv6 resources through VPN device via VPN tunneling.
PRS-364219	PSA7000f interface status in Network Settings not working.
PRS-366490	System| Temperature status value on SNMP server displaying wrong value.
PRS-371351	Citrix sessions drop regularly causing various issues. These issues are observed in PCS 9.0 with Citrix port 2598 via JSAM. This issue is not found in 8.2R8.
PRS-371699	Users unable to login as well as dropping users - LMDB full.

Known Issues

Problem Report Number	Release Note
Release 9.1R8 PRs	
PRS-393440	**Symptom:** Host Checker fails with Error "Host checker did not get installed properly. Your computer does not meet requirements" **Condition:** Cache Cleaner policy is enforced on role or realm. **Workaround:** Disable Cache Cleaner policy and restart Pulse services.
PRS-393434	**Symptom:** PCS system clock is going out of sync affecting features that depend on time such as licensing. **Condition:** When PCS is configured to sync the time with NTP servers. **Workaround:** Disable NTP on PCS. Enable "Time Sync with Host" option, if the PSA-V is deployed on VMware ESXi
PRS-393174	**Symptom:** Local proxy PAC file not working in Internet Explorer 11. **Condition:** When PAC file resides on a local system. **Workaround:** Store the PAC file on an HTTP/HTTPS-accessible server and use that link for Internet Explorer 11 proxy settings.
PRS-393172	**Symptom:** Windows client connecting to PCS using Firefox ESR 68.10 intermittently throws error during Compliance check through Proxy configuration. **Condition:** Using Firefox ESR 68.10 version. **Workaround:** Once a successful connection is established from the client to the server using Chrome/IE, try connecting to the server using Firefox ESR. This works as expected.
PRS-393146	**Symptom:** Host Checker process tncs crash. **Condition:** When user role is configured with 120 HC rules and policy check interval is every one minute and with 8K user load. **Workaround:** (Recommended) Increase the Host Checker policy check interval.
PRS-392934	**Symptom:** PCS does not restrict user logins, even though dsagentd crossed 80% CPU utilization. **Condition:** Noticed the issue especially with clusters and when changing from Active-Active to Active-Passive cluster or vice versa. **Workaround:** Restart of System Services should solve the issue.
PRS-392749	**Symptom:** Pulse collaboration client version is not same in Mac and Windows. **Condition:** When user installs 9.1R8 Pulse collaboration client. **Workaround:** None.

Problem Report Number	Release Note
PRS-392345	**Symptom:** Archiving on AWS S3 storage and Azure is failing when DNS server is not reachable from internal interface. **Condition:** When admin trying to Archive using AWS S3 bucket or Azure storage account on management port and DNS server is not reachable through internal port. **Workaround:** Admin has to configure internal port for DNS resolution, Archival interface can be internal/management for archiving on AWS S3 bucket or Azure storage account..
PRS-392236	**Symptom:** Hyper-V 9.1R8 upgrade from earlier versions is not supported. **Condition:** When upgrading from the earlier versions, say 9.1R5. **Workaround:** Install a fresh instance of 9.1R8 and import the config from the earlier version.
PRS-391999	**Symptom:** TOTP Authentication fails for all users. **Condition:** After importing TOTP users into the PCS via REST API. **Workaround:** Use Export and Import option under TOTP Authentication server in Admin UI.
PRS-391947	**Symptom:** Websocket URL is not accessible. **Condition:** When trying to access https://web.whatsapp.com/ URL. **Workaround:** None
PRS-391305	**Symptom:** Upgrading Azure images from 9.1R5 to any later releases returns with error message if the factory reset version is 9.1R5. **Condition:** When factory reset version is 9.1R5. **Workaround:** Export the existing PCS configurations, deploy the new PCS image with the latest version, and import the PCS configurations.
PRS-390577	**Symptom:** Active user page is not displaying node details correctly for the users connected in AA cluster after split and join. **Condition:** After cluster split and re-join. **Workaround:** Display issue, user sessions will not get impacted. Newly connected sessions are showing the details correctly.
PRS-390488	**Symptom:** Host checker is getting timed out (can be seen on user access log) and user is getting logged out. **Condition:** When periodic evaluation is enabled. **Workaround:** This issue is not replicable every time, but as a workaround, we have suggested to disable dynamic evaluation or increase the periodic policy evaluation interval.

Problem Report Number	Release Note
PRS-384976	**Symptom:** Host Checker installation error found Intermittently while installing Host Checker or Pulse Client [HC enabled] through browser [Chromium Edge/Chrome/Firefox]. **Condition:** Fresh Installation of Host Checker or Pulse Client [Host Checker enabled] through browser [Chromium Edge/Chrome/Firefox] after uninstalling old Host Checker components **Workaround:** 1 Uninstall the Host Checker/Pulse Client components manually and reboot the system. OR 2 Manually kill Host Checker process before installing Pulse Client/Host Checker components.
PRS-367366	**Symptom:** When using RADIUS authentication with challenge/token responses, if incorrect username/password is entered for the initial primary authentication, Pulse Client users are shown the OTP prompt (along with custom error message). **Condition:** RADIUS authentication is configured for the users with OTP (Access-challenge / Access-Reject configured) as per the KB26411 **Workaround:** No functionality impact. As the error is displayed, user may ignore the OTP screen and retry login again with correct username/password.
PCS-21262	**Symptom:** Update in PSAM Resource policies configuration from Admin portal is not getting applied immediately to existing users with UDP PSAM sessions. **Condition:** When Admin changes ACL action from Deny to Allow for a particular UDP based resource (i.e., UDP Server Application) for which user already has UDP PSAM Session active, user will still see access denied and vice-versa. But this condition might occur very rarely in real world scenario. **Workaround:** Admin can choose to delete existing UDP PSAM user sessions for which ACL action changes from Deny to Allow and vice-versa. Alternatively, user can disconnect and connect PSAM UDP based application session.
PCS-20664	**Symptom:** Pulse client is not showing correct error message when there is no bandwidth to allocate for L3 tunnel. Error message in Pulse client - "Unable to allocate IP address". **Condition:** When there is no bandwidth to allocate for L3 tunnel for that specific user. **Workaround:** Display issue, correct error message will get displayed in User Access logs. Error message in User Access logs - "Cannot find a qualified bandwidth management policy for user based on current available bandwidth."
Release 9.1R7 PRs	
PCS-20433	**Symptom**: Existing HTML5 active sessions are not displayed under "Active Virtual Desktop Sessions" tab. **Condition**: After cluster upgrade, existing HTML5 sessions are not displayed under "Active Virtual Desktop Sessions" tab. **Workaround**: User has to re-login and connect to HTML5 session.
Release 9.1R6 PRs	

Problem Report Number	Release Note
PCS-19628	**Symptom**: Platform page shows hypervisor information as KVM instead of Alibaba-Cloud-KVM or OpenStack-KVM. **Condition**: This issue is seen only with PCS deployed on Alibaba Cloud and OpenStack hypervisors. **Workaround**: None. There is no functionality loss though. PCS will function without any issues.
Release 9.1R5 PRs	
PRS-390106	**Symptom**: Inconsistent upgrade issues seen while upgrading Hyper-V images in clustering and single node. **Condition**: Upgrading a Hyper-V image to 9.1R5. **Workaround**: If cluster upgrade fails, reboot the node which is not upgraded. If the issue persists, try upgrading the nodes individually and then form cluster.
PRS-389742	**Symptom**: Cannot register the device with Intune to get SCEP profile that has IMEI as common name. **Condition**: The devices like Wi-fi only iPad / Wi-Fi only android tablets that do not have IMEI support or do not have IMEI. **Workaround**: None.
PRS-389737	**Symptom**: Cluster VIP is not getting migrated to other node when active node's internal interface is not reachable and external port is reachable. **Condition**: In AP Cluster configured with both internal and external port, when active node's internal port became unreachable. **Workaround**: Reboot the cluster node having issue with internal interface is unreachable.
PRS-389642	**Symptom**: XML import is failing if configuration file has syslog IPv6 settings. **Condition**: if one of the devices configured IPv6 syslog server on log settings, the XML import will fail on another device if the same XML is exported from first device. **Workaround**: Export the binary system configuration and import on another device.
PRS-389451	**Symptom**: TCPDump fails to capture packets when multiple interfaces are selected. **Condition**: When multiple interface - Internal, External and Management are selected. **Workaround**: Select individual interface to capture packets using TCPDump.
PRS-389409	**Symptom**: User sessions will be removed for the session logged in at the time of second node upgrade in AP cluster. **Condition**: During AP cluster upgrade, when the first node comes up after upgrading newer version, it informs other node to upgrade. During this time if any new user logs in, then all those sessions will be removed after second node goes for upgrade. **Workaround**: User needs to re-login.

Problem Report Number	Release Note
PRS-388121	**Symptom**: Reliable users may be prompted for secondary authentication despite Adaptive authentication being enabled for the realm. **Condition**: Adaptive Authentication feature may not work in some scenarios where nodes are in the cluster setup. **Workaround**: None.
Release 9.1R4.3 PRs	
No new known issues for this release	
Release 9.1R4.2 PRs	
No new known issues for this release	
Release 9.1R4.1 PRs	
No new known issues for this release	
Release 9.1R4 PRs	
PCS-18480	**Symptom**: Bookmark based access flow for Cloud based apps does NOT support MFA. **Condition**: When user tries to access any Cloud apps using Bookmark based flow, MFA based Conditional Access policies does Not work and will Deny the access to user. **Workaround**: Access Cloud apps using SP Initiated flow for MFA to work, or do NOT configure MFA for these Bookmark based Cloud apps.
PCS-18217	**Symptom**: License report did not show proper values for older dates (Dec month) after upgrading to 9.1R4 image. **Condition**: License report generated from License server running with lesser than 9.1R4 version will have older data (For example: Dec-2019) and after upgrading the license sever to 9.1R4 image, data for older months will not be accurate. **Workaround**: None
PCS-18002	**Symptom**: Pulse Collaboration meeting is not getting launched with PSAL in macOS Catalina from the second time. **Condition**: In macOS Catalina, Pulse Collaboration meeting can be launched only after the fresh download of the client. If we try to relaunch the meeting, it is getting failed. **Workaround**: Delete the Pulse Collaboration client folder and perform a fresh download before launching the meeting.
PCS-17932	**Symptom**: TOTP server, Certificate server and SAML server authentication do not work for MFA based Conditional Access policy settings. **Condition**: When TOTP server, Certificate server and SAML server are configured as MFA server for Conditional Access. **Workaround**: Any other supported Authentication server can be configured as MFA server.

Problem Report Number	Release Note
PCS-17926	**Symptom**: License report doesn't show the software version for one of the members cluster setup. **Condition**: When cluster is in license client **Workaround**: None (Display issue).
PRS-387697	**Symptom**: HOB launch on CentOS failing when Oracle JDK is installed. **Condition**: Oracle JDK installed on CentOS. **Workaround**: Install OpenJDK.
PRS-387572	**Symptom**: AliCloud PCS-7K-V: Watchdog restarting cgi-server auth processes (cgi). **Condition**: Beyond 20K concurrent users under Pulse ESP and PSAM throughput test. **Workaround**: None
PRS-387499	**Symptom**: Hob auto-launch - PSAL failing with error "Failed to contact server". **Condition**: When auto-launch is enabled on HOB bookmark. **Workaround**: Disable auto-launch.
PRS-387452	**Symptom**: SSH does not work after restarting services in AWS and Azure. **Condition**: After performing restart services. **Workaround**: SSH works after a reboot.
PRS-387192	**Symptom**: Rewriter issues with SharePoint 2019 – a few buttons and icons does not load and rename file does not work. **Condition**: When using PCS web bookmark for the new SharePoint 2019 server. **Workaround**: Switch to Classic View in SharePoint 2019.
PRS-384976	**Symptom**: Host Checker error found Intermittently while installing Pulse Client via Chromium Edge browser in presence of Host Checker configured. **Condition**: Host Checker configured. **Workaround**: Click on Ignore button.
Release 9.1R3 PRs	
PCS-15327	**Symptom**: When trying to restart PCS from vCenter, PCS shuts down instead of restart. **Condition:** When trying to restart PCS using the Restart Guest option from vCenter. **Workaround**: Restart PCS using the PSA-V virtual console.
PRS-382259	**Symptom**: DNS address and domain names are taken from DHCP server when deploying new PCS instance in AWS and Azure. **Condition:** When passing DNS address and domain name as parameter for initial configuration, DNS address and domain name are taken from DHCP server. **Workaround**: Reconfigure DNS address and domain in network over view page.

Problem Report Number	Release Note
PRS-382085	**Symptom**: Not able to enable "copy/paste" option for end user created bookmarks after upgrade from 9.1R2 to 9.1R3. **Condition:** After an upgrade, not able to enable "copy/paste" option in the end user created bookmarks. **Workaround**: The user has to delete and create the bookmarks to enable "copy/paste" option.
PRS-382083	**Symptom**: Not able to enable "copy/paste" option via RDP launcher URL. **Condition:** When trying to enable "Copy/paste" option via RDP launcher URL. **Workaround**: • User should use admin created bookmark. • User should use end-user created bookmark.
PRS-382078	**Symptom**: AWS or Azure new PCS deployment fails when customer using old templates with admin password is less than 10 characters. **Condition:** When the template contains admin password with less than 10 characters. **Workarounds**: Customer has to provide admin password length with minimum of 10 characters.
PRS-382021	**Symptom**: Dismiss until next upgrade option is not working for banner related to perpetual licensing. **Condition:** Admin clicks on Dismiss until next upgrade. **Workaround**: Use the Close button for temporary solution.
PRS-381990	**Symptom**: During peak hours when multiple users try to do browser-based login on PSA5K, a few users might not be able to connect in the very first attempt. **Condition:** When PCS is upgraded to 9.1R3 on PSA5K. **Workaround**: When the failed user tries to reconnect, the login will happen successfully.
PRS-381853	**Symptom**: Azure PCS - Network interface speed is showing as “Unknown” in the Network Overview page. **Condition:** When deploying new PCS instance in Azure, the network interface speed is showing as “Unknown” in the Network Overview page. **Workaround**: This is just a display issue.
PRS-381707	**Symptom**: Intermittently, Behavioral analytics dashboard page shows "Unable to connect to database" error. **Condition:** Sometimes, when admin navigates to Behavioral analytics dashboard page, "Unable to connect to database" error is seen. **Workaround**: Administrator can reload the Behavioral analytics dashboard page after some time to get the details on the page.
PRS-381579	**Symptom**: Sometimes logs are not shown under Log/Monitoring page. **Condition:** Not applicable. **Workaround**: Refresh the page or click on the Update button on the logs page.

Problem Report Number	Release Note
PRS-381554	**Symptom**: When File rule configured for validating a file location using System default Directories <%HOME%> policy evaluation failed on macOS 10.14x or any higher versions. **Condition:** If file located at System Directories <%HOME%> and configured a Hostcheck policy with File Rule for macOS 10.14.x or higher versions. **Workaround**: Need to add permissions for "Pulse Client" under "Accessibility" and "Full Disk Access" and which can be accessed from "System Preferences" > "Security & Privacy"-> "Privacy Or without providing permission /tmp location can be used for File validation.
PRS-381403	**Symptom**: Sharing Feature is not working in macOS Catalina. **Condition:** When Attendee Joined in Pulse Collaboration meeting via macOS Catalina, Attendee cannot share the Desktop. But Attendee can view the Presenter's screen. **Workaround**: None
PRS-367403	**Symptom**: Pulse collaboration not getting launched in macOS. **Condition:** When the Java version above 8 is installed in the macOS, Pulse collaboration will not launch. **Workaround**: Use Java version 8 for launching the Pulse collaboration in macOS.
Release 9.1R2 PRs	
PRS-14530	**Symptom**: Shutdown of PSA-V deployed on KVM hypervisor does not complete. **Conditions**: • PSA-V is deployed on KVM hypervisor. • Shutdown is initiated from PSA-V virtual console. **Workaround**: None
PRS-361501	**Symptom**: Sometimes end-user is unable to access backend resources. **Conditions**: 1 PCS is deployed as an AP cluster. 2 Admin has configured VLAN source IP under User Roles. 3 VIP changes from active node to passive node. **Workaround**: Log out and then log back in as an end user.
PRS-374575	**Symptom**: DNS Search Order notes for macOS needs correction as Device only DNS is supported in macOS. **Condition**: macOS supports Device only DNS. **Workaround**: None
PRS-377549	**Symptom**: Older PSIS is not upgrading to 9.1R2 PSIS version. **Condition**: When CTS, WTS and VDI gets upgraded to 9.1R2 in Windows 10 Redstone 5 and later, PSIS is not upgraded to latest version. **Workaround**: None. Old PSIS will continue to work and no impact seen.

Problem Report Number	Release Note
PRS-377700	**Symptom**: Using REST API - Archiving Schedule settings change from hourly to specified time does not update the hour/minute setting. **Condition**: None **Workaround**: Apply the same API again the second time.
PRS-378101	**Symptom**: JSAM fails to launch on Mac OS Catalina 10.15. **Conditions**: • Configured a role with Host checker. • Configured JSAM access with auto-launch. **Workaround**: None
PRS-379014	**Symptom**: After single logout with PCS as SP, the SP lands on either IdP page or SP page. **Condition**: PCS is configured as IdP and another PCS configured as SP with single logout enable. **Workaround**: None.
Release 9.1R1 PRs	
PRS-362240	**Symptom**: User sees detect receiver window rather than PSAL download page upon clicking the apps. **Conditions**: Users are unable to launch Citrix Apps/Desktop that are published in storefront. **Workaround**: • Forward the Cookie: CtxsClientDetectionDone=true as name value pair in SSO form or using custom header policies. • Re-click the bookmark by returning to home page and access the SF application again.
PRS-373014	**Symptom**: Virtual Appliance platform license activated message seen every 10 mins in Admin logs. **Conditions**: • Admin has installed Virtual Appliance platform license through authorization codes. • Admin has also leased cores from a license server. **Workaround**: Delete the installed Virtual Appliance platform license (as the cores are provided by license server).
PRS-373762	**Symptom**: Named User Remote Repo (NURR) mode does not work when MSSP unlimited license is installed on the License server. **Condition**: MSSP Unlimited License installed on License server. **Workaround**: Pulse Secure advises MSSP customers with MSSP SKU to not use NURR mode.
PRS-374091	**Symptom**: All client installations fail when using auth proxy in MAC OS. **Condition**: Client installations in MAC OS using auth proxy. **Workaround**: None

Problem Report Number	Release Note
PRS-374458	**Symptom**: Fresh deployment of Azure image on PCS is not available. **Condition**: Fresh deployment of Azure image on PCS. **Workaround**: Upgrade the server. A new image will be posted soon.
PRS-374790	**Symptom**: Unable to edit Power Point files within any browser from Share Point 2016 server. **Condition**: In Rewriter mode of browsing Share Point 2016 server. **Workaround**: Create Custom Header Allow policy for the Share Point URL.
PRS-375051	**Symptom**: Unable to edit existing client to increase or decrease the number of cores leased via REST/XML. **Condition**: Observed in REST PUT request and XML import. **Workaround**: Use the UI to make changes.
PRS-375138	**Symptom**: Client upload logs fails for Network Connect and JSAM. **Condition**: After launching Network Connect and JSAM on Windows 10, client upload log fails. **Workaround**: None
PRS-376021	**Symptom**: Intermittently end-user gets "Detected an Internal error" while logging into a browser-based session. **Condition**: When end-user tries to log in to Pulse Connect Secure through Safari browser on Mac. **Workaround**: Reboot the Mac laptop
PRS-376245	**Symptom**: HOB and JSAM not working in Linux. **Condition**: When end user tries to launch HOB and JSAM on Linux platform. **Workaround**: None
PCS-11922	**Symptom**: DNS Port selection will not take any effect. DNS traffic will go through Internal Port only. **Condition**: On a PCS Virtual Appliance, when Administrative Network is enabled under Traffic Segregation. This issue is not applicable for PSA Hardware Devices. **Workaround**: None
PCS-12383	**Symptom**: SNAT functionality failed to work even when it is enabled post the fresh deployment. **Condition**: In cloud instance (Azure/AWS), admin enables the NAT behavior from its initial disabled state and sees the NAT functionality failed to work. **Workaround**: PCS needs to be rebooted from the portal post the deployment.
Cloud Secure	
PRS-371781	**Symptom**: Blocked ECP users will not be updated if Generic is selected under LDAP server Type. **Condition**: LDAP server type selected is Generic. **Workaround**: Select the LDAP server type as Active Directory.

Problem Report Number	Release Note
PRS-372846	**Symptom**: Blocked ECP users will have a "Blocked till time" of 5 minutes. **Condition**: Request count for a particular user is less than 3. **Workaround**: None
PRS-372861	**Symptom**: Blocked ECP users will not be removed from the ECP reports page based on "Blocked till time". **Condition**: When a user entry is present in the ECP reports page. **Workaround**: None

Documentation

Pulse documentation is available at https://www-prev.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

Call us at 1- 844-751-7629 (toll-free USA)

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