Pulse Connect Secure

Release Notes

PCS 9.1R4.2 Build 5035.1

PDC 9.1R4.2 Build 1955

Default ESAP Version: ESAP 3.4.8

Release, Build	**9.1R4.2, Build 5035.1**
Published	**June 2020**
Document Version	**4.2.1**

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

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
4.2.1	June 2020	Updated the 9.1R1 Fixed Issues section with PRS-368927
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 9.1R4.2. 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)
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

y: Any release version

Upgrade From	Qualified	Compatible
9.1R3	Yes	-
9.1R2	-	Yes
9.1R1	-	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 or 9.0Rx|9.0Ry, and then upgrade to 9.1R4.2.

Note: If your system is running beta software, roll back to your previously installed official software release before you upgrade to 9.1R4.2. 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 9.1R4.2 without a core license installed. Follow these steps to upgrade to 9.1R4.2:

1. If PSA-V is running 8.2Rx:
   a. Upgrade to 8.3R3 or later.
   b. Install Core license through Authcode.
   c. Upgrade to 9.1R4.2.
2. If PSA-V is running 8.3R1:
   a. Upgrade to 8.3R3 or later.
   b. Install Core license through Authcode.
   c. Upgrade to 9.1R4.2.
3. If PSA-V is running 8.3R3 or later:
   a. Install Core License through Authcode.
   b. Upgrade to 9.1R4.2.

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 9.1R4 is 3.2.7 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.

New Features

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

Feature	Description
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, device and location 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.

Feature	Description
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.
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.
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.

Feature	Description
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 to be 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.
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

The following table lists issues that are fixed in the corresponding release.

Problem Report Number	Summary
Release 9.1R4.2 PRs	
Pulse Connect Secure	
PRS-380298	Summary: User Access log indicates "Login failed using Auth. server LDAP server (Failed: unable to verify the first certificate)" for wrong password.
PRS-387780	Summary: Registered PCS Appliance fails with Pulse One communication after importing user config and shows "Registration Expired" error message.
Release 9.1R4.1 PRs	
Pulse Connect Secure	
PRS-382268	Summary: PDC throws Authentication rejected by server [Error : 1319] when using global PCS url.
PRS-387062	Summary: PSAM sending unintended traffic via tunnel to VPN in 9.1R3.
Release 9.1R4 PRs	
Pulse Connect Secure	
PRS-365669	Summary: SNMP: ifAdEntAddr mapped to wrong ifAdEntIndex values.
PRS-367786	Summary: Device locked up and dropped all connections due to Web process consuming CPU.
PRS-375181	Summary: VLS does not throw any error if there is no response for Heartbeats sent to PCLS.
PRS-377456	Summary: EasyPrint feature using the Premier Java RDP Applet not working.
PRS-379345	Summary: Program dsagentd recently failed. Need RCA.
PRS-379801	Summary: Active Sync stopped working after upgrading the device to 9.0R4.
PRS-380136	Summary: Cluster communication and state storage problems on A/A cluster.
PRS-380765	Summary: Program dsagentd recently failed after upgrading PCS from 9.0R3.2 to 9.0R4.
PRS-380796	Summary: PCS-VA sending critical SNMP alerts while leasing license.
PRS-380993	Summary: DFS: process snapshot generated by snmptrap process.
PRS-381100	Summary: 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	Summary: Multiple users getting disconnected from Pulse Client.
PRS-381403	Summary: Sharing Feature is not working in macOS Catalina.
PRS-381579	Summary: Sometimes empty logs are seen under "Log/Monitoring".
PRS-381621	Summary: 9.0R4 and 9.0R5 SPE (PSA-V) do not show the User Record Sync column in Admin UI > Auth Server page.
PRS-381633	Summary: Host Checker checking for virus definition file based on Number of updates fails for Sophos Endpoint Security and Control 10.8.4.
PRS-381736	Summary: After Upgrade from 8.3R7.1 to 9.1R1, error encountered while upgrading cache (in Host Checker).
PRS-381795	Summary: [FQDN ACL / NFQUEUE] Request DEV help in determining why thousand of VPN Tunnels dropped traffic within.
PRS-381960	Summary: Facing slowness when accessing web application through Authorization-only access post upgrading to PCS OS 9.0R5.
PRS-381963	Summary: 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	Summary: https://dev.pulsesecure.net/jira/browse/PRS-362240: the cookie setting should be included in the resource profile.
PRS-382001	Summary: UI: Description incorrect on default deny in 9.1R3 initial deployment.
PRS-382021	Summary: Button to dismiss the banner on PPS/PCS Dashboard for not accepting Perpetual license is not working.

PRS-382031	**Summary**: Need to replace VA-SPE|PSA-V in "Only EVAL licenses are allowed for manual installation in VA-SPE|PSA-V".
PRS-382035	**Summary**: Proper logging for NFQUEUE full and drops needed, also consider this situation for cluster A/P failover or add to healthcheck.
PRS-382191	**Summary**: Unable to ping the IPv6 VLAN-Gateway from the PCS device after changing the Gateway address.
PRS-382240	**Summary**: User dropped from the VPN tunnel connection ##g_dhcp_proxy_wbuf is maxed!.
PRS-382350	**Summary**: Unknown RAID status in PSA7000f due to no space left on device.
PRS-382804	**Summary**: Active node went unresponsive in A/P cluster and generated multiple Watchdog snapshots.
PRS-384939	**Summary**: “Invalid EKU text” error found while configuring "E-mail protection" under EKU text.
PRS-384963	**Summary**: Host checker: After upgrading to 9.1R3, HC "Successfully loaded" message is garbled when it is initiated in browser with Japanese language.
PRS-384967	**Summary**: healthcheck.api showing incorrect MAXIMUM-LICENSED-USER-COUNT in AA cluster.
PRS-385144	**Summary**: Web Rewrite: Images not loading on the web page for a web resource configured via rewrite.
PRS-385150	**Summary**: Access via SSH port forwarding fails.
PRS-385159	**Summary**: Home page of eTime (Timesheet) Web application is not rendering properly via Rewrite in all web browsers.
PRS-385203	**Summary**: Add iOS check for 13.2, 13.2.1, 13.2.2.
PRS-385496	**Summary**: Adding default policy for Citrix resources.
PRS-385500	**Summary**: VLS should use only MSP Authcode for registering with PCLS.
PRS-385526	**Summary**: Add iOS Check for 13.2.3.
PRS-385550	**Summary**: 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	**Summary**: Unable to restore Local User Accounts Backup on PCS 9.0R5.
PRS-387517	**Summary**: DanaLoc appears to be missing when using IE11▯.
PRS-387541	**Summary**: Web Rewrite: Drop-down menu, Refresh button, Change Password option and Login button not working on the login page.
Release 9.1R3 PRs	
Pulse Connect Secure	
PRS-366490	**Summary**: System| Temperature status value on SNMP server displaying wrong value.
PRS-371351	**Summary**: 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	**Summary**: Users unable to login as well as dropping users - LMDB full.
PRS-372805	**Summary**: Realm level certificate restriction skipped with SAML Auth.
PRS-372999	**Summary**: 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	**Summary**: Dropdown option misses internal menu while accessing via web rewrite.
PRS-374124	**Summary**: VDI Session are not showing under Virtual Desktop Sessions.
PRS-374146	**Summary**: UNC path is not handled properly by HOB Applet.
PRS-374318	**Summary**: PCS deployed on the AWS Cloud showing speed 10 Mbps.
PRS-374344	**Summary**: Last core dumps being generated at customer after 9.0R2.1HF6 with fixes.
PRS-374603	**Summary**: Syslog missing event logging info when upgrading.
PRS-374765	**Summary**: PSA7000f RAID failed after upgrading.
PRS-374831	**Summary**: Login page is not rendering properly for a web resource configured through rewrite.
PRS-374992	**Summary**: PCS using DUO as secondary authentication fails the first authentication attempt after installation.
.PRS-375079	**Summary**: CORE.fqdnacl crashes continues to occur even after 9.0R2.1HF6 (with fix).
PRS-375880	**Summary**: None of the contents in the Azure web portal are loading through rewrite.
PRS-375906	**Summary**: 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	**Summary**: PCS evaluation of the custom expression "time.dayOfYear" is not working as expected.
PRS-376247	**Summary**: Factory-reset does not work in 9.1R1 instead it boot up PCS with current image.
PRS-376249	**Summary**: Logon page of SAP fiori portal displayed as blank in IE11 only via rewrite.
PRS-376343	**Summary**: 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	**Summary**: When extending Pulse Client sessions, it causes network drop.
PRS-376429	**Summary**: JSAM: JSAM stuck on loading forever on IE - Java.
PRS-376458	**Summary**: HOB: HOB stuck on loading forever on IE - Java.
PRS-376500	**Summary**: Azure 9.0R3.1 - postgresd service restarts constantly after deployment.
PRS-376520	**Summary**: Host checker fails to detect FireEye Endpoint Agent 29.7.0.
PRS-376840	**Summary**: Running Add command when the Disk is missing will cause a minor error message which requires a reboot.
PRS-376869	**Summary**: Dns_cache process snapshots persist after upgrading to 9.0R4HF6.
PRS-376953	**Summary**: Unable to view PDF files in the myDocuments application.
PRS-377022	**Summary**: File Share accessing issue in 9.0R4.
PRS-377160	**Summary**: HTML-5 -RDP requires additional authentication.
PRS-377482	**Summary**: After upgrading to 9.1R1, host checker word is garbled when it is initiated in browser with Japanese language.
PRS-377681	**Summary**: PSA7000f reports HDDs missing and inactive after upgrade to 9.1R1.
PRS-377825	**Summary**: After upgrading to 9.1R1, the name of the user role displayed in submenu is broken if the language is in Korean.
PRS-377979	**Summary**: When accessing the resources via bookmark, contents are not displayed correctly.
PRS-378049	**Summary**: Failed filesystem integrity check message seen on PSA5K console after upgrading from 9.1R1 to 9.1R2-2119.
PRS-378882	**Summary**: Periodic Snapshot settings via REST fails with error "Modification of Attribute not Allowed".
PRS-378964	**Summary**: When the admin clicks on 'Agent', they receive an error "the page you requested could not be found".
PRS-379125	**Summary**: 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	**Summary**: Chat option not working on the Medical application.
PRS-379773	**Summary**: Syslog - If an appliance is rebooted, it cannot successfully reconnect to a P1 syslog server.
PRS-379974	**Summary**: Critical Events do not get displayed in System > Overview Page.
PRS-380009	**Summary**: REST API calls failing for RDWeb Profiles in PCS.
PRS-380148	**Summary**: When syslog server's FQDN resolves to two IP addresses, one of which is reachable, PCS/PPS may fail to connect.
PRS-380762	**Summary**: Delay during session failover of PCS in Active/Active cluster in AWS.
PRS-381014	**Summary**: Japanese words are garbled when we click on the File share bookmark.
PRS-381318	**Summary**: DMI get-config of RDWeb resource profile returns badly formed XML.
Release 9.1R2 PRs	
Pulse Connect Secure	
PRS-367907	**Summary**: FQDNST denied IP is going via tunnel.
PRS-370210	**Summary**: Clear config on PSA 300 fails with unable to mount /webserver partition.
PRS-372439	**Summary**: Post failover, session resumption delayed with Pulse Client.
PRS-373290	**Summary**: Clear config on PSA 300 fails with unable to mount /webserver partition.
PRS-375013	**Summary**: Radius OTP as Secondary authentication fails for the Pulse Client.
PRS-375329	**Summary**: HOB failed to launch through Java in IE.
PRS-375886	**Summary**: JSAM launch failing for IE -JAVA.
PRS-376312	**Summary**: Factory reset from VMware VA console does not load the factory reset version and loads the current version.

PRS-376348	**Summary**: VMWare View 5.1 client does not connect after upgrade.
PRS-376859	**Summary**: Premier Java Applet for Terminal Service failed to download .jar file.
PRS-377945	**Summary**: Publishing for certain block types causes many log messages and other side effects.
Release 9.1R1 PRs	
Pulse Connect Secure	
PCS-5064	**Summary**: Remove legacy mode from Active Directory auth. server.
PRS-375534	**Summary**: JSAM Stats value (Bytes count) is not getting displayed in IE - Activex.
PRS-375067	**Summary**: DNS resolution not working for alternate VPN connections.
PRS-374597	**Summary**: The definition update is not listed for Sentinelone product in "epupdate_hist.xml" file.
PRS-374057	**Summary**: Unable to add the resource <userAttr.Framed-Route> in IPV4 address under Split tunneling policy for PCS version 9.0Rx.
PRS-374037	**Summary**: Rewrite: PSAL launching Citrix app multiple times in an infinite loop on all the browsers.
PRS-373948	**Summary**: Contents of a web response are not getting compressed as content encoding header is missing in the response from PCS.
PRS-373769	**Summary**: Host Checker IMC detects the Antivirus Change in the client PC and report it to IMV even when Perform Check every min is set to 0.
PRS-373696	**Summary**: Split tunneling FQDN policy with special character, fails to save.
PRS-370953	**Summary**: PTP: Unable to edit word documents hosted on SharePoint 2013 via PTP using MS Edge.
PRS-371023	**Summary**: Resource access dropped (RDP, SSH etc.) intermittently on SAW environment.
PRS-373102	**Summary**: Core Access: E-mail web page getting stuck on "login processing".
PRS-373076	**Summary**: Core Access:Web page shows horizontal scrollbars at the bottom of screen.
PRS-372181	**Summary**: DanaLoc fails in case of old window object reference from a new window object.
PRS-372834	**Summary**: PSAM:Pulse SAM takes at least 40 seconds to open custom start up page in UI Options compared to WSAM.
PRS-372677	**Summary**: AAA/Security/Pulse: SAML AuthnRequest leaks data across users with "Reuse NC/Pulse session" enabled.
PRS-372595	**Summary:** User getting same IP address assigned from IP pool in few hours.
PRS-372489	**Summary:** Pulse browser Toolbar is flickering when accessing OWA 2016 resource on iOS device through webrewrite.
PRS-372285	**Summary:** PSA 7000f Frequently reports one of the power supplies is back up.
PRS-372055	**Summary:** Unable to save Citrix listed application using Hostname with port number.
PRS-371973	**Summary:** HC: Compliance fails using Pulse Desktop client 9.0.2 build 1151.
PRS-371970	**Summary:** Users with username in UPN format in System Local Authserver are unable to log in using TOTP after upgrading to 9.0R3.
PRS-371944	**Summary:** Killed user session admin log "ADM23534" does not display admin user but the actual user being terminated.
PRS-371800	**Summary:** PCS device is unable to get the enrolled mobile device attribute from MDM server.
PRS-371394	**Summary:** Setting the hash property of location object causes problem in IE, Edge and Firefox browsers because the URL is appended with fragment identifier. In chrome and Safari browsers things work fine.
PRS-371602	**Summary:** Post upgrade to PCS 9.0R3, "License server low-level protocol error Code = [47]" error is triggered on license client.
PRS-371513	**Summary:** Page does not load via IE browser.
PRS-371406	**Summary:** "Auto populate domain information" behavior when unchecked: blank first then if wrong password, auto populates domain.
PRS-371357	**Summary:** HTML5 RDP logging do not show realm and shows ().
PRS-371342	**Summary:** Add iOS Check 12.1.1.
PRS-371266	**Summary:** Menu is not loading when accessing the application through web-rewrite.
PRS-371231	**Summary:** PCS 9.0 VA-DTE :: Nodes in cluster gets disabled automatically.
PRS-371205	**Summary:** Multicast Traffic not working intermittently in the VPN Tunnel in 8.3R6 / 5.3R6 version and after restarting services, works fine for all users.

PRS-371154	**Summary:** Wrong information in the log messages for Authorization Only Access when source ip restriction is configured on role.
PRS-371114	**Summary:** Add support for adding parameters "client-name' for HTML5 Access.
PRS-369351	**Summary:** LDAP authorization does not work when using ikev2 tunnel (handle 10K tunnels+few hundred ikev2 clients).
PRS-370138	**Summary:** Read-only admin sessions see an option as disabled that is actually enabled on user roles.
PRS-369960	**Summary:** Page displayed while PSAL downloads to a Mac client shows instruction for Mac; but then references Windows System Tray.
PRS-369200	**Summary:** Logs are not fully displayed if select the date as filter.
PRS-369142	**Summary:** File browsing SSO is not working with user details are given in variable form as well when configured to use system credentials.
PRS-369031	**Summary:** When a configuration object is renamed, not all of the resulting configuration changes are uploaded to Pulse One.
PRS-368927	**Summary:** Web process crashes and logs "ERR31093: Program web recently failed." in the event logs.
PRS-367879	**Summary:** Core Access: Unable to import or download the image using PTP.
PRS-367789	**Summary:** DMI agent not responding to netconf commands as expected.
PRS-367285	**Summary**: System| Active/Passive cluster responding to ICMP request even after shutdown.
PRS-366634	**Summary:** Randomly users are not able to access IPv6 resources through VPN device via VPN tunneling.
PRS-364219	**Summary:** PSA7000f interface status in Network Settings not working.

Known Issues

The following table lists known issues in the corresponding release.

Problem Report Number	Release Note
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	
Pulse Connect Secure	
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.

Problem Report Number	Release Note
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.
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-385027	Symptom: VDI Bookmark would not establish connection to the VDI resource. Condition: Without host entry or name resolution of VDI Server on client machine. Workaround: Client machine should be able to resolve to VDI server hostname via DNS or host entry.
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	
Pulse Connect Secure	
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.
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.

Problem Report Number	Release Note
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-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-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-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	
Pulse Connect Secure	
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	
Pulse Connect Secure	
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
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

Problem Report Number	Release Note
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.
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/**