Pulse Connect Secure

Release Notes
PCS 8.3R3 Build 59199.1
Default ESAP Version: ESAP 3.0.3

Release, Build	**8.3R3, 59199.1**
Published	**December, 2017**
Document Version	**5.0**

Pulse Secure, LLC

2700 Zanker Road, Suite 200

San Jose, CA 95134 **https://www.pulsesecure.net**

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at **https://www.pulsesecure.net/support/eula**. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

Introduction

This document is the release notes for Pulse Connect Secure Release 8.3R3. This document contains information about what is included in this software release: supported features, feature changes, unsupported features, known issues, and resolved issues. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

Hardware Platforms

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

- MAG2600, MAG4610, MAG6610, MAG6611, MAG SM160, MAG SM360
- PSA300, PSA3000, PSA5000, PSA7000F, PSA7000C

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

Virtual Appliance Editions

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

- Demonstration and Training Edition (DTE)
- Service Provider Edition (SPE)

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

Table 1 Virtual Appliance Editions

Platform	Qualified System
VMware	• HP ProLiant DL380 G5 with Intel(R) Xeon(R) CPU • ESXi 6.0, 5.5U3, 5.5
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 2012 R2
Microsoft Azure	• Azure Resource Manager

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

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
8.3Rx	Yes	
8.3Ry		Yes
8.2Rx	Yes	-
8.2Ry	-	Yes
8.1Rx	Yes	-
8.1Ry	-	Yes

For Versions Earlier than 8.1:

- First upgrade to release 8.1Rx|8.1Ry or 8.2Rx|8.2Ry, and then upgrade to 8.3Rx.

Note: If your system is running Beta software, roll back to your previously installed official software release before you upgrade to 8.3R3. 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 VA-SPE/PSA-V from 8.3-based OVF, when any of the following conditions are met:

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

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 SHA-2 code signing certificate to improve security and ensure compatibility with Microsoft OS's 2016 restrictions on SHA-1 code signing. This certificate will expire on Jan 13, 2019.

   Important note: Windows 7 machines must contain a March 10, 2015 Windows 7 Update in order to be able to accept and verify SHA-2-signed binaries properly. This Windows 7 update is described **here** and **here**. If this update is not installed (in other words if a Windows 7 machine has not received an OS update since March 10, 2015), then 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).
3. When custom ciphers are selected, there is a possibility that some ciphers are not supported by the web browser. Also, if any of ECDH/ECDSA ciphers are selected, they require ECC certificate to be mapped to the internal/external interface. If ECC certificate is not installed, admin may not be able to login to the box. The only way to recover from this situation is to connect to the system console and select option 8 to reset the SSL settings from the console menu. Option 8 resets the SSL setting to its default. So, the previously set SSL settings are lost. This is applicable only to Inbound SSL settings.
4. Pre-5.0 Android and pre-9.1 iOS devices don't support Suite B ciphers. So 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.

New Features in 8.3R3 Release

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

Feature	Description
Support for REST APIs (Framework and Config APIs	Enables retrieving, adding, updating and deleting configuration of PCS device through REST API calls (GET, POST, PUT and DELETE)
PSAL support for HOB & JSAM	PSAL is used to launch the following clients in the absence of the JAVA plugin support in Firefox, Chrome and MS Edge 1. HOB premiere Applet 2. Java Secure Application Manager
Log the events for any access before authentication in PCS	Enables to log all web requests to PCS before authentication.
HOB JWT Upgrade	HOB JWT applet version has been upgraded to 4.1.0794
FIPS 140-2 Level 1 compliance	Pulse Connect Secure on the PSA series appliances are now validated for FIPS 140-2 Level 1 compliance. Federal agencies protecting sensitive government data using cryptographic modules are mandated to use FIPS 140-2 validated technology. Pulse Secure MAG series appliances are already validated. For details, refer: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2017.htm#2896
VLAN Support for all interfaces	All egress traffic from PCS on internal/external/management interfaces can be optionally tagged with a VLAN ID to reduce external switch configuration overhead. This feature is currently supported only with IPv4 and on stand-alone device.
VA-SPE/PSA-V Licensing via PCLS (on-prem and in public IaaS clouds)	- Enables VA-SPE/PSA-V to obtain licenses from PCLS using authcodes. Hence, VMware VA can get licenses without the need of a physical/virtual license server - Send periodic Heartbeat messages every 12 hours to PCLS for auditing purpose. • If VA-SPE/PSA-V is not able to contact PCLS for more than 30 days, all installed licenses will get disabled. • The licenses will get re-enabled when the VA-SPE/PSA-V is able to establish communication with PCLS(through authcodes or through heartbeat) Note: • VA-SPE/PSA-V should be able to connect to pcls.pulseone.net on port 443 to download license keys and sending heartbeats • This feature is supported on VA-SPE/PSA-Vs deployed on hypervisors (VMware ESXi, Hyper-V and Azure) except KVM Hypervisor.

Feature	Description
Granular RADIUS accounting for roaming sessions	Customer's service uses RADIUS accounting to determine billing for mobile clients and allows for access on cellular & WiFi connections The current design uses the Acct-Multi-Session-Id attribute to link together the multiple related sessions of a roaming client. Each roaming session of the client gets a unique Acct-Session-ID. We send accounting packages for a roaming session only when it terminates, but not with the interim updates. The interim updates only contain accounting for the Acct-Multi-Session-Id, and not for the individual roam sessions (e.g. the Acct-Session-ID). Without the interim updates containing granular roaming data consumption, a client that has roamed from, say WiFi to a pre-paid cellular plan may end up consuming more data than allowed as the service provider only gets the accounting information at the end of the roaming session but not during it.
Cloud-VPN hosted in Azure	VPN as a service to be hosted on Azure as a IaaS offering. Deployment using JSON template. In the current release following templates will be provided. • Deploy PCS along with required network and security policies infrastructure in Azure. • Deploy PCS with existing virtual network Deployed PCS will have three interfaces configured. IP configuration for all three interfaces are configured automatically. From the azure portal following operation are supported. • Start • Stop • Restart • Move across resource groups. Most of the existing features of Pulse Connect Secure are supported, Please refer deployment guide to get info on the features which are not supported.
LMDB user sessions sync in Cluster	Initiating bulk session sync when a node rejoins after a cluster split. Sessions will be synchronized from active node to passive node.
IKEv2 phase 2 SHA2 support	SHA256 Authentication is supported during ESP key negotiation in IKEv2 Phase 2.
HSTS: Provide max-age and optional directives support	HSTS max age and optional directives like includeSubDomain and Preload can be configured from the admin UI
Clustering support in SPE Virtual Appliance	Virtual Appliances - including legacy VA-SPE as well as the new PSA-V appliances can be clustered in a 2-node Active/Active or Active/Passive configuration. Performance qualified on VMware only.
Support for Firefox 52 ESR.	Qualified support for Firefox 52 ESR.
Support for VDI 7.1.	Qualified support for VDI Profiles on VMWare Horizon view server 7.1.
Licensing for VM Models	VA-SPE/PSA-V models will be available in different models based on vCPU core counts.

Feature	Description
Cloud Secure	The Pulse Cloud Secure technology provides seamless and secure access to cloud-based applications. With this PCS release, the following capabilities are available as part of the Cloud Secure: • Cloud Secure Configuration through New UX- Configuring and Enabling Cloud Secure solution in PCS involves multiple steps like enabling SAML, Identity provider configurations, Service provider configurations, VPN settings etc. Cloud Secure UX is a simplified and intuitive user interface to enable cloud secure solution. UX enhances the admin experience by helping them by prepopulating the relevant settings, reuse of existing configurations and guiding them with help sections. • ADFS Integration: Cloud Secure solution integrates well with Third-Party Identity Providers to support the existing customer deployments who has already implemented Identity management solution from different vendors. In this release, Cloud Secure started supporting Identity Federation with Microsoft's Active Directory Federation Services. • Active-Active Cluster Support: We support Cloud Secure Use cases with PCS A/A Cluster Deployment

Fixed Issues in 8.3R3 Release

Problem Report Number	Summary
PRS-346532	Summary: Terminal Services RemoteApp feature fails on Chrome & Firefox.
PRS-348281	Summary: Network Connect: Users unable to connect with GINA on and are failing HC on Windows 10.
PRS-341742	Summary: Pulse Collaboration: Users are unable to view or change meeting details for recurring meetings.
PRS-352353	Summary: Attendee unable to join Pulse Collaboration meeting from Chrome and Firefox browser when custom sign-in page is used.
PRS-350673	Summary: Pulse One publishing error (Result of importing is unknown)
PRS-349003	Summary: SNMP alerts for high usage of disk (Sending iveDiskNearlyFull). Customer needs RCA
PRS-352858	Summary: SYSLOG traffic is send in UDP 514, when configured custom port is 32768 or above.
PRS-353985	Summary: Password option value of "Use Proxy Server" in admin page under host checker option can be identified using Inspect option of browsers.
PRS-350911	Summary: Special characters in Danish keyboard does not work using IE.

Problem Report Number	Summary
PRS-353751	Summary: Pulse Secure client displays the wrong password expiration number of days with respect to LDAPS password management.
PRS-350545	Summary: AAA - Requirement to add Variable callingStationId to the custom expression
PRS-352940	Summary: Some Host Checker components are still not digitally signed.
PRS-352207	Summary: RDP user created bookmark fails if <PASSWORD[2]> set as variable
PRS-352633	Summary: Edit HTML5 Resource Profile SSH/Telnet bookmark via Roles > HTML5 Access changes Access Type to RDP on the bookmark.
PRS-352761	Summary: Web process crashes frequently. Needs RCA.
PRS-356081	Summary: Pulse One publish failure: Failed to configure the import operation for block: [system.network.management-port] operation: replace
PRS-349124	Summary: PGM traffic causing high cpu in 8.2RX.
PRS-351215	Summary: Incomplete localization when "End-user Localization" language selection set to "Automatic (based on browser settings)".
PRS-345463	Summary: PSA: Critical or major events are generated for fan alert "Fan *X is running below threshold (*RPM)
PRS-351581	Summary: Unable to join a node to cluster via serial console.
PRS-351007	Summary: Negative number in the bytes in field for VPN tunnel logging in WELF format.
PRS-347379	Summary: PCS loses connection to Syslog server when there is an XML import (Even if no service is restarted). Need RCA/Solution.
PRS-350908	Summary: "DISCONNECTED" pop-up in HTML5 RDP session does not come
PRS-349571	Summary: Mac Sierra (10.12) slow performance issue with MTU seen as below 500 bytes.

Problem Report Number	Summary
PRS-349121	**Summary:** Config-only cluster, SNMP GET for "iveConcurrentUsers" and "clusterConcurrentUsers" are the same and should not be.
PRS-353699	**Summary:** Unable to modify HC rule name on 8.2R8, need RCA and fix.
PRS-347307	**Summary:** CPU usage spike once in every 1 or 2 days on both the nodes in Cluster.
PRS-349880	**Summary:** JSAM launching issue in firefox browser in 8.2R5 and above version.
PRS-351347	**Summary:** WSAM Bypass Application does not work as expected with McAfee AV
PRS-345283	**Summary:** DNS redirect corrupts merged PAC file for Pulse client.
PRS-346153	**Summary:** PSAL : Issue while using NC auto launch error message: " Detected incorrect data from server" on Chrome, Edge
PRS-346144	**Summary:** WTS Seamless Window feature does not work with Chrome browser
PRS-352968	**Summary:** SharePoint 2013 documents are not rendering
PRS-352143	**Summary:** PSAL: Browser redirects to PSAL download page after HC policy evaluation
PRS-353300	**Summary:** Rewrite: Backend throws error page in 2nd login attempt if form post sso is configured for the backend logout url.
PRS-350462	**Summary:** VPN tunnel assignment intermittently fails for all users
PRS-349751	**Summary:** License Client is not able to get licenses from server and in event logs we get the following error " License Server Protocol Error: Code=(0x32) Error="Stale Lease Id"
PRS-351344	**Summary:** TNCS crash occured generating core dump. Need RCA.
PRS-351273	**Summary:** PSA7000 webserver crashed with TP of 180MBps and 80% CPU, web crashed in 8.2R5
PRS-355601	**Summary:** Proxy prompt with Pulse Secure client 5.2R8 when credential provider is configured
PRS-350829	**Summary:** Pulse Application Launcher throwing failed to contact server for the first time launching Virtual desktops resource profiles
PRS-351643	**Summary:** Support of HSTS does not include the HSTS header when browsing to the base domain using HTTPS

Problem Report Number	Summary
PRS-351321	**Summary:** Web Rewrite: Unable to access Internal web resource which is protected by Kerberos.
PRS-346939	**Summary:** After a cluster split and VIP failover, users are prompted for authentication.
PRS-344879	**Summary:** VIP failover occur if we unplug and plug internal link on passive node in less than 60sec.
PRS-347945	**Summary:** Web core session is broken after a cluster split.
PRS-351673	**Summary:** VDI: Connection server is not updated on WIndows 7 machines with VMware horizon view client 4.1.0
PRS-345418	**Summary:** VA-SPE (vmware) running 8.2R4 fails during bootup after adding 2GB memory and adding CPU cores
PRS-346477	**Summary:** IKEv2 connection dropped when using a Directory/Attribute server in the realm
PRS-353159	**Summary:** Pulse One: Configuration mismatch in Roles: live-meeting-limit, live-attendee-limit, new-window
PRS-345523	**Summary:** WSAM auto-uninstall not work for non-admin users
PRS-350169	**Summary:** Disk utilization in the 8.2 New UI shows up 0% all/most of the time
PRS-344037	**Summary:** Server fails authentication with bogus "missing or invalid certificate" error.
PRS-353082	**Summary:** Newly added connection stays at "Connect Requested" indefinitely. Restarting Pulse Secure Service fixes the issue.
PRS-299313	**Summary:** WSAM : Launching WSAM via pulse and TDI drivers not intercepting DNS query [OS - 7.4R5]
PRS-350026	**Summary:** Core Rewrite: SharePoint HTML embedded mailto links getting rewritten.
PRS-351467	**Summary:** Pulse One: Deleting a role mapping using expression and deleting expression, causes "Publish Failed".
PRS-351063	**Summary:** Pulse 5.2R5 stuck at connecting and do not get the pre-signin notifications even, seems Captive Portal option caused it and need RCA.
PRS-305129	**Summary:** IE9+ will use cached ie.js after upgrade from 7.0R5 to 7.3R2.
PRS-351547	**Summary:** MAG/PSA losing config changes when power outage occurs despite saving the changes in 8.2.
PRS-352789	**Summary:** Need to change the Severity from "Major" to "Critical".

Problem Report Number	Summary
PRS-341904	Summary: Users account get locked on the AD after 3 failed attempt.
PRS-350216	Summary: Cloud Secure: Active Sync is not working with iOS devices after upgrading to 10.2

Known Issues in 8.3R3 Release

The following table lists Known issues in 8.3R3 release.

Problem Report Number	Release Note
PCS-6476	Symptom: PCS VA-SPE/PSA-V does not receive response for the heart beat messages from Pulse Cloud Licensing Service(PCLS) Conditions: 1. PCS VA-SPE/PSA-V is configured to reach PCLS via External Port 2. PCS VA-SPE/PSA-V is configured as a Cluster Workaround: Configure both the cluster nodes to use Internal port to connect to PCLS
PRS-356768	Symptom: IPv6 VPN tunneling address is not getting displayed in active user page. Conditions: When pulse client (tunnel adapter) has assigned with both IPv4 and IPv6 address. Workaround: None (Just display issue functionality is working fine.)
PRS-356068	Symptom: Enabling FIPS mode selects SSLv3 option in outbound settings page Conditions: If PCS admin does following steps, SSLv3 Option in FIPS Mode is getting enabled in Outbound Settings Page: a) Enable NDcPP Mode in Inbound SSL Security Option b) Disable FIPS Checkbox in Inbound SSL Security Option c) Change Allowed SSL and TLS version to SSLv3 in Outbound SSL Security Option d) Enable FIPS Mode in Inbound SSL Security Option Workaround: None
PRS-356844	Symptom: SSL dump option in TCPDump Sniffing on VLAN interface shows empty page. Conditions: If PCS admin sniffs on VLAN interface and viewed sniffed packets using SSL dump option, there will be an empty page displayed. Workaround: None

Problem Report Number	Release Note
PCS-6656	Symptom : Azure: End-user will not be able to establish a tunnel if admin configure "DHCP" option under IPv4 address assignment. Conditions : In VPN configuration profile if admin selects DHCP option for IPv4 address assignment. Workaround : In VPN configuration profile select IPv4 address pools option.
PCS-6612 (Azure)	Symptom : Admin will not be able to access PCS if he tries to import XML config which changes the existing network settings. This is also applicable when admin tries to deploy new PCS in Azure and if the PCS config hosted in web server contains network settings. Conditions : PCS XML config with internal/external/management port configuration. Workaround : Import PCS XML config without network settings configurations in it.
PCS-6581 (Azure)	Symptom : Admin will not be able to get SSH console access if he upgrade PCS on Azure from 8.3R3 to next available release. Conditions : Upgrading PCS on Azure from 8.3R3 to next available release. Workaround : For SSH access use Remote Debugging Code (RDC).
PCS-6601 (Azure)	Symptom : Reboot, Restart Services, Factory Reset and Shutdown operation do not work through PCS console. Conditions : System operations do not work through PCS console. Workaround : System operation works through Admin UI and Azure portal. It is always advisable to shut down the instance via the Azure portal or CLI to avoid the charges.
PCS-6609 (Azure)	Symptom: PCS configuration hosted in a web-server is not getting imported into PCS. Conditions : If the web server is using https as communication protocol. Workaround : Host PCS configuration in a web server where the communication protocol is http.
PRS-356904	Symptom: Pulse Collaboration fails to launch in MAC OS High Sierra 10.13. Conditions: If JRE installed, Pulse Collaboration fails to launch in MAC OS High Sierra 10.13 (17A365). Workaround: Install JDK and launch Pulse collaboration.
PRS-356665	Symptom: JSAM fails to launch in MAC OS High Sierra 10.13. Conditions: If JRE installed, JSAM fails to launch in MAC OS High Sierra 10.13 Beta. Workaround: Install JDK & launch JSAM.

Problem Report Number	Release Note
PRS-356307	Symptoms: HC rule policy with MD5 and SHA256 checksum fails intermittently for 64 bit process. Conditions: Fails only for 64 bit process, because Host Checker 32 bit application, trying to fetch the information about 64 bit process. Workaround: None.
PRS-356662	Symptom: HOB Applet configured with screen size as full screen is not working on Ubuntu. Conditions: Hob Applet (4.1) configured with screen size as full screen is not working on Linux Ubuntu 14.04. Accessing Hob Applet directly also seeing the same behavior, Issue is with Hob Applet not with PCS. Workaround: Configure Screen size with any other options.
PRS-356702	Symptom: Getting 500 Internal error Message while modifying the Citrix ICA Client Access settings. Conditions: While editing Citrix StoreFront Web Access Resource profile Citrix ICA Client Access settings from "HTML5 Access" to "ICA client connects over CTS". Workaround: Create a new profile with required Citrix ICA Client Access setting options without modifying the existing Citrix StoreFront Web Resource Profile.
PRS-355313	Symptom: Error mentioning "No bootable device" while deploying fresh 8.3R3 KVM SPE|DTE image with virtmanager version less than or equal to 0.9.0 on KVM server. Conditions: Qemu version 1.1 start supporting the QCOW2 lazy_refcounts feature that improves performance of snapshot operations. Starting with qemu 1.7, compat=1.1 became the default, so that newly created images can't be read by older virt-manager versions by default. From 8.3R3/5.4R3, we are supporting KVM image with QCOW2 lazy_refcounts feature. Workaround: If you need to read them in older version, you need to do the following: • Convert into old format using below command in the 'Terminal' (CLI)window: qemu-img amend -f qcow2 -o compat=0.10 <image-name> • Storage format should be set to qcow2 instead of raw in VM settings.
PRS-356406	Symptom: Users may not be able to access the resource if default VLAN ID is set on the internal interface. Conditions: If default VLAN ID is set on internal interface and user roles are mapped to internal interface, Users may not be able to access the resource. Workaround: Navigate to User roles->VLAN source IP. Map VLAN to internal_default VLAN and save changes. In case of Virtual Appliance, Navigate to System->Traffic segregation->Default Network. Include internal_default_VLAN in selected interface before mapping in user roles.

Problem Report Number	Release Note
PCS-6469	Symptom: Gateway unreachable message seen on console Conditions: If default VLAN ID is set on internal interface, gateway unreachable message seen on console while rebooting the device. Workaround: None. It will not impact any of the functionality.
PCS-5094	Symptom: Session resumption will not work properly for users connected through ESP mode (User prompted for credential during cluster failover). Conditions: When connection profile is enabled with "ESP Transport Only (No SSL fallback, this setting is for the Pulse client only)" Workaround: Disable this option in connection profile.
PRS-355727	Symptom: When IKEv2 client (not with pulse client) used with Hardware acceleration enabled, large sized packets (over 1400 bytes) will be dropped. Conditions: Users will see loss of traffic – of the packets that are big. Workaround: 1. Use SHA256 2. Disable Cavium acceleration.
PRS-347460	Symptom: Session resumption is not happening when upgrading a A/P Cluster. Conditions: Users who logged in while the cluster is upgrading will be prompted for login again. Workaround: Upgrade cluster during maintenance window.
PRS-356476	Symptom: Max concurrent users is restricted to 2, even after leasing licenses from license server Conditions: 1) PCS is a Virtual Appliance 2) Admin does a clear config after upgrade to 8.3R3 Workaround: 1. Take backup of PCS config, rollback, upgrade the VA-SPE and re-import the config. (or) 2. Apply core license through authcode
PRS-339881	Symptom: WSAM resources not samized when accessed via Edge Browser Conditions: If users try to access WSAM resources from EDGE browser, access will fail. WSAM application will not receive any traffic for the destination from the TDI driver. Workaround: Need to access the resource from other supported browsers (like IE, Firefox, etc.)

Problem Report Number	Release Note
PCS-6479	Symptom: License Summary page shows maximum concurrent users as 25000. Conditions: 1. PCS VA is running on a VMware ESXi | Hyper-V | Azure. 2. Admin has installed 8 core licenses, but has allocated less vCPUs in VM Settings Workaround: None. Admin needs to shut down the VA-SPE/PSA-V and apply same no of cores as the licensed core limit.
PRS-356722	Symptom: While configuring Cloud Secure with New UX, we might hit some UI issues / validation errors as mentioned in the PR Conditions: Configuring Cloud Secure with New UX Workaround: Configure it through Admin UI
PRS-352949	Symptom: Office 365 landing page is not displayed properly. Conditions: Office 365 page is rewritten by PCS Workaround: None
PRS-339385	Symptom: XML Import operation of SAM allowed servers/port fails Conditions: If there is a space in SAM allowed servers/port value. Workaround: Remove space from the XML configuration before import.
PRS-351894	Symptom: Client certificate based authentication will pass even though "Trusted for Client Authentication" Checkbox is unchecked in any of the CA Chain. Conditions: When "Trusted for Client Authentication" Checkbox is unchecked in any of the CA Chain. Workaround: None.
PRS-355058	Symptom: Certificate Authentication on iOS Mobiles works only with Pulse Client with version higher than 6.4.0. Conditions: When the Pulse client is configured to do Certificate authentication with PCS from mobiles. Workaround: If customer wants to test it, they can request for test ipa builds.
PRS-355916	Symptom: PCS login page redirects the end User to download activex plugin. Conditions: When the user have no pulse components installed on the PC. Workaround: None

Problem Report Number	Release Note
PRS-356607	Symptom: End User is unable to download PSAL and user is not able to proceed further. Conditions: Host checker policy is enabled and user access any SSO-enabled application downloaded from App Store on MAC OS. Workaround: None
PRS-352127	Symptom: Custom SOH Antivirus policy doesn't take Group policy configuration into consideration while evaluating in windows 10 OS. Conditions: Group policy setting are not considered while evaluating the policy Windows 10 OS. Workaround: None
PRS-352127	Symptom: Custom SOH Antispyware policy doesn't take Group policy configuration into consideration while evaluating in windows 10 OS. Conditions: Group policy setting are not considered while evaluating the policy Windows 10 OS. Workaround: None
PRS-354153	Symptom: HC process crashed when rule monitoring is on for connected session when admin tries to upgrade ESAP and change V3-V4 Opswat option. Conditions: Admin upgrades ESAP and toggles V3-V4 Opswat SDK when the user is connected with rule monitoring ON. Workaround: Restart the PPS services on endpoint.

Noteworthy Changes

- In 8.3R2, multicast traffic (Inbound and Outbound) hitting the server is captured in Enhanced Network Overview page and Throughput graph on Overview page.

Fixed Issues in 8.3R2.1 Release

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Problem Report Number	Release Note
PRS-353755	Summary: Active Sync traffic causes hpproxy and aseproxy processes to crash.
PRS-355199	Summary: The WSAM application is not passing traffic via the VPN intermittently.

Problem Report Number	Release Note
PRS-355106	Summary: Unable to connect to the WTS resource until reboot.
PRS-354777	Summary: Unable to access rewriter resource intermittently due to Rewrite server crash.
PRS-347840	Summary: HOB Java Applet fails with NLA enabled on the server.

New Features in 8.3R2 Release

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

Feature	Description
Add "MAX-LICENSED-USERS-REACHED" flag to healthcheck.cgi data for intelligent load balancing	The PCS allows another server to query it for some health check parameters. Currently, these parameters are supported: CPU-UTILIZATION SWAP-UTILIZATION DISK-UTILIZATION SSL-CONNECTION-COUNT USER-COUNT VPN-TUNNEL-COUNT The MAX-LICENSED-USERS-REACHED feature adds one more eponymous parameter that will indicate whether the maximum number of users that is supported by the installed license has been reached.
Granular RADIUS accounting	Radius accounting interim updates are sent for each sub-sessions created under parent session. For every client, such as JSAM, Network Connect, WSAM, Pulse Desktop Client etc., Two interim updates will be sent. One for parent session and one for the client session.
Support SHA2 in ESP Mode	Administrators can now use stronger algorithm SHA2 in ESP mode. This can be configured in the Encryption settings under Resource Policies > VPN Tunneling > Connection Profiles.

Fixed Issues in 8.3R2 Release

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Problem Report Number	Release Note
PRS-353972	Summary: dsagentd may show some memory growth over time on every session time out.
PRS-353479	Summary: 'Maximize Security' Text displayed for AES256-SHA1 Encryption in Connection Profile.

Problem Report Number	Release Note
PRS-353476	Summary: IKEv2 Virtual Port config is removed after changing the Virtual Port Name field.
PRS-353103	Summary: HTML5 access fails when compatibility mode is enabled in IE11.
PRS-353002	Summary: ESP SHA256 HMAC truncation size is 96 bits instead of 128 bits.
PRS-352536	Summary: On PSA3000 and PSA5000, disabling of management port causes the management port tab to disappear.
PRS-351643	Summary: Support of HSTS does not include the HSTS header when browsing to the base domain using HTTPS.
PRS-349490	Summary: When users logout, there is no recommendation to close the browser.
PRS-347492	Summary: The internal and external ports may not load correctly on the PSA7000f chassis.
PRS-352388	Summary: Configuration may fail to push from the master appliance to slave appliances in Pulse One if its slave appliance has an AD server instance with the same name in a different case.
PRS-351300	Summary: Outlook Anywhere configured on remote systems that have DNS entries that point to the PCS IP may cause the CPU and memory utilization to increase until the system is inaccessible.
PRS-349686	Summary: The user access log does not record client OS information.
PRS-347945	Summary: Users may need to reauthenticate to continue using web browsing functionality after a cluster failover.
PRS-349003	Summary: SNMP being configured may cause high disk usage alerts.
PRS-346863	Summary: SSL acceleration being enabled may cause the web server and cluster services to destabilize and fail to recover.
PRS-351873	Summary: Pushing AV product details from Pulse One may fail to import correctly.
PRS-341933	Summary: Attempting to join a meeting using a dynamically generated URL from an external server may display an access forbidden message if the dynamic URL has a trailing slash in the referrer host definition.
PRS-352232	Summary: When an older client, without AES256/SHA256 support, connects to a role with ESP only transport configured, SSL fallback will occur and data will transfer over SSL.

Problem Report Number	Release Note
PRS-348473	Summary: Auto-launch does not occur for Network Connect after session time out with "Enable session timeout warning".
PRS-348389	Summary: Pulse virtual adapter with MTU 1500 might cause connection issues.
PRS-349666	Summary: License expiration may be reached sooner than expected in a cluster after a cluster split.
PRS-350978	Summary: Network Connect (Windows) users may not be able to access the last IP in a list of tunneled networks from the split tunneling policy.
PRS-343158	Summary: If IKEv2 and OCSP are both configured on a PCS system, the daemon handling VPN traffic (dsagentd) may crash.
PRS-347025	Summary: If an archiving attempt fails, the next archiving is scheduled after 5 hours.
PRS-345645	Summary: When using RADIUS authentication with challenge/token responses and an invalid passcode response is given, Pulse does not show initial login request.
PRS-347455	Summary: Older clients are not falling back to SSL when ESP transport mode Encryption type is set to AES256/SHA256
PRS-351157	Summary: Default action in WSAM destination is deny when new role is created.
PRS-350525	Summary: RADIUS accounting statistics are calculated incorrectly using the Pulse desktop client.
PRS-350503	Summary: Pulse Secure Application Launcher fails to trigger when joining 'My Meeting' URL-based collaboration sessions.
PRS-350494	Summary: Pulse Secure Application Launcher fails to register the launch of the Collaboration client when using 'My Meeting' URL-based collaboration sessions.
PRS-349838	Summary: IKEv2 connections may fail if virtual ports are configured for the connection.
PRS-349620	Summary: The html5acc-server daemon may crash if an invalid DNS entry is defined in an HTML5 bookmark.

Known Issues in 8.3R2 Release

The following table lists Known issues in 8.3R2 release.

Problem Report Number	Release Note
PRS-347854	**Symptom:** Domain join fails in multi DC environment. **Conditions:** Domain join fails after password change gets triggered in multi DC environment. **Workaround:** Manual domain join resolves the issue.
PRS-346610	**Symptom**: IPv6 ESP Tunnels are falling back to SSL. **Conditions**: With more than 20000 tunnels established IPv6 ESP Tunnels fall back to SSL. **Workaround:** None
PRS-350719	**Symptom**: IPv6 SSL tunnels are dropped. **Conditions**: IPv6 SSL tunnels are dropped with 12K users. **Workaround:** None.
PSD-2210	**Symptom:** 'DNS Search Order' descriptions for Mac and Windows 10 does not reflect the capabilities. **Conditions:** Users of Mac & Windows 10 will not know the capabilities of 'DNS Search Order'. **Workaround:** None.

Fixed Issues in 8.3R1.1 Release

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Problem Report Number	Release Note
PRS-351573	**Summary:** Resource access through Network Connect will fail after 90 seconds and will recover automatically.
PRS-351673	**Summary:** When a user clicks on a configured VDI book mark which has the SSO parameters set, on a Windows 7 machine the SSO does not work. No parameters for VDI session are populated.

New Features in 8.3R1 Release

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

Feature	Description
Virtual License Server	In License server deployments, customers can deploy the License server as a virtual machine to support fully virtualized environments. For details, refer to the License Management Guide.
Certificate Based Active-Sync with Kerberos Constrained Delegation	Provides secure, transparent access to Exchange ActiveSync by acting as a Kerberos Proxy that translates certificate based authentication to Kerberos tickets using Kerberos Constrained Delegation, without requiring the Kerberos Key Distribution Center (KDC) to be exposed to the Internet.

Feature	Description
IPv6 Enhancements	• ESP Tunnel Mode now supports IPv6 with Pulse client bundled with 8.3R1 and later. Only 6-in-6 mode is supported. • Administrators can now create layer-3 Access Control Lists (ACLs) using IPv6 addresses. • IPv6 addresses can be configured for VLAN interfaces • Rewriter support for IPv6. This includes: Basic Web ACL Policy, Selective Re-Writing, Custom Headers, Web Proxy, Form Post SSO Support, Basic Filter Policy, HTML rewriting, JavaScript rewriting and CSS rewriting. Additional items will be added in a phased manner in following releases. • Hostchecker is qualified to work with IPv6 addresses, except for downloading updates from non-Pulse Secure servers that may still on IPv4. • IPv6 Spilt Tunneling for Windows - Pulse VPN now allows accessing both IPv4 and IPv6 corporate resources from IPv4 and IPv6 endpoints. It enable client to access both corporate network and local network at the same time. The network traffic designated are directed to tunnel interface for corporate network by configuring route policies, whereas other traffics are sent to direct interface.
SSL - SNI Extension support	PCS now supports the use of Server Name Indication (SNI) SSL extension to communicate with backend servers that require SNI. SNI is typically enabled on backend servers to support multiple hostnames on the same IP address without having to resort to wildcard certificates. SNI support is enabled for rewriter, PTP, SAML, JSAM, WSAM, Pulse One, license server, CRL, ActiveSync, Syslog, and SCEP. OCSP, LDAPS, PushConfig are not supported.
Granular control over L4 PerAppVPN functionality on iOS devices	Prior to 8.3R1 versions, we could only define the allowed destinations. Now, admins have granular control over the destination list (IP/FQDN) defined for the L4 PerAppVPN functionality on iOS devices. For example, an admin can now deny specific hosts (finance.xyz.net) and allow other destinations in the domain (*.xyz.net) or vice versa. In addition, a default Allow or Deny rule can also be configured for Non-defined WSAM Destinations. Note: This configuration is available within admin GUI under the user Role -> SAM ->Applications-> WSAM destinations -> Add Server.
Citrix StoreFront support	Customers can now use CTS client as well as WSAM to access Citrix StoreFront.
Enforce minimum client version	Admins can now enforce that end users have an updated version of the Pulse client before access is allowed
VLAN for HTML5	VLANs can now be configured for HTML5 based access to datacenter resources
SHA2, AES256 and DH14 in IKEv2 Phase 1	Customers can now use these stronger ciphers in the IKEv2 phase 1 when using IPSEC mode.
Additional personality for PSA7000	PSA7000 hardware can now be booted into Pulse One on-prem version. This is only available in the latest hardware. Please contact support for more information.
HSTS header Support	PCS sets HSTS header for all 200 OK HTTP response. This is implemented in 8.3R1 and 8.2R6.
Option for NLA classic behavior	Newer Microsoft OS (e.g. Win 10) require NLA, which was enabled by default for WTS in earlier releases that leads to double authentication prompts (NLA and RDP) after 8.1R7. While NLA will continue to be enabled by default, admin now has the option to switch to classic (pre-8.1R7) behavior at a role and bookmark level.

Feature	Description
Cloud Secure	The Pulse Cloud Secure technology provides seamless and secure access to cloud-based applications. With this PCS release, the following capabilities are available as part of the Cloud Secure: • Support for seamless and secure access to cloud services for On-Premise users by federating PPS session information to PCS • Cloud Secure Config Simplification through Wizard • Compliance check for On-Premise mobile devices using PWS
Changes to Always-On VPN	To enable users have more flexibility in adding/removing/connecting/disconnecting when Always on VPN mode is enabled.

Noteworthy Changes

- The UDP port configuration for IPv6 ESP tunnel is moved to Configuration-> VPN Tunneling page. The default value is set as 4500.

  This is a global configuration for all IPv6 ESP tunnels. The UDP port configuration under Resource Policies-> VPN Tunneling-> Connection Profiles is restricted only for IPv4 ESP tunnels.
- Default ACLs for IPv6 resources are not added while upgrading to 8.3R1. In order to access the IPv6 back-end resources, admin has to explicitly configure the desired ACLs under Resource Policies-> VPN Tunneling-> Access Control.
- From 8.3R1 onwards, we are not shipping the VA-SPE-SA-<xxxxx>-SERIAL image. If serial console access is required, then, deploy the VA-SPE-SA-<xxxx>-VT image and use the toggle console option either from PCS/PPS WebUI or console. These changes will affect only a fresh deployment. Upgrade for existing serial image will not get affected. Please refer to the **Virtual Appliance Deployment Guide** for more details.
- From 8.3R1 onwards, PCS/PPS Virtual Appliance Editions will have a disk space of 40GB. This will get reflected for fresh deployment with 8.3R1 OVF.

Fixed Issues in 8.3R1 Release

The following table lists issues that have been fixed and are resolved by upgrading to this release.

Problem Report Number	Release Note
PCS-5375	Summary: " unregister_netdevice: waiting for tun_0_68 to become free. Usage count = 3 " messages will be flooding in the console
PRS-347894	Summary: SAML ECP users should be mandated to authenticate with PWS
PRS-345230	Summary: PCS is not honoring the AuthNRequests from BambooHR SP
PRS-344470	Summary: Cloud Secure dashboard is not displaying Successful and Failed ECP flow details
PRS-346275	Summary: If the "Allowed Encryption Strength" option is set to "Maximize Security (High Ciphers)" in the SSL panels, cipher suites that employ 3DES are not selected. For example, TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA is not selected.

Problem Report Number	Release Note
PCS-4579	Summary: Need to provide drop-down box for configuring FT settings for al the cluster members.
PRS-342551	Summary: XML import of security/SSL-options settings from older versions (7.x/8.1) causes “Custom cipher does not match the available selection” error.
PRS-341063	Summary: Cluster split observed due to scheduled system arching.
PRS-342396	Summary: After upgrading, users are unable to connect – logs show error “Failed to set ACLs for user with NCIP x.x.x.x”
PRS-342944	Summary: IPv6 DNS: PCS server not sending down the IPv6 DNS server info to Pulse Client
PRS-344892	Summary: PSAL launching fail on MAC with Custom Sign-In Pages and HC configured using Safari/Chrome browser
PRS-345193	Summary: 8.2R5 checks for ive version in xml file breaking manageability via NSM
PRS-343759	Summary: PWS:Token is not pushed when many users/devices are using same workspace policy
PRS-342734	Summary: Configuration Mismatch happens when HTML5 Access is selected in User Role (upgrade bug)
PRS-343579	Summary: parevntd crashed in DSAuth::SessionManager::getIVSConcurrentUsers when one of the nodes was rebooted in PPS longevity
PRS-309431	Summary: EPS: Access Denied error for Detect Missing patches API when run as normal user for SCCM2012 and SCCM 2007
PRS-318679	Summary: EPS:OPSWAT API is not detecting the status of encrypted drives correctly for the Bitlocker Encryption
PRS-344555	Summary: OpswatV3toV4:When multiple connections happen to a pulse from servers having v3 and V4 SDK enabled, the behavior needs to be fixed and documented
PRS-343232	Summary: Hard Disk Encryption detection reports as Access denied using OESIS Tool V4 on Windows-7 as restricted user
PRS-339456	Summary: Opswat API's for detecting Missing patches takes more than 20 minutes to return the data

Problem Report Number	Release Note
PRS-343928	Summary: OpswatV3toV4: Remediation action to Turn on Firewall requires admin privilege for V3 and V4 SDK
PRS-342845	Summary: Pulse Collaboration join meeting through the iOS device fails and gives error "Exceeds license for number of users""""
PRS-344821	Summary: Accounting Stop not sent for Pulse WSAM session
PRS-338371	Summary: Not able to launch multiple desktops through chrome
PRS-344470	Summary: Cloud Secure dashboard is not displaying Successful and Failed ECP flow details
PRS-336184	Summary: PSAL: Shows Chinese Traditional instead of Chinese Simplified
PRS-342658	Summary: Syslog FT: While processing pending logs normal logs may be dropped
PRS-342551	Summary: Import of security/ssl-options XML from older (7.x/8.1) version on to 8.2R5 causes "Custom cipher does not match the available selection" error
PRS-341802	Summary: Windows 10 Redstone Preview 10.0.14291 standalone WSAM not working (non-Pulse)

Known Issues in 8.3R1 Release

The following table lists Known issues in 8.3R1 release.

Problem Report Number	Release Note
PCS-5362	Symptom: Unable to fetch service tickets for a user from a child domain using Certificate based ActiveSync with Kerberos Constrained delegation (KCD) feature. Conditions: If user is part of child domain, PCS fails to make an active sync connection, unable to fetch service tickets. Work Around: None
PCS-5059	Symptom: Device OS/Type will not be updated in case of Certificate Based ActiveSync with KCD feature. Conditions: In case of Certificate Based ActiveSync with KCD, device OS/Type are not updated in device records. Work Around: To include iOS clients in device records, navigate to System->Configuration->Client Types. Include string pattern as "iPhone" and client type as "iPad Optimized HTML". When the device client does not include the device OS in the user agent string, then those devices will be updated with device type as "Other".

Problem Report Number	Release Note
PCS-5445	Symptom: UDP v6 resource is not accessible if the udp packets get fragmented. Conditions: If the packets get fragmented at the source (client), PCS server will forward only the first fragment and drop the subsequent fragments. Work Around: None.
PRS-346610	Symptom: Pulse IPv6 ESP tunnels are falling back to SSL with user load Conditions: If the number of connections are more than 20000 then the ESP connections tend to fall back to SSL. Work Around: None.
PRS-347523	Symptom: VIP failover doesn't happen properly Conditions: User connected to the External VIP can access the resources until the VIP failover. Once the VIP is failed over the user session doesn't resume. Workaround: Ensure external port connectivity is fine. VIP failover happens properly
PCS-5455	Symptom: SNI is not supported for the following backend applications: OCSP, PushConfig and LDAPS. Conditions: SNI on PCS has no effect on OCSP, PushConfig and LDAPS backend applications. Workaround: None.
PRS-347132	Symptom: End user gets the following error message on the browser: "The request contains an invalid host header" Conditions: When the end user uses FF ESR browser to access the PCS using IPv4 mapped IPv6 address, eg: fc00:3333::3.3.113.135 Workaround: Use the normalized IPv6 address or use some other browser like Chrome or IE or Edge
PRS-317773	Symptom: End user gets the following error message in event logs: " License Server Protocol Error: Code=(0x32) Error="Stale Lease Id" Conditions: In a rare scenario, if license server information is deleted from license client and added back to it, the client might fail to fetch the licenses from server with stale lease id error Workaround: Deleting and recreating the client config on the license server fixes the problem
PCS-5170	Symptom: Admin is seeing two license ID on the virtual console of Virtual License Server(VLS) deployed on VMware ESXi Conditions: Admin performs a Clear Config or Factory Reset operation on Virtual License Server Workaround: None. This should not impact the functionality of Virtual License Server. The license ID that gets displayed when the VLS is coming up is only temporary. The one that gets displayed after the "Press Enter to Modify Settings" is the permanent one.

Problem Report Number	Release Note
PRS-347522	Symptom: VIP failover doesn't happen properly when external port connectivity is lost Conditions: External port connectivity of Passive node lost Workaround: Ensure external port connectivity is fine on the AP cluster passive node, then VIP fail over happens properly.
PRS-349891	Symptom: Applications in Citrix Storefront won't launch if user selects "Detect Citrix Receiver" or "Citrix Receiver already installed" links. Conditions: This Issue is seen only in Chrome Browser. Workaround: Do not click the links mentioned above in the Citrix Storefront Login Page.
PRS-347854	Symptom: Change machine password fails for AD mode authentication server. Conditions: If the admin has enabled "Enable periodic password change of machine account "for X days. Change machine password might fail if the Active Directory servers are configured with multiple domain controllers. Workaround: Navigate to Auth Servers->AD auth server->Enable "Save admin credentials" which will help PCS to recover automatically from machine password failure.
PRS-349373	Symptom: Group search returns empty groups when using AD mode authentication server. Conditions: When there is large LDAP query search and if it takes more time to render groups, it timeout and returns empty group list. Workaround: None.
PRS-347074	Symptom: Authentication using AD mode authentication server fails with "IO_TIMEOUT" error. Conditions: In case of multiple domain controllers, DNS resolution take longer time to respond and it timeout which leads to authentication failure. Few user logins might fail when DNS queries take long time to respond and timeout. Workaround: None.
PRS-350251 PRS-350645 PRS-349889 PRS-350505	Symptom: If PSAL is not installed and a user tries to launch application from Citrix storefront, then there will be issues during and after PSAL installation. When a user clicks on the application in Citrix storefront, then he has to wait for a minute for PSAL download page. User will see 404 error page if he/she clicks most of the links provided in PSAL Wait or PSAL Download page. In the PSAL download instead of "Citrix Terminal Services" it has been mentioned as "Windows Terminal Services". Conditions: Applicable only to PSAL dependent browsers. Also, Citrix storefront profile in PCS admin created with setting "ICA client connects over CTS client". Workaround: Pre-install PSAL before launching Citrix storefront application.

Problem Report Number	Release Note
PRS-350354 PRS-350352	Symptom: When configuring SSO for Citrix Storefront, the "POST the following data" checkbox is not enabled by default. Conditions: Issue is seen during Admin UI Configuration. Workaround: Admin needs to enable this option manually for SSO to work.
PRS-350494	Symptom: When a user tries to launch a meeting, PSAL constantly launches in Mozilla/Chrome. Conditions: If the user is using the Meeting type as MyMeeting (users have a personal meeting URL) Workaround: Open the meeting URL link in IE.
PRS-350503	Symptom: When a non-PCS user tries to join meeting for the first time, the Java applet is triggered automatically to launch the meeting instead of PSAL. Conditions: If the user is using the Meeting type as MyMeeting (users have a personal meeting URL). Workaround: As PSAL is not getting launched, Java is mandatory (i.e. user should have Java installed in PC) to launch the meeting.
PRS-350619	Symptom: Sometimes we may see HTML5 Access server crash when the user clicks on HTML5 Access server and immediately returns back to the Home page. Conditions: DNS server is not configure properly or the Hostname of the resource is not able to be resolved. Work-around: Try to reconnect to the resource again it should connect without any issue
PRS-350858	Symptom: Mask hostnames while browsing is not able to access IPv6 resource with resource profile having OWA Conditions: When Mask Hostnames while browsing is enable for User roles, IPv6 resource is failing with OWA. Workaround: Use OWA profile with hostname not with IPv6
PRS-350216	Symptom: Native Email Client in iOS prompts for password even after successful authentication Conditions: iOS Active Sync is not working when user upgrade to iOS 10.2 Work Around: None
PRS-346515	Symptom: On PSA7000, disk checks were added to make sure that the hard disk partitions are in a good state to be mounted before upgrading. We print the check messages on the screen and console when the device is upgrading. For e.g. Running fsck on /dev/md1 ... complete (0 seconds) Conditions: The disk check utility might also correct some errors. In that case you might see a message like: fsck repaired file system errors ... complete (0 seconds) Work Around: This is normal expected behavior and is not cause for concern.

Problem Report Number	Release Note
PRS-349427 PRS-343600	Symptom: In AP cluster situation, active node X fails and later rejoins. Node X would not have the latest user session state if user had logged out before node X rejoins. Conditions: In AP cluster situation, active node X fails, users are failed over to passive node Y. User's session information changed because the user logout from passive node Y, after node X rejoins to the cluster, node X doesn't have the latest user session state. Work Around: User session data is refreshed when the user login again.
PRS-348939	Symptom: IKEv2 XML/Binary configuration from a PCS running build prior to 8.3R1 can't be imported to a PCS running 8.3R1 and later. Conditions: Importing IKEv2 XML/Binary configuration from a PCS running build prior to 8.3R1 to a PCS running 8.3R1. Work Around: Manually configure IKEv2 configuration on PCS running 8.3R1.
PRS-349838	Symptom: If PCS configured multiple virtual ports of different realms with same interface label, upgrading to 8.3R1 causes IKEv2 clients of one of the realms unable to connect. Conditions: Upgrading PCS that configured with multiple virtual ports of different realms with same interface label to 8.3R1 and IKEv2 clients are configured for one of the realms. Work Around: Ensure interface label of all virtual ports are unique.
PRS-350599	Symptom: IKEv2 machine authentication fails to connect with Windows 10 native IKEv2 client if IKEv2 port is mapped to a virtual interface having large number of ACL rules. One of our tests showed issue when there are close to 5000 ACLs, and another test showed issue with 33,300 ACLs. Conditions: Windows 10 native IKEv2 client connects to a virtual interface with large number of ACL rules. Work Around: Reducing the ACL count if virtual interface is used as IKEv2 mapping will work.
PRS-348384	Symptom: Configure IKEv2 port mapped to a Realm doesn't prevent the Realm being deleted by the administrator. If the Realm is deleted, IKEv2 clients fails to connect. Conditions: IKEv2 port is mapped to a Realm and the Realm is mistakenly deleted. Work Around: Do not delete a Realm that is mapped to IKEv2 port.
PRS-346477	Symptom: When using Directory/Attribute server in the realm, and if LDAP didn't respond within 180 seconds, IKEv2 connection is dropped. Conditions: Using Directory/Attribute server in the realm, and LDAP didn't respond within 180 seconds. Work Around: None
PRS-350282	Symptom: In A/P cluster, when admin restart services on Active Node from console using option 4 and then 11, VIP will failover to the Passive node and sometimes, it may take up to 2 minutes for Pulse clients to resume sessions to the Passive node that is now the VIP owner. Note that session resumption happens immediately when admin performs the following operations: Clicking fail-over VIP button Reboot active node Conditions:

Problem Report Number	Release Note
	Users will wait up to 2 min for Pulse Client session to resume if admin restart services on the Active Node. Work Around: Don't restart the services on the active node.
PRS-350525	Symptom: Inaccurate statistics sent to accounting server when layer 3 VPN is formed with Pulse client Conditions: Accounting bytes updated in LMDB cache is not correct, there by showing wrong accounting bytes Work Around: None
PRS-349140	Symptom: PC meeting window appears for few seconds and then invisible when iOS user login via URL present in the meeting invite mail Conditions: When iOS user clicks the attendee URL present in the meeting invite mail, the PC client application comes in the front end for few seconds and then gets invisible. Work Around: Open the PC app first and then click the URL
PRS-349927	Symptom: Inconsistent behavior observed on configuring periodic snapshot stop time between manual and via XML import Conditions: When the stop time in the XML import file falls within a DST dates, there can be a variance of 1 hour in the stop time after the import. Work Around: None.
PRS-345418	Symptom: VA-SPE (VMWare) running 8.2R4 fails during boot-up after adding 2GB memory and adding CPU cores. Conditions: VA-SPE VM is deployed using pre 8.2 OVF. Workaround: • Export the configuration from running PCS-VM. • Create new PCS-VM with 8.2/8.3 OVF. • Import the configuration after PCS-VM deployed. • Go to edit setting of VM and modify memory from 2GB to 4GB.
PRS-349783	Symptom: Upgrade from pre 8.2 to 8.2/8.3 will fail on VA-SPE. Uploading any package like ESAP fails on VA-SPE. Conditions: VA-SPE VM is deployed using pre 8.2 OVF and running out of disk space on VA-SPE. Workaround: • Export the configuration from running PCS-VM. • Create new PCS-VM with 8.2/8.3 OVF. • Import the configuration after PCS-VM deployed.

Problem Report Number	Release Note
PRS-346351	Symptom: HTML5-Telnet:Configured telnet without SSO, while prompting for Credentials, says Login Incorrect and then Prompting for Login Conditions: Once launch the HTML5-Telnet bookmark, before prompting for Credentials it says Login Incorrect text Message. This is a limitation from the guacamole side. Workaround: None.
PRS-351193	Symptom: If IKEv2 EAP-TLS connections are active and PCS is configured to use license server, PCS pulls license state from license server results in all existing Pulse and IKEv2 connections to be reconnected. Conditions: • PCS is configured to use license server • PCS is configured to support IKEv2 client with ESP-TLS • Active IKEv2 EAP-TLS connections are in place Workaround: None.
PRS-350813	Symptom: Old client (Market client 6.2.0.71127) does not honor default catch all rule DENY (WSAM-DENIED-SERVERS–*) of 8.3R1 Conditions: This is observed while using market client with new server and when WSAM destinations are empty and default action is set to DENY. Workaround: Define one of the deny servers in the list and keep default action as DENY for servers not in the list.
PRS-351406	Symptom: Unable to access protected resources through rewriter after upgrade to 8.3R1. Conditions: This problem occurs under the following conditions: • Customer is using VLANs and has set VLAN Source IP to a VLAN. • Web resource resolves to both IPv4 and IPv6 • Preferred DNS response is set to Both in pre-8.3R1 • User session timeout is large such that the session persists across upgrades Workaround: If the user logs out and logs back in to the browser session, the IPv6 resource should be accessible.
PRS-351162	Symptom: IKEv2 client traffic fails when IKEv2 client connection is made to MAG SM360 enabled with hardware acceleration. Conditions: Using IKEv2 clients on MAG SM360 enabled with hardware acceleration. Workaround: Turn off hardware acceleration.
PRS-347333	Symptom: UDP resource is not accessible if the UDP packets get fragmented. Conditions: VPN Tunneling Access Control with specific port number or with range of port numbers (eg: udp://ipaddress:portnumber, udp://ipaddress:prange1-prange2,) does not work with fragmented UDP packets from client or backend server. Workaround: When creating ACLs for UDP resource do not specify the port number.
PRS-351574	Symptom: 90 seconds after tunnel establishment, the resource access fails for about 60 seconds and recovers automatically. Conditions: If user is using Network Connect Windows client. Work Around: Wait for 60 seconds to allow the Network Connect client to recover.

Problem Report Number	Release Note
PRS-351673	Symptom: When a user clicks on a configured VDI book mark which has the SSO parameters set, on a Windows 7 machine the SSO does not work. No parameters for VDI session are populated. Conditions: User has a configured VDI bookmark and SSO parameters are set. Workaround: No workaround.

Documentation

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

Note: The 8.3R3 Context-Sensitive Help and Task Guidance have been modified to Pulse Secure's look and feel.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to **techpubs-comments@pulsesecure.net.**

Technical Support

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

- **https://www.pulsesecure.net/support**
- **support@pulsesecure.net**
- Call us at 1- 844-751-7629 (toll-free USA)

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

Revision History

The following table lists the revision history for this document.

Table 6 Revision History

Revision		Description
4.0	October, 2017	8.3R3
3.0	June, 2017	8.3R2
2.0	May, 2017	8.3R1.1 Update
1.0	March, 2017	Initial Publication – 8.3R1