Pulse Desktop Client

Release Notes

PDC 9.0R2.1, 1421

PDC 9.0R2 Linux, 819

Release	9.0R2.1
Published	February 2019
Document Version	1.7

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 is the release-notes document for the Pulse Secure desktop client version 9.0R2.1. This document provides a cumulative list of all enhancements, fixes and known issues for the 9.0R2.1 client. If the information in the release notes differs from the information found in the documentation set, follow the release notes.

The Pulse Secure desktop client provides a secure and authenticated connection from an endpoint device (either Windows, macOS or Linux) to a Pulse Secure gateway (either Pulse Connect Secure or Pulse Policy Secure). For a complete description of the capabilities of this desktop client, please see the online help within the desktop client itself, or the Pulse Desktop Client Administration Guide available at https://www.pulsesecure.net/techpubs/.

Interoperability and Supported Platforms

Please refer to the Pulse Desktop Client Supported Platforms Guide for supported versions of operating systems, browsers, and servers in this release.

General Notes

Security-related issues are not normally covered in Pulse Secure release notes. To find more information security advisories affecting Pulse Secure products, please refer the Pulse Secure security advisory page.

Upgrade Paths

The following table describes the tested upgrade paths.

Release	Description
9.0Rx	You can upgrade directly to 9.0R2.1
5.3Rx	You can upgrade directly to 9.0R2.1
5.2Rx	You can upgrade directly to 9.0R2.1
5.0Rx or 5.1Rx	You can upgrade directly to 5.2Rx simply by installing the 5.2Rx update

Caveats, Important Changes, and Deprecated Features

Please note that client upgrades are not supported to or from beta releases. As such, if you participated in the 9.0R2.1. Pulse Secure desktop client beta program, please uninstall the beta 9.0R2.1 client before attempting to install any subsequent Pulse desktop client releases.

Important note: In order to run the Pulse Secure desktop client version 5.3R1 or later on a Windows 7 machine, the machine 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. 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 Pulse 5.3R1 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.)

Fixed Issues in 9.0R2.1 Release

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

Problem Report Number	Release Note
PRS-364786	**Summary:** The Pulse desktop connections are shown against a black background on macOS Mojave (10.14).
PRS-367325	**Summary:** Captive portal detection when using the embedded browser fails (blank page is rendered rather than the captive portal login) on macOS.
PRS-363544	**Summary:** DNS access may fail for 2 minutes when the VPN tunnel is created.
PRS-368115	**Summary:** Users may not be able to change Wi-Fi networks from the system tray on Windows 10.
PRS-368112	**Summary:** The Wi-FI selector is not available on Windows 10.

Product Codes (GUIDs) for SCCM Deployments in 9.0R2.1 Release

If you deploy the Pulse Secure desktop client using System Center Configuration Manager (SCCM, formerly SMS), it can be helpful to know the Product Codes (GUIDs) of Pulse Secure desktop client installation bundles. SCCM uses these codes to determine whether products are already installed. The table below gives the product codes for version 9.0R2.1 of the desktop client for the given the architecture (32-bit or 64-bit) and locale (language environment).

PulseSecure.x86.msi

- English - {D6CAE4C8-27B8-4984-988E-B5A4868070CC}
- Chinese (Taiwan) - {DC7B0813-D8DB-45C4-A534-C5C151BA257E}
- German - {C8C79FAD-DCB2-46CA-98E1-A0ABB087C2B8}
- Spanish - {16818F89-E523-479D-8A38-882148F47931}
- French - {DB41FCB2-A14D-46D9-B958-1C897541ADC1}
- Italian - {640D33BA-8B76-4BB5-81DB-CD3A73BD10C2}
- Japanese - {7344AB24-315C-41C6-B721-FB580688AD3B}
- Korean - {B13C4B3A-774F-436B-8293-D4EEEBE3E396}
- Polish - {22744FC4-829F-429E-8650-DC041101EB00}
- Chinese (China) - {831DE793-91DE-44F9-80BA-79B79DB041BD}

PulseSecure.x64.msi

- English - {7D2309C6-3F67-48B8-B524-522E2756795E}
- Chinese (Taiwan) - {A783DB66-CB52-464F-8D1E-F83FEA3E8B20}
- German - {5BBD43FA-672A-4FDF-99A7-C58A18D5C50E}
- Spanish - {3A5CC515-4CE0-46E0-8827-C0BA95427473}
- French - {C11B1C27-06EF-4CFE-AB40-3B6A809468F9}
- Italian - {453DF73A-7AD6-4C68-B672-305EB597B91E}

- Japanese - {C3630C44-69BC-4010-B83E-6C728C948F2F}
- Korean - {4D0E8CF1-208F-4C23-83A5-471A69CCC5D8}
- Polish - {B33FF264-31D7-4875-98F5-BD4E00ED69B7}
- Chinese (China) - {44E6B9C9-5D46-4931-ADB9-B06725773FE5}

New Features in 9.0R2 Release

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

Feature	Description
Traffic Enforcement on macOS	Pulse Desktop Client on macOS now supports Traffic Enforcement feature. With Traffic Enforcement feature enabled, Pulse client will terminate all existing TCP connections from the laptop device so that all network traffic will follow the split tunneling rules configured for VPN. The new TCP connections will be established based on split tunnel rules configured on PCS. This provides a security mechanism for administrators to tighten the network traffic before allowing users to establish VPN sessions.
64-bit Pulse Desktop Client for macOS	Pulse Desktop Client for macOS is now available in 64-bit format. Newer macOS will support 64-bit applications only in which case the newer Pulse client should be used for secure remote access.
Always-On Exception on macOS	Pulse Desktop Client for macOS now supports Exception rules for Always-On functionality. Exceptions are now supported on both Windows and macOS platforms.
Ubuntu 18.04 Support	Pulse Desktop Client for Linux is now enhanced to support Ubuntu 18.04 LTS release.

Note: From 9.0R2 release onwards, Pulse Secure Desktop client for macOS is not supported for Version 10.10 and below.

Product Codes (GUIDs) for SCCM Deployments in 9.0R2 Release

If you deploy the Pulse Secure desktop client using System Center Configuration Manager (SCCM, formerly SMS), it can be helpful to know the Product Codes (GUIDs) of Pulse Secure desktop client installation bundles. SCCM uses these codes to determine whether products are already installed. The table below gives the product codes for version 9.0R2 of the desktop client for the given the architecture (32-bit or 64-bit) and locale (language environment).

PulseSecure.x86.msi

- English - {6E31DBE8-6F48-4D22-AB10-EA76718532C4}
- Chinese (Taiwan) -{A52873A6-E7E4-42F9-BBF5-D32A10B2E3A6}
- German - {4416349F-08EE-4628-AC56-7C3D228240E6}
- Spanish - {B16BAECD-7C60-4B1F-9681-F118AF30A18A}
- French - {E228CFE7-3C58-4BBE-B92C-2C46C73D3C5E}
- Italian - {05AA9BE6-6881-48CA-AA57-7841BF041030}
- Japanese - {D420ADFB-239E-4E99-B97A-F800CEBEDB95}
- Korean - {BA0C5397-CA3B-4619-8AED-539FBDCE304F}
- Polish - {D5D83037-9E5F-4C39-876C-49AA2A3F2780}
- Chinese (China) - {0355F18A-195B-46F9-8EF9-25B70A60E9CE}

PulseSecure.x64.msi

- English - {7A39E355-B3CA-4217-A508-05C2FCB7766B}
- Chinese (Taiwan) - {AD08CFB6-9DA2-43C7-B425-B60F3CA1B109}
- German - {231F18D1-31A4-42A7-83F6-0045663C3EBE}
- Spanish - {D07BFE32-6CA5-41E5-B441-7CC05A2AD6B0}
- French - {A9F9AE24-384B-41C6-8E8F-9BADE4C93541}
- Italian - {9F9F1040-5038-4A9C-8F69-3ACDF8C5ADC9}
- Japanese - {34B79A90-3148-4056-B25D-BFC13F54D4FB}
- Korean - {9806BFC7-8088-444D-90AB-741A342D9B06}
- Polish - {BA27D522-BAA7-4744-8971-3EFAEA0914A4}
- Chinese (China) - {41827188-C1AD-431E-B212-49CCC9BC29B4}

Fixed Issues in 9.0R2 Release

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

Problem Report Number	Release Note
PRS-363205	**Summary:** If FQDN-based Split – tunnel deny policy is configured for VPN tunneling and that route is deleted, the resource will be accessible through the tunnel.
PRS-360565	**Summary:** If only FQDN routes are mentioned in both [allow and deny policy] and [allow only policy] the PCS server will not send the default route. All the IPV4 traffic will not go through the tunnel. If only FQDN routes are mentioned as deny policy, then default route will be sent from the PCS server.
PRS-361777	**Summary:** If the Fedora Linux user installs 9.0 R1 version of Pulse Desktop Client over Fedora Core 26 and upgrade the OS to Fedora Core 27 then Pulse Desktop Client will not be launched after the installation.
PRS-360661	**Summary:** Captive Portal Detection under lock down mode is failing for the first time when user is moved to captive portal environment.
PRS-366347	**Summary:** ARDAgent spikes to 100% CPU when lock down mode is enabled.
PRS-365483	**Summary:** Lockdown exceptions are ignored if multiple connections have lockdown. exceptions configured
PRS-365277	**Summary:** Location awareness rules may trigger lockdown rules to be applied.
PRS-365449	**Summary:** FTP using FileZilla on macOS over Pulse causes kernel panic.
PRS-365328	**Summary:** If always-on VPN is configured with exception rules and one of the resources defined is IPv6, it cannot be reached when the tunnel is down.
PRS-365282	**Summary:** Captive portal URL redirection fails using the Pulse embedded browser on macOS.
PRS-364837	**Summary:** /sbin/route is reported as missing after connection is established using Pulse UI on Linux.
PRS-364732	**Summary:** Certificate authentication fails if a user has previously used the embedded browser to present the certificate.
PRS-364682	**Summary:** Required dependencies may not be listed or installed when issuing “install_dependency_packages”.
PRS-364261	**Summary:** Captive portal redirection fails using the embedded browser when lockdown mode is configured.
PRS-360116	**Summary:** Pulse may fail to upgrade from legacy Juniper branded versions OR fail to upgrade if a Juniper branded version was installed previously and removed outside the add/remove programs interface.
PRS-362066	**Summary:** Pulse Secure client fails to install correctly when Cisco AnyConnect is present on

Problem Report Number	Release Note
	32-bit Windows-based systems.
PRS-357647	**Summary:** Startup script launch fails when lockdown is enabled on the Pulse Secure client configuration.
PRS-362159	**Summary:** DNS settings are not refreshed properly after Pulse launches on Windows 10 Redstone3 and later.
PRS-358500	**Summary:** Traffic enforcement does not function as expected on macOS clients.
PRS-363203	**Summary:** If an IPv6 only client connects to a PCS with FQDN-based VPN tunneling ACLs and split-tunneling network policies, Pulse will crash.
PRS-363072	**Summary:** SAML authentication using the embedded browser fails when using SAML on the default “*/“ URL.
PRS-362258	**Summary:** install_dependency_packages script does not function as expected on Fedora Core.
PRS-358184	**Summary:** Lockdown configuration is not enforced as expected when location awareness is enabled.

Known Issues in 9.0R2 Release

The following table lists known issues in this release.

Problem Report Number	Description
PRS-364505	**Symptom:** Traffic Enforcement is not getting applied for FQDN split tunneling resource. **Work Around:** None
PRS-365025	**Symptom:** Local IPv6 SSH/RDP session getting dropped and unable to establish again once the tunnel is up, when route precedence is "Tunnel routes with local subnet access" with Traffic Enforcement is enabled. **Work Around:** None
PRS-366655	**Symptom:** [macOS]Lockdown exception is not working when configure multiple process of specific application in single rule. **Work Around:** None
PRS-365195	**Symptom:** Lockdown Exception is not applying for UDP incoming traffic on MAC. **Work Around:** None
PRS-364865	**Symptom:**

Problem Report Number	Description
	macOS: Lockdown exception rule not able to create for macOS using Always-On VPN wizard. **Work Around:** None
PRS-366774	**Symptom:** macOS: Unable to access the resource once the tunnel is up when Kaspersky protection is ON. **Work Around:** None
PRS-364809	**Symptom:** Added macOS Lock down Exception rules are not displaying in Always-On VPN wizard. **Work Around:** Only Windows platform can configure through Always-On VPN wizard.
PRS-366596	**Symptom:** macOS: Standalone upgrade is failing when upgrading from 64-bit Pulse9. 0R2.xxxx to 64-bit Pulse9. 0R2.yyyy using 9.0R1 PCS. **Work Around:** Upgrade should be done through browser.
PRS-365870	**Symptom:** Lock-down mode is not working as expected if user clicks on cancel button after initiating the connection, when multiple lock down connections exists. **Work Around:** 1. Administrator must configure same LA rule on all lock down enabled connection. 2. Otherwise administrator must uncheck “Allow user to override the connection “checkbox while configuring lock down by enabling auto-connect.
PRS-365739	**Symptom:** For macOS, Lock-down mode is not working as expected if user establishes tunnel with non-lock down enabled connection. **Work Around:** Administrator must uncheck the “Allow User connection” checkbox, while creating VPN Only Access connection and administrator should not create any non-lock down connection while creating lock-down connection for VPN Only Access enabled connection.
PRS-365144	**Symptom:** From 9.0R2 release onwards, Pulse Secure Desktop client for macOS is not supported for version 10.10 or below. **Work Around:** User needs to upgrade macOS to 10.11 version or above.

New Features in 9.0R1 Release

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

Feature	Description
Embedded Browser for Pulse Desktop Client (Windows and macOS)	Pulse Desktop Clients on Windows and macOS now support an embedded browser that is used for SAML flows for a built-in streamlined user experience. This also integrates the host checking across browser and tunnel contexts speeding up user logins.
Always-On with VPN-only support on macOS	Always-On provides a highly seamless user experience where the secure VPN connection is established automatically when user moves outside of corporate network and the VPN connection is terminated once user comes into the corporate network. In addition to Always-On, if Lockdown mode feature is enabled, it provides compliance enforcement by preventing all network traffic if VPN is not established. Together, Always-On with Lockdown mode provide tight compliance solution with best end-user experience. This feature is supported on Windows from 8.3R3 onwards.
Always-On Wizard	Always-On VPN, VPN-only access provides lot of flexibility for the administrator. To simplify the configuration of this solution, a dedicated wizard will be provided so that administrator can complete the configuration from one place and roll out the production.
Minimum Client Enforcement	This release adds enhancements to minimum client version enforcement to handle older clients, and to prevent the tunnel from being established at all if the client version is below the minimum specified. This addresses shortcoming in the earlier implementation where clients could get access for a brief window before being disconnected even when they were not meeting the minimum client version criteria.
Linux Support	Pulse Desktop Client on Linux has been validated on all the below distributions. • Ubuntu 16.04 (long term release – LTS) – 32 bit and 64 bit • Ubuntu 17.10 (short release cycle) – 64 bit only • Debian 9.3 – 32 bit and 64 bit • Cent OS 7.4 (Build 1708) – 64 bit only • RHEL 7.4 – 64 bit only • Fedora 27 – 32 bit and 64 bit
Captive Portal Support on macOS	When Always-On with Lockdown mode is configured, and if the user is connecting from network protected with captive portal (For example: Hotel Wi-Fi), an exception is required to allow connection to captive portal before VPN can be established. This scenario is handled by the Pulse Desktop Client so that user can connect to captive portal and then proceed to VPN connection automatically.
FQDN based split tunneling Resources	Administrator can now configure split tunnel rules (Include / Exclude) by specifying the domain names instead of just IP Address/Netmask. Pulse Desktop Clients will now determine the traffic to be tunneled or not based on domain names that are configured in split tunnel rules. This capability provides a very efficient way of handling split tunnel decisions for SaaS apps or apps controlled using automation infrastructure where IP address assignment is dynamic. Note: This feature is supported only for IPv4.

Product Codes (GUIDs) for SCCM Deployments in 9.0R1 Release

If you deploy the Pulse Secure desktop client using System Center Configuration Manager (SCCM, formerly SMS), it can be helpful to know the Product Codes (GUIDs) of Pulse Secure desktop client installation bundles. SCCM uses these codes to determine whether products are already installed. The table below gives the product codes for version 9.0R1 of the desktop client for the given the architecture (32-bit or 64-bit) and locale (language environment).

PulseSecure.x86.msi

- English - {EE3930B3-E66B-4EAD-BC27-42B8F2142C4E}
- Chinese (Taiwan) - {AE6100E7-C860-420D-8D89-0D06FC4CA4AC}
- German - {08580796-F9A9-4A68-AA94-888FD3EDA611}
- Spanish - {1A044462-44A7-4AB8-88CB-07015D0242AA}
- French - {0A843FE3-A7F1-4B28-9655-C51F98414769}
- Italian - {921C2EFF-4BD7-42BF-A31E-B26F91D0B2E4}
- Japanese - {41D0A593-32F2-49AF-A545-1B38CA85935A}
- Korean - {5E98BE22-BE02-49CB-8773-18AAB89E00DB}
- Polish - {02A6D93F-9B20-4F49-BB26-335DD8CEE055}
- Chinese (China) - {E51C4C30-8EC9-47BC-A9C9-8B25BC873915}

PulseSecure.x64.msi

- English - {28E3A8E9-0D70-4418-BBBE-13504BE951ED}
- Chinese (Taiwan) - {5363250F-B693-4D34-85D9-9F6C89926E8E}
- German - {38624669-9517-4086-BFAD-1F19AA9B6BB7}
- Spanish - {0822E1DA-C92F-4297-A191-188B1817723C}
- French - {B7B80A9C-91AA-4DE8-A757-7EC5A7CE69DD}
- Italian - {7BAD308D-9737-470A-93DB-52BDA3B05B72}
- Japanese - {99F26B30-923C-41FC-84B5-9880F419451A}
- Korean - {124777B5-3E6A-4D49-835A-529C74819C20}
- Polish - {E1CD56A2-79E5-414D-8ECD-13093BF3A0CC}
- Chinese (China) - {9CBB3A35-0BCF-4EF3-A4D6-E96919258E3E}

Fixed Issues in 9.0R1 Release

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

Problem Report Number	Release Note
PRS-360114	**Summary:** Incorporate final fix for Docker software's virtual adapter is being identified as physical, breaking wireless suppression.
PRS-361636	**Summary:** Pulse Secure Desktop client crash when SalesForce IDP and Embedded Browser is used.
PRS-360540	**Summary:** Pulse: Use Desktop Credentials with CP does not work if LDAP with UPN is configured.

Problem Report Number	Release Note
PRS-360378	**Summary:** Pulse Desktop Client: Lock down mode enforced on the windows PC is disabled in certain scenario.
PRS-360104	**Summary:** Pulse Desktop Cred Prov hanging with 5.3R4.1 on a number of Win7 machines and Win 10.
PRS-360083	**Summary:** Pulse Linux client issue with MTU.
PRS-360034	**Summary:** Pulse Desktop Cred-Prov and AD account lockout (pulse client 5.3R3).
PRS-359984	**Summary:** On a Failed standard AD authentication attempt, two failed authentication artempts are recorded.
PRS-359564	**Summary:** Pulse Desktop cred prov hanging with 5.3R4.1 on a number of Win7 machines.
PRS-358499	**Summary:** Pulse adding a backslash in front of UPN when Credential Provider is enabled so LDAP authentication fails.
PRS-357445	**Summary:** Credential provider tile is defaulting to username and password instead of last user authentication method.
PRS-357157	**Summary:** EXIT (退出) button for the Pulse client icon in Windows taskbar notification tray is wrongly displayed as EDIT (编辑) for Chinese Simplified language.
PRS-355816	**Summary:** "Failed to register accept socket handler" when creating loopback proxy url with Pulse Secure Desktop client.
PRS-355602	**Summary:** Proxy prompt with Pulse Secure client 5.2R8 when credential provider is configured.
PRS-347650	**Summary:** Pulse secure client displays pre sign -in notification message without Word wrap.
PRS-302221	**Summary:** Host Checker crashes (OPSWAT) on client PC with McAfee installed.
PRS-358632	**Summary:** Revert the docker fix from master since it did not solve customer issue.
PRS-343837	**Summary:** Inconsistency may observe when using certificate authentication on cent OS 6.4.
PRS- 350525	**Summary:** Inaccurate statistics sent to accounting server when layer 3 VPN is formed with Pulse client.
PRS-359721	**Summary:** Unable to install pulse client - Cisco Any connect Inter-compatibility.
PRS-359668	**Summary:** Pulse Client "Connect" button greyed out for RSA Secondary Auth after upgrade of Pulse Client.
PRS-359614	**Summary:** Truncated message is displayed on Pulse client UI, when change password failed due to restriction on Japanese OS.

Problem Report Number	Release Note
PRS-359611	**Summary:** Truncated message is displayed on Pulse client UI, when change password failed due to restriction on Japanese OS.
PRS-359264	**Summary:** Pulse: After applying MS Patch KB4056892, VPN session establishment fail with Error:1308. HC applied at realm level.
PRS-359259	**Summary:** After applying MS Patch KB4056892, VPN session establishment fail with Error:1329. HC applied at role level.
PRS-358829	**Summary:** MITM attack can influence the user interface of the Pulse Secure client.
PRS-357157	**Summary:** EXIT (退出) button for the Pulse client icon in Windows taskbar notification tray is wrongly displayed as EDIT (编辑) for Chinese Simplified language.
PRS-353991	**Summary:** Junos Pulse Operational logs in event viewer is missing after upgrading the pulse client version from 5.1Rx to 5.2Rx.
PRS-344377	**Summary:** Agent version doesn't get populated in Active User Screen when pulse is launched from browser.
PRS-316880	**Summary:** [UAC] Time issue with GUAM access after upgrade from 4.2R4 to 5.0R5.

Known Issues in 9.0R1 Release

The following table lists known issues in this release.

Problem Report Number	Description
PRS-363203	**Symptom:** VPN traffic will not go through tunnel when IPv4 stack is disabled on client machine and Split tunneling is enabled on the PCS server. **Condition:** The issue is observed in PDC 9.0R1. **Work Around:** Enable IPv4 stack on client machine.
PRS-363205	**Symptom:** Deleting the FQDN route added by the PDC on the client machine will make the FQDN resource take the tunnel route. **Condition:** The issue is observed in PDC 9.0R1. **Work Around:** None
PRS-363072	**Symptom:** Embedded browser remains stuck on "Signing in to Pulse Secure" with OKTA IDP when SAML is configured for the default Sign-in URL. **Condition:** The issue is observed in PDC 9.0R1. **Work Around:** Use a custom Sign in URL like */saml (i.e. */*)

Problem Report Number	Description
PRS-362545	**Symptom:** SAML 1.1 version is not working with embedded browser. **Condition:** The issue is observed in PDC 9.0R1. **Work Around:** None
PRS-363126	**Symptom:** Need to remove the "custom sign-in or token-based authentication" string in "embedded browser for authentication" description. **Condition:** The issue is observed in PDC 9.0R1. **Work Around:** None
PRS-362895	**Symptom:** Cert Auth not working in Cent OS 6.9. **Condition:** The issue is observed in PDC 9.0R1. **Work Around:** The certificate authentication through UI will be supported only on the machines using libsoup 2.48 and above.
PRS-360565	**Symptom:** If only FQDN routes are mentioned in both [allow and deny policy] and [allow only policy] the PCS server will not send the default route. All the IPV4 traffic will not go through the tunnel. If only FQDN routes are mentioned as deny policy, then default route will be sent from the PCS server. **Condition:** The issue is observed in PDC 9.0R1. **Work Around:** NA
PRS-360938	**Symptom:** After unchecking the Enable minimum client version enforcement, Save button is not working. **Condition:** The issue is observed in PDC 9.0R1. **Work Around:** None
PRS-362258	**Symptom:** Installation of 32-bit Linux PDC client in Fedora Core 26 shows webkitgtk as a dependency, but fails to install it. **Condition:** The issue is observed in PDC 9.0R1 on Linux Client. **Work Around:** Install the dependencies using the following command: `yum install webkitgtk.i686`
PRS-361894	**Symptom:** VPN connection established through Linux Pulse Client will get disconnected after 2 minutes once the user clicks on “OK” or “Cancel” button on the dialogue box that states “Your session expired due to inactivity. Click on [OK] to login again” **Condition:** The issue is observed in PDC 9.0R1 on Linux Client. **Work Around:** None.

Problem Report Number	Description
PRS-361777	**Symptom:** If the Fedora Linux user installs 9.0 R1 version of Pulse Desktop Client over Fedora Core 26, and upgrade the OS to Fedora Core 27 then Pulse Desktop Client will not be launched after the installation. **Work Around:** Execute the following command as root user: /usr/local/pulse/ConfigurePulse_x86_64.sh install_dependency_packages.
PRS-360661	**Symptom:** Captive Portal Detection under lock down mode is failing for the first time when user is moved to captive portal environment. **Work Around:** None.
PRS-360657	**Symptom:** User credentials are getting auto-saved. **Work Around:** None.
PRS-359288	**Symptom:** FQDN resource with server-side proxy enabled does not get routed through the proxy. **Work Around:** None.
PRS-360005	**Symptom:** Previously added client routes are not getting deleted from the client PC. **Work Around:** None.
PRS-360054	**Symptom:** Error message will not get displayed if Pulse Desktop Client version is lesser than the Minimum Client Version Enforcement. **Condition:** The issue is observed in Pulse Desktop Client 5.2 R10 and 5.3 R2 on Windows and macOS. **Work Around:** None.
PRS-360039	**Symptom:** Tab and Enter keys are not working in embedded browser on Windows. **Work Around:** User should click the button using mouse point.
PRS-360414	**Symptom:** SAML authentication is failing when configure IP based URL instead of FQDN based URL in PDC. **Work Around:** User should use FQDN based URL instead of IP based URL.
PRS-358184	**Symptom:** Lock down is not applied for network traffic started before Pulse Firewall Kernel extension is loaded. **Work Around:** User needs to restart the machine.
PRS-358397	**Symptom:** Host checker doesn't detect AVG antivirus on Windows Server 2016. **Work Around:** None

Problem Report Number	Description
PRS-357472	**Symptom:** PDC is not supporting IPv6 DNS server of SA if "device only" is selected in DNS search order with Split Tunneling. **Work Around:** User needs to provide an IPv4 DNS server in SA.
PRS-358153	**Symptom:** From 5.3R4 release onwards, Pulse Secure Desktop client for macOS is not supported for version 10.9 or below. **Work Around:** User needs to upgrade macOS to 10.10 version or above.
PRS-356847	**Symptom:** Pulse Application Launcher detects incorrect OS for Windows Server 2012 R2 and Windows Server 2016. **Work Around:** None
PRS-356967	**Symptom:** Agent type is displayed as Windows Pulse Secure instead of Windows Server 2012 R2, 2016, once tunnel has been established in PCS active users page. **Work Around:** None
PRS-356794	**Symptom:** Displays wrong agent type in active users for Windows Server 2008, 2012 and 2016 when logged in through browser. **Work Around:** None
PRS-357966	**Symptom:** Session Time Left does not get updated once PulseUI is relaunched. **Work Around:** None
PRS-358002	**Symptom:** Session Idle Timeout and Max. Session Length warnings do not get displayed during an active session if Pulse Linux Desktop Client is in closed state. **Work Around:** None
PRS-358519	**Symptom:** Host Checker Compliance does not get updated after re-launching Linux Pulse Desktop Client. **Work Around:** None
PRS-355909	**Symptom:** When older clients try to connect to a PCS device which is configured with Encryption type as ESP SHA2 and ESP Transport only as enabled on a server, client fails to establish the session. **Work Around:** Disable the ESP Transport only option till all the clients upgraded to latest Pulse client build. Re-enable the option, once all the clients are upgraded.
PRS-355316	**Symptom:** Pulse Secure Linux Client can be configured to authenticate to a SAML server. However, enabling Host Checker feature on SAML connections is not supported **Work Around:** Disable the Host Checker.
PRS-355466	**Symptom:**

Problem Report Number	Description
	Unable to ping through the tunnels created by Pulse Secure Linux Client when installed on default installation of Ubuntu 15.04 with Kernel version 3.19.0-15. **Work Around:** Upgrading the kernel to 3.19.0-84.
PRS- 347284	**Symptom:** Upgrading Pulse from 5.2R5 (or prior) to 5.2R6 on Linux shows "downgrading" **Work Around:** None

Documentation

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

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation.

You can send your comments to techpubs-comments@pulsesecure.net.

Technical Support

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

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

For more technical support resources, browse the support (https://www.pulsesecure.net/support).

Revision History

The following table lists the revision history for this document.

Revision	Date	Description
9.0R2.1	February 2019	Updated feature **Linux Support** under section "New Features in 9.0R1 Release".
9.0R2.1	October 2018	Product GUIDs added for 9.0R2.1
9.0R2.1	September 2018	9.0R2.1 Update
9.0R2	August 2018	9.0R2 Update
9.0R1	April 2018	9.0R1 Update
9.0R1 Beta	February 2018	Initial Publication – 9.0R1 Beta