



Pulse Desktop Client

Release Notes

PDC 9.0R1, 571

Release, Build

9.0R1, 571

Published

April, 2018

Document Version

1.1

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

© 2018 by Pulse Secure, LLC. All rights reserved.

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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

END USER LICENSE AGREEMENT

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

Contents

Introduction4

Interoperability and Supported Platforms4

General Notes4

Upgrade Paths4

Caveats, Important Changes, and Deprecated Features4

New Features in 9.0R1 Release.....4

Product Codes (GUIDs) for SCCM Deployments in 9.0R1 Release5

Fixed Issues in 9.0R1 Release6

Known Issues in 9.0R1 Release7

Documentation 11

DocumentationFeedback 11

Technical Support..... 11

Revision History..... 11

Introduction

This release-notes document for the Pulse Secure desktop client version 9.0R1. This document provides a cumulative list of all enhancements, fixes and known issues for the 9.0R1 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 or Mac OS 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 (which can be found at Pulse Secures Technical Publications site).

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
5.3Rx	You can upgrade directly to 9.0R1
5.2Rx	You can upgrade directly to 9.0R1
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 9.0R1. Pulse Secure desktop client Beta program, please un-install the Beta 9.0R1 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 SHA-2-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.)

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 Mac)	Pulse Desktop Clients on Windows and Mac now support an embedded browser that is used for SAML flows for a built-in streamlined user experience.

Feature	Description
	This also integrates the host checking across browser and tunnel contexts speeding up user logins.
Always-On with VPN-only support on Mac OSX	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	<p>Pulse Desktop Client on Linux has been validated on all the below distributions. Both 32-bit and 64-bit Clients are validated.</p> <ul style="list-style-type: none"> • Ubuntu 16.04 (long term release – LTS) • Ubuntu 17.10 (short release cycle) • Debian 9.3 • Cent OS 7.4 (Build 1708) • RHEL 7.4 • Fedora 27
Captive Portal Support on Mac OS	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	Incorporate final fix for Docker software's virtual adapter is being identified as physical, breaking wireless suppression.
PRS-361636	Pulse Secure Desktop client crash when Salesforce IDP and Embedded Browser is used.
PRS-360540	Pulse: Use Desktop Credentials with CP does not work if LDAP with UPN is configured.
PRS-360378	Pulse Desktop Client: Lock down mode enforced on the windows PC is disabled in certain scenario.
PRS-360104	Pulse Desktop cred prov hanging with 5.3R4.1 on a number of Win7 machines and Win 10.
PRS-360083	Pulse Linux client issue with MTU.
PRS-360034	Pulse Desktop Cred-Prov and AD account lockout (pulse client 5.3R3).
PRS-359984	On a Failed standard AD authentication attempt, two failed authentication attempts are recorded.
PRS-359564	Pulse Desktop cred prov hanging with 5.3R4.1 on a number of Win7 machines.
PRS-358499	Pulse adding a backslash in front of UPN when Credential Provider is enabled so LDAP authentication fails.
PRS-357949	PSIRT: PDC on MAC Local privilege escalation from /tmp folder.
PRS-357946	PSIRT: PDC on MAC - Metacharacter Injection.
PRS-357935	PSIRT : PDC on MAC - Format string vulnerability.

Problem Report Number	Release Note
PRS-357445	Credential provider tile is defaulting to username and password instead of last user authentication method.
PRS-357157	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	"Failed to register accept socket handler" when creating loopback proxy url with Pulse Secure Desktop client.
PRS-355602	Proxy prompt with Pulse Secure client 5.2R8 when credential provider is configured.
PRS-347650	Pulse secure client displays pre sign -in notification message without Word wrap.
PRS-302221	Host Checker crashes (OPSWAT) on client PC with McAfee installed.
PRS-358632	Revert the docker fix from master since it did not solve customer issue.
PRS-343837	Inconsistency may observe when using certificate authentication on cent OS 6.4.
PRS- 350525	Inaccurate statistics sent to accounting server when layer 3 VPN is formed with Pulse client.
PRS-359721	Unable to install pulse client - Cisco Any connect Inter-compatibility.
PRS-359668	Pulse Client "Connect" button greyed out for RSA Secondary Auth after upgrade of Pulse Client.
PRS-359614	Truncated message is displayed on Pulse client UI, when change password failed due to restriction on Japanese OS.
PRS-359611	Truncated message is displayed on Pulse client UI, when change password failed due to restriction on Japanese OS.
PRS-359264	Pulse: After applying MS Patch KB4056892, VPN session establishment fail with Error:1308. HC applied at realm level.
PRS-359259	After applying MS Patch KB4056892, VPN session establishment fail with Error:1329. HC applied at role level.
PRS-358829	MITM attack can influence the user interface of the Pulse Secure client.
PRS-358008	PSIRT: PDC on MAC local privilege escalation net.pulsesecure.UninstallPulse.plist.
PRS-358005	PSIRT: PDC on MAC local privilege escalation /Library/Application Support/Pulse Secure/Pulse (777).
PRS-357157	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	Junos Pulse Operational logs in event viewer is missing after upgrading the pulse client version from 5.1Rx to 5.2Rx.
PRS-344377	Agent version doesn't get populated in Active User Screen when pulse is launched from browser.
PRS-316880	[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	<p>Symptom: VPN traffic will not go through tunnel when IPv4 stack is disabled on client machine and Split tunnelling is enabled on the PCS server.</p> <p>Condition: The issue is observed in PDC 9.0R1.</p> <p>Work Around: Enable IPv4 stack on client machine.</p>
PRS-363205	<p>Symptom: Deleting the FQDN route added by the PDC on the client machine will make the FQDN resource take the tunnel route.</p> <p>Condition: The issue is observed in PDC 9.0R1.</p> <p>Work Around: None</p>
PRS-363072	<p>Symptom: Embedded browser remains stuck on "Signing in to Pulse Secure" with OKTA IDP when SAML is configured for the default Sign-in URL.</p> <p>Condition: The issue is observed in PDC 9.0R1.</p> <p>Work Around: Use a custom Sign in URL like */saml (i.e. */*)</p>
PRS-362545	<p>Symptom: SAML 1.1 version is not working with embedded browser.</p> <p>Condition: The issue is observed in PDC 9.0R1.</p> <p>Work Around: None</p>
PRS-363126	<p>Symptom: Need to remove the "custom sign-in or token based authentication" string in "embedded browser for authentication" description.</p> <p>Condition: The issue is observed in PDC 9.0R1.</p> <p>Work Around: None</p>
PRS-362895	<p>Symptom: Cert Auth not working in Cent OS 6.9.</p> <p>Condition: The issue is observed in PDC 9.0R1.</p> <p>Work Around: None</p>
PRS-360565	<p>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.</p> <p>Condition: The issue is observed in PDC 9.0R1.</p> <p>Work Around: NA</p>
PRS-360938	<p>Symptom: After unchecking the Enable minimum client version enforcement, Save button is not working.</p> <p>Condition: The issue is observed in PDC 9.0R1.</p> <p>Work Around: None</p>

Problem Report Number	Description
PRS-362258	<p>Symptom: Installation of 32 bit Linux PDC client in Fedora Core 26 shows webkitgtk as a dependency, but fails to install it.</p> <p>Condition: The issue is observed in PDC 9.0R1 on Linux Client.</p> <p>Work Around: Install the dependencies using the following command: <code>yum install webkitgtk.i686</code></p>
PRS-361894	<p>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"</p> <p>Condition: The issue is observed in PDC 9.0R1 on Linux Client.</p> <p>Work Around: None.</p>
PRS-361777	<p>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.</p> <p>Work Around: Execute the following command as root user: <code>/usr/local/pulse/ConfigurePulse_x86_64.sh install_dependency_packages.</code></p>
PRS-360661	<p>Symptom: Captive Portal Detection under lock down mode is failing for the first time when user is moved to captive portal environment.</p> <p>Work Around: None.</p>
PRS-360657	<p>Symptom: User credentials are getting auto-saved.</p> <p>Work Around: None.</p>
PRS-359288	<p>Symptom: FQDN resource with server-side proxy enabled does not get routed through the proxy.</p> <p>Work Around: None.</p>
PRS-360005	<p>Symptom: Previously added client routes are not getting deleted from the client PC.</p> <p>Work Around: None.</p>
PRS-360054	<p>Symptom: Error message will not get displayed if Pulse Desktop Client version is lesser than the Minimum Client Version Enforcement.</p> <p>Condition: The issue is observed in Pulse Desktop Client 5.2 R10 and 5.3 R2 on Windows and Mac.</p> <p>Work Around: None.</p>
PRS-360039	<p>Symptom: Tab and Enter keys are not working in embedded browser on Windows.</p> <p>Work Around: User should click the button using mouse point.</p>
PRS-360414	<p>Symptom: SAML authentication is failing when configure IP based URL instead of FQDN based URL in PDC.</p> <p>Work Around: User should use FQDN based URL instead of IP based URL.</p>

Problem Report Number	Description
PRS-358184	<p>Symptom: Lock down is not applied for network traffic started before Pulse Firewall Kernel extension is loaded.</p> <p>Work Around: User needs to restart the machine.</p>
PRS-358397	<p>Symptom: Host checker doesn't detect AVG antivirus on Windows Server 2016.</p> <p>Work Around: None</p>
PRS-357472	<p>Symptom: PDC is not supporting IPv6 DNS server of SA if "device only" is selected in DNS search order with Split Tunneling.</p> <p>Work Around: User needs to select other DNS searching order or IPv4 DNS server.</p>
PRS-358153	<p>Symptom: From 5.3R4 release onwards, Pulse Secure Desktop client for Mac OSX is not supported for version 10.9 or below.</p> <p>Work Around: User needs to upgrade Mac OSX to 10.10 version or above.</p>
PRS-356847	<p>Symptom: Pulse Application Launcher detects incorrect OS for Windows Server 2012 R2 and Windows Server 2016.</p> <p>Work Around: None</p>
PRS-356967	<p>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.</p> <p>Work Around: None</p>
PRS-356794	<p>Symptom: Displays wrong agent type in active users for Windows Server 2008, 2012 and 2016 when logged in through browser.</p> <p>Work Around: None</p>
PRS-357966	<p>Symptom: Session Time Left does not get updated once PulseUI is relaunched.</p> <p>Work Around: None</p>
PRS-358002	<p>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.</p> <p>Work Around: None</p>
PRS-358519	<p>Symptom: Host Checker Compliance does not get updated after re-launching Linux Pulse Desktop Client.</p> <p>Work Around: None</p>
PRS-355909	<p>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.</p> <p>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.</p>
PRS-355316	<p>Symptom:</p>

Problem Report Number	Description
	<p>Pulse Secure Linux Client can be configured to authenticate to a SAML server. However, enabling Host Checker feature on SAML connections is not supported</p> <p>Work Around: Disable the Host Checker.</p>
PRS-355466	<p>Symptom: 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.</p> <p>Work Around: Upgrading the kernel to 3.19.0-84.</p>
PRS- 347284	<p>Symptom: Upgrading Pulse from 5.2R5 (or prior) to 5.2R6 on Linux shows "downgrading"</p> <p>Work Around: None</p>

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 ([website https://www.pulsesecure.net/support](https://www.pulsesecure.net/support)).

Revision History

The following table lists the revision history for this document.

Revision History

Revision	Date	Description
9.0R1	April, 2018	9.0R1 Update
9.0R1 Beta	February, 2018	Initial Publication – 9.0R1 Beta