



Pulse Desktop Client

Release Notes 9.1R2

PDC 9.1R2 Build 901

PDC 9.1R2 Linux Build 69

Release

9.1R2

Published

September 2019

Document Version

1.2.1

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

© 2019 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.

Revision History

The following table lists the revision history for this document.

Revision	Date	Description
9.1R2	September 2019	Cosmetic Change
9.1R2	September 2019	Updated the "Known Issues in 9.1R2 Release" section.
9.1R2	July 2019	Initial Publication – 9.1R2
9.1R1	May 2019	Initial Publication – 9.1R1

Contents

Revision History	3
Introduction.....	5
Interoperability and Supported Platforms	5
General Notes.....	5
Upgrade Paths.....	5
Caveats, Important Changes, and Deprecated Features.....	5
New Features in 9.1R2 Release	6
Product Codes (GUIDs) for SCCM Deployments in 9.1R2 Release.....	6
Fixed Issues in 9.1R2 Release	7
Known Issues in 9.1R2 Release	7
New Features in 9.1R1 Release	8
Product Codes (GUIDs) for SCCM Deployments in 9.1R1 Release.....	8
Fixed Issues in 9.1R1 Release	9
Known Issues in 9.1R1 Release	10
Documentation.....	14
Documentation Feedback.....	14
Technical Support	14

Introduction

This is the release-notes document for the Pulse Secure Desktop Client version 9.1R2. This document provides a cumulative list of all enhancements, fixes and known issues for the 9.1R2. 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](#).

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

Upgrade Paths

The following table describes the tested upgrade paths.

Release	Description
9.0Rx	You can upgrade directly to 9.1R2.
5.3Rx	You can upgrade directly to 9.1R2.
5.0Rx or 5.1Rx or 5.2Rx	You can upgrade directly to 5.3Rx by installing the 5.3Rx update.

Note: For Pulse SAM connection, user will not be able to upgrade to 9.1Rx from pre-9.0R3 builds. User needs to upgrade via the browser. Also, on Windows 7 machine, user will not be able to establish the Pulse SAM connection with pre-9.1R1 PCS.

Caveats, Important Changes, and Deprecated Features

Please note that client upgrades are not supported to or from beta releases.

Important Note: To run the Pulse Secure Desktop Client version 5.3R1 or later a Windows 7 machine, the machine must contain a March 10, 2015 Windows 7 Update 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). 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 9.1R2 Release

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

Feature	Description
FQDN resource and IPv4 resource-based split tunneling conflict resolution	Pulse Connect Secure (PCS) supports both FQDN-based and IP-based split tunneling capability. When customers use both the split tunneling rules, PCS now provides flexibility for the customers to choose which rules to give precedence, and ensures the resource access is not impacted when there are conflicting rules.
Manage Pulse Secure Client Versions feature support	Pulse Connect Secure now supports ability to enforce minimum client version that can connect to the VPN. Admin will have the flexibility to provide minimum version separately for desktop and mobiles to enforce the different client versions.
Support for Windows 10 Version 1903 (OS build 10.0.18362.207)	Pulse Desktop Client on Windows now supports Windows 10 Version 1903 (OS build 10.0.18362.207) Enterprise, 64 bit and Windows 10 Version 1903 (OS build 10.0.18362.207) Professional, 64 bit.
macOS KEXT Notarization	Apple mandates that all macOS applications are notarized by Apple. Pulse macOS Client KEXT component is now notarized by Apple.

Product Codes (GUIDs) for SCCM Deployments in 9.1R2 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 9.1R2 of the desktop client for the given the architecture (32-bit or 64-bit) and locale (language environment).

PulseSecure.x86.msi

- English - {25CFACD8-CAAC-4FA5-9054-34C58140B1D3}
- Chinese (Taiwan) - {DD6DA542-4D51-4182-98CD-7F73A0B15B81}
- German - {AA83EB42-3662-49DB-A6B9-7F70AA74E439}
- Spanish - {605BC1B9-FF40-4073-A3D0-C943CC668DAF}
- French - {7740527C-A2E4-42FD-8A12-F4337AB3DA17}
- Italian - {B1ABE9F2-1C59-45B9-BB7F-EA1F4689A0FA}
- Japanese - {32285458-FE60-481C-B618-0E50285C2C91}
- Korean - {AEDDC0C0-756A-4DEC-9862-A88083535CA7}
- Polish - {A549BAFC-D6D7-4A54-A147-3D72D7C082FB}
- Chinese (China) - {4E8E635F-9443-4250-89F3-9D5F046AEA45}

PulseSecure.x64.msi

- English - {DDFE22C2-8C81-45D6-8C95-932C1EDAD5EF}
- Chinese (Taiwan) - {7031AF51-BC44-4C6D-8649-AC8D5F3FC796}

- German - {F1133159-3AC3-41D1-A5BE-49958C4E3AA1}
- Spanish - {A73D39F3-AE14-4BE5-823E-F42A79557956}
- French - {C6B0EC3E-F8C1-4001-A2AF-8E23968460B4}
- Italian - {B515EF30-FDB1-4200-A468-7BE0DEABED51}
- Japanese - {0B5AB9AA-5639-4DB9-B429-D9E491B995CB}
- Korean - {678B1E92-9DFC-4D6C-B6E8-AA6117249E55}
- Polish - {198BB78A-1907-45BD-8DBC-36C2FC73AA95}
- Chinese (China) - {8F7E1898-6918-4929-BCCB-55E259DD4364}

Fixed Issues in 9.1R2 Release

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

Problem Report Number	Summary
PRS-372170	Summary: Missing certificate issue when Pulse client is launched in Ubuntu 18.0.4 version.
PRS-360574	Summary: IPv6 - After upgrading the Pulse Desktop Client from 5.3R2 to 5.3R4.1 on macOS machine, IPv6 DNS is not getting set on the Virtual adapter.
PRS-374418	Summary: Pulse Client Uninstall.app is not code signed.
PRS-376098	Summary: Logon Scripts are not running with lockdown mode enabled.
PRS-371051	Summary: Installing Pulse Desktop Client 9.0R2+ on macOS creating crippling performance hit over time.
PRS-371718	Summary: Kernel panic issues is observed on MAC Mojave (10.14) with Pulse Desktop Client version 9.0R3 (build 1599).
PRS-374606	Summary: Machine tunnel is not working as expected with DNS domain suffix and step up deletes domain from the list incorrectly.
PRS-372350	Summary: NSIS error message is thrown after installing Pulse Desktop Client through SCCM.
PRS-372096	Summary: Smart card (Certificate) authentication is failing with Pulse Desktop Client 9.0R3 after Gemalto SafeNet client is upgraded to 10.2.
PRS-372087	Summary: Overwrite DNS suffixes on Mac clients.
PRS-368845	Summary: Pulse Random IPv4 resource is failing when ACL and split tunneling are configured with FQDN.

Known Issues in 9.1R2 Release


The following table lists known issues in this release.

Problem Report Number	Release Note
PRS-368884	<p>Symptom: 802.1x connection is not successful when performing switch user.</p> <p>Condition: 802.1x is configured for wired or wireless connection.</p> <p>Workaround: Connection type should be either machine only or user-then-machine.</p>
PRS-377549	Symptom: Older PSIS is not upgrading to 9.1R2 PSIS version.

Problem Report Number	Release Note
	<p>Condition: When Pulse Desktop Client is deployed from 9.1R2 on Windows endpoints, PSIS is not upgraded to the latest version.</p> <p>Workaround: Old PSIS will continue to work and no impact seen.</p>
PRS-378873	<p>Symptom: Pulse Desktop Client is getting disconnected frequently after connecting to PCS on macOS.</p> <p>Condition: Endpoint should be dual stack. PCS should be configured for FQDN based split tunneling with Route Monitor enabled.</p> <p>Workaround: Disable the option Route Monitor.</p>

New Features in 9.1R1 Release

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

Feature	Description
Launching Pulse Desktop Client using URL	<p>Pulse Desktop Client can now be launched using a URL. Customers can insert the URL in any tools (For example: Support ticket management tool), so that when user clicks on the URL, Pulse Desktop Client gets invoked and connects to the VPN.</p> <p> Note: Allow saving logon information option must be enabled in Pulse Connect Secure server settings to use Launching Pulse Desktop Client using URL feature. (Enable Allow saving logon information > Users > Pulse Secure Client > Connections > <connection name>).</p>
Pulse SAM IPv6 Support	<p>Pulse Desktop Client now supports IPv6 traffic tunneling in Pulse SAM mode on Windows 10, Windows 8.1 and Windows 7 platforms.</p>
Automatic Keyboard popup on Surface Pro	<p>When users select the username or password field on Pulse Desktop Client installed on a Windows Surface device, the virtual keyboard automatically pops up so that user can enter the credentials.</p>

Product Codes (GUIDs) for SCCM Deployments in 9.1R1 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 9.1R1 of the desktop client for the given the architecture (32-bit or 64-bit) and locale (language environment).

PulseSecure.x86.msi

- English - {D9BD510B-2DC6-4A20-8B26-D07C799C41FC}
- Chinese (Taiwan) - {174C857C-11BE-45D8-9063-37B02C1508B8}
- German - {BE7A60AA-3FF5-4D35-9CA7-461851369C4A}
- Spanish - {F3F3B743-BCF2-4601-BF6B-1078C0CE0704}

- French - {488CE0C8-77B0-4A2C-B3BA-D0A5CE2BDAC4}
- Italian - {376E943E-958C-47CD-9EE5-A40CBE6483B7}
- Japanese - {63B578ED-BD3E-40A6-B3F7-166708E49BA4}
- Korean - {972FA217-F5B6-4715-917F-BC0EF7407EFC}
- Polish - {C38E6C1E-9BA6-44C5-8E9B-16C8445AF457}
- Chinese (China) - {1953E341-C083-4661-8AE5-930A0A1E2106}

PulseSecure.x64.msi

- English - {AB8FE63C-3C46-4F5E-96AE-ED50CAF74723}
- Chinese (Taiwan) - {63EDC13F-9910-429A-AB79-0CA61FFB2CF1}
- German - {AA936E6F-A772-4974-9856-EBD778381786}
- Spanish - {F14E4340-BDC5-433E-A3AC-D822B84746B6}
- French - {F83F8C27-DAB0-4E6D-9DB0-EDAEA0EED12A}
- Italian - {F5492346-A562-4FD9-9F3D-E2A1A9A7B2CA}
- Japanese - {70F811F4-4269-4F3C-BB89-AE4AC46EA3ED}
- Korean - {9BA77365-3010-41EA-B35B-9FFFD3D9989C}
- Polish - {4D41B4DD-A16F-41B6-A38E-D9C19BD02CDE}
- Chinese (China) - {26D8FD5B-7B82-458C-8F61-C783E6F8619B}

Fixed Issues in 9.1R1 Release

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

Problem Report Number	Summary
PRS-376174	Summary: Symbolic link creation fails after Pulse upgrade.
PRS-369889	Summary: Authentication with Host Checker verification fails on Kernel 4.18.0-10.
PRS-371071	Summary: Unable to add multiple certificates to gnome-keyring.
PRS-375343	Summary: Pulse: Customer facing frequent disconnection post adding FQDN and IPv4 addresses in Split tunneling rules.
PRS-372327	Summary: Wireless suppression fails to re-enable wireless NIC when surface PRO's USB network adapter is unplugged.
PRS-371725	Summary: Pulse: macOS: Re-branding: Modified Username and Password Label not showing completely on MAC machines.
PRS-371066	Summary: Color management is not working in macOS 10.14(Mojave) when French language is used.
PRS-370972	Summary: Wireless disconnects after upgrading to Win 10 1803.
PRS-370894	Summary: Pulse desktop client prompts for proxy credentials when wild card exception is used in PCS URL.
PRS-370690	Summary: Captive Portal detection via Pulse client fails and shows a blank page with latest 9.0R2.1 version in Windows 10 OS.
PRS-370459	Summary: Pulse is not honoring the zscaler proxy exception.
PRS-370348	Summary: 20 seconds delay is observed to establish the tunnel when the unreachable proxy PAC is unreachable.

Known Issues in 9.1R1 Release

The following table lists known issues in this release.

Problem Report Number	Release Note
PRS-373432	<p>Symptom: For launching Pulse Desktop Client from the URL, the following are the prescribed parameters:</p> <ul style="list-style-type: none"> • <i>connect</i> • <i>name</i> • <i>server</i> • <i>userrealm</i> • <i>username</i> <p>Launching Pulse Desktop Client using URL might throw an error, if</p> <ul style="list-style-type: none"> • Same parameter is included multiple times while crafting the URL. • If any other non-prescribed parameter, other than above-mentioned five prescribed parameters are used. <p>Condition: Entering multiple values for the five parameters (<i>name</i>, <i>server</i>, <i>userrealm</i>, <i>username</i> and <i>store</i>) or any additional parameter, as shown in the following URLs:</p> <ol style="list-style-type: none"> 1. <code>pulsesecureclient://connect?name=NAME&server=SERVERURL&userrealm=REALM&username=USER1&username=USER2&store=TRUE&store=FALSE</code> In this example, multiple values (USER1 and USER2) for the parameter <i>username</i> and multiple values (TRUE and FALSE) for the parameter <i>store</i> are entered. 2. <code>pulsesecureclient://connect?name=NAME&server=SERVERURL&userrealm=REALM&username=USER&store=TRUE&extra=TRUE&other=SOMETHING</code> In this example, non-prescribed parameter(<i>other</i>) is used. <p>Workaround: None</p>
PRS-374076	<p>Symptom: When launching Pulse Desktop Client using URL, some characters in the <i>username</i> parameter might not get displayed in the Pulse Desktop UI as expected.</p> <p>Condition: Entering <i>username</i> parameter in the following URL:</p> <pre>pulsesecureclient://connect?name=NAME&server=SERVERURL&userrealm=REALM&username=test&=user&store=TRUE</pre> <p>In this example, username will be considered as test instead of test&=user.</p> <p>Workaround: Use ascii encoding values for special characters.</p> <p>In the above-mentioned example, for the username to be considered as test&=user, use %26 for & and %3D for = in the URL, as shown below:</p> <pre>pulsesecureclient://connect?name=NAME&server=SERVERURL&userrealm=REALM&username=test%26%3Duser&store=TRUE</pre>
PRS-373177	<p>Symptom: Launching Pulse Desktop Client using URL feature is not working as expected for differently worded values for the <i>server</i> parameter.</p> <p>Condition: Entering differently worded values for the <i>server</i> parameter.</p> <p>The following three URLs refer to the same connection, but server values are worded differently:</p> <p>Though the connections with the below three server URLs (<code>https://pcserver.com/sign-in/</code>, <code>https://pcserver.com/sign-in</code>, <code>pcserver.com/sign-in</code>) would ideally be the same connection, these three connections will be treated as different connections while launching PDC from URL.</p> <ul style="list-style-type: none"> • <code>pulsesecureclient://connect?name=Pulse Connection&server=https://pcserver.com/sign-in/&userrealm=Users&username=user1&store=TRUE</code> • <code>pulsesecureclient://connect?name= Pulse Connection &server=https://pcserver.com/sign-</code>

Problem Report Number	Release Note
	<p><i>in&userrealm=Users&username=user1&store=TRUE</i></p> <ul style="list-style-type: none"> <i>pulsesecureclient://connect?name= Pulse Connection &server=pcserver.com/sign-in&userrealm=Users&username=user1&store=TRUE</i> <p>Workaround: None</p>
PRS-374087	<p>Symptom: L3 based FQDN Split Tunneling feature with PSAM coexistence is not supported. Condition: Dual Stack is enabled in Pulse Desktop Client machine. Workaround: None</p>
PRS-374384	<p>Symptom: User will not be able to download the Pulse Desktop Client from any package. Condition: Pulse Desktop Client package is uploaded before the Pulse Connect Secure upgrade. Workaround: Upload the junosepulse.pkg and download the installers.</p>
PRS-374876	<p>Symptom: Unable to connect to Pulse Connect Secure Server from Pulse Desktop Linux Client. Condition: Primary network card of a machine has multiple aliased IP addresses set. Workaround: Ensure that the primary network card does not have multiple aliased IP addresses.</p>
PRS-374627	<p>Symptom: Wireless LAN L2 connection disconnects immediately when the LAN L2 connection is established. Condition: When FIPS is enabled for L2 wireless connection. Workaround: Disable the FIPS in wireless connection.</p>
PRS-375458	<p>Symptom: Pre Pulse9.0R3 client fails to establish the Pulse SAM connection with Pulse Connect Secure 9.1R1 version. Condition: Pulse SAM connection fails when Pre Pulse9.0R3 client tries to establish the Pulse SAM connection with PCS 9.1R1. Workaround: To upgrade Pulse Desktop Client, launch the Pulse Desktop Client through the browser 9.1R1.</p> <p> Note: Pulse SAM connection fails to connect due to the following error:</p> <p><i>"Failed to set dns name query event, err:87" or "Failed to set netbios query event " or "Failed to set tcp/udp samize event" or "Failed to set tcpConnect event" or "Failed to set dns srv query event".</i></p>
PRS-375900	<p>Symptom: Shutting down the client PC will trigger the machine tunnel. Condition: Credential Provider option is enabled, and the user shuts down the client PC. Workaround: None</p>
PRS-375897	<p>Symptom: Pulse Desktop Client will take few seconds to show as connected when the client PC goes from sleep mode to awake mode. Condition: Credential Provider option is enabled, and the client PC goes to sleep mode. Workaround: None</p>
PRS-373995	<p>Symptom: Pulse Desktop Client fails to trigger the Credential Provider. Condition: When the Windows machine gets restarted. Workaround: None</p>
PRS-375916	<p>Symptom: While launching Pulse Desktop Client from URL, it prompts for the realm name information, even if the realm name is mentioned in the URL. Condition: When Allow saving logon information option is not enabled in connection profile.</p>

Problem Report Number	Release Note
	Workaround: Enable Allow saving logon information option in connection profile.
PRS-375956	<p>Symptom: In case of an upgrade triggered from pulse desktop client from PDC 9.0R3 to 9.1R1 and once the upgrade process is completed, the user is unable to connect, and a network error is displayed in the connection status of the PDC UI.</p> <p>Condition: Upgrade using PDC on Windows 10 (x64) Redstone 5.</p> <p>Workaround: Reboot the machine after the upgrade or restart pulse secure service.</p>
PRS-376021	<p>Symptom: User's attempt to log in to a browser-based session fails with error message "Detected an Internal Error" sometimes.</p> <p>Condition: When accessing Mac via Safari.</p> <p>Workaround: Restart the machine.</p>
PRS-375766	<p>Symptom: Pulse Desktop Client fails to add the route in case of FQDN based split tunneling.</p> <p>Condition: While adding the route in the local system.</p> <p>Workaround: None</p>
PRS-376174	<p>Symptom: Upgrade of Linux Pulse Desktop Client displays the following warnings:</p> <ul style="list-style-type: none"> • In: failed to create symbolic link '/usr/local/pulse/libjavascriptcoregtk-1.0.so': File exists • In: failed to create symbolic link '/usr/local/pulse/libjavascriptcoregtk-1.0.so.0': File exists • In: failed to create symbolic link '/usr/local/pulse/libwebkitgtk-1.0.so': File exists • In: failed to create symbolic link '/usr/local/pulse/libwebkitgtk-1.0.so.0': File exists <p>Condition: While adding the route in the local system.</p> <p>Workaround: None</p>
PRS-376205	<p>Symptom: Advanced connection details are not displaying as expected for SAML embedded browser-based authentication.</p> <p>Condition: When Enable Session Extended option is enabled.</p> <p>Workaround: None</p>
PRS-376209	<p>Symptom: FQDN resource is going through the tunnel, even though it is configured in split tunneling excluded policy.</p> <p>Condition: When FQDN based split tunneling is enabled.</p> <p>Workaround: None</p>
PRS-376071	<p>Symptom: L2 Wireless suppression fails to re-enable the wireless NIC.</p> <p>Condition: Unplugging the wired USB network adapter from Surface Pro.</p> <p>Workaround: None</p>
PRS-376034	<p>Symptom: For stealth mode connection Use Desktop Credentials option should not be enabled while creating the connection.</p> <p>Condition: When stealth tunnel is configured for "Machine only" mode.</p> <p>Workaround: None</p>
PRS-376235	<p>Symptom: Pulse Desktop Client will be in connect state after replacing the connection set with the manually added connection.</p> <p>Condition: When added Sign-In URL is configured with VPN Only Access/Always-on VPN and Lock-down option is enabled.</p> <p>Workaround: Click on cancel instead of retry and try to establish the connection after one minute.</p>
PRS-376278	<p>Symptom: Unable to establish Pulse SAM connection on Windows 7 machine using Pulse Secure Desktop Client 9.1R1 connecting to pre-9.1R1 PCS.</p> <p>Condition: Pulse Secure Desktop Client 9.1R1 will not able to establish Pulse SAM connection with pre-9.1R1 PCS.</p> <p>Workaround: Use 9.1R1 PCS build.</p>
PRS-372921	<p>Symptom: TFTP connection is getting a timeout error.</p> <p>Condition: When Pulse SAM connection is established.</p> <p>Workaround: None</p>

Problem Report Number	Release Note
PRS-376378	Symptom: Delay is observed while accessing FQDN resources. Condition: When Split Tunneling with route monitor is enabled. Workaround: 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>).