Pulse Secure Desktop Client Release Notes

Pulse Secure Desktop Client v5.1r9.1
Build 61697

For more information on this product, go to **www.pulsesecure.net/products**.

Product Release	**5.1r9.1, #61697**
Published	**July 2016**
Revision	**1.4**

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

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 http://www.pulsesecure.net/support/eula. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

Introduction

This release-notes document for the Pulse Secure desktop client version 5.1. This document provides a cumulative list of all enhancements, fixes and known issues for the 5.1 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 or Mac OS X) 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 Secure's Technical Publications site).

General Notes

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: https://kb.pulsesecure.net/?atype=sa.

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.

New Features

No new features were introduced in the Pulse Secure Desktop Client version 5.1r9.1.

Caveats, Important Changes, and Deprecated Features

The Pulse Secure Desktop Client version 5.1r9.1 addresses issues described in security advisory SA40241.

Important note: In order to run the **Pulse Secure desktop client version 5.1R8 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 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 Pulse 5.1R8 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.)

Problems Resolved in 5.1R9.1

The Pulse Secure Desktop Client version 5.1r9.1 addresses issues described in security advisory SA40241.

Problems Resolved in Pulse5.1R9

The following table lists important fixes and enhancements that were introduced in Pulse 5.1r9.

Problem Report Number	Description

PRS-337218	Location awareness fails with 4G USB Dongles that report as virtual adapters rather than physical adapters.
PRS-339960	Users may be able to extend their session through Pulse if “Session Timeout Warning” is enabled AND “Session Extension” option is disabled.

Problems Resolved in Pulse5.1R8

The following table lists important fixes and enhancements that were introduced in Pulse 5.1r8.

Problem Report Number	Description
PRS-318774	Smart card authentication fails for Mac OS clients only when using the Pulse Secure desktop client.
PRS- 330425	Pulse fails to create a VPN tunnel on Mac OS X after disconnecting a VNC session.
PRS- 332159	Pulse does not create a default route for IPv6 after establishing VPN tunnel that assigns an IPv6 address.
PRS- 335786	Resolved CVE-2015-3194.
PRS- 338253	IPv6 default route is not created for the Pulse virtual adapter on Mac OS X clients.

Known Issues in Pulse5.1R8

The following table lists known issues in Pulse 5.1r8.

Problem Report Number	Description

PRS-337311	As described in the "Caveats" section of this document, the Pulse Secure desktop client version 5.1R8 and later are code-signed with SHA-2 certificates in order to meet new restrictions enforced by enforced by Microsoft operating systems in 2016. This new code-signing feature causes certain issues with older versions of Windows 7. Specifically, versions of Windows 7 that have not been patched since March 10, 2015 will not be able to load certain drivers and executables signed with SHA-2. These unpatched versions of Windows 7 will experience the error "An unexpected error occurred" when trying to run the Pulse SAM (either the standalone WSAM or the Pulse-integrated SAM) app-specific tunneling feature. Users' log files will contain the message: "The Juniper Networks TDI Filter Driver (NEOFLTR_821_42283) service failed to start due to the following error: Windows cannot verify the digital signature for this file. A recent hardware or software change might have installed a file that is signed incorrectly or damaged, or that might be malicious software from an unknown source." The workaround for this issue is to update the Windows 7 operating system to include the March 10, 2015 patch that allows for the loading of SHA-2-signed binaries and drivers.

Problems Resolved in Pulse5.1R7

The following table lists important fixes and enhancements that were introduced in Pulse 5.1r7.

Problem Report Number	Description
PRS-321099	802.1x authentication fails on a virtual NIC.
PRS- 331140	Location awareness may fail if moving between networks that share DNS servers.
PRS- 331871	The VPN tunnel may take extended time to connect if the proxy on the client cannot be reached and the Connection Profile is configured for "Preserve Client proxy" or "No Proxy".
PRS- 332223	Machine authentication fails if FIPS mode is enabled in the client connection set.
PRS- 332264	Pulse location awareness rules fail when connected via USB dongle.
PRS- 333690	Wireless suppression erroneously activates when the OpenVPN adapter is present.
PRS - 331517	Pulse client download and upgrade performance has been improved. Note: In order to avail this fix, customers need to do one of the following:

	a. Upgrade PCS/PPS to 8.1r7/C5.1r7 or greater. b. MSI/DMG upgrade of pulse5.1r7 client.

Problems Resolved in Pulse5.1R6

The following table lists important fixes and enhancements that were introduced in Pulse 5.1r6.

Problem Report Number	Description
PRS-332314	VMware virtual adapters are incorrectly identified as connected wired LAN NICs for wireless suppression.
PRS-331187	Client applications in 8.1R1 and earlier fail to launch when Pulse Setup Client 8.1R2+ is installed. Note that a PPS upgrade to 8.1r6 is needed for this fix.
PRS-331147	If Pulse has a manual and preconfiguration connection defined for the same appliance (PCS or PPS), a duplicate connection attempt is observed.
PRS-329331	Pulse prompts for credentials even when they are saved when PPS/PCS device is configured for machine to user authentication.
PRS-328642	Certificate authentication fails on Mac OSX 10.11.
PRS-328635	If Pulse is installed from a server (PCS or PPS) with the location set with "https://" prefix, browser-based launch of Pulse fails.
PRS-328615	SAML-based authentication fails against a PCS or PPS appliance if the connection URL is defined with "https://" prefix.
PRS-328555	If a user-created connection is defined in Pulse for a SAML-based URL, a second connection is created by the PCS/PPS gateway when the user connects.
PRS-331706	In wireless 802.1x, dsAccesservice crashes on the Window client when multiple SSIDs are configured pointing to a preferred realm.
PRS-330032	On Windows 7 that haven't been updated with Microsoft updates, clients do not launch. Note that a PPS upgrade to 8.1r6 is needed for this fix.
PRS-330934	Pulse secure service is triggering an override of a 3rdparty wireless suppression software.
PRS-326650	Pulse disregards SSID priority order configured in Scan list of connection set .

PRS-328555	When adding a manual connection in Pulse UI, a second connection is created when using SAML authentication server.
PRS-329334	When both primary and secondary authentication are used, Pulse user is unable to change secondary password when it expires. Note that a PPS/PCS upgrade to 8.1r6 or C5.1r6 is needed for this fix. An upgrade of the Pulse client is not required.
PRS-312175	Pulse fails to upgrade if the initial connection is through machine authentication.
PRS-330432	Some Pulse users might having trouble setting up a connection when the Pulse Connect Secure device is under load. Note that a PPS/PCS upgrade to 8.1r6 or C5.1r6 is needed for this fix. An upgrade of the Pulse client is not required.
PRS-326846	Pulse tunnels are unable to connect if Bandwidth management is enabled. Note that the PPS upgrade to 8.1r6 for this fix.
PRS-326712	Pulse Desktop does support 802.1x in hyper-v environments.

Known Issues in Pulse5.1R6

The following table lists known issues in Pulse 5.1r6.

Problem Report Number	Description
PRS-333039	Intermittently, uninstall of the Pulse client on Windows 10 prompts for a reboot.

Problems Resolved in Pulse5.1R5

The following table lists important fixes and enhancements that were introduced in Pulse 5.1r5.

Problem Report Number	Description
PRS-323072	Under certain circumstances, Pulse Secure Client attempts to create more than one connection to the same PCS device.

Problems Resolved in Pulse5.1R4

The following table lists important fixes and enhancements that were introduced in Pulse 5.1r4.

Problem Report Number	Description
PRS-326898	Location awareness evaluation may delay Pulse connection to PCS/PPS.
PRS-320795	Discrepancy in Pulse Secure captive portal detection feature UI and tray status
PRS-315232	If the EAP MTU is set to 1500 the RADIUS packets are fragmented. The EAP size has been adjusted to 1200 starting in this release.
PRS-327308	Pulse Secure Client generates a http-based proxy PAC file for IE 9 and 10.
PRS-323197	Repair and Uninstall options are missing in the Start Menu in Windows 8 and later.
PRS-321624	The “Connect” button is hard to read on Mac OS 10.10 (Yosemite)
PRS-310334	Pulse doesn’t restore proxy settings in normal windows shutdown

Problems Resolved in Pulse5.1R3.2

The following table lists important fixes and enhancements that were introduced in Pulse 5.1r3.2.

Problem Report Number	Description
PRS-326751	On a Windows platform, when upgrading Pulse desktop from an older release to Pulse5.1r3 or Pulse5.1r3.1, the openssl libraries will not get upgraded.
PRS-326751	Pulse L2 connection might go in a loop showing service not running and connection failure after upgrade to Pulse 5.1R3.

Problems Resolved in Pulse5.1R3

The following table lists important fixes and enhancements that were introduced in Pulse 5.1r3.

Problem Report Number	Description
PRS-322975	SAML authentication fails.

PRS-322384	Pulse Launcher does not support New Pin Mode
PRS-323699	In the event of user session deletion or time out, the Pulse Secure client reconnects to the last used IP rather than issuing a new DNS lookup
PRS-323615	Captive Portal detection prevents successful connections if there is no rejection of the HTTP probe
PRS-323598	If a VPN session is active and a user attempts to login to a second system, the client continually authenticates to the second node
PRS-325285	L2/802.1x connection does not timeout even if the L3 TCP connection to the Pulse Policy Secure (PPS/IC) is lost

Problems Resolved in Pulse5.1R2

The following table lists important fixes and enhancements that were introduced in Pulse 5.1r2.

Problem Report Number	Description
PRS-315530	A tunnel cannot be established when running Pulse over a 3G connection in Windows 8.1.
PRS-322849	Pulse is sending a reconnect message every 5 seconds in L2 connection when the user disjoins the domain.
PRS-322752	Garbled characters are displayed when uninstalling Pulse Secure on a Japanese OS client
PRS-322041	Pulse may crash when choosing the option to “Forget Saved Settings” when uninstalling Pulse on a Mac OS X client
PRS-321594	Excessive CPU utilization may be observed when viewing the “About” box with the default Windows 7 theme
PRS-319801	Invalid character/resource string displayed next to the connection when using Chinese language settings

PRS-319255	Pulse 802.1x connections fail when password expiration messages are displayed.
PRS-318525	When using machine authentication AND single user session, changing network type may trigger disconnects.
PRS-315530	Connecting on a cellular data connection may prevent access to protected resources on Windows 8.1.
PRS-309684	Pulse goes into reconnect mode when signing out using the browser with SSL Acceleration enabled
PRS-257980	Pulse Credential Provider tile “Other User” should display the Pulse icon on Windows 7.
PRS-324077	Upgrading through the browser from Pulse 5.0 to 5.1 does not trigger an automatic user reconnection

Known Issues in this release

The following table lists open issues in this release. the open issues in this release.

Problem Report Number	Description
PRS-324077	Upgrading through the browser from Pulse 5.0 to 5.1 does not trigger an automatic user reconnection

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

If you need additional information or assistance, you can contact the Pulse Secure Global Support Center (PSGSC) in the following ways:

- **http://www.pulsesecure.net/support**
- **support@pulsesecure.net**
- Call us at 844-751-7629 (outside the U.S., see phone numbers here)

Revision History

This table lists the revision history for this document.

Version	Revision	Description
1.4	July 2016	PDC 5.1R9.1 release notes
1.3	6th May 2016	PDC 5.1R9 release notes
1.2	3rd March 2016	PDC 5.1R8 release notes
1.1	17th Dec 2015	PDC 5.1r7 release notes
1.0	16th Dec 2015	Initial publication.