Pulse Secure Universal App for Windows Release Notes

Version 5.2.8

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

Product Release	**5.2.8**
Published	**July 2016**
Revision	**1.5**

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 document is the release notes for version 5.2 of the Pulse Secure Universal App for Windows. This document provides a cumulative list of all enhancements, fixes and known issues with all releases of this client.

The Pulse Secure Universal App for Windows is downloadable from the Microsoft Store. The Universal App provides secure connectivity between a Windows 10 device (for example, a PC, tablet, smartphone, Xbox, or Windows 10 IoT device) and a Pulse Connect Secure (PCS) gateway. For a complete description of the capabilities of this lightweight client, please see the Pulse Secure Universal App for Windows Quick Start Guide, which can be found here. For assistance with Pulse Secure software and solutions, consult Pulse Secure's support page.

Interoperability and Supported Platforms

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

Important Changes and Deprecated Features

- Microsoft released a fix for a VPN-upload performance issue in a November, 2015 Windows 10 update (sometimes referred to as the Windows 10 "Threshold 2" update). Updating your operating system to this version of Windows resolves the performance issue – no upgrade of the Pulse Secure Universal App itself is necessary. This issue was tracked by Pulse Secure as PRS-329662.
- No features were deprecated in this release.

New Features in 5.2.8

The Pulse Secure Universal App for Windows 10 now supports the "Statement of Health" (SoH) setting in Windows 10 "Redstone" and beyond. The SoH setting can be used to enforce certain connectivity restrictions based on the posture and health of an endpoint. For example, system administrators can configure restrictions based on whether antivirus, antispyware and/or a software firewall is enabled. Note: Currently, the Windows OS itself does **not** support checks for whether antivirus/antispyware is up-to-date and whether OS auto-update is enabled.

See the screen shot of the administrative console, below, for details:

[PSD-1674]

Problems Resolved in 5.2.8

The following table describes issues that have been fixed in 5.2.8.

Problem Report Number	Description
PSD-1830	Split Tunneling Disabled (also called “force tunnel” – this is the state that is set when the “Split Tunneling” configuration option is set to “Disable” in the administrative console) was not working properly on Windows 10 mobile devices.

New Features in 5.2.7

The Pulse Secure Universal App for Windows version 5.2.7 introduces support for Source IP Enforcement via a Pulse Policy Secure gateway! Source IP Enforcement allows a Pulse Policy Secure gateway to communicate with an “Infranet Enforcer” (i.e., a firewall) to permit the Windows device to communicate through the firewall. To use this feature, the Universal App simply must connect to a PPS gateway, authenticate and (optionally) pass the Host OS Check. Once authenticated and once the Host Checker policy is passed, the PPS gateway communicates with the Infranet Enforcer to open the appropriate firewall port for the endpoint Windows device. Periodic Host Checker enforcement can be configured to ensure that the port can later be closed if the endpoint device changes in a manner that should cause a cessation of firewall transit. For

more information on configuring a PPS gateway to enable Source IP Enforcement, see the "Understanding Infranet Enforcer Source IP Security Policies" section of the Pulse Policy Secure Complete Software Guide.

Problems Resolved in 5.2.7

The following table describes issues that have been fixed in 5.2.7.

Problem Report Number	Description
PRS-338767	Improved robustness by ensuring connections are resumed in the event of certain connection failures, plus cosmetic user-interface improvements.

Problems Resolved in 5.2.6

The following table describes issues that have been fixed in 5.2.6.

Problem Report Number	Description
PRS-336477	When an RSA ACE server was used as a RADIUS server with a Pulse Connect Secure gateway, the token-card challenge-response dialog (the credentials popup window) would display the passcode characters in the input window. The input window now replaces each character with a dot to obscure the passcode and be consistent with other credential dialogs.
PRS-336471	When an RSA ACE server was used as a RADIUS server with a Pulse Connect Secure gateway, the "passcode" field was being displayed with the label "Password", which was confusing. The label has been changed to "Passcode".
PRS-337209	The Universal App would fail with the error "Missing or invalid certificate" when "Allow all users and remember certificate information while user is signed in" is selected on the User Realm.
PSD-1197	The Universal App now will display customized username and password prompts if the "Pulse Client displays customized username and password prompts" checkbox is checked appropriately on the administrative console.

Problems Resolved in 5.2.5

The following table describes issues that have been fixed in 5.2.5.

Problem Report Number	Description

PRS-334094	When using certificate authentication in which the private key is stored in a TPM (Trusted Platform Module), Pulse was incorrectly prompting the user to “Connect a smart card”.
PSD-1021	The Pulse Universal App was incorrectly displaying HTML tags under certain circumstances – for example, when telling that a user that a connection has been denied as the result of failing to meet realm/role/policy restrictions.
PRS-326578	The Pulse Universal App was not properly processing PAC (Proxy auto-config) files.

Problems Resolved in 5.2.4

The following table describes issues that have been fixed in 5.2.4.

Problem Report Number	Description
PRS-324713	Symptom: The Pulse plugin (Windows 8.1 "Inbox" VPN Plugin, Windows 8.1 Phone app, Windows 10 Universal App) would fail to properly place traffic in the tunnel if a policy was configured on the PCS gateway such that all traffic should go in the tunnel except for a few exclusions. Cause: Originally, this Pulse security policy was mapped on the client to split tunnel with deny policy and a default route in which everything goes into the tunnel. The Windows OS gave the default route the wrong priority/weight and was therefore ignored, causing data to not go through the tunnel. Resolution: A change was made in the 5.2.4 Universal App to map this PCS gateway configuration to "force tunnel" mode with exclusions. This fixes the issue with the default route and allows the configuration to work properly. Note that this issue has not been fixed in the Windows 8.1 Pulse plugins.

Problems Resolved in 5.2.1

n/a (Version 5.2.1 was the initial release of the Pulse Secure Universal App for Windows.)

Known Issues in this Release

The following table describes open issues in this release.

Problem Report Number	Description

PRS-326578	**Problem**: The Universal App manually configured proxy server port is limited to port 80. Regardless of what port number is specified in the PCS gateway manual proxy setting in the admin console, the number will be treated as 80. This is a constraint of the Windows 10 operating system. **Workaround**: There are two possible workarounds: 1) Use a Proxy PAC file rather than a manual proxy configuration 2) Use the Microsoft VPN Proxy setting on the Microsoft VPN Connection Profile (created manually on the Windows device itself or through an MDM system).
PRS-327771	If the Pulse Connect Secure gateway sends a change-password request to the Universal App, in some circumstances there will be no prompt to change password, and instead an error message stating 'An internal error occurred' will appear. The following Microsoft SysDev ticket was created to track this Windows 10 issue: *#3608687 PulseSecure VPNP 10240: Window10 changepassword 'An internal error occurred' - Enterprise VPN* To work around this issue, the end user can click the "Clear sign-in info" button on the "VPN connection Advanced Options" page, and then reconnect to the Pulse Connect Secure gateway. The user should then be prompted to change his/her password.
PRS-310697	The Universal App will not automatically reconnect to the PCS gateway after the reboot of the PCS gateway to which Pulse was connected. After a PCS gateway reboot, the user must manually restart the VPN connection from the client.
PRS-327627	The client's session information on the PCS gateway will not be immediately removed from the PCS gateway if a Universal App user logs out or shuts down the Windows 10 device while a VPN connection is active. The session information will remain on the PCS gateway until either the idle timeout or the max-session lifetime is reached, or until the user re-establishes a connection. The workaround is to manually disconnect the VPN before logging off or shutting down the client machine. Note: See also issue PRS-330292.
PRS-330292	If a user logs off or shuts down the client with a Universal App VPN connection active, and then the user logs back on, the user's session may be resumed (assuming a timeout has not expired), leveraging the credentials used from the previous session. (With other Pulse clients like the Pulse Desktop client for Windows, VPN sessions are automatically resumed with the previous session's credentials only after events like sleep/wakeup, transient network events, etc.) The following Microsoft SysDev ticket was created to track this Windows 10 issue:

	3765760 VPNP 10240: Window10 Logoff/Logon resumes connection (should get connect,disconnect,connect behavior) Note: See also issue PRS-327627.
PRS-329623	The error message "The network connection couldn't be found" may be displayed erroneously when a user enters invalid credentials. The Event log shows a correct error message of "auth rejected by server". The following Microsoft SysDev ticket was created to track this Windows 10 issue: *3720739 PulseSecure VPNP 10240: Window10 Failed authentication sometimes shows wrong message 'The network connection could not be found".*
PRS-330030	If a user launches the Universal App and only splash screen comes up, it means that the Universal App is already running in the background. Note: Once the Universal App is installed, there is no need to launch the app manually. The Universal App gets launched "on demand" – in other words, whenever a request is made to establish a VPN connection.

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 USA, see numbers here)

Revision History

Revision	Date	Description
1.5	July 2016	Release Notes for 5.2.8
1.4	April 2016	Release Notes for 5.2.7

1.3	February 2016	Release Notes for 5.2.6
1.2	December 2015	Release Notes for 5.2.5
1.1	October 2015	Release Notes for 5.2.4
1.0	July 2015	Release Notes for 5.2.1

