



Pulse Secure Desktop Client Supported Platforms Guide

Pulse Secure Desktop Client v5.2r5

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

Product Release	5.2r5
Published	June 2017
Document Version	1.3

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

© 2017 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

Introduction	4
Documentation	4
Hardware Requirements	4
Server Platform Compatibility.....	5
Platform and Browser Compatibility	5
Smart Card and Soft Token Compatibility.....	6
Language Support	7
Adaptive Delivery	7
Access Methods	9
Client Interoperability	11


Introduction

Pulse Secure is a dynamic, integrated and easy-to-use network client that delivers anytime/anywhere secure connectivity. The *Pulse Secure Desktop Client Supported Platforms Guide* describes which operating environments are supported by Pulse Secure desktop clients for Windows and macOS.

The Pulse Secure client testing environment provides the following types of software qualifications:

Qualified Platform: The platforms listed as *qualified* have been systematically tested by the Pulse Secure Quality Assurance department as part of this release.

Compatible Platform: The platforms listed as *compatible* have not been systematically tested by our QA department in this release; however, Pulse Secure expects that the Pulse functionality will work based on testing of previous releases and knowledge of the platform.

 **Note:** The Pulse Secure client for Windows and the Pulse Secure client for macOS are different clients with different feature sets. For more information, see the Pulse Secure documentation.

Documentation

All Pulse Secure documentation is available at <https://www.pulsesecure.net/techpubs>.

Hardware Requirements

Table 1 lists the minimum hardware configuration required to support the Pulse Secure desktop clients.

Table 1: Pulse Secure Desktop Client Hardware Requirements

Hardware Component	Requirement
CPU	Intel / AMD, 1.8GHz, 32-bit (x86) or 64-bit (x64) processor
System Memory	2 GB RAM
Disk Space	Install: 33 MB Logging: 50 MB

Server Platform Compatibility

Table 2 lists the server platforms that were tested with this release of the Pulse Secure desktop clients for Windows and macOS.

Table 2: Pulse Secure Client/Server Compatibility

Product	Qualified	Compatible
Pulse Connect Secure (formerly Secure Access Service, or SA)	8.2Rx, 8.1Rx	8.0Rx, 7.4R4
Pulse Policy Secure (formerly Access Control Service, or Unified Access Control/UAC)	5.3Rx, 5.2Rx, 5.1Rx	5.0Rx, 4.4R4



Note: Previous versions of the Pulse Secure client can be used with the latest release of Pulse Secure server software, but new features that were added after the release of that client will not be available.

Platform and Browser Compatibility

Table 3 lists *qualified* platforms and **Table 4** lists *compatible* platforms for version 5.2 of the Pulse Secure desktop clients for Windows and macOS.

Unless otherwise noted, a major and minor version number (for example, 10.9), means that all revisions (10.9.x) with that major/minor version are supported. When major, minor, and revision version number are specified (for example, 10.7.3), only that revision and later revisions of that major/minor version are supported. For example, 10.7.3 means that 10.7.3 through 10.7.x are supported, where x is the latest revision available.

Table 3: Pulse Secure Desktop Client Qualified Platforms

Platform	Operating System	Web Browser
Windows	Windows 10 Enterprise, 64 bit	Internet Explorer 9, 10, 11
	Windows 8.1 Enterprise, 64 bit	Edge Browser ¹
	Windows 8 Enterprise, 64 bit	Firefox ESR
	Windows 7 SP1 Enterprise, 64 bit	
macOS	macOS 10.12, 10.11 and 10.10, 64 bit	Safari 10.x, 9.x and 8.x

¹Windows 10 only

Table 4: Pulse Secure Desktop Client Compatible Platforms

Platform	Operating System	Web Browser
Windows	Windows 10 Enterprise, 32 bit	Internet Explorer 8
	Windows 10 (non-Enterprise), 32 and 64 bit	Firefox 3.0 and later
	Windows 8.1 Enterprise, 32 bit	Google Chrome ¹
	Windows 8.1 (non-Enterprise), 32 and 64 bit	
	Windows 8, 32 and 64 bit	
	Windows 8 Enterprise, 32 and 64 bit	
	Windows 8 Pro, 32 and 64 bit	
	Windows 7 Ultimate, 32 and 64 bit	
	Windows 7 Professional, 32 and 64 bit	
	Windows 7 Home Basic, 32 and 64 bit	
	Windows 7 Home Premium, 32 and 64 bit	
Windows Embedded Standard 7, 32 and 64 bit		
macOS	macOS 10.9, 64 bit	Safari 7.x

¹Google Chrome is *compatible* rather than *qualified* because of Google's policy to support a "rapid release cycle" rather than an Extended Support Release (ESR) model.

Smart Card and Soft Token Compatibility

Table 5 lists the compatible smart cards and **Table 6** lists compatible soft tokens. The listed items are compatible on the following platforms (all 64-bit):

- Windows 10 Enterprise
- Windows 8.1 Enterprise
- Windows 8 Enterprise
- Windows 7 Enterprise
- macOS 10.12
- macOS 10.11
- macOS 10.10
- macOS 10.9

Table 5: Compatible Smart Cards

Cards	Software Version
Aladdin eToken	PKI client version 5.1 and drivers version of 5.1
Safenet iKey 2032	PKI client version 7.0.8.0022, driver version v4.0.0.20

Cards	Software Version
Gemalto .Net cards	Driver version 2.1.3.210

Table 6: Compatible Soft Tokens

Soft Tokens	Software Version
RSA	Application version 4.1.0.458
Server	RSA Authentication Manager 8.1
Client	RSA SecurID Software Token

Language Support

User-interface, message and online-help text in the Pulse Secure desktop clients for Windows and Mac OS X have been localized in the following languages:

- DE – German
- EN – English
- ES – Spanish
- FR – French
- IT – Italian
- JA – Japanese
- KO – Korean
- PL – Polish
- ZH-CN – Chinese (Simplified)
- ZH – Chinese (Traditional)

In order for the Pulse Secure desktop client to use a language listed above, the corresponding locale must be set on the local operating system.

Adaptive Delivery

Pulse Secure clients (both Windows/macOS desktop clients, and also Network Connect, Host Checker, WSAM, Windows Terminal Services, and Secure Meeting clients) feature “Adaptive Delivery”, which is a mechanism for installing and launching Pulse Secure clients from a web browser. The exact mechanism used for Adaptive Delivery depends on a number of factors, including:

- 1) The Pulse Secure client being launched/installed
- 2) The client operating system type and version
- 3) The web browser type and version
- 4) The security settings of the client operating system and browser

In order to leverage Adaptive Delivery for a particular client/OS/browser combination, you may need to enable the appropriate technology on the endpoint device. For example, to launch the Pulse Secure desktop client from Internet Explorer on Windows, you will need to ensure that either ActiveX or Java is enabled in Internet Explorer on the end user's endpoint device.


 **Note:** Pulse Connect Secure 8.2r1 and Pulse Policy Secure 5.3r1 introduced a new Adaptive Delivery mechanism called “Pulse Application Launcher” (PAL). PAL leverages “URL handler” functionality by invoking a custom URL in a manner that instructs the web browser to execute a program that launches/install the appropriate Pulse Secure client. PAL was created to address both the restrictions placed on Java on Mac OS X and the deprecation of Java (and ActiveX) plugins in Google Chrome version 45 and the Microsoft Edge browser. You can read more about the PAL in Pulse Secure's KB (Knowledge Base) article [KB40102](#).

Table 7 shows the Adaptive Delivery mechanism for client/OS/browser combinations.

Table 7: Adaptive Delivery Mechanisms

Operating System	Pulse Secure client	Web Browser	Pulse Secure Client Adaptive Delivery Mechanism
Windows	All Pulse Secure clients	Internet Explorer	ActiveX / Java ¹
Windows	All Pulse Secure clients	Firefox ² Google Chrome ³ Edge Browser ^{4,5}	Pulse Application Launcher (PAL)
macOS	Pulse Secure desktop client Host Checker (HC)	Safari ⁶	Pulse Application Launcher (PAL)
macOS	Network Connect (NC) JSAM	Safari	Java

¹With Adaptive Delivery on Internet Explorer, ActiveX is tried first, but Java is tried second if ActiveX is disabled.

²PAL support for Firefox was added in PCS 8.2r5 / PPS 5.3r5. Previous versions of the gateways attempted to invoke Java for Firefox.

³Note that Chrome is *compatible* rather than fully *qualified* on Windows

⁴Windows 10 only.

⁵Edge browser support for launching *Pulse Secure desktop clients* was introduced in PCS 8.2r1 & PPS 5.3r1. Edge browser support for *other Pulse Secure gateway functions* (admin console, other clients, etc.) was added in PCS 8.2r3 and PPS 5.3r3. For details about Pulse Secure gateway support for the Edge browser, please see the relevant Pulse Secure gateway documentation.

⁶Note that Chrome and Firefox on macOS are not supported (only Safari is supported on macOS), but PAL will be invoked if an attempt is made to use either Chrome or Firefox on macOS for the Pulse Secure desktop client or Host Checker.

Access Methods

The Pulse Secure desktop client supports the following kinds of connections to Pulse Secure gateways:

- Layer 3 VPN connections to Pulse Connect Secure
- Layer 2 (802.1x) and Layer 3 connections to Pulse Policy Secure
- Per-application VPN tunneling to Pulse Connect Secure (Windows Secure Access Manager (WSAM))

There are a vast number of possible combinations of connections and configurations. For example, both Layer 2 (wired and wireless) and Layer 3 connections can be configured either with or without enforcement (Host Checker enforcement of system health and policy compliance). Although an endpoint can have only one active VPN connection to Pulse Connect Secure, an endpoint can have multiple simultaneous Pulse Policy Secure connections with or without a VPN connection. Also, Pulse Policy Secure IPsec enforcement in Pulse Connect Secure (TLS) tunnels is supported.

Table 8 lists the configurations that are qualified and compatible. Any combination not mentioned in **Table 8** is not supported.

Table 8: Access Method Configurations

Access Method Configuration	Description	Level of Support
Layer 3 IPsec tunnel inside VPN outer tunnel	<p><i>Outer tunnel:</i> TLS or ESP VPN tunnel to Pulse Connect Secure gateway</p> <p><i>Inner tunnel:</i> Layer 3 IPsec tunnel authenticated through Pulse Policy Secure to ScreenOS or SRX firewall</p>	Qualified
Layer 2 Pulse Policy Secure + Multiple Layer 3 Pulse Policy Secure	One Pulse Policy Secure Layer 2 connection running in parallel to multiple Pulse Policy Secure Layer 3 connections	Qualified

Table 9 lists the supported nested tunnel (tunnel-in-tunnel) configurations. The configurations are for a Pulse Connect Secure v8.2 outer tunnel, a Pulse Policy Secure v5.3 inner tunnel, and the Pulse Secure desktop client v5.2.

Table 9: Tunnel in Tunnel Support

Pulse Connect Secure (Outer Tunnel Config)				Pulse Policy Secure (Inner Tunnel Support)				
Split-Tunneling Mode	Route Precedence	Route Monitor	Traffic Enforcement	IPsec (with VA)	IPsec (without VA)	Dynamic IPsec	Source IP	Dynamic Source IP
Disabled	Tunnel Routes ¹	Disabled	Disabled	Supported	Supported	Supported	Supported	Supported
Disabled	Tunnel Routes ¹	Disabled	IPv4 Disabled and IPv6 Enabled	Supported	Supported	Supported	Supported	Supported
Disabled	Tunnel Routes ¹	Disabled	IPv4 Enabled and IPv6 Disabled	Not Supported	Supported	Supported	Supported	Supported
Disabled	Tunnel Routes	Enabled	Enabled or Disabled	Not Supported	Supported	Supported	Supported	Supported
Enabled	Tunnel Routes ¹	Disabled	Enabled or Disabled	Supported ²	Supported ³	Supported	Supported	Supported
Enabled	Tunnel Routes ¹	Enabled	Enabled or Disabled	Supported ²	Supported ³	Supported	Supported	Supported
Enabled or Disabled	Endpoint routes	Enabled or Disabled	Enabled or Disabled	Supported ²	Supported ³	Supported	Supported	Supported

¹Tunnel Routes and Tunnel Routes with Local Subnet Access behave the same way.

²Pulse Policy Secure IP address, IE IP address, and Pulse Policy Secure VA pool IP addresses should be added in the Pulse split-tunneling network policy.

³Pulse Policy Secure IP address, IE IP address, and protected resources should be added in a Pulse split-tunneling network policy, and Pulse Connect Secure should have a route to the Pulse Policy Secure protected resource.



NOTE: Pulse WSAM does not interoperate with Pulse Policy Secure.

Client Interoperability

Pulse Secure offers many different clients, and there are third parties that offer clients that attempt to manipulate traffic in a manner similar to that of the Pulse Secure clients. The tables below describe the consequences of having multiple clients on the same machine.

Table 10 describes Pulse Secure client interoperability. **Table 11** describes third-party client interoperability.

Runtime Coexistence means that both products can be installed and running at the same time. **Install Coexistence** means that both products can be installed on the same machine at the same time; however, only one product can be active (running) at a time.

Table 10: Pulse Secure Client Interoperability

Product	Version	Coexistence	Nested Tunnel Operation
Network Connect	8.1, 8.2	Runtime	Limited support (see Table 9)
Network Connect	6.3, 6.4, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 8.0	Install	Not supported
Odyssey Access Client (OAC)	5.6	Runtime	OAC 802.1x in Layer 2 with Pulse 5.2 in Layer 3 is supported. No other combinations are supported.
Odyssey Access Client (OAC)	5.5 and earlier	Not supported	Not supported
WSAM/JSAM	Any	Install	Not supported
Secure Meeting Client	Any	Runtime	Supported

Table 11: Third-Party Client Interoperability

Product	Version	Coexistence	Nested Tunnel Operation
Juniper (Netscreen) NSRemote Client	Any	Install	Not supported
Juniper Access Manager (Dynamic VPN Client)	Any	Not supported	Not supported

		(installation will terminate)	
Nortel Contivity Server 1010 with Pulse Secure Client	Server Version: V04_80.124 Client Version: V06_01.109 (Win XP SP3)	Install	Not supported
Cisco ASA 5505 with Pulse Secure Client	Server Version: 8.0(3) Client Version: 5.0.07.0290 (Win 7 64 bit)	Install	Not supported
Cisco VPN 3000 Concentrator with Pulse Secure Client	Server Version: 4.1.7 D Client Version: 5.0.07.0290 (Win 7 64-Bit)	Runtime	Supported
