Pulse Secure®

Pulse Secure Desktop Client

Supported Platforms Guide

PDC 9.1R4 Build 1761.1
PDC 9.1R4 Linux Build 143.1

Pulse Secure, LLC
2700 Zanker Road, Suite 200
San Jose, CA 95134
https://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 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	Document Version	Date	Description
9.1R4	1.6	January 2020	Removed Cent OS 6.x, 64 bit and 32 bit from Table 4: Pulse Secure Desktop Client Compatible Platforms. Added macOS 10.15.2, 64 bit in Table 4: Pulse Secure Desktop Client Compatible Platforms. Updated Table 3: Pulse Secure Desktop Client Qualified Platforms for Windows and macOS support. Updated Smart Card and Soft Token Compatibility for Yubikey support. Updated Table 7: Adaptive Delivery Mechanisms.
9.1R3.1	1.5	November 2019	Updated Windows operating system support in Table 3: Pulse Secure Desktop Client Qualified Platforms. Updated Windows, macOS operating system and web browsers support in Table 4: Pulse Secure Desktop Client Compatible Platforms.
9.1R3	1.4	October 2019	Added Windows 10 and web browsers support in Table 3: Pulse Secure Desktop Client Qualified Platforms. Removed NC, OAC, and WSAM from Client Interoperability.
9.1R2	1.3	September 2019	Added Safari 13.x and 12.x in Table 3: Pulse Secure Desktop Client Qualified Platforms.
9.1R2	1.2	July 2019	Added 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 in Table 4: Pulse Secure Desktop Client Compatible Platforms.
9.1R1	1.1	June 2019	Added Windows 10 Version 1903 (OS build 10.0.18362.175) Enterprise, 64 bit and Windows 10 Version 1903 (OS build 10.0.18362.175) Professional, 64 bit in Table 4: Pulse Secure Desktop Client Compatible Platforms.
9.1R1	1.0	May 2019	Added Windows 10 Redstone 5 Version 1809 (OS build 17763.437), Enterprise, 64 bit in Table 3: Pulse Secure Desktop Client Qualified Platforms. Added macOS 10.14.4 (64 bit), macOS 10.14.3 (64 bit), macOS 13 (64 bit), macOS 12 (32 bit and 64 bit) in Table 3: Pulse Secure Desktop Client Qualified Platforms. Added macOS 10.11 (32 bit and 64 bit) in Table 4: Pulse Secure Desktop Client Compatible Platforms.

Contents

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, macOS and Linux.

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.

The Pulse Secure client on Windows, macOS and Linux 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, macOS and Linux.

Table 2: Pulse Secure Client/Server Compatibility

Product	Qualified	Compatible
Pulse Connect Secure (formerly Secure Access Service, or SA)	9.1Rx, 9.0Rx	8.3Rx, 8.2Rx
Pulse Policy Secure (formerly Access Control Service, or Unified Access Control/UAC)	9.1Rx, 9.0Rx	5.4Rx, 5.3Rx

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 9.1R4 of the Pulse Secure Desktop Clients for Windows, macOS and Linux.

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 Version 1909 10.0.18363.535 Windows 10 Version 1903 10.0.18362.449 Windows 10 Redstone 5 Version 1809 (OS build 17763.437), Enterprise, 64 bit Windows 10 Redstone 4 Version 1803 (OS build 17134.228) Windows 8.1 Enterprise, 64 bit Windows 7 SP1 Enterprise, 64 bit Windows 2012	Edge Browser 44.18362.449.0 Internet Explorer 11.535.18362.0 Firefox ESR 68.9.0esr Chrome 79.0.3945.88 Chromium-based Edge Browser 79/0.309.58
macOS	macOS 10.15.1, 64 bit macOS 10.14, 64 bit macOS 10.13, 64 bit macOS 10.12, 32 bit and 64 bit	Safari 13.x, 12.x, 11.x,10.x, 9.x and 8.x
Linux	Ubuntu 18.04, 64 bit Ubuntu 17.10, 64 bit Ubuntu 16.04.04, 64 bit and 32 bit Debian 9.4, 64 bit and 32 bit Cent OS 7.4, 64 bit RHEL 7.4, 64 bit Fedora 27, 64 bit and 32 bit ⓘ **Note**: The Linux Pulse Desktop Client is qualified in the above supported operating systems with the kernel that is installed by default during fresh installation.	N/A

Table 4: Pulse Secure Desktop Client Compatible Platforms

Platform	Operating System	Web Browser
Windows	Windows 10 Version 1903 (OS build 10.0.18362.476) Professional, 64 bit Windows 10 Enterprise, 32 bit Windows 10 non-Enterprise, 32 and 64 bit Windows 10 Redstone Windows 10 Enterprise, 32 and 64 bit Windows 8.1 non-Enterprise, 32 and 64 bit Windows 8, 32 and 64 bit Windows 8 Enterprise, 32 and 64 bit Windows 8 Professional, 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 Windows 2008, Windows 2016	Edge browser 44.18362.449.0 Internet Explorer 11.418.18362.0 Google Chrome 78.0.3904.97
macOS	macOS 10.15.2, 64 bit macOS 10.11, 32 bit and 64 bit	N/A

Platform	Operating System	Web Browser
Linux	Ubuntu 17.x, 64 bit Ubuntu 16.x, 64 bit and 32 bit Debian 9.x, 64 bit and 32 bit Debian 8.x, 64 bit and 32 bit Cent OS 7.x, 64 bit RHEL 7.x, 64 bit Fedora 26, 64 bit and 32 bit	N/A

Note: Google 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.

The listed items are compatible on the following platforms (all 64-bit):

- Windows 10 version 1909
- Windows 10 version 1903
- Windows 10 Enterprise
- Windows 8.1 Enterprise
- Windows 8 Enterprise
- Windows 7 Enterprise
- macOS 10.15.1, 64 bit
- macOS 10.15, 64 bit
- macOS 10.14
- macOS 10.13
- macOS 10.12
- macOS 10.11
- Windows 10 Redstone
- Windows 10 Redstone2
- Windows 10 Redstone3
- Windows 10 Redstone4
- Windows 10 Redstone5

Table 5: Compatible Smart Cards

Cards	Software Version
Yubikey	Driver Version 10.0.18362.1 **Note**: Yubikey supports both Windows and macOS with below authentication modes under certificates: • Authentication • Digital Signature • Card Authentication

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
Gemalto .Net cards	Driver version 2.1.3.210

Table 6 lists compatible soft tokens.

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 macOS 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)

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, Host Checker, 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 many 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

To leverage Adaptive Delivery for a 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 Secure Application Launcher" (PSAL). PSAL leverages "URL handler" functionality by invoking a custom URL in a manner that instructs the web browser to execute a program that launches/installs the appropriate Pulse Secure client. PSAL was created to address both the restrictions placed on Java on macOS and the depreciation of Java (and ActiveX) plugins in Google Chrome version 45 and the Microsoft Edge browser. You can read more about the PSAL 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 / Java1
Windows	All Pulse Secure clients	Firefox Google Chrome Edge Browser	Pulse Secure Application Launcher (PSAL)
macOS	Pulse Secure Desktop Client Host Checker (HC)	Safari	Pulse Secure Application Launcher (PSAL)
macOS	JSAM	Safari	Pulse Secure Application Launcher (PSAL)

Note:

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

2. PSAL support for Firefox was added in PCS 8.2r5 / PPS 5 .3r5. Previous versions of the gateways attempted to invoke Java for Firefox.

3. Chrome is compatible rather than fully qualified on Windows.

4. Edge 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.

5. Chrome and Firefox on macOS are not supported (only Safari is supported on macOS), but PSAL 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)

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	Outer tunnel: TLS or ESP VPN tunnel to Pulse Connect Secure gateway Inner tunnel: Layer 3 IPsec tunnel authenticated through Pulse Policy Secure to ScreenOS or SRX firewall	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 v9.0 outer tunnel, a Pulse Policy Secure v9.0 inner tunnel, and the Pulse Secure Desktop Client v9.0.

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

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

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

③Pulse Policy Secure IP address, IE IP address, and protected resources should be added to 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 different clients and there are third parties that offer clients that attempt to manipulate traffic in a manner like 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.

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
Secure Meeting Client	Any	Runtime	Supported