# Pulse Secure Desktop Client

## Supported Platforms Guide

PDC 9.0R1
Build - 571

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


| | |
|---|---|
| Product Release | 9.0R1 |
| Published | May, 2018 |
| Document Version | 1.2 |

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

# 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<br>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<br>(formerly Secure Access Service, or SA) | 9.0R1, 8.3Rx | 8.2Rx, 8.1Rx, 8.0Rx and 7.4R4 |
| Pulse Policy Secure<br>(formerly Access Control Service, or Unified Access Control/UAC) | 9.0R1, 5.4Rx | 5.3Rx, 5.2Rx, 5.1Rx and 5.0Rx |

**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 9.0R1 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 Redstone 3 Version 1709 (OS build 16299.371)<br>Windows 10 Redstone 2 version 1703 build 10.0.15063.332, 64 bit<br>Windows 8.1 Enterprise, 64 bit<br>Windows 7 SP1 Enterprise, 64 bit<br>Windows 2012 | Edge Browser<br>Internet Explorer 9, 10, 11<br>Firefox 52 ESR<br>Chrome 58 |
| macOS | macOS 10.13, 10.12, and 10.11 64 bit | Safari 11.x,10.x, 9.x and 8.x |
| Linux | Ubuntu 17.10, 64 bit<br>Ubuntu 16.04.04, 64 bit and 32 bit<br>Debian 9.4, 64 bit and 32 bit<br>Cent OS 7.4, 64 bit<br>RHEL 7.4, 64 bit<br>Fedora 27, 64 bit and 32 bit | N/A |

### Table 4: Pulse Secure Desktop Client Compatible Platforms

| Platform | Operating System | Web Browser |
|---|---|---|
| Windows | Windows 10 Redstone 4 Version 1803 (OS build 17134)<br>Windows 10 Enterprise, 32 bit<br>Windows 10 (non-Enterprise), 32 and 64 bit<br>Windows 10 Redstone<br>Windows 10 Enterprise, 32 and 64 bit<br>Windows 8.1 (non-Enterprise), 32 and 64 bit<br>Windows 8, 32 and 64 bit<br>Windows 8 Enterprise, 32 and 64 bit<br>Windows 8 Pro, 32 and 64 bit<br>Windows 7 Ultimate, 32 and 64 bit<br>Windows 7 Professional, 32 and 64 bit<br>Windows 7 Home Basic, 32 and 64 bit<br>Windows 7 Home Premium, 32 and 64 bit<br>Windows Embedded Standard 7, 32 and 64 bit<br>Windows 2008, Windows 2016 | Edge browser<br>Internet Explorer 8, 11<br>Firefox 3.0 and later<br>Google Chrome1 |
| MacOS | macOS 10.10, 64 bit | Safari 7.x |

| Platform | Operating System | Web Browser |
|---|---|---|
| Linux | Ubuntu 17.x, 64 bit<br>Ubuntu 16.x, 64 bit and 32 bit<br>Debian 9.x, 64 bit and 32 bit<br>Debian 8.x, 64 bit and 32 bit<br>Cent OS 7.x, 64 bit<br>Cent OS 6.x, 64 bit and 32 bit<br>RHEL 7.x, 64 bit<br>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 Enterprise
- Windows 8.1 Enterprise
- Windows 8 Enterprise
- Windows 7 Enterprise
- macOS 10.13
- macOS 10.12
- macOS 10.11
- macOS 10.10
- Windows 10 Redstone
- Windows 10 Redstone2
- Windows 10 Redstone3

### 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 |
| 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 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)

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 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 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 Mac OS X 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<br>Google Chrome<br>Edge Browser | Pulse Secure Application Launcher (PSAL) |
| macOS | Pulse Secure desktop client<br>Host Checker (HC) | Safari | Pulse Secure Application Launcher (PSAL) |
| macOS | Network Connect (NC)<br>JSAM | Safari | Java |

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<br>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 Routes1 | Disabled | Disabled | Supported | Supported | Supported | Supported | Supported |
| Disabled | Tunnel Routes1 | Disabled | IPv4 Disabled and IPv6 Enabled | Supported | Supported | Supported | Supported | Supported |
| Disabled | Tunnel Routes1 | 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 Routes1 | Disabled | Enabled or Disabled | Supported2 | Supported3 | Supported | Supported | Supported |
| Enabled | Tunnel Routes1 | Enabled | Enabled or Disabled | Supported2 | Supported3 | Supported | Supported | Supported |
| Enabled or Disabled | Endpoint routes | Enabled or Disabled | Enabled or Disabled | Supported2 | Supported3 | 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 many 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.

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, 8.3 | 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 5.3 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 (installation will terminate) | Not supported |
| Nortel Contivity Server 1010 with Pulse Secure Client | Server Version: V04_80.124<br>Client Version: V06_01.109<br>(Win XP SP3) | Install | Not supported |
| Cisco ASA 5505 with Pulse Secure Client | Server Version: 8.0(3)<br>Client Version: 5.0.07.0290<br>(Win 7 64 bit) | Install | Not supported |
| Cisco VPN 3000 Concentrator with Pulse Secure Client | Server Version: 4.1.7 D<br>Client Version: 5.0.07.0290<br>(Win 7 64-Bit) | Runtime | Supported |