Pulse Secure Desktop Client Supported Platforms Guide

Pulse Secure Desktop Client v5.1

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

Product Release	**5.1R5**
Published	**October 2015**
Document Version	**1.2**

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 and Mac OS X.

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 Mac OS X 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 (Windows or Mac) client.

Table 1: Pulse Secure 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 clients for Windows and Mac OS X.

Table 2: Pulse Secure Client/Server Compatibility

Product	Qualified	Compatible
Pulse Connect Secure (formerly Secure Access Service, or SA)	8.1Rx, 8.0Rx, 7.4R4	7.3R7, 7.2 Rx, 7.1Rx
Pulse Policy Secure (formerly Access Control Service, or Unified Access Control/UAC)	C5.1Rx, C5.0Rx, C4.4R4	C4.3R6, C4.2Rx, C4.1Rx
SRX Series Services Gateways	12.1Rx, 11.4R3.x	11.x, 10.x

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 the qualified platforms, and [1]Windows 10 support for the Pulse Secure desktop client was introduced in version 5.1r4. See here for details.
[2]Includes Windows 8.1 Update 1
[3]Mac OSX 10.11 supports certificate authentication in versions greater than Hotfix 5.1R5.1 & release 5.1R6.

Table 4 lists the compatible platforms, for this release of the Pulse Secure client for Windows and Mac OS X. 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 Client Qualified Platforms

Platform	Operating System	Web Browser
Windows	Windows 10 Enterprise, 64 bit[1] Windows 8.1 Enterprise, 64 bit[2] Windows 8.1, 32 bit[2] Windows 8 Enterprise, 64 bit Windows 7 SP1 Enterprise, 64 bit Windows Embedded Standard 7, 32 and 64 bit	Internet Explorer 9, 10, 11 Firefox ESR

Mac OS X	Max OSX 10.11[3] , 10.10 and 10.9, 64 bit	Safari 9.x, 8.x and 7.x

[1]Windows 10 support for the Pulse Secure desktop client was introduced in version 5.1r4. See here for details.
[2]Includes Windows 8.1 Update 1
[3]Mac OSX 10.11 supports certificate authentication in versions greater than Hotfix 5.1R5.1 & release 5.1R6.

Table 4: Pulse Secure Desktop Client Compatible Platforms

Platform	Operating System	Browsers and Java Environment
Windows	Windows 10 Enterprise, 32 bit[1] Windows 10 (non-Enterprise), 32 and 64 bit[1] Windows 8.1 Enterprise, 32 bit[2] Windows 8, 32 bit or 64 bit Windows 8 Enterprise, 32 bit Windows 8 Pro, 32 bit or 64 bit Windows 7 Ultimate, 32 bit or 64 bit Windows 7 Professional, 32 bit or 64 bit Windows 7 Home Basic, 32 bit or 64 bit Windows 7 Home Premium, 32 bit or 64 bit	Internet Explorer 8.0 Internet Explorer 7.0 Firefox 3.0 and later Google Chrome[3]
Mac OS X	Mac OS X 10.8, 64 bit	Safari 6.0, 6.1, Oracle JRE 7 & 8

[1]Windows 10 support for the Pulse Secure desktop client was introduced in version 5.1r4. See here for details.
[2]Includes Windows 8.1 Update 1
[3]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 qualified smart cards and Table 6 lists qualified soft tokens. The listed items have been qualified on the following platforms:

- Windows 8.1 Enterprise, 64 bit
- Windows 8 Enterprise, 64 bit
- Windows 7 Enterprise, 64 bit

Table 5: Qualified 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: Qualified Soft Tokens

Cards	Software Version
RSA	Application version 4.1.0.458
Server	RSA Authentication Manager 7.1
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:

1. DE – German
2. EN – English
3. ES – Spanish
4. FR – French
5. IT – Italian
6. JA – Japanese
7. KO – Korean
8. PL – Polish
9. ZH-CN – Chinese (Simplified)
10. 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

In cases where ActiveX is disabled or is not available because of platform or privilege limitations, the client application is installed using Java. Adaptive delivery is available for Pulse Secure Client and for legacy clients (WSAM, Network Connect, Windows Terminal Services, and Secure Meeting).

Sun JRE 1.7 or later must be installed on the client system to use adaptive delivery for Pulse Secure client applications.

Access Methods

Pulse Secure client supports the following access methods:

- Pulse NC Access Method (PNC)—Layer 3 VPN connection to Pulse Connect Secure
- Pulse UAC Access Method (PUAC)—Layer 2 (802.1x) connection and Layer 3 connections to Pulse Policy Secure
- Pulse Firewall Access Method (FWAM)—VPN connection to SRX Series Services Gateways (Dynamic VPN)
- Windows Secure Access Manager (WSAM)—Per-application VPN tunneling to Pulse Connect Secure

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.

Table 7 lists the configurations that are qualified and compatible. Any combination not mentioned in **Table 7** is not supported. Pulse Policy Secure IPSec enforcement in Pulse Secure Connect Secure (TLS) tunnels is supported.

Table 7: Access Method Configurations

Configuration	Description	Notes
PUAC inside PNC outer tunnel	Inner tunnel: Layer 3 IPSec tunnel authenticated through Pulse Policy Secure to ScreenOS or SRX device firewall sending enforcement information. Outer tunnel: PNC (TLS or ESP) VPN tunnel to Pulse Connect Secure	Qualified
PUAC inside PNC outer tunnel + FWAM	PUAC Layer 3 source IP or IPSec enforcement over PNC remote access (TLS) to Pulse Connect Secure, running in parallel with FWAM IPSec connection to another SRX device	Compatible
PUAC (L2/L3) + PUAC(L3)	One Pulse UAC Layer 2 connection running in parallel to multiple PUAC Layer 3 connections	Qualified
PUAC + FWAM	PUAC enforcement tunnel to one ScreenOS or SRX device running in parallel with FWAM IPSec connection to another SRX device	Compatible

Table 8 lists the supported nested tunnel (tunnel-in-tunnel) configurations. The configurations are for a Pulse Connect Secure v8.1 outer tunnel, a Pulse Policy Secure v5.1 inner tunnel, and the Pulse Secure client v5.1.

Table 8: 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[4]	Supported	Supported
Disabled	Tunnel Routes[1]	Disabled	IPv4 Disabled and IPv6 Enabled	Supported	Supported	Supported[4]	Supported	Supported
Disabled	Tunnel Routes[1]	Disabled	IPv4 Enabled and IPv6 Disabled	Not Supported	Supported	Supported[4]	Supported	Supported
Disabled	Tunnel Routes	Enabled	Enabled or Disabled	Not Supported	Supported	Supported[4]	Supported	Supported
Enabled	Tunnel Routes[1]	Disabled	Enabled or Disabled	Supported[2]	Supported[3]	Supported[4]	Supported	Supported
Enabled	Tunnel Routes[1]	Enabled	Enabled or Disabled	Supported[2]	Supported[3]	Supported[4]	Supported	Supported
Enabled or Disabled	Endpoint routes	Enabled or Disabled	Enabled or Disabled	Supported[2]	Supported[3]	Supported[4]	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 in the Pulse split-tunneling network policy.
[3]Pulse 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.
[4]Supported on ScreenOS but not supported on SRX.

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

Client Interoperability

Pulse Secure client provides all of the services of previous Pulse Secure clients (except for services announced as deprecated). You can install the Pulse Secure client on endpoints that have other Pulse Secure clients. 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 9 describes Pulse Secure client interoperability. **Table 10** 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 9: Pulse Secure Client Interoperability

Product	Version	Coexistence	Nested Tunnel Operation
Network Connect	7.4, 8.0	Runtime	Limited support – see Table 7.
Network Connect	6.3, 6.4, 6.5, 7.0, 7.1, 7.2, 7.3	Install	Not supported
Odyssey Access Client (OAC)	5.6	Runtime	OAC 802.1x in Layer 2 with Pulse 5.0 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
Juniper (Netscreen) NSRemote Client	Any	Install	Not supported
Juniper Access Manager (Dynamic VPN Client)	Any	Not supported (installation will terminate)	Not supported

Table 10: Third-Party Client Interoperability

Product	Version	Coexistence	Nested Tunnel Operation
Cisco VPN 300	Server Version: 4.1.7D	Install	Concentrator with Pulse

Secure Client	Client Version: 4.6.04.0043	Install	Not supported

Product	Version	Coexistence	Nested Tunnel Operation
Nortel Contivity Server 1010 with Pulse Secure Client (non-APP ACCEL)	Server Version: V04_80.124 Client Version: V06_01.109 (Win XP SP3)	Install	–
Cisco ASA 5505 with Pulse Secure Client (non-APP ACCEL)	Server Version: 8.0(3) Client Version: 4.6.04.0043 (Win XP SP3) 5.0.07.0290 (Win 7 64 bit)	Install	–
Cisco VPN 3000 Concentrator with Pulse Secure Client (using only APP ACCELAM)	Server Version: 4.1.7 D Client Version: 4.6.04.0043 (Win XP SP3) 5.0.07.0290 (Win 7 64-Bit)	Runtime	Supported
Nortel Contivity Server 1010 with Pulse Secure Client (using only APP ACCELAM)	Server Version: V04_80.124 Client Version: V06_01.109 (Win XP SP3)	Runtime	Supported
Cisco ASA 5505 with Pulse Secure Client (using only APP ACCELAM)	Server Version: 8.0(3) Client Version: 6.04.0043 (Win XP SP3) 0.07.0290 (Win 7 64 bit)	Runtime	Supported
Checkpoint CP Secure Remote	Client Version: NGX R60 HFA2 (Build 002) (Win XP SP3)	Install	Not supported

Revision History

Table 11 lists the revision history for this document.

Table 11: Revision History

Revision	Date	Description
1.3	April 2016	Added Safari 9.x
1.2	September 2015	Added Mac OSX 10.11 El Capitan Support
1.1	September 2015	Added Windows 10 Support
1.0	December 2014	Initial publication