Pulse Policy Secure

Supported Platforms Guide

PPS 9.1R1
Build- 1231

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

Product Release	**9.1R1**
Published	**May 2019**
Revision	**1.1**

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

Table 1 lists the revision history for this document.

Table 1: Revision History

Revision	Description
May 2019	Added Juniper switch model as qualified for Policy Enforcement using SNMP (ACL based).
April 2019	PPS Release Notes 9.1R1 updates.

Contents

Revision History 3
Introduction 5
Hardware 6
Administrator Web User Interface 7
Pulse Secure Client Software 8
Third-Party Wireless LAN Controller 8
Third-Party 802.1X Supplicants 9
Agentless Access (Browsers) 11
Agentless Access (Java-Based) 14
Host Checker 14
Platform Support for Device Onboarding 16
Platform Support for AAA 16
MDM Solutions 18
802.1X Authenticators in Layer 2 Network Access Control Deployments 19
Endpoint Security Assessment Plug-in (ESAP) Compatibility 20
Infranet Enforcers in Layer 3 Resource Policy Deployments 20
Admission/Identity Control 21
Behavioral Analytics 21
IF-MAP Compatibility 22
Policy Enforcement Using SNMP 22
Profiling using Network Infrastructure Device collector 23
Agentless Host Checker with Profiler 24

Introduction

This document describes the client environments and IT infrastructure that are compatible with this release.

In this document, we identify compatibility testing for this release with the following terminology:

- Qualified (Q) –Indicates that the item was systematically tested by QA for this release.
- Compatible (C)–Indicates that the item was not tested for this release, but based on testing done for previous releases, we support it.

Pulse Secure supports all items listed as qualified or compatible.

Hardware

You can install and use Release software on the following platforms.

- PSA300
- PSA3000
- PSA5000
- PSA7000f
- PSA7000c
- Virtual Appliances (PSA-V) on ESXi, KVM and Hyper-V

Administrator Web User Interface

Table 2 lists supported platforms for the administrator user interface.

Table 2: Admin User Interface

Operating System	Browsers/Java	Qualified	Compatible
Windows			
• Windows 10, Redstone 5, 64-bit • Windows 8.1 Enterprise, 64-bit • Windows 7 Enterprise, 64-bit	• Firefox 60 ESR • Google Chrome 74	Q	
• Windows 10, Redstone 4, 64-bit • Windows 10, Redstone 3 (1709) Enterprise, 64-bit • Windows 10, Redstone 2 (1703) Enterprise, 64-bit • Windows 8.1 Enterprise, 64-bit Windows 7 Enterprise, 64-bit	Internet Explorer 11/Edge Browser Firefox 52 ESR		C
• Windows 8.1 Professional, 64-bit • Windows 8 basic edition / Enterprise / Professional, 32-bit or 64-bit • Windows 7 Ultimate / Professional / Home Basic / Home Premium, 32-bit or 64-bit • Windows 7 SP1 Enterprise, 32-bit • Windows Vista Enterprise / Ultimate / Business / Home-Basic / Home-Premium, 32-bit or 64-bit	• Internet Explorer 11 • Internet Explorer 9.0 • Internet Explorer 8.0 • Internet Explorer 7.0 • Google Chrome • Firefox 3.0 and later		C
Mac			
• Mac OS X 10.14, 64-bit	Safari 12.1	Q	
• Mac OS X 10.13, 64-bit • Mac OS X 10.12, 64-bit • Mac OS X 10.11, 64-bit • Mac OS X 10.11, 64-bit • Mac OS X 10.10, 64-bit • Mac OS X 10.9, 64-bit • Mac OS X 10.8, 64-bit	• Safari 11.1 • Safari 11.0 • Safari 10.0 • Safari 9.0 • Safari 8.0 • Safari 7.0 • Safari 5.1		C

Pulse Secure Client Software

For a list of supported platforms for the Pulse Secure desktop client, please consult the Pulse Secure Desktop Client Supported Platforms Guide, which can be found here.

Third-Party Wireless LAN Controller

Table 3 lists platform requirements for third-party wireless LAN Controller.

Table 3: Third-Party Wireless Controller

Platform	Environment	Qualified	Compatible
Cisco			
	• Cisco 2500 WLC [version 8.0.140.0] AIR-CAP702I [version is 15.2(4) JB6] • Cisco catalyst 3850 [Cisco IOS Software, IOS-XE Software, • Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 03.07.00E] AIR-CAP702I (version is 15.3(3) JNB)	Q	
	• Cisco 5500 Series WLC • Cisco 7500 Series WLC • Cisco 8500 Series WLC		C
Aruba			
	• Aruba 650 WLC [Aruba OS 6.1.3.6], AP-105 [ArubaOS Version 6.1.3.6] • Aruba 3400 WLC [Aruba OS 6.4.4.6], AP-205 [ArubaOS Version 6.4.2.4] • Aruba Instant Access Point 205 AP-205 [6.4.2.3-4.1.1.3]	Q	
	• Aruba 600 Series WLC • Aruba 3200 Series WLC • Aruba 3600 Series WLC • Aruba Instant Access Point 200 Series		C
Ruckus			
	• Zone Director 1200 Series WLC [9.9.0.0.216] • Virtual SmartZone – High Scale [3.2.0.0.790]	Q	

Cisco Meraki			
	Model: MR 42 Firmware version: MR 25.13	Q	

Third-Party 802.1X Supplicants

Table 4 lists platform requirements for third-party 802.1X supplicants.

Table 4: Third-Party 802.1X Supplicants

Platform	Environment	Qualified	Compatible
Windows			
	Windows 10, Redstone 5, 64-bit • Windows 10, Redstone 4, 64-bit • Windows 8.1 Enterprise, 64-bit • Windows 7 SP1 Enterprise, 64-bit.	Q	
	• Windows 10, Redstone 3 (1709) Enterprise, 64-bit • Windows 10, Redstone 2 (1703) Enterprise, 64-bit • Windows 10, Redstone 1 (1607) Enterprise, 64-bit • Windows 8 basic edition / Professional / Enterprise,32-bit or 64-bit • Windows 7 Ultimate / Professional / Home Basic / Home Premium, 32-bit or 64- bit • Windows 7 SP1 Enterprise, 32-bit • Windows Vista Ultimate / Business / Home-Basic / Home-Premium with SP 2, 32-bit or 64-bit		C
Mac			
	• Mac OS X 10.14, 64-bit • Mac OS X 10.13, 64-bit • Mac OS X 10.12, 64-bit • Mac OS X 10.11, 64-bit	Q	
	• Mac OS X 10.10, 32-bit/64-bit • Mac OS X 10.9, 64-bit • Mac OS X 10.8, 64-bit • Mac OS X 10.7.3, 32-bit, and 64-bit		C
Google Android			

	Android 8.1, 8.0	Q
	Android 7.0	C
	Android 6.0	C
Apple iOS		
	iOS 12.1, 11.2.6	Q
	iOS 10, 9.0, 8.0	C

Agentless Access (Browsers)

Table 5 lists desktop platform requirements for the agentless access using browsers.

Table 5: Agentless Access (Browsers)

Operating System	Browsers/Java	Qualified	Compatible
Windows			
• Windows 10, Redstone 5, 64-bit • Windows 10, Redstone 4, 64-bit • Windows 8.1 Enterprise, 64-bit • Windows 7 SP1 Enterprise, 64-bit	• Firefox 60 ESR • Google Chrome • Oracle JRE 8	Q	
• Windows 10, Redstone 3 (1709) Enterprise, 64-bit • Windows 10, Redstone 2 (1703) Enterprise, 64-bit	• Internet Explorer 11/Edge Browser • Firefox 60 ESR • Google Chrome • Oracle JRE 8		C
• Windows 10, Redstone 1 (1607) Enterprise, 64-bit	• Internet Explorer 11/Edge Browser • Firefox 60 ESR • Firefox 52 ESR • Google Chrome • Oracle JRE 8		C
• Windows 8.1 Professional, 64-bit • Windows 8 basic edition / Enterprise / Professional, 32-bit or 64-bit • Windows 7 Ultimate / Professional / Home Basic / Home Premium, 32-bit, or 64-bit platforms • Windows 7 SP1 Enterprise, 32-bit or 64-bit • Windows Vista Ultimate / Business / Home-Basic / Home-Premium with SP 2, 32-bit, or 64-bit platforms	• Internet Explorer 11 • Internet Explorer 10 • Internet Explorer 9.0 • Internet Explorer 8.0 • Internet Explorer 7.0 • Firefox 3.0 and later • Google Chrome • Oracle JRE 6 and later		C
Mac			
• Mac OS X 10.14, 64-bit • Mac OS X 10.13, 64-bit • Mac OS X 10.12, 64-bit	• Safari 11.1.1 • Safari 11.0 • Safari 10.0	Q	

Operating System	Browsers/Java	Qualified	Compatible
• Mac OS X 10.11, 64-bit • Mac OS X 10.10, 64-bit • Mac OS X 10.9, 32-bit /64-bit • Mac OS X 10.8, 64-bit • Mac OS X 10.7.4, 32-bit or 64-bit	• Safari 11.1.1 • Safari 9.0 • Safari 8.0 Sun JRE 7 • Safari 7.0 Sun JRE 7 • Google Chrome		C
Linux			
• Ubuntu 18.04 • Ubuntu 14.x • openSUSE 12.1	• Firefox 52 ESR • Oracle JRE 8	Q	
• openSUSE 10.x and 11.x • Ubuntu 9.10, 10.x, and 11.x • Red Hat Enterprise Linux 5	• Firefox 3.0 and later • Google Chrome • Oracle JRE 6 and later		C
Solaris			
Solaris 10, 32-bit	Firefox 24 ESR		C
Solaris 10, 32-bit	Mozilla 2.0 and later		C

Table 6 lists requirements for the smart mobile devices that can gain agentless access to the network using the Web browsers indicated.

Table 6: Smart Mobile Devices for Layer 3 Access

Device/Operating System	Browsers/Java	Qualified	Compatible
Apple 12.1.1	Safari	Q	
Apple iOS 11.4.1	Safari		C
Apple iOS 12	Safari		C
Apple iOS 11.2.6	Safari		C
Apple iOS 8.0	Safari		C
Apple iOS 7.0 and later	Safari		C
Google Android			
Android 8.0	Android native browser	Q	
Android 7.0			C
Android smart phones with Android 4.4 and later	Android native browser		C

Agentless Access (Java-Based)

Table 7 lists platform requirements for the agentless access that is Java-based.

Table 7: Agentless Access (Java-Based)

Operating System	Browsers/Java	Qualified	Compatible
Linux			
• openSUSE 12.1, 32-bit • Ubuntu 18.x, 32-bit • Ubuntu 14.x, 32-bit	• Firefox 52 ESR • ORACE JRE 8 Iced Tea	Q	
• openSUSE 11.x and 10.x • Ubuntu 11.x, 10.x, and 9.10 • Red Hat Enterprise Linux 5	• Firefox 3.0 and later • Oracle JRE 6 and later		C
Solaris OS 12	Firefox 24 ESR		C

Host Checker

Table 8 lists the HC support on different platforms

Table 8: Host Checker

Operating System	Browsers	Qualified	Compatible
Windows			
Windows-10 Redstone 5 OS Build 1809 Version 10.0.17763.134, 64 bit	Google Chrome 74, Firefox ESR 60, Oracle JRE 8 Internet Explorer 11, Edge	Q	
Windows-10 Redstone 4 OS Build 1803 Version 10.0.17134, 64-bit	Google Chrome 74, Firefox 60 ESR, Oracle JRE 8 update 144		C
Windows 10 Enterprise/Pro/Home	Internet Explorer 11, Edge Google Chrome 74 Firefox 60 ESR, Oracle JRE 8		C
Windows 8.1 Update/ Professional / Enterprise, 64-bit	Internet Explorer 11, Google Chrome 74 and Firefox 60 ESR, Oracle JRE 8	Q	
Windows 8.1 Update/ Professional / Enterprise, 32-bit	Internet Explorer 11, Google Chrome 74 and Firefox 60 ESR, Oracle JRE 8		C
Windows 8 Basic edition / Professional/ Enterprise, 32-bit & 64-bit	Internet Explorer 10, Google Chrome 74 and Firefox 60 ESR, Oracle JRE 7 and later		C

Windows 7 Enterprise SP1, 64-bit	Internet Explorer 11, Google Chrome 74 and Firefox 60 ESR, Oracle JRE 8		C
Windows 7 Ultimate / Professional / Home Basic / Home, 32-bit or 64-bit Windows 7 Enterprise (32-bit)	Internet Explorer 11, Google Chrome 74 Firefox 60 ESR, Oracle JRE 7 and later		C
Mac OSX			
Mac OS Mojave Version 10.14	Safari 12.1, Google Chrome 73	Q	
Mac OS High Sierra Version 10.13	Safari 11.0, Google Chrome 73	Q	
Mac OS X 10.12	Safari 10.1, Safari 9.0, Google Chrome 73	Q	
Mac OS X 10.10, 10.11	Safari 10.1, Safari 8.0, Google Chrome		C
Mac OS X 10.9	Safari 9.1.3, Safari 9.0, Safari 7.0, Google Chrome 61		C
Mac OS X 10.8	Safari 6.2.8, Safari 6.0, Google Chrome 61		C
Linux			
openSUSE 12.1	Firefox 38 ESR Firefox 52 ESR, 32-bit		C
openSUSE 11.x, 10.x	Oracle JRE 8		C
Ubuntu 16.04 LTS	Firefox 52, ESR, 64-bit		C
Ubuntu 15.04	Firefox 52, ESR, 64-bit		C
Ubuntu 14.04 LTS	Firefox 52, ESR, 64-bit	Q	
Ubuntu 12.04 LTS, 11.x, 10.x, 9.10	Oracle JRE 7 and later		C
RHEL 5,7	Firefox 52 ESR, 32-bit, 64-bit		C
Fedora 23 (32 bit, 64 bit)	Firefox 52 ESR 32-bit, 64-bit		C
CentOS 6.4	Firefox 52, 32- bit, 64- bit		C

Platform Support for Device Onboarding

Table 9 lists platform requirements for device onboarding features that are qualified with this release.

Table 9: Device Onboarding Features

Operating System/Feature	VPN	Certificate	Wifi
iOS 11.4.1	Q	Q	Q
iOS 12.1	Q	Q	Q
*Android 8.0	Q	Q	Q
*Android 7.0	Q	Q	Q
Windows 8.1 Desktop		Q	Q
Windows 7		Q	Q
Mac OS X 10.13		Q	Q
Mac OS X 10.12, Safari 9.x		Q	Q

*Enterprise onboarding is not working on Android devices. See the Release Notes for more details.

Platform Support for AAA

Table 10 lists platform requirements for third-party AAA servers that are compatible with this release.

Table 10: Third-Party AAA Servers

Third-Party AAA Server	Qualified	Compatible
Active Directory	• Windows 2016	• Windows 2012 R2 • Windows 2008 R2 • Windows 2003
LDAP using Active Directory	• Windows 2016 • Windows 2012 R2	• Windows 2008 R2 • Windows 2003

Third-Party AAA Server	Qualified	Compatible
LDAP using Novell eDirectory		Novell Client for Windows 2000 / XP Version 4.91 SP2
LDAP using Sun ONE iPlanet Server		Sun ONE Directory Server 5.2
LDAP with Greatbay Endpoint Profiler		Beacon 4.2.0_42
LDAP (other standards-compliant servers)	OpenLDAP 2.3.27	Authentication and authorization based on user attributes or group membership
RADIUS	• Steel-Belted Radius (SBR) 6.1 • RSA Authentication Manager 6.1 • Defender 5.2 • Windows IAS 2008	
RADIUS (other standards compliant servers)		C
ACE	• RSA Authentication Manager 7.1 SP4 • RSA Authentication Manager 6.1 • RSA Authentication Manager 5.2	
Siteminder	• CA Siteminder 12.0 SP3 • CA Siteminder 6.0 SP4 • CA Siteminder 5.5	
Certificate	• Windows Server 2008 R2 Certificate Services • RSA Keon Certificate Manager 6.5.1	
Certificate (other standards-compliant servers)		C
SQL	• Oracle 11g Express Edition	
*SAML 2.0,1.1	Okta, Ping One, ADFS, PCS	Q
*SAML 2.0,1.1	Ping Federate	C

*For information on the SAML SSO profiles, bindings, and protocols that are supported, see here.

MDM Solutions

Table 11 lists the requirements for integration with mobile device management (MDM) vendors.

Table 11: MDM Vendors

Solution	Qualified	Compatible
AirWatch		
Cloud service	19.03.0.6	18.10.0.4
Appliance OS		C
Virtual appliance OS		C
MobileIron		
Cloud service	10.1.0.2	9.7.0.2 Build 10
Appliance OS		C
Virtual appliance OS		C
Microsoft Intune		C (with AD user names only)

802.1X Authenticators in Layer 2 Network Access Control Deployments

Table 12 lists the 802.1X authenticators that have been qualified with this release. 802.1X authenticators are Layer 2 Ethernet switches. In addition to the qualified platforms, other 802.1X standards-compliant Ethernet switches are compatible.

Table 12: 802.1X Authenticators

Platforms	Hardware Models	OS Version	Qualified	Compatible
EX Series	EX 8200 EX 6200 EX 4500 EX 4200	Junos OS 15.1R4, 17.0	Q	
Cisco Series	Cisco 2960 Cisco 3850 Cisco 3750 Cisco WLC 2500 Series Meraki MR 42	15.2(6) E2 16.9.1 12.2(55) SE11 8.5.135.0 MR 25.13	Q	
Huawei	Huawei S5720	5.170	Q	
HP Procurve	2920 series	WB.15.12.0015	Q	
Aruba	Aruba3400	6.4.4.6	Q	
Ruckus	Zone Director SmartZone	9.9.0.0 build 216 3.5.1.0.296	Q	
SRX Series	SRX 650 SRX VM	Junos 12.3X48-D30.7 Junos 15.1X49-D140.2	Q	
SRX Series	SRX 3400 SRX 1400 SRX 240 SRX 220 SRX 210 SRX 100	Junos OS 12.1X46-D35.1		C
802.1X (other standards-compliant Ethernet switches)				C

Endpoint Security Assessment Plug-in (ESAP) Compatibility

The default version for ESAP is 3.3.5

Infranet Enforcers in Layer 3 Resource Policy Deployments

Table 13 lists Infranet Enforcers that have been qualified with this release. Infranet Enforcers are enforcement points in Layer 3 resource policy deployments. In addition to the qualified platforms, other Screen OS, SRX Series, and EX Series models are compatible, provided the firewall or switch model and software version supports integration with Pulse Policy Secure.

Table 13: Infranet Enforcers

Platform	Hardware Models	Software Versions
Checkpoint Firewall	Virtual Appliance	R80.20 R80.10
Palo Alto Network	Virtual Appliance	9.0.0
SRX Series	• SRX 220 • SRX 650	Junos OS 12.3X48-D30.7 Junos OS 12.3X48-D70.3
*ScreenOS	• SSG550 • SSG20 • ISG-1000	ScreenOS 6.3.0R21
EX Series	• EX 4200	Junos OS 12.3R10.2* Unsupported in latest Junos versions.

Admission/Identity Control

Table 14 lists the IDP devices that are supported.

Table 14: IDP Devices in Admission Control Deployments

Hardware Models	Software Versions
Fortinet Fortigate Firewall	Fortinet Firewall: v6.0.4 build0231 (GA) Fortinet Firewall: v6.0.2 build0163 (GA) Fortinet Firewall v5.6.2, build1486 (GA) Fortinet Firewall: v5.4.2, build1100 (GA)
Forti Authenticator	v6.0.0, build0010 (GA) v 5.5.0, build0366(GA) v5.2.1, build0161 (GA) v4.00-build0019-20151007-patch00
Forti Analyzer	v6.0.4-build0292 190109 (GA) v6.0.2-build0205 180813 (GA) v5.4.2-build1151 161213 (GA) v5.6.2-build1151 161213 (GA)
Palo Alto Networks Firewall	9.0.0 8.0.7
Juniper SDSN Solution	Junos SRX 15.1X49-D140.2 Junos Space 18.3

Behavioral Analytics

Table 1415 lists the switch models that are supported.

Hardware Models	Software Versions
Cisco 3850	03.06.08E
Cisco 2960	15.2(6)E1

IF-MAP Compatibility

Table 16 lists the IF-MAP clients that are supported.

Table 16: IF-MAP clients

IF-MAP Client	Qualified	Compatible
Pulse Connect Secure	Q	
Pulse Policy Secure	Q	Older than 9.0R3

Policy Enforcement Using SNMP

Table 17: Switch List lists the switches which are qualified for Policy Enforcement using SNMP.

Table 17: Switch List

Platform	Hardware Models	Software Version	Qualified
VLAN Based			
Cisco	• 2960 Series • 3750 Series • 3850 Series	• 15.0.(2)EX5 • 12.2(55)ES8 • IOS-XE 03.07.00E	Q
HP	• 2920 Series	• WB.15.12.0015	Q
ACL Based			
Cisco	• 2960 Series • 3750 Series	• 15.0.(2)EX5 • 12.2(55)ES8	Q
HP	• 2920 Series	• WB.15.12.0015	Q
Juniper	• EX4200	• 15.1R4.6	Q

Profiling using Network Infrastructure Device collector

Table 18: lists the devices which are qualified for device profiling using Network Infrastructure Device Collector.

Table 18: Device List

Platform	Hardware Models	Software Version	Qualified	Compatible
Cisco	2960 Series	15.2(2) E3	Q	
HP	2920 Series	WB.15.12.0015	Q	
Juniper	EX 2200 Series	12.3R12.4	Q	
Foundry	FESX424 Series	07.2.02		C
Nortel	2526T Series	4.0.0.000		C
D-Link	DES-3226S	4.01-B21		C
Cisco WLC	2500 WLC	7.6.130.0	Q	
Aruba WLC	3400 WLC	6.4.2.4	Q	
Ruckus WLC	1200 WLC	9.9.0.0.216	Q	
Trapeze WLC	WLC-V	9.0.1.2.0		C
FortiGate	100D	5.4.2-1000	Q	
Palo Alto Networks Firewall	PA 3000	OS 7.0.1/OS 7.0.1 (VM)	Q	
Huawei	S5720		Q	

Agentless Host Checker with Profiler

Table 19 lists supported Windows platforms and Security Products for Agentless Host checking with Profiler.
Note: Applicable with ESAP version 3.3.3 and greater.

Table 19: Agentless Host Checker with Profiler

Operating System	Security Products (Antivirus / Firewall / Antispyware)	Qualified	Compatible
Windows 7/64-bit	Symantec Endpoint Protection 14.x	Q	
Windows 7/64-bit	McAfee Total Protection 16.x		C
Windows 8/64-bit	McAfee Total Protection 16.x	Q	
Windows 8/64-bit	Symantec Endpoint Protection 14.x		C
Windows 10/64-bit	Symantec Endpoint Protection 14.x	Q	
Windows 10/64-bit	McAfee Total Protection 16.x		C
Windows 7/32-bit	McAfee Total Protection 16.x	Q	
Windows 7/32-bit	Symantec Endpoint Protection 14.x		C
Windows 8/32-bit	Symantec Endpoint Protection 14.x McAfee Total Protection 16.x		C
Windows 10/32-bit	Symantec Endpoint Protection 14.x McAfee Total Protection 16.x		C