



Pulse Policy Secure

Supported Platforms Guide

PPS 9.0R3
Build- 51661

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

Product Release	9.0R3
Published	December 2018
Revision	2.2

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

© 2018 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.

Revision History

Table 1 lists the revision history for this document.

Table 1: Revision History

Revision	Description
December 2018	PPS Release 9.0R3 updates. Newly added: Behavioral Analytics, Agentless HC with Profiler, Huawei switch support for 802.1X, Admission Control (Juniper SDN)
April 2018	PPS Release 9.0R1 updates.
December 2017	PPS Release 5.4R4 updates- Added Check Point version R80.10.
September 2017	PPS Release 5.4R3 updates.
September 2017	Checkpoint, Fortinet, Microsoft Intune entries are newly added.

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).....	10
Agentless Access (Java-Based)	13
Platform Support for Device Onboarding	13
Platform Support for AAA	14
MDM Solutions.....	15
802.1X Authenticators in Layer 2 Network Access Control Deployments	16
Endpoint Security Assessment Plug-in (ESAP) Compatibility	17
Infranet Enforcers in Layer 3 Resource Policy Deployments	18
Admission/Identity Control	19
Behavioral Analytics.....	19
IF-MAP Compatibility.....	20
Policy Enforcement Using SNMP.....	20
Profiling using Network Infrastructure Device collector	21
Agentless Host Checker with Profiler	22

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 9.0R3 software on the following platforms.

- PSA300
- PSA3000
- PSA5000
- PSA7000f
- PSA7000c
- Virtual Appliances (VA-SPE/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			
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Internet Explorer 11/Edge Browser Firefox 52 ESR Google Chrome 	X	
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Internet Explorer 11 Internet Explorer 9.0 Internet Explorer 8.0 Internet Explorer 7.0 Google Chrome Firefox 3.0 and later 		X
Mac			
<ul style="list-style-type: none"> Mac OS X 10.14, 64-bit Mac OS X 10.13, 64-bit Mac OS X 10.12, 64-bit 	<ul style="list-style-type: none"> Safari 11.0 Safari 10.0 Safari 9.0 	X	
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Safari 8.0 Safari 7.0 Safari 5.1 		X

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			
	<ul style="list-style-type: none"> Cisco 2500 WLC [version 8.0.140.0] AIR-CAP7021 [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-CAP7021 (version is 15.3(3)JNB) 	X	
	<ul style="list-style-type: none"> Cisco 5500 Series WLC Cisco 7500 Series WLC Cisco 8500 Series WLC 		X
Aruba			
	<ul style="list-style-type: none"> 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] 	X	
	<ul style="list-style-type: none"> Aruba 600 Series WLC Aruba 3200 Series WLC Aruba 3600 Series WLC Aruba Instant Access Point 200 Series 		X
Ruckus			
	<ul style="list-style-type: none"> Zone Director 1200 Series WLC [9.9.0.0.216] Virtual SmartZone – High Scale [3.2.0.0.790] 	X	

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			
	<ul style="list-style-type: none"> Windows 10, Redstone 4, 64-bit 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 8.1 Enterprise, 64-bit Windows 7 SP1 Enterprise, 64-bit. 	X	
	<ul style="list-style-type: none"> 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 		X
Mac			
	<ul style="list-style-type: none"> 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 	X	
	<ul style="list-style-type: none"> 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 		X
Google Android			
	Android 8.1, 8.0	X	
	Android 7.0		X
	Android 6.0		X
Apple iOS			
	iOS 12.1, 11.2.6	X	
	iOS 10, 9.0, 8.0		X

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			
<ul style="list-style-type: none"> Windows 10, Redstone 4, 64-bit Windows 8.1 Enterprise, 64-bit Windows 7 SP1 Enterprise, 64-bit 	<ul style="list-style-type: none"> Internet Explorer 11/Edge Browser Firefox 60 ESR Google Chrome Oracle JRE 8 	X	
<ul style="list-style-type: none"> Windows 10, Redstone 3 (1709) Enterprise, 64-bit Windows 10, Redstone 2 (1703) Enterprise, 64-bit 	<ul style="list-style-type: none"> Internet Explorer 11/Edge Browser Firefox 60 ESR Google Chrome Oracle JRE 8 		X
<ul style="list-style-type: none"> Windows 10, Redstone 1 (1607) Enterprise, 64-bit 	<ul style="list-style-type: none"> Internet Explorer 11/Edge Browser Firefox 60 ESR Firefox 52 ESR Google Chrome Oracle JRE 8 		X
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> 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 		X
Mac			

Operating System	Browsers/Java	Qualified	Compatible
<ul style="list-style-type: none"> Mac OS X 10.14, 64-bit Mac OS X 10.13, 64-bit Mac OS X 10.12, 64-bit 	<ul style="list-style-type: none"> Safari 11.1.1 Safari 11.0 Safari 10.0 	X	
<ul style="list-style-type: none"> 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 	<ul style="list-style-type: none"> Safari 11.1.1 Safari 9.0 Safari 8.0 Sun JRE 7 Safari 7.0 Sun JRE 7 Google Chrome 		X
Linux			
<ul style="list-style-type: none"> Ubuntu 14.x openSUSE 12.1 	<ul style="list-style-type: none"> Firefox 52 ESR Oracle JRE 8 	X	
<ul style="list-style-type: none"> openSUSE 10.x and 11.x Ubuntu 9.10, 10.x, and 11.x Red Hat Enterprise Linux 5 	<ul style="list-style-type: none"> Firefox 3.0 and later Google Chrome Oracle JRE 6 and later 		X
Solaris			
Solaris 10, 32-bit	Firefox 24 ESR	X	
Solaris 10, 32-bit	Mozilla 2.0 and later		X

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 iOS 11.4.1	Safari	X	
Apple iOS 12	Safari	X	
Apple iOS 11.2.6	Safari		X
Apple iOS 8.0	Safari		X
Apple iOS 7.0 and later	Safari		X
Google Android			
Android 8.0	Android native browser	X	
Android 7.0			X
Android smart phones with Android 4.4 and later	Android native browser		X

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			
<ul style="list-style-type: none"> openSUSE 12.1, 32-bit Ubuntu 14.x, 32-bit 	<ul style="list-style-type: none"> Firefox 52 ESR Oracle JRE 8 	X	
<ul style="list-style-type: none"> openSUSE 11.x and 10.x Ubuntu 11.x, 10.x, and 9.10 Red Hat Enterprise Linux 5 	<ul style="list-style-type: none"> Firefox 3.0 and later Oracle JRE 6 and later 		X
Solaris OS 12	Firefox 24 ESR		X

Platform Support for Device Onboarding

Table 8 lists platform requirements for device onboarding features that are qualified with this release.

Table 8: Device Onboarding Features

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

Platform Support for AAA

Table 9 lists platform requirements for third-party AAA servers that are compatible with this release.

Table 9: Third-Party AAA Servers

Third-Party AAA Server	Qualified	Compatible
Active Directory	<ul style="list-style-type: none"> Windows 2016 Windows 2012 R2 	<ul style="list-style-type: none"> Windows 2008 R2 Windows 2003
LDAP using Active Directory	<ul style="list-style-type: none"> Windows 2016 Windows 2012 R2 	<ul style="list-style-type: none"> Windows 2008 R2 Windows 2003
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	<ul style="list-style-type: none"> Steel-Belted Radius (SBR) 6.1 RSA Authentication Manager 6.1 Defender 5.2 Windows IAS 2008 	
RADIUS (other standards compliant servers)		X
ACE	<ul style="list-style-type: none"> RSA Authentication Manager 7.1 SP4 RSA Authentication Manager 6.1 RSA Authentication Manager 5.2 	
Siteminder	<ul style="list-style-type: none"> CA Siteminder 12.0 SP3 CA Siteminder 6.0 SP4 CA Siteminder 5.5 	
Certificate	<ul style="list-style-type: none"> Windows Server 2008 R2 Certificate Services RSA Keon Certificate Manager 6.5.1 	
Certificate (other standards-compliant servers)		X
SQL	<ul style="list-style-type: none"> Oracle 11g Express Edition 	

MDM Solutions

Table 10 lists the requirements for integration with mobile device management (MDM) vendors.

Table 10: MDM Vendors

Solution	Qualified	Compatible
AirWatch		
Cloud service	18.10.0.4	9.3.0.2 8.4.7.0
Appliance OS		X
Virtual appliance OS		X
MobileIron		
Cloud service	9.7.0.2 Build 10	Core 9.1.1.0 Build 29 Core 9.5.0.0 Build 77
Appliance OS		X
Virtual appliance OS		X
Microsoft Intune		
		X (with AD user names only)

802.1X Authenticators in Layer 2 Network Access Control Deployments

Table 11 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 11: 802.1X Authenticators

Platforms	Hardware Models	OS Version	Qualified	Compatible
EX Series	EX 8200	Junos OS 15.1R4, 17.0	X	
	EX 6200			
	EX 4500			
	EX 4200			
Cisco Series	Cisco 2960	15.2(2) E3	X	
	Cisco 3850	16.3.1		
	Cisco 3750	12.2(55) SE8		
	Cisco WLC 2500 Series	8.0.140.0 8.5.135.0		
Huawei	Huawei S5720	5.170	X	
HP Procurve	2920 series	WB.15.12.0015	X	
Aruba	Aruba3400	6.4.4.6	X	
Ruckus	Zone Director	9.9.0.0 build 216	X	
	SmartZone	3.5.1.0.296		
SRX Series	SRX 650	Junos 12.3X48-D30.7	X	
	SRX VM	Junos 15.1X49-D140.2		
SRX Series	SRX 3400	Junos OS 12.1X46-D35.1		X
	SRX 1400			
	SRX 240			
	SRX 220			
	SRX 210			
SRX 100				
802.1X (other standards-compliant Ethernet switches)				X

Endpoint Security Assessment Plug-in (ESAP) Compatibility

ESAP package version 3.2.7 is the minimum version with this release. The default version for ESAP is 3.3.2

Infranet Enforcers in Layer 3 Resource Policy Deployments

Table 12 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 12: Infranet Enforcers

Platform	Hardware Models	Software Versions
Checkpoint Firewall	Virtual Appliance	R80.10
		R77.30
Palo Alto Network	<ul style="list-style-type: none"> • PA 500 • PA 3000 	OS 6.0.6
		OS 7.0.1 /OS 7.1.0 (VM)
		OS 8.0.1 (VM)
		OS 8.0.7 (VM)
SRX Series	<ul style="list-style-type: none"> • SRX 220 • SRX 650 	Junos OS 12.3X48-D30.7
		Junos OS 12.3X48-D70.3
*ScreenOS	<ul style="list-style-type: none"> • SSG550 • SSG20 • ISG-1000 	ScreenOS 6.3.0R21
EX Series	<ul style="list-style-type: none"> • EX 4200 	Junos OS 12.3R10.2*
		Unsupported in latest Junos versions.

Admission/Identity Control

Table 13 lists the IDP devices that are supported.

Table 13: IDP Devices in Admission Control Deployments

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

Behavioral Analytics

Table 13 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 14 lists the IF-MAP clients that are supported.

Table 14: IF-MAP clients

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

Policy Enforcement Using SNMP

Table 15: Switch List lists the switches which are qualified for Policy Enforcement using SNMP.

Table 15: Switch List

Platform	Hardware Models	Software Version	Qualified
Cisco	• 2960 Series	• 15.0.(2)EX5	X
	• 3750 Series	• 12.2(55)ES8	
	• 3850 Series	• IOS-XE 03.07.00E	
HP	• 2920 Series	• WB.15.12.0015	X

Profiling using Network Infrastructure Device collector

Table 16: lists the devices which are qualified for device profiling using Network Infrastructure Device Collector.

Table 16: Device List

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

Agentless Host Checker with Profiler

Table 16 lists supported Windows platforms and Security Products for Agentless Host checking with Profiler.

Note: Applicable with ESAP version 3.3.3 and greater.

Table 16: Agentless Host Checker with Profiler

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

