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
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**

<table>
<thead>
<tr>
<th>Revision</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2019</td>
<td>Added juniper switch model as qualified for Policy Enforcement using SNMP (ACL based).</td>
</tr>
<tr>
<td>April 2019</td>
<td>PPS Release Notes 9.1R1 updates.</td>
</tr>
</tbody>
</table>
## 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**

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

<table>
<thead>
<tr>
<th>Platform</th>
<th>Environment</th>
<th>Qualified</th>
<th>Compatible</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Cisco 2500 WLC [version 8.0.140.0]</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· AIR-CAP702I [version is 15.2(4)J86]</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Cisco catalyst 3850 [Cisco IOS Software, IOS-XE Software, Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Version 03.07.00E]</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· AIR-CAP702I (version is 15.3(3)JNB)</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Cisco 5500 Series WLC</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Cisco 7500 Series WLC</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Cisco 8500 Series WLC</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td><strong>Aruba</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Aruba 650 WLC [Aruba OS 6.1.3.6], AP-105 [ArubaOS Version 6.1.3.6]</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Aruba 3400 WLC [Aruba OS 6.4.4.6], AP-205 [ArubaOS Version 6.4.2.4]</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Aruba Instant Access Point 205 AP-205 [6.4.2.3-4.1.1.3]</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Aruba 600 Series WLC</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Aruba 3200 Series WLC</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Aruba 3600 Series WLC</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Aruba Instant Access Point 200 Series</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td><strong>Ruckus</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Zone Director 1200 Series WLC [9.9.0.0.216]</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>· Virtual SmartZone – High Scale [3.2.0.0.790]</td>
<td>Q</td>
<td></td>
</tr>
</tbody>
</table>
### Third-Party 802.1X Supplicants

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

#### Table 4: Third-Party 802.1X Supplicants

<table>
<thead>
<tr>
<th>Platform</th>
<th>Environment</th>
<th>Qualified</th>
<th>Compatible</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows 10, Redstone 5, 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 10, Redstone 4, 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 8.1 Enterprise, 64-bit</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 7 SP1 Enterprise, 64-bit</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 10, Redstone 3 (1709)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise, 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 10, Redstone 2 (1703)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise, 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 10, Redstone 1 (1607)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise, 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 8 basic edition /</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Professional / Enterprise,32-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>or 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 7 Ultimate /</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Professional / Home Basic /</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Home Premium, 32-bit or 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 7 SP1 Enterprise, 32-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Vista Ultimate /</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Business / Home-Basic / Home-</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Premium with SP 2, 32-bit or 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mac</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mac OS X 10.14, 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mac OS X 10.13, 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mac OS X 10.12, 64-bit</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mac OS X 10.11, 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mac OS X 10.10, 32-bit/64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mac OS X 10.9, 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mac OS X 10.8, 64-bit</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Mac OS X 10.7.3, 32-bit, and 64-bit</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Google Android</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platform</td>
<td>Version</td>
<td>Status</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>------------------</td>
<td>--------</td>
<td></td>
</tr>
<tr>
<td>Android</td>
<td>8.1, 8.0</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>7.0</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6.0</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Apple iOS</td>
<td>iOS 12.1, 11.2.6</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>iOS 10, 9.0, 8.0</td>
<td>C</td>
<td></td>
</tr>
</tbody>
</table>
Agentless Access (Browsers)

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

### Table 5: Agentless Access (Browsers)

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browsers/Java</th>
<th>Qualified</th>
<th>Compatible</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Windows</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows 10, Redstone 5, 64-bit</td>
<td>Firefox 60 ESR</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>• Windows 10, Redstone 4, 64-bit</td>
<td>Google Chrome</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>• Windows 8.1 Enterprise, 64-bit</td>
<td>Oracle JRE 8</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>• Windows 7 SP1 Enterprise, 64-bit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows 10, Redstone 3 (1709) Enterprise, 64-bit</td>
<td>Internet Explorer 11/Edge Browser</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>• Windows 10, Redstone 2 (1703) Enterprise, 64-bit</td>
<td>Firefox 60 ESR</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Google Chrome</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oracle JRE 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows 10, Redstone 1 (1607) Enterprise, 64-bit</td>
<td>Internet Explorer 11/Edge Browser</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firefox 60 ESR</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Google Chrome</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oracle JRE 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows 8.1 Professional, 64-bit</td>
<td>Internet Explorer 11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows 8 basic edition / Enterprise / Professional, 32-bit or 64-bit</td>
<td>Internet Explorer 10</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows 7 Ultimate / Professional / Home Basic / Home Premium, 32-bit, or 64-bit platforms</td>
<td>Internet Explorer 9.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows 7 SP1 Enterprise, 32-bit or 64-bit</td>
<td>Internet Explorer 8.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Windows Vista Ultimate / Business / Home-Basic / Home-Premium with SP 2, 32-bit, or 64-bit platforms</td>
<td>Internet Explorer 7.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Firefox 3.0 and later</td>
<td>Google Chrome</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>• Oracle JRE 6 and later</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mac</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mac OS X 10.14, 64-bit</td>
<td>Safari 11.1.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mac OS X 10.13, 64-bit</td>
<td>Safari 11.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mac OS X 10.12, 64-bit</td>
<td>Safari 10.0</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td>Browsers/Java</td>
<td>Qualified</td>
<td>Compatible</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------</td>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td>• Mac OS X 10.11, 64-bit</td>
<td>Safari 11.1.1</td>
<td>Q</td>
<td>C</td>
</tr>
<tr>
<td>• Mac OS X 10.10, 64-bit</td>
<td>Safari 9.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mac OS X 10.9, 32-bit /64-bit</td>
<td>Safari 8.0 Sun JRE 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mac OS X 10.8, 64-bit</td>
<td>Safari 7.0 Sun JRE 7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Mac OS X 10.7,4, 32-bit or 64-bit</td>
<td>Google Chrome</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Linux**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browsers/Java</th>
<th>Qualified</th>
<th>Compatible</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ubuntu 18.04</td>
<td>Firefox 52 ESR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Ubuntu 14.x</td>
<td>Oracle JRE 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• openSUSE 12.1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browsers/Java</th>
<th>Qualified</th>
<th>Compatible</th>
</tr>
</thead>
<tbody>
<tr>
<td>• openSUSE 10.x and 11.x</td>
<td>Firefox 3.0 and later</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Ubuntu 9.10, 10.x, and 11.x</td>
<td>Google Chrome</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Red Hat Enterprise Linux 5</td>
<td>Oracle JRE 6 and later</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Solaris**

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browsers/Java</th>
<th>Qualified</th>
<th>Compatible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solaris 10, 32-bit</td>
<td>Firefox 24 ESR</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solaris 10, 32-bit</td>
<td>Mozilla 2.0 and later</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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**

<table>
<thead>
<tr>
<th>Device/Operating System</th>
<th>Browsers/Java</th>
<th>Qualified</th>
<th>Compatible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple 12.1.1</td>
<td>Safari</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Apple iOS 11.4.1</td>
<td>Safari</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>Apple iOS 12</td>
<td>Safari</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>Apple iOS 11.2.6</td>
<td>Safari</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>Apple iOS 8.0</td>
<td>Safari</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>Apple iOS 7.0 and later</td>
<td>Safari</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>Google Android</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Android 8.0</td>
<td>Android native browser</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Android 7.0</td>
<td></td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>Android smart phones with</td>
<td>Android native browser</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>Android 4.4 and later</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Agentless Access (Java-Based)

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

Table 7: Agentless Access (Java-Based)

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

Host Checker

Table 8 lists the HC support on different platforms

Table 8: Host Checker

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Browsers</th>
<th>Qualified</th>
<th>Compatible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows-10 Redstone 5 OS Build 1809 Version 10.0.17763.134, 64 bit</td>
<td>Google Chrome 74, Firefox ESR 60, Oracle JRE 8 Internet Explorer 11, Edge</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Windows-10 Redstone 4 OS Build 1803 Version 10.0.17134, 64-bit</td>
<td>Google Chrome 74, Firefox 60 ESR, Oracle JRE 8 update 144</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>Windows 10 Enterprise/Pro/Home</td>
<td>Internet Explorer 11, Edge Google Chrome 74 Firefox 60 ESR, Oracle JRE 8</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>Windows 8.1 Update/ Professional / Enterprise, 64-bit</td>
<td>Internet Explorer 11, Google Chrome 74 and Firefox 60 ESR, Oracle JRE 8</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Windows 8.1 Update/ Professional / Enterprise, 32-bit</td>
<td>Internet Explorer 11, Google Chrome 74 and Firefox 60 ESR, Oracle JRE 8</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>Windows 8 Basic edition / Professional/ Enterprise, 32-bit &amp; 64-bit</td>
<td>Internet Explorer 10, Google Chrome 74 and Firefox 60 ESR, Oracle JRE 7 and later</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>Supported Platform</td>
<td>Browser Compatibility</td>
<td>Version</td>
<td></td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Windows 7 Enterprise SP1, 64-bit</td>
<td>Internet Explorer 11, Google Chrome 74 and Firefox 60 ESR, Oracle JRE 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 7 Ultimate / Professional / Home Basic / Home, 32-bit or 64-bit Windows 7 Enterprise (32-bit)</td>
<td>Internet Explorer 11, Google Chrome 74 Firefox 60 ESR, Oracle JRE 7 and later</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mac OSX</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mac OS Mojave Version 10.14</td>
<td>Safari 12.1, Google Chrome 73</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Mac OS High Sierra Version 10.13</td>
<td>Safari 11.0, Google Chrome 73</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Mac OS X 10.12</td>
<td>Safari 10.1, Safari 9.0, Google Chrome 73</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Mac OS X 10.10, 10.11</td>
<td>Safari 10.1, Safari 8.0, Google Chrome</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Mac OS X 10.9</td>
<td>Safari 9.1.3, Safari 9.0, Safari 7.0, Google Chrome 61</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Mac OS X 10.8</td>
<td>Safari 6.2.8, Safari 6.0, Google Chrome 61</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td><strong>Linux</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>openSUSE 12.1</td>
<td>Firefox 38 ESR Firefox 52 ESR, 32-bit</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>openSUSE 11.x, 10.x</td>
<td>Oracle JRE 8</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Ubuntu 16.04 LTS</td>
<td>Firefox 52, ESR, 64-bit</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Ubuntu 15.04</td>
<td>Firefox 52, ESR, 64-bit</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Ubuntu 14.04 LTS</td>
<td>Firefox 52, ESR, 64-bit</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Ubuntu 12.04 LTS, 11.x, 10.x, 9.10</td>
<td>Oracle JRE 7 and later</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>RHEL 5,7</td>
<td>Firefox 52 ESR, 32-bit, 64-bit</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Fedora 23 (32 bit, 64 bit)</td>
<td>Firefox 52 ESR 32-bit, 64-bit</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>CentOS 6.4</td>
<td>Firefox 52, 32-bit, 64-bit</td>
<td>C</td>
<td></td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Operating System/Feature</th>
<th>VPN</th>
<th>Certificate</th>
<th>Wifi</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS 11.4.1</td>
<td>Q</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>iOS 12.1</td>
<td>Q</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>*Android 8.0</td>
<td>Q</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>*Android 7.0</td>
<td>Q</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Windows 8.1 Desktop</td>
<td>Q</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 7</td>
<td></td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Mac OS X 10.13</td>
<td></td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Mac OS X 10.12, Safari 9.x</td>
<td>Q</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*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

<table>
<thead>
<tr>
<th>Third-Party AAA Server</th>
<th>Qualified</th>
<th>Compatible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Directory</td>
<td>• Windows 2016</td>
<td>• Windows 2012 R2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Windows 2008 R2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Windows 2003</td>
</tr>
<tr>
<td>LDAP using Active Directory</td>
<td>• Windows 2016</td>
<td>• Windows 2008 R2</td>
</tr>
<tr>
<td></td>
<td>• Windows 2012 R2</td>
<td>• Windows 2003</td>
</tr>
<tr>
<td>Third-Party AAA Server</td>
<td>Qualified</td>
<td>Compatible</td>
</tr>
<tr>
<td>-----------------------------------------------------</td>
<td>-----------------------------------</td>
<td>-------------------------------------------------</td>
</tr>
<tr>
<td>LDAP using Sun ONE iPlanet Server</td>
<td>Sun ONE Directory Server 5.2</td>
<td></td>
</tr>
<tr>
<td>LDAP with Greatbay Endpoint Profiler</td>
<td>Beacon 4.2.0.42</td>
<td></td>
</tr>
<tr>
<td>LDAP (other standards-compliant servers)</td>
<td>OpenLDAP 2.3.27</td>
<td>Authentication and authorization based on user attributes or group membership</td>
</tr>
<tr>
<td>RADIUS</td>
<td>Steel-Belted Radius (SBR) 6.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RSA Authentication Manager 6.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defender 5.2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Windows IAS 2008</td>
<td></td>
</tr>
<tr>
<td>RADIUS (other standards compliant servers)</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>ACE</td>
<td>RSA Authentication Manager 7.1 SP4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RSA Authentication Manager 6.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RSA Authentication Manager 5.2</td>
<td></td>
</tr>
<tr>
<td>Siteminder</td>
<td>CA Siteminder 12.0 SP3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA Siteminder 6.0 SP4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CA Siteminder 5.5</td>
<td></td>
</tr>
<tr>
<td>Certificate</td>
<td>Windows Server 2008 R2 Certificate Services</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RSA Keon Certificate Manager 6.5.1</td>
<td></td>
</tr>
<tr>
<td>Certificate (other standards-compliant servers)</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>SQL</td>
<td>Oracle 11g Express Edition</td>
<td></td>
</tr>
<tr>
<td>*SAML 2.0,1.1</td>
<td>Okta, Ping One, ADFS, PCS</td>
<td></td>
</tr>
<tr>
<td>*SAML 2.0,1.1</td>
<td>Ping Federate</td>
<td></td>
</tr>
</tbody>
</table>

*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**

<table>
<thead>
<tr>
<th>Solution</th>
<th>Qualified</th>
<th>Compatible</th>
</tr>
</thead>
<tbody>
<tr>
<td>AirWatch</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud service</td>
<td>19.03.0.6</td>
<td>18.10.0.4</td>
</tr>
<tr>
<td>Appliance OS</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Virtual appliance OS</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>MobileIron</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud service</td>
<td>10.1.0.2</td>
<td>9.7.0.2 Build 10</td>
</tr>
<tr>
<td>Appliance OS</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Virtual appliance OS</td>
<td>C</td>
<td></td>
</tr>
<tr>
<td>Microsoft Intune</td>
<td>(with AD user names only)</td>
<td></td>
</tr>
</tbody>
</table>
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

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

802.1X (other standards-compliant Ethernet switches)
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

<table>
<thead>
<tr>
<th>Platform</th>
<th>Hardware Models</th>
<th>Software Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checkpoint Firewall</td>
<td>Virtual Appliance</td>
<td>R80.20</td>
</tr>
<tr>
<td></td>
<td></td>
<td>R80.10</td>
</tr>
<tr>
<td>Palo Alto Network</td>
<td>Virtual Appliance</td>
<td>9.0.0</td>
</tr>
<tr>
<td>SRX Series</td>
<td>• SRX 220</td>
<td>Junos OS 12.3X48-D30.7</td>
</tr>
<tr>
<td></td>
<td>• SRX 650</td>
<td>Junos OS 12.3X48-D70.3</td>
</tr>
<tr>
<td>*ScreenOS</td>
<td>• SSG550</td>
<td>ScreenOS 6.3.0R21</td>
</tr>
<tr>
<td></td>
<td>• SSG20</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ISG-1000</td>
<td></td>
</tr>
<tr>
<td>EX Series</td>
<td>• EX 4200</td>
<td>Junos OS 12.3R10.2*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unsupported in latest Junos versions.</td>
</tr>
</tbody>
</table>
Admission/Identity Control

Table 14 lists the IDP devices that are supported.

Table 14: IDP Devices in Admission Control Deployments

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

Behavioral Analytics

Table 1415 lists the switch models that are supported.

Table 1415: Switch Models in Behavioral Analytics

<table>
<thead>
<tr>
<th>Hardware Models</th>
<th>Software Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco 3850</td>
<td>03.06.08E</td>
</tr>
<tr>
<td>Cisco 2960</td>
<td>15.2(6)E1</td>
</tr>
</tbody>
</table>
IF-MAP Compatibility

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

Table 16: IF-MAP clients

<table>
<thead>
<tr>
<th>IF-MAP Client</th>
<th>Qualified</th>
<th>Compatible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pulse Connect Secure</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Pulse Policy Secure</td>
<td>Q Older than 9.0R3</td>
<td></td>
</tr>
</tbody>
</table>

Policy Enforcement Using SNMP

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

Table 17: Switch List

<table>
<thead>
<tr>
<th>Platform</th>
<th>Hardware Models</th>
<th>Software Version</th>
<th>Qualified</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN Based</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco</td>
<td>• 2960 Series</td>
<td>• 15.0.(2)EX5</td>
<td>Q</td>
</tr>
<tr>
<td></td>
<td>• 3750 Series</td>
<td>• 12.2(55)ES8</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 3850 Series</td>
<td>• IOS-XE 03.07.00E</td>
<td></td>
</tr>
<tr>
<td>HP</td>
<td>• 2920 Series</td>
<td>• WB.15.12.0015</td>
<td>Q</td>
</tr>
<tr>
<td>ACL Based</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cisco</td>
<td>• 2960 Series</td>
<td>• 15.0.(2)EX5</td>
<td>Q</td>
</tr>
<tr>
<td></td>
<td>• 3750 Series</td>
<td>• 12.2(55)ES8</td>
<td></td>
</tr>
<tr>
<td>HP</td>
<td>• 2920 Series</td>
<td>• WB.15.12.0015</td>
<td>Q</td>
</tr>
<tr>
<td>Juniper</td>
<td>• EX4200</td>
<td>• 15.1R4.6</td>
<td>Q</td>
</tr>
</tbody>
</table>
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**

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

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Security Products (Antivirus / Firewall / Antispyware)</th>
<th>Qualified</th>
<th>Compatible</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows 7/64-bit</td>
<td>Symantec Endpoint Protection 14.x</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td></td>
<td>McAfee Total Protection 16.x</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td>Windows 8/64-bit</td>
<td>McAfee Total Protection 16.x</td>
<td>Q</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Symantec Endpoint Protection 14.x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 10/64-bit</td>
<td>McAfee Total Protection 16.x</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Symantec Endpoint Protection 14.x</td>
<td>Q</td>
<td></td>
</tr>
<tr>
<td>Windows 7/32-bit</td>
<td>McAfee Total Protection 16.x</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Symantec Endpoint Protection 14.x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 8/32-bit</td>
<td>McAfee Total Protection 16.x</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>McAfee Total Protection 16.x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Windows 10/32-bit</td>
<td>McAfee Total Protection 16.x</td>
<td></td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Symantec Endpoint Protection 14.x</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>