



# **Pulse Connect Secure 9.1R12 Supported Platforms Guide**

**PCS 9.1R12**

**Build 14139**

---

## **Copyright Notice**

This document is provided strictly as a guide. No guarantees can be provided or expected. This document contains the confidential information and/or proprietary property of Ivanti, Inc. and its affiliates (referred to collectively as "Ivanti") and may not be disclosed or copied without prior written consent of Ivanti.

Ivanti retains the right to make changes to this document or related product specifications and descriptions, at any time, without notice. Ivanti makes no warranty for the use of this document and assumes no responsibility for any errors that can appear in the document nor does it make a commitment to update the information contained herein. For the most current product information, please visit [www.ivanti.com](http://www.ivanti.com).

Copyright © 2021, Ivanti. All rights reserved.

Protected by patents, see <https://www.ivanti.com/patents>.

---

# Table of Contents

---

<b>Revision History</b> .....	<b>4</b>
<b>Introduction</b> .....	<b>5</b>
<b>Hardware</b> .....	<b>6</b>
<b>Windows Supported Platforms</b> .....	<b>7</b>
<b>Mac OS Supported Platforms</b> .....	<b>10</b>
<b>Linux Supported Platforms</b> .....	<b>12</b>
<b>Hypervisor Supported Platforms</b> .....	<b>13</b>
<b>Pulse Secure Installer Service</b> .....	<b>14</b>
<b>Cross-Platform Features</b> .....	<b>15</b>
<b>Pulse Secure Application Launcher (PSAL) Support</b> .....	<b>16</b>
<b>Pulse Desktop Client</b> .....	<b>17</b>
<b>Pulse Secure Collaboration Client Recommendations</b> .....	<b>18</b>
<b>Pulse Secure Mobile Client</b> .....	<b>19</b>
<b>Platform Support for Device Onboarding</b> .....	<b>20</b>
<b>MDM Solutions</b> .....	<b>21</b>
<b>Platform Support for AAA</b> .....	<b>22</b>
<b>Third-Party Applications</b> .....	<b>24</b>
<b>Change History</b> .....	<b>29</b>

# Revision History

The following table lists the revision history for this document:

Date	Revision	Description
September 2021	9.1R12 Doc ver. 1.4	<ul style="list-style-type: none"> <li>Hardware: Added a line on "For more information".</li> <li>Added a new table "Hypervisor Supported Platforms".</li> <li>Deleted a few rows from the "Third-Party Applications" table.</li> </ul>
June 2021	9.1R11.5 Doc ver. 1.2	Removed support for FireFox on macOS.
February 2021	9.1R11 Doc ver. 1.0	Updated supported platforms for JSAM
February 2021	9.1R11 Doc ver. 1.0	Initial Publication
December 2020	9.1R10 Doc ver. 1.0	Initial Publication
October 2020	9.1R9 Doc ver. 1.0.1	Updated the MDM Solutions section.
October 2020	9.1R9 Doc ver. 1.0	Initial Publication
September 2020	9.1R8.2 Doc ver. 1.0	Initial Publication
July 2020	9.1R8, Doc ver. 1.0	Initial Publication
May 2020	9.1R6, Doc ver. 1.0	Initial Publication
April 2020	9.1R5, Doc ver. 1.0	Initial Publication
January 2020	9.1R4, Doc ver. 1.1	EOL of NC and WSAM
January 2020	9.1R4, Doc ver. 1.0	Initial Publication
October 2019	9.1R3, Doc ver. 1.0	Initial Publication
July 2019	9.1R2, Doc ver. 1.0	Initial Publication

# 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 9.1 software on the following platforms.

- PSA300
- PSA3000
- PSA5000
- PSA7000f
- PSA7000c
- Virtual Appliances (PSA-V) on ESXi, Hyper-V, Microsoft Azure, Amazon AWS, OpenStack KVM and Alibaba Cloud.

For more information, refer to ["Hypervisor Supported Platforms" on page 13](#).

# Windows Supported Platforms

The following table lists the **Supported Windows Platforms vs PCS features**:

Windows Platform		Admin UI	BYOD	Cross Platform Features	Advanced HTML5	Host Checker	PSAL	PSIS	Terminal Services	JSAM
<b>Windows 10 Version 21H1</b> <b>(OS build 10.0.19043.1110)</b>  <b>Professional, 64-bit</b>	Internet Explorer 11,  Edge 91.0.864.71,  Google Chrome 91.0.4472.164,  Firefox ESR 78.12,  Oracle JRE 8 update 291	Q	Q	Q	Q	Q	Q	Q	Q	Q
<b>Windows 10 Version 20H2</b> <b>(OS build 10.0.19042.572)</b>	Internet Explorer 11,  Edge 86,  Google Chrome 83,	C	C	C	Q	C	C	C	C	C

Windows Platform		Admin UI	BYOD	Cross Platform Features	Advanced HTML5	Host Checker	PSAL	PSIS	Terminal Services	JSAM
<b>Professional, 64-bit</b>	Firefox ESR 68, Oracle JRE 8, 9 and 10 update 251									
<b>Windows 10 Version 2004 (OS Build 10.0.19041.329) Enterprise, 32-bit and 64-bit</b>	Internet Explorer 11, Edge 83, Google Chrome 83, Firefox ESR 68, Oracle JRE 8, 9 and 10 update 251	Q	Q	Q	Q	Q	Q	Q	Q	Q
<b>Windows 10 Version 2004 (OS Build 10.0.19041.264)</b>	Internet Explorer 11, Edge 83, Google Chrome 83,	C	C	C	-	C	C	C	C	C



Windows Platform		Admin UI	BYOD	Cross Platform Features	Advanced HTML5	Host Checker	PSAL	PSIS	Terminal Services	JSAM
<b>Enterprise, 32-bit and 64-bit</b>	Firefox ESR 68, Oracle JRE 8, 9 and 10 update 144									
<b>Windows 10 Redstone 6 Version 1903 (OS Build 10.0.18362.338) 64-bit</b>	Internet Explorer 11, Edge, Google Chrome 61, Firefox ESR 60, Oracle JRE 8, 9 and 10 update 144	Q	Q	Q	-	C	Q	Q	Q	Q



From 9.1R2 release onwards, Network Connect (NC) client and legacy Windows Secure Application Manager (WSAM) client are not supported.

# Mac OS Supported Platforms

The following table lists the **supported Mac OS platforms vs PCS features**:

Mac Platform		Admin UI	BYOD	AdvancedHTML5	Cross Platform Features	Host Checker	PSAL	PSIS	Terminal Services	JSAM
<b>Mac OS Big Sur Version 11.4</b>	Safari 14.0, Chrome 86, Java 8 update 291	Q	Q	Q	Q	Q	Q	-	-	Q
<b>Mac OS Big Sur Version 11.0.1 (20B29)</b>	Safari 14.0 Chrome 86	C	C	C	C	C	C	-	-	C
<b>Mac OS Catalina Version 10.15.5 64-bit</b>	Safari 13.0, Chrome 83, Oracle JRE, JDK 8, 9 and 10	Q	Q	Q	Q	Q	Q	-	-	Q

Mac Platform		Admin UI	BYOD	AdvancedHTML5	Cross Platform Features	Host Checker	PSAL	PSIS	Terminal Services	JSAM
<b>Mac OS Catalina Version 10.15.3 64-bit</b>	Safari 12.0, Chrome 73, Oracle JRE, JDK 8, 9 and 10	C	C	-	C	Q	C	-	-	Q

**i** Pulse Secure Application Launcher supports Pulse Client and Host Checker.

**i** Network Connect Support EOL from 8.3R1 onwards on MAC platforms.

# Linux Supported Platforms

The following table lists the **supported Linux platforms vs PCS features**:

Linux Platform		Admin UI	BYOD	Cross Platform Features	Host Checker	PSAL	PSIS	Terminal Services	JSAM
<b>Ubuntu 20.04 LTS</b>	Firefox ESR 78.12, 64-bit	Q	Q	Q	Q	Q	Q	Q	Q
<b>Ubuntu 16.04 LTS</b>	Firefox ESR 78.7.1, 64-bit	C	-	C	C	C	-	-	C
<b>Ubuntu 18.04 LTS</b>	Firefox ESR 78.7.1, 64-bit	C	-	C	C	C	-	-	C

# Hypervisor Supported Platforms

The following **Hypervisor Supported Platforms** table lists supported third-party applications:

Application	Support Summary	Qualified	Compatible
<b>Virtual SA</b>			
ESXi 7.0	PSA-V	Q	
ESXi 6.7 Update 2c	PSA-V	Q	
ESXi 6.5	PSA-V		C
ESXi 6.0	PSA-V		C
ESXi 5.5, 5.5 U3	PSA-V		C
<b>OpenStack KVM</b>			
Controller: CentOS 7.6 QEMU version: 2.12.0	PSA-V	Q	
Compute: Ubuntu 8.04.2 LTS QEMU version: 3.1.0	PSA-V	Q	
<b>Hyper-V</b>			
Microsoft Hyper-V Server 2016 and 2019		Q	
Microsoft Hyper-V Server 2012 R2			C



The table specifies the qualified or compatible versions for the Hypervisors. Customers can deploy PCS on other versions at their own discretion.

# Pulse Secure Installer Service

Pulse Secure Installer Service is supported for the following client applications:

- Host Checker
- Pulse Collaboration
- Terminal Services

# Cross-Platform Features

The Pulse Connect Secure supports the following features on multiple platforms:

- File Browsing
- HTML5 RDP
- Java Secure Application Manager (JSAM)
- Premier Java Applet
- Pulse Collaboration
- Secure Terminal Access
- Web Browsing

# Pulse Secure Application Launcher (PSAL) Support

Pulse Connect Secure 8.2R1 introduced a new mechanism, "Pulse Secure Application Launcher" (PSAL), for launching and installing Pulse Secure clients from a web browser which have deprecated Java Plugin, ActiveX technologies and have restrictions on Java.

- Supported on Mozilla Firefox, Google Chrome & Edge Browser on Windows Platform.
- Supported on Safari 12 and Chrome 61 on Mac OS High Sierra 10.13 and Mac OS Mojave 10.14

Details are listed in Windows Supported Platforms.

Pulse Application Launcher supports delivery & installation of following Components:

- Pulse Desktop Client
- Host Checker
- Pulse Collaboration
- Terminal Services
- Terminal Services – Premiere JAVA Applet (HOB Applet)
- Java Secure Application Manager



# Pulse Desktop Client

See the Pulse Secure Desktop Client Supported Platforms Guide.

# Pulse Secure Collaboration Client Recommendations

The following table lists the **Recommended Minimum Platform Requirements for Pulse Secure Collaboration Client**:

Component	Requirements
<b>CPU</b>	1 GHz or more for Windows Client. 1 GHz G4 or Intel processor for a Mac.
<b>Memory</b>	256 MB of available RAM or more.
<b>Color Quality</b>	For best results, use 16 bits. 8 bits, 16 bits, 24 bits, and 32 bits are also supported.
<b>Monitor Resolution</b>	1024 x 768 pixels. Up to 2048 x 2048 pixels is supported.



Pulse Secure Collaboration Client is not supported on a Mac PowerPC. It is supported only on Intel-based Mac machines.



Pulse Collaboration sharing features are not supported on Ubuntu 12.04, Linux openSUSE 11.x, 10.x, and Linux openSUSE 12.1.

# Pulse Secure Mobile Client

The following table lists the **Supported Mobile Platforms for the Pulse Secure Mobile Client**:

Mobile Platforms	Active Sync	Host Checker	HTML5 RDP	VPN	Pulse Collaboration
<b>Android</b> 8.1, 9.0, 10.0, 11.0	C	C	C	C	-
<b>IOS</b> 11.x, 12.x, 13.x, 14.x	C	C	C	C	C
<b>IOS</b> iOS 10.2.1, 9.3.5	Q	Q	Q	Q	Q

# Platform Support for Device Onboarding

The following **Device Onboarding Features** table lists Device onboarding features that are qualified with this release:

Operating System/Feature	VPN	Certificate	WiFi	Secure Email
IOS 14.x, 13.x, 12.x, 11.x, 10.x, 9.x	Q	Q	Q	Q
Android 11.x, 10.x, 9.x, 8.x	Q	Q	Q	-
Windows 10	-	Q	Q	-
Windows 8.1	-	Q	Q	-
Mac OS X 10.12, Safari 9.0 & Safari 10.0	-	Q	Q	-
Mac OS X 10.10.5, Safari 8.0.8	-	Q	Q	-
Mac OS X 10.9.5 Safari 7.0.x	-	Q	Q	-
Mac OS Big Sur Version 11.0.1 (20B29)	-	Q	Q	-
Mac OS Catalina Version 10.15.5 64-bit	-	Q	Q	-

# MDM Solutions

The following **MDM Vendors** table lists the requirements for integration with mobile device management (MDM) vendors:

Solution	Qualified	Compatible
<b>AirWatch</b>		
Cloud service	19.11.1.5	19.03.0.6
Appliance OS		C
Virtual appliance OS	Q	
<b>MobileIron</b>		
Cloud service	10.5.0.0.107R	10.1.0.2
Appliance OS		C
Virtual appliance OS	Q	
<b>Microsoft Intune</b>		
Cloud service	Release version 2106	
<b>Pulse Workspace</b>		
Cloud service	1.8.0-1628	

# Platform Support for AAA

The following **Third-Party AAA Servers** table lists supported third-party AAA servers:

Third-Party AAA Server	Qualified	Compatible
Active Directory*	Windows Server 2019 Windows Server 2016 Windows Server 2012 R2**	Windows Server 2008 R2 Windows Server 2003
LDAP using Microsoft Active Directory	Windows Server 2019 Windows Server 2016 Windows Server 2012 R2	Windows Server 2008 R2 Windows Server 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 (other standards-compliant servers)	OpenLDAP 2.3.27	C Authentication and authorization based on user attributes or group membership.
RADIUS	Steel-Belted RADIUS (SBR) 6.1 Defender 5.2 RSA Authentication Manager 8.4.0.3.0	Azure MFA Radius Windows IAS 2008 RSA Authentication Manager 8.3
RADIUS IPv6 Support	Steel-Belted RADIUS (SBR) 6.1	Windows NPS 2012 R2 Free-RADIUS 2.1
RADIUS (other standards-compliant servers)		C
ACE	RSA Authentication Manager 8.4.0.3.0	RSA Authentication Manager 8.3

Third-Party AAA Server	Qualified	Compatible
		RSA Authentication Manager 8.2 RSA Authentication Manager 8.1 RSA Authentication Manager 8.0 SP4
Siteminder	CA Siteminder 12.7 CA Siteminder 12.52 SP1 CA Siteminder 12.0 SP3	CA Siteminder 5.5 CA Siteminder 6.0 SP4
Certificate	Windows Server 2019 Windows Server 2016 Windows Server 2012 R2	Windows Server 2008R2 RSA Keon Certificate Manager 6.5.1
Certificate (other standards-compliant servers)		C
SAML*** 2.0, 1.1	PingFederate 6.4.1.1	Azure AD Microsoft ADFS 2.0 (Server 2008 R2) Oracle Identity Federation 11.1.1.2.0
SAML 2.0, 1.1 (other standards-compliant servers)		C
<p>*Additional requirements and limitations apply. See Active Directory section in the PCS Administration Guide.</p> <p>** Applicable only for New AD mode Auth server.</p> <p>***For information on the SAML SSO profiles, bindings, and protocols that we support, see Supported SAML SSO Profiles section in the PCS Administration Guide.</p>		

# Third-Party Applications

The following **Third-Party Applications** table lists supported third-party applications:

Application	Support Summary	Qualified	Compatible
<b>Outlook Web Access (OWA)</b>			
OWA 2019	Web Profiles (Rewriter, Passthrough Proxy)	Q	
OWA 2016	Web Profiles (Rewriter, Passthrough Proxy)	Q	
OWA 2013 SP1	Web Profiles (Rewriter, Passthrough Proxy)	Q	
OWA 2010 SP2, SP1	Web Profiles (Rewriter, Passthrough Proxy)		C
OWA 2007	Web Profiles (Rewriter, Passthrough Proxy)		C
<b>SharePoint</b>			
SharePoint 2019 (Classic UI only)	Web Profiles (Rewriter, Passthrough Proxy)	Q	
SharePoint 2016	Web Profiles (Rewriter, Passthrough Proxy)		C
SharePoint 2013 SP1	Web Profiles (Rewriter, Passthrough Proxy)		C
SharePoint 2010, 2007	Web Profiles (Rewriter, Passthrough Proxy)		C
<b>IBM Domino</b>			
Lotus iNotes 9.0	Web Profiles (Rewriter, Passthrough Proxy)	Q	
Lotus iNotes 8.5.3	Web Profiles (Rewriter, Passthrough Proxy)		C
Lotus Connect 3.0, 2.5	Rewriter		C
<b>Citrix</b>			



Application	Support Summary	Qualified	Compatible
Citrix Virtual Apps and Desktops 7 1912 LTSR	HTML5 Access and CTS	Q	
Citrix Virtual Apps and Desktops 7 below 1912	HTML5 Access and CTS		C
Citrix StoreFront 1912 LTSR	HTML5 Access and CTS	Q	
Citrix StoreFront versions 3.16 and below	HTML5 Access and CTS		C
Citrix StoreFront with HTML5 Access	Custom Web Profile		C
Citrix Listed Applications with Server 6.5 SP1, 6.0, 7.6, 7.8	Citrix Terminal Services		C
Citrix Workspace version 2002	Web, Terminal Services and SAM Profile	Q	
Citrix Receiver versions below 4.11	Web, Terminal Services and SAM Profile		C
Citrix Virtual Apps and Desktops 7 1912 LTSR	Citrix Terminal Services	Q	

Application	Support Summary	Qualified	Compatible
Citrix XenApp and XenDesktop 7.18 and below	Citrix Terminal Services		C
Citrix Virtual Apps and Desktops 7 1912 LTSR	VDI Profiles	Q	
Citrix XenDesktop 7.15 and below	VDI Profiles		C
Citrix Web Interface 5.4 Web Profiles	Rewriter, JSAM, and WSAM	Q	
<b>VMWare</b>			
VMWare Horizon View Connection Server version 8.0, 8.1	Rewriter	Q	
VMWare Horizon View Connection Server version 7.12	Rewriter	Q	
VMWare Horizon View Connection Server version 7.12	Rewriter	Q	

Application	Support Summary	Qualified	Compatible
VMWare Horizon View Connection Server versions below 7.12	Rewriter		C
VMWare Horizon Agent version 8.0, 8.1	VDI Profiles	Q	
VMWare Horizon Agent version 7.12	VDI Profiles	Q	
VMWare Horizon Agent versions below 7.12	VDI Profiles		C
VMWare Horizon View HTML Access version 5.4	VDI Profiles	Q	
VMWare Horizon View HTML Access versions below 5.4	VDI Profiles		C
VMWare Horizon View Client version 8.0	VDI Profiles	Q	
VMWare Horizon View Client version 5.4	VDI Profiles	Q	

Application	Support Summary	Qualified	Compatible
VMWare Horizon View Client versions below 5.4	VDI Profiles		C
VMWare View Server version 4.6, 5.0, 5.1, 2.3.x	VDI Profiles		C
<b>Exchange ActiveSync</b>			
Office 365	Secure Mail Resource Profile	Q	
Exchange 2016	Secure Mail Resource Profile	Q	
Exchange 2013, 2010 SP1, and 2007	Secure Mail Resource Profile		C
<b>ESAP Package</b>			
ESAP 3.4.8 (default version)	Host Checker	Q	
ESAP 3.3.5 (minimum version)	Host Checker	Q	

# Change History

The following table lists changes to this document from the previous release:

Section	Add/Update	Drop or Moved	Effective Release	Notes
MacOS Supported Platforms	Updated with MacOS Big Sur 11.0 versions		9.1R10	Compatible
MDM Solutions	Updated with cloud service versions		9.1R9	Qualified
Windows Supported Platforms	Updated with Windows 10 Version 20H2		9.1R9	Compatible
Windows Supported Platforms	Updated with Windows 10 Version 2004		9.1R8	Qualified
MacOS Supported Platforms	Updated with MacOS Catalina and MacOS Mojave latest versions		9.1R8	Qualified
Windows Supported Platforms	Updated with Windows 10 Version 2004		9.1R6	
Windows Supported Platforms		Removed support for Windows 7	9.1R5	
Windows Supported Platforms	Updated Host Checker feature		9.1R5	
MacOS Supported Platforms	Updated Host Checker feature		9.1R5	
Third-Party Applications	Updated ESAP Package default version 3.4.8		9.1R5	

Section	Add/Update	Drop or Moved	Effective Release	Notes
Windows Supported Platforms	Updated with Redstone 6 OS Build 1909		9.1R4	Qualified in this release
Third-Party Applications	Updated SharePoint, VMware and Citrix sections		9.1R4	Qualified in this release
Third-Party Applications	Added support for ESXi 6.7 Update 2c		9.1R3	Qualified in this release
Platform Support for AAA	Added Windows Server 2019		9.1R3	Qualified in this release
Windows Supported Platforms	Added Windows 10 Redstone 6		9.1R2	Added Windows 10 Redstone 6 compatible
Platform Support for AAA	Added RSA AM 8.4.0.3.0 support for RADIUS and ACE servers		9.1R2	Qualified in this release
Mac OS Supported Platforms				
Pulse Secure Application Launcher (PSAL) Support	Added Chrome 61 support		9.1R1	Qualified in this release
Linux Supported Platforms	Added openSUSE Linux with Host Checker support		9.1R1	