Pulse Secure®
Acquired by Ivanti

Pulse Connect Secure: Supported Platforms Guide

PCS 9.1R11.5

Build 13127

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

Pulse Connect Secure: Supported Platforms Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

Contents

Revision History

Table 1   lists the revision history for this document.

Date	Revision	Description
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, KVM, Hyper-V, Microsoft Azure, Amazon AWS, OpenStack Fabric and Alibaba Cloud.

Client Environment Contents

You can install and use Release 9.1 software on the following platforms.

Windows Supported Platforms

Table 2   Lists supported windows platforms vs PCS features:

Windows Platform		Admin UI	BYOD	Cross Platform Features	Advanced HTML5	Host Checker	PSAL	PSIS	Terminal Services	JSAM
Windows 10 Version 20H2 (OS build 10.0.19042.572) Professional, 64 bit	Internet Explorer 11, Edge 86, Google Chrome 83, Firefox ESR 68, Oracle JRE 8, 9 and 10 update 251	C	C	C	Q	C	C	C	C	C
Windows 10, Version 2004 **OS Build 10.0.19041.329, Enterprise, 32-bit and 64-bit**	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
Windows 10, Version 2004 **OS Build 10.0.19041.264, Enterprise, 32-bit and 64-bit**	Internet Explorer 11, Edge 83, Google Chrome 83, Firefox ESR 68, Oracle JRE 8, 9 and 10 update 144	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
Windows-10 Redstone 6 OS Build 1903 Version 10.0.18362.338, 64-bit	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

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

Mac OS Supported Platforms

Table 3   lists supported Mac OS platforms vs PCS features:

Mac Platform		Admin UI	BYOD	Advanced HTML5	Cross Platform Features	Host Checker	PSAL	PSIS	Terminal Services	JSAM
Mac OS Big Sur Version 11.0.1 (20B29)	Safari 14.0 Chrome 86	C	C	C	C	C	C	-	-	C
Mac OS Catalina Version 10.15.5 64-bit	Safari 13.0, Chrome 83, Oracle JRE, JDK 8, 9 and 10	Q	Q	Q	Q	Q	Q	-	-	Q
Mac OS Catalina Version 10.15.3 64-bit	Safari 12.0, Chrome 73, Oracle JRE, JDK 8, 9 and 10	C	C	-	C	Q	C	-	-	Q

Note: Pulse Secure Application Launcher supports Pulse Client and Host Checker.

Note: Network Connect Support EOL from 8.3R1 onwards on MAC platforms.

Linux Supported Platforms

Table 4   lists supported Linux platforms vs PCS features:

Linux Platform		Admin UI	BYOD	Cross Platform Features	Host Checker	PSAL	PSIS	Terminal Services	JSAM
Ubuntu 16.04 LTS	Firefox ESR 78.7.1, 64-bit	C	-	C	C	C	-	-	C
Ubuntu 18.04 LTS	Firefox ESR 78.7.1, 64-bit	C	-	C	C	C	-	-	C

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

Table 5   lists the recommended minimum platform requirements for Pulse Secure collaboration client.

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

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

Note: 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

Table 6   lists supported mobile platforms for the Pulse Secure Mobile Client.

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

Platform Support for Device Onboarding

Table 7   Device Onboarding Features – 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 • Windows 8.1	-	Q	Q	-
• Mac OS X 10.12, Safari 9.0 & Safari 10.0 • Mac OS X 10.10.5, Safari 8.0.8 • Mac OS X 10.9.5 Safari 7.0.x	-	Q	Q	-
• Mac OS Big Sur Version 11.0.1 (20B29) • Mac OS Catalina Version 10.15.5 64-bit	-	Q	Q	-

MDM Solutions

Table 8   MDM Vendors - Lists the requirements for integration with mobile device management (MDM) vendors.

Solution	Qualified	Compatible
AirWatch		
Cloud service	19.11.1.5	19.03.0.6
Appliance OS		C
Virtual appliance OS	Q	
MobileIron		
Cloud service	10.5.0.0.107R	10.1.0.2
Appliance OS		C
Virtual appliance OS	Q	
Microsoft Intune		
Cloud service	Release version 2002	
Pulse Workspace		

Solution	Qualified	Compatible
Cloud service	1.8.0-1628	

Platform Support for AAA

Table 9   Third-Party AAA Servers - 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 • 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

Third-Party AAA Server	Qualified	Compatible
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

*Additional requirements and limitations apply. See Active Directory section in the PCS Administration Guide.

** Applicable only for New AD mode Auth server.

***For information on the SAML SSO profiles, bindings, and protocols that we support, see Supported SAML SSO Profiles section in the PCS Administration Guide.

Third-Party Applications

Table 10   Third-Party Applications - Lists supported third-party applications

Application	Support Summary	Qualified	Compatible
Outlook Web Access (OWA)			
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
SharePoint			
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
IBM Domino			
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
Citrix			
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	

Application	Support Summary	Qualified	Compatible
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	
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	Q4	
VMWare			
VMWare Horizon View Connection Server version 7.12	Rewriter	Q	
VMWare Horizon View Connection Server versions below 7.12	Rewriter		C
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 5.4	VDI Profiles	Q	
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
Exchange ActiveSync			
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

Application	Support Summary	Qualified	Compatible
ESAP Package			
ESAP 3.4.8 (default version)	Host Checker	Q	
ESAP 3.3.5 (minimum version)	Host Checker	Q	
Virtual SA			
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
KVM			
CentOS 6.6 with Kernel cst-kvm 2.6.32-504.el6.x86_64	PSA-V	Q	
Hyper-V			
Microsoft Hyper-V Server 2016 and 2019		Q	
Microsoft Hyper-V Server 2012 R2			C

Change History

Table 11   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	
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

Section	Add/Update	Drop or Moved	Effective Release	Notes
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	