



Pulse Connect Secure: Supported Platforms Guide

PCS 9.1R6

Build 5801

Published

May 2020

Document Version

1.0

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

www.pulsesecure.net

© 2020 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.

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

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 <http://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.

Date	Revision	Description
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

Contents

REVISION HISTORY	4
INTRODUCTION	6
HARDWARE	7
CLIENT ENVIRONMENT CONTENTS	8
WINDOWS SUPPORTED PLATFORMS.....	8
MAC OS SUPPORTED PLATFORMS	11
LINUX SUPPORTED PLATFORMS.....	12
PULSE SECURE INSTALLER SERVICE.....	13
CROSS-PLATFORM FEATURES.....	13
PULSE SECURE APPLICATION LAUNCHER (PSAL) SUPPORT	14
PULSE DESKTOP CLIENT	14
PULSE SECURE COLLABORATION CLIENT RECOMMENDATIONS	14
PULSE SECURE MOBILE CLIENT.....	15
PLATFORM SUPPORT FOR DEVICE ONBOARDING.....	15
MDM SOLUTIONS	16
PLATFORM SUPPORT FOR AAA	17
THIRD-PARTY APPLICATIONS.....	18
CHANGE HISTORY	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 9.1 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

- [Windows Supported Platforms](#) 8
- [Mac OS Supported Platforms](#) 10
- [Linux Supported Platforms](#) 11
- [Pulse Secure Installer Service](#) 11
- [Cross-Platform Features](#)..... 12
- [Pulse Secure Application Launcher \(PSAL\) Support](#) 12
- [Pulse Desktop Client](#) 12
- [Pulse Secure Collaboration Client Recommendations](#)..... 13
- [Pulse Secure Mobile Client](#)..... 13
- [Platform Support for Device Onboarding](#) 14
- [MDM Solutions](#)..... 14
- [Platform Support for AAA](#)..... 15
- [Third-Party Applications](#) 16

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	Host Checker	Pulse Secure Application Launcher	Pulse Secure Installer Service	Terminal Services
Windows 10, Version 2004 OS Build 10.0.19041.264, Enterprise, 32-bit and 64-bit	Internet Explorer 11, C	C	C	C	C	C	C
Windows-10 Redstone 6 OS Build 1909 Version 10.0.18363.476, 64-bit	Internet Explorer 11, Q	Q	Q	Q	Q	Q	Q
Windows-10 Redstone 6 OS Build 1903 Version 10.0.18362.338, 64-bit	Internet Explorer 11, Q	Q	Q	C	Q	Q	Q

Windows Platform	Admin UI	BYOD	Cross Platform Features	Host Checker	Pulse Secure Application Launcher	Pulse Secure Installer Service	Terminal Services
Windows-10 Redstone 5 OS Build 1809 Version 10.0.17763.134, 64-bit	Internet Explorer 11, C Edge Google Chrome 61 Firefox ESR 60, Oracle JRE 8, 9 and 10 update 144	C	C	C	C	C	C
Windows-10 Redstone 4 OS Build 1803 Version 10.0.17134, 64-bit	Internet Explorer 11, C Edge, Google Chrome 61, Firefox 52 ESR, Oracle JRE 8 update 144	C	C	C	C	C	C
Windows-10 Redstone 3 OS Build 1709, Version 10.0.16299.15, 64-bit	Internet Explorer 11, C Edge, Google Chrome 61, Firefox 52 ESR, Oracle JRE 8 update 144	C	C	C	C	C	C
Windows 10 RedStone-2 Enterprise/Pro/Home, Build 1703 Version 10.0.15063.332, 64-bit	Internet Explorer 11, C Edge, Google Chrome 58, Firefox 52 ESR, Oracle JRE 8 update 131	C	C	C	C	C	C
Windows 10 Enterprise/ Pro/Home	Internet Explorer 11, C Edge, Google Chrome, Firefox 52 ESR. Oracle JRE 8	C	C	C	C	C	C
Windows 8.1 Update/ Professional / Enterprise, 64-bit	Internet Explorer 11, Q Google Chrome, Firefox 52 ESR, Oracle JRE 8	Q	Q	Q	Q	Q	Q
Windows 8.1 Update/ Professional / Enterprise, 32-bit	Internet Explorer 11, C Google Chrome, Firefox 38 ESR, Oracle JRE 8	C	C	C	C	C	C
Windows 8 Basic edition / Professional/ Enterprise, 32-bit & 64-bit	Internet Explorer 10, C Google Chrome, Firefox 31 & later. Oracle JRE 7 and later	C	C	C	C	C	C

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:

Windows Platform		Admin UI	BYOD	CrossPlatform Features	Host Checker	Pulse Secure Application Launcher	Pulse Secure Installer Service	Terminal Services
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	-	-
Mac OS Mojave Version 10.14.5 64-bit	Safari 12.0 Chrome 73, Oracle JRE, JDK 8, 9 and 10	Q	Q	Q	Q	Q	-	-
Mac OS High Sierra Version 10.13	Safari 11.0 Chrome 73, Oracle JRE, JDK 8, 9 and 10	Q	Q	Q	C	Q	-	-
Mac OS X 10.12	Safari 10.1 Chrome 73, Safari 9.0 Oracle JRE 8	C	Q	Q	C	Q	-	-
Mac OS X 10.10, 10.11	Safari 10.1 Safari 8.0 Oracle JRE 8	C	C	C	C	C	-	-
Mac OS X 10.9	Safari 9.1.3 Safari 9.0, Safari 7.0 Oracle JRE 8	C	C	C	C	-	-	-
Mac OS X 10.8	Safari 6.2.8 Safari 6.0 Oracle JRE 8	C	C	C	C	-	-	-

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	Pulse Secure Application Launcher	Pulse Secure Installer Service	Terminal Services
openSUSE 12.1	Firefox 38 ESR,	C	-	Q	C	-	-	-
	Firefox 52 ESR, 32-bit			C				
openSUSE 11.x, 10.x	Oracle JRE 8	C	-	C	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	C	-	Q	Q	-	-	-
Ubuntu 12.04 LTS, 11.x, 10.x, 9.10	Oracle JRE 7 and later	C	-	C	C	-	-	-
RHEL 5	Firefox 52 ESR, 32-bit	C	-	C	C	-	-	-
RHEL 7	Firefox 52 ESR, 64-bit	-	-	-	C	-	-	-
Fedora 23 (32 bit)	Firefox 52 ESR 32-bit	-	-	-	C	-	-	-
Fedora 23 (64 bit)	Firefox 52 ESR 64-bit				C	-	-	-
CentOS 6.4	Firefox 52, 32- bit/64-bit	-	-	-	C	-	-	-
					C			
CentOS 7.0	Firefox 52, 64-bit	-	-	-		-	-	-

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 Android 7.0 and 6.0	Q	Q	Q	Q	-	-
Android 5.1.1, 4.4.4, 4.4.3, 4.4.2 and 4.3	C	C	C	C	-	-
iOS iOS 10.2.1, 9.3.5, 64-bit	Q	Q	Q	Q	C	-
iOS iOS 8.4.2 64-bit iOS 7.1.2 64-bit & 32-bit iOS 7.1 and 6.x 64-bit and 32-bit	C	C	Q	C	C	-
Windows Phone 8.1	Q	-	-	-	-	C

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
• OS 10.x and 11.0, 64-bit	Q	Q	Q	Q
• IOS 9.x • OS 8.3 64-bit • iOS 7.1.2 64-bit & 32-bit • iOS 7.1 and 6.x 64-bit and 32-bit	C	C	C	C
• Android 6.0.1 and 5.1.1	Q	Q	Q	-
• Android 4.4.4, 4.4.3, 4.4.2 and 4.3	C	C	C	-
• 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 X 10.8.5, Safari 7.0.x and 6.0.x	-	C	C	-

MDM Solutions

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

Solution	Qualified	Compatible
AirWatch		
Cloud service	Q 8.4.7.0	
Appliance OS		C
Virtual appliance OS	Q	
MobileIron		
Cloud service	Q Core 9.1.1.0 Build 29	
Appliance OS		C
Virtual appliance OS	Q	

Solution	Qualified	Compatible
Pulse Workspace		
Cloud service	Q 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*	<ul style="list-style-type: none"> Windows Server 2019 Windows Server 2016 Windows Server 2012 R2** 	<ul style="list-style-type: none"> Windows Server 2008 R2 Windows Server 2003
LDAP using Microsoft Active Directory	<ul style="list-style-type: none"> Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 	<ul style="list-style-type: none"> 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)	<ul style="list-style-type: none"> OpenLDAP 2.3.27 	C Authentication and authorization based on user attributes or group membership.
RADIUS	<ul style="list-style-type: none"> Steel-Belted RADIUS (SBR) 6.1 Defender 5.2 RSA Authentication Manager 8.4.0.3.0 	<ul style="list-style-type: none"> Azure MFA Radius Windows IAS 2008 RSA Authentication Manager 8.3
RADIUS IPv6 Support	Steel-Belted RADIUS (SBR) 6.1	<ul style="list-style-type: none"> Windows NPS 2012 R2 Free-RADIUS 2.1
RADIUS (other standards-compliant servers)		C
ACE	RSA Authentication Manager 8.4.0.3.0	<ul style="list-style-type: none"> RSA Authentication Manager 8.3 RSA Authentication Manager 8.2 RSA Authentication Manager 8.1 RSA Authentication Manager 8.0 SP4
Siteminder	<ul style="list-style-type: none"> CA Siteminder 12.7 CA Siteminder 12.52 SP1 CA Siteminder 12.0 SP3 	<ul style="list-style-type: none"> CA Siteminder 5.5 CA Siteminder 6.0 SP4
Certificate	<ul style="list-style-type: none"> Windows Server 2019 Windows Server 2016 Windows Server 2012 R2 	<ul style="list-style-type: none"> Windows Server 2008R2 RSA Keon Certificate Manager 6.5.1

Third-Party AAA Server	Qualified	Compatible
Certificate (other standards-compliant servers)		C
SAML*** 2.0, 1.1	<ul style="list-style-type: none"> • PingFederate 6.4.1.1 	<ul style="list-style-type: none"> • 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 1909	HTML5 Access and CTS	Q	
Citrix StoreFront 3.16	HTML5 Access and CTS		C

Application	Support Summary	Qualified	Compatible
Citrix StoreFront 3.12, 3.11 and 3.8	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 Receiver 4.9, 4.10 and 4.11	Web, Terminal Services and SAM Profiles	Q	
Citrix Receiver 4.3.100	Web, Terminal Services and SAM profiles.		C
Citrix XenApp and XenDesktop 7.18	Citrix Terminal Services	Q	
Citrix XenApp and XenDesktop 7.15, 7.14, 7.11	Citrix Terminal Services		C
Citrix XenDesktop 7.14 and 7.15	VDI Profiles	Q	
Citrix XenDesktop 7.11, 7.9, 7.8, 7.0, 5.6, 5.0	VDI Profiles		C
Citrix Web Interface 5.4	Web Profiles (Rewriter, JSAM, and WSAM)	Q	
VMWare			
VMWare Horizon View HTML Access, version 7.9, 7.10	Rewriter	Q	
VMWare Horizon View HTML Access, version 7.7, 7.6, 7.5, 7.4	Rewriter		C
VMWare Horizon Agent version 7.9, 7.10	VDI Profiles	Q	
VMWare Horizon Agent version 7.7, 7.6, 7.5, 7.4	VDI Profiles		C
VMWare Horizon View Server version 7.9, 7.10	VDI Profiles	Q	
VMWare Horizon View Server version 7.7, 7.6, 7.5, 7.4, 7.1, 7.0, 6.2, 6.1, 6.0, 5.3, 5.2	VDI Profiles		C
VMWare Horizon View Client version 4.10.0, to 4.1.0	VDI Profiles	Q	
VMWare View Server version 4.6, 5.0, 5.1, 2.3.x	VDI Profiles		C
VMWare View Client version 4.6, 5.0, 5.1, 5.2			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 <code>cst-kvm 2.6.32-504.el6.x86_64</code>	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
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
Platform Support for AAA	Added RSA AM 8.4.0.3.0 support for RADIUS and ACE servers		9.1R2	Qualified in this release
<ul style="list-style-type: none"> 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	