



# Pulse Connect Secure Supported Platforms Guide

PCS 9.1R2

Build 2331

For more information, go to [www.pulsesecure.net/products](http://www.pulsesecure.net/products)

Product Release	<b>9.1R2, 2331</b>
Published	<b>July 2019</b>
Document Version	<b>1.0</b>

Pulse Secure, LLC

2700 Zanker Road, Suite 200

San Jose, CA 95134 <https://www.pulsesecure.net>

© 2019 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://support.pulsesecure.net/product-service-policies/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
July 2019	9.1R2, Doc ver. 1.0	Initial Publication

## Contents

Revision History .....	3
Introduction .....	5
Hardware.....	6
Client Environment Contents .....	7
Windows Supported Platforms .....	8
Mac OS Supported Platforms.....	10
Linux Supported Platforms .....	11
Pulse Secure Installer Service.....	12
Cross-Platform Features .....	12
Network Connect Notes .....	12
Pulse Secure Application Launcher (PSAL) Support.....	13
Pulse Desktop Client.....	13
Pulse Secure Collaboration Client Recommendations .....	13
Pulse Secure Mobile Client.....	13
Platform Support for Device Onboarding .....	14
MDM Solutions.....	15
Platform Support for AAA.....	15
Third-Party Applications.....	16
Change History.....	19

# 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.

# Client Environment Contents

- [Windows Supported Platforms](#)
- [Mac OS Supported Platforms](#)
- [Linux Supported Platforms](#)
- [Pulse Secure Installer Service](#)
- [Cross-Platform Features](#)
- [Network Connect Notes](#)
- [Pulse Secure Application Launcher \(PSAL\) Support](#)
- [Pulse Desktop Client](#)
- [Pulse Secure Collaboration Client Recommendations](#)
- [Pulse Secure Mobile Client](#)
- [Platform Support for Device Onboarding](#)
- [MDM Solutions](#)
- [Platform Support for AAA](#)
- [Third-Party Applications](#)

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	Network Connect	Pulse Secure Application Launcher	Pulse Secure Installer Service	Windows Secure Application Manager	Terminal Services
<b>Windows-10 Redstone 6 OS Build 1903 Version 10.0.18362.207, 64-bit</b> Internet Explorer 11, Edge, Google Chrome 61, Firefox ESR 60, Oracle JRE 8, 9 and 10 update 144	C	C	C	C	-	C <sup>②</sup>	C	C <sup>③</sup>	C
<b>Windows-10 Redstone 5 OS Build 1809 Version 10.0.17763.134, 64-bit</b> Internet Explorer 11, Edge, Google Chrome 61, Firefox ESR 60, Oracle JRE 8, 9 and 10 update 144	Q	Q	Q	Q	-	Q <sup>②</sup>	Q	Q <sup>③</sup>	Q
<b>Windows-10 Redstone 4 OS Build 1803 Version 10.0.17134, 64-bit</b> Internet Explorer 11, Edge, Google Chrome 61, Firefox 52 ESR, Oracle JRE 8 update 144	C	C	C	C	-	C	C	C	C
<b>Windows-10 Redstone 3 OS Build 1709, Version 10.0.16299.15, 64-bit</b> Internet Explorer 11, Edge, Google Chrome 61, Firefox 52 ESR, Oracle JRE 8 update 144	C	C	C	C	-	C	C	C	C
<b>Windows 10 RedStone-2 Enterprise/Pro/Home, Build 1703 Version 10.0.15063.332, 64-bit</b> Internet Explorer 11, Edge, Google Chrome 58, Firefox 52 ESR, Oracle JRE 8 update 131	C	C	C	C	-	C	C	C	C



Windows Platform	Admin UI	BYOD	Cross Platform Features	Host Checker	Network Connect	Pulse Secure Application Launcher	Pulse Secure Installer Service	Windows Secure Application Manager	Terminal Services
<b>Windows 10 Enterprise/Pro/Home</b> Internet Explorer 11, Edge Google Chrome Firefox 52 ESR. Oracle JRE 8	C	C	C	C	-	C	C	C	C
<b>Windows 8.1 Update/ Professional / Enterprise, 64-bit</b> Internet Explorer 11, Google Chrome & Firefox 52 ESR. Oracle JRE 8	Q	Q	Q	Q	-	Q <sup>②</sup>	Q	Q	Q
<b>Windows 8.1 Update/ Professional / Enterprise, 32-bit</b> Internet Explorer 11, Google Chrome & Firefox 38 ESR. Oracle JRE 8	C	C	C	C	-	C <sup>②</sup>	C	C	C
<b>Windows 8 Basic edition / Professional/ Enterprise, 32-bit &amp; 64-bit</b> Internet Explorer 10, Google Chrome and Firefox 31 & later. Oracle JRE 7 and later	C	C	C	C	-	C <sup>②</sup>	C	C	C
<b>Windows 7 Enterprise SP1, 64-bit</b> Internet Explorer 11, Google Chrome & Firefox 52 ESR. Oracle JRE 8	Q	Q	Q	Q	-	Q <sup>②</sup>	Q	Q	Q
<b>Windows 7 Ultimate / Professional / Home Basic / Home, 32-bit or 64-bit Windows 7 Enterprise (32-bit)</b> Internet Explorer 11, Google Chrome & Firefox 31 and later. Oracle JRE 7 and later	C	C	C	C	-	C <sup>②</sup>	C	C	C

Windows Platform	Admin UI	BYOD	Cross Platform Features	Host Checker	Network Connect	Pulse Secure Application Launcher	Pulse Secure Installer Service	Windows Secure Application Manager	Terminal Services	
Windows 7 Enterprise SP1, 64-bit										
Windows 8.1 Update/ Professional / Enterprise, 64-bit	Firefox 52 ESR, 32-bit Oracle JRE 8	C	C	C	-	-	-	C	C	C
Windows 10 Enterprise/Pro/Home										

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

**Note:** On RS5 client, WSAM behavior is not consistent, i.e. at times when WSAM is launched, the traffic for the configured resources is not SAMized. As a workaround, use Pulse SAM.

## Mac OS Supported Platforms

Table 3 lists supported Mac OS platforms vs PCS features:

Mac OS Platform	Admin UI	BYOD	Cross Platform Features	Host Checker	Network Connect	Pulse Secure Application Launcher	Pulse Secure Installer Service	Windows Secure Application Manager	Terminal Services
Mac OS Mojave Version 10.14	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	Q	Q	Q	Q	-	Q	-	-
Mac OS X 10.12	Safari 10.1 Chrome 73 Safari 9.0 Oracle JRE 8	C	Q	Q	Q	-	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	Network Connect	Pulse Secure Application Launcher	Pulse Secure Installer Service	Windows Secure Application Manager	Terminal Services	Pulse Secure Linux
openSUSE 12.1 Firefox 38 ESR, 32-bit	C	-	Q	C	C	-	-	-	-	-
openSUSE 11.x, 10.x Oracle JRE 8	C	-	C	C	C	-	-	-	-	-
Ubuntu 16.04 LTS Firefox 52, ESR, 64-bit	-	-	-	C	Q	-	-	-	-	Q
Ubuntu 15.04 Firefox 52, ESR, 64-bit	-	-	-	C	C	-	-	-	-	Q
Ubuntu 14.04 LTS Firefox 52, ESR, 64-bit	C	-	Q	Q	Q	-	-	-	-	Q
Ubuntu 12.04 LTS, 11.x, 10.x, 9.10 Oracle JRE 7 and later	C	-	C	C	C	-	-	-	-	C
RHEL 5 Firefox 52 ESR, 32-bit	C	-	C	C	C	C	-	-	-	C
RHEL 7 Firefox 52 ESR, 64-bit	-	-	-	C	Q	-	-	-	-	Q

Linux Platform	Admin UI	BYOD	Cross Platform Features	Host Checker	Network Connect	Pulse Secure Application Launcher	Pulse Secure Installer Service	Windows Secure Application Manager	Terminal Services	Pulse Secure Linux
<b>Fedora 23 (32 bit)</b>	Firefox 52 ESR 32-bit	-	-	-	C	C				Q (Pulse Secure Linux does not support browser launch)
<b>Fedora 23 (64 bit)</b>	Firefox 52 ESR 64-bit				C	Q				Q (Pulse Secure Linux does not support browser launch)
<b>CentOS 6.4</b>	Firefox 52, 32-bit/64-bit	-	-	-	C	Q	-	-	-	C
<b>CentOS 7.0</b>	Firefox 52, 64-bit	-	-	-		C	-	-	-	Q

## Pulse Secure Installer Service

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

- Network Connect
- Windows Secure Application Manager
- 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

## Network Connect Notes

For Network Connect, a Linux endpoint can run a 32-bit client on a 64-bit Linux platform.

## 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.

### @Note:

- 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
- Network Connect
- Windows Secure Application Manager
- 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
<b>Android</b> Android 7.0 and 6.0	Q	Q	Q	Q	-	-
<b>Android</b> 5.1.1, 4.4.4, 4.4.3, 4.4.2 and 4.3	C	C	C	C	-	-
<b>IOS</b> iOS 10.2.1, 9.3.5, 64-bit	Q	Q	Q	Q	C	-
<b>IOS</b> 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	-
<b>Windows Phone 8.1</b>	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
<ul style="list-style-type: none"> <li>iOS 10.x and 11.0, 64-bit</li> </ul>	Q	Q	Q	Q
<ul style="list-style-type: none"> <li>IOS 9.x</li> <li>iOS 8.3 64-bit</li> <li>iOS 7.1.2 64-bit &amp; 32-bit</li> <li>iOS 7.1 and 6.x 64-bit and 32-bit</li> </ul>	C	C	C	C
<ul style="list-style-type: none"> <li>Android 6.0.1 and 5.1.1</li> </ul>	Q	Q	Q	-
<ul style="list-style-type: none"> <li>Android 4.4.4, 4.4.3, 4.4.2 and 4.3</li> </ul>	C	C	C	-
<ul style="list-style-type: none"> <li>Windows 10</li> <li>Windows 8.1</li> <li>Windows 7</li> </ul>	-	Q	Q	-
<ul style="list-style-type: none"> <li>Mac OS X 10.12, Safari 9.0 &amp; Safari 10.0</li> <li>Mac OS X 10.10.5, Safari 8.0.8</li> <li>Mac OS X 10.9.5 Safari 7.0.x</li> </ul>	-	Q	Q	-
<ul style="list-style-type: none"> <li>Mac OS X 10.8.5, Safari 7.0.x and 6.0.x</li> </ul>	-	C	C	-

## MDM Solutions

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

Solution	Qualified	Compatible
<b>AirWatch</b>		
Cloud service	✓ 8.4.7.0	
Appliance OS		✓
Virtual appliance OS	✓	
<b>MobileIron</b>		
Cloud service	✓ Core 9.1.1.0 Build 29	
Appliance OS		✓
Virtual appliance OS	✓	
<b>Pulse Workspace</b>		
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*	<ul style="list-style-type: none"> <li>Windows Server 2016</li> <li>Windows Server 2012 R2**</li> </ul>	Windows Server 2008 R2 Windows Server 2003
LDAP using Microsoft Active Directory	<ul style="list-style-type: none"> <li>Windows Server 2016</li> <li>Windows Server 2012 R2</li> </ul>	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"> <li>OpenLDAP 2.3.27</li> </ul>	✓ Authentication and authorization based on user attributes or group membership.
RADIUS	<ul style="list-style-type: none"> <li>Steel-Belted RADIUS (SBR) 6.1</li> <li>Defender 5.2</li> <li>RSA Authentication Manager 8.4.0.3.0</li> </ul>	Azure MFA Radius Windows IAS 2008 RSA Authentication Manager 8.3
RADIUS IPv6 Support	<ul style="list-style-type: none"> <li>Steel-Belted RADIUS (SBR) 6.1</li> </ul>	<ul style="list-style-type: none"> <li>Windows NPS 2012 R2</li> <li>Free-RADIUS 2.1</li> </ul>

Third-Party AAA Server	Qualified	Compatible
RADIUS (other standards-compliant servers)		✓
ACE	<ul style="list-style-type: none"> <li>RSA Authentication Manager 8.4.0.3.0</li> </ul>	<ul style="list-style-type: none"> <li>RSA Authentication Manager 8.3</li> <li>RSA Authentication Manager 8.2</li> <li>RSA Authentication Manager 8.1</li> <li>RSA Authentication Manager 8.0 SP4</li> </ul>
Siteminder	<ul style="list-style-type: none"> <li>CA Siteminder 12.7</li> <li>CA Siteminder 12.52 SP1</li> <li>CA Siteminder 12.0 SP3</li> </ul>	<ul style="list-style-type: none"> <li>CA Siteminder 5.5</li> <li>CA Siteminder 6.0 SP4</li> </ul>
Certificate	<ul style="list-style-type: none"> <li>Windows 2008 R2</li> <li>Windows 2012 R2</li> </ul>	RSA Keon Certificate Manager 6.5.1
Certificate (other standards-compliant servers)		✓
SAML*** 2.0, 1.1	<ul style="list-style-type: none"> <li>PingFederate 6.4.1.1</li> </ul>	<ul style="list-style-type: none"> <li>Azure AD</li> <li>Microsoft ADFS 2.0 (Server 2008 R2)</li> <li>Oracle Identity Federation 11.1.1.2.0</li> </ul>
SAML 2.0, 1.1 (other standards-compliant servers)		✓

\*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
<b>Outlook Web Access (OWA)</b>			
OWA 2016	Web Profiles (Rewriter, Passthrough Proxy)	✓	
OWA 2013 SP1	Web Profiles (Rewriter, Passthrough Proxy)	✓	
OWA 2010 SP2, SP1	Web Profiles (Rewriter, Passthrough Proxy)		✓
OWA 2007	Web Profiles (Rewriter, Passthrough Proxy)		✓
<b>SharePoint</b>			
SharePoint 2016	Web Profiles (Rewriter, Passthrough Proxy)	✓	
SharePoint 2013 SP1	Web Profiles (Rewriter, Passthrough Proxy)	✓	
SharePoint 2010, 2007	Web Profiles (Rewriter, Passthrough Proxy)		✓
<b>IBM Domino</b>			



Application	Support Summary	Qualified	Compatible
Lotus iNotes 9.0	Web Profiles (Rewriter, Passthrough Proxy)	✓	
Lotus iNotes 8.5.3	Web Profiles (Rewriter, Passthrough Proxy)		✓
Lotus Connect 3.0, 2.5	Rewriter		✓
<b>Citrix</b>			
Citrix StoreFront 3.16	HTML5 Access, CTS and WSAM	✓	
Citrix StoreFront 3.12, 3.11 and 3.8	HTML5 Access, CTS and WSAM		✓
Citrix StoreFront with HTML5 Access	Custom Web Profile		✓
Citrix Listed Applications with Server 6.5 SP1, 6.0, 7.6, 7.8	Citrix Terminal Services		✓
Citrix Receiver 4.9, 4.10 and 4.11	Web, Terminal Services and SAM Profiles	✓	
Citrix Receiver 4.3.100	Web, Terminal Services and SAM profiles.		✓
Citrix XenApp and XenDesktop 7.18	Citrix Terminal Services	✓	
Citrix XenApp and XenDesktop 7.15, 7.14, 7.11	Citrix Terminal Services		✓
Citrix XenDesktop 7.14 and 7.15	VDI Profiles	✓	
XenDesktop 7.11, 7.8	VDI Profiles		✓
XenDesktop 7.8, 7.0, 5.6, 5.0	VDI Profiles		✓
Citrix Web Interface 5.4	Web Profiles (Rewriter, JSAM, and WSAM)	✓	
<b>VMWare</b>			
VMWare Horizon View HTML Access, version 7.7, 7.6, 7.5, 7.4	Rewriter	✓	
VMWare Horizon Agent version 7.7, 7.6, 7.5, 7.4	VDI Profiles	✓	
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	✓	
VMWare Horizon View Client version 4.10.0, to 4.1.0	VDI Profiles	✓	
VMWare View Server version 4.6, 5.0, 5.1, 2.3.x	VDI Profiles		✓
VMWare View Client version 4.6, 5.0, 5.1, 5.2			✓
<b>Exchange ActiveSync</b>			
Office 365	Secure Mail Resource Profile	✓	
Exchange 2016	Secure Mail Resource Profile	✓	
Exchange 2013, 2010 SP1, and 2007	Secure Mail Resource Profile		✓

Application	Support Summary	Qualified	Compatible
<b>ESAP Package</b>			
ESAP 3.0.3	Host Checker	✓	
<b>Virtual SA</b>			
ESXi 6.7		✓	
ESXi 6.5			✓
ESXi 6.0	PSA-V		✓
ESXi 5.5, 5.5 U3	PSA-V		✓
<b>KVM</b>			
CentOS 6.6 with Kernel cst-kvm 2.6.32-504.el6.x86_64	PSA-V	✓	
<b>Hyper-V</b>			
Microsoft Hyper-V Server 2016 and 2019		✓	
Microsoft Hyper-V Server 2012 R2			✓

# 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	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"> <li>Mac OS Supported Platforms</li> <li>Pulse Secure Application Launcher (PSAL) Support</li> </ul>	Added Chrome 61 support		9.1R1	Qualified in this release
Linux Supported Platforms	Added openSUSE Linux with Host Checker support		9.1R1	
Third-Party Applications	Added Citrix Storefront Server 3.16, XenApp Server 7.18, XenDesktop Server		9.0R4	Qualified in this release
Third-Party Applications	Added VMWare Horizon View Server 7.6 and 7.7, VMWare Horizon View Client 4.10.0 to 4.1.0		9.0R4	Qualified in this release
Third-Party Applications	Added Virtual SA ESXi 6.7		9.0R4	Qualified in this release
Third-Party Applications	Hyper-V 2016 and 2019		9.0R4	Qualified in this release
Windows Supported Platforms	Added Windows 10 Redstone 5		9.0R3	Added Windows 10 Redstone 5 qualified
Mac OS Supported Platforms	Added Mac OS Mojave 10.14		9.0R3	Added Mac OS Mojave 10.14 qualified
PSAL Support	Added PSAL support on Mac OS		9.0R3	Added PSAL support on Mac OS Mojave 10.14 and Mac OS High Sierra 10.13
Third-Party Applications	Added VMWare Horizon Agent		9.0R3	Added VMWare Horizon Agent for VDI Profiles version 7.5 and 7.4
Third-Party Applications		Removed Citrix Web Interface 4.5	9.0R3	Removed Citrix Web Interface 4.5
Third-Party Applications		Removed Citrix Program Neighborhood Agent with Citrix Server 6.0	9.0R3	Removed Citrix Program Neighborhood Agent with Citrix Server 6.0

Section	Add/Update	Drop or Moved	Effective Release	Notes
Third-Party Applications	Updated Citrix StoreFront 3.11 and 3.12		9.0R3	Consolidated Citrix StoreFront 3.12 Citrix Storefront 3.11
Third-Party Applications	Updated Custom Web Profile		9.0R3	Changed from Rewriter
Third-Party Applications	Updated Citrix XenApp and XenDesktop 7.11		9.0R3	Changed from Citrix Listed Applications with Server XenApp 7.11
Third-Party Applications	Added Citrix XenApp and XenDesktop 7.14 and 7.15		9.0R3	Consolidated Citrix Listed Applications with Server XenApp 7.15 and
Windows Supported Platform	Windows 10 Redstone-4 compatible		9.0R2	Added Windows 10 Redstone-4 compatible
Third-Party Applications	Added Lotus iNotes 9.0		9.0R2	Added Web Profiles (Rewriter, Passthrough Proxy) support for Lotus iNotes 9.0
Third-Party Applications	Added VMWare Horizon view HTML Access, version 7.5, 7.4		9.0R2	Added rewriter support for VMWare Horizon view HTML Access, version 7.5, 7.4
Third-Party Applications	Added VMWare Horizon view server version 7.5, 7.4		9.0R2	Added VDI profiles support for VMWare Horizon view server version 7.5, 7.4
Platform Support for AAA	Added RSA AM 8.3		9.0R2	Added support for RSA Authentication Manager 8.3
Platform Support for AAA	Removed RSA AM 7.1		9.0R2	Removed support for RSA Authentication Manager 7.1
Third-Party Applications	Added VMWare Horizon view HTML Access, version 7.3.1, 7.2		9.0R1	Added rewriter support for VMWare Horizon view HTML Access, version 7.3.1, 7.2
Third-Party Applications	Citrix Receiver 4.9 and 4.11		9.0R1	Citrix Receiver 4.9 and 4.11 has been qualified in this release
Third-Party Applications	Citrix StoreFront 3.12		9.0R1	Citrix StoreFront 3.12 has been qualified in this release
Third-Party Applications	Citrix XenDesktop 7.14 and 7.15		9.0R1	Citrix XenDesktop 7.14 and 7.15 has been qualified in this release