



PULSE CONNECT SECURE, PULSE POLICY SECURE AND PULSE CLIENT UPDATES FOR 9.1R4

Bulletin Date

January 2020

Applicable to All

Regions Effective

Change Date

January 2020

Introduction

Today's digital era is challenging workforce productivity, from the 9-to-5 workdays to means of accessing and digesting data. More importantly, access to data and applications across different mediums, mobile to cloud, are redefining traditional IT processes and policies. Pulse Secure has made it easier to secure your data center, provide mobile access and enable new cloud services with our integrated Secure Access Solution. This Product Bulletin describes new features and functions available in the 9.1R3 release of Pulse Connect Secure, Pulse Policy Secure, and the Pulse Secure Desktop Client.

These new releases from Pulse Secure enable network administrators to expand their secure access solution support for network performance and security.

This release focuses on customer requirements, Cisco ACS migration use cases, support for SDP enabled client on macOS and FQDN based Split tunneling improvements.

What's New

Common Features for Pulse Connect Secure and Pulse Policy Secure

Key Feature	Benefit
<ul style="list-style-type: none">REST API enhancements	<ul style="list-style-type: none">Enhancements include:<ul style="list-style-type: none">- Update to "Getting Active Sessions"- Update to "Getting System Information"- Added "Fetching the User Login Statistics"- Added "Health Check Status"- Added "VIP Failover"- Added "Applying License"- Added "Deleting License"- Added "Getting License Clients"- Added "Getting License Report from License Server"- Added Profiler REST APIs

Pulse Connect Secure 9.1R4

For detailed information on SDP, refer to the following SDP documents on <https://www.pulsesecure.net/techpubs>.

- SDP Release Notes
- SDP Supported Platforms Guide
- SDP Getting Started Guide
- SDP Deployment Guide

The following table lists the non-SDP features for Pulse Connect Secure 9.1R4.

Highlighted Features in this Release

Key Feature	Benefit
<ul style="list-style-type: none"> • PCS VA on Alibaba Cloud 	<ul style="list-style-type: none"> • PCS now supports VA deployment on Alibaba Cloud.
<ul style="list-style-type: none"> • vTM and PCS Integration for Load Balancing 	<ul style="list-style-type: none"> • The Platform Limit, Maximum Licensed User Count and Cluster Name attribute values are available for optimal load balancing.
<ul style="list-style-type: none"> • Support for Windows Redstone 6 	<ul style="list-style-type: none"> • In 9.1R4 release, Windows Redstone 6 - version 1909 is qualified.
<ul style="list-style-type: none"> • Support for SharePoint 2019 	<ul style="list-style-type: none"> • In 9.1R4 release, SharePoint 2019 is qualified.
<ul style="list-style-type: none"> • Support for VMware VDI 7.9, and 7.10 	<ul style="list-style-type: none"> • In 9.1R4 release, VMware VDI versions 7.9 and 7.10 are qualified.
<ul style="list-style-type: none"> • Support for Citrix Virtual Apps and Desktops 7 1909 	<ul style="list-style-type: none"> • In 9.1R4 release, Citrix Virtual Apps and Desktops 7 1909 is qualified.
<ul style="list-style-type: none"> • Protect passwords stored in local auth server using stronger hash 	<ul style="list-style-type: none"> • When a new local authentication server is created, now admin has a choice to store the password with strong hashing using pbkdf2.
<ul style="list-style-type: none"> • Support license reporting per license client 	<ul style="list-style-type: none"> • Licensing report is enhanced with usage statistics for each PCS instance - maximum user count per month per PCS/per MSSP. • MSSPs can now: <ul style="list-style-type: none"> - generate accurate usage reports of their customers. - make the structured report in XML format to enable parsing and dashboard usage.

Cloud Secure Specific Features in Pulse Connect Secure 9.1R4

Highlighted Features in this Release

Key Feature	Benefit
<ul style="list-style-type: none">• Conditional Access	<ul style="list-style-type: none">• Conditional Access feature for Cloud Secure provides a mechanism to enforce access control policies based on user, device and location parameters by defining policies for applications.• Conditional Access policies are evaluated during application access time while roles are mapped to the session during the session creation time.

Pulse Policy Secure and Profiler 9.1R4

Highlighted Features in this Release

Key Feature	Benefit
<ul style="list-style-type: none"> • UEBA on pulse one 	<ul style="list-style-type: none"> • Sends the required data from Pulse Connect Secure and Pulse Policy Secure to Pulse One for generating dashboards for UEBA on Pulse One.
<ul style="list-style-type: none"> • Huawei - Guest Access 	<ul style="list-style-type: none"> • Supports guest access use case with Huawei WLC.
<ul style="list-style-type: none"> • PPS on Azure 	<ul style="list-style-type: none"> • Provides NAC services (802.1x, MAC Auth, L3 Firewall Enforcement etc.) to multiple on-premise networks using PPS deployed in Azure cloud.
<ul style="list-style-type: none"> • Mist Juniper WLC 	<ul style="list-style-type: none"> • Supports 802.1x and guest access with Mist Juniper WLC.
<ul style="list-style-type: none"> • TACACS+ support for Arista Switch 	<ul style="list-style-type: none"> • Support Administrator access control for Arista.
<ul style="list-style-type: none"> • CAC support with TACACS+ 	<ul style="list-style-type: none"> • In this feature, CAC authentication will be supported with TACACS+, so that two-factor authentication is enabled.
<ul style="list-style-type: none"> • Provisioning only User-ID information to PAN firewall 	<ul style="list-style-type: none"> • Provides an option to admin to allow sending only IP-User mapping to PAN firewall.
<ul style="list-style-type: none"> • System Local user attribute support (Framed-IP-Address) 	<ul style="list-style-type: none"> • Allows to map Framed-IP to local User id mapping to authenticate users.
<ul style="list-style-type: none"> • Profiler Rest API support for approval functionality 	<ul style="list-style-type: none"> • Allow admin to approve/disapprove a device from his email or using the Rest API.
<ul style="list-style-type: none"> • Match Device attributes with LDAP attributes 	<ul style="list-style-type: none"> • This is an LDAP enhancement. This feature allows to identify the corporate device for pure agentless scenario by comparing device attributes with LDAP attributes.

Pulse Secure Desktop Client 9.1R4

For detailed information on SDP, refer to the following SDP documents on <https://www.pulsesecure.net/techpubs>.

- SDP Release Notes
- SDP Supported Platforms Guide
- SDP Getting Started Guide
- SDP Deployment Guide

The following table lists the non-SDP features for Pulse Desktop Client 9.1R4.

Highlighted Features in this Release

Key Feature	Benefit
<ul style="list-style-type: none"> • PSAM details tab 	<ul style="list-style-type: none"> • This allows the PSAM users to see the details of the applications which are tunneled via SAM client.
<ul style="list-style-type: none"> • Support after Linux NPAPI removal 	<ul style="list-style-type: none"> • This allows to launch Pulse Desktop Client from Linux Firefox browser after deprecation of NPAPI support.
<ul style="list-style-type: none"> • Yubikey smart card support 	<ul style="list-style-type: none"> • Yubikey can be used as PIV smart card for VPN authentication. <p>Note: Accept certificates with smartcard logon Enhanced Key Usage option should be enabled on PCS.</p>
<ul style="list-style-type: none"> • Windows Hello for Business 	<ul style="list-style-type: none"> • Pulse Desktop Client will now support Windows Hello for business using certificate trust.

Learn More

Resources

- [Pulse Connect Secure datasheet](#)
- [Pulse Policy Secure datasheet](#)
- [Pulse Cloud Secure product brief](#)

www.pulsesecure.net

About Pulse Secure, LLC

Pulse Secure, LLC is a leading provider of access and mobile security solutions to both enterprises and service providers. Enterprises from every vertical and of all sizes utilize Pulse Secure's Virtual Private Network (VPN), Network Access Control (NAC) and mobile security products to enable secure end-user mobility in their organizations. Pulse Secure's mission is to provide integrated enterprise system solutions that empower business productivity through seamless mobility.

Corporate and Sales
Headquarters Pulse
Secure LLC
2700 Zanker Rd. Suite
200
San Jose, CA 95134
www.pulsesecure.net

Copyright 2020 Pulse Secure, LLC. All rights reserved. Pulse Secure and the Pulse Secure logo are registered trademarks or Pulse Secure, LLC. All trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Pulse Secure assumes no responsibility for any inaccuracies in this document. Pulse Secure reserves the right to change, modify, transfer, or otherwise revise this publication without notice.