PRODUCT BULLETIN

# PULSE CONNECT SECURE, PULSE POLICY SECURE AND PULSE CLIENT UPDATES FOR 9.1R2

## Bulletin Date

July 2019

## Applicable to All

## Regions Effective

## Change Date

July 2019

## 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 9.1R2 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 |
| --- | --- |
| • Backup configs and archived logs on AWS S3/Azure Storage | • Two new methods of archiving the configurations and archived logs are available now apart from SCP and FTP methods:<br>Pulse Connect Secure now supports pushing configurations and archived logs to the S3 bucket in the Amazon AWS deployment and to the Azure storage in the Microsoft Azure deployment. |
| • Flag Duplicate Machine ID in access logs | • Pulse client expects the machine ID is unique on each machine. If multiple endpoints have the same machine ID, for security reasons, the existing sessions with the same machine id are closed.<br>A new access log message is added to flag the detection of a duplicate Machine ID in the following format:<br>*Message: Duplicate machine ID "<Machine_ID>" detected. Ending user session from IP address <IP_address>. Refer document KB25581 for details.* |
| • VA Partition Expansion | • PCS/PPS supports upgrading from 8.2Rx to 9.1R2 for the following supported platforms:<br>• VMWare ESXi<br>• KVM<br>• Hyper-V<br>When upgrading a VA-SPE running 8.2R5.1 or below that was deployed with an OVF template to a higher version, the upgrade was failing. This feature solves the upgrade problem for VMWare, KVM and Hyper-V. Refer KB41049 for more details. |
| • Report Max Used Licenses to HLS\|VLS | • From 9.1R2 release, the licensing client (PCS) starts reporting maximum used sessions count instead of the maximum leased licenses count.<br>For MSP customers, this change helps in billing the tenants based on maximum sessions used. |
| • V3 to V4 OPSWAT SDK migration | • PCS/PPS supports the migration of servers and clients to OPSWAT v4 to take advantage of latest updates. |

### Pulse Connect Secure 9.1R2

From 9.1R2 release onwards, Pulse Secure is introducing Pulse Secure Software Defined Perimeter on macOS. 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 9.1R2.

**Highlighted Features in this Release**

| Key Feature | Benefit |
|---|---|
| • SP-Initiated SAML SSO | • Pulse Secure supports SP-initiated SAML SSO when PCS is configured as IdP in gateway mode. PCS uses the existing user session in generating SAML assertion for the user for SSO. |
| • Microsoft RDWeb HTML5 Access | • The newly introduced Microsoft RDWeb resource profile controls access to the published desktops and applications based on HTML5. The Microsoft RDWeb templates significantly reduce the configuration time by consolidating configuration settings into one place and by pre-populating a variety of resource policy settings.<br>Note: In the 9.1R2 release, Microsoft RDWeb HTML5 access does not support Single Sign On. SSO will be made available in the future release. |

### Cloud Secure Specific Features in Pulse Connect Secure 9.1R2

### Highlighted Features in this Release

| Key Feature | Benefit |
|---|---|
| • IDP initiated SAML Single Logout | • This feature provides a single logout functionality wherein if a user gets logged out of a session from one application, PCS (configured as IdP) notifies all other connected applications of that user with Single Logout. |

## Pulse Policy Secure and Profiler 9.1R2

### Highlighted Features in this Release

| Key Feature | Benefit |
|---|---|
| • EasiSMS Gateway support | • PPS supports EasiSMS gateway through the SMTP server. EasiSMS uses an email format to send SMS to end user mobile phones. |
| • CISCO ACS migration | • CISCO ACS to PPS migration helps to achieve contextual based endpoint visibility, a much stronger security posture with unified access policies that extend from BYOD systems to their perimeter defenses. |
| • V3 to V4 Opswat SDK migration | • PPS supports the migration of servers and clients to Opswat v4 to take advantage of latest updates. |
| • Alert based integration with Nozomi Networks | • PPS along with Nozomi Networks provides threat detection and threat response in ICS/OT environment. |
| • Profiler | |
| • Windows defender and Microsoft Security Essentials support | • Agentless Host Checker with Profiler supports Windows defender and Microsoft Security Essentials. |
| • Profiler dashboard update | • Profiler dashboard supports chart for Profile Groups. This chart is also part of downloaded PDF report. |

### Pulse Secure Desktop Client 9.1R2

From 9.1R2 release onwards, Pulse Secure is introducing Pulse Secure Software Defined Perimeter on macOS. 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 9.1R2.

**Highlighted Features in this Release**

| Key Feature | Benefit |
|---|---|
| • FQDN resource and IPv4 resource-based Split Tunneling Conflict Resolution | • Pulse Connect Secure (PCS) supports both FQDN-based and IP-based split tunneling capability. When customers use both the split tunneling rules, PCS now provides flexibility for the customers to choose which rules to give precedence, and ensures the resource access is not impacted when there are conflicting rules. |
| • Manage Pulse Secure Client Versions feature support | • Pulse Connect Secure now supports ability to enforce minimum client version that can connect to the VPN. Admin will have the flexibility to provide minimum version separately for desktop and mobiles to enforce the different client versions. |
| • Support for Windows 10 Version 1903 (OS build 10.0.18362.207) | • Pulse Desktop Client on Windows now supports Windows 10 Version 1903 (OS build 10.0.18362.207) Enterprise, 64-bit and Windows 10 Version 1903 (OS build 10.0.18362.207) Professional, 64-bit. |
| • macOS KEXT Notarization | • Apple mandates that all macOS applications are notarized by Apple. Pulse macOS Client KEXT component is now notarized by Apple. |
| • SDP enabled Pulse Desktop Client on macOS | • The Pulse Desktop Client for macOS now supports SDP use case along with the classic VPN use case. As a part of SDP support, the Pulse Desktop Client on macOS can enroll the user device, connect to the SDP Controller, and provide access to multiple applications simultaneously by connecting to the multiple gateways. |

## 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