

PULSE CONNECT SECURE, PULSE POLICY SECURE AND PULSE CLIENT UPDATES FOR 9.1R11

Bulletin Date

February 2021

Applicable to All

Regions Effective

Change Date

February 2021

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 9.1R11 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.

What's New

Pulse Connect Secure 9.1R11

The following table lists the features for Pulse Connect Secure 9.1R11.

Key Feature	Benefit
Advanced HTML5 solution (General Availability version)	PCS supports Advanced HTML5 Access solution. This Advanced HTML5 Access solution supports two Advanced HTML5 sessions by default and includes multiple monitors, session recording, audio recording, high sound quality, and camera support. From 9.1.R11, Advanced HTML5 access is available as General Availability version.

Pulse Policy Secure and Profiler 9.1R11

Key Feature	Benefit
PPS and Profiler reporting enhancements	PPS supports report generation and sending it as a PDF attachment in a scheduled email based on filters and time settings.

Pulse Secure Desktop Client 9.1R11

The following table lists the features for Pulse Desktop Client 9.1R9.

Key Feature	Benefit
YubiKey support with CEF on Mac OS	This feature allows Unified Pulse Client to use Chromium Embedded Framework (CEF), to support YubiKey authentication using U2F protocol and MacOS.
Windows 20H2 Qualification	Pulse Client now supports Windows 20H2.
MacOS Big Sur Qualification	Pulse Client now supports MacOS BigSur.
Apple Silicon (M1) Support on Rosetta 2	Pulse Client supports Apple Silicon (M1) Support on Rosetta 2.
Single logout support for PDC on Linux	SAML Single Logout (SLO) is the protocol that allows users to logout from Service Provider (SP) as well as Identity Provider (IdP) and requiring users to provide credentials again upon next SAML authentication.
Lock-down exception enhancements	This feature allows the PCS to populate the list of core access rules depending on the platforms. Administrators can modify and reorder the list.

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 2021 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.