

VMware Secure Access Release Notes

VMware Secure Access

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

<https://docs.vmware.com/>

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to <https://www.broadcom.com>. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. [Copyright and trademark information](#).

Contents

- 1** Introduction 4
- 2** VMware Secure Access End of Availability (EOA), and End-of-Life (EOL) 5
- 3** Overview 6
- 4** New Features, Enhancements, and Resolved Issues 8
 - v.1.1.4 8

Introduction

1

VMware Secure Access | 06 June 2024

Check for additions and updates to these release notes.

VMware Secure Access End of Availability (EOA), and End-of-Life (EOL)

2

Important VMware has announced End of Availability (EOA) for VMware Secure Access starting January 31, 2024, with End-of-Life (EOL) starting August 31, 2024.

For more information see the Knowledge Base article: [Announcement: End of Life \(EOL\) for VMware Secure Access](#).

Overview

3

VMware Secure Access™ is part of the [VMware SASE™](#) solution and is a remote access solution that is based on a Zero Trust Network Access (ZTNA) framework. The cloud-hosted solution offers multiple benefits over traditional VPN solutions, enabling users a consistent, optimal, and secure cloud application process.

The solution leverages VMware's global Points of Presence (PoPs) footprint and optimizes traffic handling capabilities for lower latency and better application performance, enabling customers to provide a branch-like experience to remote workers.

The Secure Access Release Notes documents resolved Secure Access issues as well as new features and enhancements. Where previously this material was documented in the VMware SASE Release Notes, it is exclusively documented here going forward. Secure Access issues include those caused by a defect in the VMware SASE Orchestrator UI and those caused by a defect in the Secure Access service itself.

Secure Access follows a versioning system different from VMware SD-WAN and should be understood as separate from SD-WAN or the SASE Orchestrator.

The Secure Access version for a customer deployment is found on the Orchestrator by first selecting the **Secure Access** screen, and then clicking the (?) icon to open the **Help** menu. The Secure Access version is displayed at the bottom of the **Help** menu.

Figure 3-1. Secure Access Version Location

The screenshot displays the VMware Orchestrator Secure Access web interface. The top navigation bar includes the VMware logo, 'Orchestrator', and a 'Secure Access' dropdown menu. A red box highlights the 'Secure Access' dropdown. To the right, there is a link to 'Open Classic Orchestrator' and a help icon (a circle with a question mark) which is also highlighted with a red box and a red arrow pointing to it. Below the navigation bar, the main content area is divided into 'Monitor' and 'Configure' tabs. The 'Monitor' tab is active, showing a list of 'Events' and 'Logs'. The 'Events' section shows a table of events with columns for 'Event', 'User', and 'Severity'. The 'Logs' section shows a list of logs. On the right side, there is a 'Help' sidebar with links to 'Quick Start Guide', 'Product Documentation', and 'Knowledge Base'. Below these links, the 'About' section is visible, showing the 'Version' as 1.1.4, which is highlighted with a red box. The 'Build' information is also displayed: 202305301900-af4e1067c3. At the bottom of the sidebar, there is a 'Cookie Usage' link and a copyright notice: ©2023 VMware.

vmw Orchestrator Secure Access

Open Classic Orchestrator

Monitor Configure

Events

Secure Access Events

Logs

Secure Access Logs

Events

Past 6 Months Jan 13, 2023, 4:52:41 PM

FILTERS CSV

Event	User	Severity
SA service created		Info
SA service tunnel pod deployment completed		Info
SA service tunnel pod deployment started		Info

Help

Quick Start Guide

Product Documentation

Knowledge Base

About

Version 1.1.4

Build 202305301900-af4e1067c3

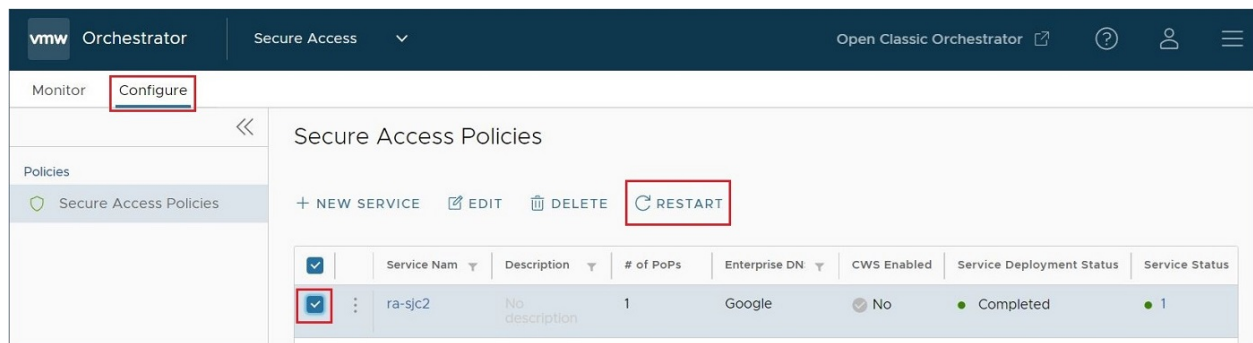
Cookie Usage

©2023 VMware

New Features, Enhancements, and Resolved Issues

4

Important In order to take advantage of new **Workspace ONE Tunnel** features and enhancements, the customer must **Restart** their **Secure Access** deployment from the Secure Access Configuration page. This is only true for **Workspace ONE Tunnel**. A restart is not required for any other **Secure Access** feature, enhancement, or fix as those are not service impacting changes and are automatically updated by VMware.



Read the following topics next:

- [v.1.1.4](#)

v.1.1.4

Secure Access version **1.1.4** was released on **19 July 2023**.

This version adds new enhancements and resolved issues.

The enhancements and fixed issues added in Secure Access version **1.1.4**:

- **Workspace ONE Tunnel Enhancement, and Fixes**

The following enhancement is added to the **Workspace ONE Tunnel**:

- Session Multi-Factor Authorization for Mobile Devices.

Note This enhancement requires using Workspace ONE UEM 2302.

The following issues are resolved for the **Workspace ONE Tunnel**:

- Authentication with SAML does not validate the assertion in SAML correctly.

- DNS caching logic improvements.
- Client connectivity sometimes fails due to duplicate client sessions.
- **New Secure Access Enhancement: SASE PoPs Updated Together by Default**

Introduces an enhancement to the existing **Restart** capability that prevents selecting individual SASE PoPs for restarts in Secure Access deployments. The restart action is necessary to complete the update of a SASE PoP. The default behavior is now to restart across all PoPs.

As a result, the customer no longer needs to track which SASE PoPs are updated and which are not updated, they will always be on the same version after each restart.

Note The **Restart** capability forces the Secure Access service to use the latest version of the Workspace ONE tunnel.
