General Availability of Symantec PAM v3.4.2

Product:	**Published date:** 11-02-2020
CA Privileged Access Manager (PAM)	**Updated Date:** 11-02-2020

November 2nd, 2020

To: Symantec Privileged Access Manager Customers

From: The Symantec Privileged Access Manager Product Team

Subject: General Availability Announcement for Symantec Privileged Access Manager v3.4.2

On behalf of Broadcom, we appreciate your business and the opportunity to provide you with high-quality, innovative software and services. As part of our ongoing commitment to customer success, we regularly release updated versions of our products. Today, we are pleased to announce that Symantec Privileged Access Manager v3.4.2 is now available.

New features for Symantec Privileged Access Manager v3.4.2 include:

Password View Request Updates

This release includes the following updates to the Password View Request feature:

- The “Reason Description” and “Reference Code” fields are mandatory when a user attempts to view or access an account which has the ‘Reason Required for View’ option or the ‘Reason Required for Auto Connect’ option enabled in the Password View Policy.
- A Comments field for a Password View Request is available when the ‘Reason Required for View’ option or the ‘Reason Required for Auto Connect’ option is enabled in the Password View Policy.
- A banner is displayed on Password View Requests when the ‘Reason Required for View’ or ‘Reason Required for Auto-connect’ option is enabled in the Password View Policy. This banner can contain information about what users need to enter in the Reason Description and Reference Code fields when they attempt to view a password for an account.

Ability to Update the PAM Host File when Deployed in Restricted High Security Data Centers

This feature enables users to update the PAM host file from the PAM user interface when doing so through Symantec PAM Support’s assisted Remote SSH Debug Access is not permitted.

Enable Public Key Authentication

You can configure a TCP/UDP Service to connect to a target device using the Public Key Authentication method for a native SSH Application.

Ability to Customize the SSH Cipher Suite Used by PAM for Connections

PAM provides the ability to configure a subset of ciphers used by SSH connections for accessing devices. The option to configure older vulnerable KEX/Ciphers/HMAC allows the management of legacy devices where newer ciphers are not supported or for systems that have not yet been updated to support the secure default cipher suite of PAM. This feature was originally introduced in 3.3.4

We encourage you to visit the Symantec PAM product information page on the Support Online website at https://casupport.broadcom.com/ for more information.

To learn about the new features offered in Symantec PAM 3.4.2, refer to the product documentation at https://techdocs.broadcom.com/. To connect, learn and share with other customers, join and participate in our Symantec Privileged Access Manager Community at https://community.broadcom.com/home. To review Support lifecycle policies, please review the Support Policy and Terms located at: https://casupport.broadcom.com/.

Your success is very important to us, and we look forward to continuing our successful partnership with you.

To review Broadcom Support lifecycle policies, please review the Broadcom Support Policy and Terms located at: https://support.broadcom.com/.

Thank you again for your business.