

Symantec Privileged Access Manager v4.0 Release Announcement

April 27th, 2021

To: Symantec Privileged Access Management (PAM) Customers
From: The Symantec Privileged Access Management Product Team
Subject: Announcing the Release of Symantec Privileged Access Manager v4.0

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 4.0 is now available.

New features for Symantec PAM 4.0 include:

- **Unification of PAM Server Control and PAM**

Symantec PAM Server Control, formerly a standalone product for fine-grained privileged access control, is now part of the Symantec PAM platform. This unification significantly simplifies and streamlines the administration and management of privileged access. Key components and capabilities of this unification include:

- **PIM and PAM SC Policy Deployment integrated into the PAM User Interface**

Policy deployment functionality allows you to deploy fine-grained access policies to the Endpoint Agents from the PAM UI.

- **New Utility Appliance**

In the PAM environment, PAM SC Distribution Servers are replaced by a new hardened Utility Appliance. These Utility Appliances are VMware, AWS, or Azure virtual machines that you can freely download and deploy. Utility Appliances host preloaded Distribution Server software that is backwards compatible with the PIM and PAM SC endpoint agents that are currently installed on endpoints.

- **Simplification of PAM Server Control Agent Deployments**

Integrated Server Control allows you to simplify PIM and PAM SC Endpoint installations, upgrades, and patches with no downtime and provides a rollback mechanism if there is failure. This simplification reduces the time to deploy from several months to days. Simplified agent installation is supported on all Linux implementations.

- **Unix Authentication Broker (UNAB)**

The UNIX Authentication Broker (UNAB) consists of several components that manage and control access to the UNIX host by Active Directory users. You can manage the following UNAB functions through PAM:

- UNAB Login Authorization - Host or Host Group

From the PAM UI, you can control users and groups access to the UNIX hosts and can configure your UNAB host. You can also control user and group access to the UNIX host by granting access to only those users and groups that are permitted to log into that host.

- Configure a UNAB Host or Host Group

From the PAM UI, configure UNAB hosts in the same manner that you configure control access to the host. You can control the functionality of UNAB hosts in the enterprise once and then apply it to all the hosts.

- **Migration package for CA Privileged Identity Management and PAM Server Control deployments**

This release includes a Migration Utility wizard that migrates DMS data (Devices, Device Groups, Policies, and Deployments) from existing PIM and PAM SC environments to PAM. Migration involves tasks such as data extraction, validation, data backup, and finalization.

- **Microsoft® Azure support for PAM Threat Analytics module**

The PAM Threat Analytics Module, in vhd format, is now supported for deployment in the Microsoft Azure cloud environment.

- **Ability to use SFTP or SCP for file transfers via the SSH Proxy**

You can configure a TCP/UDP SSH Service to do the file transfer operations for a native SFTP or SCP application. Session recording is not activated when either of these features are invoked (the files are not copied into the recording).

- **The ability to run a network mapping job from the PAM Configuration page**

With the Bulk Network Scan tool, Administrators can run a bulk scan of their network (Host/Port) to determine the status of ports (open/filtered).

- **Support for Web Portal traffic through Web Proxy**

Support for all web portal traffic to be routed through a configured proxy. If Symantec ProxySG is configured as a proxy in the PAM client, a policy configuration change can be made on the ProxySG to allow protocols such as SSH and RDP through the ProxySG.

- **External Directory Authentication and auto registration of Privileged Users**

This feature provides the ability for PAM to auto-register users at run time both for authentication and authorization without importing the entire user group members. This ensures that the large, and frequently changing Users' group member relationship update does not affect PAM performance or cause a breach in governance rules due to access changes.

For more information, please visit the Symantec Privileged Access Manager product information page on the Broadcom Support Online website at <https://support.broadcom.com/>.

You can download your copy of Symantec Privileged Access Manager 4.0 from Broadcom Support Online <https://support.broadcom.com/>. If you have any questions or require assistance please contact Broadcom Customer Care online at <https://www.broadcom.com/support/software/contact> where you can submit an online request using the Customer Care web form:

https://ca-broadcom.wolkenservicedesk.com/web-form?_ga=2.205828371.1432263889.1590607313-713014253.1588711301 . You can also call Broadcom Customer Care at +1-800-225-5224 in North America or see <https://www.broadcom.com/support/software/contact> for the local number in your country.

Should you need any assistance, our Broadcom Services experts can help. For more information on Broadcom Services and how you can leverage our experience, please visit <https://www.broadcom.com/support/ca/services-support/ca-services>.



Symantec plans to support the Privileged Access Manager v4.0 release, including all subsequent service packs, until **April 27th, 2023**.

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

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

Thank you again for your business.