Proactive Notification: Product Update

April 24th, 2018

To: CA Privileged Access Manager (PAM) Customers
From: The CA Privileged Access Manager Product Team
Subject: Announcing the Release of CA Privileged Access Manager v3.2

On behalf of CA Technologies, 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 the release CA Privileged Access Manager (CA PAM) v3.2. This release includes significant new capabilities designed to extend support for hybrid enterprise protection and enhance security, automation and auditability.

New features for CA PAM 3.2 include:

- **Support for Microsoft® Azure**

  CA Privileged Access Manager now offers a VHD image that you can deploy on Microsoft® Azure. With CA Privileged Access Manager 3.2, you can:

  - Deploy a Virtual appliance on Azure
  - Deploy a Management Console on Azure
  - Use Azure CIFS Storage for Session Recording and Database Backup
  - Import Azure Virtual Machines
  - Azure Active Directory as a SAML IdP

- **External API's for audit operations**

  The CA Privileged Access Manager External API includes new audit operations for the **devices** and **users** resources. You can use these audit operations to monitor activity in your organization and mitigate risk. Only the GET method is available with these new operations.

- **Enhancements to the Remote Command Line Interface (CLI)**

  The Remote CLI has the following enhancements:

Filter Password View Requests Based on Start and End Time

Using the Remote CLI, you can now filter password view requests based on the start and end time of the request. To implement time-based filters, the following parameters have been added to three of thesearchPasswordViewRequest CLI commands:

- PasswordViewRequest.requestPeriodStart
- PasswordViewRequest.requestPeriodEnd

Obtain the Device ID when Listing Target Accounts

The listTargetAccounts command returns information about a target account, the target application, and the device name associated with this account. The listTargetAccounts command now also returns the device ID. The device ID can help users obtain more details about a device. The return value abbreviation for the device ID is **di**.

Activate the Windows® Proxy using the Remote CLI

You can now activate and manage the CA PAM Windows Proxy using the Remote CLI. The new command is the **updateAgent** command because CA PAM considers the Windows Proxy a type of agent.

- **Mobile support for Password View Requests**
  The CA Privileged Access Manager Access User Interface (UI) has been optimized for Password View Requests on mobile browsers. This limited enhancement is supported on Chrome® for Samsung Galaxy® 7 and 8, Safari® for iPhone® 8 and X, and iPad® Pro 10.5 and 12.9.

- **New Logging of UI interactions for Troubleshooting**
  You can now capture logs from user interface interactions to help troubleshoot problems.

- **Forward Secrecy for CA PAM RDP Client**

  The CA PAM RDP client now supports forward secrecy with the following cipher suites:

- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

- **New Fields for Linking Access and Request Logs**

  In version 3.2, Target Account and Password View Request ID fields have been added to logs. If you are using an external database with a previous version, a table update is required.

- **Disable Concurrent Remote Connections**

  With this version, concurrent user connections by the same user from different IP addresses can be disabled. Because there are use cases where this concurrence might be necessary, it is allowed by default. The option is found in the UI on the **Configuration**, **Security**, **Access** page.

- **Enhanced support for Service Desk Integration**

  Service Desk integration has been updated to work with new versions of Service Desk solutions. If you have to troubleshoot your service desk integration, you can now download CA NIM logs.

- **Paris region added for Amazon AWS support**

  CA Privileged Access Manager 3.2 adds support for the Amazon® AWS® EU (Paris) Region.

- **Update to REST API calls**

  CSPM REST API calls to the CA PAM External API has changed.
  NOTE: If you have API calls that begin with /cspm/rest/*, you will need to* ***update these calls to use /cspm/ext/rest.***

The CA Privileged Access Manager v3.2 release, including all subsequent service packs, will be supported until **April 24th, 2020** with an additional one year of Basic Extended Support (Paid option) ending **April 24th, 2021.**

We encourage you to visit the CA Privileged Access Management product information page on the CA Support Online website at https://support.ca.com/ for more information.

If you have any questions or require assistance contact CA Customer Care online at http://www.ca.com/us/customer-care.aspx where you can submit an online request

using the Customer Care web form: https://support.ca.com/irj/portal/anonymous/customercare. You can also call CA Customer Care at +1-800-225-5224 in North America or seehttp://www.ca.com/phone for the local number in your country.

To learn about the new features offered in CA PAM 3.2, refer to the product documentation at docops.ca.com. Should you need further assistance in understanding these new features, or implementing this latest release, our CA Services experts can help. For more information on CA Services and how you can leverage our expertise, please visit www.ca.com/services. To connect, learn and share with other customers, join and participate in our CA Privileged Access Manager CA Community at https://communities.ca.com/.

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

Thank you again for your business.