Upgrading CA Privileged Access Manager

CA Privileged Access Manager (CA PAM) is designed to secure all IT resources, facilitate compliance and minimize costs. Available as either a hardened hardware, virtual or Amazon Web Services (AWS) Amazon Machine Images (AMI) appliance, CA PAM is designed to prevent security breaches by consistently protecting sensitive administrative credentials, such as root and administrator passwords, controlling privileged user access, proactively enforcing security policies and monitoring and recording privileged user activity across virtual, cloud and physical environments.

Upgrading to the latest CA PAM version provides new features, cumulative bug fixes, and security and operational efficiency improvements. Key enhancements available in CA PAM 3.1 include:

- **Integration with Sailpoint®.** Enables you to provision and de-provision CA PAM users, process privileged access requests, define role inheritance and certify privileged access through integration with SailPoint.
- **Enhanced mainframe support.** Introduces a mainframe proxy, "bring your own client" approach, auto-login and session recording. Support for Mainframe 3270 and 5250 systems.
- **Microsoft Windows® proxy agent alternative.** Minimizes footprint by allowing the appliance to directly perform service, task, credential management and discovery functions instead of using an agent.
- **Expanded active directory support.** Enables retention of policies and credential rotations as accounts move to different Active Directory operating units.
- **Expanded Amazon AWS support.** Provides enhanced regional support for protecting international AWS instances in: Frankfurt, Germany; Seoul, South Korea; London and U.S. East (Ohio).

In addition, the table below provides a simplified summary of enhancements introduced in recent versions. For additional detail related to the items in the table below, please review the product documentation.

New Features and Enhancements	2.7*	2.8*	3.0*	3.1
Core CA Privileged Access Management Capabilities				
Sailpoint integration. You can now integrate the solution with Sailpoint IQ to provide full privileged identity lifecycle management and governance.	X	X	X	✓
Enhanced mainframe support. Introduces a mainframe proxy, "bring your own client" approach, auto-login and session recording. Support for Mainframe 3270 and 5250 systems.	X	X	X	✓
Microsoft Windows proxy agent alternative. Minimizes CA PAM footprint by allowing the appliance to directly perform service, task, credential management and discovery functions instead of using an agent.	X	X	X	✓
Enhanced Kerberos PIV/CAC authentication. Offers support for Kerberos and PIV/CAC card access including Microsoft Windows RDP and Web portal access. Enhancements also include support for single and multiple smart card readers.	X	X	X	✓
***= some of these enhancements introduced in SPs and CRs on these releases.**				

New Features and Enhancements	2.7*	2.8*	3.0*	3.1
Integration with CA Threat Analytics. CA Threat Analytics continuously analyzes user activity data and sends back user-specific risk assessment decisions so that the solution can appropriately control, or mitigate, user activity.	X	✓	✓	✓
Privileged identity governance. Integrates with CA Identity Suite to provide full privileged identity lifecycle management and governance.	X	✓	✓	✓
Palo Alto target connector. A new target connector allows you to manage accounts on Palo Alto routers and PAN-OS. This connector uses the SSHv2 protocol for communication.	X	✓	✓	✓
Oracle target connector enhanced. The Credential Manager Oracle Target Connector supports Oracle Internet Directory and Oracle Database.	X	✓	✓	✓
Automatic password change when session ends. You can set a new option that automatically changes a password that is used during a CA session after that session is closed, times out or the session is terminated.	X	✓	✓	✓
Transparent login extended to Korn shell. Transparent Login KSH support for SSH Proxy and Applet on AIX 7.1.	X	✓	✓	✓
Enhanced Kerberos PIV/CAC authentication. The RDP smart card login dialog for Kerberos with PIV/CAC authentication now supports mapping one smart card certificate to multiple accounts.	X	✓	✓	✓
Multisession support in Citrix XenApp. Multiple users can launch multiple PAM Client instances from different XenApp sessions.	X	✓	✓	✓
Service desk integration. You can now provision privileged account access to your service desk solution, as well as update the passwords of your service desk, including: BMC Remedy, CA Service Desk Manager, HP ServiceManager, ServiceNow and Salesforce Service Cloud.	✓	✓	✓	✓
CA Single Sign-On integration. You can use CA Single Sign-On to protect resources on the product itself.	✓	✓	✓	✓
Kerberos-PIV/CAC authentication. Kerberos authentication can be implemented for users with PIV/CAC smart cards.	✓	✓	✓	✓
Administration and Supportability				
Enhanced user interface. The user interface was rewritten to improve usability. In particular, Credential Manager controls are now included in the main UI instead of opening in a separate tab or window.	X	X	✓	✓
Management console. This new interface is provided for customers or MSPs that are administering large cluster deployments or multiple disparate sets of clusters.	X	X	✓	✓

***= some of these enhancements introduced in SPs and CRs on these releases.**

New Features and Enhancements	2.7*	2.8*	3.0*	3.1
Microsoft Windows Proxy Account Discovery. This release adds the ability to discover local Microsoft Windows accounts, services and tasks using the Microsoft Windows proxy.	X	X	✓	✓
Logging improvements. Access and credential management components return unified log messages that show the associated user, device name and target account.	X	X	✓	✓
Remote engineer. CA Remote Engineer with telemetry greatly simplifies the ability to collect and securely deliver environmental and log data to CA Support, helping to accelerate troubleshooting and problem resolution.	X	X	✓	✓
External Rest APIs. The following categories of rest APIs are now included: configProperties; Radius and TACACS; sessionRecordingConfiguration; sessionRecordings; splunk and sysLogConfiguration.	X	X	✓	✓
Extra LDAP attributes for password modification. You can now specify attribute name/value pairs to be updated with password modifications.	X	✓	✓	✓
User-generated public keys for backup file transfers. You can generate your own public keys for a database backup file transfer operation (SCP or SFTP).	X	✓	✓	✓
Preload upgrade files while the cluster Is active. You can preload an upgrade file on each node in a cluster while the cluster is still up and running, then only turn off the cluster to apply the upgrade itself.	X	✓	✓	✓
Scheduled purge of session recordings. You can automatically purge old session recordings after X days.	X	✓	✓	✓
Compact database. Your database can compacted to reclaim storage space used by previously deleted entries.	X	✓	✓	✓
Device discovery. A streamlined and enhanced interface is provided for device discovery and registration.	✓	✓	✓	✓
Account discovery and SSH key discovery. Credential Management Account discovery and registration is introduced. Key discovery and reporting is also provided.	✓	✓	✓	✓
Database backup enhancements. The automated database backup has been enhanced to provide storage on NFS, CIFS and Amazon S3 mounts in addition to the existing options for SCP or SFTP file transfer.	✓	✓	✓	✓
SAML JIT user group membership enhancements. You can now configure the solution such that every IdP assertion to a JIT-permitted PAM SP can potentially alter a JIT User Groups membership.	✓	✓	✓	✓
Transparent login customization. The ExternalAPI now provides parameters and operations supporting Transparent Login data manipulation.	✓	✓	✓	✓

***= some of these enhancements introduced in SPs and CRs on these releases.**

New Features and Enhancements	2.7*	2.8*	3.0*	3.1
Platforms and Internals				
Microsoft Windows® 2016 certification. Full support for Microsoft Windows 2016 operating systems including RDP access, Windows proxy, Socket Filtering, Transparent Login and Remote Command Line Interface.	X	X	X	✓
Expanded Amazon AWS support. Enhanced regional support for protecting international AWS instances in: Frankfurt, Germany; Seoul, South Korea; London and U.S. East (Ohio).	X	X	X	✓
Microsoft Windows Trust Certificates support. Enable CA PAM client to automatically trust certificates in the Microsoft Windows trust store.	X	X	X	✓
Session recording encryption. All session recordings are now encrypted using the AES-256 cipher.	X	X	✓	✓
Session recording storage failover. To avoid losing session recording ability due to a network share failure, you can now mount a secondary share to provide failover.	X	X	✓	✓
FIPS 140-2 encryption support. When FIPS mode is configured, the appliance automatically uses the new, NIST-approved, FIPS 140-2 certified CA Technologies C-Security Kernel for cryptographic operations.	X	X	✓	✓
Ability to disable the TLS communication protocols. By default, the TLS 1.0, 1.1 and 1.2 communication protocols are enabled. You can now disable these protocols to enhance security for inbound communication.	X	X	✓	✓
Network teaming. You can set up network teaming—also known as NIC teaming, bonding or aggregation—to combine multiple network cards together for enhanced performance or redundancy.	X	X	✓	✓
AWS Linux AMIs delivered as HVM. CA Privileged Access Manager delivers version 3.0.1 as HVM only, as this type is supported in more AWS regions.	X	X	✓	✓
Localization. Solution supports Japanese localization and use of international Japanese and Italian keyboards for RDP connections.	X	X	✓	✓
LDAP Over SSL (LDAPS) support. You can now configure an LDAP domain using an LDAP over SSL (LDAPS) connection.	X	✓	✓	✓
Localization. Solution supports use of international Canadian French keyboards for RDP connections.	X	✓	✓	✓
SHA-2 support for the MindTerm SSH applet. SHA-2 Hash-based Message Authentication Code (HMAC) for the embedded MindTerm SSH applet (include SHA-256 and SHA-512) now included.	X	✓	✓	✓

***= some of these enhancements introduced in SPs and CRs on these releases.**

New Features and Enhancements	2.7*	2.8*	3.0*	3.1
Integrity checks for PowerShell A2A scripts. PowerShell scripts can be hashed as part of the integrity check option when using the Microsoft Windows A2A Manager Client.	X	✓	✓	✓
Multi-site clustering. Clustering across multiple geographically dispersed sites is now supported.	X	✓	✓	✓
Server Message Block (SMB) support. SMB2 and SMB3 support added for CIFS Network Shares.	X	✓	✓	✓
Secure communication enhancements. The communication path between the appliance and Socket Filter Agents (SFAs) has been upgraded to use TLS 1.2.	✓	✓	✓	✓
***= some of these enhancements introduced in SPs and CRs on these releases.**				

For more information, please visit **ca.com/pam**

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.