Securden

Unified PAM

Product use cases →

Securden Unified PAM Use Cases

This document provides a quick summary of various use cases of Securden Unified PAM. Explore how PAM helps secure privileged accounts and fortify the overall security posture in any organization.

Keep all your passwords & files in a secure, central vault

Details:

- Discover all privileged accounts in your organization spread across systems, servers, databases & network devices

- Consolidate and securely store all logins, passwords, privileged accounts, SSH access keys, documents, and other sensitive data in a central, highly available, access-controlled vault

Benefits:

- Eliminate passwords stored on notepads, excel sheets, and scripts

- Gain centralized control over all credentials

- Prevent unauthorized access to credentials and IT assets

- Eliminate siloed structure and gain 360-degree visibility and total control over privileged access

Classify and organize passwords for efficient management

Details:

- Organize accounts by types (Web accounts, DevOps secrets, access keys, servers, databases, devices, applications and so on)

- Create custom account types

- Differentiate and classify accounts into work and personal

- Utilize tags and notes for organization and easy identification

- Mark accounts as favorites, pin entries for quick access
- Color code accounts for identification at a glance
- Define complexity rules and enforce strong, unique, random passwords
- Set maximum age for passwords and send expiration alerts reminding users to change their passwords

Benefits:

- Maintain passwords in a well-organized manner
- Allow a secure personal vault within the organizational vault
- Keep the right passwords in the right place
- Locate required accounts/passwords quickly
- Eliminate security risks arising due to weak passwords
- Enforce strong password usage discipline across the organization by using the password generator tool
- Gain centralized control over all credential
- Prevent unauthorized access to credentials and IT assets
- Eliminate siloed structure and gain 360-degree visibility and total control over privileged access

Maintain well-defined ownership for accounts and passwords

Details:

- Define ownership for each account and let owners decide who all in the team can access the specified account
- Share accounts owned by users with granular access permissions
- Transfer ownership of accounts when someone leaves

Benefits:

- Control access to passwords based on job needs and requirements
- Never leave any password an orphan - there will be an owner to take care
- Keep access to important passwords when users leave the organization

Selectively share passwords with granular permissions

Details:

- Share passwords with the required team member, or a member group
- Grant granular permissions to allow users to perform limited actions on the shared account
- Flexibility to show or hide passwords while sharing
- Revoke share access anytime with ease

Benefits:

- Maintain control on ‘who’ can access ‘what’
- Safely share administrator passwords
- Prevent passwords from being widely known
- Grant remote access without revealing passwords

Launch remote connections without disclosing passwords

Details:

- Provide your users and third-parties secure, one-click access to remote servers, databases, devices and applications without disclosing the passwords to them
- Choice of web-based connections and using native client applications (RDP, SSH, SQL)
- Browser extensions to autofill passwords on websites

- Application Server, and API-based application servers to carry out remote operations on external networks

Benefits:

- Cross-platform access flexibility for users (Remote employees can use machines running any operating system (Windows, Linux, or Mac) to connect to target machines running any operating system. They can launch connections by clicking a link in the Securden web-interface
- Safely carry out remote operations - Carry out remote operations on devices in another network without opening database ports from the Securden server instance using the API Application Server
- Seamless access, no VPN hassles, enhanced productivity
- Grant remote access without revealing passwords

Periodically randomize passwords of IT assets

Details:

- Automatically change the passwords of ~~remote~~ IT assets at periodic intervals
- Assign strong, unique passwords for accounts based on your IT password policy

Benefits:

- Eliminate vulnerabilities arising from identity thefts
- Comply with regulations and best practices that mandate periodic password resets

Just-in-Time access with approval workflows

Details:

- Enforce users to raise requests to access IT assets and applications
- Grant just-in-time access to resources
- Automatically randomize password after access

- Enforce users to provide a reason before requesting access

Benefits:

- Maintain complete control over access to sensitive devices
- Grant access to users only when they require
- Ensure one or more levels of approvals to access resources

Hierarchical folders for grouping accounts

Details:

- Organize logins as hierarchical folders reflecting the organizational hierarchy
- Maintain the passwords belonging to each factory/division as a folder
- Restrict access to that folder to the members of the division only

Benefits:

- A vault for each department within the central vault
- Full control on department-wise access to passwords
- Complete access control over the IT infrastructure

Manage machine/application identities using APIs

Details:

- Comprehensive list of APIs to perform various functions
- Allow applications/scripts to use APIs to fetch passwords from PAM and connect to other applications, websites or database services
- Support machine to machine authentication using APIs for robotic processes

Benefits:

- Eliminate hard-coded passwords embedded in configuration files, scripts, and code

- Automate application passwords usage in development environments

Active Directory, SSO integration for user provisioning

Details:

- Integrate with Active Directory and allow users to login with their AD credentials and the convenience of AD SSO
- Import users from AD, Azure AD, LDAP AD or from a file
- Keep user database in synchronization with Active Directory
- Leverage identity federation through integration with any SAML-based Single Sign On solution (Okta, One Login, Ping Identity, ADFS, Azure AD SSO, etc.) for user onboarding, authentication and management

Benefits:

- Ready integration with existing on-prem/cloud infrastructure
- Keep the user/group list synchronized with the directory service
- Provide easy log on experience for your users with SSO integration
- Automate application passwords usage in development environments

Implement Role-based Access Controls

Details:

- Restrict access to credentials and vault applications based on pre-defined user roles.
- Control application privileges based on roles
- Create custom roles to meet specific requirements

Benefits:

- Central administrators can manage the application without having access to the passwords of other departments
- Optional super-administrator role for emergency access to all passwords

Password policy creation and enforcement

Details:

- Define complexity rules and enforce strong, unique, random passwords
- Set maximum age for passwords and send expiration alerts reminding users to change their passwords

Benefits:

- Eliminate security risks arising due to weak passwords
- Enforce strong password usage discipline across the organization by using the built-in password generator

Track activities with comprehensive audit trails, record sessions

Details:

- Maintain a complete trail of privileged activity across the organization
- Trace actions to specific individuals or to specific accounts
- Real-time notifications upon the occurrence of specific events
- Record and playback privileged sessions launched by users
- Terminate live user sessions on finding suspicious activity

Benefits:

- Quick, precise and comprehensive audit trails
- Culture of accountability for actions
- Track ‘who’ did, ‘what’ and ‘when’
- Administer complete control of user activities
- Optional super-administrator role for emergency access to all passwords

Gain actionable intelligence on privileged access

Details:

- Get actionable intelligence with informative dashboard
- Gain security insights with analytical reports
- Get analytical scores on password strength

Benefits:

- Complete visibility regarding password access, usage
- Assess the strength of stored passwords
- Generate and download detailed reports to prove compliance

Customize the application to meet specific organizational needs

Details:

- Add custom fields for accounts
- Create custom account types
- Create custom user roles with varied permissions
- Switch on and switch off specific features/controls
- Display custom messages on the login page

Benefits:

- Readily meet organization's password-related security requirements
- Customize application features to easily navigate within Securden, and have an intuitive experience

Scalable, enterprise-ready capabilities

Details:

- Highly scalable architecture with provision to deploy multiple application servers in different locations
- In-built high availability mechanism through redundancy for uninterrupted access
- Secure offline access provisions that are protected with passphrases
- Backup options for disaster recovery
- Integration with SSO, ticketing systems and SIEM tools
- Mobile apps for anytime, anywhere access

Benefits:

- Handle password management for different locations with strict access controls and centralized management
- Manage hundreds of thousands of passwords
- Easy integration with enterprise infrastructures
- Obtain actionable insights from the integrated SIEM solution

Secure by design

Details:

- Strong AES-256 encryption standards
- Encrypted data transmission
- Wide range of MFA options and enforcement, with MFA options customizable for different users
- Tamper-proof audit trails
- Real-time alerts to keep a tab on activities
- IP-based access restrictions

Benefits:

- Prevent unauthorized access to passwords
- Lockdown sensitive data and bolster internal controls
- Enforce accountability for actions
- Stay secure and organized
- Prevent users from elevating their own permissions

Prevent malware, and ransomware propagation

Details:

- Remove local admin rights on endpoints and enforce the concept of least privilege
- Elevate applications on-demand for users using the Securden agent
- Enforce Multi factor authentication for all users and selectively enforce MFA methods for different users

Benefits:

- Reduced risk surface as endpoints with least privilege stops malware propagation

Gain visibility and control over Windows dependencies

Details:

- Automatically fetch windows dependencies, scheduled tasks, and services, and manage them from Securden
- Create and enforce password policies and complexity rules for Windows Domain Accounts
- Carry out periodic password resets on Domain accounts and propagate the changes to the respective dependencies and services

Benefits:

- Discover and gain visibility over windows dependencies and services that run in the background
- Ensure password security best practices are followed for Windows Domain/Service accounts

X

Eliminate local admin rights on windows servers and endpoints

Details:

- Identify and track the list of users and groups that are part of the local admin group on computers in the domain
- Remove the local admin privileges of users/groups across all servers and endpoints to make them standard users

Benefits:

- Restrict what applications and software must be used by users in the organization
- Define and control which applications can be run by standard users and prevent malware

X

Control application usage across the organization

Details:

- Add applications and commands and associate application control policies
- Whitelist trusted applications and blacklist malignant ones through centalized control policies
- Allow users to access certain Windows control panel items
- Launch native and thick client applications directly from Securden with custom application launcher

Benefits:

- Allow users to access only the applications, and Windows built-in programs that they require

- Seamless, One-click elevation of applications

- Achieve least privilege across the enterprise and control application usage without impacting enduser experience

- Remove applications from remotely from end-user systems

X

Enforce zero-standing privilege across the enterprise

Details:

- Provision users only with the privileges they require based on their roles and responsibilities

- Continuously monitor who all have administrator privileges. Detect if new local administrator accounts are added

Benefits:

- Eliminate users from having standing privileges to resources

- Allow users to have privileges temporarily only when they need them

X

Ensure least privilege controls even in offline scenarios

Details:

- Allow users in the organization to get approval for applications even when they are offline/disconnected from the network

- Allow users to generate and securely store offline access codes to run applications when offline

- Allow administrators to send users offline access codes which they can utilize to run applications while being standard users

Benefits:

- Ensure least privilege and application controls even when the endpoint is offline or away from the network or when users are working from home

Summary of Security Controls Achieved

- Controlled and monitored access to IT resources
- Improved password security
- 360° visibility over privileged access
- Locked down privileged identities
- Time-restricted privileged access
- Restricted access to vendors and technicians
- Identification of breached passwords
- Protected remote access to IT assets
- Safeguarding against internal/external threats
- Eliminate hard-coded credentials
- Secure Windows service, domain accounts
- Remove local administrator rights across endpoints
- Enforce password policies
- Prevent malware, ransomware propagation