Securden

Unified PAM

Implementation Guide →

Index

← Back to Index

Overview

This document helps security engineers define an internal implementation plan and successfully deploy Unified PAM to align with their business objectives and requirements. Unified PAM takes at most two weeks to deploy directly in your production environment.

Implementation Essentials

To get started with deploying PAM in your organization, you would need to consider a few essential practices:

1. **Discuss business and security requirements**

   Carry out discussions with executives and the security team. For an effective rollout, consult all relevant stakeholders to gather expectations. This may include - executive decision makers (C-Suite), infra operations team, IT teams, security experts, and end users. Meeting these expectations contributes to a successful PAM implementation.

   Discussions with the end user can be of importance as it will help successfully drive adoption of the solution across the organization.

2. **Define objectives of the PAM program**

   Once expectations are gathered from crucial members, you need to define the goals you wish to achieve with the PAM solution. This can be derived based on the security framework your organization has in place now, compliance requirements, newly emerging threats, and more.

Objectives could be something like:

- Satisfying regulations such as NIST, Essential Eight, etc.
- Strengthening overall security posture to secure cyber insurance
- Improve operational efficiency by streamlining privileged access
- Bolster internal controls and prevent identity thefts, malware propagation, and insider exploitation
- Enforcing the Principle of Least Privilege (PoLP) for Users
- Data Protection to comply with GDPR or other requirements

3. List out the success criteria

Have a list of success criteria, aligning them with the overall goals of the PAM project. This helps determine the success rate of your PAM project.

4. Strategize the PAM design and infrastructure

Before diving directly into deployment, it is important to have an implementation strategy in place. This acts as a guideline for the various aspects of implementation – timeline, resources, deliverables etc.

Review current state and define a PAM strategy

The primary objective of PAM is to protect 'superhero' accounts – these are accounts with higher capabilities than a normal user account.

In your infrastructure, these could be - local admin accounts, domain admin accounts, user accounts of a high-level IT personnel, etc. Having an idea of the accounts that exist can help plan your implementation.

← Back to Index

Conduct a thorough assessment of current privileged access management practices, including identifying critical assets and privileged accounts.

In your assessment you may consider the following:

- Existing control policies for access to sensitive assets, governance of 'superhero' (privileged) accounts and management of IT assets.
- Practices and protocols in place for provisioning, automation, gating, etc.
- Protective controls to detect, secure, and monitor access.

In an average, the number of identified accounts that are shared among people could be thrice as much as the number of employees in the organization. Therefore, a planned and steady phase-wise implementation would be the best way to set achievable goals.

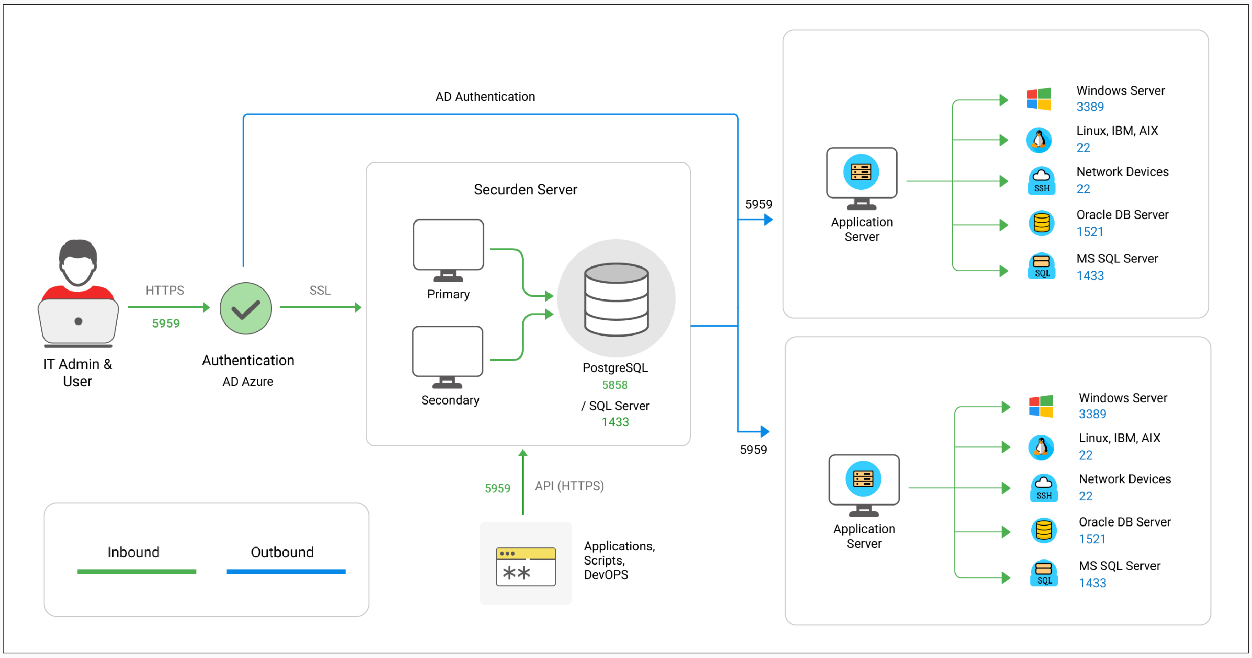
Go over the architecture, requirements and pre-requisites to plan the deployment of Unified PAM.

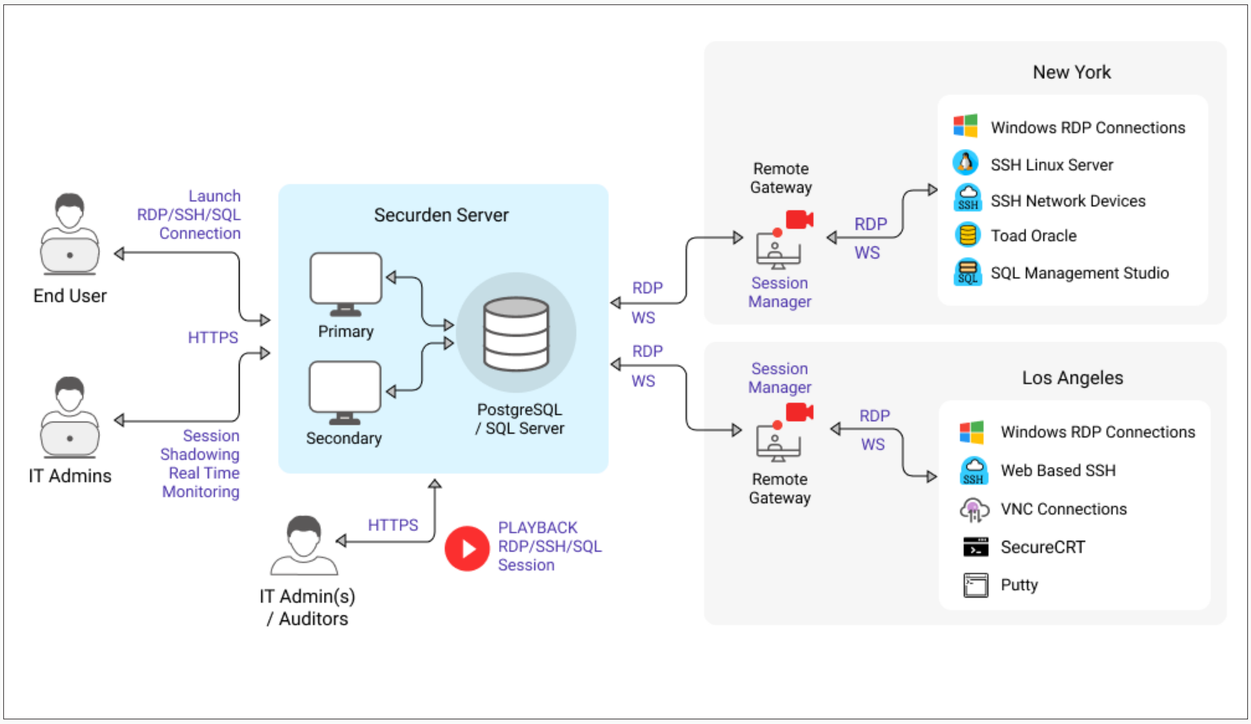
A recap of Securden Unified PAM architecture

Securden Unified PAM is a web-based, on-premise, self-hosted software-only solution available as a binary for installation on Windows. Securden Unified PAM comes as an all-in-one package, you don't require any additional hardware or software for the functioning of the product. It comes with an inbuilt web server and PostgreSQL server as the default RDBMS. Optionally, you can configure MS SQL Server as the backend database.

An installation instance can just have two physical servers (primary and secondary), or multiple application servers as required. The solution runs on a central server connected to a backend database.

The web server handles all the business logic. End-users can connect to the server from their machines using any standard web-browser.



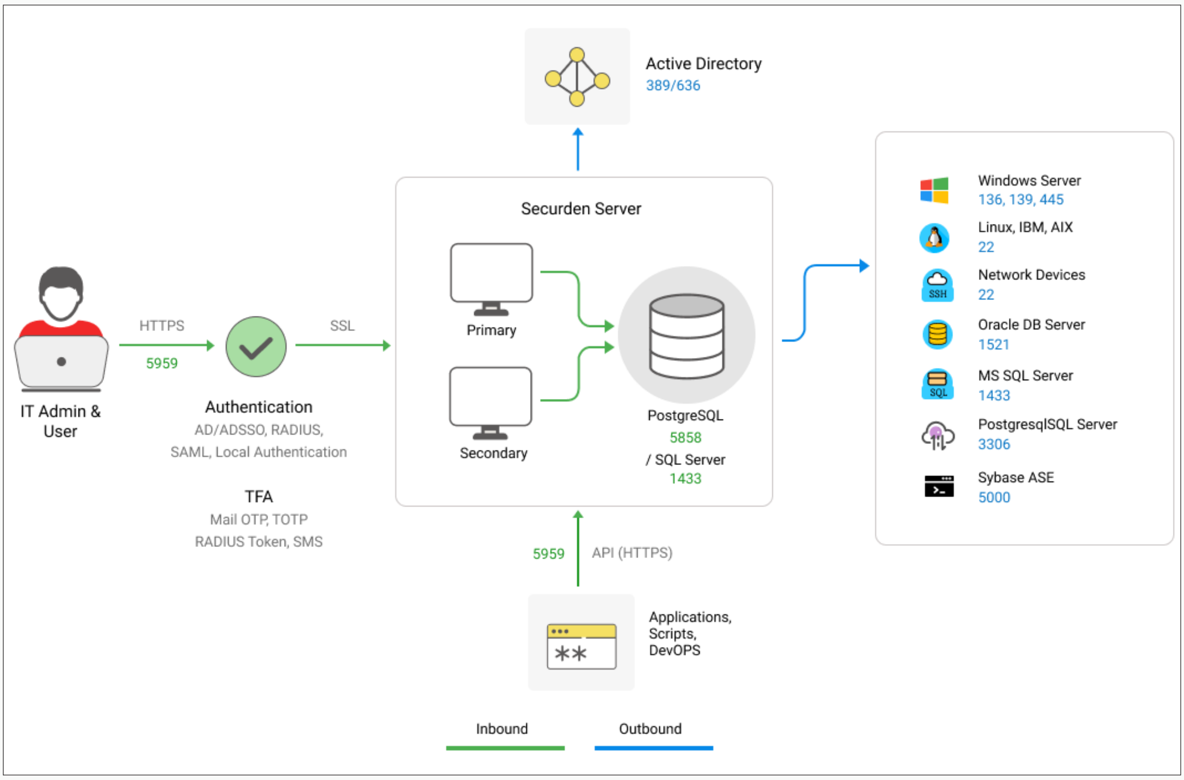


The product stores all sensitive information in a fully encrypted manner in a secure, digital vault. Securden uses AES-256 for encryption. The encryption key is unique to every installation and is automatically generated.

For remote connections, session management and recording, Securden provides the option for a gateway approach. All remote connections from endpoints to target IT resources are routed through the remote gateway.

This approach eliminates the need for direct connectivity between the endpoints and the sensitive IT infrastructure and ensures a higher level of security. The design also proves to be highly scalable, capable of handling a large number of concurrent remote connections.

The remote gateway approach is supported by the option to deploy multiple application servers, which help in handling privileged account management for a distributed network or distributed data center environments from a central installation.



Recommended System Configurations

In order to provide uninterrupted access to privileged credentials, you can configure two application servers (primary and secondary) connected to a common database.

This comes in handy in cases where one application server fails or becomes unresponsive, and the load balancer effectively redirects the incoming traffic to the other active application server. This way, business processes are not interrupted. Application servers can either be two separate physical machines or virtual machines split up from a single physical server.

Please refer to the system configurations below to deploy Unified PAM in your production environment. Any physical or virtual server holding the configurations below is fine.

Unit	Primary Server	Secondary Server	You can use the bundled PostGreSQL as the backend. Optionally, you may use MS SQL server as the backend too.
Memory	16 GB RAM	16 GB RAM	16 GB RAM
HDD	50 GB or more	50 GB or more	50 GB or more
vCPU (Intel or AMD Processors)	4 or more cores	4 or more cores	4 or more cores
OS (Windows Server License)	Windows Server 2016 or above	Windows Server 2016 or above	Windows Server 2016 or above
IP	1 STATIC IP	1 STATIC IP	1 STATIC IP
Quantity	1	1 or more	1
Details	-	For High Availability	Database Server

To facilitate remote connections and support certain remote functionalities across multiple networks, you need to deploy SSM/Gateway Server and API Server.

Remote Gateway (RG) Pre-requisites

You need to deploy either **Securden Session Manager (SSM)** or **Securden Application Server (API Server)** or both on the machine that is going to serve as the gateway. If your requirement is related only to launching remote sessions/session recording, you need to deploy Securden Session Manager alone. If you want to handle remote password resets, you need to associate with the application server. The SSM must be deployed on a Domain Machine.

The requirements for remote gateway (SSM and API Server are as below).

Unit	SSM Server/ Remote Gateway Server	API Server
Memory	16 GB RAM	16 GB RAM
HDD	50 GB or more	50 GB or more
vCPU (Intel or AMD Processors)	4 or more cores	4 or more cores
OS (Windows Server License)	Windows Server 2016	Windows Server 2016 or above
IP	1 STATIC IP	1 STATIC IP
Quantity	1 or more	1
Details	Terminal Server	To support remote functionalities (such as remote password reset, remote password verification, accounts discovery, and more).

Securden Agent Requirements - To be installed on machines running Windows 7 or above as an .msi file (Windows installer)

Terminal Licenses - MS Remote Desktop Service (RDS) License (In case of using Remote Gateway Server)

How RDS works in Securden - A single domain account is used to log in to the remote gateway devices, which will then connect to all the target devices.

Even if multiple users need to launch a connection, they would use the same domain account to log in to the gateway server. From this remote gateway server, their actual user account will be used to connect to the target devices.

Based on the above scenario, you need to explore the appropriate licensing mechanism (one user CAL or multiple user CALs) with Microsoft and buy the licensing from them accordingly. Since it is a third-party licensing, we are not in a position to recommend or comment on the licensing part.

The following knowledge base article of Microsoft throws some light on this:

https://learn.microsoft.com/en-us/windows-server/remote/remote-desktop-services/rds-client-access-license

Deployment Prerequisites

- **Firewall and Port Settings -** Refer to the Ports section for full details.

- **Domain Settings -** A domain service account needs to be created in your Active Directory domain controller, that has domain admin rights or local admin rights for the Unified PAM server and for the remote privileged systems you would like to manage.

- **SMTP -** An external mail server needs to be set up and integrated with Unified PAM for users to receive email notifications.

- **DNS -** Public DNS Record needs to be created, one for Securden PAM, the other for SSM Gateway (to maintain domain details of the servers).

- **SSL Certificate -** A public SSL certificate needs to be installed on the application server to authenticate and encrypt connections between user devices and the Unified PAM server.

- **Service Account for Remote Operations -** Organizations would be required to create a dedicated service account with domain admin privileges that will be used by Securden to carry out various privileged operations such as - discovering domain computers, managing domain accounts, and more.

Ports Used

Securden Unified PAM uses a range of ports to ensure secure communication. The following are the TCP (Transmission Control Protocol) ports used in Securden PAM.

- By default, Securden Unified PAM comes with PostgreSQL server as the default RDBMS. Optionally, you can use MS SQL Server as the backend database. Port 5858 connects all the primary, secondary, and application servers to the PostgreSQL database. The port 1433 connects the product servers (primary and application servers) to the SQL server.

- End-users connect to the User Interface of the product using port 5959. Administrators can choose to change this port to 443 or any other port if required.

- When Securden Session Manager is employed, remote desktop sessions are launched through port 3389. Administrators can also define custom ports and users can use those specified references for SSH tunnelling.

- Web remote connections use the port 5622 for SSH and 5626 for RDP.

Port Name	Source	Destination	Port (TCP)	Details
PostgreSQL Database Port	Primary, Secondary, and all Application Servers	PostgreSQL Server	5858	-
MS SQL Database Port	Primary and Application Servers	MS SQL Server	1433	-
Securden Server Port	To all Users (End Machines), Agents, and Secondary Servers	Primary	5959 (Web-Port)	For all servers this port can be changed if required
		Secondary		
SSM Port (Inbound)	All Client machines	SSM Server installed machine(s)	3389 (RDP Port)	3389 is opened on the SSM for all client machines
SSM Port (Outbound)	SSM Server installed machine(s)	To all Target Machines		3389 is opened to all target machines from the SSM Server
Web - SSH	To all Users (End Machines)	On all application servers	5622	-
Web - RDP			5626	
SMTP Sever Port (Mail Server Port)	-	-	587	TLS
			465	SSL

Proxy Server Port - This port must be open if your organization makes use of a proxy server to regulate internet traffic. Navigate to **Admin** >> **General** >> **Proxy Server Settings** and configure the port details to facilitate Securden to connect to the internet.

AD Port is used for the account discovery purpose while integrating with the Active Directory.

RADIUS Server Port - You can integrate the RADIUS server or any RADIUS-compliant two-factor authentication system like OneSpan Digipass, RSA SecurID, etc., for the second-factor authentication. Navigate to **Admin** >> **Authentication** >> **Two-Factor Authentication**. Click the configure option on **RADIUS Authentication**. In the **RADIUS Server Settings** page that opens up, you may configure the details of the authentication port.

Port Name	Source	Destination	Port (TCP)	Details
Proxy Server Port	Primary Server	Proxy Server	Based on your settings	**If needed**
AD (DC) Port	Primary/application server	AD DC	636	SSL/TLS
	-	-	339	If there is no SSL
RADIUS Server Port	-	-	1812	**If needed**
Azure AD	Primary/application server	Azure AD	Graph API	**If needed**
Breached Password Identification	Primary Server (Requires internet connection)	-	API	https://api.pwned-passwords.com/
Other Ports	-	-	-	Check your integration port requirements

Implementation Phases

Implementing a Privileged Access Management (PAM) solution requires careful planning and execution to ensure a smooth deployment while minimizing disruptions to operations. Once you have gone through the requirements and pre-requisites - you can proceed with implementation.

You can make use of the suggested phases of implementation.

Phase 1: Planning, preparation and information gathering

During this phase the Securden technical team will discuss with the stakeholders to gather information regarding the various applications in scope. All the prerequisites will be identified and shared with the customer during this phase. Additionally, cybersecurity gaps that exist in the organization will be identified. Corrective measures will be suggested to the customer.

- Establish project scope, objectives, and timelines.
- Conduct a risk assessment and gap analysis.
- Secure necessary budget and resources.

Phase 2: Implementation

During this phase, the Securden team will carry out the implementation of the product. Implementation of the Securden Server and configurations related to Unified PAM will be carried out.

Once the configurations are completed, the Securden team will work with individual application owners to assign the right set of access for various administrators, users, and teams.

Any other fine-tuning required will be covered during this Phase.

- Design architecture and deployment model.
- Develop policies and procedures for PAM implementation.
- Deploy Unified PAM in a controlled environment.
- Test functionality and user experience.
- Gather feedback from pilot users.

The implementation phase will broadly cover the following activities:

It's important to note that the timeline may vary depending on the size and complexity of the organization types of IT assets, network segmentation, access patterns, Unified PAM requirements and the availability of resources.

The following represents a typical implementation schedule. Regular communication and collaboration between stakeholders, including IT teams, security teams, and business units, are essential throughout the deployment process to ensure alignment with business goals and successful implementation of the PAM solution.

Plan	Details
Day 1,2	Kick-off Discussion - Discuss business and security requirements. Deployment plan, timeline and the detailed steps involved. Identify success criteria and stakeholders for implementation.
Day 3,4,5	**General Settings**
	Mail Server Settings
	Proxy Server Settings
	Securden Server Connectivity & Starting the PAM Server
	User Onboarding
	Integration with AD/Azure AD/LDAP for user provisioning and authentication
	User Import Options
	Add Users Manually
	Assigning Roles to Users
	Custom Roles
	User Reports

Plan	Details
Day 3,4,5	User Groups
	Import Groups Options
	Group Settings
	Basic Configurations
	Integration with multiple AD domains / Azure AD
	Integration with SAML 2.0 based Single Sign On Solutions
	Multi Factor Authentication Setup
Day 6,7,8	**Account Management**
	Automatic discovery of IT assets and privileged accounts
	Importing Accounts - Flexible import options to build inventory
	Secure, Centralized Repository of Accounts
	Storing SSH keys, documents, files, images, digital identities
	Organizing data as folders for bulk management
	Optional personal vault within organization's vault
	Manage Shared Admin Passwords
	Granular Sharing and Controls
	Secure sharing with third-parties
	Option to allow access without showing the password
	Periodically synchronizing assets and accounts
	Windows service accounts and dependencies management
	Password Management
	Automated, periodic remote password resets
	Self-supporting any SSH-enabled device for password resets
	Password release control workflow for just-in-time access
	Password policy creation and enforcement
	Role based access controls
	Remote Access and Session Management
	Support for one-click remote session initiation - RDP, SSH, SQL, HTTPS etc.
	Web-based remote connection launching
	Remote connection through native tools for RDP, SSH, SQL
	Session access without disclosing password

Plan	Details
Day 6,7,8	Session Recording, Playback, Live Remote Session Monitoring, Concurrency Controls
	Custom connector for launching any application - Custom Application Launcher
	Remote gateways to manage distributed networks
	Application-to-Application Password Management
	APIs for managing machine identities, application identities, secrets, keys
	Eliminate embedded credentials on script files, applications
	Privilege Elevation & Delegation
	Remove admin rights across Windows endpoints, servers
	Configure Applications and commands for privilege elevation
	Elevate applications for standard users on-demand
	Configure policy-based application control
	Provision for granting temporary admin rights
	Support for command filtering and controls on Unix
	Technician Access - (/Third Party Access)
Day 9,10,11	**Audit, Reports and Notifications**
	Explore comprehensive auditing & reporting
	Searchable text-based audit trails
	Filtering audit trails to create custom reports
	User access and activity reports
	Policy compliance reports
	Password expiration reports
	Micro reports for specific requirements
	Breached passwords identification and notification
	Password security analysis report
	Provision to trigger automated follow-up actions upon events
	Password event notifications (real-time and periodic)
	Advanced Settings, High Availability, and Architecture
	On-prem, private cloud deployments
	Distributed server deployment architecture

Plan	Details
Day 9,10,11	Database backup for disaster recovery
	High-availability
	Option to use Always-on MS SQL clusters, Amazon Aurora
	Best Practices, Security Hardening, Miscellaneous
	Configure ticketing system integration
	Configure cloud storage integration
	Provision web-based access to end users
	Enforce security settings and controls (IP restrictions, enabling/disabling access)
	Provision for restricted access over the internet
	Explore browser extensions
	Cross-platform access
	Mobile Apps
	Secure offline access
Day 12	**User Acceptance Testing**
Day 13, 14	**Delivery and closure**

Phase 3: Monitoring and troubleshooting

During this phase, Securden will familiarize the team with product components and their uses. The customer team will be walked through the architecture configured for the customer. We will also explain various use cases, day-to-day handling, best practices approach, and troubleshooting tips. The training will be delivered in person and cost estimates have been provided as part of the commercial proposal.

- Implement monitoring and reporting mechanisms.
- Monitor Unified PAM for performance and security issues.
- Conduct regular audits and reviews with users.
- Track all issues and gather troubleshooting material
- Continuously update policies and procedures based on lessons learned.

Phase 4: Project Closure, Documentation

The project closing phase will involve gathering insights, checking implementation success based on the success criteria defined, handing over the project and gathering documentation.

- Gather security insights based on audits
- Deployment architecture and configuration documents
- Collect product guides and manuals

With all phases of implementation complete, you can track your progress and inform the executives of the program's success. While implementation is complete with these four phases, it is important to review your PAM objectives, and keep in touch with the Securden team to align with future goals.

When set up well, Unified PAM provides holistic access security for all your sensitive data and IT assets. It regulates privileged access, protects sensitive accounts, automates repetitive tasks and best practices, enforces policies and controls, safeguards your infrastructure from internal/external threats, and mitigates security risks. All while keeping operational efficiency high.

Securden

Unified PAM

Administrator Guide →

Note: You may refer to the **PAM Admin Guide** to know about the product configurations, troubleshooting steps, and other features to start working on the solution.