Securden

Unified PAM (SaaS) Implementation Guide

Securden

Unified PAM (SaaS)

Implementation Guide

Table of Contents

Overview

This document helps security engineers define an internal implementation plan and successfully deploy Unified PAM (Cloud) to align with their business objectives and requirements. The cloud edition of Unified PAM takes at most 7 days to fully implement.

Implementation Essentials

To get started with deploying Unified PAM (SaaS) 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 (SaaS) 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, NIS2, 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.

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.

Review who needs access

Privileged access accounts fall into one of two categories, human and non-human. Determine which employees, applications and systems actually need access to your privileged accounts. Tighter restrictions on access can help reduce the risk of a ransomware and malware attack.

Consider if third-party contractors have access and whether they need it. Third-party contractors that need access to privileged accounts can be one of the highest risks

because you don’t have full control over how they access and manage privileged accounts or where they store the credentials.

Many breaches in recent years have involved stolen or hacked contractor access points that led to valuable and sensitive data.

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.

Securden Unified PAM: Cloud Architecture

Securden Unified PAM Cloud Edition is a complete privileged access management solution that is available as a SaaS offering. Enterprise-grade features like data backup, database replication, high availability, and disaster recovery are built into the product.

With the cloud solution, customers don't need to worry about managing infrastructure, updates, or scalability; Securden handles all of these aspects.

The product integrates with any LDAP-compliant directory service (including AD), Azure AD, and single-sign-on (SSO) solutions for user management and authentication and with two-factor authentication providers like TOTP authenticator, RSA SecurID, Email to SMS, Duo, YubiKey, and any RADIUS-based MFA.

Encryption

Securden Unified PAM as a service is a cloud-hosted solution. The encryption is unique to each customer, and the encryption keys are managed using Amazon KMS along with AWS HSM for cryptographic operations. Securden partners with AWS data centers to provide Unified PAM as a Service. The data centers are HIPAA and PDPA compliant.

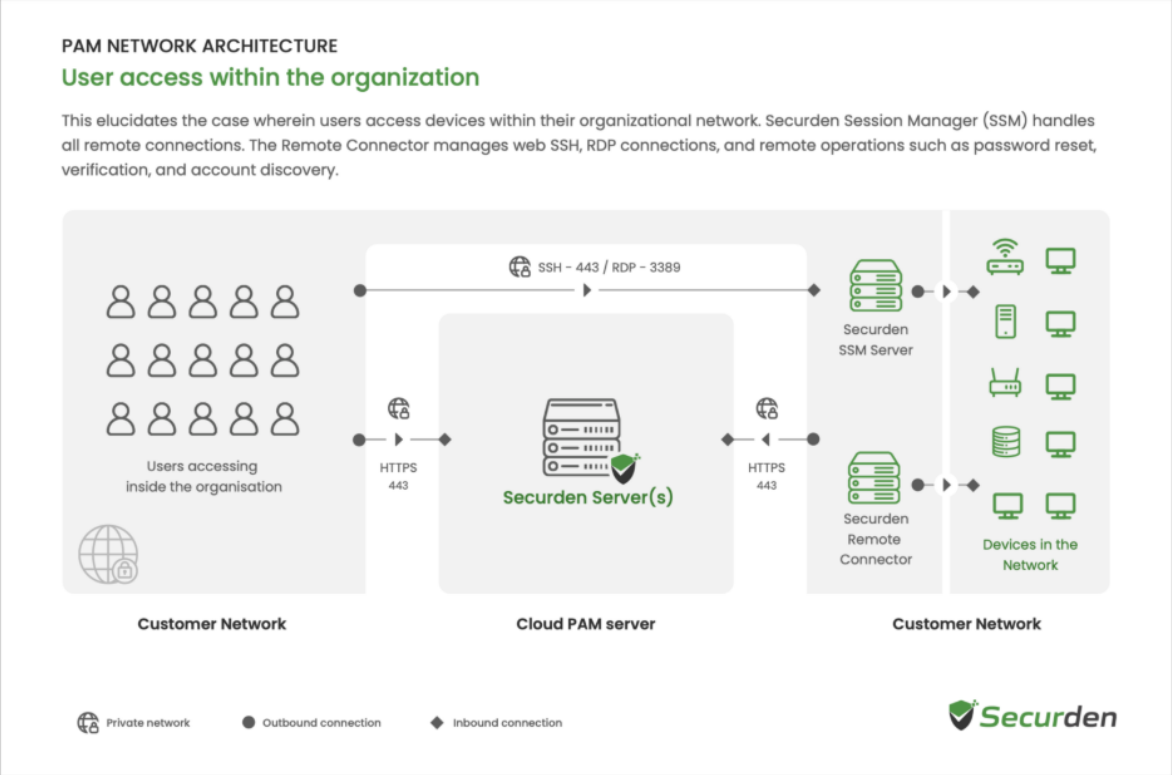
The credential repository is implemented as strictly access-controlled and securely encrypted database columns in the backend database. The application has all the business logic that drives this, right from generating unique encryption keys. Securden Unified PAM is built upon a secure framework and ensures sensitive data stays secure

when stored in the database and while in transit.

The PAM architecture for different types of organization's existing IT infrastructure is explained below with three use cases.

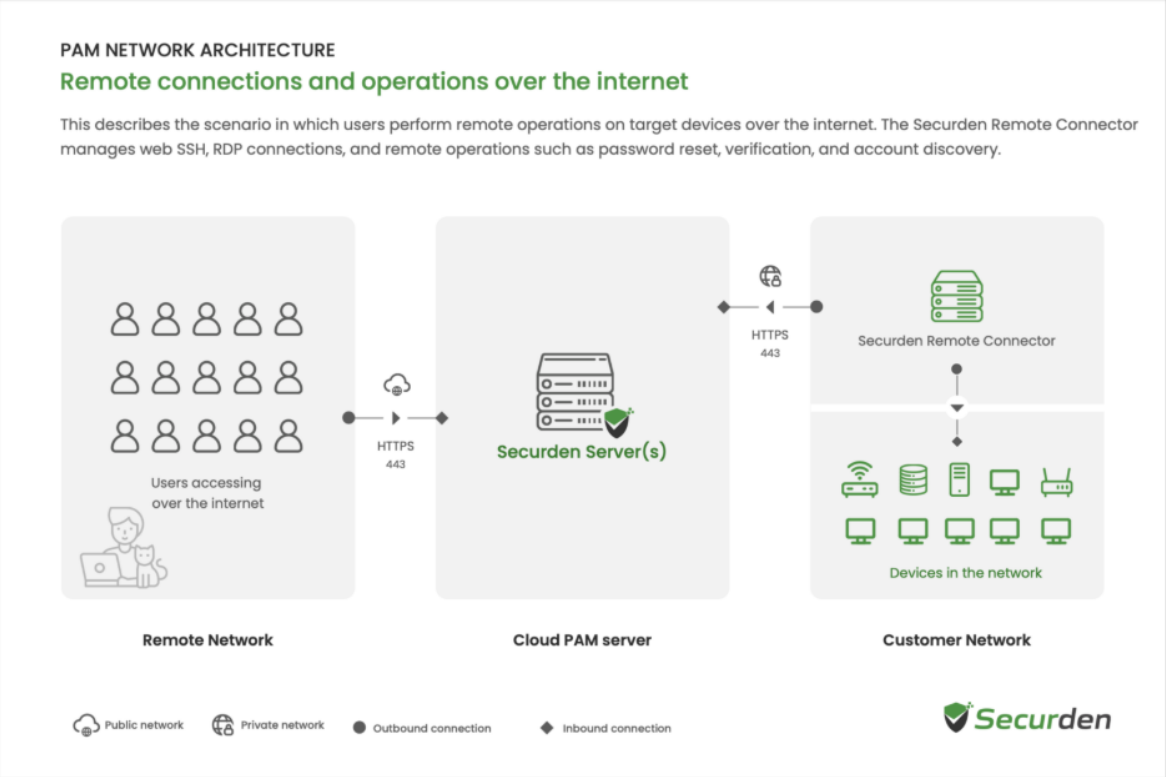
Case 01: User access within the network

This architecture diagram is applicable for the users who access assets within their organizational network. The Securden Remote Connector manages remote operations such as password reset, verification and privileged account discovery while the Securden Session Manager handles all remote connections to the devices.



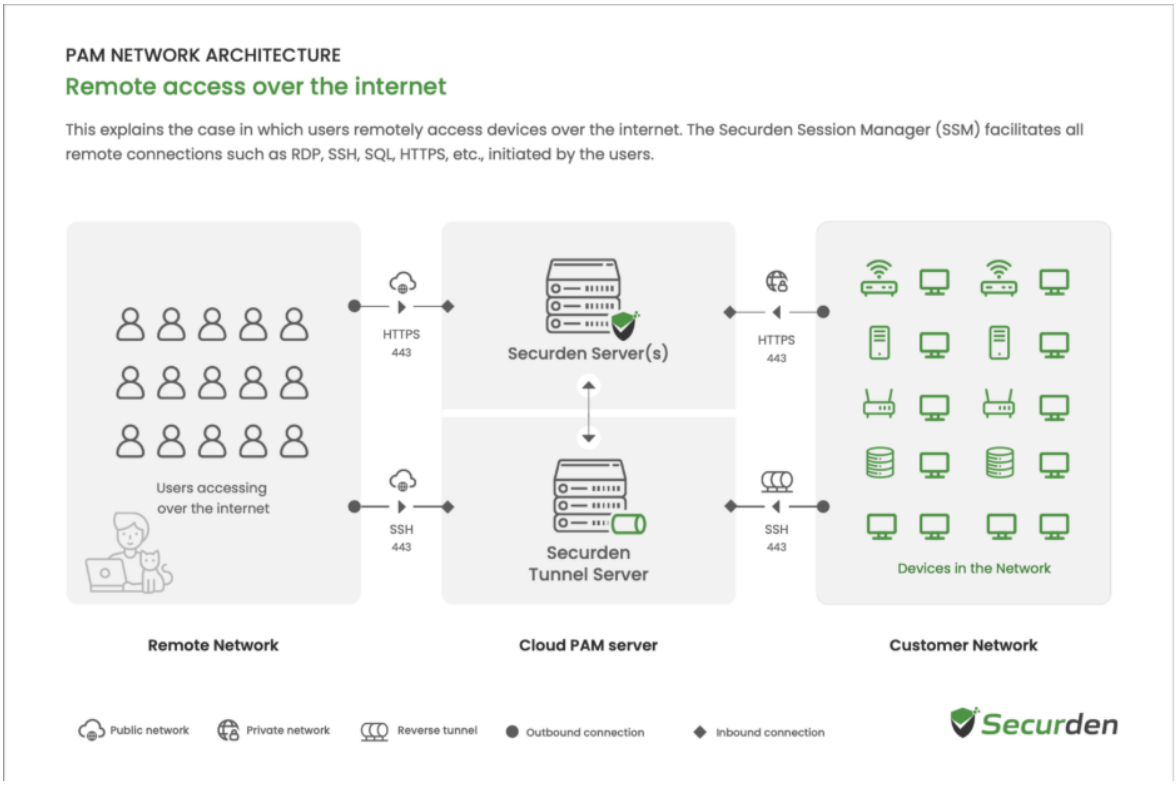
Case 02: Remote connections and operations over the internet

This architecture diagram applies for all users accessing devices within the organizational network from remote devices over the internet. Securden Remote Connector handles remote connections such as SSH and RDP along with remote operations such password reset, verification, and privileged account discovery.



Case 03: Remote access over the internet

This architecture diagram below depicts a case where remote connections are routed through a reverse tunnel for encrypted data transfer. The users connect to the Securden Server over the internet to initiate remote connections. The Securden Session Manager (SSM) installed in the device-network facilitates all remote connections such as RDP, SSH, SQL, HTTPS, etc., initiated by the users.



SSM & Remote Connector Pre-requisites

You need to deploy the Securden Session Manager (SSM) and Securden Remote Connector or both in a device that is part of your network. If your requirement is related only to launching remote sessions/session recording, you need to deploy Securden Session Manager alone (On a domain machine). If you want to handle remote password resets, you need to associate a Remote Connector.

The requirements for SSM and Remote Connector are as below.

Unit	Memory	HDD	vCPU (Intel or AMD Processors)	OS (Windows Server License)	IP	Quantity	Details
SSM Server	16 GB RAM	50 GB or more	4 or more cores	Windows Server 2016	1 STATIC IP	1 or More	Terminal Server

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

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

Endpoint Privilege Management Pre-requisites

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

Deployment Prerequisites

- Firewall and Port Settings – Refer to the Ports section for full details.
- DNS – Public DNS Record needs to be created the other for SSM Gateway (to maintain domain details of the servers).

- 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 - Cloud uses a few ports to ensure secure communication. The following are the TCP (Transmission Control Protocol) ports used in Securden PAM.

- End-users connect to the User Interface of the product using the web access URL. (Port: 443)
- When Securden Session Manager (SSM) 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.

Port Name	Source	Destination	Port (TCP)	Details
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 (RDP Port)	3389 is opened to all target machines from the SSM Server

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, you may configure the details of the authentication port.

AD (DC) Port	Primary/application server	AD DC	636	SSL/TLS
AD (DC) Port			339	If there is no SSL

AD (DC) Port	Primary/application server	AD DC	636	SSL/TLS
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.pwnedpasswords.com/

Phases of Implementation

Implementing a Cloud 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 configuration 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.

Proposed Timeline	Detailed Description
DAY 1	Kick-off Discussion - Discuss business and security requirements. Deployment plan, timeline and the detailed steps involved. Identify success criteria and stakeholders for implementation.
	General Settings
	Securden Server Connectivity - Connecting to the cloud hosted interface
	Remote Connector Deployment (To connect and manage AD)
	User Onboarding
	Integration with AD/Azure AD for user provisioning, authentication
	User Import Options - Import from File, KeePass, LastPass
	Add Users Manually - Local users
	Assigning Roles to Users
	Custom User Roles

Proposed Timeline	Detailed Description
DAY 1	User Reports
	User Groups
	Import Groups Options
	Group Settings
	Vendor Onboarding (If Included)
	Create Vendor Invitations for Self-Registration
	Add Vendor Users Manually
	Associate Accounts, Assets with vendors
	Basic Configurations
	Integration with multiple AD / Azure AD domains
	Integration with SAML 2.0 based Single Sign On Solutions
	Multi Factor Authentication Setup
DAY 2, 3 and 4	Privileged 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

Proposed Timeline	Detailed Description
DAY 2, 3 and 4	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 for devices, accounts
	Self-supporting any SSH-enabled device for password resets
	Password release control workflow for just-in-time access (JIT Access)
	Enforce valid reason (justification) to access passwords and accounts
	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
	Time-limited access to remote resources
	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

Proposed Timeline	Detailed Description
DAY 2, 3 and 4	Privilege Elevation & Delegation
	Remove admin rights across Windows endpoints, servers
	Configure Applications and commands for privilege elevation
	Elevate applications for standard users on-demand
	Policy-based application control
	Provision for granting temporary admin rights
	Support for command filtering and controls on Unix
	Technician Access - (/Third Party Access)
DAY 4, 5 and 6	Audit, Reports and Notifications
	Comprehensive auditing & reporting
	Searchable text-based audit trails
	Send audit logs to SIEM tools for SOC
	Filtering audit trails to create custom reports
	User access and activity reports
	Policy compliance reports
	Password expiration reports
	Configure event notifications
	Micro reports for specific requirements
	Breached passwords identification and notification
	Password security analysis report
	Provision to trigger automated follow-up actions upon events
	Download specific audit trails and reports

Proposed Timeline	Detailed Description
DAY 4, 5 and 6	Password event notifications (real-time and periodic)
	Advanced Settings and Architecture
	Simple and scalable architecture with built-in database
	Distributed server deployment architecture
	Best Practices, Security Hardening, Miscellaneous
	Web-based access to end users
	Security settings and controls (IP restrictions, enabling/disabling access)
	Provision for restricted access over the internet
	Browser extensions
	Cross-platform access
	Mobile and Desktop Apps
	File Transfer
	User Behavior Analytics
	Secure offline access
Day 7	User Acceptance Testing
Day 8	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 (Cloud) 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.