

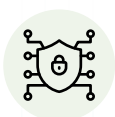


Unified PAM

— MSP Edition —

Privileged Access Management for Managed Service Providers

A unified platform for MSPs to securely manage privileged identities, credentials, sessions, endpoints, and access across multiple customer organizations while maintaining client-level segregation, access governance, and administrative control.



Multi-Tenant PAM Management

Manage privileged access across customer environments with tenant-specific controls, centralized administration and data separation.



Privileged Access Security

Protect privileged accounts across customer environments with password vaulting, access control, session monitoring and auditing.



Least Privilege & Endpoint Control

Control endpoint privileges across customer environments with application control, privilege elevation, technician access and least privilege.



Product Datasheet

On-Premises

For enterprise security, IT operations, compliance, and infrastructure leadership teams.

Product Overview

Platform Goal	MSP Operating Model	Primary Security Outcome
Secure and control privileged access across multiple customer organizations through a centralized MSP platform.	Centrally manage multiple client organizations while maintaining client-specific controls and segregated data.	Reduce privileged access risk, enforce least privilege, secure remote administration, and maintain auditable access across customer environments.

Securden Unified PAM MSP enables managed service providers to centrally secure, manage, and monitor privileged access across multiple customer environments through a multi-tenant architecture. It combines privileged credential management, privileged session management, endpoint privilege management, secure remote access, Just-in-Time access, auditing, and related privileged access controls within a centralized MSP architecture.

MSPs can centrally manage customer organizations while maintaining client-specific administration, access policies, and data segregation.

Core Capabilities

Capability Area	Technical Functionality
Enterprise Password Management	Centralized credential vault; controlled sharing; automated rotation of administrator, service-account, and shared-account passwords, and SSH keys. Supports credential import from a standard CSV, XLSX, KeePass, CyberArk, Keeper, and Delinea.
Privileged Account and Session Management	Discovery of privileged accounts across Windows, Linux, macOS, databases, SSH devices, network devices, virtual machines, services, scheduled tasks, and IIS application pools. Supports secure RDP, SSH, and SQL sessions with monitoring, recording, and playback.
Endpoint Privilege Management	Removal of local administrator rights, granular application control, just-in-time elevation and least-privilege enforcement.

Capability Area	Technical Functionality
Self-Service Password Reset	User-initiated password reset and account unlock for Active Directory and Microsoft Entra ID environments.
DevOps Secrets Management	Management of API keys, tokens, service accounts, application credentials, CI/CD secrets, SDK and CLI integrations, REST API access, and secrets used across DevOps pipelines.
Multi-Client PAM Administration	Centrally manage privileged access across multiple customer organizations with client-specific administration, roles, policies, feature scopes, and segregated data.
Technician Access	Provide controlled technician access to managed endpoints and control which applications technicians are permitted to elevate during their access sessions.
Just-in-Time	Grant time-limited access to passwords and remote connections through request-and-approval workflows. Automatically revoke access when the approved duration expires.

Architecture and Deployment

Area	Details
Server Operating System	Windows Server 2019 or later.
Installation Package	Single binary installer with bundled components and database.
Backend Database	PostgreSQL bundled by default; Microsoft SQL Server supported as an optional backend.
Database Selection	Database is chosen at install. Migration between databases is supported through Securden support.
System Sizing	4+ cores, 16 GB RAM, and 50 GB disk per application server. Additional sizing may be required based on deployment scale and workload.

Area	Details
MSP Deployment Model	Support fully managed and co-managed models, allowing MSPs to centrally manage privileged access or share administration with client organizations.
Agentless Operations	Agentless for discovery, rotation, and session brokering.
Client Organizations	Centrally create and manage multiple customer organizations from the MSP platform.
Client Data Segregation	Segregate customer data so each client organization's privileged access data remains isolated from other clients.
Flexible Client Management	Host, co-manage, or fully manage privileged access for customer organizations.
Client Feature Controls	Use custom client scopes to control which PAM capabilities are available to individual customer organizations.
MSP-to-Client Administrator Assignment	Assign specific MSP administrators, user groups, or client-specific management roles to designated client organizations.
Client-Side Remote Connector	Deploy a lightweight connector within each client network to establish outbound-only connectivity with the MSP-hosted PAM server and securely route remote operations.
Shared Remote Gateway	Deploy a centralized MSP Remote Gateway to broker privileged remote sessions and share it across multiple customer organizations.

Security Architecture

MSP Security Architecture

MSP Security Area	Technical Functionality
Vault Model	Dedicated central server connected to a backend database; server handles business logic and users connect through a standard web browser.

MSP Security Area	Technical Functionality
Data Encryption	Sensitive vault data is encrypted at the application level using AES-256 before being stored in the database.
Encryption Key Management	Each installation uses an automatically generated unique random installation key that must be kept separate from encrypted data and made available only during vault startup.
Database Protection	Database accepts secure connections; localhost-only access by default and specific IP allow-listing for high-availability configurations.
Data Integrity	Encrypted data cannot be decrypted without the installation key, even if the database is exfiltrated.
Client Data Segregation	Segregate privileged access data between customer organizations so each client's data remains isolated from other managed clients.
Client-Specific Administration	Define client-specific administrative roles, permissions, and management responsibilities independently for each customer organization.
Centralized Audit Visibility	Provide MSP administrators with centralized visibility into privileged access and administrative activity across managed customer organizations while maintaining client-level segregation.

Security Controls

Security Control	Details
Credential Encryption	AES-256 encryption.
Encryption Key Management	Per-installation encryption key stored separately from encrypted database; HSM support available.
FIPS Mode	FIPS-compliant mode available.
Certificate Handling	Self-signed certificate by default; CA-signed certificates supported.

Security Control	Details
Breached Credential Monitoring	Stored credentials checked against known breach data; requires internet connectivity.
Certifications and Testing	ISO/IEC 27001, SOC 2 Type II, GDPR certified, and periodic third-party penetration testing.
Access Governance	Granular RBAC, credential access policies, request-release workflows, emergency access controls, and just-in-time access.
Passwordless Privileged Use	Access to privileged systems without revealing passwords to users.
Session Auditability	Audit trails for privileged credential use, remote sessions, and administrative activity.
MSP Administrative Access Control	Apply granular restrictions to MSP administrators, technicians, and client-side IT teams based on assigned roles and client organizations.
Client-Specific Access Policies	Define policies and access controls independently for different client organizations based on their security and access governance requirements.
Concurrency Controls	Allow controlled concurrent privileged access while maintaining granular permissions and activity tracking.

MSP Privileged Access Control Design

Control Layer	Technical Detail
Primary Authentication	Vault access can be controlled through LDAP-compliant directory services such as Active Directory and Microsoft Entra ID, SAML-based SSO, RADIUS authentication, smart card authentication, or native local authentication.
Directory-Based Authentication	When directory authentication is used, the vault authenticates through the configured directory and does not store directory user passwords.

Control Layer	Technical Detail
User Lifecycle	Directory integrations support user onboarding, offboarding, authentication, and access provisioning workflows.
Second Factor	Supports MFA through any TOTP authenticator, Securden Authenticator, email OTP, RADIUS-based MFA, Duo Security, RSA SecurID and YubiKey. Securden also supports FIDO2 and WebAuthn-based passkeys for secure, passwordless login.
Access Policies	Granular role-based access controls, request-release workflows, just-in-time access, and passwordless sessions limit credential exposure.
Tenant-Level Access Scope	Enforce tenant-level access restrictions so MSP administrators, technicians, or client-side IT teams can access only the client organizations and data they are permitted to manage.
Client-Specific Access Controls	Maintain client-specific roles, access permissions, policies, and approval controls based on individual customer requirements.

Identity, MFA, and Integration Support

Integration Area	Supported Options
Primary Authentication	Local accounts, Active Directory, Microsoft Entra ID, LDAP, and RADIUS.
SSO	SAML 2.0 support for Okta, Microsoft Entra ID, ADFS, OneLogin, Ping Identity, Google Workspace, and other SAML identity providers.
MFA	TOTP apps such as Google Authenticator and Microsoft Authenticator, Securden Authenticator, Duo Security, RSA SecurID, YubiKey, email OTP and RADIUS-based MFA.
Smart Card Authentication	Supported for on-premises deployments.
RBAC	Predefined and custom roles.
Supported Browsers	Chrome, Edge, Firefox, and Safari.

Integration Area	Supported Options
Client Applications	Web browser; desktop apps for Windows, macOS, and Linux; iOS and Android apps; and browser extensions for Chrome, Firefox, Edge and Safari.
API Access	REST API with token-based authentication for credential retrieval and management. A token generated by the MSP can be reused to access APIs for individual client organizations.
Client-Specific MFA	Configure different MFA solutions for individual client organizations based on customer requirements. This includes TOTP apps such as Google Authenticator and Microsoft Authenticator, Securden Authenticator, Duo Security, RSA SecurID, YubiKey, email OTP, and RADIUS-based MFA.

Product Specifications Snapshot

Specification	Details
Supported Access Types	Privileged account passwords, shared administrator accounts, service accounts, SSH keys, machine identities, API keys, tokens, application credentials, CI/CD secrets, remote sessions and endpoint privileges.
Remote Session Protocols	RDP, SSH, and SQL sessions (both browser-launched and native tools) with access without password disclosure, session monitoring, recording, and playback.
Enterprise Integrations	Active Directory, Microsoft Entra ID, LDAP, Google Workspace, SAML SSO, SIEM, ticketing systems, MFA providers, SDKs, CLI access, and APIs.
Endpoint Controls	Removal of local administrator rights, application control, on-demand elevation for standard users, temporary administrator rights, and least-privilege enforcement.
MSP Capabilities	Multi-tenant architecture for managed service providers, with data segregation and client-specific administration.

Specification	Details
Audit and Reporting	Visibility into who has access to what, privileged activity tracking, password hygiene monitoring, access reports, and compliance support.
MSP-to-Client Administration Models	Support fully managed and co-managed privileged access service models for client organizations.

Discovery and Operations

Operational Area	Details
Account Discovery	Windows, Linux, macOS, databases, network devices, cloud applications, SSH-enabled devices, virtual machines, services, scheduled tasks, and IIS application pools.
Credential Import	Standard CSV, XLSX, KeePass, Keeper, CyberArk, Delinea.
Automated Rotation	Rotation scheduled per folder or policy. Dependent services, scheduled tasks, and IIS application pools are updated as part of the same rotation.
Remote Connection Types	RDP, SSH, and SQL through web-based and native client access.
Session Recording	RDP, SSH, and SQL recording; requires remote gateway; enabled globally and then per account or folder.
Emergency Access	Configurable designated users, maximum duration, and release delay.
Client Onboarding	Centrally onboard and manage customer organizations, including bulk client import where supported.
Centralized Audit Visibility	Review privileged account activity and MSP administrative actions across managed client organizations.

Scale and Resilience

Resilience	Details
High Availability	Secondary application server with automatic failover; read-only database replica on a separate subnet. Encrypted HTML backup.
Database Clustering	SQL clusters supported with Microsoft SQL Server backend.
Disaster Recovery	Scheduled full database backup to remote destination; minimum hourly interval.
Offline Access	Offline access through the desktop application, or an encrypted HTML export protected by a passphrase.
Distributed Architecture	Application servers and remote gateways deployable per network.

Commercial Notes

Commercial Area	Details
Endpoint Privilege Management	EPM module included. Per-endpoint agent licenses sold separately.
Self-Service Password Reset	Self-Service Password Reset user licenses purchased separately.
Non-Production Environments	No separate license required for test, staging, or DR instances.
Support	24x5 standard support; 24x7 premium support.
Upgrade Cadence	Minor monthly releases; major quarterly releases.
Free Trial	30 days; no credit card required.

Commercial Area	Details
Licensing Model	Licensed per user, based on the number of users added to the Unified PAM: MSP Edition platform, regardless of the number of client organizations managed. There is no limit on the number of client organizations or tenants; the number of users that can be added is determined by the purchased license count.

Common Use Cases

Use Case	Description
Credential Governance	Consolidating and rotating privileged credentials across Windows, Linux, macOS, databases, network devices, applications, and cloud infrastructure.
Privileged Remote Access	Providing secure privileged remote access while recording and auditing all sessions.
Endpoint Least Privilege	Removing local administrator rights and enabling just-in-time privilege elevation for standard users.
DevOps Secrets	Reducing risks from hard-coded secrets in DevOps pipelines and application environments.
Multi-Client Privileged Access Management	Centrally manage privileged access across multiple customer organizations while maintaining client-level segregation and administration.
Technician Access Management	Provide controlled technician access to customer endpoints and restrict which applications technicians can elevate during support sessions.
Client-Specific Access Controls	Apply client-specific roles, access policies, approval workflows, MFA requirements, and feature scopes based on individual customer requirements.

See how Securden can help your organization

[Book a Demo](#)



 +1 844 228 0327  +44 203 868 6147

 support@securden.com  www.securden.com

2810 N Church St, PMB 75693, Wilmington, Delaware 19802-4447, United States.