Securden

Password Vault for Enterprises

A centralized platform to securely store, manage, share, monitor, and audit passwords, credentials, secrets, and remote access across the enterprise.

Credential Storage

Securely store and organize passwords, credentials, and keys in one vault.

Granular Access

Securely share credentials, grant just-in-time access, and enable secure remote access to target systems.

Enterprise Readiness

Audit trails, security reports, SIEM integration, high availability, and database backup.

Product Datasheet | SaaS, On-Premises, and Private Cloud Deployment Options

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

Product Datasheet

Platform Goal	Deployment Model	Primary Security Outcome
Discover, securely store, organize, manage, share, and govern passwords, credentials, keys, documents, and other sensitive identities across the organization.	SaaS, On-premises, and private cloud options.	Control who can access what. Audit, monitor, and record password-related activity. Automate password-management best practices through centralized policies, and support compliance while reducing credential risk.

Product Overview

Securden Password Vault for Enterprises is a comprehensive platform for securely storing, managing, sharing, and governing enterprise passwords, keys, and shared credentials. It enables granular access controls, approval-based just-in-time access, centralized policy enforcement, and secure web, RDP, SSH, SQL, and custom application connections without exposing credentials to users. With strong encryption, centralized oversight, session monitoring, and comprehensive audit trails, Securden strengthens password security while simplifying access to critical business resources.

Core Technical Capabilities

Capability Area	Technical Functionality
Enterprise Password Management	Centralized credential vault; controlled sharing; automated rotation of administrator passwords, service account passwords, SSH keys, and shared administrative accounts. Supports credential import from a standard CSV, XLSX, KeePass, CyberArk, Keeper, and Delinea.
Remote Connections	Provide one-click access to websites and web applications, RDP systems, SSH systems, and SQL databases without requiring users to view, copy, or manually enter credentials.
Just-in-Time Access	Grant time-limited access to passwords and remote connections through request-and-approval workflows. Automatically revoke access when the approved duration expires.
Custom Application Launcher	Securely launch thick-client, legacy, administrative, and custom applications using predefined parameters and credentials without exposing the underlying passwords to users.
Machine, AI, and DevOps Secrets	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.
Auditing and Reporting	Keep track of all users and account activities and generate standard and customized reports.

Architecture and Deployment

Deployment Area	Detail
Deployment models	On-premises, SaaS, private cloud
Server operating system (for on-prem)	The product can be installed on any machine running Windows 7 and later, or Windows Server 2008 R2 and later.
Installation package (for on-prem)	Single binary installer with bundled components and database.
Backend database (for on-prem)	PostgreSQL (bundled by default); Microsoft SQL Server optional.
Browser support	Chrome, Firefox, Edge, Safari, Internet Explorer 10 and above.
System sizing	Up to 1,000 accounts: 4 cores, 16 GB RAM, 50 GB disk. 1,000–10,000 accounts: 8 cores, 32 GB RAM, 100 GB disk. Above 10,000 accounts: contact Securden support.

Security Architecture: On-Premises vs SaaS

Security Area	On-Premises Edition	SaaS Edition
Vault model	Dedicated central server installed within your premises and connected to a backend database; users access the vault through a standard web browser.	Access-controlled, highly available vault instance hosted on AWS cloud with browser-based user access.

Security Area	On-Premises Edition	SaaS Edition
Data encryption	Sensitive vault data is encrypted at the application level using AES-256 before being stored in the database.	Customer data is encrypted using AES-256 and stored in segmented, encrypted cloud storage.
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.	Each customer segment uses a unique encryption key stored through Amazon KMS with cryptographic operations handled in an AWS CloudHSM cluster.
Database protection	Database communication is protected using SSL-encrypted connections; the backend database is deployed within the organization's environment.	Customer data is encrypted and stored in the Securden-hosted cloud environment, with a unique encryption key and access controls protecting customer data.
Data integrity	Encrypted data cannot be deciphered without the installation key even if the database is compromised.	Encrypted customer data cannot be deciphered without the corresponding organization-specific key.

Security Controls

Security Control	Details
Credential Encryption	AES-256 encryption.
Encryption Key Management	Unique per-installation encryption key, automatically generated for self-hosted deployments; AWS CloudHSM-backed key management for the SaaS edition.
Data Transmission Security	SSL over HTTPS; server–database transmission is also SSL-encrypted.
Access Governance	Controls on who can access what passwords; ownership, team sharing, provisioning, and deprovisioning controls.
Password Policy Enforcement	Create and enforce policies to ensure compliance with password management best practices.
Credential Monitoring	Track password access and changes across the organization through complete activity trails.
Offline Access Protection	Passwords can be exported as an encrypted HTML file for secure offline access.
Certificate-based Authentication	Authenticate users with digital certificates instead of or in addition to traditional username/password credentials. Self-signed certificate by default; CA-signed certificate installable. On-premises only.
Emergency Access	Designated users, maximum duration, and mandatory waiting period configurable.

Enterprise Password Access Control Design

Control Layer	Technical Detail
Primary Authentication	Access to Securden Password Vault can be secured through directory services such as Active Directory and Microsoft Entra ID, SAML-based SSO, RADIUS, smartcard authentication, or native local authentication.
Directory-Based Authentication	When directory authentication is enabled, users are authenticated through the configured identity source. Securden does not need to store their directory passwords.
User Lifecycle Management	Integrations with enterprise directories support user onboarding, authentication, group synchronization, access provisioning, and timely offboarding from the vault.
Multi-Factor Authentication	Cloud and on-premises deployments support MFA through TOTP applications, Securden Authenticator, email OTP, RADIUS-based solutions, Duo, YubiKey, and other supported authentication methods.
Granular Access Controls	Role-based permissions and configurable sharing controls determine who can view, use, modify, manage, or share passwords and other credentials stored in the vault.
Request-Approval Workflows	Users can request access to passwords and remote connections when needed. Requests are routed to designated approvers, who can grant access based on the user, resource, and business requirement.

Control Layer	Technical Detail
Just-in-Time Access	Request-and-approval workflows provide temporary, time-bound access to passwords and remote connections. Access is automatically revoked when the approved duration expires.

Identity, Integration, MFA, and Cross-platform Capabilities

Integration Area	Supported Options
Primary Authentication	Active Directory, RADIUS, SAML, Native (local) authentication, passkey
Single Sign-On (SAML-based)	SAML 2.0 support for Okta, Microsoft Entra ID, ADFS, OneLogin, PingIdentity, Google Workspace, and other SAML identity providers.
Multi-Factor Authentication	Any TOTP authenticator (Google/Microsoft Authenticator), any RADIUS-based MFA (RSA SecurID, Digipass, and others), Duo Security, YubiKey, Email-to-SMS gateway, OTP via email, smart card authentication.
SIEM Integration	Any SIEM tool can be integrated with Securden Password Vault, for example ArcSight and Splunk.
DevOps / Secrets Management	Ansible, Jenkins, Chef, Puppet, Terraform, SDK, CLI
Directory Services	Active Directory, Entra ID, LDAP
Browser Extensions	Chrome, Firefox, Edge, Safari — autofill and credential capture
Mobile Applications	Native iOS and Android applications

Integration Area	Supported Options
Desktop Applications	Native desktop application access on Windows, Linux, and macOS
API Access	APIs for application-to-application and database services communication

Product Specifications Snapshot

Specification	Details
Password Expiration and Alerts	Set maximum password age and send expiration alerts and event notifications to users.
Autofill and Credential Capture	Autofill credentials on websites and applications using browser extensions and automatically save new credentials to the vault.
Custom Application Launcher	Launch thick-client and legacy applications directly from Securden using reusable launcher profiles with dynamic placeholders, centralized administration, and approval controls.
Audit Trails and Activity Monitoring	Maintain complete audit trails of password access, changes, and user activities across the organization.
Post-Event Action Triggers	Automatically trigger predefined actions following specific events or activities in the Password Vault, enabling automated security and administrative workflows.
High Availability	Redundant servers pointing to the same database; Microsoft SQL Server clusters.

Specification	Details
Disaster Recovery	Periodic database backup and recovery; encrypted HTML offline copy accessible to super administrators.
Remote Connections (on-prem)	Web-based and native client applications for RDP, SSH, SQL, and web applications.
Remote Connections (SaaS)	Native client applications for RDP, SSH, SQL, and web applications.

Scale and Resilience

Resilience Area	Details
High Availability	Deploy a secondary application server with automatic failover to help maintain uninterrupted access to the password vault. A read-only application server can also be deployed on a separate subnet for additional resilience.
Database Clustering	Supports Microsoft SQL Server clustering to improve database availability and minimize service disruption.
Disaster Recovery	Schedule full database backups to a remote destination at configurable intervals, with a minimum interval of one hour.
Offline Access	Enable authorized users to access credentials during connectivity disruptions through the Securden desktop application or an encrypted, passphrase-protected HTML export.

Resilience Area	Details
Deployment Flexibility	Deploy Securden Password Vault on-premises or use the SaaS version based on your infrastructure, security, scalability, and data-residency requirements.

Commercial Notes

Commercial Area	Details
Starter Edition	Free, up to 5 users
Teams Edition	Quote-based pricing. 14-day free trial available.
Enterprise Edition	Quote-based pricing. 14-day free trial available.
Deployment Options	Available as on-premises and SaaS.
Free Trial	14-day free trial available for Teams and Enterprise editions.
Support	24x5 standard support; 24x7 premium support.

Common Use Cases

Use Case	Description
Credential Governance	Centrally store, classify, and share passwords, keys, documents, and other identities while retaining owner control.
Just-in-Time Access	Grant time-bound access to passwords and remote connections through request-and-approval workflows, with automatic revocation.

Use Case	Description
Privileged Remote Access	Provide one-click RDP, SSH, SQL, and web access without disclosing passwords, using web-based and native clients.
Custom Application Launch	Launch thick-client and legacy applications from Securden using reusable launcher profiles without exposing underlying credentials.
DevOps Secrets	Manage API keys, tokens, service accounts, and CI/CD secrets through APIs, SDK, CLI, and pipeline integrations.
Audit and Compliance	Maintain complete activity trails, enforce password policies, and produce actionable security reports across the organization.