Securden

Password Vault

For Enterprises

- Achieve password hygiene
- Track ‘who’ has access to ‘what’
- Prevent identity thefts

Securden’s on-premise, self-hosted Password Manager lets you centrally store, organize, share, and keep track of all passwords. It redefines the way your organization handles sensitive passwords and lets you collaborate better and smarter.

Centrally Store and Organize

Securely store all logins, passwords, keys, documents, and other identities in the central vault. Classify and organize for quick access.

Collaborate and Share with Team

Define ownership for accounts and let owners share passwords with their team while retaining control.

Remote Connections

Provide your users one-click access to remote servers, databases, devices, and applications without disclosing the passwords.

Control Access to IT

Establish controls on who can access what passwords. Provision and deprovision access seamlessly.

Active Directory Integration

Integrate with Active Directory for user authentication, onboarding, and automatic offboarding.

Single Sign-On Convenience

Integrate with any SAML-based SSO solution (Okta, GSuite, ADFS, OneLogin, PingIdenity, Azure AD SSO, and others).

Multi-Factor Authentication

Securely store all logins, passwords, keys, integrate with popular MFA tools, and enforce two-step verification for secure user access.

APIs for Application Passwords

Comprehensive list of APIs for managing application-to-application and database services communication.

Password Policy Enforcement

Create and enforce policies to ensure compliance to password management best practices.

Track Activities with Trails

Maintain a complete trail of activities, including password access and changes across the organization.

Actionable Security Reports

Gain organization-wide visibility and actionable security insights on IT access through analytical reports.

Expiration Alerts

Set maximum age for passwords and send expiration alerts reminding users to change their passwords.

Autofill Credentials

Autofill credentials on websites and applications using browser extensions. Autosave new credentials to the vault.

Mobile Access

Access your passwords from mobile devices through Securden native apps for iOS and Android.

Cross-platform Access

Convenience of accessing the web-interface from devices running any operating system.

Technical Specifications

Product Installation	Windows Server 2019 (OR) Windows Server 2008 R2 and later
Deployment Model	On-prem, VMs (or) private cloud (AWS/Azure)
Web-interface	IE, Chrome, Safari, Edge, Firefox
Backend Database	PostgreSQL (bundled) or MS SQL server
Primary Authentication	Active Directory, RADIUS, SAML, Native
MFA	Any TOTP authenticator (Google authenticator or Microsoft authenticator), any RADIUS-based authentication mechanism (RSA SecurID, Digipass, and others), Duo Security, Yubikey, Email to SMS gateway, and OTP through email
Data Encryption	AES-256
Data Transmission	SSL over HTTPS
Remote Connections	Web-based and native client applications RDP, SSH, SQL, and web applications

Password Resets	Agentless
Integrations	Active Directory, SIEM solutions, enterprise single sign-on applications
High Availability	Redundant servers pointing to the same database, MS SQL clusters
Disaster Recovery	Periodic database backup and recovery

Securden | support@securden.com | www.securden.com

Trusted by hundreds of SMBs and Enterprises across the globe

Securden, Inc.
2035 Sunset Lake Road,
Suite B-2, Newark,
Delaware, 19702