Securden

Password Vault | On-prem

Security Design and Specifications

Index

1. Introduction 03
2. Data Encryption 03
3. Authentication Methods 05
4. Data Transmission 07
5. Data Access Controls 08
6. Secure Remote Access 10
7. Accountability for Actions 11
8. Data Availability 12
9. Miscellaneous 13

Introduction

Securden Password Vault for Enterprises is meticulously designed with top-tier security standards, safeguarding an organization's most sensitive data. Securden is dedicated to delivering an enterprise-grade vault solution to safeguard customers' most valuable assets. This document explains in detail the security design and standards implemented by Securden across different levels.

Data Encryption

The design of the vault

Every installation is secured with an automatically generated, unique random key. The key serves as the master key for various encryption operations in the digital vault.

Data storage

All sensitive data gets stored in an encrypted form inside the digital vault. Securden uses the AES-256 algorithm to do the encryption.

- The sensitive data provided as input to the Securden server is encrypted using the unique installation key. This happens at the application level.
- The encrypted data is securely stored in the database.

Data integrity

- The encryption key cannot be held together with the encrypted data.
- The encryption key is needed only for starting the Securden Password Vault. It has to be kept somewhere outside and made available to the Securden server during startup.

Even if the database gets into a malicious user's hands, sensitive data cannot be deciphered in plain text without the installation key.

Database connections

The database accepts only secure connections. Clients can connect only from the same localhost. In high availability configuration, where the server and the database run on different servers, the database accepts connections only from specific IP addresses.

FIPS compliant

Securden Password Vault for Enterprises can be configured to operate in FIPS-compliant mode, ensuring that all encryption processes are performed using FIPS-certified systems and libraries.

Securosys HSM

Securden Password Vault for Enterprises additionally offers support for Securosys HSM, allowing users to store and manage the master encryption key in Securosys.

Multi-tenant architecture

Securden Password Vault for Enterprises also provides an MSP edition designed to facilitate multi-tenancy and secure data segregation among different client organizations.

Design Highlights

Data Encryption and Storage

- AES-256 encryption
- Encryption key separated from encrypted data
- FIPS-compliant mode
- Securosys HSM for storage and management of master encryption key
- Multi-tenant architecture

Authentication Methods

Access to the vault is primarily controlled in two ways. The vault can communicate with LDAP-compliant directory servers (Active Directory/Azure AD) for user onboarding, management, and authentication. It also communicates with SAML-based Single Sign On solutions for authentication. Securden also leverages RADIUS authentication and Smartcard authentication too as the primary authentication mechanism.

Alternatively, the vault comes with its native authentication as part of which accounts are created for users locally.

How does AD authentication / Azure AD authentication work?

In this case, Securden doesn't store the passwords. Instead, it connects with the AD through SSL and authenticates against AD or Azure AD.

How secure is the native authentication?

Securden uses the *bcrypt* hash function, which is considered an advanced algorithm that could withstand brute force attacks, to create one way hash of the Securden user password. The hash is then encrypted using the AES-256 algorithm.

The Securden installation key (which is unique to every installation) is used as the encryption key. *Bcrypt* enforces security best practices by requiring a salt as part of the hashing process. Hash when combined with salts guards against attacks.

Even if the database containing hashed values reaches a malicious user's hands, passwords cannot be deciphered in plain text.

Security Reinforcement

An additional layer of security with MFA

As an additional layer of security, Securden helps enforce a second authentication factor to grant access to the vault. It integrates with a variety of MFA solutions to achieve this.

Token-based authentication for API access

The vault can be programmatically accessed using APIs and Securden follows a token-based authentication. Authorised users need a URL and an Auth Token to access the permitted data.

Design Highlights

Primary Authentication

- Active Directory/Azure AD authentication
- RADIUS authentication
- Smart card authentication
- Securden's native authentication
- SAML 2.0-based single sign-on

MFA Enforcement for Additional Security

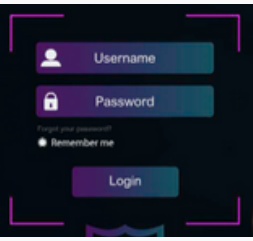
- Any TOTP Authentication
- Any RADIUS-based Authentication
- Duo Security
- Yubikey
- OTP through email
- Email-to-SMS gateway

Design Highlights

API Access

- Token-based authentication for authorised users
- Dynamic tokens

Data Transmission



Endusers and administrators connect to the vault through the web-interface, browser extensions, mobile apps, and programmatically through APIs. In all the cases, Securden ensures that the data transmission happens through secure channels in encrypted form.

Data transmission between the 'Securden Web-Interface and Server' and 'Server and Database'

All data transmission to and from Securden Password Vault is encrypted. The communication between the Securden web-interface and the server is encrypted and happens through HTTPS. Data transmission between the Securden server and database happens through SSL. Securden enforces deploying a third-party signed or a wildcard SSL certificate.

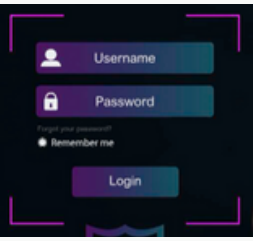
Access through APIs, mobile apps, and browser extensions

Access to credentials and other data through APIs, browser extensions, and mobile apps are as secure as the web version. There is no offline caching in extensions and mobile apps. They always connect to the Securden server to fetch data. You have complete control in granting or revoking access to users through APIs, extensions, and mobile apps.

Design Highlights

- Data Transmission (Server and Web-Interface) - Encrypted over HTTPS
- Data Transmission (Server and Database) - SSL

Data Access Control



The data access control measures in Securden ensure that after successful authentication, users get access only to the passwords that are allocated to them after successful authentication. They won't get to know about the accounts that are not related to their job profile. Besides, granular permissions determine the level of control over the passwords accessed.

Well-defined ownership

By default, the person who adds an account is designated as the owner of the account. This way, all accounts have well-defined ownership. No account is allowed to be left an orphan. When a user leaves the organization, the ownership has to be transferred to some other user. The security issues arising out of orphaned accounts are mitigated.

Folders as ‘Micro Vaults’

Accounts can be grouped as folders, which are like ‘micro vaults’. Each such micro vault can be granularly shared with the members of a group. For example, all Windows accounts can be grouped as a folder, and it can be shared with the ‘Windows Administrators’ group with granular privileges. When a new device gets added to the folder, it becomes available to the group and vice-versa.

Just-in-time access with release controls

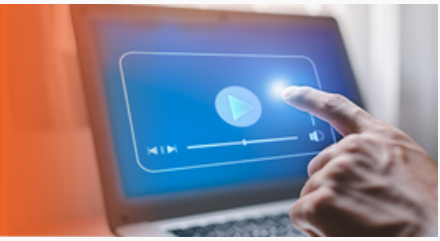
Securden offers provision for ensuring just-in-time access to sensitive devices through password/access release controls. Users will have to raise a request, which is approved by administrators for time-limited access. At the end of the access period, the password can be automatically randomised.

Design Highlights

Data Access Control

- Access control is intrinsically linked with user roles.
- Well-defined ownership for accounts
- Workflow-based release controls

Secure Remote Access



Securden facilitates launching remote connections with servers, databases, network devices, and others. By default, all remote connections and operations happen through the Securden server. This approach ensures that there is no direct connectivity between the end users and the target devices.

The remote access mechanism helps grant remote privileged access to users and third parties without punching holes on the corporate firewall to protocols like RDP and SSH. The remote connection is either a web-based one through 'HTTPS' or standard native clients for RDP and SSH.

Granting access without revealing passwords

The remote access architecture enables granting access to target devices and applications without revealing the underlying passwords or keys. This practice helps minimise the security risks associated with misuse of privileged access.

Design Highlights

Remote Connections

- No direct connection between end-user machines and target devices.
- Secure, encrypted connection

Accountability for Actions

Comprehensive audit trails

Securden captures all activities in the form of audit trails. You can view and search the trails to find 'who' did 'what' and 'when'. In addition, you can also gain security insights with various analytical reports such as Account activities, User activities, and Session activities.

Alerts and notifications

You can choose to send or receive email alerts upon the occurrence of any specific event like password retrieval, addition, deletion, and other modification activities. You can choose which events you would like to receive alerts about. The notifications can be sent out in real-time as and when the event occurs or as a consolidated email once a day.

SIEM support

Securden allows for the periodic sharing of privileged access data logs with SIEM solutions. You can choose to send events related to all activities in Securden to the SIEM tool, or only specific events as desired.

Design Highlights

- Complete visibility through comprehensive audit trails
- Actionable real-time notifications upon occurrences of specific events
- Event correlation via SIEM integration

Data Availability

Reliable, uninterrupted access to the vault is critical for business continuity. If a password management solution goes down, it affects all business operations. There should be provisions for data backup to handle unexpected situations like a server crash or physical damage to machines in addition to continuous availability. While the backup and high availability provisions are offered to handle these scenarios, it is important to ensure security around these measures.

The high availability architecture ensures security in all aspects. As the configuration involves running the Securden server and the database on different servers, the database has been configured to accept connections only from specific IP addresses - typically, the servers configured as 'high availability servers' alone. Besides, the database is enforced to accept only SSL connections. The database is guarded not to accept other connections.

To ensure security, the backup copy remains fully encrypted. The encryption key is separated from the backup copy. Typically, the live version and the backup share the same encryption key. While trying to restore data from the backup, the encryption key is needed. Without that, the restoration will not happen.

Miscellaneous

Input validation

Securden validates all inputs in the web-interface, and the application is guarded against attacks like SQL injections, cross-site scripting, buffer overflow, and other attacks.

Browser extensions - The security aspects

- Content Security Policy (CSP) is enforced.
- Inline JavaScript execution and AJAX requests to other sites are prohibited.

Server hardening

Securden is recommended to be run on a dedicated, hardened server. Except for the web-server port, no other port needs to be opened on the firewall. No other communication happens with outside entities.

Tamper-proof trails

The securely stored audit logs contain detailed information, including user actions, timestamps, and originating locations, ensuring their integrity against tampering. Any attempts to manipulate these logs will promptly trigger alerts.