Securden

CLOUD EDITION

Password Vault

Security Design and Specifications

Index

The Securden Password Vault for Enterprises is meticulously designed with top-tier security standards, as it safeguards an organization's critical information. 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.

Software Development Life Cycle

Software development life cycle

Security framework

Ideation and design	Development of software	Quality assurance	Release
Collaborate and brainstorm to identify the possible security flaws and loopholes.	Develop business logic for the new features and security improvements and test the logic for sanity.	Integrate the newly developed modules into the code and perform penetration testing to identify and rectify vulnerabilities.	Run security assessment to identify further areas of improvement for future releases.
Prepare an action plan taking into account the different flaws and loopholes identified in the brainstorm session along with difficulties faced by users in previous releases, and security recommendations by penetration testing partners.	Continuously test the newly added features and modules to check whether the intended purpose of each feature and module is satisfied.	Continuous sanity testing to ensure the core funtionalities of the product are working as intended after integration of newly developed features and modules.	Run continuous penetration testing activities through partners for identification and timely response to identified vulnerabilities in the product after release.
Fabricate a design framework and a prototype including all the changes, updates, and security fixes and submit it to the change management team for approval.	Check and verify whether all the third-party libraries used in the product are free from known vulnerabilities before incorporation.		

Our development repositories are secured through the HTTPS protocol and are subjected to strict authentication and access controls. The Securden engineering team works tightly with the security and quality assurance team to identify, address, and prevent vulnerabilities in the product before and after release.

The team partners and collaborates with third party penetration testing teams to identify areas of improvement and obtains suggestions to improve our security posture.

Apart from the security measures mentioned above, the engineering team and quality assurance team work tirelessly to make the application as secure as possible. The sections below explain the different measures undertaken to ensure the security and sanity of Securden Password Vault.

Data Encryption

Securing access through encrypted central vault

The encrypted centralized vault forms the core of Securden Password Vault for Enterprises. The vault is a completely access controlled, highly available server instance hosted on AWS cloud. While the server manages the business logic, end users can access it through a web browser.

Design of the vault

Each customer's data is completely segregated and stored in the database. Each customer segment can be considered a separate database since each customer's data in the database will be encrypted using a unique encryption key.

Encryption key management

The unique encryption key is generated automatically and stored in Amazon's Key Management Solution and cannot be accessed by anyone outside your organization. This is ensured by enforcing the use of AWS CloudHSM keystores for encrypting and decrypting the database using the key.

Whenever a customer's data is in the queue for decryption or encryption, a separate slot is created with the corresponding key. The key is stored in an unextractable form by the key management system within the CloudHSM cluster.

Data integrity

An organisation's data stored in the Securden database cannot be accessed by anyone outside the organization. Even if outsiders try to infiltrate, they get access only to the encrypted data. It cannot be deciphered in plain text without the encryption key.

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.

Design Highlights

- AES-256 data encryption
- Every new installation is stored in a separate database
- Encryption key is stored in Amazon KMS and all cryptographic operations are handled within a CloudHSM cluster
- FIPS-compliant mode

Controlling Access to the Vault Authentication Methods

Primary authentication

You can integrate Securden with LDAP-compliant directory services such as AD, Azure AD, and others. If your organization uses smart cards for authenticating user logons, you can leverage the same for Securden authentication. SAML-compatible federated identity management solutions like Okta, G Suite, Microsoft ADFS, OneLogin, PingIdentity, Azure AD SSO, and others can be integrated for Single Sign On.

MFA for additional security

Users can enforce multiple layers of authentication to access their Securden account. As part of two-factor authentication, Securden integrates with Email to SMS gateway, Duo Security, Microsoft Authenticator, RADIUS Authenticator, Yubikey, and more.

Certificate-based authentication

To meet the demands of remote work scenarios, you can enable all or select users of your organization to securely access the Securden web interface over the internet. Enabling this access involves configuring an additional certificate-based client authentication, which allows users to authenticate using certificate-based methods for remote work scenarios.

Programmatic access through authentication tokens

Securden provides APIs for querying the database programmatically, retrieving credentials, and performing various other tasks. Users can create authentication tokens for carrying out various operations using APIs.

Design Highlights

Primary authentication

- Securden's native authentication
- Active Directory/Azure AD authentication
- Smart card authentication
- RADIUS authentication

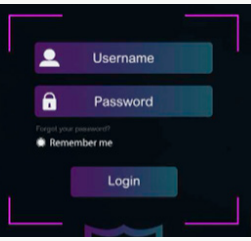
MFA enforcement for additional security

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

API Access

- Token-based authentication for authorised users
- Dynamic tokens

Securing Data in Transit



All data transmitted between the vault and the interface is encrypted and communication is handled through HTTPS. Access to the database is authenticated through SSL certificates. Securden forces the installation of a trusted CA-signed SSL certificate or a wild card SSL certificate.

Secure cross-platform access

Accessing the vault via alternative platforms such as mobile applications, desktop applications, browser extensions, and programmatic access through APIs maintains the same level of security as accessing the web UI. Data retrieval occurs directly from the Securden server, and access to extensions, APIs, mobile applications, and desktop clients can be revoked for specific users through the interface at any time.

Design Highlights

Data transmission between server and web-interface is encrypted over HTTPS and the data transmission between the server and database is encrypted over SSL.

Data Access Controls

Clear ownership of accounts

The person who adds an account to the vault is designated as the default owner. If an owner leaves the organization, all passwords owned by the user can be transferred to a different user. This way none of the accounts stored in Securden is orphaned. Risks associated with orphaned accounts such as stale passwords and privilege creeps can be averted.

Streamlined access provisioning via folder structure

Securden allows users and administrators to group similar accounts into folders. These entities can be shared with other users and user groups with granular access privileges. For example, if there is a group of Windows administrators in your

organization, you can create a user group in Securden for them and share the folder containing all the corresponding accounts in it. When a new Windows administrator is onboarded into the organization, they will automatically gain access to the accounts. This way a folder works as a micro vault for a group of users requiring access to the same resources.

Just-in-time access and approval workflow

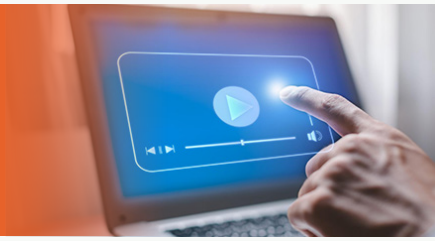
Granular access sharing ensures that users receive only the necessary level of control over a credential, limiting their access solely to the accounts they own and those that are shared to them by others. They are unable to access any other accounts or credentials present in the vault.

You can establish an additional layer of security for sensitive accounts by enforcing your users to go through approval workflows. Securden achieves this through the just-in-time access provisioning workflow. Whenever the passwords of such accounts need to be accessed, users will have to raise a request and select administrators or account managers, who are designated as Approvers. The approver will grant time-limited access to the particular system for the particular user. At the end of the stipulated time period, the password will be automatically reset.

Design Highlights

- Just-in-time access requests and approval workflow
- Transfer ownership
- Categorizing into folders for efficient organization

Secure Remote Access



Securden helps launch secure connections to servers, databases, network devices, and other assets. By default, all remote connections and remote operations are routed through Securden to prevent direct access from end user machines to target devices.

This method helps launch remote connections without adopting perimeter-based security systems such as VPN or perforating the corporate firewall. The remote connection can either be web-based or through native RDP and SSH clients.

Web based connections

Web-based connections are supported out of the box and no ports are required to be opened. All connections are routed through a remote gateway.

Native clients for RDP and SSH

To launch remote connections to IT assets through native RDP and SSH clients, you need to install a lightweight remote launcher on end-user machines.

Grant access without revealing passwords

The remote access mechanism allows you to grant access to IT assets without revealing the underlying passwords, SSH keys, and certificates. This helps avert risks associated with privilege misuse. Also, Securden provides the flexibility to selectively mask and reveal passwords based on different user categories.

Design Highlights

- Secured native and web-based remote connections.
- All connections are routed through Securden server, ensuring no direct connectivity between end-user machines and target devices.

Accountability for Actions

Comprehensive text-based 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 get alerted 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
- Real-time notifications upon occurrences of specific events
- SIEM integration

Data Availability

Reliable and uninterrupted access to critical credentials is crucial for businesses to operate seamlessly. When a solution that regulates access to sensitive credentials is down, the critical business operations suffer and at times fail. Scenarios such as server crashes or physical damage to machines are very real and to prevent unnecessary downtime, Securden has deployed redundancies and secondary application servers that provide continuous availability of credentials.

Scalable design to handle huge quantities of requests

The solution is hosted in various data centers around the world. Organizations from different locations will use the data center that is geographically closest. Databases specific to the data center will only accept connections from the application server(s). Within a data center, multiple application servers will be used along with a load balancer for optimum scalability.

All application servers are deployed in AWS and have the same security measures. AWS provides an RDS PostgreSQL database which is redundant and highly available.

Emergency access

In Securden, you can enable a designated list of users to access all passwords (work accounts) stored in Securden, breaking the usual access controls. This is to meet password access needs during certain emergencies. Users who are given this privilege will be able to configure the emergency access.

Design Highlights

- Database backup
- Emergency access

Miscellaneous

Input validation

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

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.

Security highlights in web browser extensions

Connections established through Securden browser extensions to websites and applications are safeguarded by Content Security Policy (CSP). Inline JavaScript execution and AJAX requests to external sites are prohibited as a preventive measure against XSS attacks.

Design Highlights

- Input validation
- Tamper proof trails
- Secured connections through browser extensions