Securden

Password Vault

Deployment Guide →

Index

1. Overview 3
2. Securden Pasword Vault Architecture 3
3. Recommended System Configurations 5
4. Deployment Prerequisites 6
5. Ports Used 6
6. Implementation Checklist 9

← Back to Index

Overview

Securden Password Vault is a full-fledged enterprise password management solution. It is delivered as a binary package, which can be installed on a standard Windows server within your premises or can be hosted on virtual machines. It can also be deployed on your private cloud instances too. The installation is simple and takes only a few minutes.

This document outlines the architecture, preparatory steps, and prerequisites for installing Securden Password Vault in your environment.

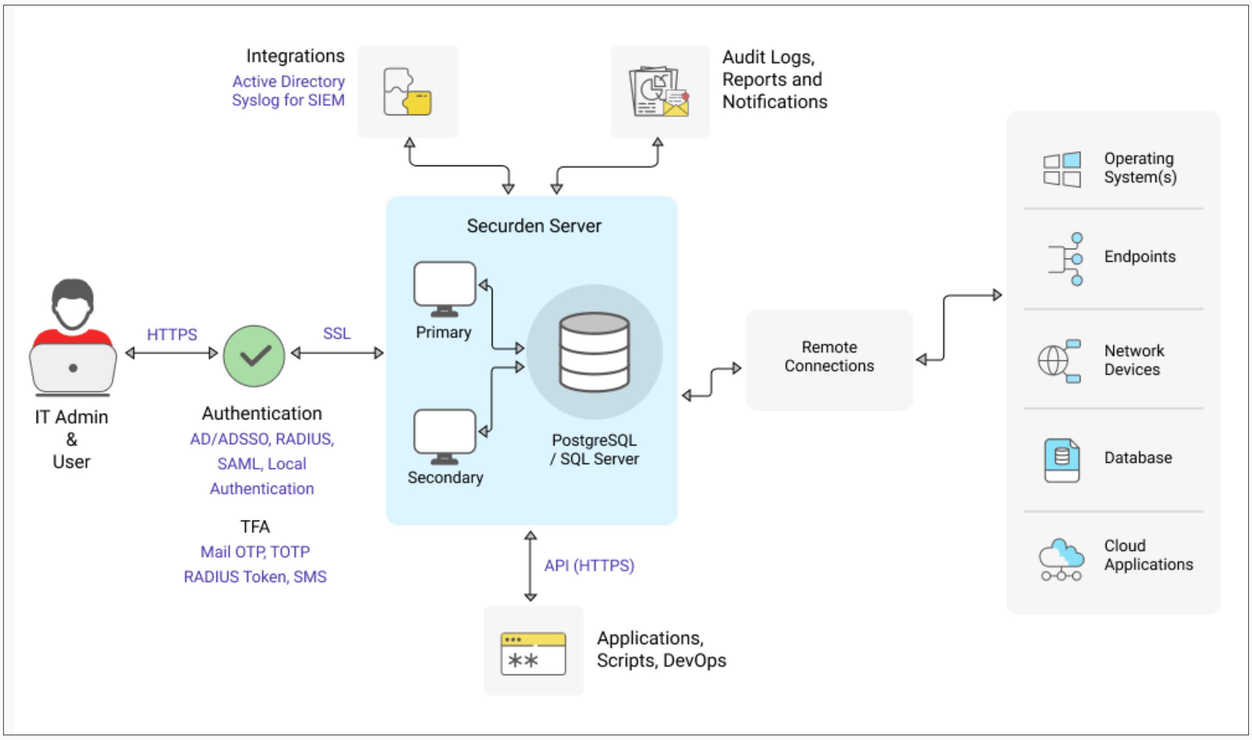
Securden Password Vault Architecture

Securden Password Vault is a web-based, on-premise, self-hosted software-only solution available as a binary for installation on Windows. Securden Password Vault comes as an all-in-one package, you don’t require any additional hardware or software for the functioning of the product.

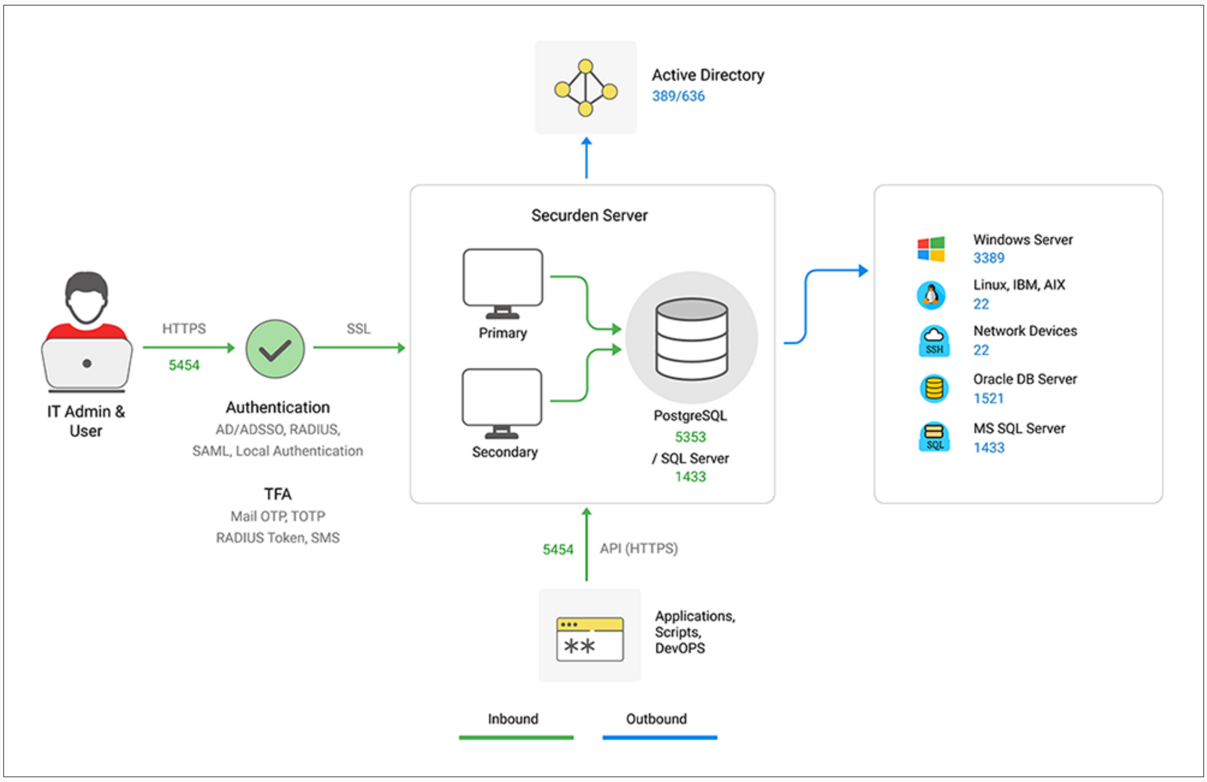
It comes with an inbuilt web server and PostgreSQL server as the default RDBMS. Optionally, you can configure MS SQL Server as the backend database.

An installation instance can just have two physical servers (primary and secondary), or multiple application servers as required. The solution runs on a central server connected to a backend database.

The web server handles all the business logic. End-users can connect to the server from their machines using any standard web-browser.



The product stores all sensitive information in a fully encrypted manner in a secure, digital vault. Securden uses AES-256 for encryption. The encryption key is unique to every installation and is automatically generated.



Recommended System Configurations Production Deployment

In order to provide uninterrupted access to privileged credentials, you can configure two application servers (primary and secondary) connected to a common database.

This comes in handy in cases where one application server fails or becomes unresponsive, and the load balancer effectively redirects the incoming traffic to the other active application server. This way, business processes are not interrupted. Application servers can either be two separate physical machines or virtual machines split up from a single physical server.

Please refer to the system configurations below to deploy Securden Password Vault in your production environment. Any physical or virtual server holding the configurations below is fine.

Unit	Primary Server	Secondary Server	Backend PostGreSQL server (Optionally, MS SQL server)
Memory	16 GB RAM	16 GB RAM	16 GB RAM
HDD	50 GB or more	50 GB or more	50 GB or more
vCPU (Intel or AMD Processors)	4 or more cores	4 or more cores	4 or more cores
OS (Windows Server License)	Windows Server 2016 or above	Windows Server 2016 or above	Windows Server 2016 or above
IP	1 STATIC IP	1 STATIC IP	1 STATIC IP
Quantity	1	1 or more	1
Details	-	For High Availability	Database Server

Deployment Prerequisites

- **Firewall and Port Settings –** Refer to the Ports section for full details.

- **Domain Settings –** A domain service account needs to be created in your Active Directory domain controller.

- **SMTP –** An external mail server needs to be set up and integrated with Securden Password Vault for users to receive email notifications.

- **DNS –** Public DNS Record needs to be created, one for Securden Password Vault, the other for SSM Gateway (to maintain domain details of the servers).

- **SSL Certificate –** A public SSL certificate needs to be installed on the application server to authenticate and encrypt connections between user devices and Securden Password Vault server.

Ports Used

Securden Password Vault uses a range of ports to ensure secure communication. The following are the TCP (Transmission Control Protocol) ports used in Securden password Vault.

- By default, Securden Password Vault comes with PostgreSQL server as the default RDBMS. Optionally, you can use MS SQL Server as the backend database. Port 5353 connects all the primary, secondary, and application servers to the PostgreSQL database. Port 1433 connects the product servers (primary and application servers) to the SQL server.

- End-users connect to the User Interface of the product using port 5454. Administrators can choose to change this port to 443 or any other port if required.

- Web remote connections use the port 5422 for SSH and 5426 for RDP.

Port Name	Source	Destination	Port (TCP)	Details
PostgreSQL Database Port	Primary, Secondary, and all Application Servers	PostgreSQL Server	5353	-
MS SQL Database Port	Primary and Application Servers	MS SQL Server	1433	-
Securden Server Port	To all Users (End Machines), Agents, and Secondary Servers	Primary	5454 (Web-Port)	For all servers this port can be changed if required
		Secondary		
SSM Port (Inbound)	All Client machines	SSM Server installed machine(s)	3389 (RDP Port)	3389 is opened on the SSM for all client machines
SSM Port (Outbound)	SSM Server installed machine(s)	To all Target Machines		3389 is opened to all target machines from the SSM Server
Web - SSH	To all Users (End Machines)	On all application servers	5426	-
Web - RDP			5626	
SMTP Sever Port (Mail Server Port)	-	-	587	TLS
			465	SSL

Proxy Server Port - This port must be open if your organization makes use of a proxy server to regulate internet traffic. Navigate to **Admin** >> **General** >> **Proxy Server Settings** and configure the port details to facilitate Securden to connect to the internet.

AD Port is used for the account discovery purpose while integrating with the Active Directory.

RADIUS Server Port - You can integrate the RADIUS server or any RADIUS-compliant two-factor authentication system like OneSpan Digipass, RSA SecurID, etc., for the second-factor authentication. Navigate to **Admin** >> **Authentication** >> **Two-Factor Authentication**. Click the configure option on **RADIUS Authentication**. In the **RADIUS Server Settings** page that opens up, you may configure the details of the authentication port.

Port Name	Source	Destination	Port (TCP)	Details
Proxy Server Port	Primary Server	Proxy Server	Based on your settings	**If needed**
AD (DC) Port	Primary/application server	AD DC	636	SSL/TLS
	-	-	339	If there is no SSL
RADIUS Server Port	-	-	1812	**If needed**
Azure AD	Primary/application server	Azure AD	Graph API	**If needed**
Breached Password Identification	Primary Server (Requires internet connection)	-	API	https://api.pwned-passwords.com/
Other Ports	-	-	-	Check your integration port requirements

Implementation Checklist

Refer to the implementation checklist below to deploy and get started with Securden Password Vault in your production environment.

The implementation starts with choosing the backend database and involves various basic settings, including mail server and proxy server settings, integrating with directory services for user management, enforcing multi-factor authentication (MFA) and single sign-on (SSO), configuring additional features for remote connections, and session recordings. The entire process should take no longer than a week.

S.No	Feature	Notes
	Backend Database	
1.	Decide if you are going to use the PostgreSQL database bundled with the product or MS SQL server as the backend database.	Both databases are scalable and work well. However, you need to make the choice at the time of moving to production as data migration is not supported if you wish to change later.
	Mandatory Settings	
2.	Installation Encryption Key	When you apply the registered license key, you will be prompted to move the installation encryption key to a location other than the installation folder. This is to ensure that the encrypted data and the encryption key are not kept together. Follow the instructions on the interface to complete this step.

S.No	Feature	Notes
3.	Mail Server Settings	Securden sends various email notifications to the admins/users and to facilitate that SMTP server details are to be configured. Navigate to **Admin** >> **General** >> **Mail Server Settings** in the GUI to perform this step.
4.	Proxy Server Settings	If your organization makes use of a proxy server to regulate internet traffic, configure the proxy server details here to facilitate Securden to connect to the internet. Navigate to **Admin** >> **General** >>**Proxy Server Settings** in the GUI to perform this step. Internet connectivity is required if you want to run the report that checks breached passwords.
5.	Server Connectivity Settings	This setting is to specify how to connect to the Securden web interface from client machines and the name with which the client machines identify the Securden server host. Navigate to **Admin** >> **General** >> **Securden Server Connectivity** in the GUI to perform this step.
User Onboarding and Management		
6.	Integration with Directories	You can integrate with Active Directory/Azure AD /LDAP and import the required users and/or groups. You can keep the user database in synchronization with the respective directories and also leverage the authentication mechanism for allowing access to users. Navigate to **Users** >> **Add** section to do this.
7.	Assign Roles to Users	After importing users, assign roles to them. You may make use of any of the predefined user roles or create custom roles as required. Use the '**Edit**' icon next to the respective users to assign the role. You may

S.No	Feature	Notes
		create custom roles from **Admin** >> **Customization** >> **Custom Roles.** In addition, decide if you want to have super administrator role. If yes, you can also decide how many super admins you would like to have. The recommended approach is to create one or two super administrators and then completely turn off further creation. This can be done from **Admin** >> **Customization** >> **Configurations.**
8.	Delete the default Securden Administrator account	By default, Securden comes with the administrator role as a locally created account. Delete that account. You may create another local account to serve emergency access scenarios such as active directory domain is down etc.
9.	Enforce Two Factor Authentication	For enhanced security, you can enforce a second layer of authentication for your users to access their Securden accounts. Users will have to authenticate through two successive stages. It is strongly recommended to activate Two Factor Authentication (2FA). You can do this from **Admin** >> **Authentication** >> **Two Factor Authentication.**
10.	Explore SSO	Securden integrates with various SAML-compatible federated identity management solutions such as Okta, G Suite, Microsoft ADFS, OneLogin, Ping Identity, Azure AD SSO, and others for Single Sign On. Securden serves as the SAML Service Provider (SP) and it integrates with SAML Identity Providers (IdP). If you are using any SSO solution already, you may integrate that with Securden **(Admin** >> **Integrations** >> **SAML SSO).**

S.No	Feature	Notes
Privileged Account Management, Remote Session Management		
11.	Create Password Policies	Security best practices recommend usage of strong, unique passwords for every account. Password policy in Securden helps you define the strength, complexity requirements, periodicity for password resets and other conditions. Wherever automation is possible, Securden password generator will automatically assign unique passwords as per the policy defined. Navigate to **Admin** >> **Account Management** >> **Password Policy** in the GUI to create password policies. After creating a policy that suits your requirements, you can set that policy as the default policy for your organization from **Admin** >> **Account Management** >> **Password Policy** >> **Set As Default Policy** section in the GUI.
12.	Create Account Types	Account types help identify and classify the accounts being added in Securden. Proper classification comes in handy to carry out various operations such as sharing, reporting etc. Super Administrators, Administrators, and Account Managers have the privilege to add custom types, edit and delete existing ones. When creating your own account types, you can define the fields needed for that type, decide if certain fields should be marked as 'mandatory', if any field to hold default values and so on. **Navigate to Admin** >> **Account Management** >> **Account Types** to create new account types and to manage existing ones.
13.	Decide about allowing Personal accounts management	Securden allows classifying the accounts into 'work' and 'personal' categories. Work accounts belong to the organization and can be shared with others. 'Personal' accounts are purely personal to the user who is adding them and can't be shared with others. Even super administrators can't view them. If you don't want to allow managing personal passwords, you can disable this from **Admin** >> **Customization** >> **Configurations.**

S.No	Feature	Notes
14.	Import Account from CSV, XLSX, or KeePass	If you have your passwords in CSV or XLSX files, you may import them to Securden. Navigate to **Accounts** >> **Add** >> **Import from File** to perform this.
15.	Manual Addition of Accounts	On an ongoing basis, you can add accounts manually too. You can make use of this provision to add website accounts and others that are not discoverable. Navigate to **Accounts** >> **Add** >> **Add Accounts Manually** in the GUI to perform this step.
16.	Add SSH Keys	In addition to storing passwords, you can also store and manage SSH keys. The provision to manage SSH keys helps you store the keys securely, track their usage, and associate them with required Unix devices for authentication and remote access.
17.	Create Folders	You can organize the accounts in Securden by grouping them as folders for easy and efficient management. At any point in time, a specific account could remain a member of one folder only. That means the same account cannot become a member of multiple folders. You can recreate your organization's hierarchy in the form of folders and multiple levels of subfolders.
18.	Share Accounts and Folders	If you want to allot certain specific accounts or folders to specific users or groups, you can use the sharing mechanism available at the accounts level and at the folder level. Explore the granular sharing options, including the 'Open Connection' option that allows you to share accounts without showing passwords in plain-text.
19.	Remote Connection Options	Securden allows users to launch RDP, SSH, SQL and other connections and supports launching web-based connections and using native applications.

S.No	Feature	Notes
		If you want to launch remote connections to multiple computers and IT assets, you may add the required IT resources from **Admin >> Remote Connections and Session Recordings >> Assets for Remote Connections.** After adding the IT assets, you need to pick specific assets for associating them with specific users/user groups and accounts/folders in Securden. This can be done from **Admin >> Remote Connections and Session Recordings >> Domain Account - Assets Association.**
20.	Custom Application Launcher	In addition to the default modes of launching web-based connections and through native clients, you can define custom application launchers to supply credentials and automatically launch any application, including thick application clients. Basically, you will be creating a profile for each such application capturing the input fields as found in the target application. The profile will have placeholders to replace the required values from Securden repository at the time of launching the connections **(Admin >> Remote Sessions >> Custom Application Launcher).**
21.	Configure Just-in-time Access Workflow for Sensitive Accounts	You can establish an additional layer of security for sensitive accounts by enforcing your users to go through approval workflows. This also serves as a just-in-time access provisioning mechanism. Whenever the passwords of such accounts are to be accessed, users will have to raise a request and select administrators or account managers, who are designated as ‘Approvers’ will grant time-limited access. At the end of the usage period, the password will be automatically reset. This feature comes with adequate provisions to handle various scenarios such as obtaining permission in advance, granting automated approvals.

S.No	Feature	Notes
22.	Explore APIs for managing non-human identities/ application identities	Securden provides APIs for application-to-application and application-to-database communication. APIs can be used to connect to Securden and fetch the required data automatically. Navigate to **Admin** >> **General** >> **Authentication Token for API Access** to start using the APIs.
23.	Configure Notifications	Securden can send email notifications upon the occurrence of certain events such as password retrieval, deletion, change in share permissions, and others. You can choose the events for which you want to receive notifications. The notifications can be triggered real-time or as one consolidated email once a day. Navigate to **Admin** >> **Notifications** >> **Event Notifications** section to configure notifications. You may configure notifications at the folder level too.
24.	Granularly Customize Product Features	You can customize the features of Securden in a granular manner. You can switch on and switch off certain features anytime as desired. Navigate to **Admin** >> **Customization** >> **Configurations** section to exercise the customization options.
	Miscellaneous	
25.	Integrations	Securden integrates with SIEM solutions and ticketing systems. Navigate to **Admin** >> **Integrations** to explore integrations.
26.	Configure Emergency Access	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. In this interface, you can designate the users who should get the emergency access privilege. You can define the maximum time duration until which the user should have emergency access.

S.No	Feature	Notes
		As an additional control, you can define a mandatory waiting period (in minutes) until the person should wait before gaining emergency access. All administrators will be notified when someone wants to gain emergency access. Navigate to **Admin** >> **Emergency Access** to configure this.
27.	Rebrand Product Logo	You can replace Securden logo with your company logo from **Admin** >> **Customization** >> **Logo, Theme, Text.**
28.	Granularly Customize Product Features	You can restrict access to the Securden interface to users only from specific IP addresses. Explore various security settings from **Admin** >> **Security.**
29.	Configure High Availability	To ensure uninterrupted access to accounts and passwords, Securden comes with high availability architecture. This is achieved by deploying another application server, which would serve as the secondary server. In the event ofthe primary server going down, users can connect to the secondary server. Navigate to **Admin** >> **High Availability** in the GUI to configure High Availability. Note: You can configure any number of additional application servers and deploy them in different locations. If you are using MS SQL server as the backend database, you can make use of SQL clusters.
30.	Replace Self-signed Certificate	By default, Securden comes bundled with a self-signed certificate. You can add your own CA-signed certificate by following the steps below. Basically, Securden requires the certificate and the private key. Instructions to do this are available in the Quick Start guide.

S.No	Feature	Notes
31.	Configure Database Backup	To ensure access to your data and passwords even in the unlikely scenario of something going wrong with the current installation, Securden offers disaster recovery provisions. You can take backup of the entire database periodically. In the event of a disaster, you can recover data from the backup. Securden allows you to specify the "Backup Destination". You may give the network path of a remote machine, where the backup copy will be stored. The periodicity could be as low as one hour and you may decide to maintain x number of past backup copies. Navigate to **Admin** >> **High Availability** >> **Database Backup** in the GUI to perform this.
32.	Passwords Backup as Encrypted HTML file	Super Administrators can create a scheduled task for taking a backup of all work accounts in the form of an encrypted HTML file. When configuring the schedule, a passphrase has to be provided, which will be used as the encryption key. Whenever the backup copy is to be viewed, passphrase has to be supplied. Without the passphrase, the backup copy cannot be opened. The encrypted HTML file can be stored in a secure, remote location. Navigate to **Admin** >> **High Availability** >> **Passwords Backup** to perform this.
33.	Monitor Product Upgrades	Securden releases minor and major upgrades periodically. You can monitor new releases from **Admin** >> **Product Upgrades** section and carry out upgrades from there.

Note: You may refer to the **Securden Password Vault Guide** to know about the product configurations, troubleshooting steps, and other features to start working on the solution.