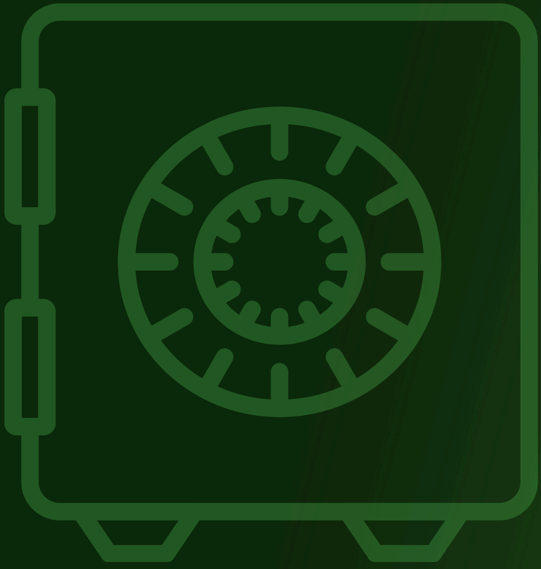
Securden

Password Vault for Enterprises

Installation Guide



Securden Password Vault for Enterprises Installation Guide

Welcome to Securden Password Vault for Enterprises. This document is for administrators and provides information on installing the solution and getting started with the initial settings.

System Requirements for Installation

Securden Password Vault comes with everything bundled and does not require any specific software to be installed separately. Following are the minimum hardware and software configuration required by Securden:

Description	**Specification**
Operating System	Any machine running Windows Servers 2008R2 and above (64 bit) **Recommended**: Windows Server 2019
Memory and Storage	8 GB RAM and 50 GB Hard Disk Space in each machine (Primary and Secondary servers in High Availability setup)
Backend Database	You can either use the **PostgreSQL** database bundled with the product by default. Alternatively, you can make use of **MS SQL Server 2008** and above (including **SQL Server Express** edition) **Recommended:** SQL Server 2017

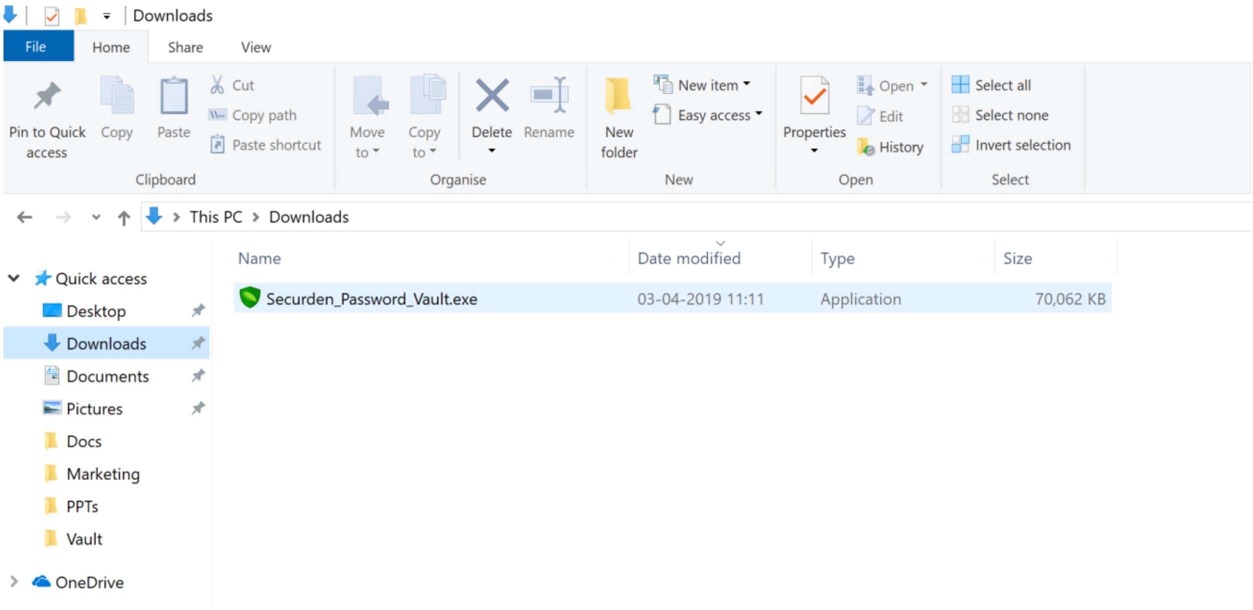
Web-Interface	Chrome, Firefox, Edge, Safari, Internet Explorer 10 and above.

Securden Password Vault consists of the following components:

- Securden server
- PostgreSQL database bundled with the product. PostgreSQL process accepts connections only from the host in which the server is running.

Installation

- Download **Securden_Password_Vault.exe** and execute it by double-clicking the file.

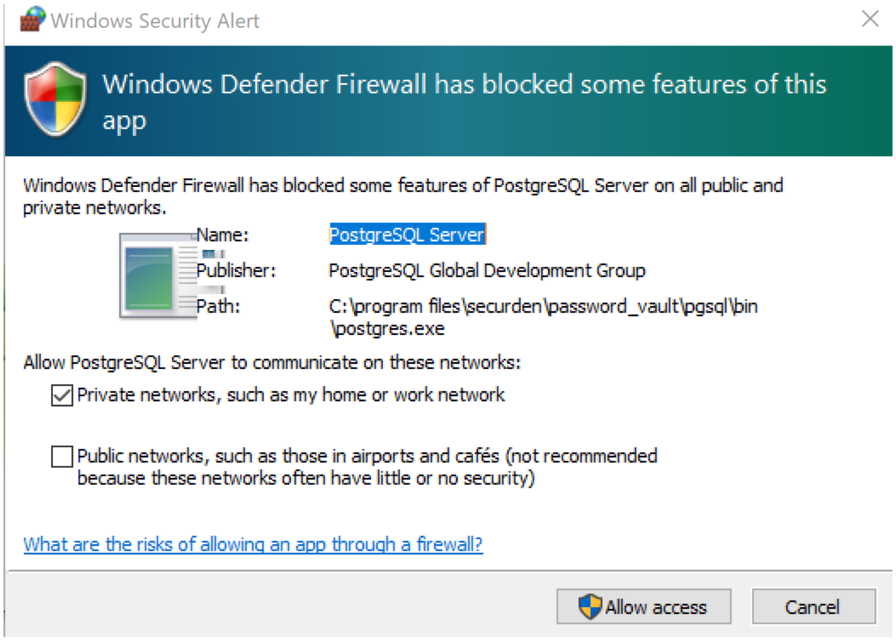


Name	Date modified	Type	Size
Securden_Password_Vault.exe	03-04-2019 11:11	Application	70,062 KB

- The installation wizard will guide you through the installation process
- Specify the directory where the product has to be installed - by default, it will be installed in **C:/Program Files/Securden;** Henceforth, this installation directory path shall be referred to as **"Vault_Home"**

- Finally, Securden server will start and it will automatically launch the web-interface.
- Click "**Finish**" in the wizard to complete the installation process.

Note: During the installation process, the Windows Defender will display the following warning message. Click "**Allow Access**" to proceed with the installation.



Windows Security Alert

Windows Defender Firewall has blocked some features of this app

Windows Defender Firewall has blocked some features of PostgreSQL Server on all public and private networks.

Name: PostgreSQL Server

Publisher: PostgreSQL Global Development Group

Path: C:\program files\securden\password_vault\pgsql\bin \postgres.exe

Allow PostgreSQL Server to communicate on these networks:

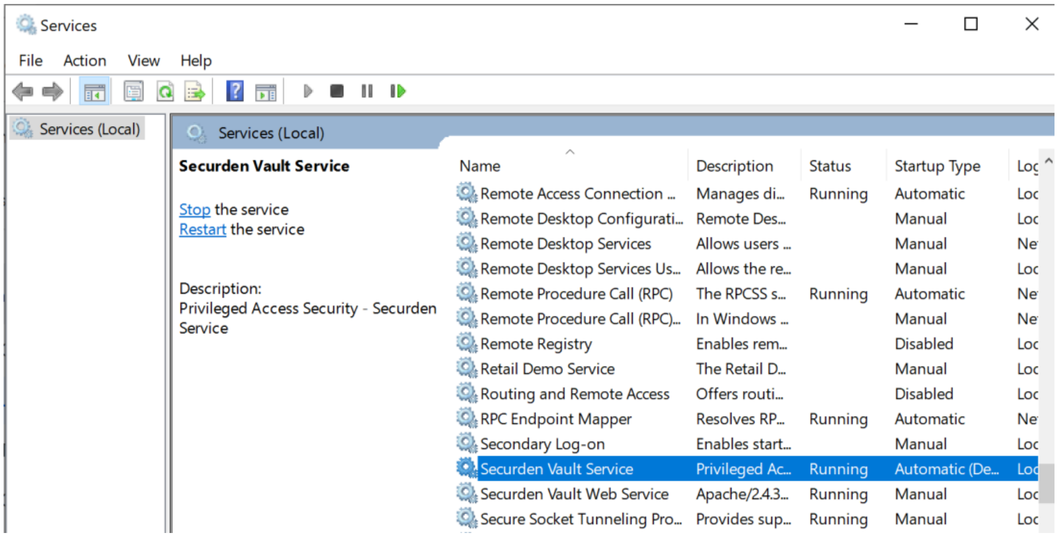
☑ Private networks, such as my home or work network

☐ Public networks, such as those in airports and cafés (not recommended because these networks often have little or no security)

What are the risks of allowing an app through a firewall?

Starting & Shutting Down Vault

- You can start and shutdown the Vault from Windows Services Manager (services.msc).



Services (Local)

Securden Vault Service

Stop the service
Restart the service

Description:
Privileged Access Security - Securden Service

Name	Description	Status	Startup Type	Loc
Remote Access Connection ...	Manages di...	Running	Automatic	Loc
Remote Desktop Configurati...	Remote Des...		Manual	Loc
Remote Desktop Services	Allows users ...		Manual	Ne
Remote Desktop Services Us...	Allows the re...		Manual	Loc
Remote Procedure Call (RPC)	The RPCSS s...	Running	Automatic	Ne
Remote Procedure Call (RPC)...	In Windows ...		Manual	Ne
Remote Registry	Enables rem...		Disabled	Loc
Retail Demo Service	The Retail D...		Manual	Loc
Routing and Remote Access	Offers routi...		Disabled	Loc
RPC Endpoint Mapper	Resolves RP...	Running	Automatic	Ne
Secondary Log-on	Enables start...		Manual	Loc
Securden Vault Service	Privileged Ac...	Running	Automatic (De...	Loc
Securden Vault Web Service	Apache/2.4.3...	Running	Manual	Loc
Secure Socket Tunneling Pro...	Provides sup...	Running	Manual	Loc

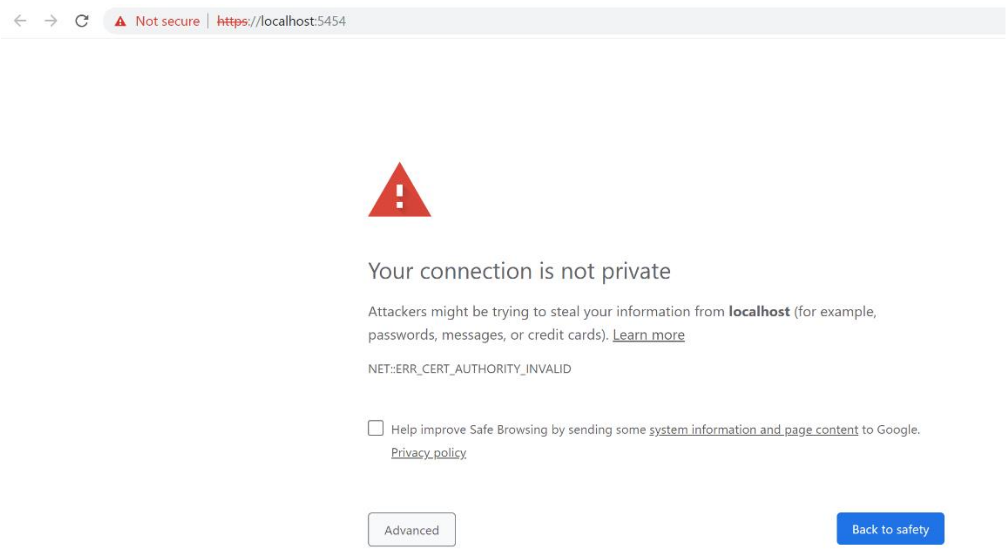
- Locate **Securden Vault Service** and start, stop it as required. This takes care of starting and stopping the dependent services too. You may safely ignore the other service named Securden Vault Web Service, which is taken care of by Securden automatically.

Launching Web Interface

To launch the web-interface manually, open a browser and connect to the URL as explained below:

https://<VAULT server hostname>:5454

During this process, you might see this warning message displayed by the browser:



Not secure | ~~https~~://localhost:5454

Your connection is not private

Attackers might be trying to steal your information from **localhost** (for example, passwords, messages, or credit cards). Learn more

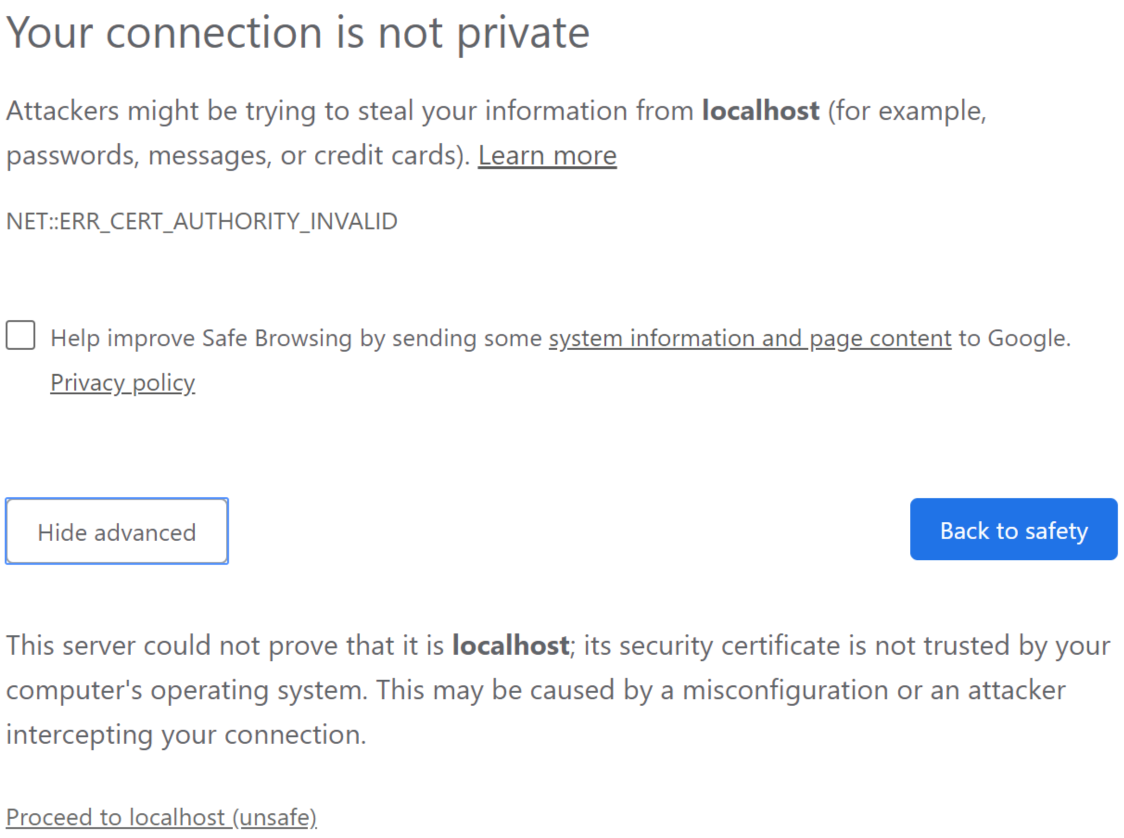
NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

This message appears because Securden comes bundled with a self-signed certificate. (If you add your own CA signed certificate, this message will vanish. **Detailed procedure to replace the self-signed certificate with your own certificate is provided below).**

To proceed with the testing, click ‘**Advanced**’ and then click ‘**Proceed to**

localhost (unsafe)'.



Your connection is not private

Attackers might be trying to steal your information from **localhost** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Help improve Safe Browsing by sending some system information and page content to Google. Privacy policy

This server could not prove that it is **localhost**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to localhost (unsafe)

This opens up the web-interface. To access an unconfigured setup, the default login details are as below:

Username: admin
Password: admin

Replacing 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. If you have the certificate in **.pfx** format, follow the steps below:

Step 1: Download OpenSSL (if you don't have that installed already)

Download OpenSSL from http://www.slproweb.com/products/Win32OpenSSL.html . Make sure the 'bin' folder under the OpenSSL installation is included in the 'PATH' environment variable.

Step 2: Copy your certificate (e.g. certificate.pfx) and paste it in the system from where you can execute OpenSSL exe.

The *.pfx file is in PKCS#12 format and includes both the certificate and the private key.

Step 3: Run the following commands to export the private key

```
openssl pkcs12 -in certificate.pfx -nocerts -out securden-key.pem -nodes
openssl rsa -in securden-key.pem -out securden-key.pem
```

Step 4: Run the following command to export the certificate

```
openssl pkcs12 -in certificate.pfx -nokeys -out securden-cert.pem
```

Once you execute the above steps, you will get a SSL certificate and a private key.

Step 5: Copy the certificate and private key created above and navigate to **<Securden-Installation-Folder>/conf** directory and paste the keys.

Step 6: In services.msc, **restart Securden PAM Service**

This replaces the self-signed certificate with your certificate.

Optional: Change Backend Database to MS SQL Server

If you want, you can change your backend database from the default PostgreSQL to MS SQL server. When you change the backend, you will be starting afresh - that means, your existing data in PostgreSQL will **not** be migrated.

To change the backend database from the default PostgreSQL to MS SQL Server, follow the steps below:

- Stop "**Securden PAM Service**" from services.msc (in the machine in which Securden is installed)
- Navigate to **<Securden Installation Folder>/bin** folder and execute "**ChangeDatabase.exe**" and in the GUI, supply SQL instance name, database name, username, and password to connect to the database.
- Now, start the "**Securden PAM Service**" from services.msc (you may ignore the other service named Securden Web Service, which is automatically taken care of)
- Connect to the web interface https://<local-host>:5959 (or) https://<host-name>:5959
- Clear browser cache

Browser Extensions

Securden provides browser extension to facilitate auto-fill of credentials on websites and web applications. When you create new accounts on websites, the same can be added to Securden without leaving that website. You can view accounts, passwords and also launch connections with websites from within the browser extension. Securden browser extensions are now available for Chrome, Firefox and Edge. The installation instructions and how to work with the extensions are available in this document.

Mobile Apps

Securden offers native apps for iOS and Android. You may download the apps directly from the AppStore/Play Store.