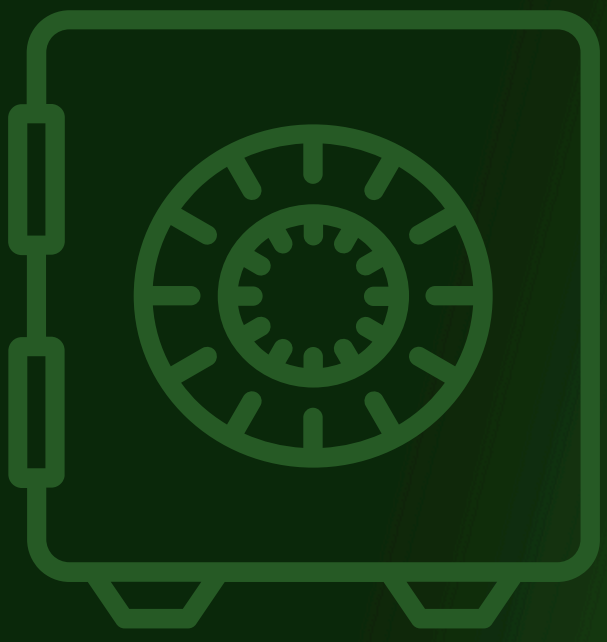
Securden

Password Vault for Enterprises

User Guide



Introduction

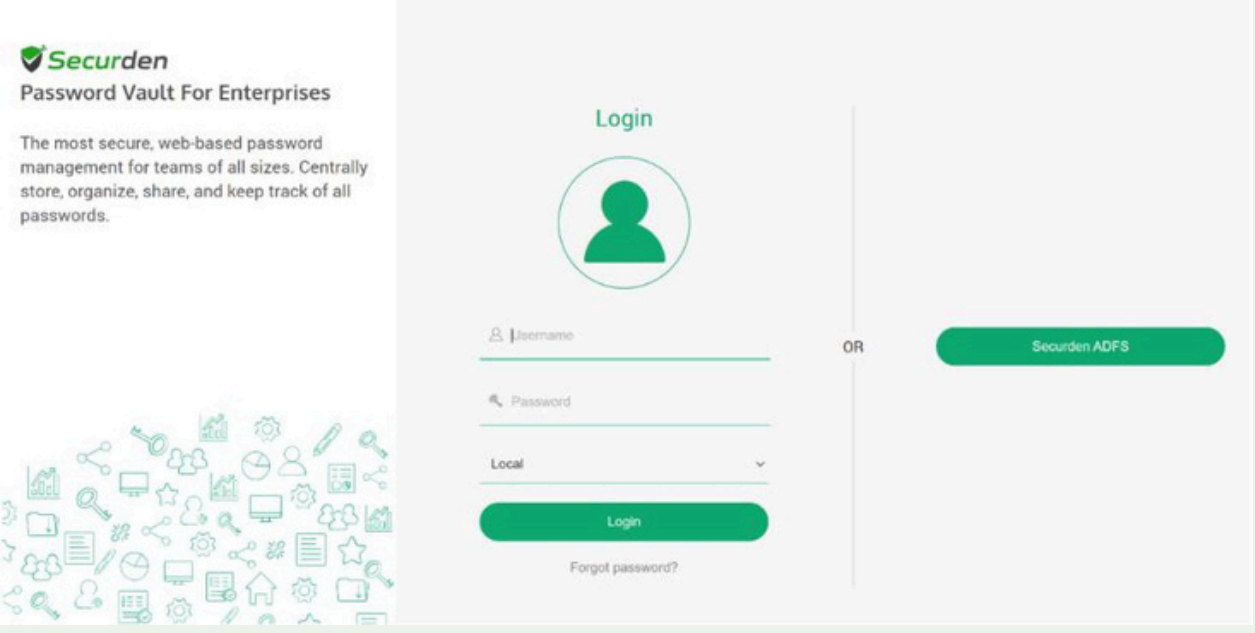
This guide provides the essential information for end users to get started with Securden Password Vault. It throws light on what operations you can generally perform as a standard user.

Accessing the Web-interface

Your administrator would have provided you with the URL to connect to the web interface, which typically looks like
https://<Hostname or IP address of Securden server>:5454
To access vault web interface, simply open any browser and type the URL.

Logging in to Securden Vault

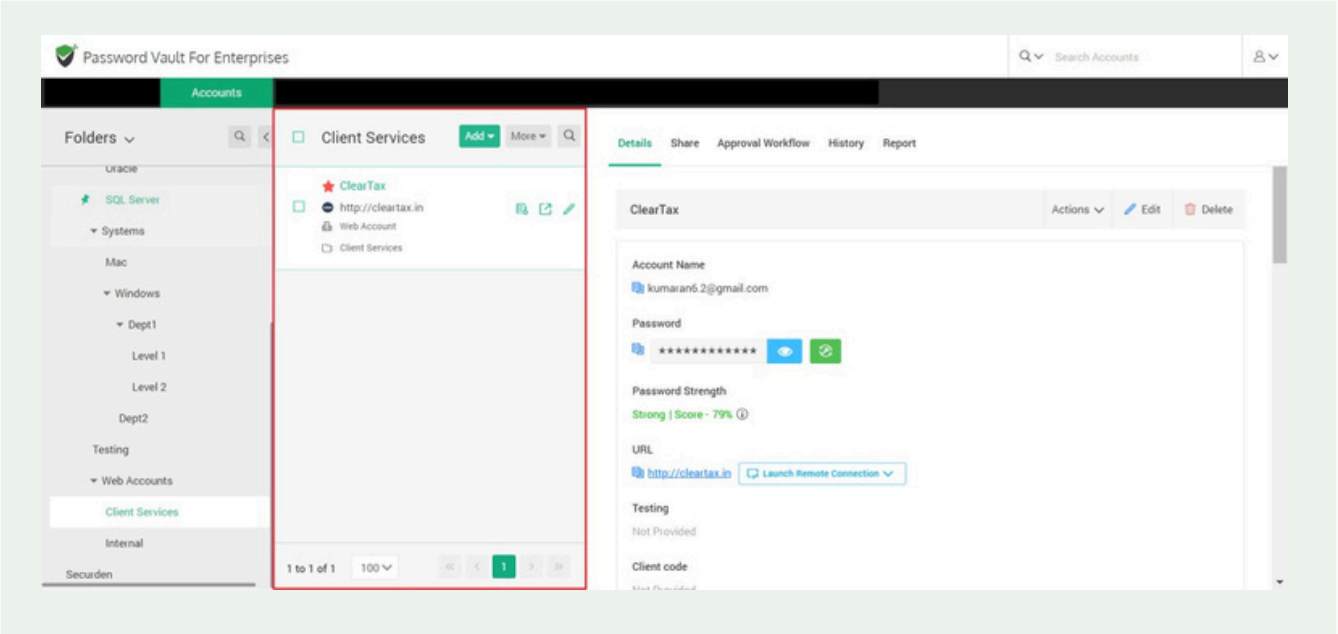
You can make use of various authentication options, including Active Directory authentication, native local authentication of the application, and different Single Sign- On options. Choose the appropriate option on the login screen



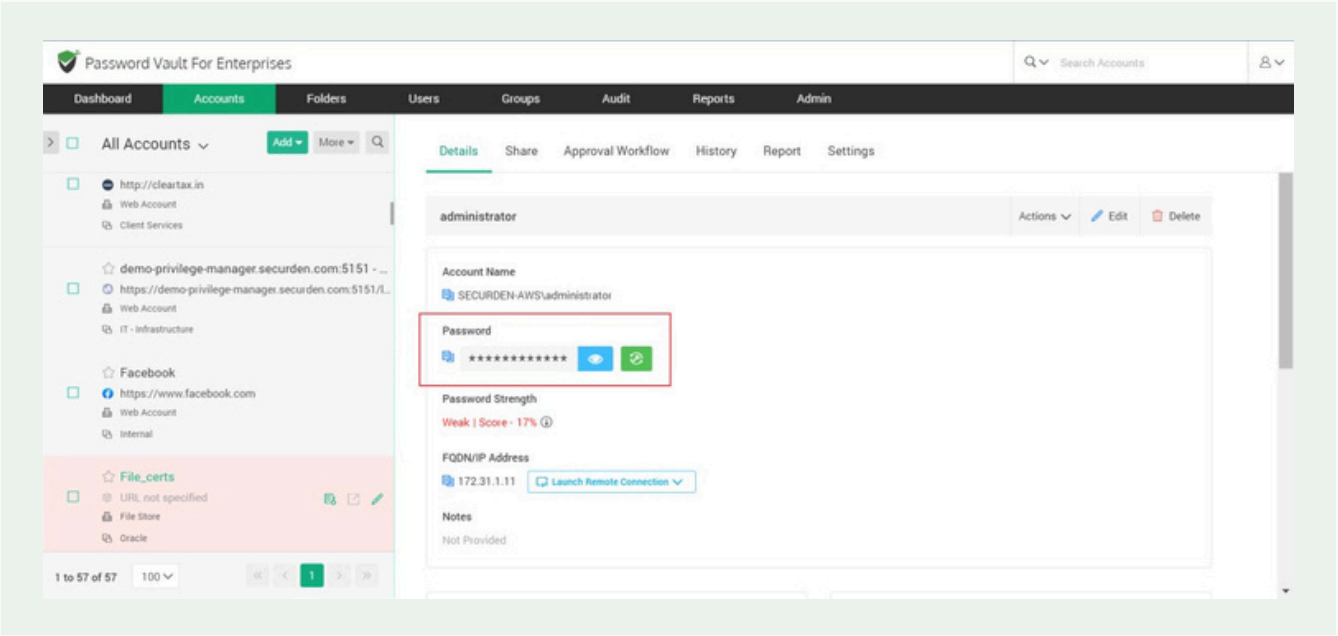
Working with the Interface

Upon logging in to the web interface, you will see different tabs based on the permissions granted. All password management operations are performed from the **Accounts** tab. Any login information (username and password) stored in Securden is referred to as an account.

The account tab has all the accounts shared with you and ones that you newly create. You can view the account details and passwords by clicking on an account.



If you have been provided with permission to view the password of any particular account, you can view that by clicking the 'Eye' icon. Otherwise, the password will not be displayed.

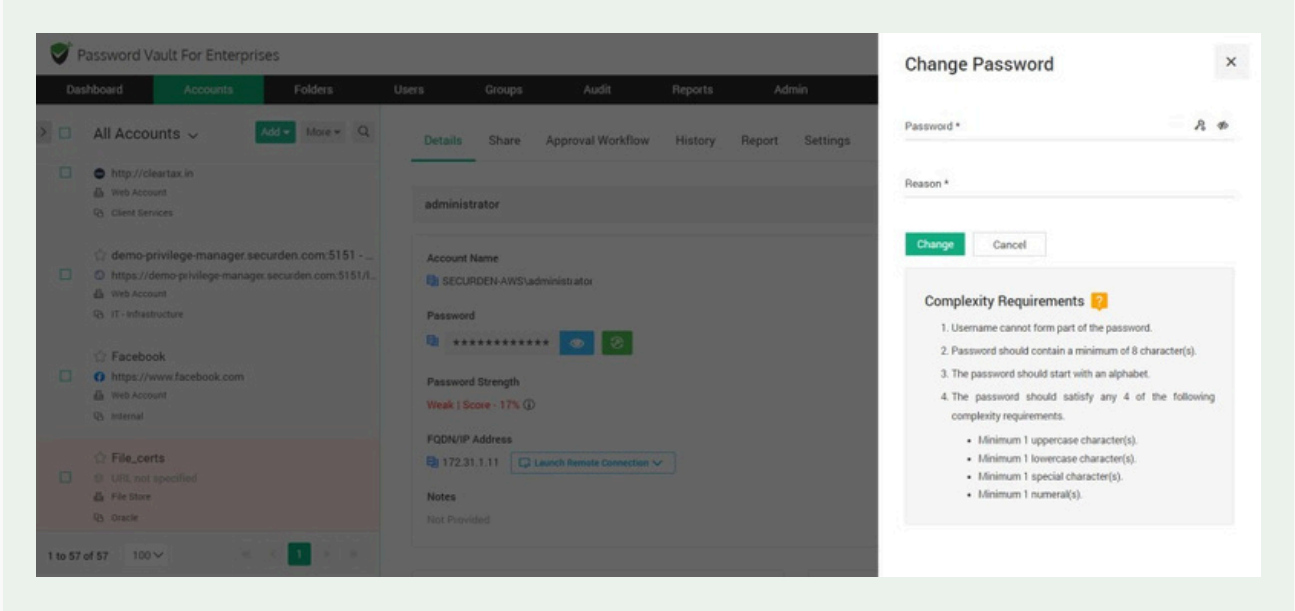


For some sensitive accounts, if the administrator had enforced the approval workflow, you would have to click '**Request Access**' to raise a request to get access to the password.

The bottom of the 'Details' section provides more information about the other attributes of the account. In addition, security-related information such as account creation time, ownership details, last access, and modification details are also displayed. Click 'Show More Details' link to view these details.

Change Password

If your administrator has given the '**Modify**' permission for an account, you will be able to change the password, not just locally, but also on the remote devices. When you click the green '**Change button**' to change the password, it opens a dialog where you can specify the new password.



You can also make use of the password generator, which helps generate strong passwords. When you select the option “Change the password on remote machine”, the new password will be applied on the remote device too. In addition, you may have to justify why you are changing the password by mentioning the reason. The reason you enter here is captured in the audit trail.

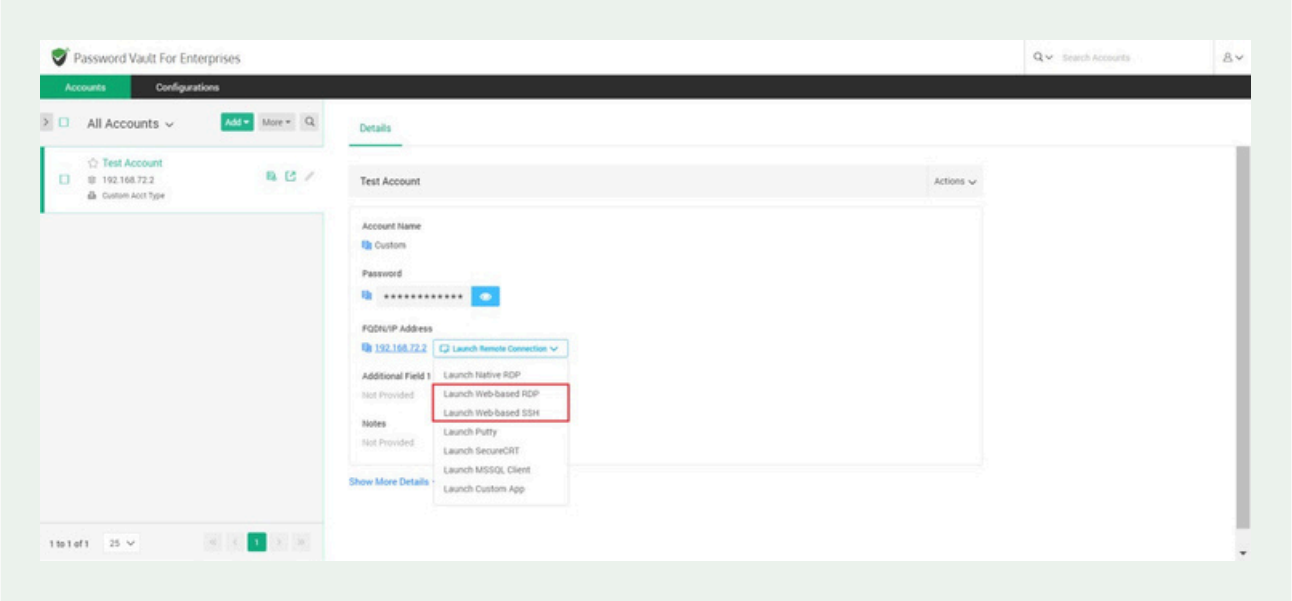
Launching Remote Connections using Password Vault (RDP, SSH, SQL, Website Connections)

You can launch direct remote connections with Windows, Linux, and other devices from Securden GUI. You can straightaway launch web-based connections or use native client applications. The choice of web-based connection is available for RDP and SSH. Native client application support is offered for all RDP, SSH (PuTTY, SecureCRT), and SQL connections.

Web-based Connections

Web-based remote connections support (RDP and SSH) is readily available. There are no pre-requisites for this option. You can launch connections using a web browser directly without installing anything. To launch web-based RDP,

SSH connections, select the required account, click “Launch RDP Connection” or “Launch SSH Connection” and then choose the web-based option.



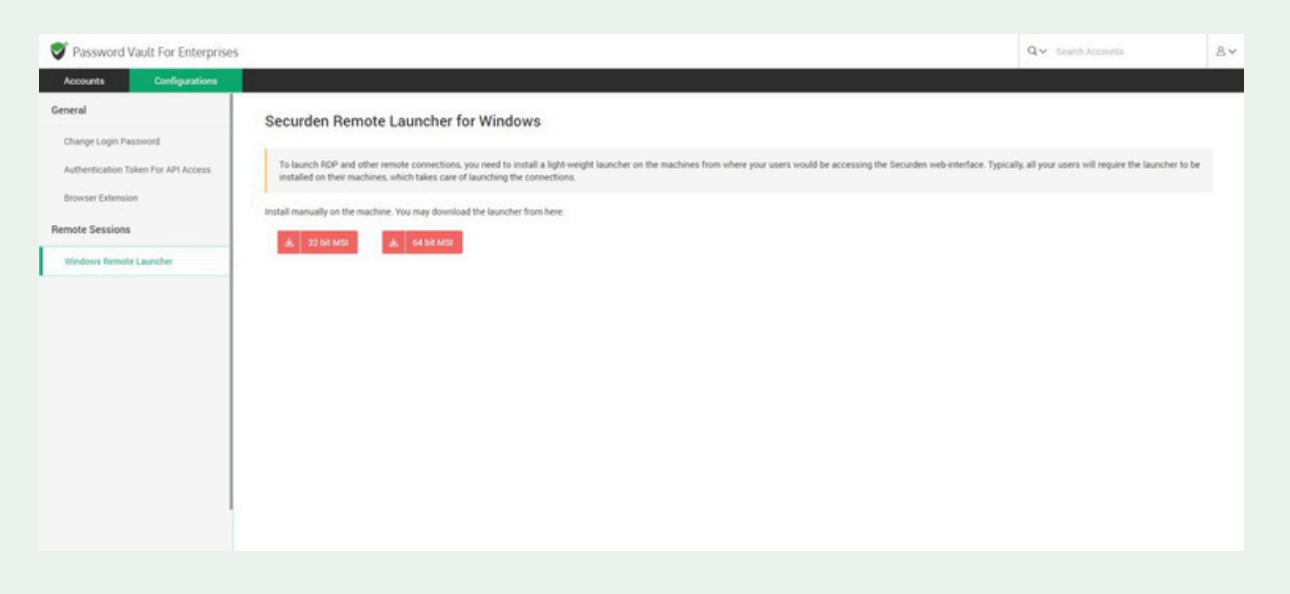
Using Native Client Applications

To use native client applications for RDP, SSH (PuTTY, SecureCRT etc.) and SQL, a lightweight launcher application has to be installed in all the end-user machines.

Launcher for RDP Connections

As mentioned above, to launch RDP connections, you need to install a lightweight launcher called ‘Securden Remote Launcher’ on all the machines from which you would be connecting to Securden web interface.

The launcher can be downloaded and installed from Configurations >> Remote Sessions >> Windows Remote Launcher.



To launch RDP connection

Navigate to Accounts section in the GUI, click the required account, click the 'Launch RDP Connection' button appearing alongside the account information on the left-hand side.

To launch SSH connections

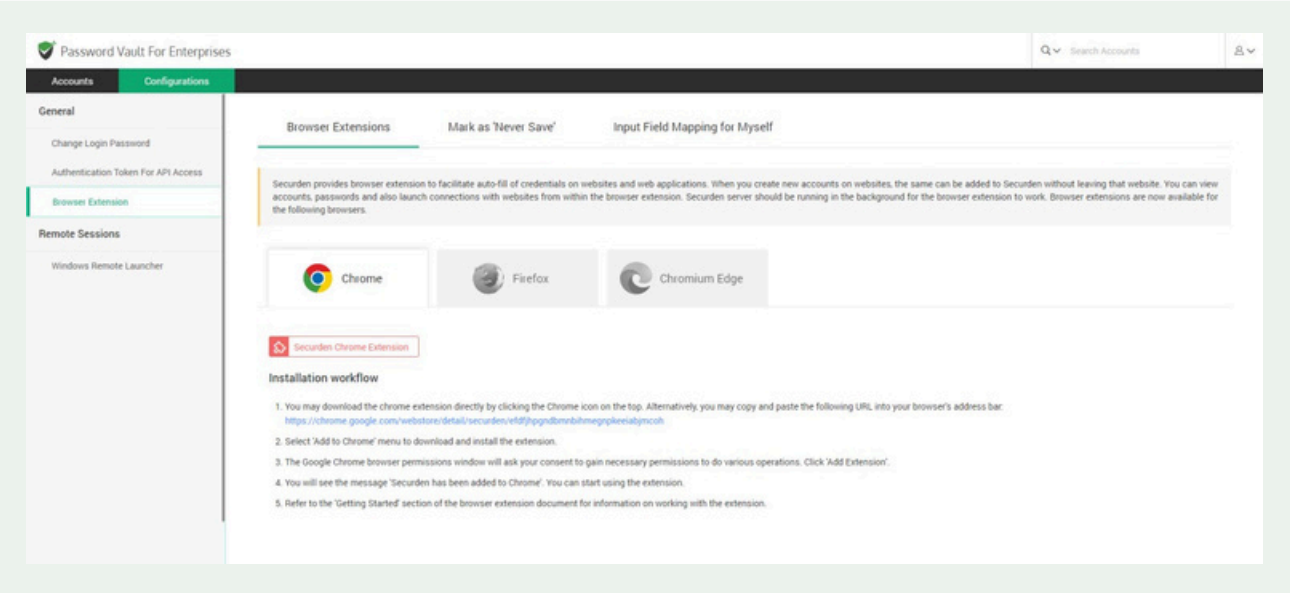
Navigate to Accounts section in the GUI, click the required account, click the 'Launch SSH Connection' icon appearing alongside the account information on the LHS. (As mentioned earlier, web-based SSH connections don't require installation of remote launchers).

To launch SQL connections

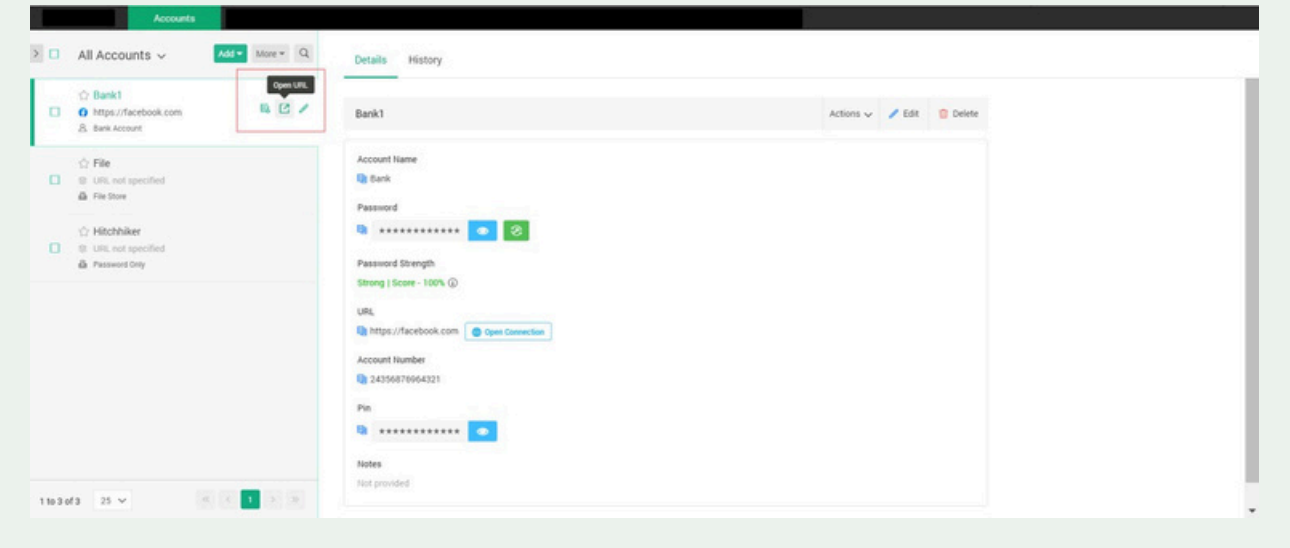
Navigate to the Accounts section in the GUI, click the required account, click the 'Launch SQL Connection' icon appearing alongside the account information on the LHS.

Auto-fill Credentials on Websites

Pre-requisite: Securden provides browser extensions to facilitate auto-fill of credentials on websites and web applications. Securden browser extensions are now available for Chrome, Firefox, and Edge. You can install the browser extensions from the **Configurations >> General >> Browser Extensions** section in the GUI.

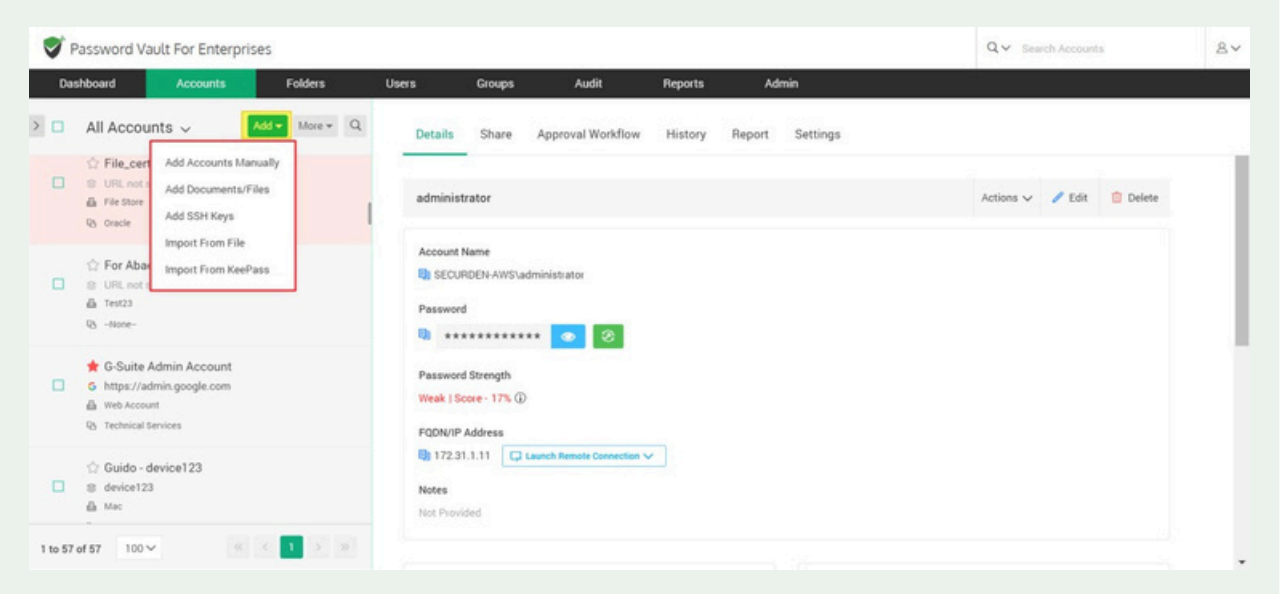


To auto-fill credentials/automatically login to a website, click the required account, click the **Open URL** icon appearing alongside the account information on the LHS.



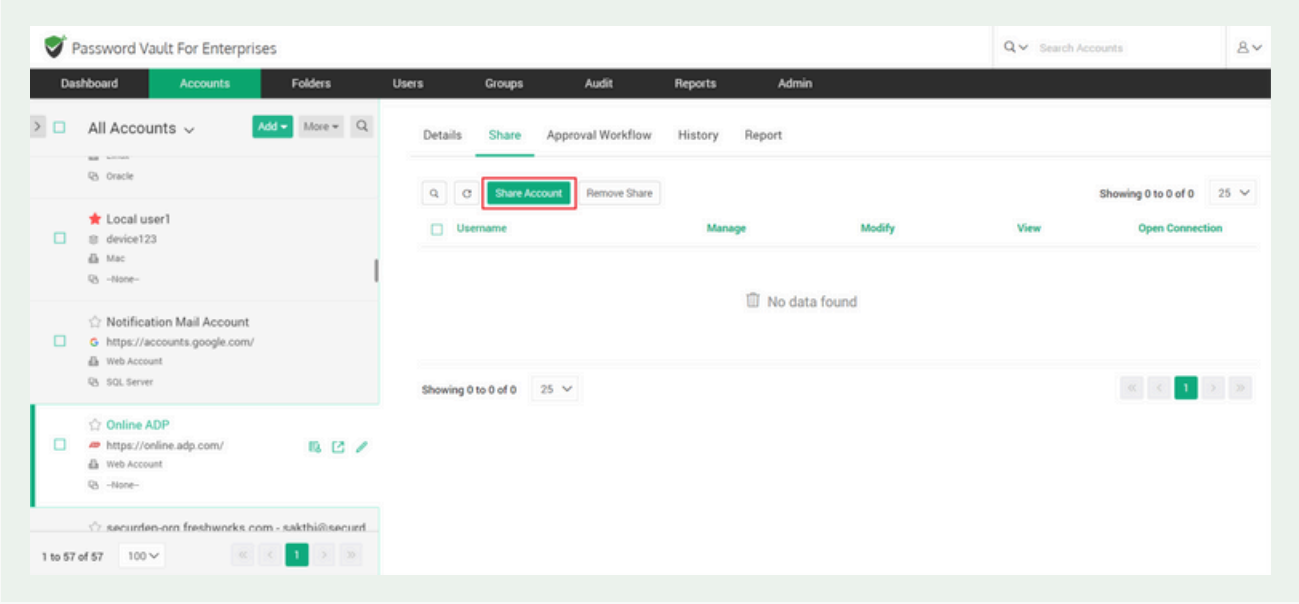
Adding new accounts and sharing them

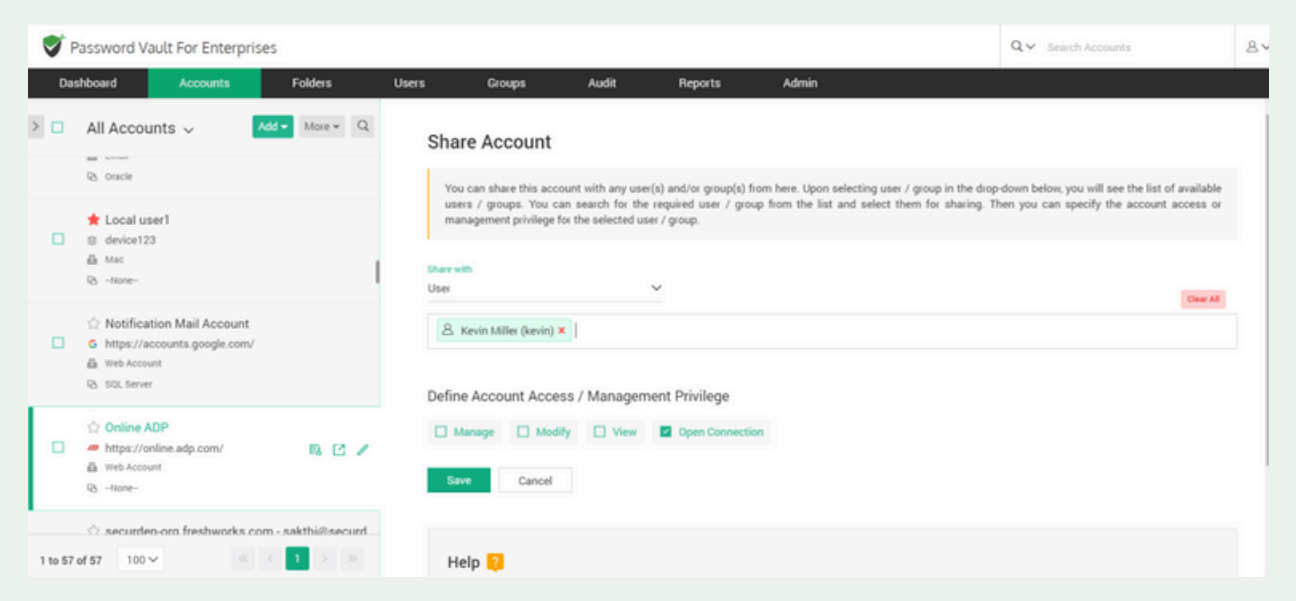
As a password vault user, you can add accounts in the vault and share them with other users if necessary. Click on **Add** and pick a suitable option as shown below.



Sharing Accounts

Once you add an account it is visible in the accounts tab. You can share the account with other users/user groups in your organization. Select the account to be shared, click on **Share** and select the users/groups.





Once you select the user, you can define the account access privilege and click **Save**.

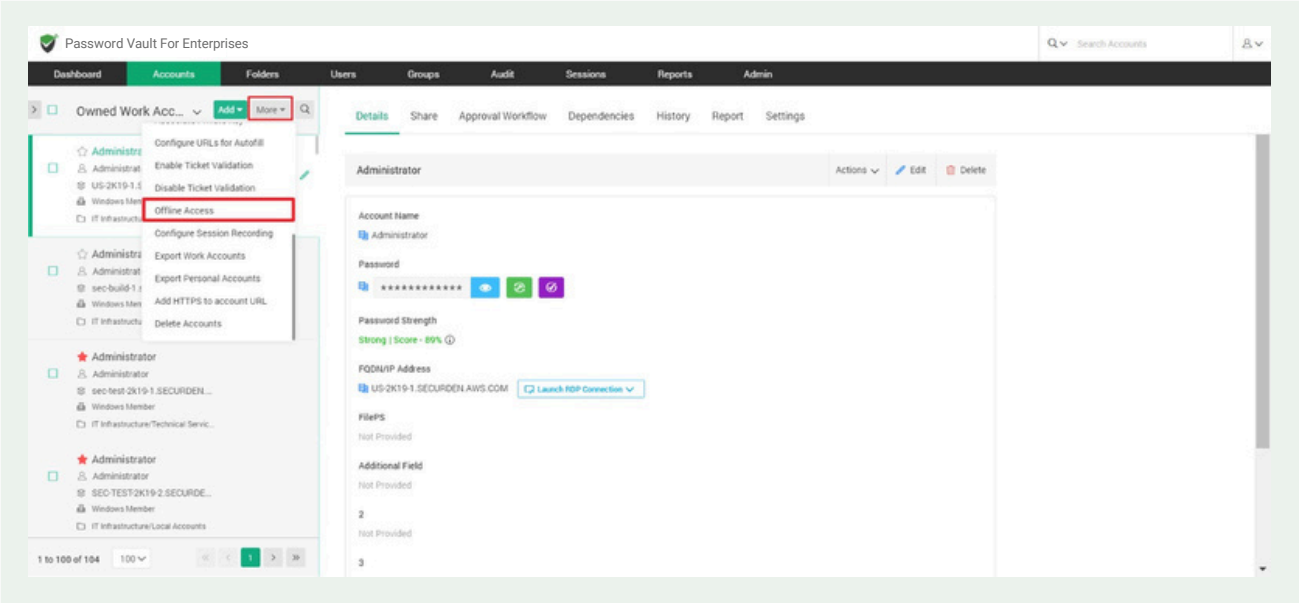
Configure Offline Access

As an end user, you can access your accounts and passwords even when you go outside your network or don't have internet access. Securden provides the passwords in the form of an encrypted HTML copy for offline access. You can open this file in any web browser, and you will see the same interface as that of the online version.

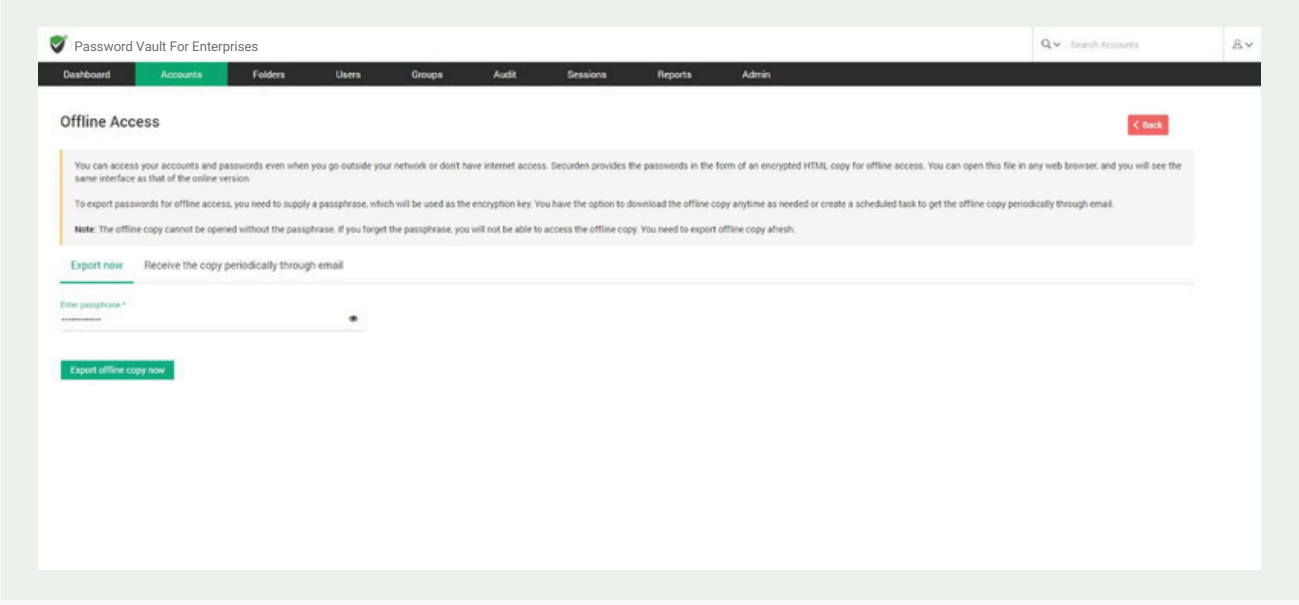
To export passwords for offline access, you need to supply a passphrase, which will be used as the encryption key. You have the option to download the offline copy anytime as needed or create a scheduled task to get the offline copy periodically through email.

Note: The offline copy cannot be opened without the passphrase. If you forget the passphrase, you will not be able to access the offline copy. You need to export offline copy afresh.

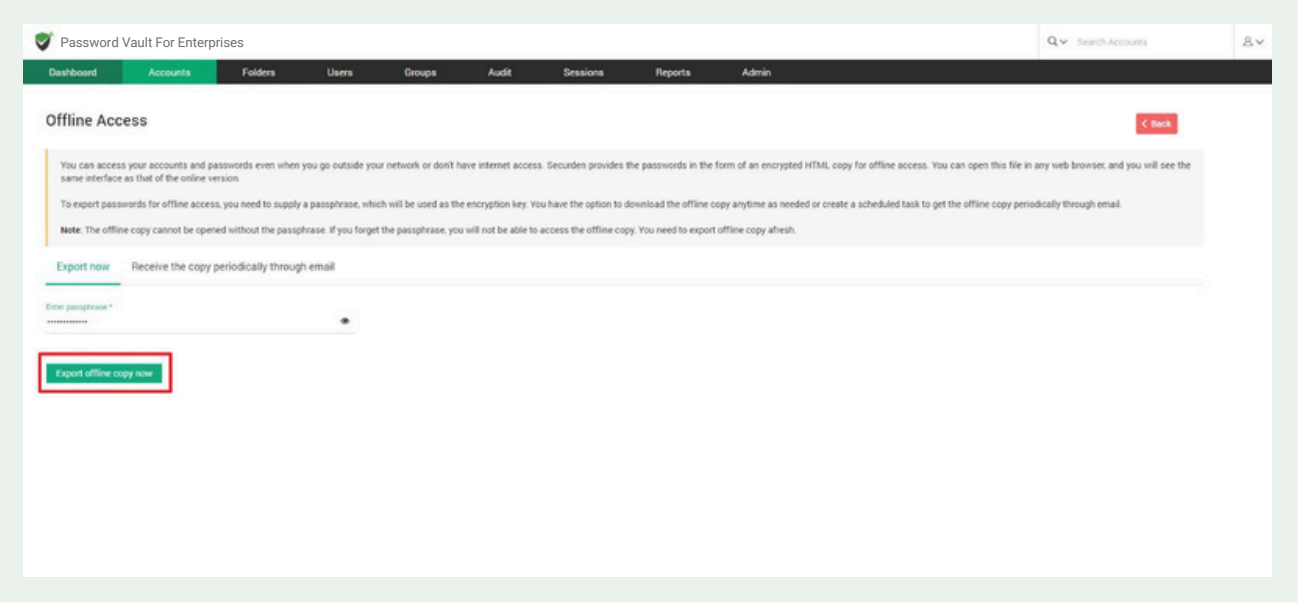
End-users can save an offline copy of all accounts they have access to. Users need to navigate to **Accounts >> More >> Offline Access.**



Users can export the account at once from the **Export now** tab, they need to enter a passphrase to open the exported offline copy. This passphrase will be used to open the offline copy of passwords.



Once you have decided a strong passphrase, key it in and click **Export offline copy now**.

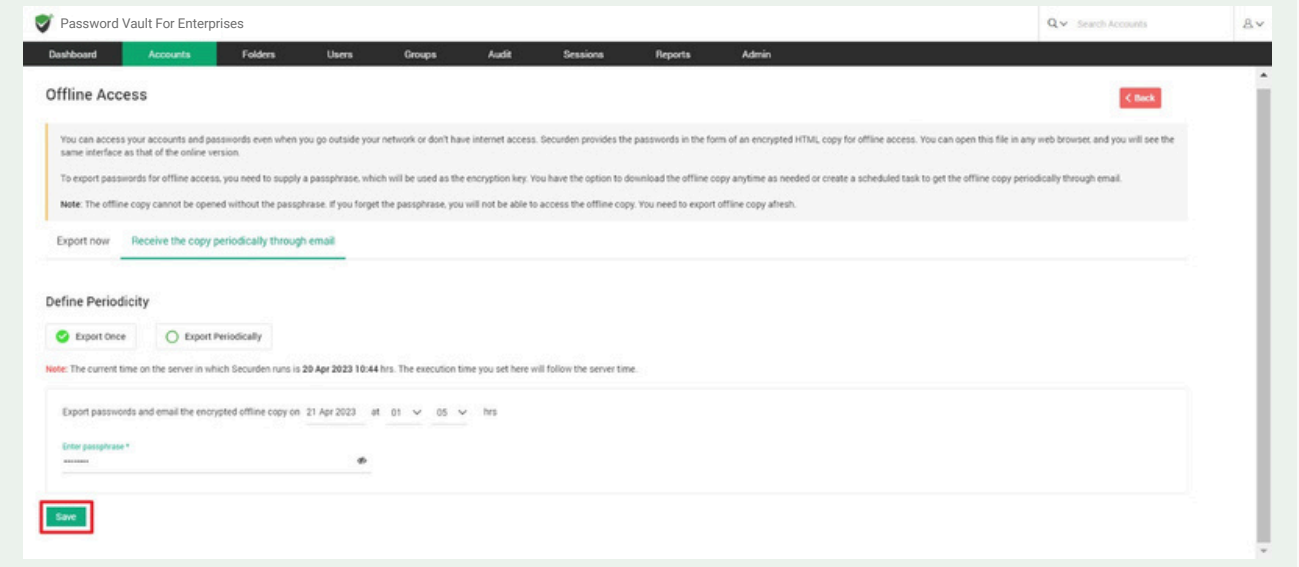


Receive the offline copy through email

Users can choose to export their passwords in an offline copy to their email id. Users who wish to export a copy once can select '**Export Once**'.

They then need to select the date and time at which an offline copy of passwords should be sent to them.

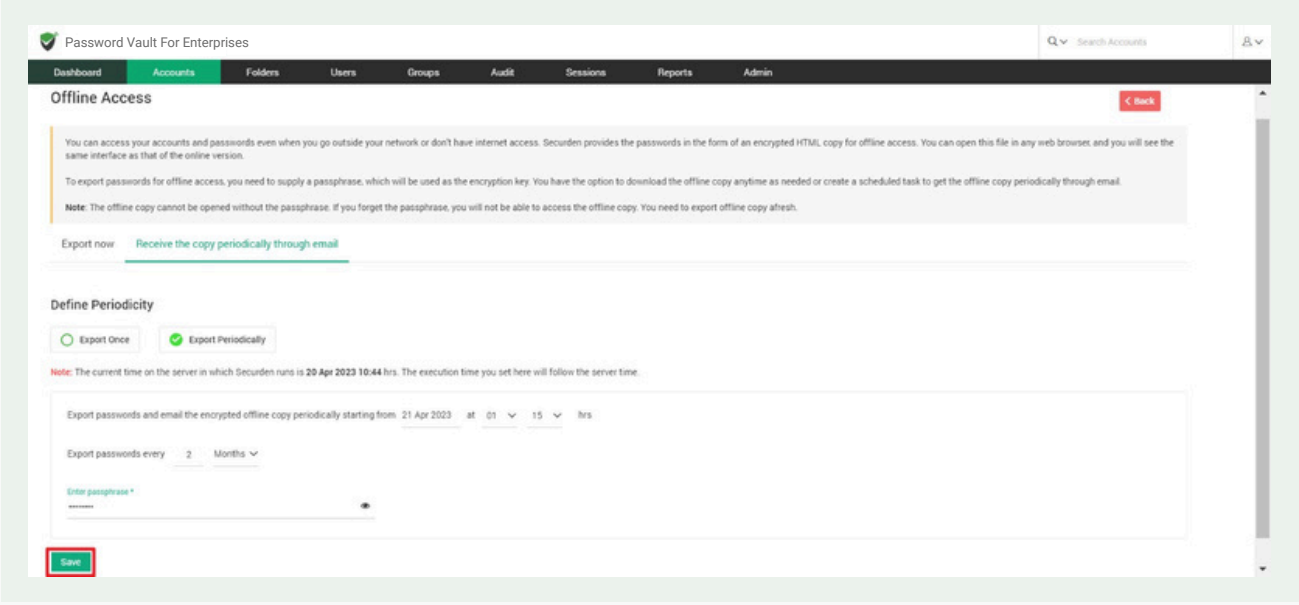
Once all the fields are selected, they can click '**Save**'.



Users who wish to periodically export their passwords can select '**Export Periodically**'.

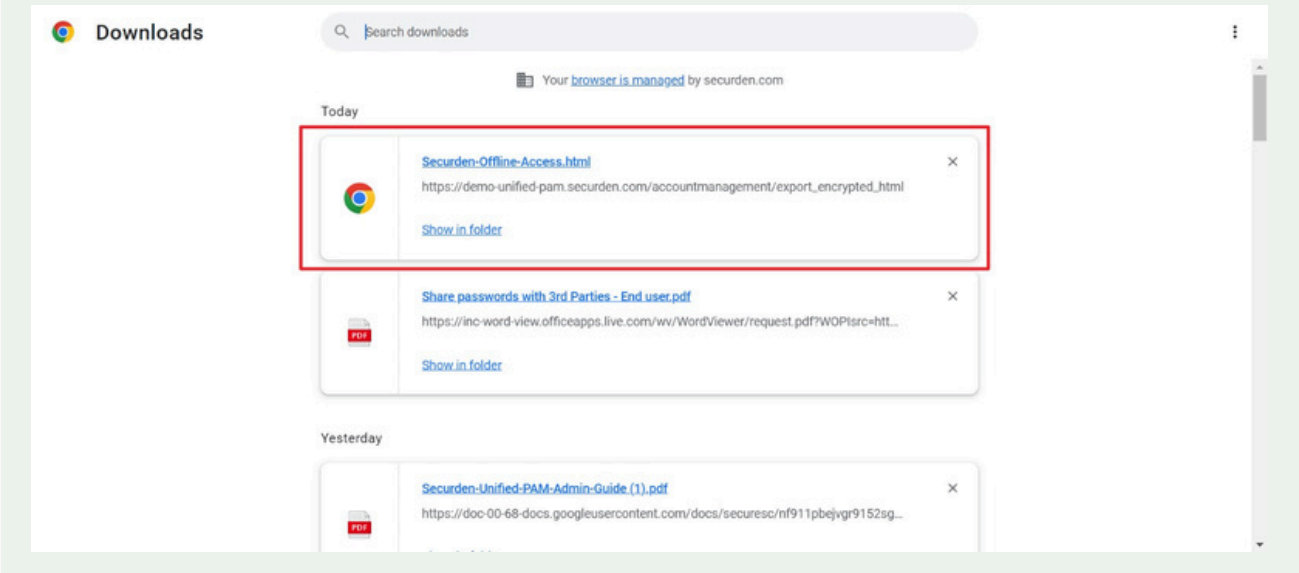
They then need to select the date and time at which they receive the first offline copy of passwords.

Users must then specify the periodicity at which they receive subsequent copies. This can be set as an interval of Hours, Days, or Months.

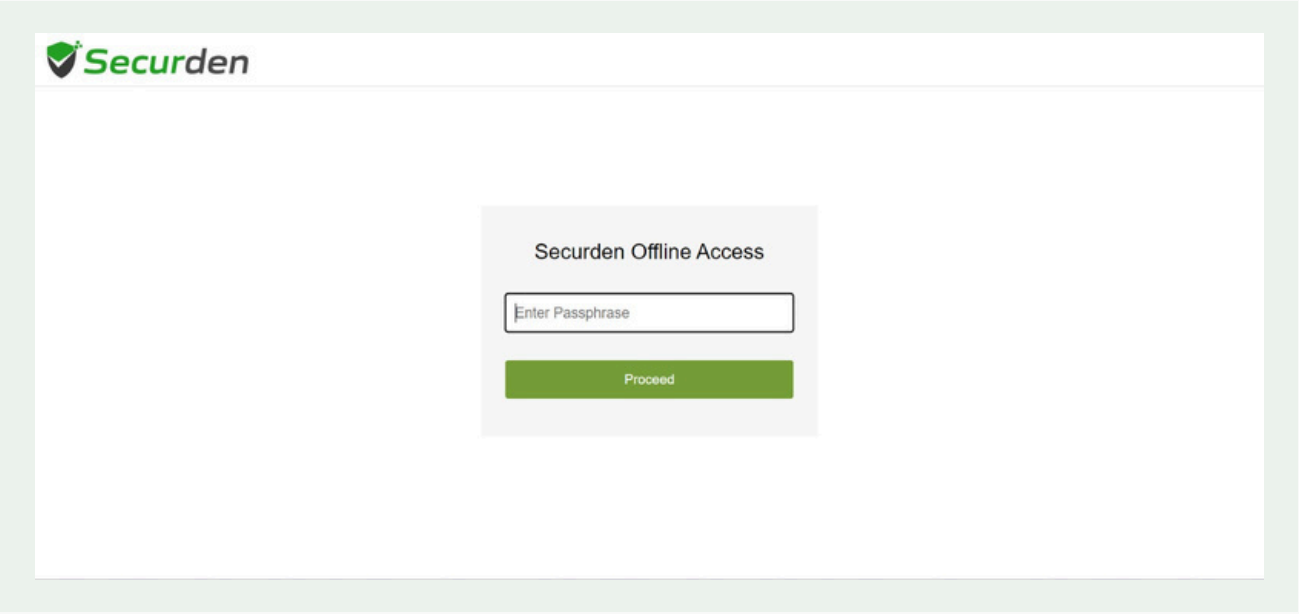


Once all the fields are selected, they can click '**Save**'.

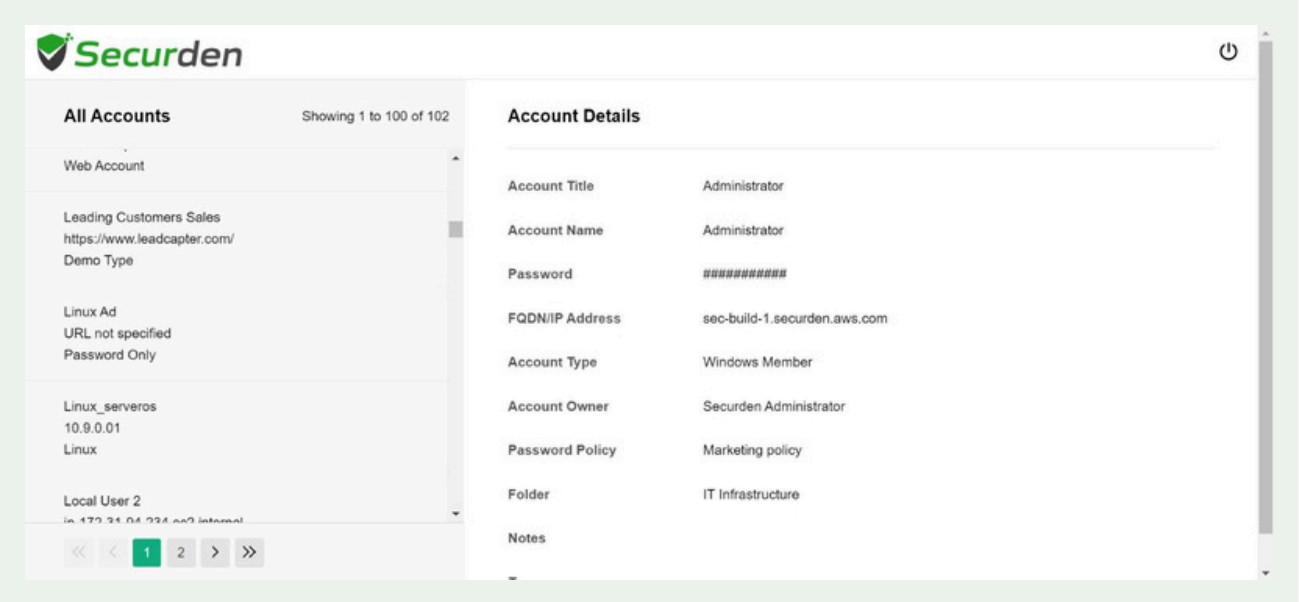
Users can access the downloaded HTML or access it from their email id.



On clicking the link, users have to enter the passphrase that they keyed in on configuring offline access.



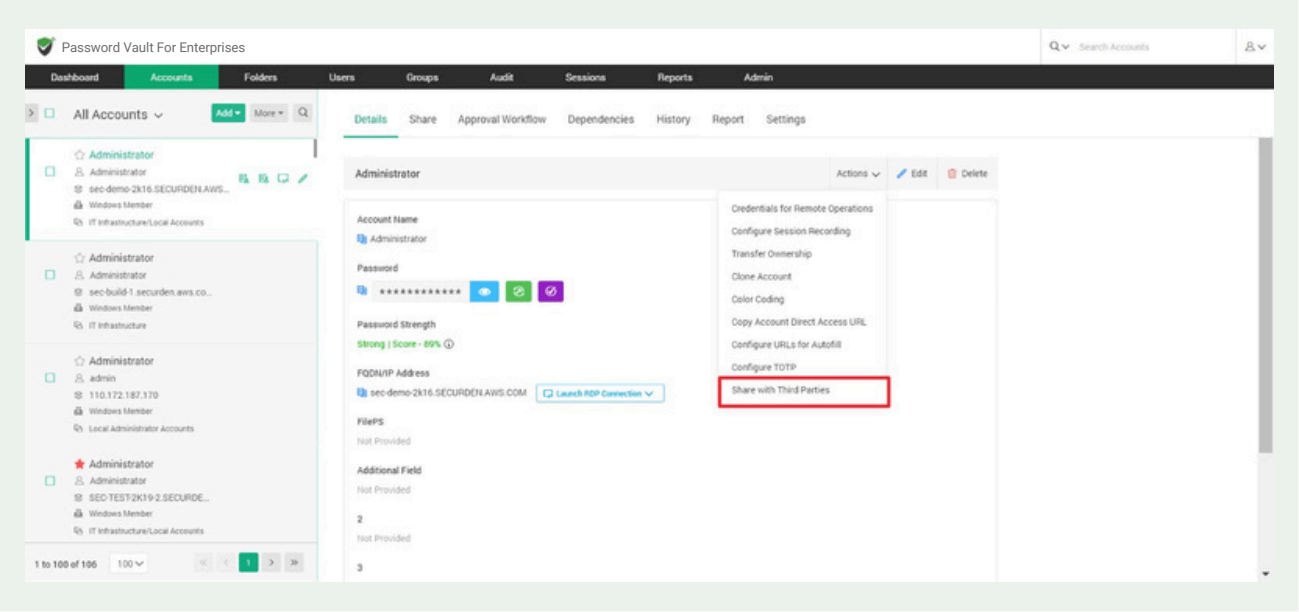
On successfully entering the passphrase, users can access all their passwords offline.



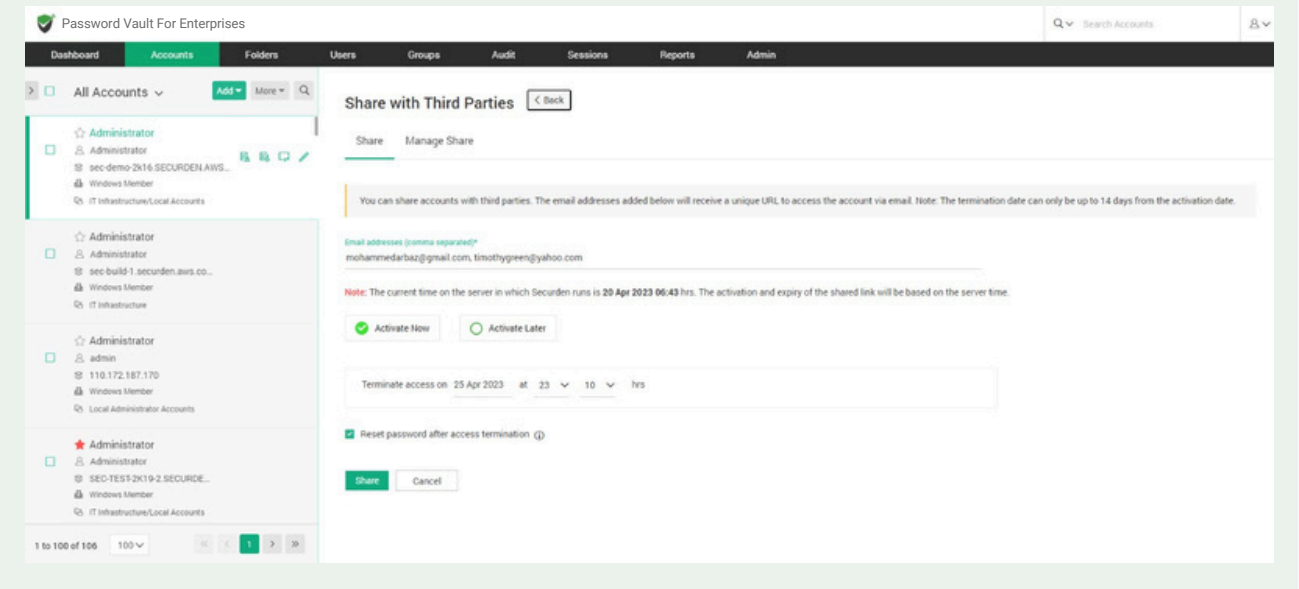
Share Passwords with Third Parties

Any user in Securden can share accounts owned by them/shared with them to a third-party user outside the organization. They need the email address(es) of the third party who needs access to the account. **Pre-requisite**: As a prerequisite to send accounts to external user emails, you need to configure the email server settings which are available under **Admin >> General >> Mail Server Settings.**

To share an account, navigate to **Accounts >> Select the account to be shared >> Click on 'Actions' >> Select 'Share with Third Parties'**



This opens up the GUI shown below:

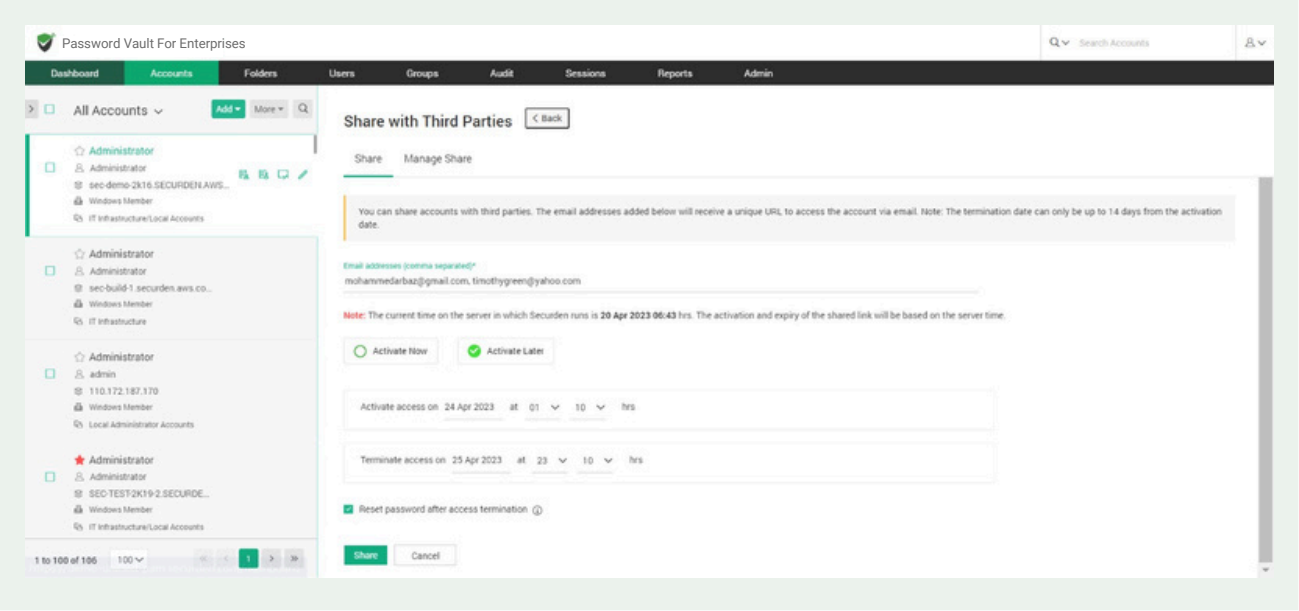


Each account is shared with an access timeframe to the third-party users. You need to specify the following details before sharing the account:

- **Email addresses:** If you are sending this account to one or more people, you need to specify their email addresses in a comma separated format.

- **Activate Now:** You can select this option to allow the third-party to access the account immediately after sharing it.

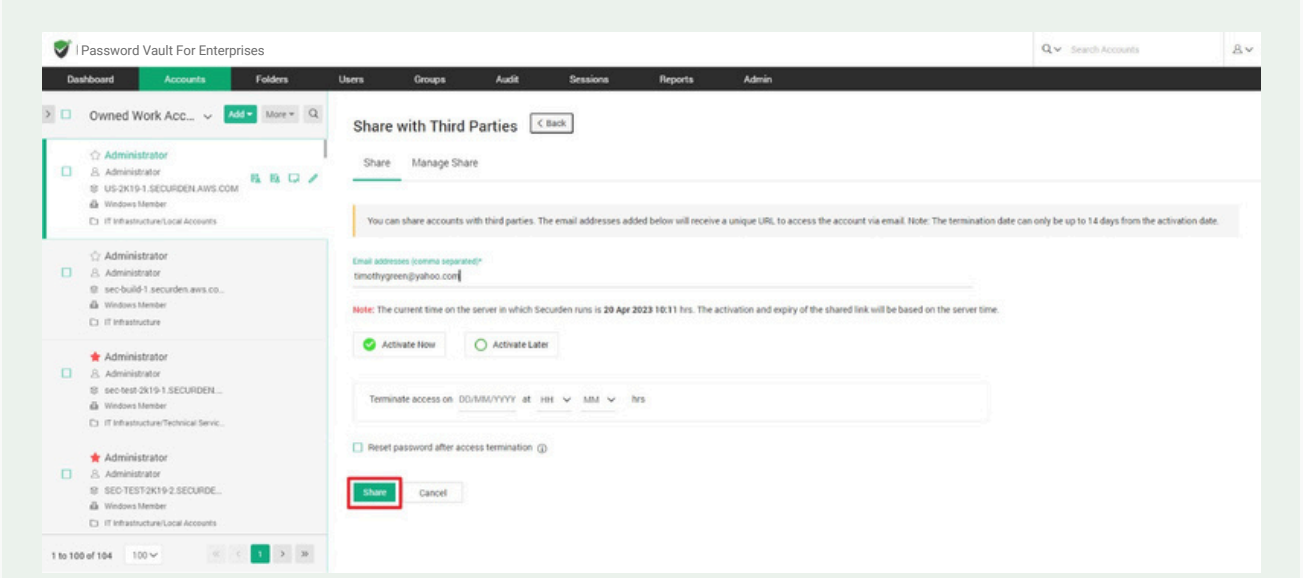
- **Activate later:** You can select this option to allow the third-party to access the account from a specified date and time.



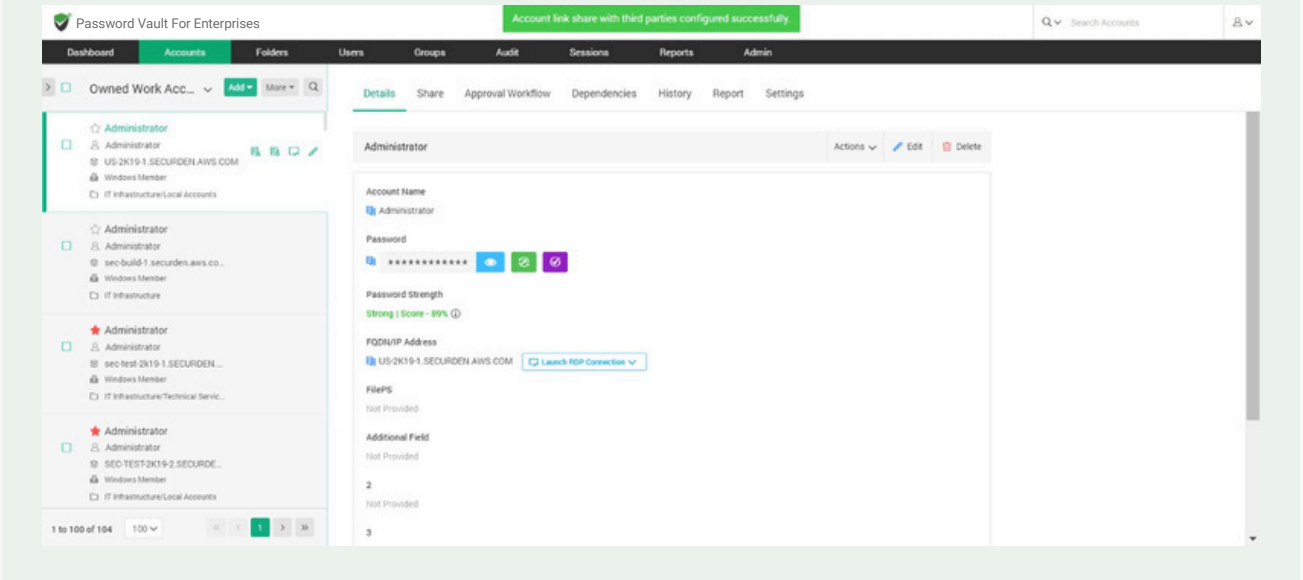
- **Terminate access:** You have specify when the account access should be revoked from the third-party. Specify the date and time after which they will be unable to access the shared account.

- **Reset password after access termination:** Enabling this checkbox will ensure that the password of the remote machine is changed after the third-party access is revoked.

Once you have set up the access duration and password reset configurations, click on **Share** to send the account as a HTML link to the third party.

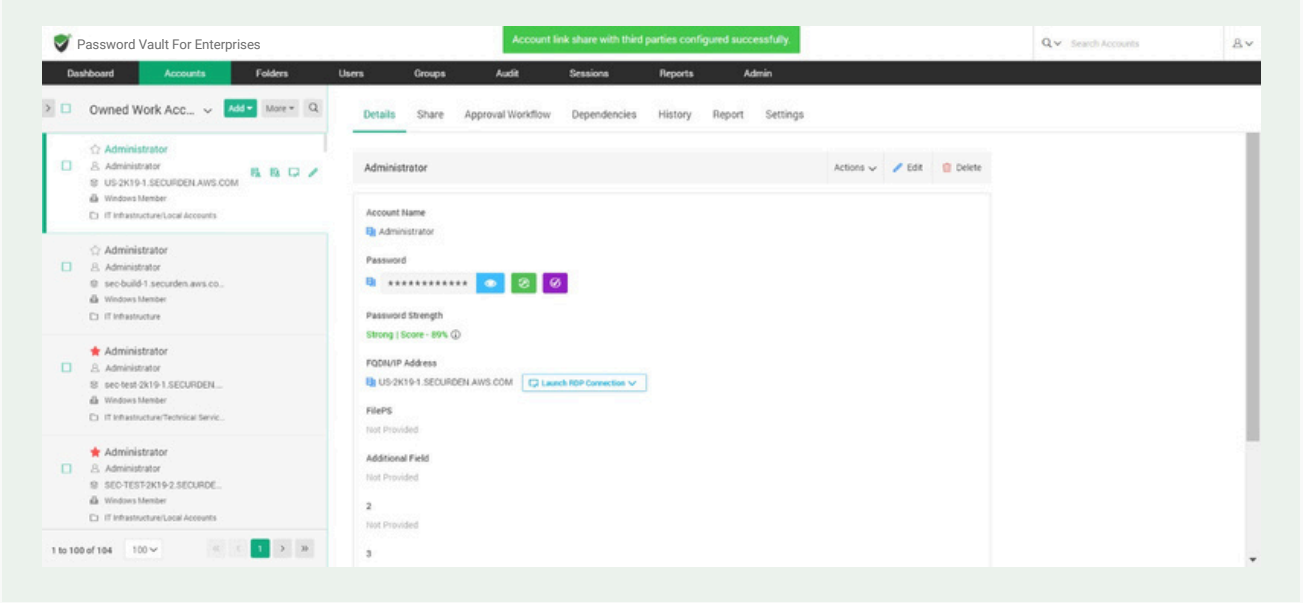


If this is successful, you will receive a message as shown below. The external user will now have access to the account.



Manage Share Permissions

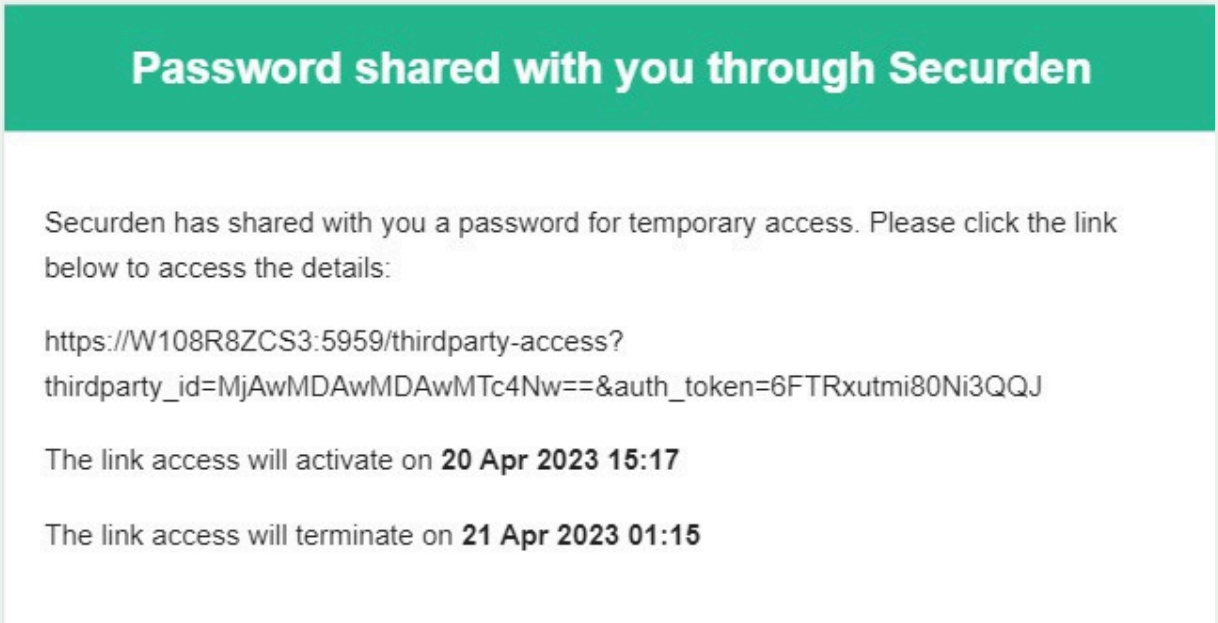
You can see which external users have shared access to this account from the Manage Share tab



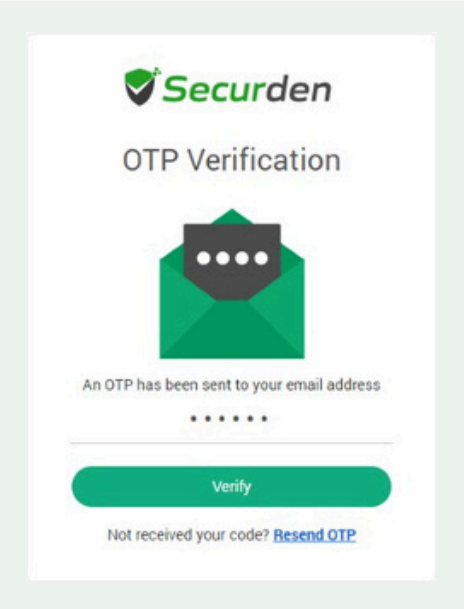
If required, you can select the email of the user and 'Terminate Access' to the account. This will end their access regardless of the time-duration defined.

How the external users access the shared account

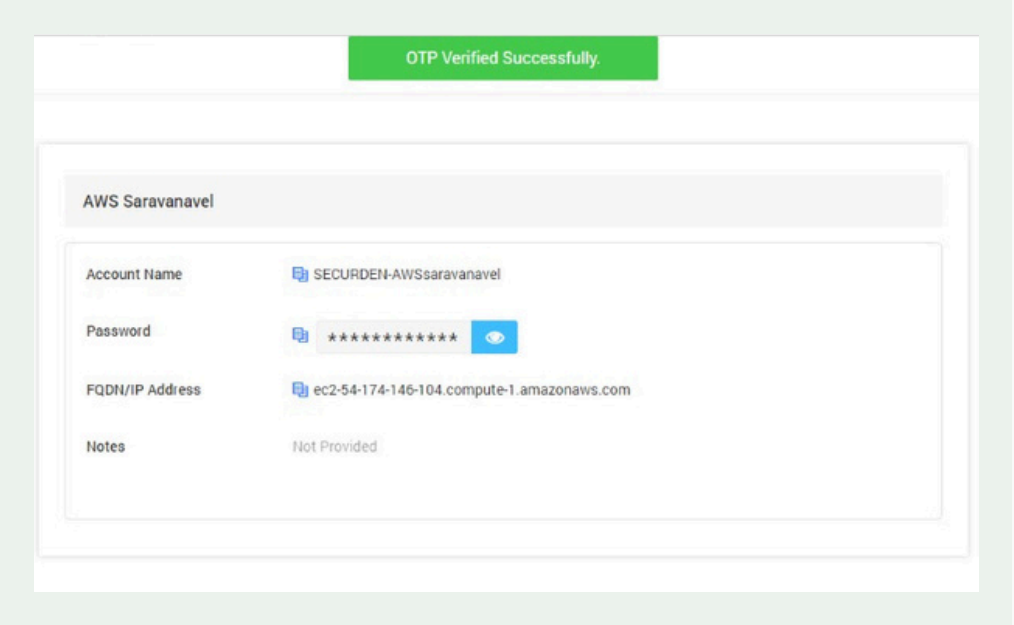
The external user who receives the shared account will find a link in their email id. This is as shown below.



On clicking the link, they will be taken to a Securden OTP verification page. This OTP can be found in the inbox of the external user.



On entering the OTP and clicking '**Verify**', they will be able to access the account shared with them.



They can click the '**View password**' to see the hidden passwords. When the duration of access expires, the account access is revoked, URL becomes unavailable, and the password of the machine is reset.

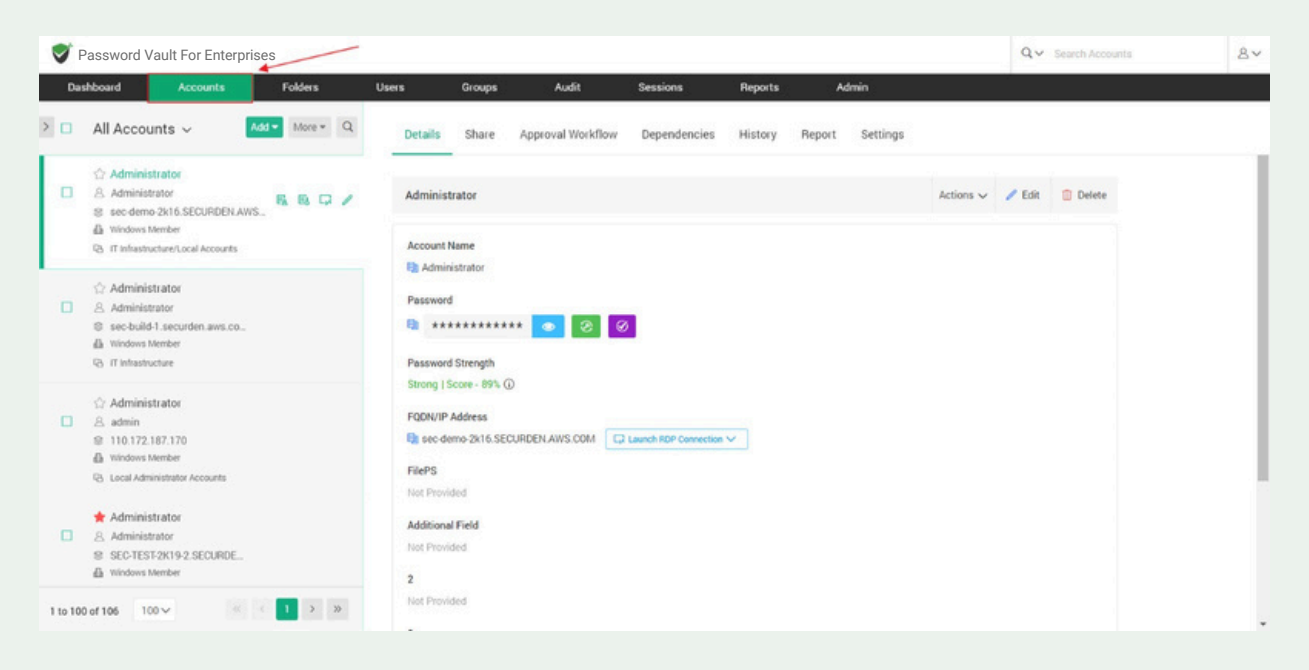
Configure Autofill on URLs

Securden helps you to autofill username and passwords on web applications and webpages. You can specify the URLs on which the username and password should be auto filled. When the user launches a connection to the web application/webpages, the Securden browser extension will auto fill the credentials on the webpage.

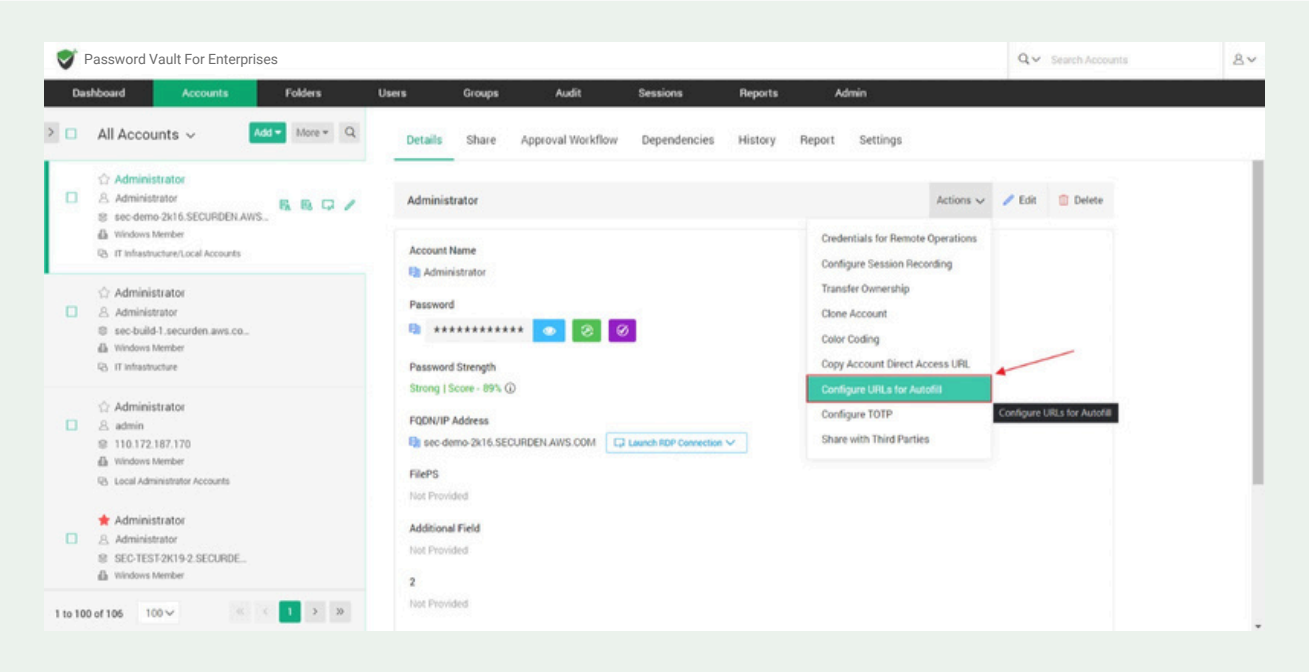
How to Add URLs to Accounts?

Follow the steps below to configure URLs for auto filling credentials.

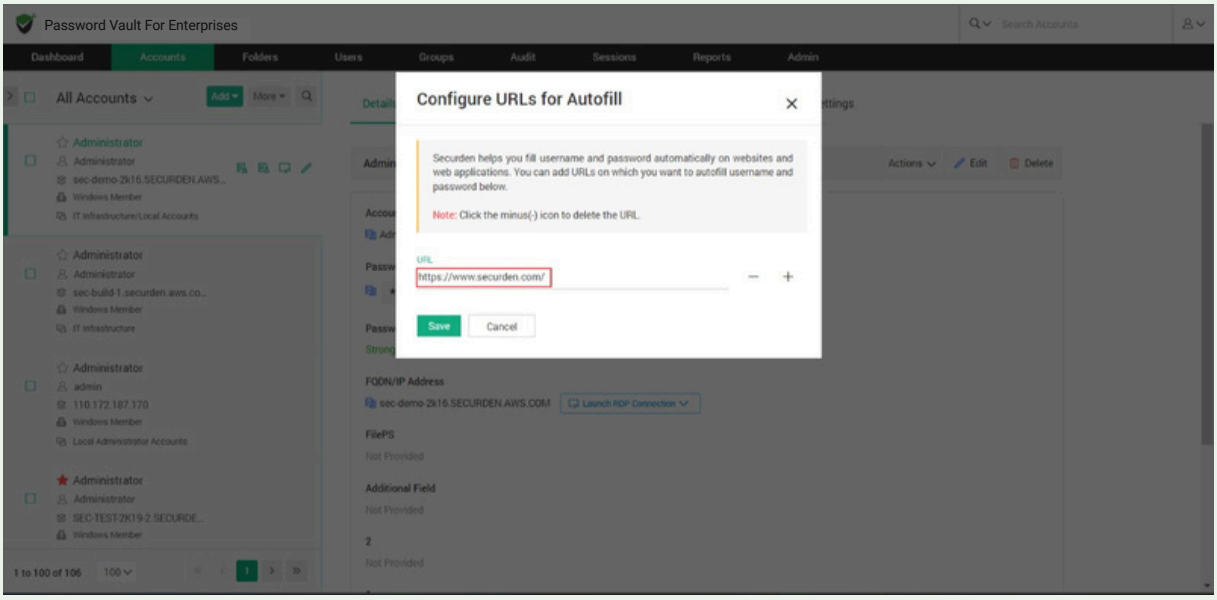
1. Navigate to **Accounts** tab and select the required account.



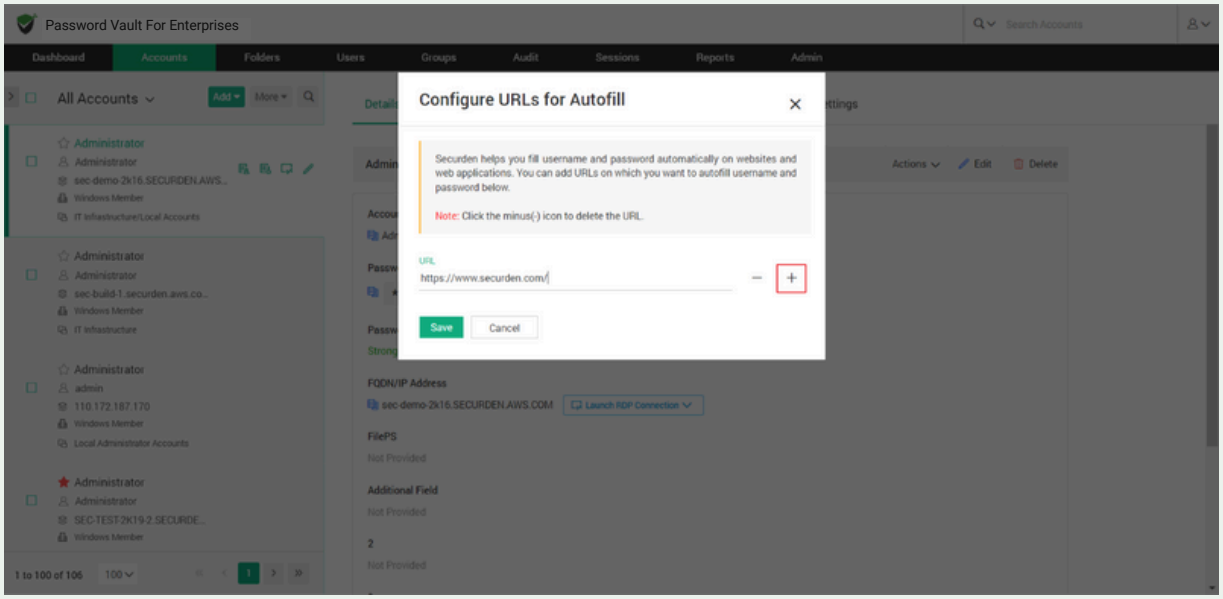
2. In the **Accounts** tab, navigate to **Actions >> Configure URLs for Autofill.**



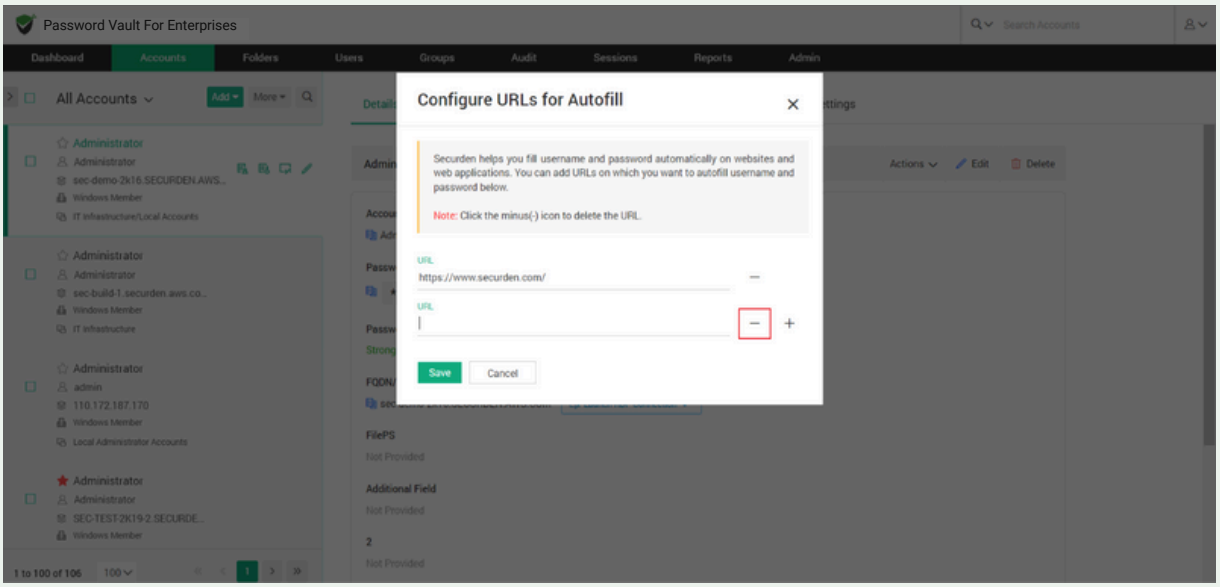
3. In the popup, you need to specify the URL on which username and password should be auto filled.



4. You can add multiple URLs on which the account credentials can be auto filled. Click on the '+' sign to add a second URL.



5. To remove a URL, click on the '-' symbol.



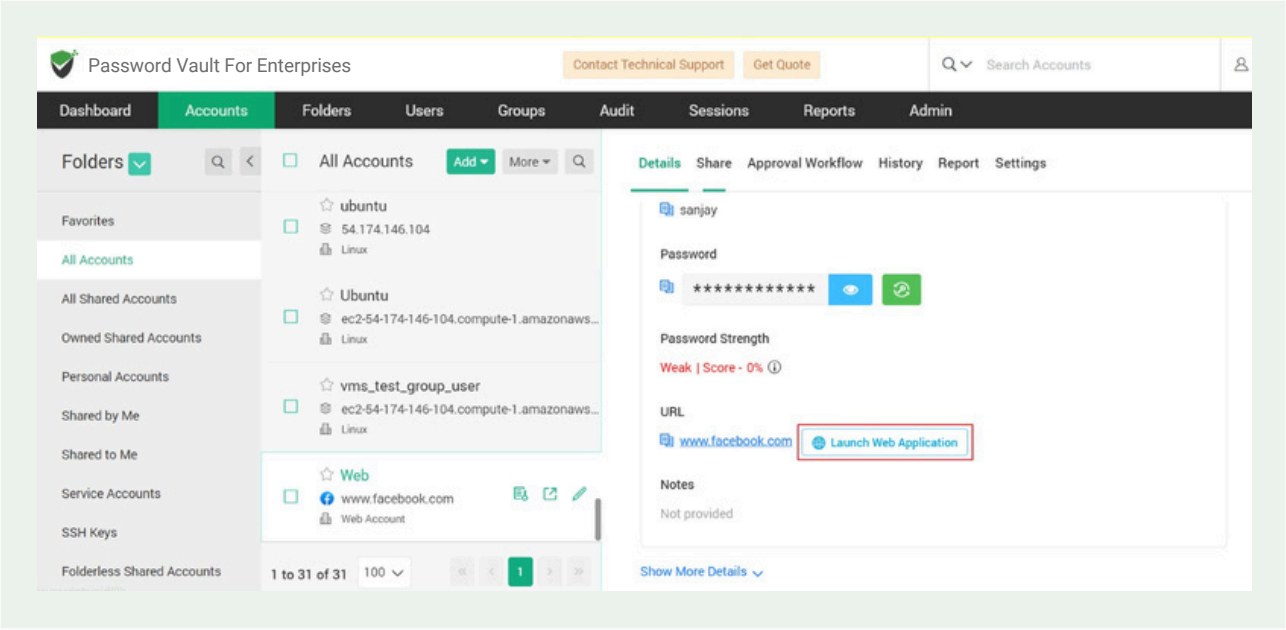
6. Once you have configured all the URLs you need, click **Save**.

How to Auto fill Credentials on the Website?

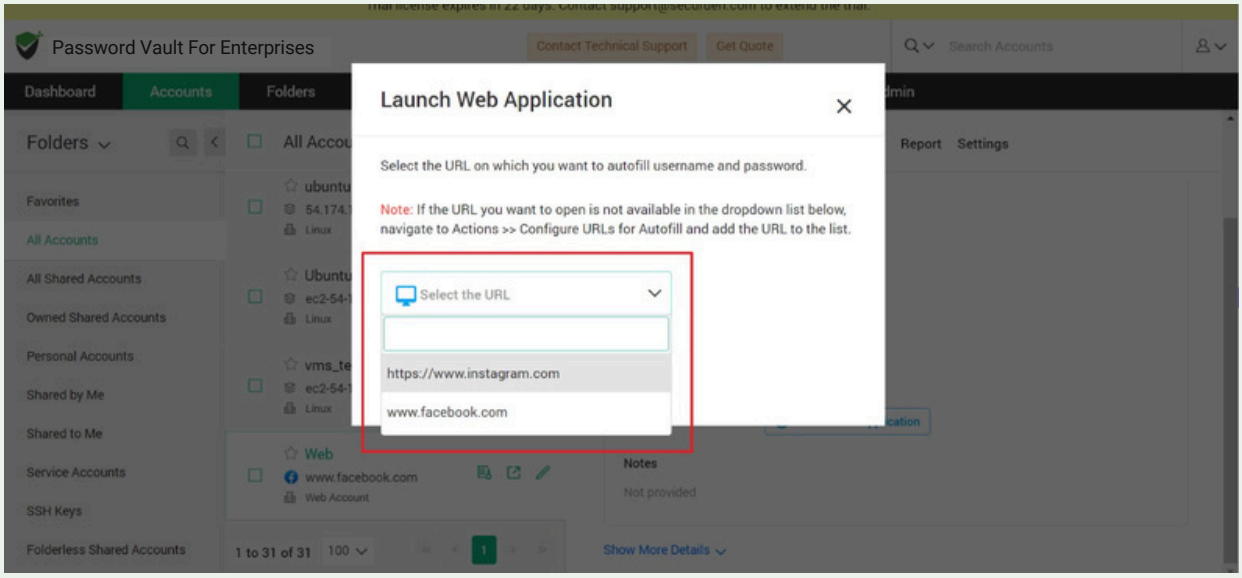
Note: You need to install the Securden Browser Extension on the required browser to be able to utilize the auto fill feature. To install the browser extension, navigate to **Admin >> General >> Browser Extension**.

Once the URLs are configured, you can connect to the webpage or web application by navigating to Accounts tab.

In the accounts tab, select the required account and click on **Launch Web Application.**



In the window that opens, all the added URLs to the selected account will be available in the drop down.



You can select the required URL and the web application/webpage will be opened and the credentials will be auto filled.