Securden

Password Vault

Administrator Guide →

Table of Contents

Section 1: Getting Started..... 6
Starting the Securden Vault Service..... 6
Launching the Web Interface..... 7

Section 2: General Configuration Settings..... 9
Configure Mail Server Settings..... 9
Proxy Server Settings..... 12
Securden Server Connectivity..... 14
Web-based RDP Connections..... 17
Web-based SSH Connections..... 17
Replace Self-signed Certificate..... 18

Section 3: User Management..... 20
User Management..... 20
Import Users from Active Directory..... 20
Import Users from LDAP..... 29
Import from Azure AD..... 34
Import Users from File..... 38
Add Users Manually..... 42
Assigning Roles to Users..... 48
Custom User Roles..... 52
User Reports..... 76
User Groups..... 82
Import User Groups from AD..... 83
Import groups from LDAP..... 87
Import from Azure AD..... 92
Explore Single Sign-On Options..... 99
Configure Single Sign-On..... 104
Configure Single Sign-On for Okta..... 104

Configure Single Sign-On for Azure AD 109
Configure Single Sign-On for Ping Identity..... 111
Configure Single Sign-On for One Login 114
Configure Single Sign-On for G-Suite 117
Configure Single Sign-On for Microsoft ADFS 119

Section 4: Configuring Two Step Verification 123
Enforcing Two Factor Authentication (MFA) 123
Mail OTP 126
Google Authenticator/Microsoft Authenticator/TOTP Authenticator 126
Yubikey 127
Global 2FA Enforcement 130
Selective 2FA Enforcement 130

Section 5: Account Management 143
Adding Accounts 143
Importing Accounts from CSV/XLSX Files 143
Adding Accounts Manually 146
Importing accounts from KeePass 153
Add and Manage SSH Keys 154
Add Documents/Files 158
View Account Details, Passwords 160
Password Management Operations 162
Launching Remote Connections 165
Web-based and native connections: 166
Launching Native RDP connections 170
Launching Native SSH connection 178
Launching Native SQL connections 179
Launching connections to thick application clients 179
Share Accounts/Passwords with Third Parties 195
Just-in-time Access through Approval Workflows 201
Accounts Report 206
Performing Operations on Multiple Accounts 217

Add and Manage Account Types 217
Offline Access 230
Delete Accounts 237

Section 6: Notifications 239
Event Notification 239
Account Expiration Notification 241
Password Expiration Notification 243
Breached Password Identification..... 244
Expired Password Rotation 247
Event Listener 249

Section 7: API Access 260
APIs for Programmatic Access 260

Section 8: Folder Management 268
Organize Accounts with Folders 268
Import Folders from Files 270
Share Folders 283
Configure Automated, Periodic Remote Password Resets 289
Folder Reports 293
Folder Settings 293

Section 9: Audits 302
Account activities: 302
User activities 309
Session Trails: 311
Export and scheduled export: 312
Event notification: 312
Add Assets for Remote Connections 313
Domain Accounts - Asset Associations 318
User – Assets/Application Association..... 323
Custom Application Launcher 327
Creating a native app launcher profile 332
Creating a custom app launcher profile 335

Launching Remote Connections Using the Custom Launcher 336
Take connections through Remote Gateway 336
Configure an existing app launcher profile 337

Section 10: Customization 338
Customize Password Vault 338
Configurations 338
Login Page Text 368
Color Theme 369
Product Language Selection 370

Section 11: Security Settings 372
Change the Encryption Key Location 372
IP Address Restriction 374
Block Access through API, Extensions, Mobile Apps 375

Section 12: Emergency Access Settings 377
Configure Emergency Access 377
Disaster Recovery Settings: Database Backup..... 380
Backup of Passwords as an Encrypted HTML File..... 383

Section 13: High Availability 384
Configure High Availability 384

Section 14: Reports 395
Standard Reports 395
Concise Reports 406
Account Management 407
User Management 407
Password Security Analysis 408

Section 15: Miscellaneous 411
Change Database..... 411
Browser Extensions 414
Moving Securden Installation from One Machine to Another 419

Section 16: Product License Key 420

Note:

This administrator guide also includes features that are available in the **Enterprise PAM Edition** of Securden Password Vault. You can find them labeled as ENTERPRISE PAM

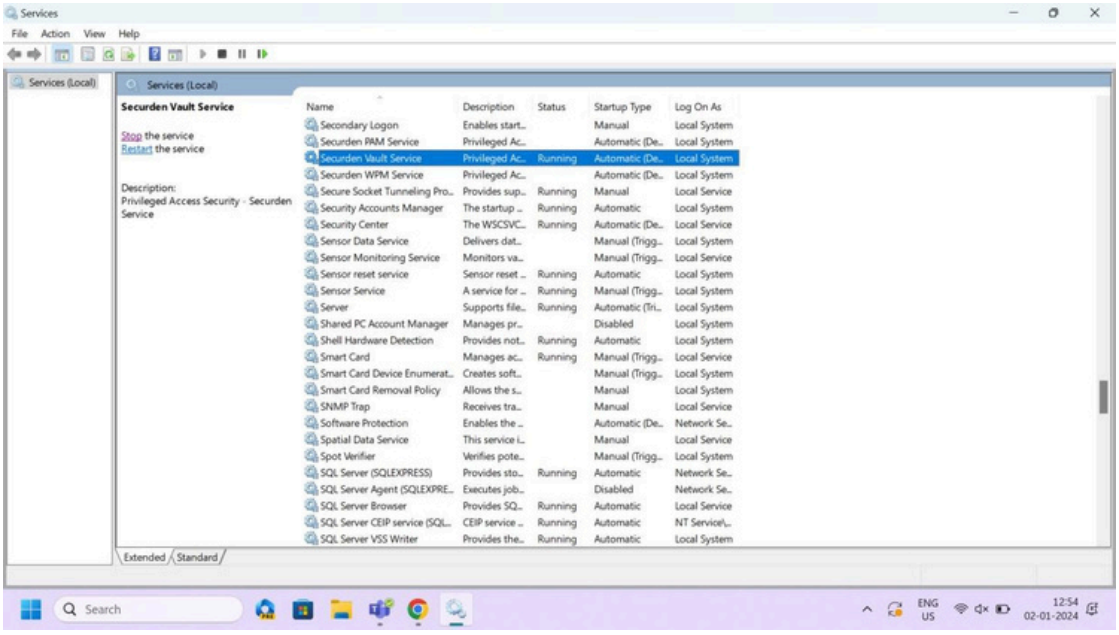
If you want to try the free version of **Enterprise PAM**, you can begin by signing up for a free trial here.

Section 1: Getting Started

Starting the Securden Vault Service

• You can start and shut down the Vault service from the Windows Services Manager.

• Locate **Securden Vault Service** and start or stop it as required. This takes care of starting and stopping the dependent services too.



Note: You need not start **Web Service – Securden Vault** manually, as Securden automatically takes care of this.

Troubleshooting tips:

1. The Vault Service/Web Service does not start automatically Ensure the following:

- The **Securden-cert.pem** file must be present in the **<Securden Installation directory>/Conf** folder.
- Web Service – Securden should be set to **Manual**.
- Securden Vault Service needs to be set to **Automatic (Delayed Start).**

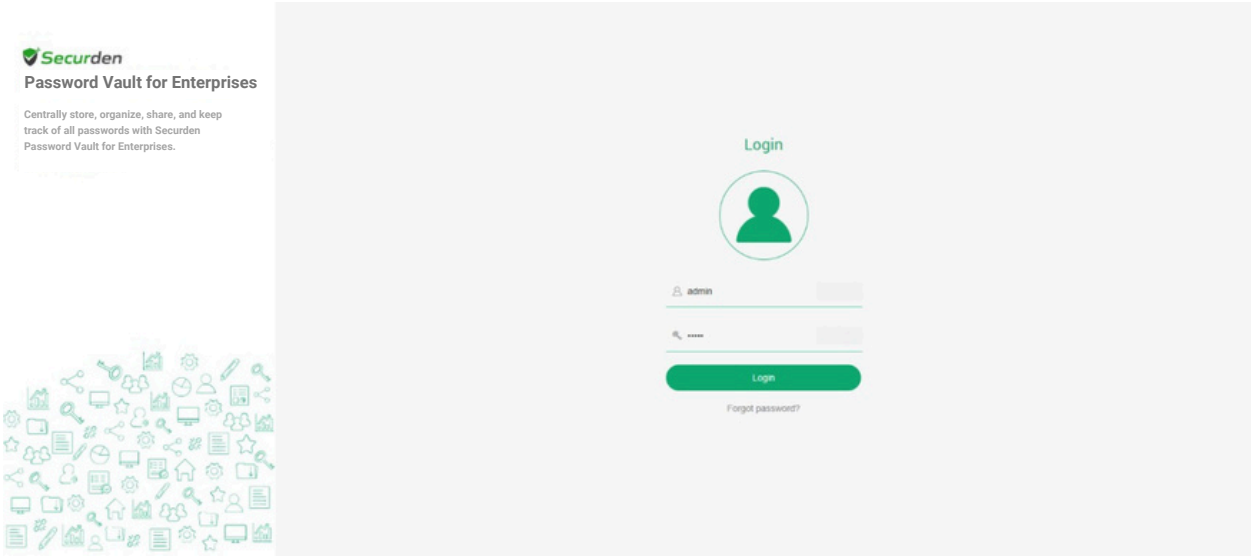
Launching the Web Interface

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

https://<Vault server hostname>**:5454**

If you have configured a port to be something other than the default port **5454**, you need to enter that port in the URL instead.

In the web-login page you need to enter the login credentials.



To access the initial unconfigured setup, make use of the default login details as below:

Username: admin

Password: admin

Troubleshooting Tips:

During this process, you might see warning messages displayed by the browsers. This message appears because Securden comes bundled with a self-signed certificate. (If your administrator adds a CA-signed certificate, this message will vanish)

- In Chrome, click **Advanced** and then click **Proceed to <hostname> (unsafe).**

- In the case of Internet Explorer, click **Details** and then **Go on to the webpage.**

Section 2: General Configuration Settings

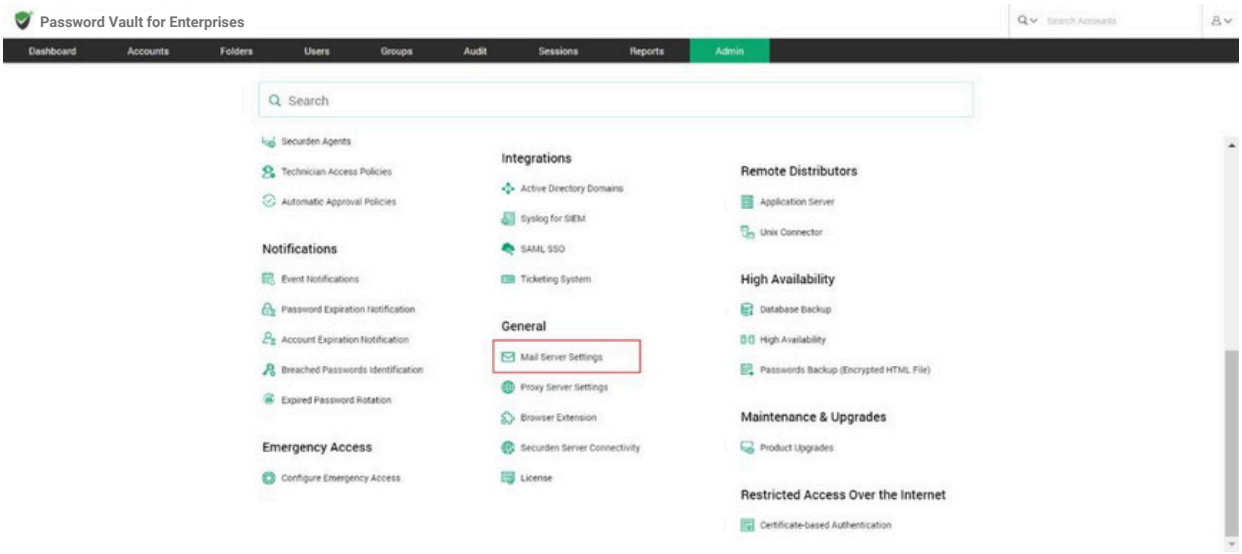
Upon deploying Securden, you need to carry out certain settings before proceeding with configuring the features. These settings are classified under the **Admin >> General** section.

They include – setting up the mail server to enable Securden to send email notifications, proxy server settings (if your organization makes use of a proxy server to regulate internet traffic), and Securden server connectivity settings specifying how to connect to the Securden web interface from the client machines and the name with which the client machines identify the Securden server host. The details of configuring these settings are explained in the sections that follow.

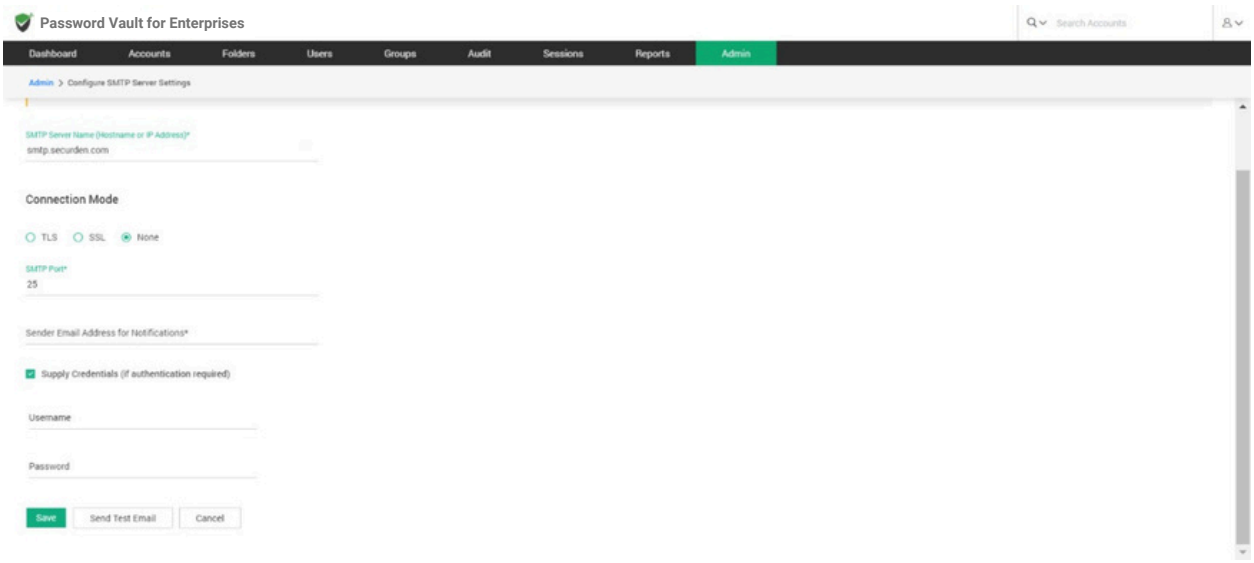
Configure Mail Server Settings

Securden sends various email notifications to users/admins. This includes the email notification that enables new users to set up access to the Vault interface. Other email notifications include activity alerts, reports, and more.

To facilitate these emails, SMTP server details are to be configured. Navigate to **Admin >> General >> Mail Server Settings** in the GUI to perform this step.



In the GUI that opens, you need to enter the SMTP server details.



Enter the following details:

SMTP server name: Enter the hostname or IP address of the machine that runs the SMTP server.

Connection Mode: Select the mode in which the SMTP accepts connections.

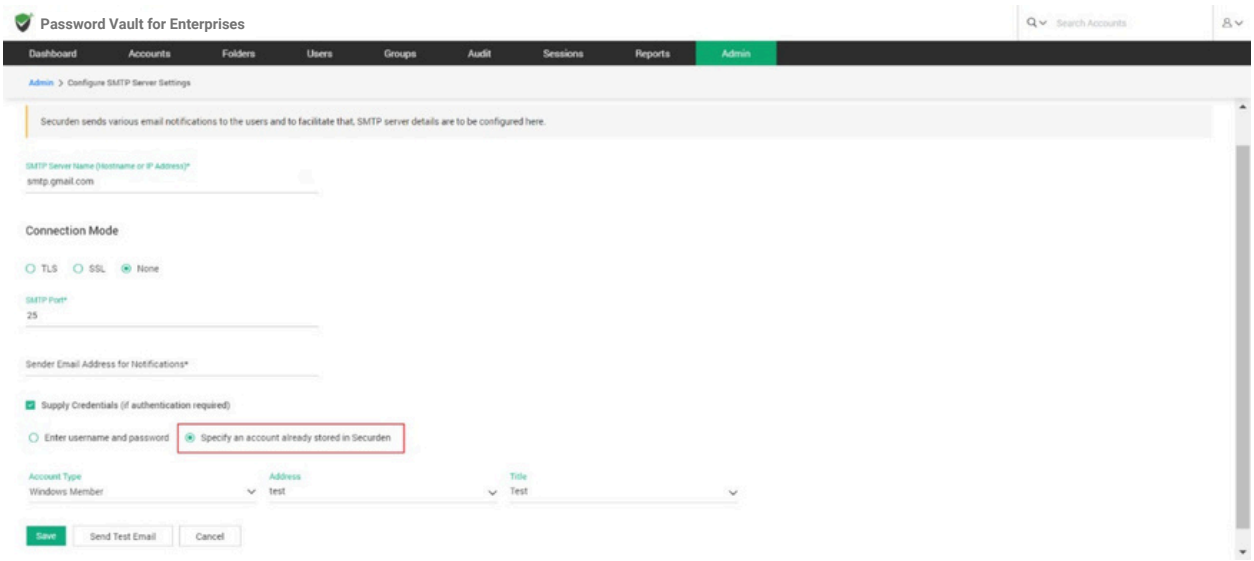
Select TLS or SSL for encrypted connections. The option **None** indicates the default SMTP connection mode (not recommended).

SMTP Port: Specify the port in which the SMTP service listens. The default port for TLS is 587 and SSL is 465.

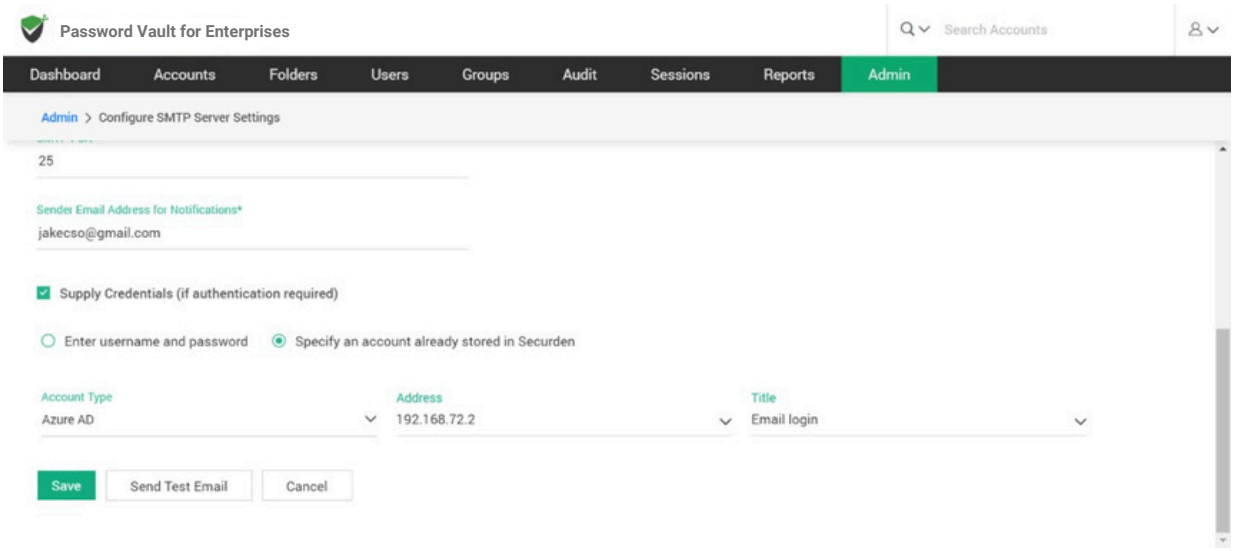
Sender email address for notifications: The email address you enter here will be displayed as the 'sender' when Securden triggers email notifications to users.

Supply Credentials: If your SMTP server requires authentication to access it, you need to supply the credentials.

Note: If you have added accounts in Vault and wish to utilize one of the added accounts to authenticate the SMTP server, you may click on **Specify an account already stored in Securden** and select a corresponding account.



You need to select the **Account Type**, its **Address,** and **Title** in Securden.

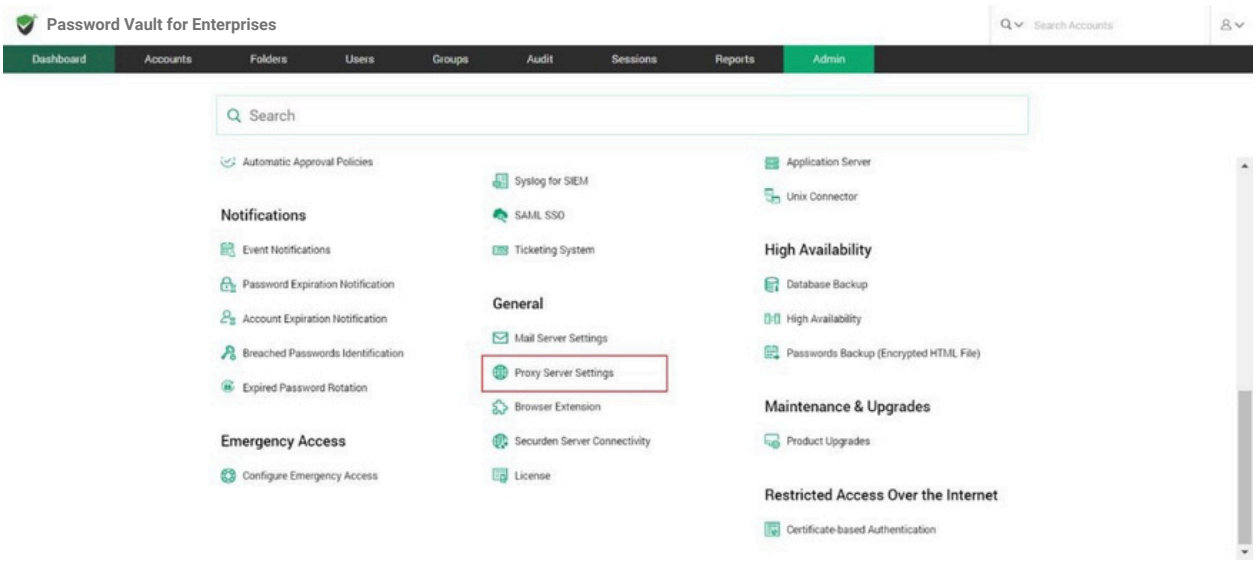


After providing the required details and authentication credentials, click **Save**. You can also test and validate the configuration setting by sending a test email.

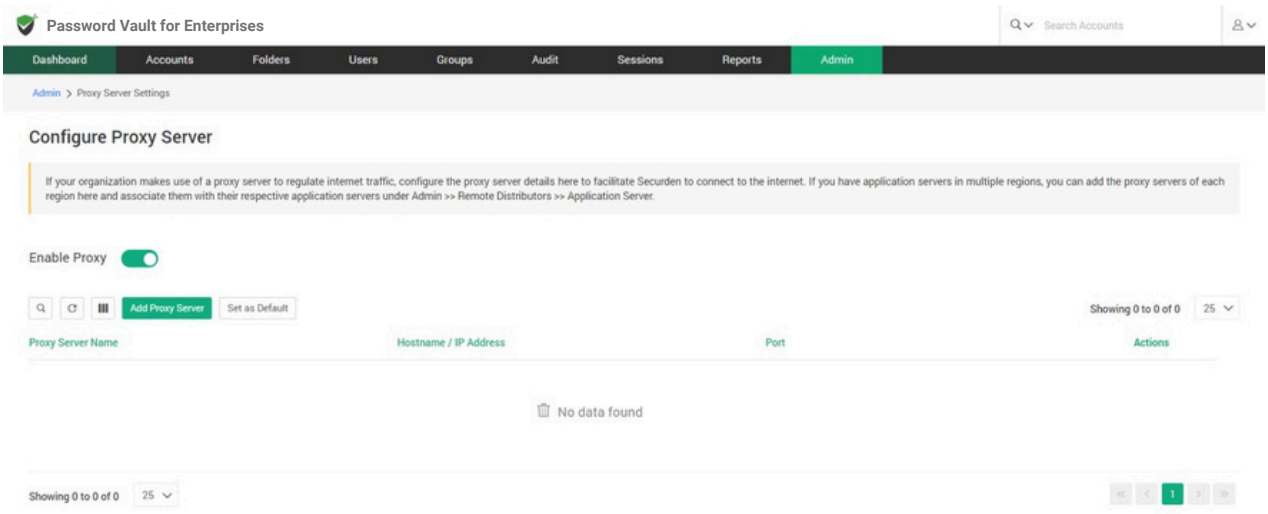
Proxy Server Settings

If your organization makes use of a proxy server to regulate internet traffic, configure the proxy server details to facilitate Securden to connect to the internet.

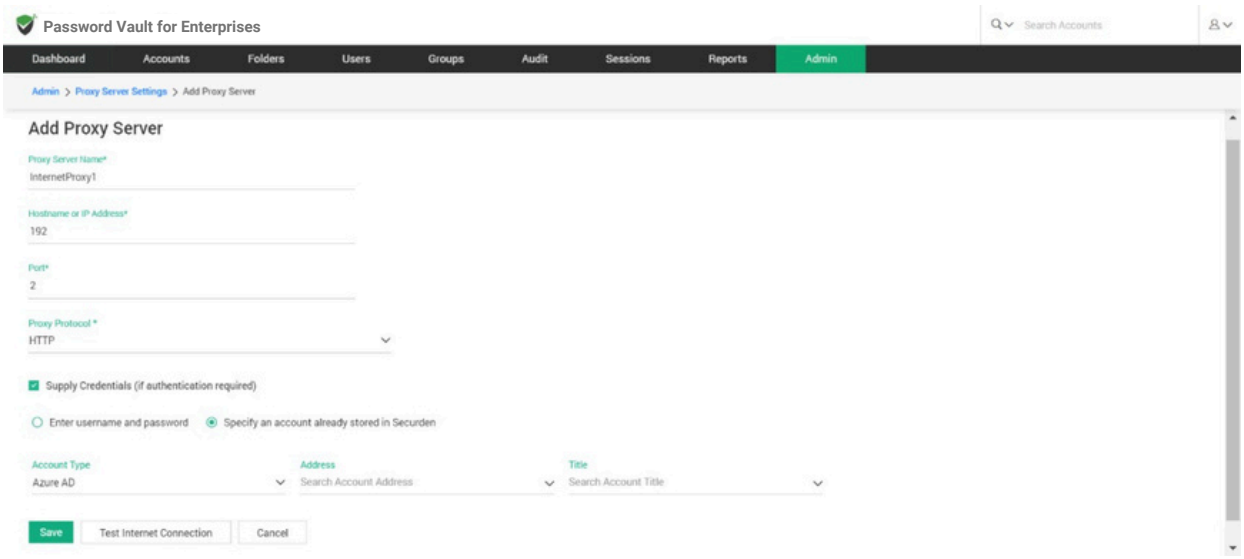
To configure proxy server details, navigate to **Admin >> General >> Proxy Server Settings.**



In the GUI that opens, toggle the **Enable Proxy** button and then click on **Add Proxy Server**



In the text fields below, enter the hostname or IP address of the machine that hosts the proxy server. Also enter the port used by the proxy server to allow client connections.



Note: If the proxy server requires authentication, you need to enter the credentials to enable Securden to connect to the proxy server. Click the checkbox **Supply Credentials**. You can either select an account added in Securden, or enter username and password to authenticate.

If you want to choose an account stored in Securden, you can do so by searching for the **Account type**, **Address,** and **Title** in Securden. **Save** the settings and then run a test to verify the internet connection.

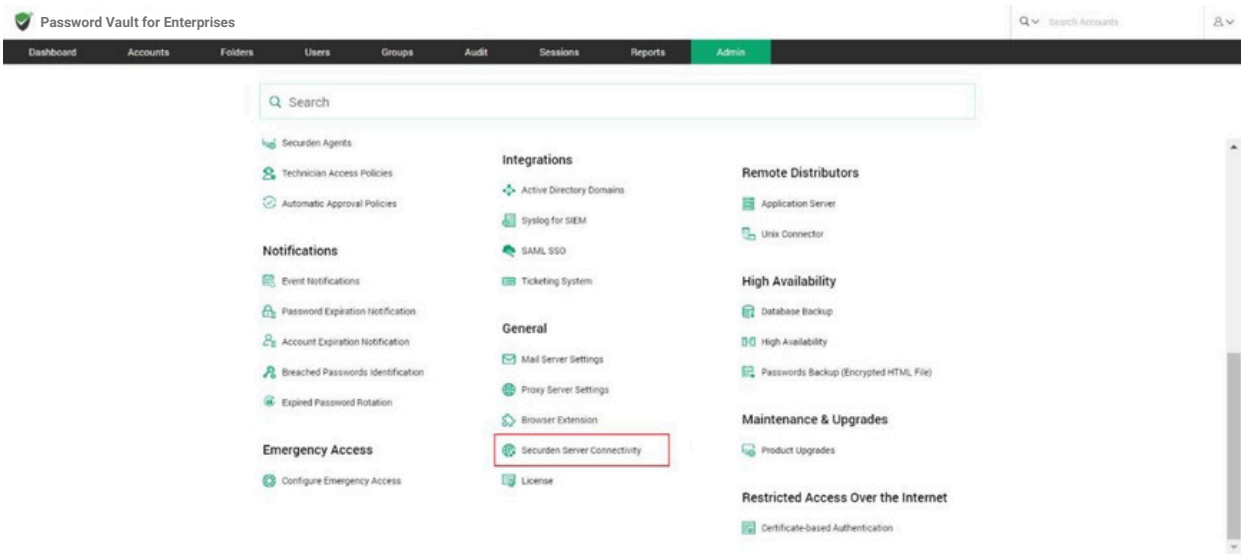
Securden Server Connectivity

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.

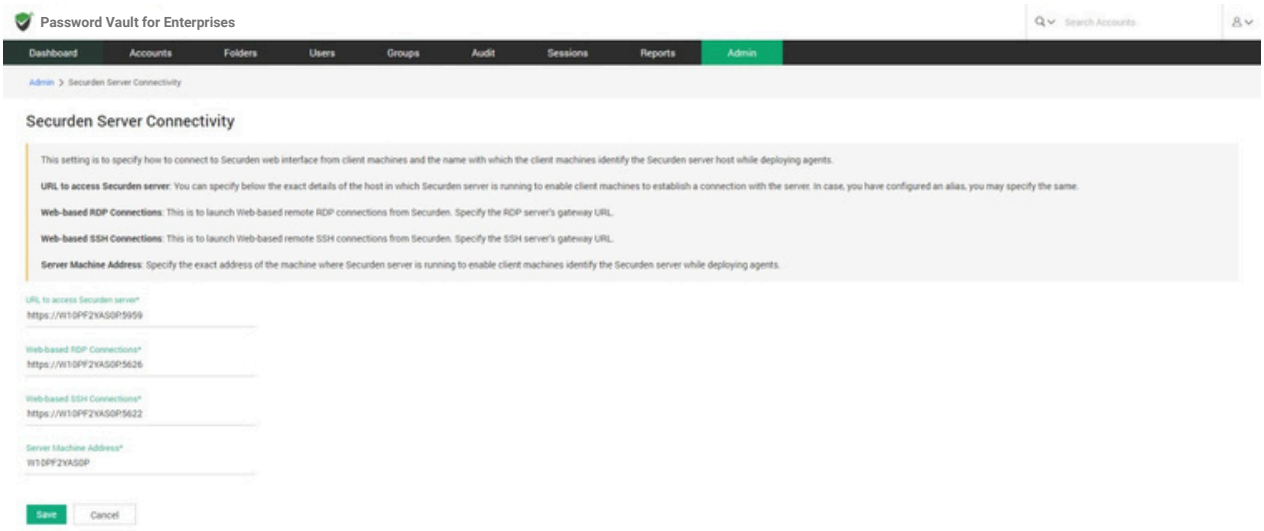
In addition to specifying how the Securden server can be accessed, you can specify the gateway URLs for RDP and SSH connections.

15

To configure server connectivity settings, navigate to **Admin >> General >> Securden Server Connectivity**



In the GUI that opens, enter the following details.



URL to access Securden server

This URL refers to the exact details of the host in which the Securden server is running to enable client machines to establish a connection with the server. If you have configured an alias name, you may specify the same. You can also enter the IP address or domain name.

Securden server uses port **5454** by default. If you wish to change the Server port, follow the steps below.

To change server port:

1. Navigate to the Securden installation folder/conf directory and open the ‘server.properties’ file with Wordpad or notepad++

2. Look for the entry "SERVER_PORT" and enter the required port number

3. Restart Securden Vault Service alone (DO NOT restart ‘Web Service – Securden Vault’)

If you do not wish to enter the port number, you can change the port number to default 443 to access Securden.

To change the https port to the default 443, follow the below steps:

- Navigate to the Securden installation folder / conf directory and open the ‘server.properties’ file with Wordpad or notepad++
- Look for the entry "SERVER_PORT" and enter the required port number
- Restart Securden Vault Service alone (DO NOT restart ‘Web Service – Securden Vault’)

After updating the ‘server.properties’ file, you may enter the modified port in the Server Connectivity field.

Troubleshooting tip

If you are not able to connect to Securden Server using the domain name, then you can connect to it using the IP address.

Web-based RDP Connections

Securden helps in launching one-click, web-based RDP connections from the interface. To facilitate that, you can specify the RDP server's gateway URL. By default, Securden uses port 5626 for RDP connections.

If you want, you can change the RDP gateway port by following the steps below and then enter the new port number here.

To change RDP Server Gateway Port:

- Navigate to the Securden installation folder/conf directory and open the ‘server.properties’ file with Wordpad or Notepad++
- Look for the entry "RDP GATEWAY PROXY PORT" and enter the new value
- Restart Securden VaultService alone (DO NOT restart ‘Web Service – Securden Vault)

Web-based SSH Connections

Securden helps in launching one-click, web-based SSH connections from the interface. To facilitate that, you can specify the SSH server's gateway URL. By default, Securden uses port 5622 for SSH connections. If you want, you can change the SSH gateway port by following the steps below and then enter the new port number here.

To change SSH Server Gateway Port Number,

● Navigate to the Securden installation folder/conf directory and open the 'server.properties' file with Wordpad or Notepad++

● Look for the entry "TORNADO PROXY PORT" and enter the new value

● Restart Securden Vault Service alone (DO NOT restart 'Web Service – Securden Vault').

Server Machine Address

Specify the exact address of the machine where the Securden Server is running to enable client machines to identify the Securden Server while deploying agents.

Replace Self-signed Certificate

By default, Securden comes bundled with a self-signed certificate. You can add your own Certificate Authority signed certificate by following the steps below.

Securden requires the certificate and the private key separately. If you have the CA certificate in .pfx format, follow the steps below:

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

You can 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.

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.

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

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 an SSL certificate and a private key.

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

6. In services.msc, restart Securden Vault Service

Troubleshooting tips:

- In some cases, the PEM file does not contain the private key, and this brings up the error - **Expecting: ANY PRIVATE KEY**. Ensure that you have the key along with the certificate.

- Ensure that the .pfx file is in PKCS#12, as this format holds both the certificate and key in it. Hence, we recommend the certificate be exported in PKCS#12 format to extract the certificate and key separately.

Section 3: User Management

User Management

User Management deals with onboarding users in your organization into Securden. It extends to assigning them different roles, enforcing security settings, managing their access and permissions, de-provisioning departing users, and more. Before you proceed with onboarding the users, certain prerequisites are to be carried out.

Onboard Your Users

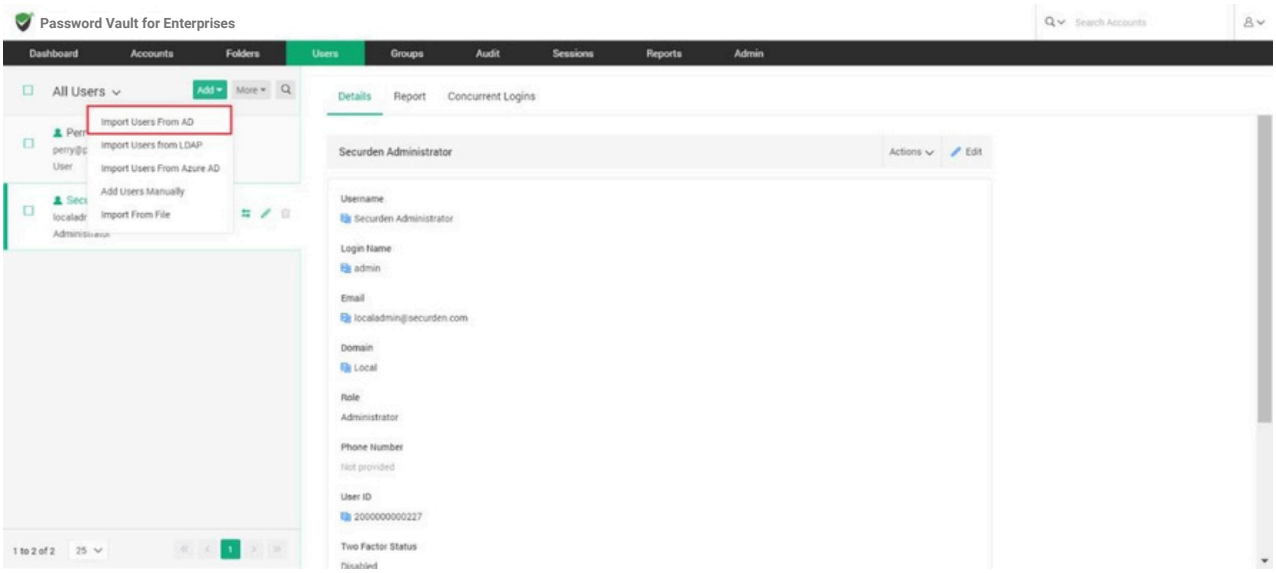
You need to create accounts for your team members to enable them to use Securden. There are multiple options to do this. The options are:

- Importing Users from Active Directory
- Importing Users from Azure AD
- Importing Users from LDAP
- Adding Users Manually
- Importing Users from a File

Import Users from Active Directory

When you integrate with AD, Securden scans your AD domain and obtains the users and groups in the domain. You can discover any specific user(s) or a group of users and add them to Securden.

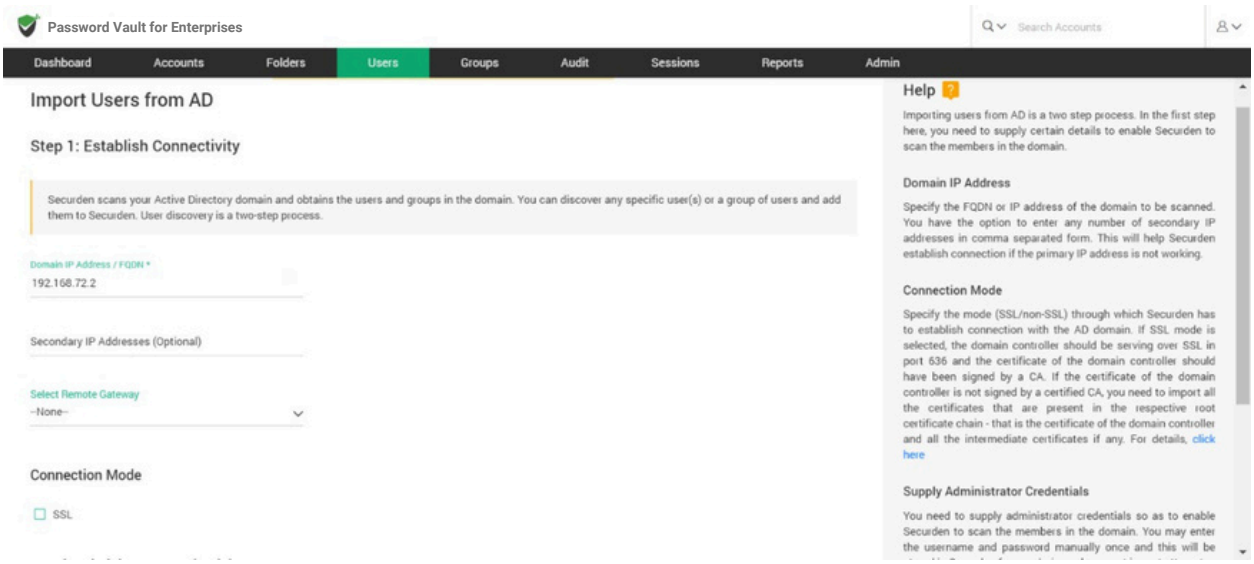
Navigate to **Users >> Add >> Import Users From AD** in the GUI to perform this step.



Importing from AD is a two-step process. In the first step here, you need to supply certain details to enable Securden to scan the members in the domain.

Step 1: Establish Connectivity

This step requires you to provide certain details to enable Securden to scan members of the domain.



***Domain IP Address*:** Specify the FQDN or IP address of the domain controller to be scanned. You have the option to enter any number of secondary IP addresses (secondary domain controllers) in comma separated form. This will help Securden establish a connection if the primary is not accessible.

***Connection Mode*:** Specify the mode (SSL/non-SSL) through which Securden has to establish a connection with the AD domain.

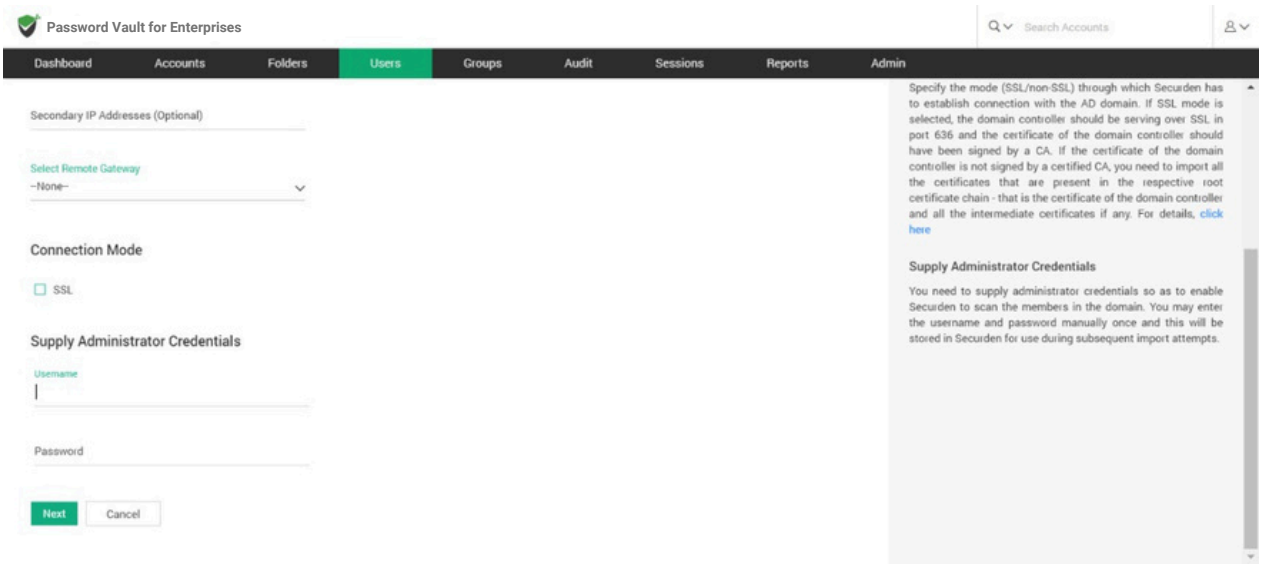
- If SSL mode is selected, the domain controller should be serving over SSL in port 636 and the certificate of the domain controller should have been signed by a CA.
- If the certificate of the domain controller is not signed by a certified CA, you need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the domain controller and all the intermediate certificates if any.

You can follow the example given below to import the domain controller's certificate into the certificate store of the Securden server machine. (However, you may use any procedure that you would normally use to import the SSL certificates to the machine's certificate store).

- In the Securden server machine, launch Microsoft Edge and navigate to **Tools >> Internet Options >> Content >> Certificates.**
- In the GUI that pops up, click **Install Certificate** and then choose **Local Machine** in the next step.
- Browse and locate the root certificate issued by the CA.
- Click **Next** and choose the option **Automatically select the certificate store based on the type of certificate** and install.
- Click **Import** again.
- Browse and locate the domain controller certificate.
- Click **Next** and choose the option **Automatically select the certificate store based on the type of certificate** and install.
- Apply the changes and close the wizard.
- Repeat the procedure to install other certificates in the root chain.

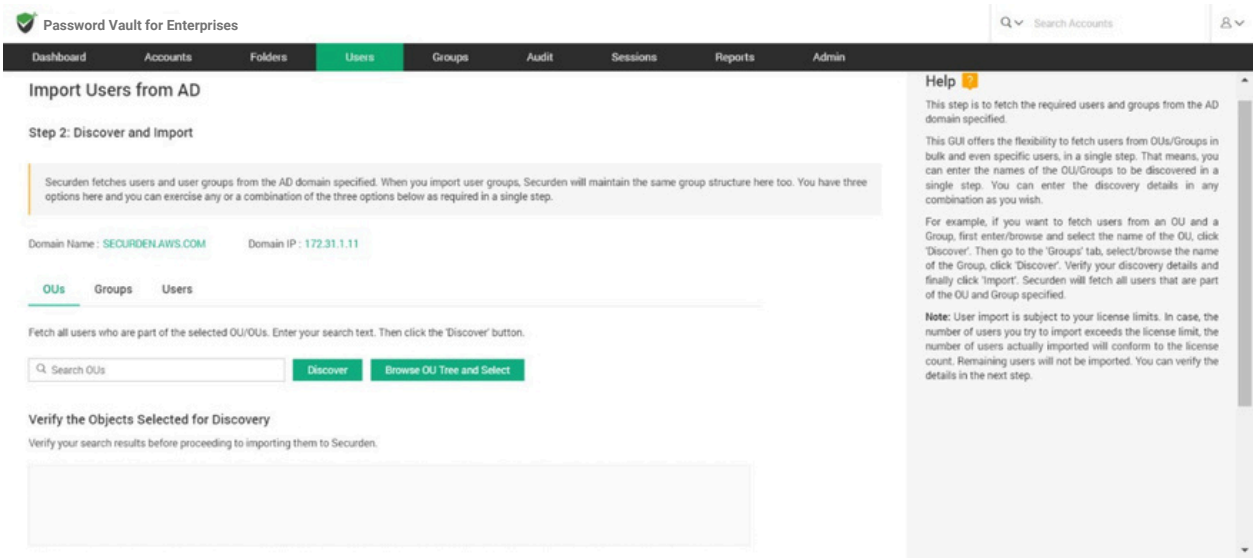
***Supply Administrator Credentials*:**

You need to supply administrator credentials to enable Securden to scan the members in the domain. You may enter the username and password manually once and this will be stored in Securden for use during subsequent import attempts.



Once you've entered the Administrator Credentials, click **Next**. This is the end of step 1.

In the next step, you can discover any specific user(s) or a group of users and add them to Securden.



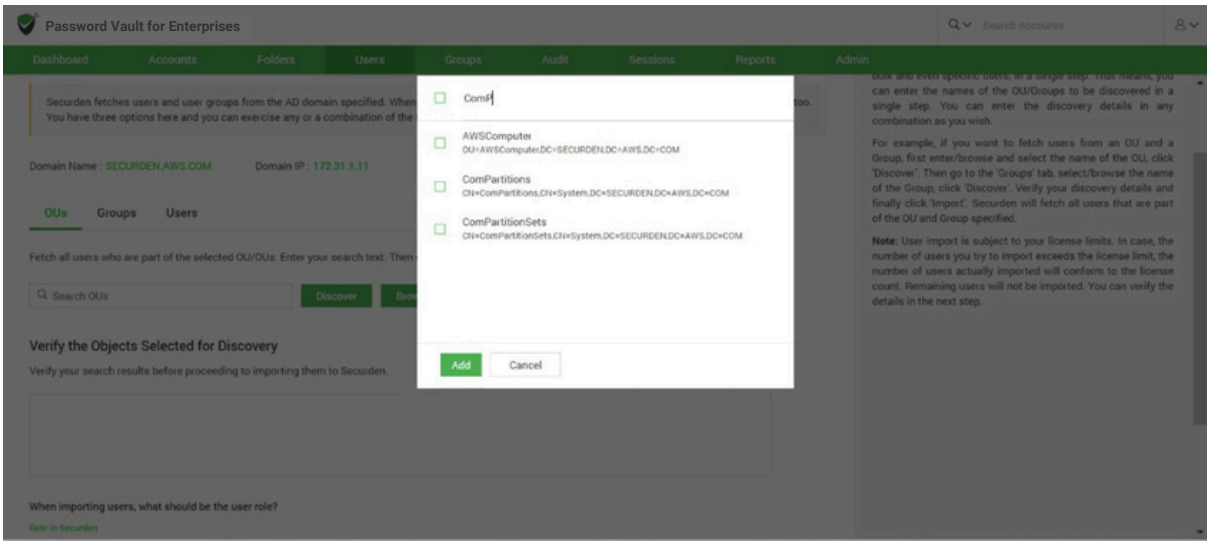
Step 2: Select Users to Import

This step is to fetch the required users and groups from the AD domain specified. When you import user groups from AD, Securden maintains the same group structure here too.

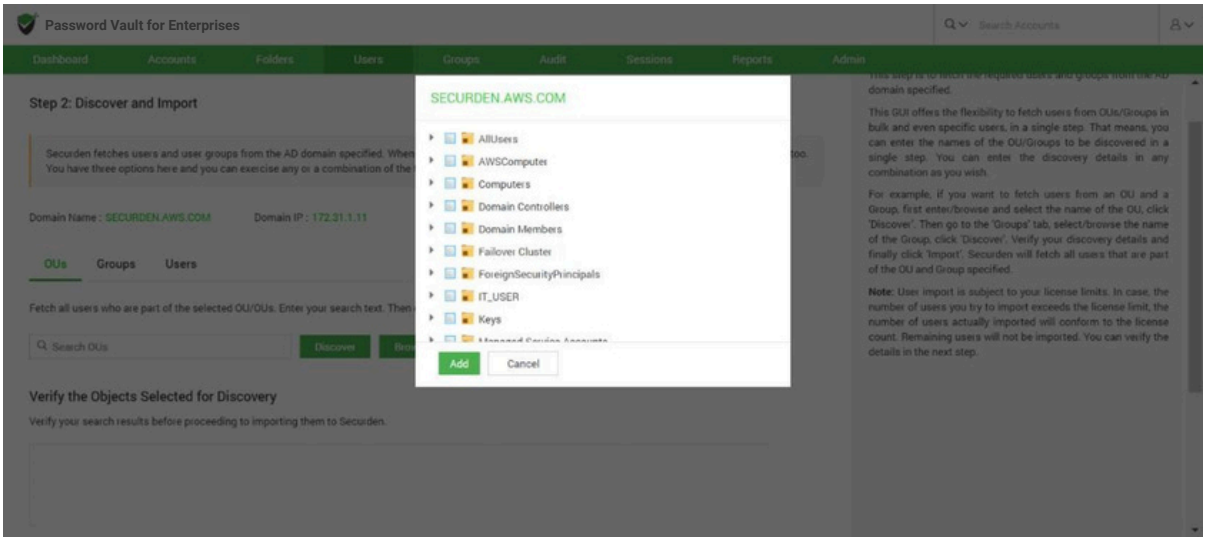
This GUI offers the flexibility to fetch users from OUs/Groups in bulk and even specific users, in a single step. That means you can enter the names of the OU/Groups to be discovered in a single step. You can enter the discovery details in any combinations (OUs, Groups, Users) as you wish.

To import OUs, select the OU tab.

1. Enter the OU name and select **Discover.**



2. You can also browse from the OU tree by clicking on the **Browse OU Tree and Select** option. You can select one or multiple OUs and select **Add.**



3. You can then verify your selection in the **Verify the Objects Selected for Discovery.**
4. You can then select the role for the users in OUs using the **Role in Securden** dropdown.
5. Before selecting the import button, you can look into the additional settings which are explained below.
6. Select **Import.**

To import Groups, select the Groups tab.

1. Enter the Group name and select **Discover.**

2. You can also browse by clicking on the **Browse Groups and Select** option. You can select one or multiple groups and select **Add.**
3. You can then verify your selection in the **Verify the Objects Selected for Discovery.**
4. You can then select the role for the imported users in groups using the **Role in Securden** dropdown.
5. Before selecting the import button, you can look into the additional settings which are explained below.
6. Select **Import.**

To import Users, **select the Users tab.**

1. Enter the user name and select **Discover.**
2. You can then verify your selection in the **Verify the Objects Selected for Discovery.**
3. You can then select the role for the individual users imported using the **Role in Securden** drop down. This is set to the **User** role by default.
4. Before selecting the import button, you can look into the additional settings which are explained below.
5. Select **Import.**

Advanced Settings:

This option allows you to either include domain users of all subgroups to the group being imported or ignore the subgroups and import only the users of the first level group.

Note: User import is subject to your license limits. In case, the number of users you try to import exceeds the license limit, the number of users actually imported will conform to the license count. The remaining users will not be imported. You can verify the details in the next step.

***User Groups to Import*:** You can import all or specific user groups to import, depending on your requirements. You can type in the names in the respective text fields in comma separated form.

***Configure Synchronization*:** Securden also allows Periodic Synchronization with AD. After you import the required users, you can configure periodic synchronization with AD. This helps you import users automatically. Click **Save** to save the domain details.

Troubleshooting tips:

1. Trying to fetch local admin accounts from a PC gets the error - The username/password does not exist (or) the user does not have the remote launch or remote.

This might be due to insufficient account permissions. Try to to re-run the discovery by providing a domain admin credential.

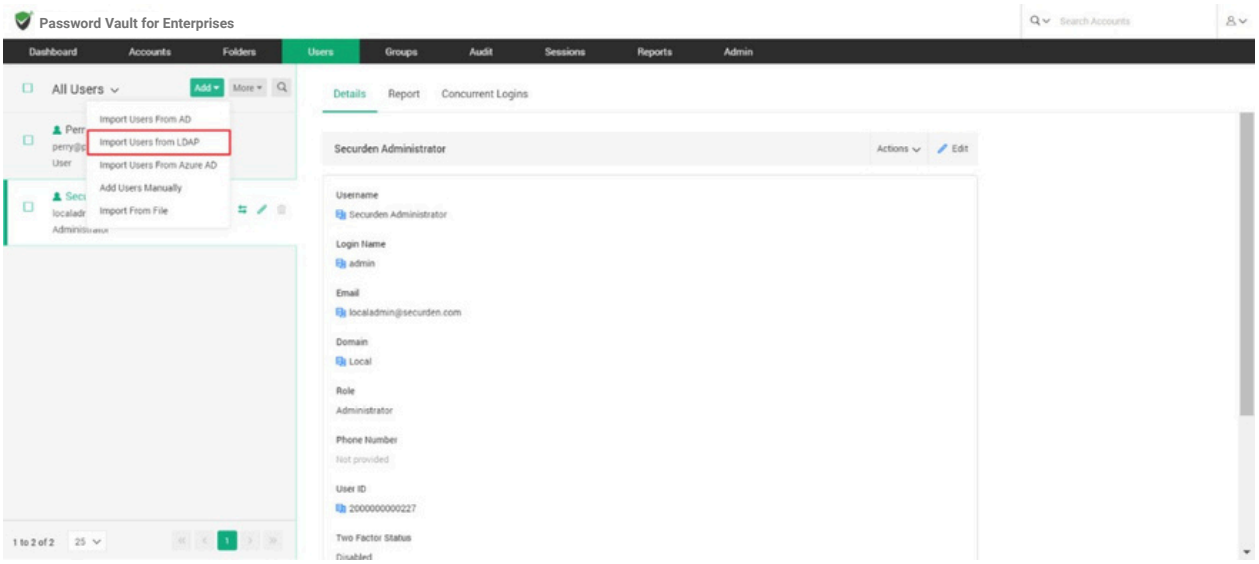
Navigate to **Accounts >> Discover Accounts >> Windows**. Click "Modify" >> Enter username and password

You can enter a **domain admin credential** and try to discover the computers again to fetch local accounts. If it still fails, you can try disabling the firewall and check once again.

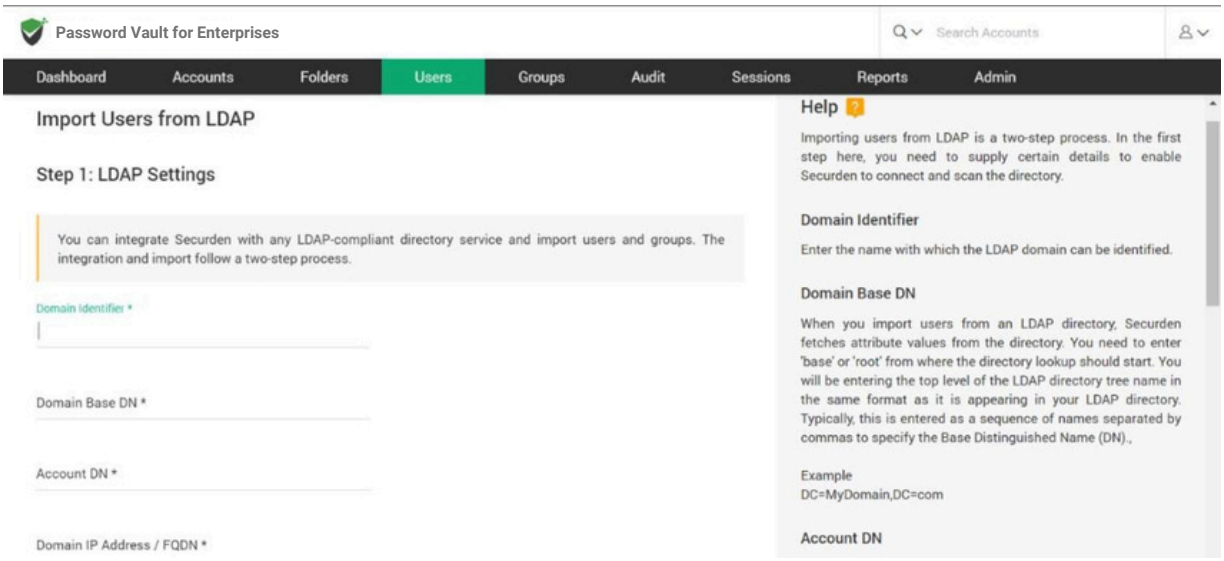
Import Users from LDAP

If your organization makes use of an LDAP to interact with your directory service, you have the option to import your users from the LDAP compliant directory.

Navigate to **Users >> Add >> Import Users from LDAP**.



Importing from LDAP is a two-step process. In the first step here, you need to supply certain details to enable Securden to connect and scan the directory.



Step 1: LDAP Settings

You can integrate Securden with any LDAP-compliant directory service and import users and groups. In the GUI that opens, enter the following credentials to proceed with the integration.

Domain Identifier: Enter the name with which the LDAP domain can be identified.

Domain Base DN: When you import users from an LDAP directory, Securden fetches attribute values from the directory. You need to enter **base** or **root** from where the directory lookup should start. You will be entering the top level of the LDAP directory tree name in the same format as it is appearing in your LDAP directory. Typically, this is entered as a sequence of names separated by commas to specify the Base Distinguished Name (DN).

Example

DC=MyDomain,DC=com

Account DN: For connection authentication, Securden needs access to an LDAP account that has read access and is password-protected. You need to enter the Account DN here. You may enter the account name and password in the last step.

Example

CN=Bob.Smith,CN=Users,DC=MyDomain,DC=com

Domain IP Address: Specify the FQDN or IP address of the LDAP domain to be scanned. You have the option to enter any number of secondary IP addresses in a comma-separated form. This will help Securden establish a connection if the primary IP address is not working.

Connection Mode: Specify the mode (SSL / non-SSL) through which Securden has to establish a connection with the LDAP domain.

- If SSL mode is selected, the domain controller should be serving over SSL in port 636 and the certificate of the domain controller should have been signed by a CA.
- If the certificate of the domain controller is not signed by a certified CA, you need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the domain controller and all the intermediate certificates if any.

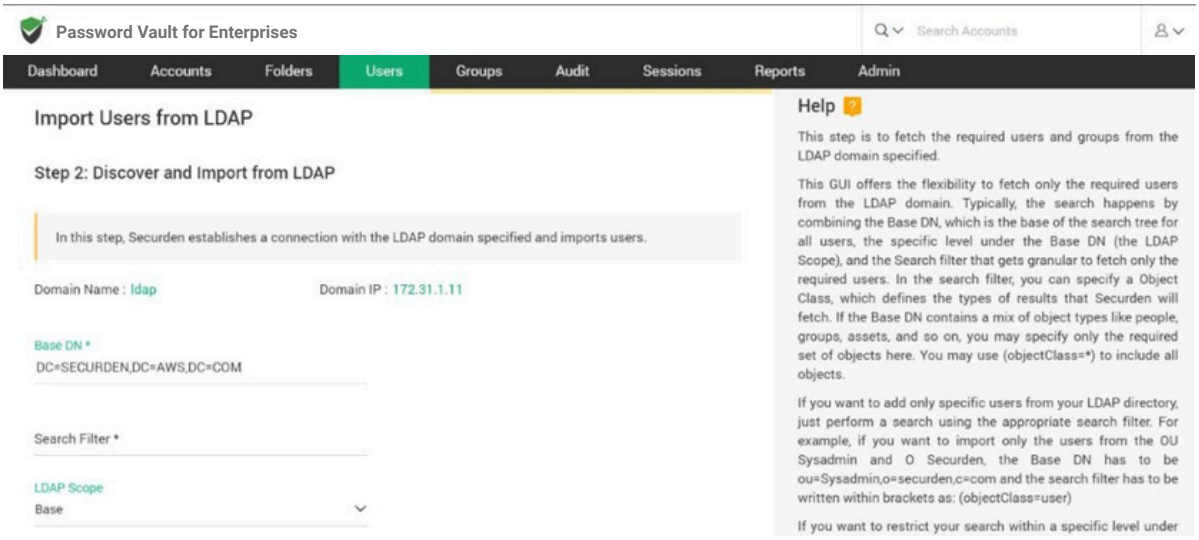
Supply Administrator Credentials:

You need to supply administrator credentials so as to enable Securden to scan the members in the domain. You may enter the username and password manually once and this will be stored in Securden for use during subsequent import attempts. If the users belong to a different network than the Securden server, you can route the connection through a remote gateway. You can select the appropriate remote gateway from the drop-down and the discovery will happen through the selected gateway.

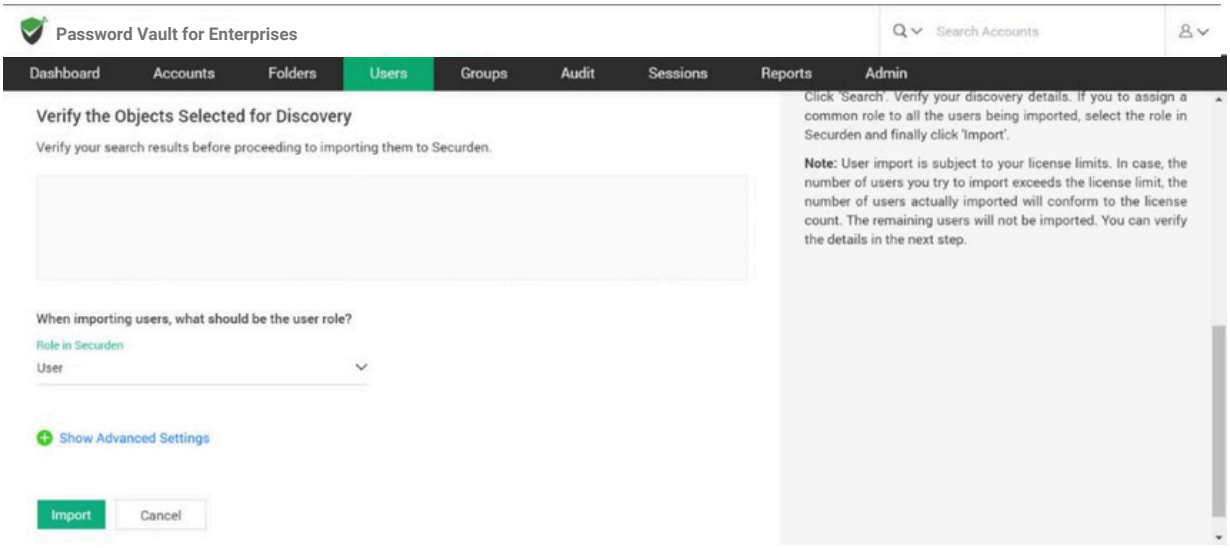
Step 2: Discover and Import from LDAP

In this step, Securden establishes a connection with the LDAP domain specified and imports users.

This GUI offers the flexibility to fetch only the required users from the LDAP domain.



In the GUI, you need to enter the details such as the **Base DN**, **Search filter**, **LDAP Scope, Role in Securden,** and certain advanced settings.



- **Base DN** - Typically, the search happens by combining the **Base DN**, which is the base of the search tree for all users, the specific level under the Base DN (the **LDAP Scope**), and the **Search Filter** that gets granular to fetch only the required users.

- **Search filter -** In the search filter, you can specify an Object Class, which defines the types of results that Securden will fetch. If the Base DN contains a mix of object types like people, groups, assets, and so on, you may specify only the required set of objects here. You may use (objectClass=*) to include all objects.

- If you want to add only specific users from your LDAP directory, just perform a search using the appropriate search filter. For example, if you want to import only the users from the OU Sysadmin and O Securden, the Base DN has to be ou=Sysadmin,o=securden,c=com, and the search filter has to be written within brackets as: (objectClass=user)

- If you want to restrict your search to a specific level under the BaseDN, you may select the required scope from the drop-down.

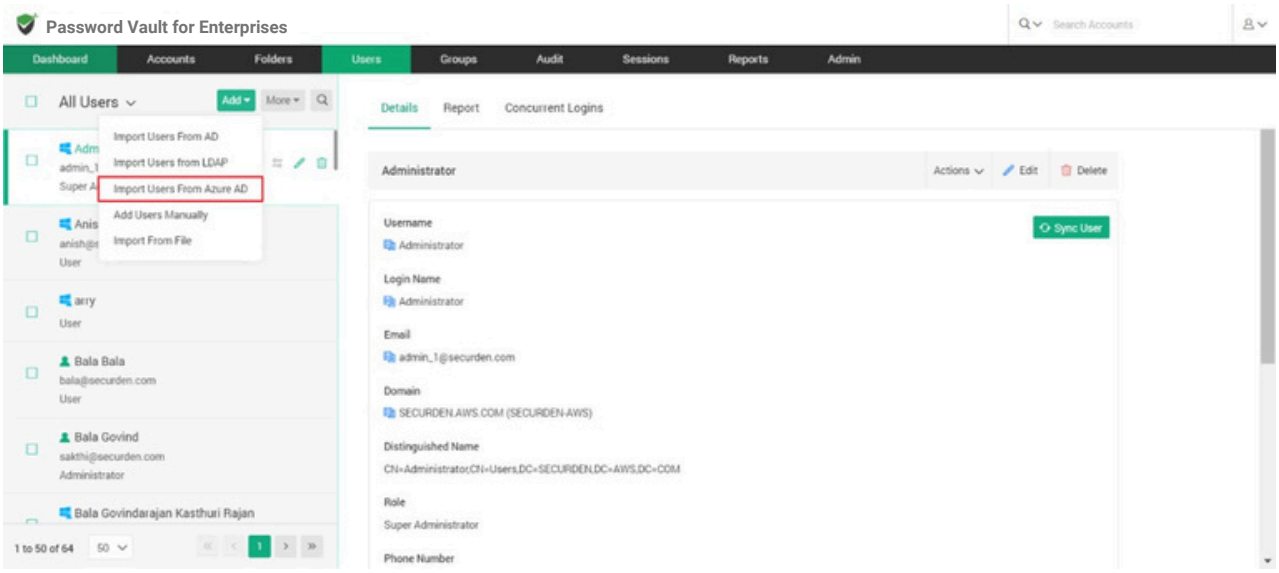
• Click **Search**. Verify your discovery details under **Verify the Objects Selected for Discovery**. If you want to assign a common role to all the users being imported, select the role in Securden and finally click **Import.**

Advanced Settings:

This option allows you to either include domain users of all subgroups to the group being imported or ignore the subgroups and import only the users of the first level group.

Import from Azure AD

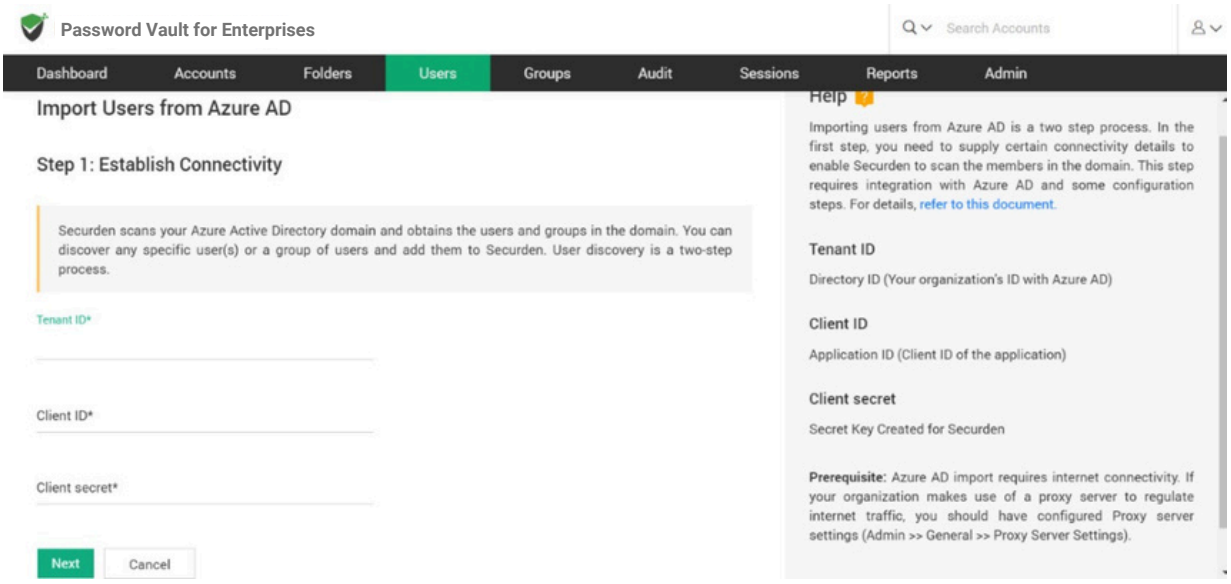
Securden allows you to import users from Azure AD. Navigate to **Users >> Add >> Import Users from Azure AD**.



This is a two-step process. In the first step, you need to supply certain connectivity details to enable Securden to scan the members in the domain. This step requires integration with Azure AD and some configuration steps. For details, refer to ***Securden-Azure-AD-Guide.pdf***

Prerequisites: Azure AD import requires internet connectivity. If your organization makes use of a proxy server to regulate internet traffic, you should have configured proxy server settings. (Admin >> General >> Proxy Server Settings).

Step 1 : Establish Connectivity



In the GUI page that appears, enter the following details:

Tenant ID: Enter the Directory ID i.e., Your organization's ID with Azure AD.

Client ID: Enter the Client ID of the application.

Client Secret: This is the Secret Key created for Securden.

Step 2: Import Users

This step is to fetch the required users and groups from the AD domain specified.
This GUI offers the flexibility to fetch users from OUs/Groups in bulk and even specific users, in a single step. That means you can enter the names of the OU/Groups to be discovered in a single step. You can enter the discovery details in any combination (OUs, Groups, Users) as you wish.

To import OUs, select the OU tab.

1. Enter the OU name and select **Discover.**
2. You can also browse from the OU tree by clicking on the **Browse OU Tree and Select** option. You can select one or multiple OUs and select **Add.**
3. You can then verify your selection in the **Verify the Objects Selected for Discovery.**
4. You can then select the role for the users in OUs using the **Role in Securden** dropdown.
5. Before selecting the import button, you can look into the additional settings which are explained below.
6. Select **Import.**

To import Groups, select the Groups tab.

1. Enter the Group name and select **Discover.**

2. You can also browse by clicking on the **Browse Groups and Select** option. You can select one or multiple groups and select **Add.**
3. You can then verify your selection in the **Verify the Objects Selected for Discovery.**
4. You can then select the role for the imported users in groups using the **Role in Securden** dropdown.
5. Before selecting the import button, you can look into the additional settings which are explained below.
6. Select **Import.**

To import Users, **select the Users tab.**

1. Enter the user name and select **Discover.**
2. You can then verify your selection in the **Verify the Objects Selected for Discovery.**
3. You can then select the role for the individual users imported using the **Role in Securden** drop down.
4. Before selecting the import button, you can look into the additional settings which are explained below.
5. Select **Import.**

Advanced Settings:

This option allows you to either include domain users of all subgroups to the group being imported or ignore the subgroups and import only the users of the first level group.

Note: User import is subject to your license limits. In case, the number of users you try to import exceeds the license limit, the number of users

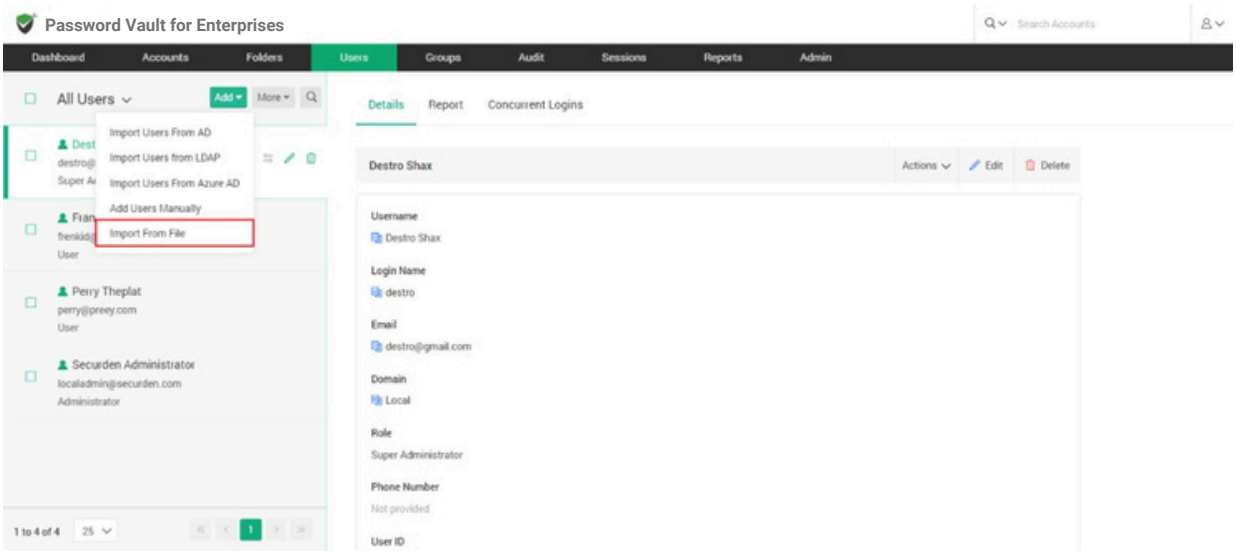
actually imported will conform to the license count. The remaining users will not be imported. You can verify the details in the next step.

***User Groups to Import*:** You can import all or specific user groups to import, depending on your requirements. You can type in the names in the respective text fields in comma separated form.

***Configure Synchronization*:** Securden also allows Periodic Synchronization with AD. After you import the required users, you can configure periodic synchronization with AD. This helps you import users automatically. Click **Save** to save the domain details.

Import Users from File

If you have the details of your users stored in an excel sheet or in another password manager, you can import them into Securden by Navigating to **Users >> Add >> Import From File**.



File Format

Importing users is very flexible in Securden. You can simply import your CSV/XLSX file stored on your computer or the exported file from another password manager.

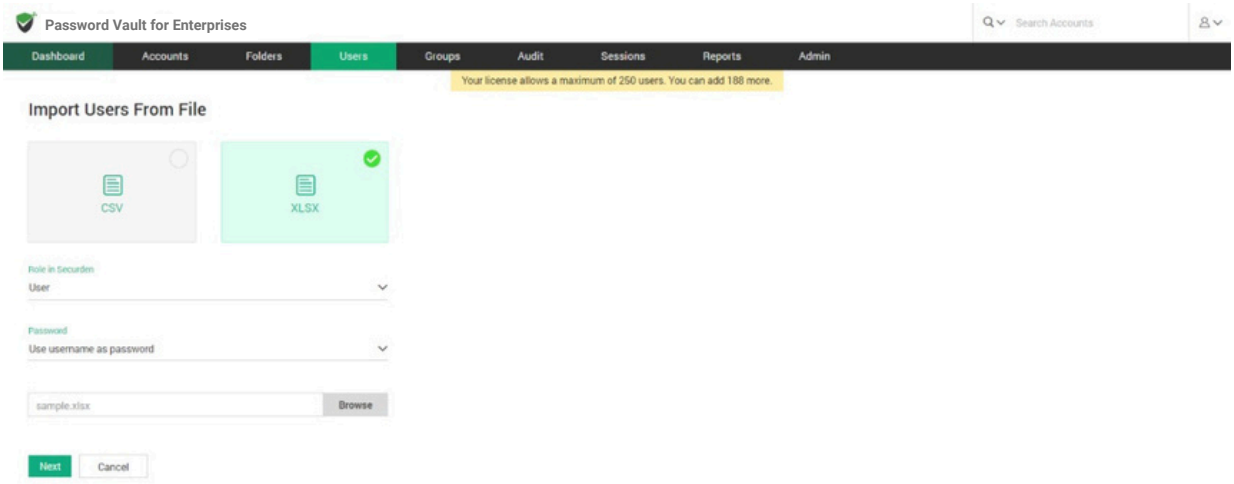
The details of the users such as usernames and passwords that you have entered in the file gets captured, and these are listed as separate parameters. In the second step of user import, you can map the listed columns in the input file to that of Securden.

Steps to import CSV file:

1. Navigate to **Users >> Add** and click on the **CSV** option.
2. Select the **Delimiter**. This can either be Comma/Tab/Colon/Semi-Colon separated.
3. You can then select the role of the user in **Role in Securden.**
4. You then have the option to choose between **Email Password Creation** and **Use username as password** under **Password.**

5. Browse and select the file.
6. Click **Next**. In the second step of the import, we provide the option to map the columns in the input file and that of attributes in Securden.

Steps to import XLSX file:



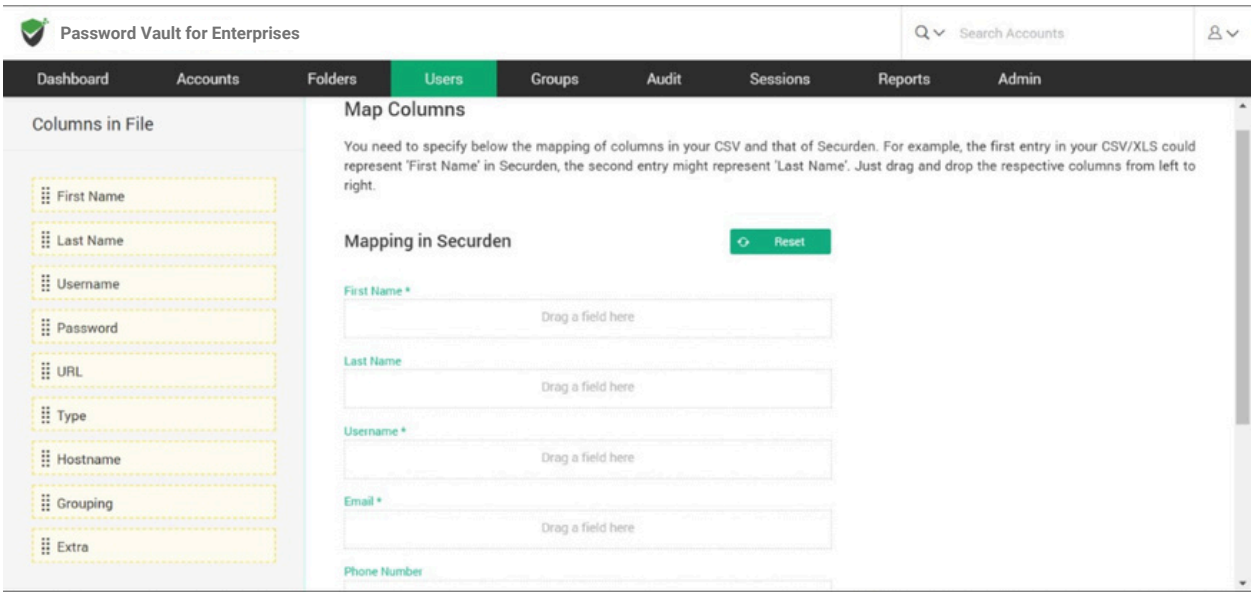
1. Navigate to **Users >> Add** and click on the **XLSX** option.
2. You can then select the role of the user in **Role in Securden.**
3. You then have the option to choose between **Email Password Creation** and **Use username as password** under **Password.**
4. Browse and select the file.
5. Click **Next**. In the second step of the import, we provide the option to map the columns in the input file and that of attributes in Securden.

Mapping

In the second step of import (refer to the screenshot below), you can drag and map the columns (from the panel on the left) to the respective attribute in Securden (on the right.)

For example, the first entry in your CSV/XLS could represent 'First Name' in Securden, the second entry might represent 'Last Name'.

Similarly, you can map Username --> Username, Password --> Password, URL --> URL, Hostname --> Hostname (created as additional field), Extra --> Extra (created as additional field), Grouping ---> Folders, and more.



Include first row

The first row on the excel sheet is excluded by default. You can opt to include this by clicking the checkbox.

Add Additional Fields

To include the additional fields present in your file, you can edit the attributes of an existing user role and add these additional fields or create a custom user role to map the additional attributes present.

To create a custom user role, navigate to **Admin >> Customization >> Custom User Roles.** (Refer *Custom User Roles* section for more details.)

User import configurations

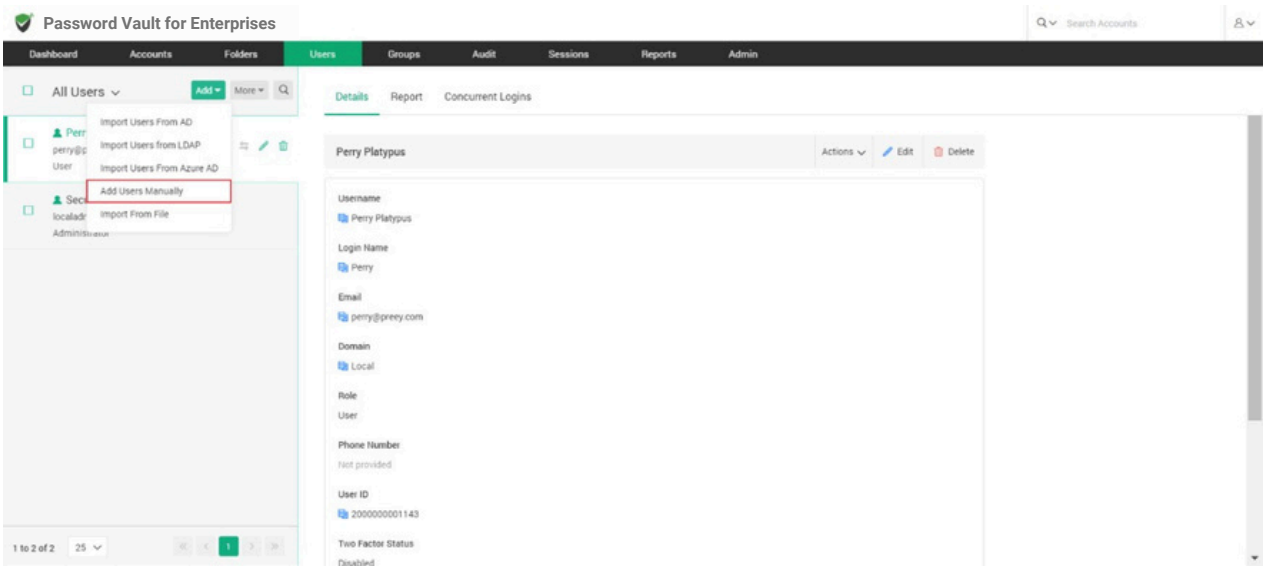
You have the option to modify the default role that is set while importing users from AD or from a file.

To do so, navigate to **Admin >> Customization>> Configurations** and find the configuration as follows - **When importing users from AD or file, what should be the default role?**

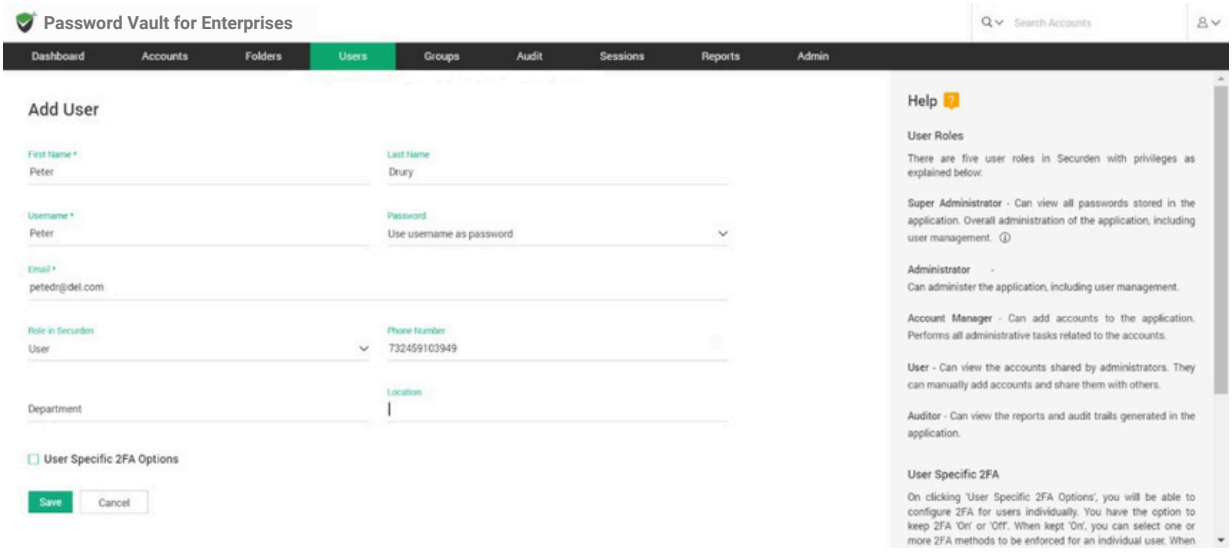
Add Users Manually

You can also onboard your users by making use of native authentication, i.e., adding users manually to access the application (typing creating a username and password for your users to access the Vault Interface).

Navigate to **Users >> Add >> Add Users Manually** in the GUI to perform this step.



In the GUI that opens, enter the user details as explained below:



You'll have to provide the following information to add a user manually in Securden:

- ***First Name*** - Enter the user's first name in the respective field.

- **Last Name** - Enter the user's last name. This field is not mandatory.
- **Username** - Enter a unique username with which the user can log in to Securden.
- For the **password**, you may choose from two options:
- **Email Password Creation Link** – If you have selected this option and provided the email address of the user, they will recieve an email allowing them to login to Securden Password Vault.
- **Use Username as Password -** The password will be the same as the username provided.
- **Email** - Enter the user's email address. Login credentials for Securden will be emailed to this address once the user account is created.
- **Role in Securden** – You can set the access level of each user by assigning them a specified user role. You can select from the five predefined user roles, Super Administrator, Administrator, Auditor, Account Manager, and User. You also have provision to create any number of custom user roles. The access level of default user roles are explained under the section **Default User Roles**. The **Custom User Roles** section explains in detail how user roles can be customized.
- **Phone number, Department, and Location** - These three fields are not mandatory, but you can add them to ensure precise user information for efficient management.
- **Enforce Two Factor Authentication** – You can choose to enable or disable two factor authentication for the added user. Once you've filled all the fields, click Save to add the user.

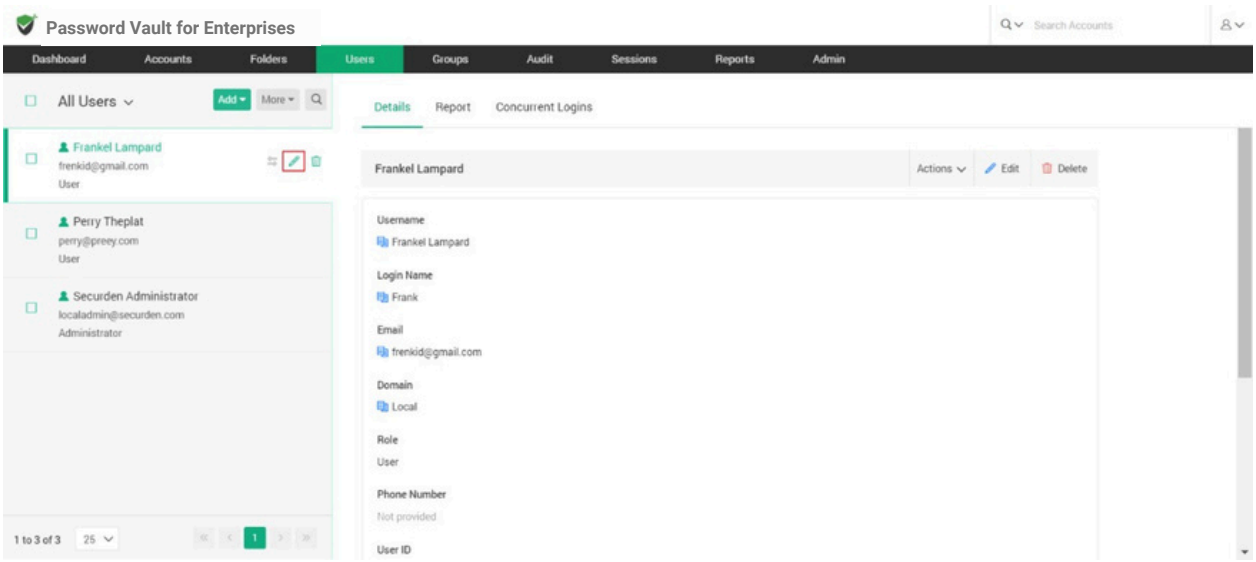
Once you've filled all the fields, click **Save** to add the user.

Note: Once users login into Password Vault for the first time, they need to set a new password. This must be in compliance with the password policy enforced

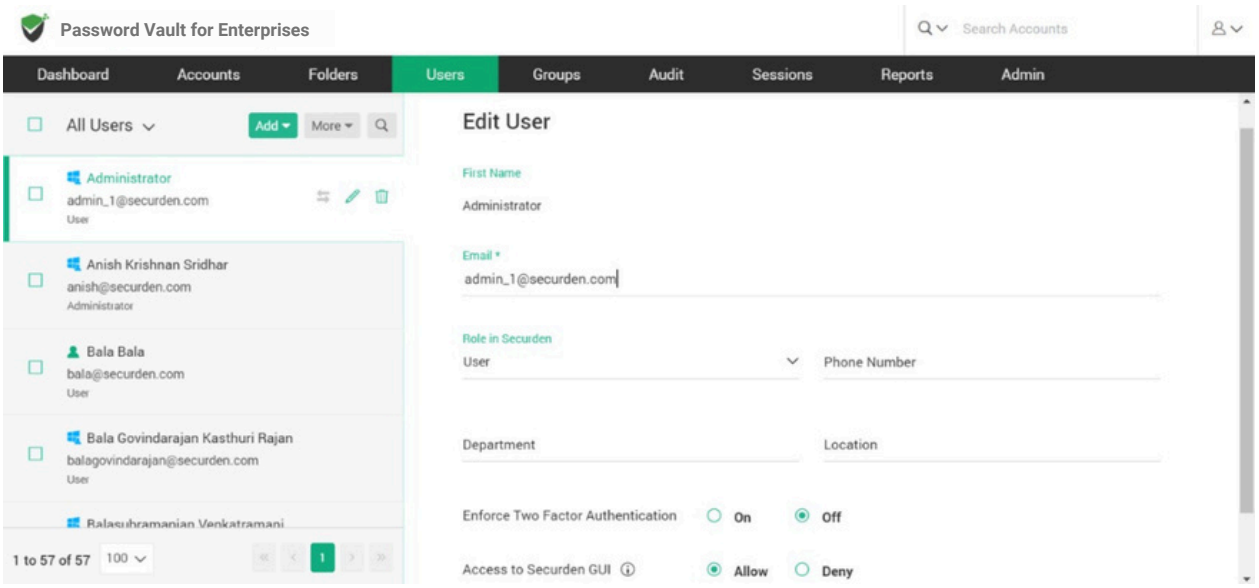
by the administrator, and can be configured under **Admin >> Account Management >> Password Policy**.

Editing Users added in Securden

After adding/importing the users into Securden's database, you can still make modifications or edit their attributes. You can do this by clicking on the '**Edit**' icon on the User tab, beside each user. (Shown below)



You can modify various details like the user's first name, email, user role, etc.

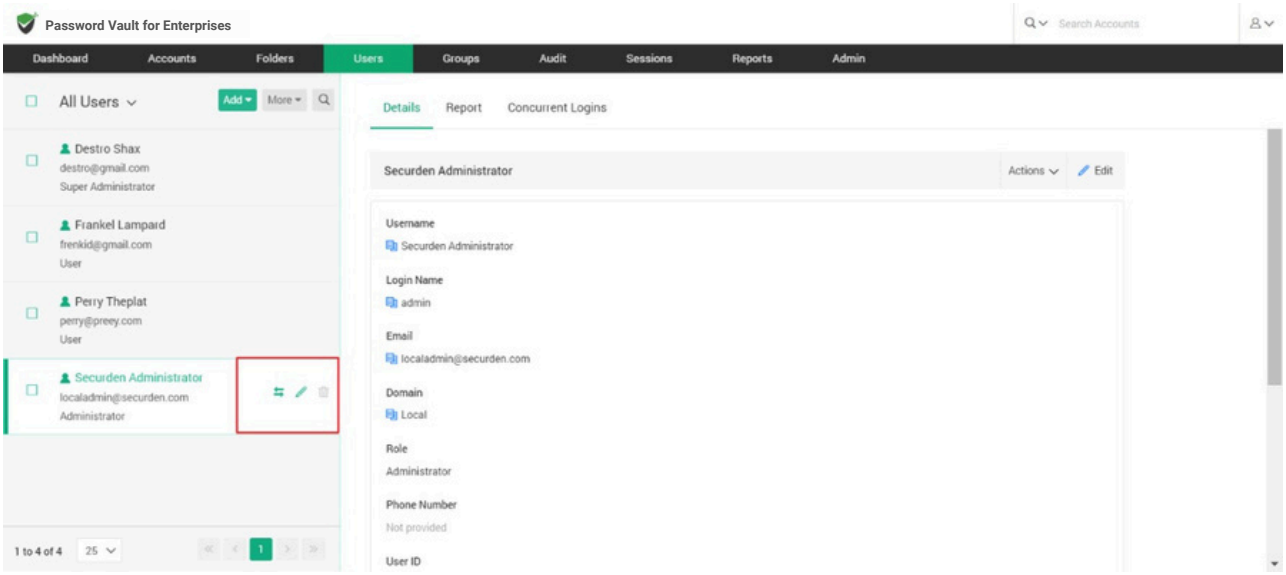


You also have these options:

- **Enforce Two Factor Authentication:** You can turn off 2FA for specific users by turning 2FA off.
- **Access to Securden GUI:** You can allow/deny users from accessing the Securden GUI from here.

Quick Access Options – Users

On the quick access pane on the left side of the Users GUI, if you hover the pointer over a user account, you will see three icons, Transfer Ownership (⇆), Edit (✎), and Delete (🗑).

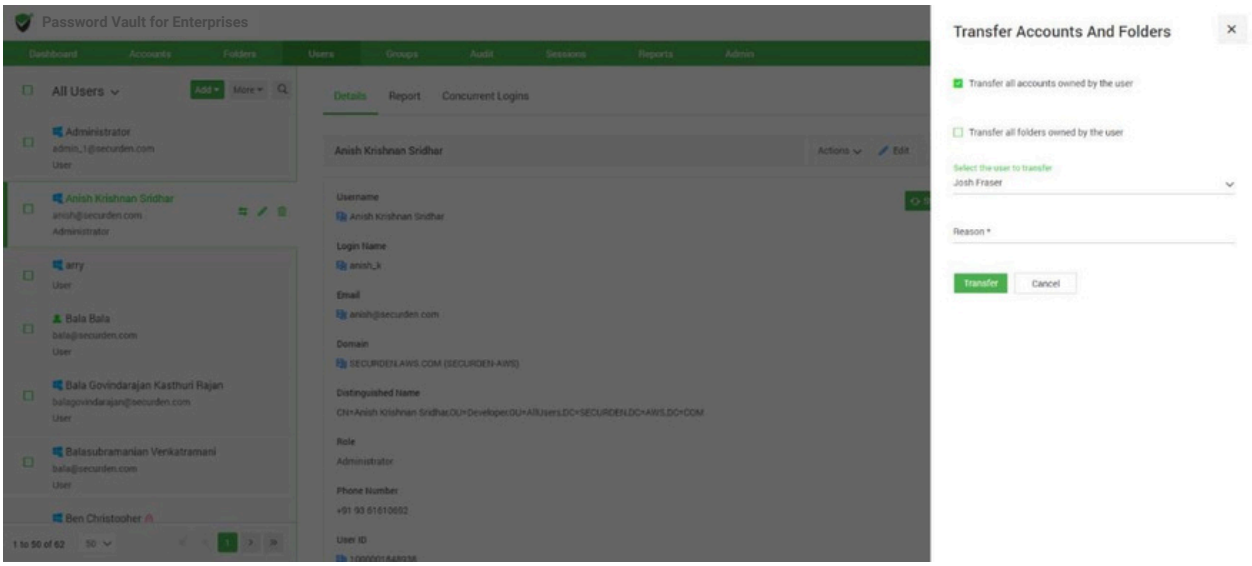


Transfer Ownership

You can transfer the ownership of all the accounts and folders owned by a user to another user. In such an event, the transferer will lose access to the accounts and folders already owned and the transferee will get complete ownership of those accounts and folders.

This feature is particularly helpful when a user leaves the organization. You can simply transfer all the accounts they owned to another.

Once you click the transfer icon, you have the option to transfer all accounts owned by the user, or all folders owned by the user. To transfer the ownership, select the transferee from the list of users, state the reason, and click Transfer.



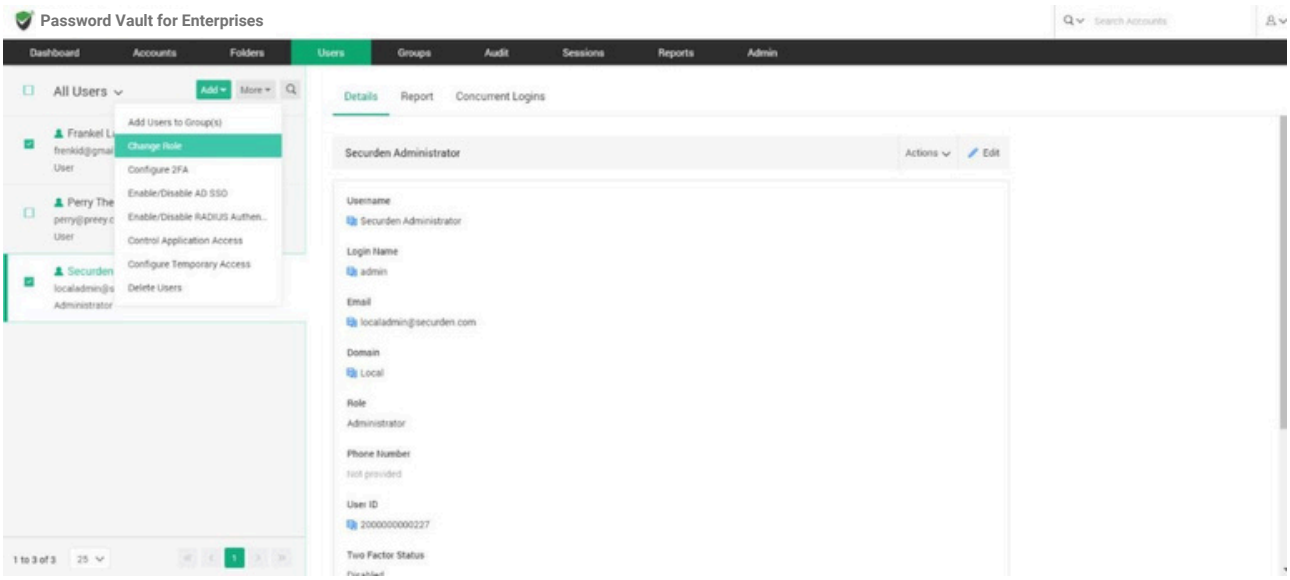
In addition to accessing the Edit, and Delete options in the user dashboard, you can also make use of the icons in quick access pane.

Assigning Roles to Users

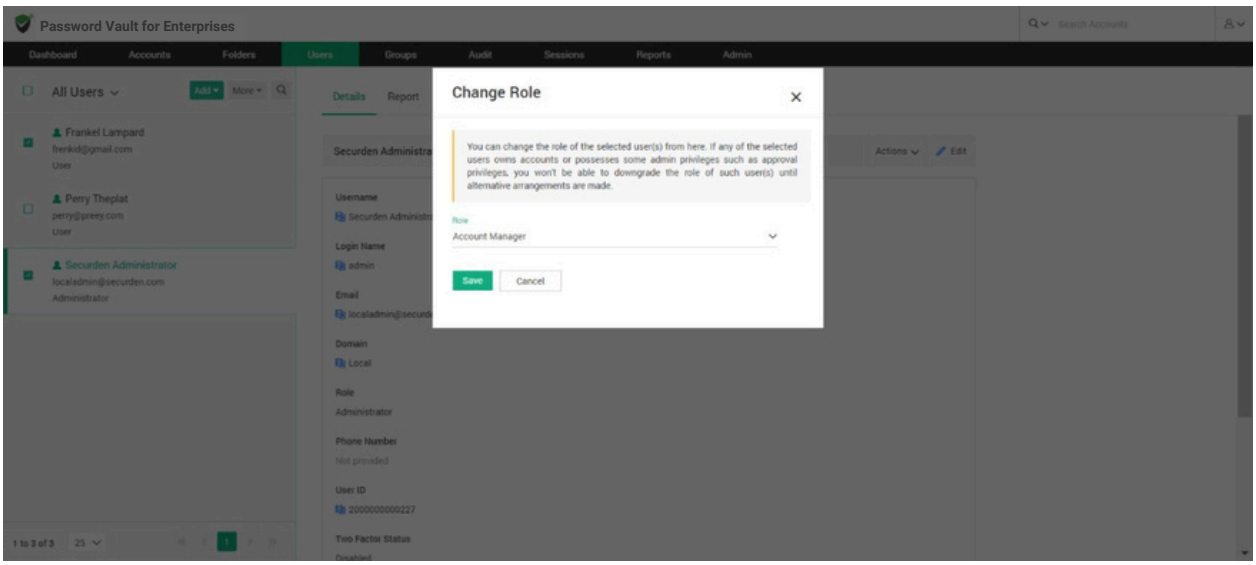
By default, users added or imported will have the role **User** in Securden. This can be changed while importing/adding them, or after you have added them. Each Role has certain privileges associated with them, that let the user carry out certain operations within the Vault. You have the option to create custom user roles outside the default roles available. These settings are further explained under **Default User Roles** and **Custom User Roles.**

To change the role assigned to multiple users,

Navigate to the **Users** section in the GUI, and select the required users.



Once you've selected the users, click **More >> Change Role.**

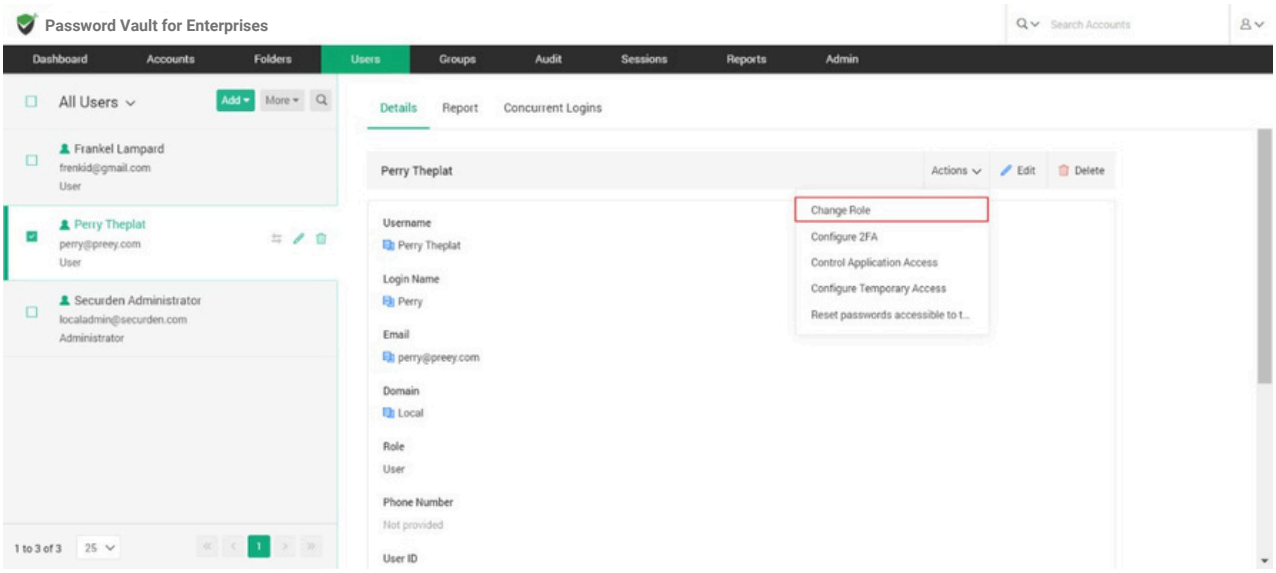


You can select the required role from the dropdown and **Save** changes.

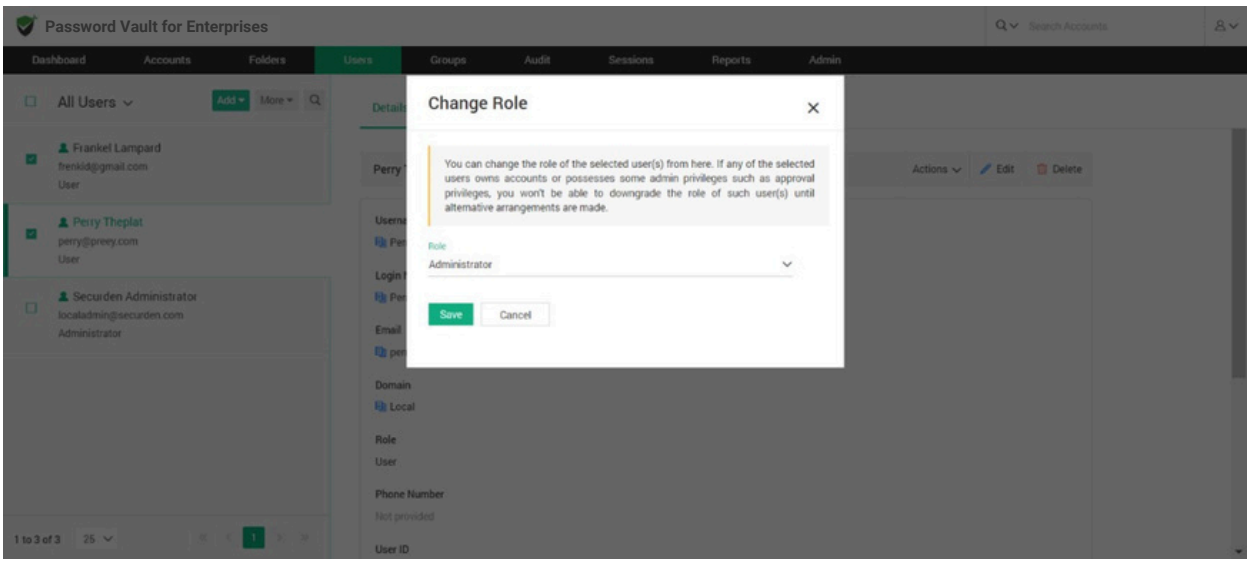
Note: If any of the selected users owns accounts or possesses some admin privileges such as approval privileges, you won't be able to downgrade the role of such user(s) until alternative arrangements are made.

To change the role assigned to an individual user,

Navigate to the **Users** section in the GUI, and select the required user. Select **Change Role** under the **Actions** drop-down.



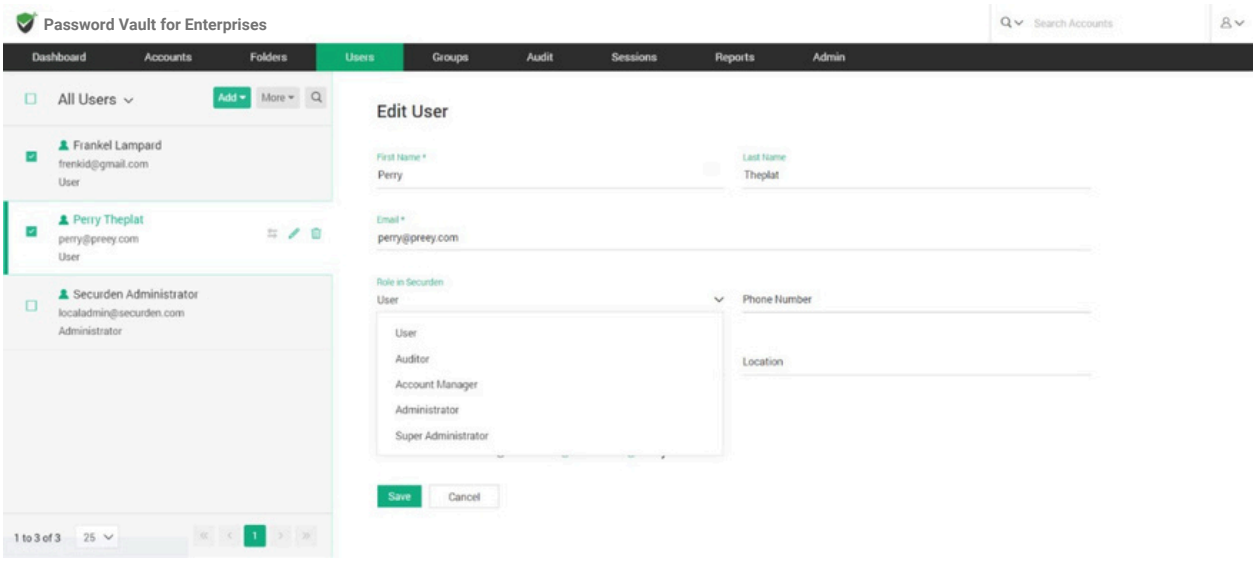
In the popup that opens, you can select the **Role** from the list of available ones in the drop-down.



You may **Save** the changes once you have assigned the role.

Note: If the selected users owns accounts or possesses some admin privileges such as approval privileges, you won't be able to downgrade the role the user until alternative arrangements are made.

Alternatively, you can **Edit** the user attributes to change their role.



Default User Roles

There are five predefined user roles in Securden Password Vault with privileges as explained below:

- **Super Administrator** - This is like an emergency/break-glass account which allows viewing all the work-related passwords stored in the application. They can also view the overall administration of the application, including user management.

- **Administrator** - They can administer the application, including user management. Unlike super administrators, administrators can see only the passwords that are owned by them and the ones that are shared with them.

- **Account Manager** - They can add accounts to the application. They can also perform all administrative tasks related to the accounts.

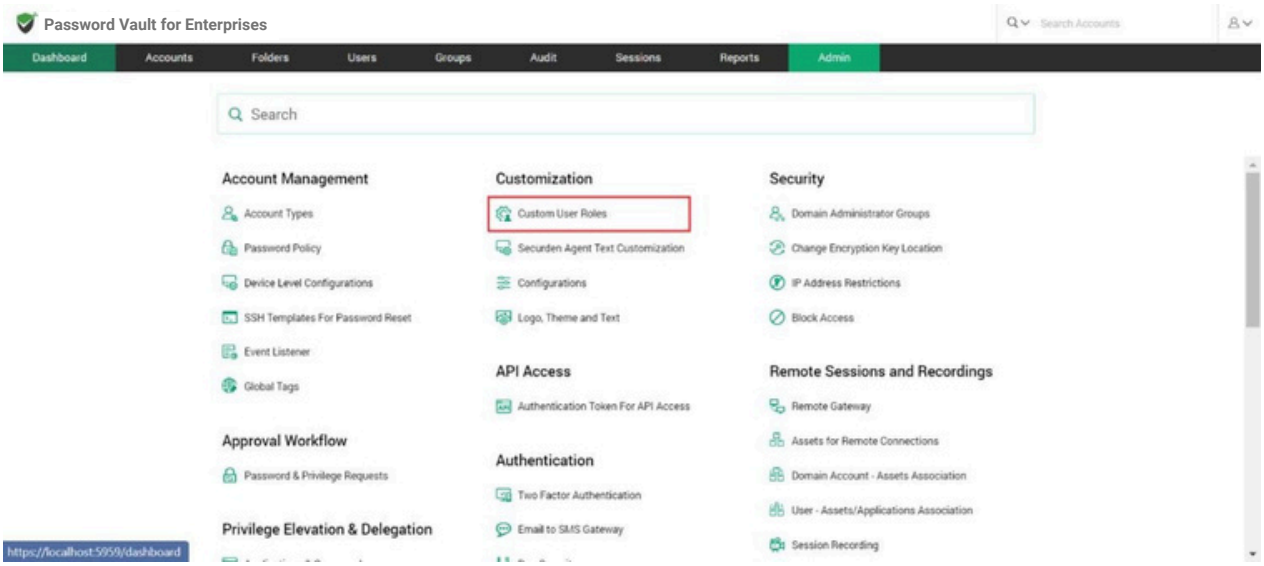
- **User** - They can view the accounts shared by administrators. They can manually add accounts and share them with others. (They do not have the privilege to import accounts). If needed, you can disable account addition privilege for users.

- **Auditor** - They can view the reports and audit trails generated in the application. They can manually add accounts and share them with others.

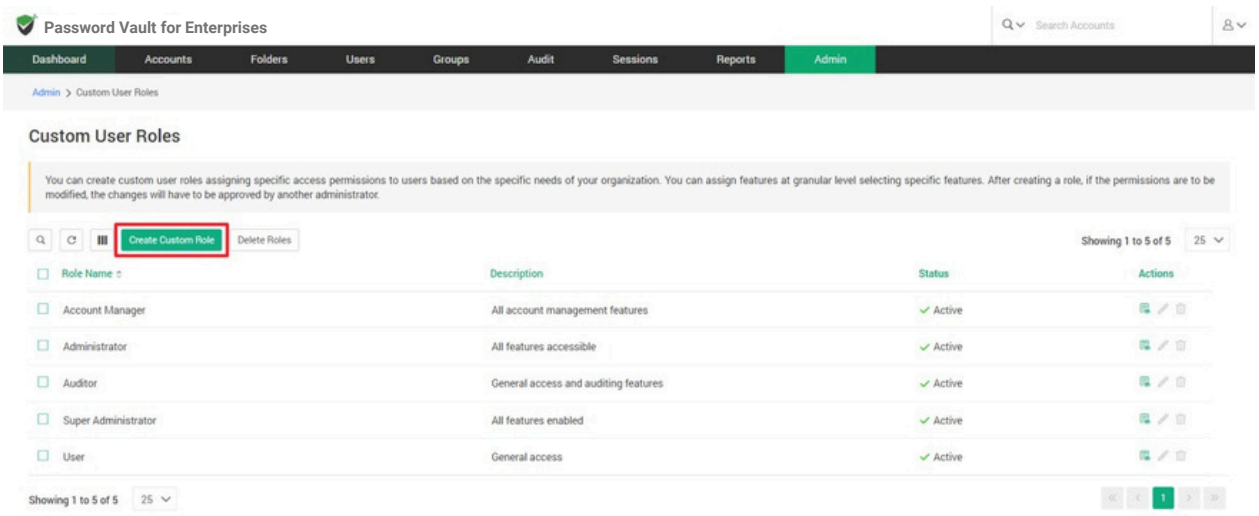
Custom User Roles

Other than the predefined/default roles, you can also create custom user roles based on the specific needs of the organization. You can assign features at a granular level by selecting specific features under each category.

To create custom user roles navigate to **Admin >> Customization >> Custom User Roles.**



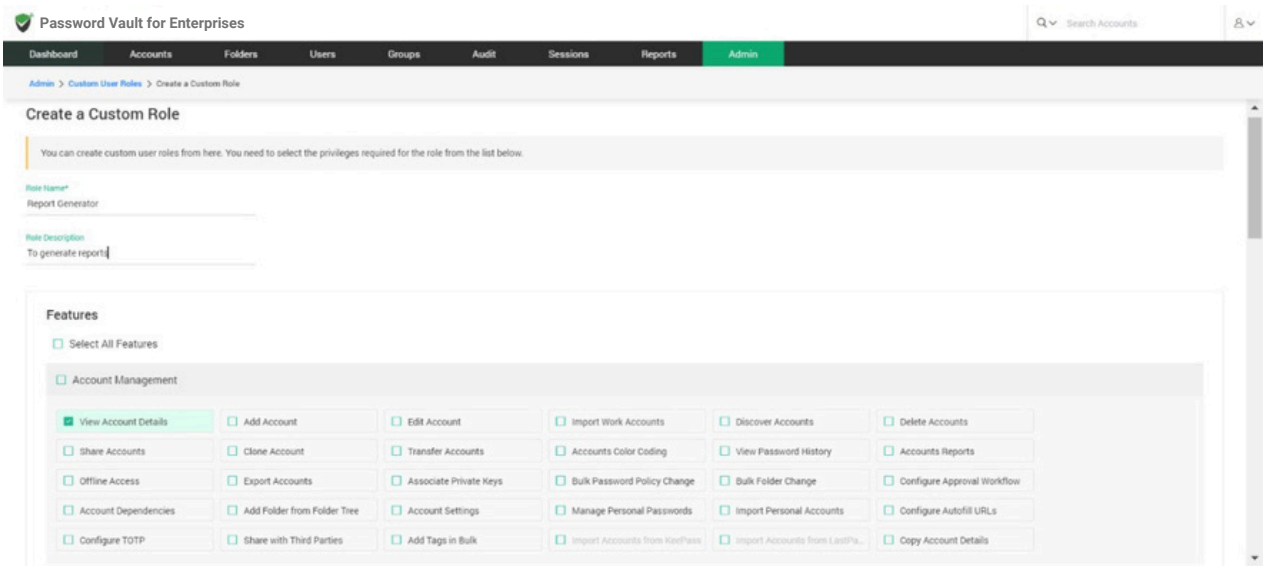
In the page that opens, click on the **Create Custom Role** button



This opens up the role creation page. Each custom role can be given selected privileges from the following categories:

- **Account Management**

- **Folder Management**
- **User Management**
- **Group Management**
- **Audit**
- **Reports**
- **Admin Operations**
- **Miscellaneous**

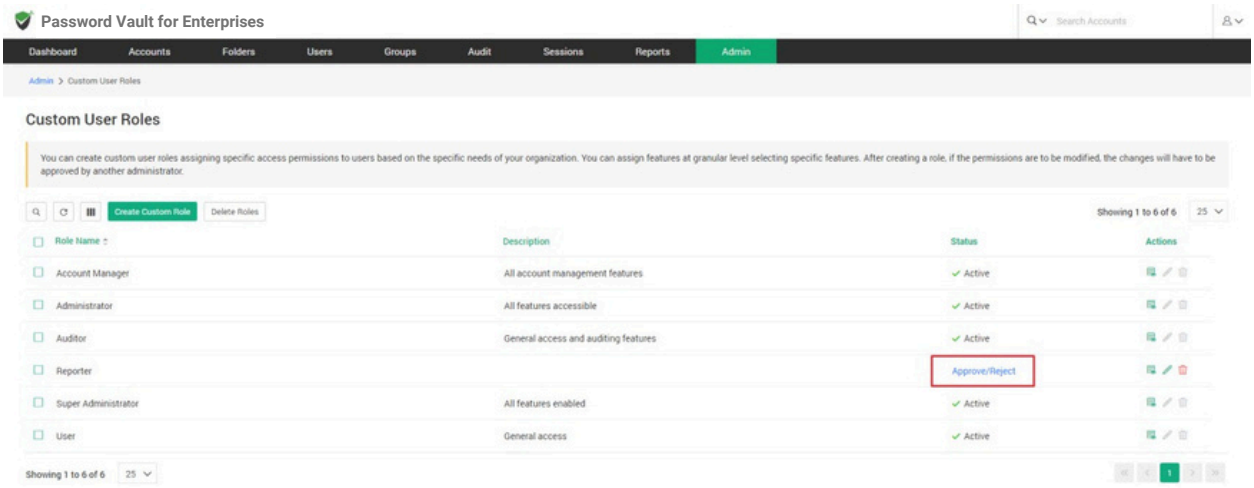


To create a custom role, you need to enter the **Role Name** you want to create and a suitable **Role Description.** You may then select the privileges you would like to provide for this new role.

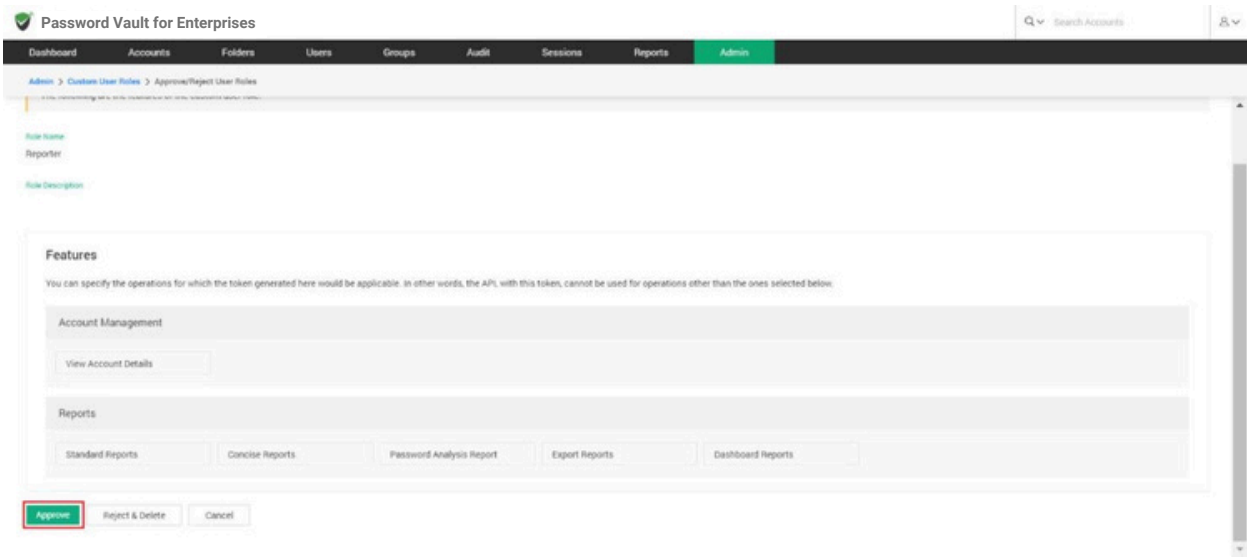
Users assigned with a custom role will be able to carry out select operations in Vault based on the privileges provided to them here.

Once you have selected role privileges, click on the **Save** button to finish role creation.

Note: A new custom role will have to be approved by an administrator other than the one creating it for it to take effect and be available in the product.



The new administrator can review the privileges of that role and **Approve** or **Reject & Delete** this new role.



List of privilege operations for custom user roles

Securden Password Vault has a comprehensive set of privileges that can be modified for each custom role. All such custom role privileges have been explained in the table that follows.

Custom Role Feature	Description
Account Management	
View Account Details	Users with this privilege will be able to view the details for all accounts to which they have access. (Accounts owned by them/shared with them)
Add Account	Users with this privilege will be able to add accounts to the centralized repository. They will be the owners of the accounts they added.
Edit Account	Users with this privilege will be able to edit the attributes of all accounts to which they have access.
Import Work Accounts	Users with this privilege can import work accounts into the database. (Work accounts can be shared with other users, and can be viewed by the Superadmin)
Delete Accounts	Users with this privilege can delete accounts owned by them/shared with them.

Share Accounts	Users with this privilege will be able to share the accounts they own with other users with granular access permissions.
Clone Account	Users with this privilege will be able to make a copy of the selected accounts with all the account details duplicated. Cloned accounts will carry the suffix 'copy'.
Transfer Accounts	Users with this privilege will be able to transfer ownership of the accounts they own to other users added in Securden.
Accounts Color Coding	Users with this privilege will be able to change the background display color for all accounts to which they have modify access permission.
View Password History	Users with this privilege will be able to view all the previous passwords assigned to accounts to which they have ‘View’ permissions.
Accounts Reports	Users with this privilege can view individual account reports for accounts present in Securden.
Offline Access	Users with this privilege will be able to make offline copies of the accounts they have access to. The offline copy will be protected with a passphrase chosen by the user.
Export Accounts	Users with this privilege will be able to export all the accounts they have access to in a CSV or XLSX file.
Associate Private Keys	Users with this privilege will be able to associate private keys (SSH) with the

	accounts to which they have ‘Modify’ access permissions.
Bulk Password Policy Change	Users with this privilege will be able to carry out password policy changes for multiple accounts at the same time. The user should have “Modify” access permissions to all the selected accounts in addition to this ability to be able to carry out bulk password policy change.
Bulk Folder Change	Users with this privilege will be able to carry out a folder change for multiple accounts at the same time. The User should have “Modify” access permissions to all the selected accounts and the destination folder in addition to this ability to be able to carry out folder change.
Configure Approval Workflow	Users with this privilege will be able to configure approvers for request release workflows. The user will need to have ‘Manage’ access permissions for the account involved to be able to configure approvers.
Account Dependencies ENTERPRISE PAM	Users with this privilege will be able to fetch the dependencies of accounts they have access to.
Add Folder from Folder Tree	Users with this privilege will be able to add a folder from the folder tree option that is available to the left of the accounts list.

Account Settings ENTERPRISE PAM	Users with this privilege will be able to modify the preferences available in the Account Settings section.
Manage Personal Passwords	Users with this privilege will be able to generate and rotate passwords of their personal accounts.
Import Personal Accounts	Users with this privilege will be able to import personal accounts (such as internet banking credentials, membership accounts, streaming service account credentials, etc.)
Configure Autofill URLs	Users with this privilege will be able to configure auto-filling credentials on URLs to accounts they have access to.
Configure TOTP	Users with this privilege will be able to configure TOTP generation for specific accounts for which MFA has been enabled.
Share with Third Parties	Users with this privilege will be able to share the account with third parties and specify a time period until which they have access to the account. They can also choose to rotate the password once third party access ends.
Add Tags in Bulk	Users with this privilege will be able to add tags to multiple accounts at the same time.
Folder Management	

Add Folder	Users with this privilege will be able to add folders to Securden.
Edit Folder	Users with this privilege will be able to edit different attributes of folders to which they have access.
Import Folders	Users with this privilege will be able to import folders and their structure from files.
Delete Folder	Users with this privilege will be able to delete folders to which they have access to.
Transfer Folders	Users with this privilege will be able to transfer ownership of folders that they own (Along with the accounts it contains).
Share Folders	Users with this privilege will be able to share folders with other users with a granularity they choose.
Folder Reports	Users with this privilege will be able to view the reports section of folders they have access to.
Folder Settings	Users with this privilege will be able to view and change the preferences in the 'Settings' section of the folders they can access.
Configure Approval Workflow	Users with this privilege will be able to designate approvers for accounts in a folder for request-release workflows.
Change Folder Inheritance in Bulk	Users with this privilege will be able to modify inheritance permissions preferences for multiple folders at the same time.

User Management	
Add User	Users with this privilege will be able to add other users to Securden.
Edit User	Users with this privilege will be able to edit attributes of existing users such as roles, permissions, etc.
Import Users from File	Users with this privilege will be able to import users into Securden from a CSV or an XLSX file.
Delete Users	Users with this privilege will be able to permanently delete existing users in Securden.
Import Users from AD	Users with this privilege will be able to import users from AD using existing Active Directory domain credentials.
Import Users from Azure AD	Users with this privilege will be able to import users from Azure AD using existing domain credentials.
Import Users from LDAP	Users with this privilege will be able to import users from LDAP using existing domain credentials.
Transfer Ownership	Users with this privilege will be able to transfer the ownership of all the accounts owned by them.
Concurrent Logins	Users with this privilege will be able see if any users have concurrently signed in to Securden on another device or browser, and will also be able to terminate any or all the

	logins, which will forcefully log out the user from Securden GUI.
User Reports	
Configure temporary Access	Users with this privilege will be able to grant temporary access to Securden web interface to selected user(s) by specifying access expiration time.
Change User role	Users with this privilege will be able to change the roles of other users.
Control Application Access	Users with this privilege can allow or deny access to other user(s) to access the Securden interface.
Change 2FA	Users with this privilege can alter the two-factor authentication login method used by the selected users(s) to access the Securden interface.
Change Radius Authentication in Bulk	Users with this privilege can alter RADIUS authentication for many users at once.
Reset passwords of accounts accessible to a user ENTERPRISE PAM	Users with this privilege can reset the passwords of accounts that are owned / shared with them.
Add Users to Groups	Users with this privilege will be able to add other users to groups.
User Group Management	
Add User Group	Users with this privilege will be able to create new user group(s) in Securden.

Edit User Group	Users with this privilege will be able to edit user groups.
Delete User Group	Users with this privilege will be able to delete user groups. Deleting user groups does not delete the users in them.
User Group Reports	Users with this privilege will be able to view reports specific to user groups.
Import User Groups from AD	Users with this privilege will be able to import user groups from AD using existing domain credentials.
Import User Groups from Azure AD	Users with this privilege will be able to import user groups from Azure AD using existing domain credentials.
Import User Groups from LDAP	Users with this privilege will be able to import user groups from LDAP using existing domain credentials.
Change 2FA in Bulk	Users with this privilege will be able to change the 2FA method used by users in a user group to login to the Securden interface.
Audit	
View Account Activity Trails	Users with this privilege will be able to view and access all the records of account-related activities.
View User Activity Trails	Users with this privilege will be able to view and access all the records of user- related activities.
Reports	

Standard Reports	Users with this privilege will be able to access all the standard reports, which include the following reports: Account access, Account Activity, Password Compliance, Password Expiry, User Access, User Activity, Dependencies, Processes and Software Inventory, Processes Inventory, Software Inventory, and Securden Agents on Computers.
Concise Reports	Users with this privilege will be able to view and access concise/micro reports pertaining to accounts and users. (Reports >> Concise Reports)
Password Analysis Report	Users with this privilege will be able to view the password security analysis report. This includes the Work Account Analysis report and Personal Accounts Analysis report.
Exported Report	Users with this privilege can view all the reports that were exported and downloaded by other users.
Dashboard Reports	Users with this privilege can view the detailed summary of all the users and accounts present on the dashboard.
Admin Operations	
Manage Account Types	Account Types define the type of accounts being added under 'Work' and 'Personal'

	accounts in Securden. Users with this privilege will be able to add custom account types or edit and delete existing account types.
Manage Password Policies	Password policy in Securden helps you define the strength, complexity requirements, periodicity for password resets and other conditions. Users with this privilege will be able to add/delete a password policy and perform all actions related to it. (Under Admin >> Account Management > Password Policy)
Manage Event Listeners	You can trigger an action after the occurrence of any specific event or a sequence of events in Securden. For example, when the password of an account is changed, you can trigger a follow-up action automatically. This privilege lets the user add/delete and manage the listeners.
Device Level Configurations ENTERPRISE PAM	A user with this privilege will be able to manage all device level configurations that includes managing remote credentials, session recording, remote gateway, and reports.
Approve Password Access Requests ENTERPRISE PAM	Users with this privilege will be able to approve all the requests from other users to access certain passwords.
Manage Event Notifications	Securden can send email notifications upon the occurrence of certain events such as password retrieval, deletion, change in share permissions, and others.

ENTERPRISE PAM *Feature available only in the **Enterprise PAM** edition of Securden Password Vault*

	Users given this privilege will be able to configure the event notifications.
Manage Expiration Notifications	You can send email notifications a certain number of days prior to the expiration date of the passwords to serve as a reminder to change the password. Users with this privilege will be able to manage the notifications sent during password expiry.
Manage Breached Passwords Identification	Securden can periodically scan the breached passwords database and check if any of the passwords stored in the product matches with the passwords that have been exposed in known data breaches. Users with this privilege can enable this feature and configure how often Securden should check for breached passwords.
Manage Account Expiration Notification	You can keep track of the expiration dates of license keys and certificates stored in Securden. You can send email notifications a certain number of days prior to the expiration date to serve as a reminder. Users with this privilege will be able to configure this expiration notification for accounts.
Manage Custom Roles	You can create custom user roles assigning specific access permissions to users based on the specific needs of your organization. Users with this privilege will be able to create customized user roles with varied features.

Securden Agent Text Customization ENTERPRISE PAM	You can customize the labels and messages in the Securden Agent interface. Users with this privilege will be able to modify the text of the interface.
Manage Configuration Settings	You can customize the features of Securden in a granular manner. You can switch on and switch off certain features anytime as desired under the 'Configurations' section in the ‘Admin’ tab. Users with this privilege will be able to access it.
Customize Logo, Text	You can replace the Securden logo that appears in the login page and also the text that appears throughout the GUI as you wish. Users with this privilege will be able to customize it.
Change Product Language	Securden supports multiple languages, and you can carry out the desired language selection. Users with this privilege will be able to change the product language.
Access and Manage APIs	Securden provides APIs for querying the database programmatically, retrieving credentials, and performing various other tasks. Users with this privilege will be able to create authentication tokens for carrying out various operations using APIs.
Configure 2FA	You can enforce a second layer of authentication for your users to access their Securden account. Users with this

	privilege will be able to activate two - factor authentication.
Manage Email to SMS Gateway	As part of two-factor authentication, Securden integrates with Email to SMS gateway providers to send one-time passwords as SMS to the phone numbers of the users. This privilege lets users configure this feature.
Manage Duo Configuration	Securden integrates with Duo Security for two factor authentication. Once configured, users will be enforced to authenticate through Duo for accessing the web interface. Users given this privilege will be able to configure this feature.
Configure RADIUS Server Settings	You can integrate RADIUS server or any RADIUS-compliant two-factor authentication system like OneSpan Digipass, RSA SecurID, Swivel Secure etc. for the second factor authentication. Users given this privilege will be able to configure these settings.
Smart Card Authentication	If your organization uses smart cards for authenticating user logons, you can leverage the same for Securden authentication. Users given this privilege will be able to enable smart card authentication.
Manage SIEM Integration	You can periodically share privileged access data logs with SIEM solutions. Users given this privilege will be able to

	manage the Syslog configuration in Securden.
Manage SAML SSO Integration	Securden leverages SAML 2.0 to integrate with SAML-compatible federated identity management solutions like Okta, G Suite, Microsoft ADFS, OneLogin, PingIdentity, Azure AD SSO, and others for Single Sign On. Users given this privilege will be able to enable SAML SSO and configure it.
Manage Ticketing System Integration ENTERPRISE PAM	Securden integrates with web-based ticketing systems. The integration helps trace specific activities like password retrieval in Securden to corresponding entries in the ticketing system. This privilege lets users activate and configure ticketing system integration in Securden.
Manage Mail Server Settings	Securden sends various email notifications to the users and to facilitate that, SMTP server details are to be configured. Users with this privilege will be able to configure the server settings.
Manage Proxy Server Settings	If your organization makes use of a proxy server to regulate internet traffic, you should configure the proxy server details in Securden to connect to the internet. Users who are given this ability will be able to configure the proxy server settings.
Manage Securden Server Connectivity Settings	Securden server connectivity specifies how client machines connect to the Securden web interface and the name with which

ENTERPRISE PAM *Feature available only in the **Enterprise PAM** edition of Securden Password Vault*

	client machines identify the Securden server host when deploying agents. Users who are given this privilege will be able to configure these settings.
Manage Securden License	Users with this privilege can apply for the Securden license key and get information about the existing license from the 'Admin' section. Users who are given this privilege will be able to view the available information about the existing license, and also can apply for a new license.
Manage Domain Administrator Groups ENTERPRISE PAM	You can create a scheduled task to get notified if there is any modification in the domain administrator groups. Users with this privilege will get access to the Domain Administrator Groups and can also schedule the notifications.
Change Encryption Key Location	Every installation of Securden is protected with a unique encryption key. Securden doesn't allow the encryption key and the encrypted data to reside in the same location to ensure security. Hence, the key has to be moved outside the Securden installation folder. Users who are given this privilege will be able to change the location of the encryption key.
Manage 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. This access requires configuring an

	additional security measure by way of certificate-based client authentication. This privilege lets users enable certificate-based authentication and configure it.
Manage IP-based Restrictions	You can control access to Securden server based on the IP addresses of users. Users with this privilege will be able to enable IP restrictions for other users.
Manage User Access to Securden	If required, you can block access to Securden server from the browser extensions, APIs, and mobile apps. Users who are given this privilege will be able to block access, which will take effect for all users, including the super admin globally.
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. Users who are given this privilege will be able to schedule the backup.
Configure High Availability	To ensure uninterrupted access to the web application, Securden comes with high availability architecture. You can deploy any number of additional application servers, which would serve as the secondary servers. In the event of the primary server going

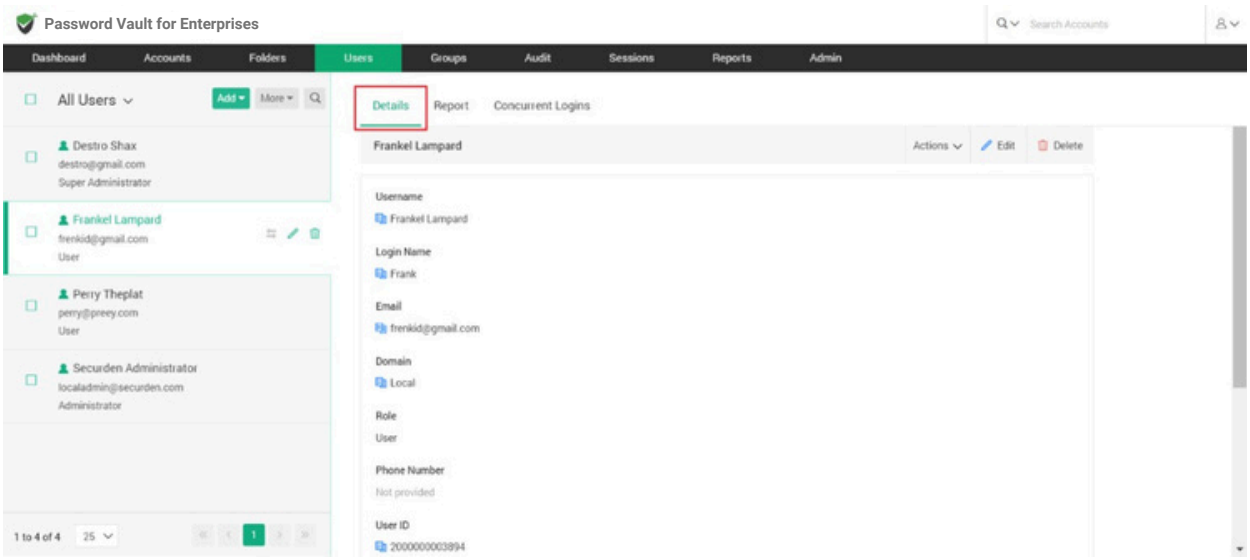
	down, users can connect to any of the secondary servers. Securden agents will also connect to the secondary server, when the primary goes down. Users who are given this privilege will be able to set this feature on and configure the secondary application server(s).
Maintenance and Upgrades	Users who are given this privilege will be able to access 'Product Upgrades' section where the latest product updates, release notes, and the steps to upgrade the latest version are present.
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. Users who are given this privilege will be able to configure the emergency access.
Configure Assets and Assets Association for Remote Connections	Users who have this privilege can add their IT assets to Securden and configure the association between domain accounts and assets for launching remote connections.
User Assets Association for Remote Connections	You can allow your users to launch remote connections to specific resources using the AD account with which they have logged in to Securden. You can associate the IT assets with the users, which will permit them to launch the connection with the assets

	allotted. This privilege lets the user configure the association between users and assets for launching remote connections.
Configure Expired Password Rotation ENTERPRISE PAM	Securden can automatically rotate passwords for accounts that support remote password reset when they expire or are about to expire. Users who have this privilege will be able to configure the password rotation upon expiration.
Configure 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. Users who have this privilege will be able to create a profile for any such application and manage them in Securden to launch remote connections.
Manage Global Tags	When user tag creation is disabled, they have the option to select from tags created globally. So, the user with this privilege will be able to create, edit, and delete global tags.
Miscellaneous	
Access Browser Extensions	Users with this privilege can access browser extensions to facilitate auto-fill of credentials

	on websites and web applications.
Manage Browser Extensions	Users with this privilege will be able to manage and configure the browser extension settings.
Use Windows Remote Launcher	Users with this privilege will be able to launch RDP and other remote connections from Securden web interface.

User Details

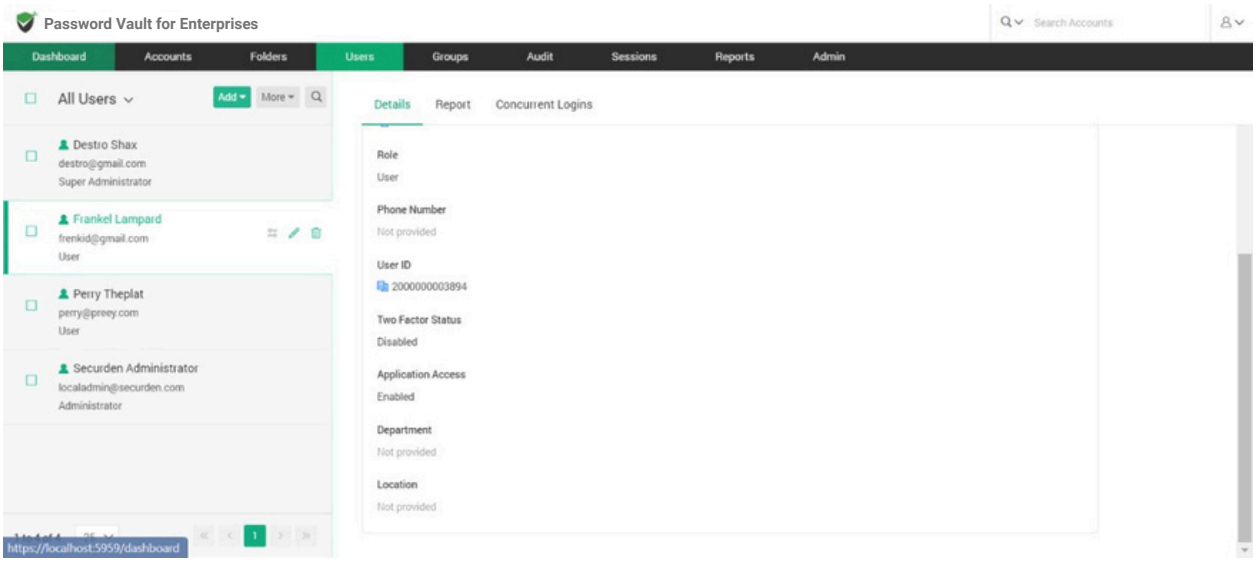
You can get detailed information about user accounts from the **Details** tab when you select each user.



The details contain main information such as the Username, Login Name, Email address, Domain name, and their role.

Other details include the Phone number, 2FA status, Application Access, Location, and User ID.

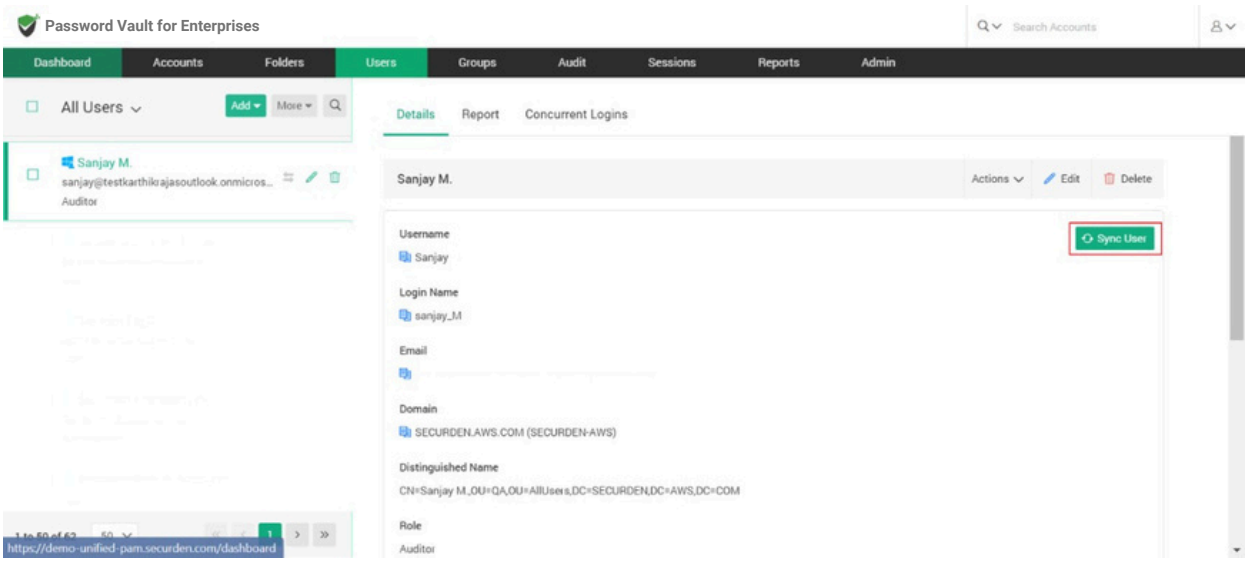
User ID is particularly useful for making use of APIs to retrieve or modify user information. You can copy the User ID with the icon available beside it.



Keeping users in Synchronization with your Active Directory

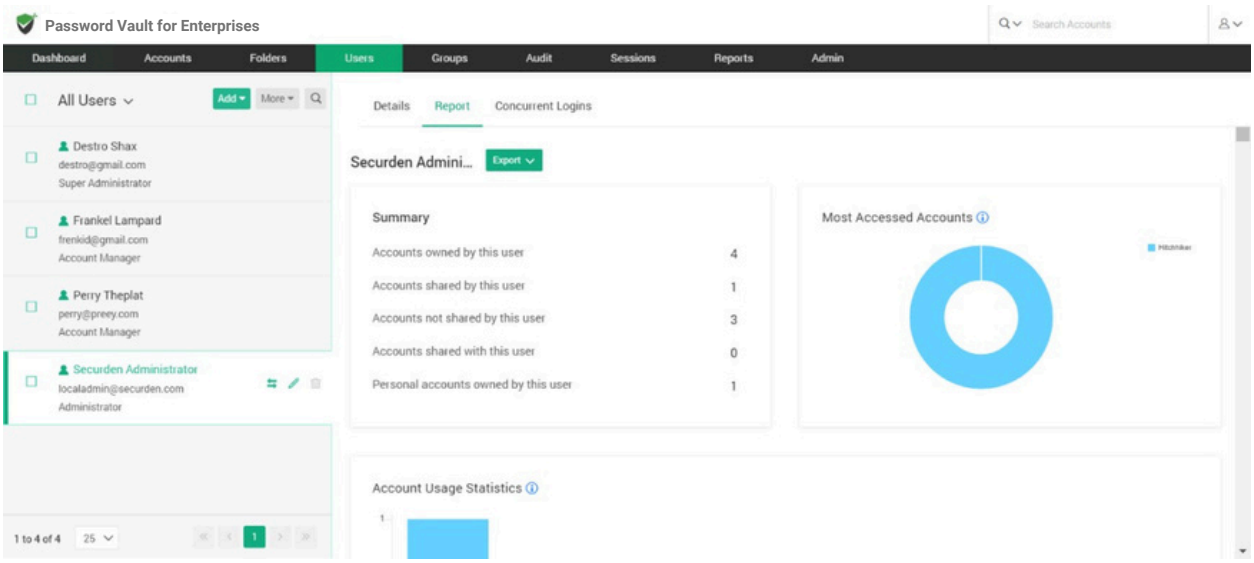
You can select the **Sync User** option to sync the user details with your AD. If the user has been deleted from AD, they will be disabled in Securden.

Note: This is only applicable for users imported from domain, and not for manually added users or those imported from a file.



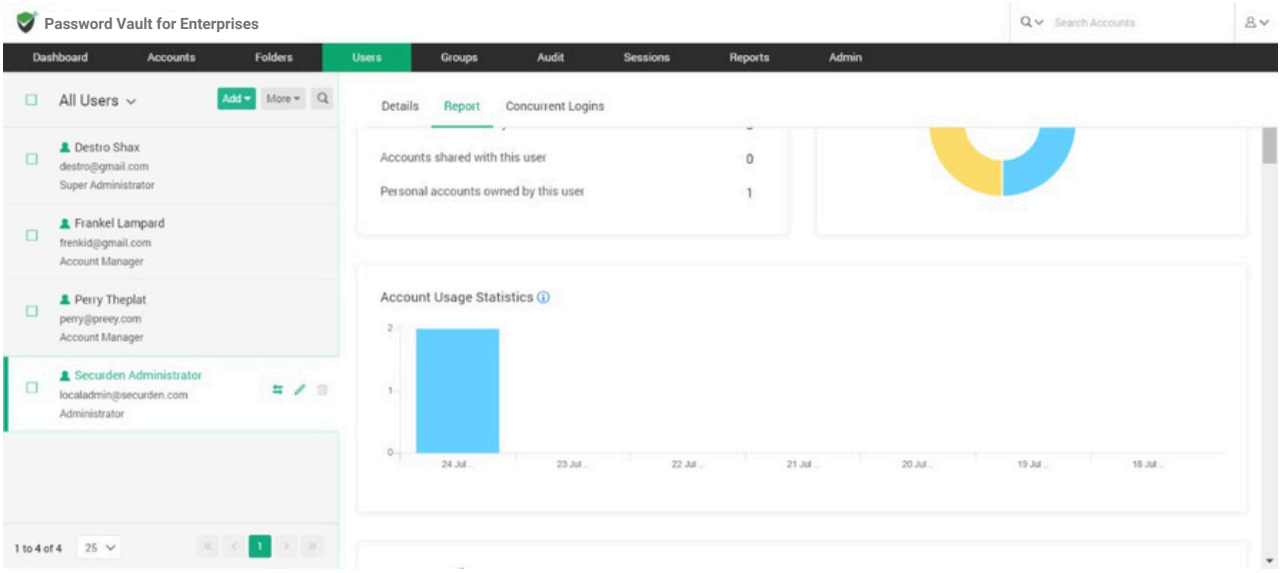
User Reports

Under the User Report, you can view a comprehensive summary of a particular user account. It gives you a detailed report on what all accounts have been accessed and what permissions a user has on each account.



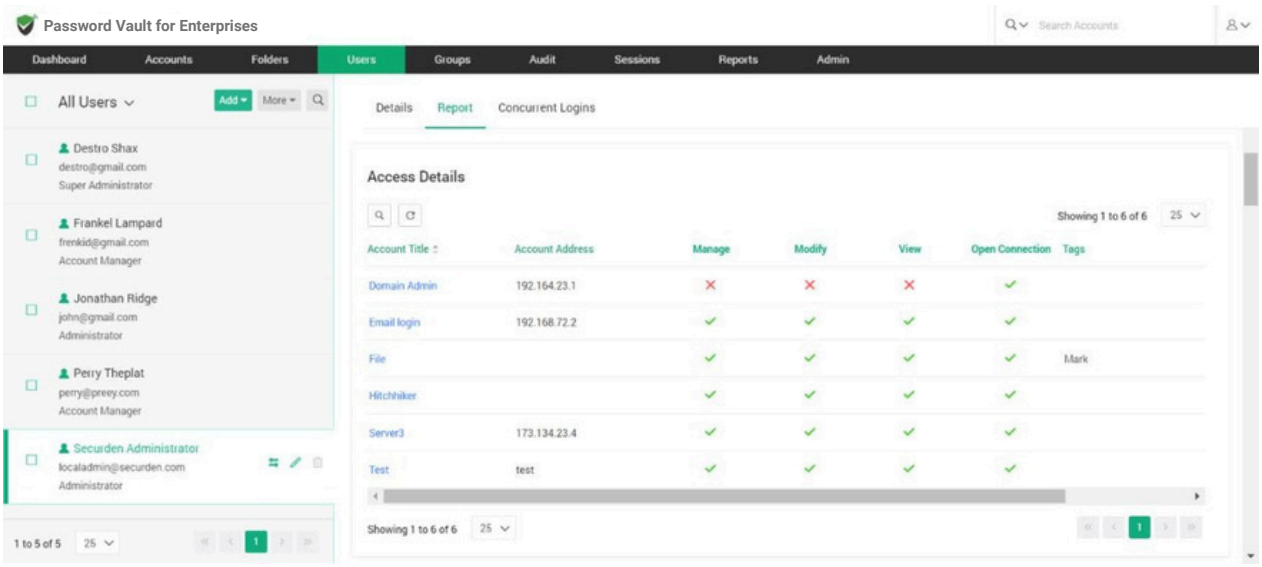
Account Usage Statistics

Here, you can see the day-wise statistics of different activities carried out by the user account such as password retrievals, remote connections launched, and password auto-fills on websites.



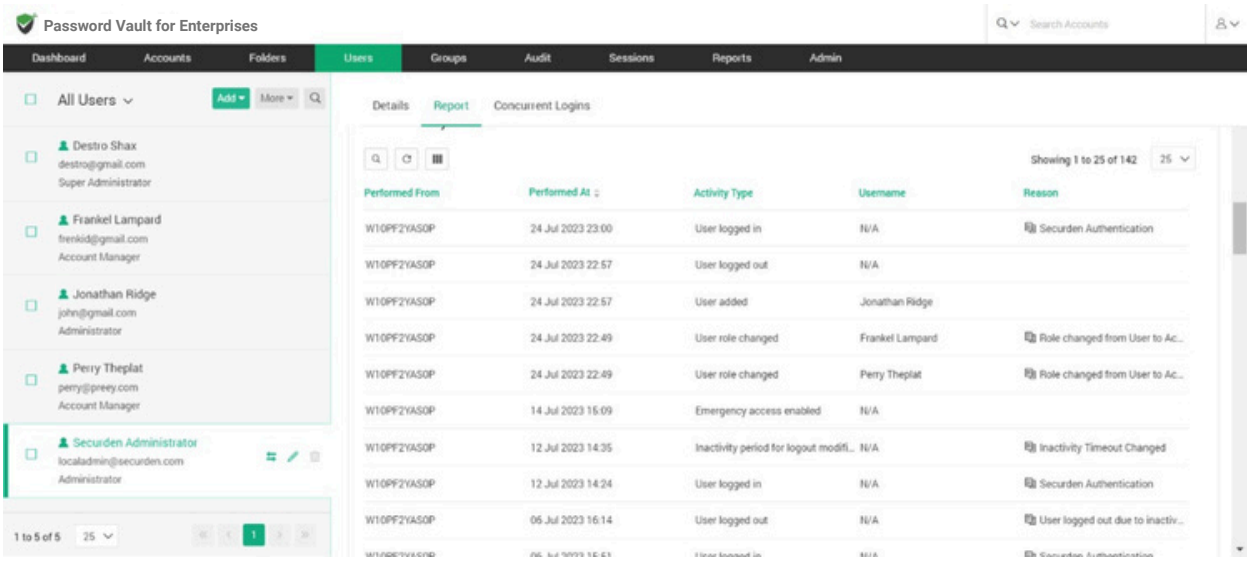
Access Details

This gives you the list of accounts owned by a user and the accounts that are shared with them. Alongside this, it shows the level of access permissions (Manage, Modify, View, and Open Connection) that the user has on different accounts.



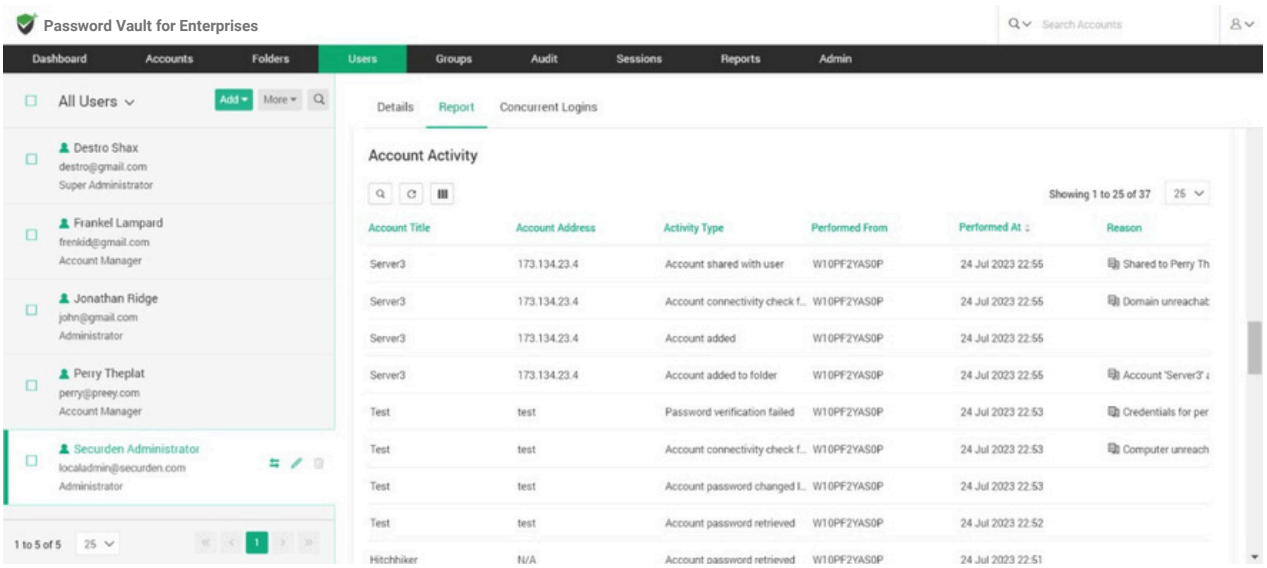
User Activity

User Activity explains the 'where', 'when', and 'what' of various activities performed by a user.

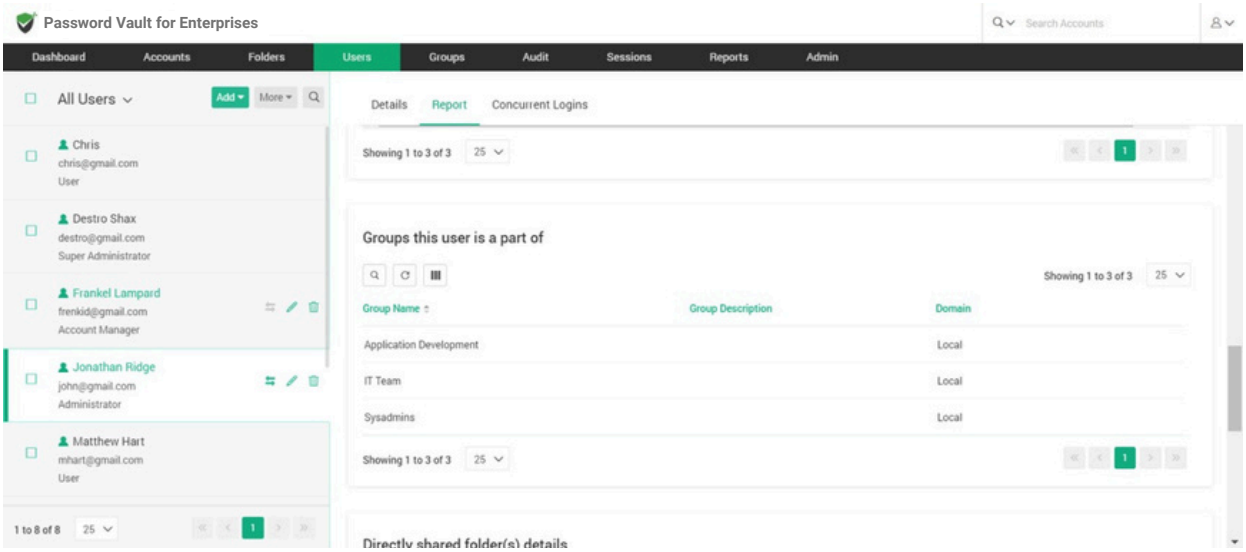


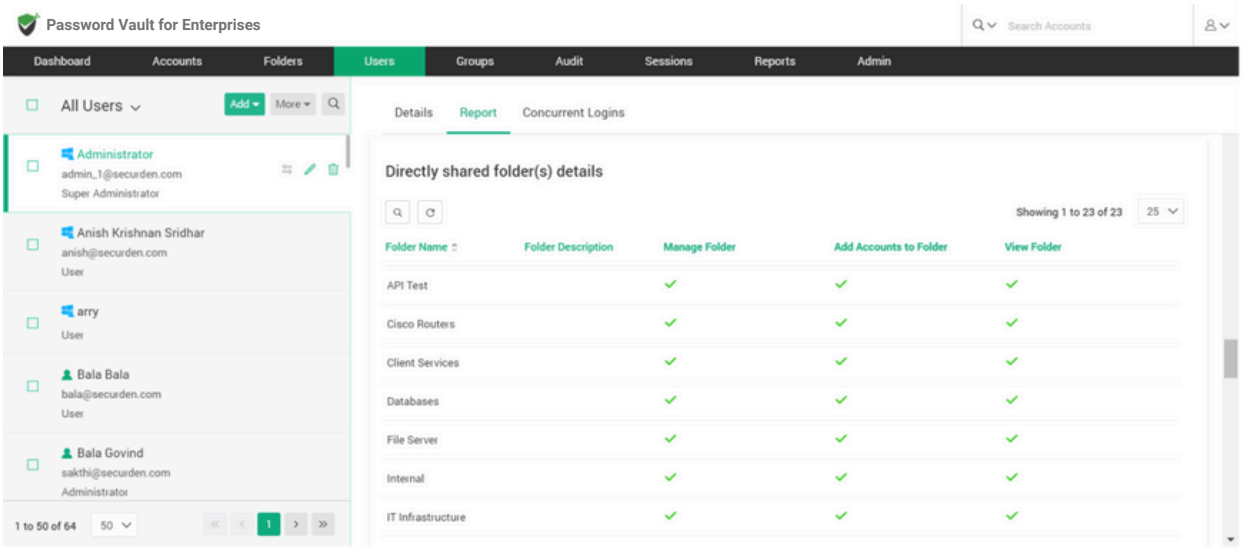
Account Activity

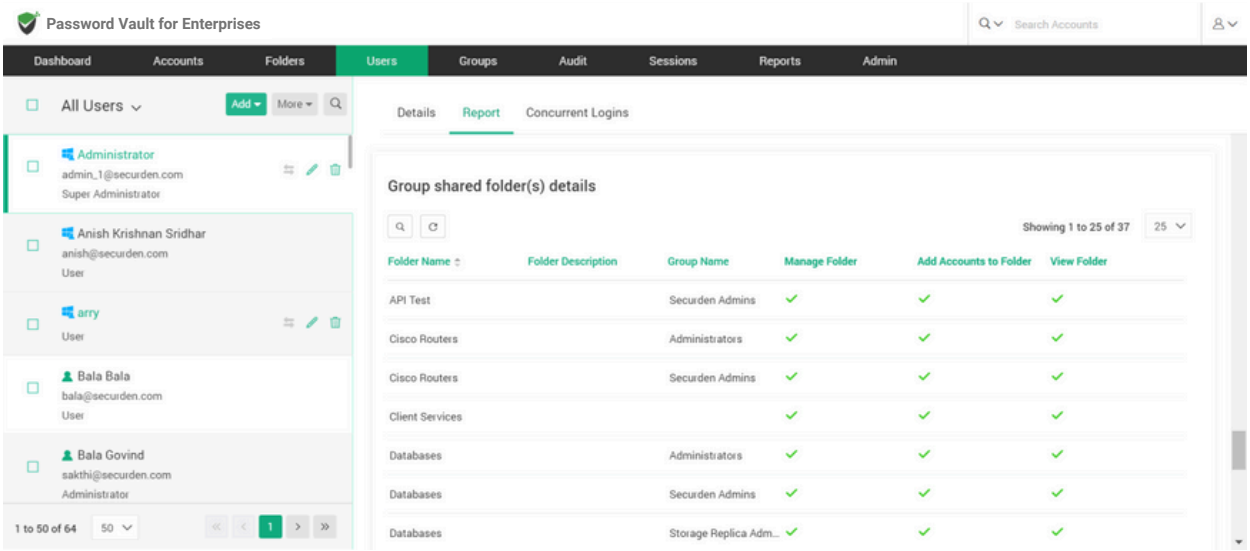
Account Activity gives the list of accounts and the actions carried out on those accounts.



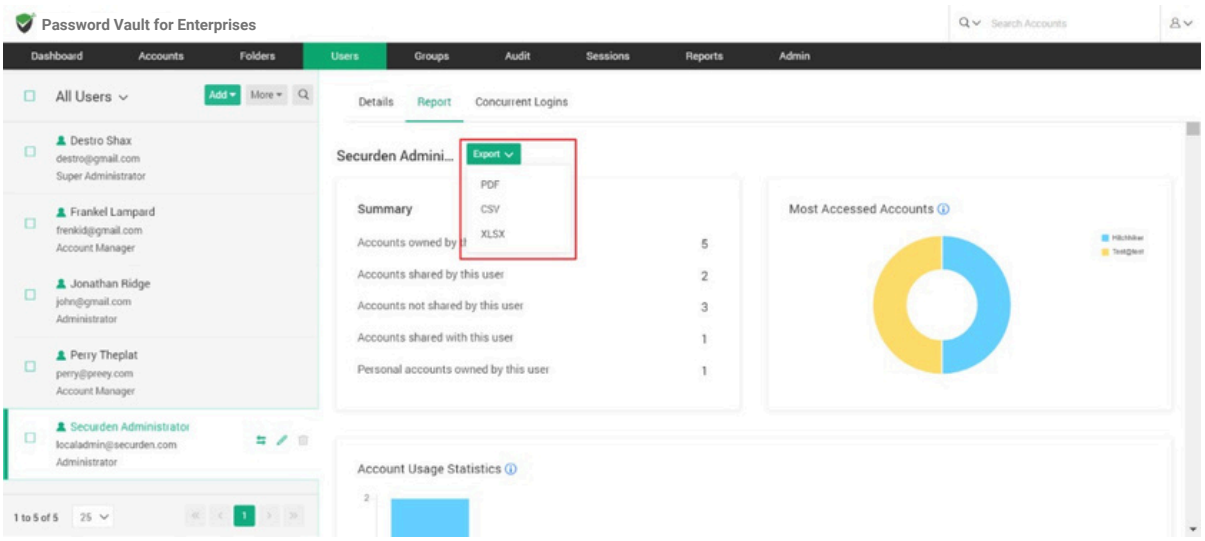
Groups this user is a part of, **Directly shared folder(s) details**, and **Group shared folder(s) details** are the other insights of User Report section.




Password Vault for Enterprises
Search Accounts
Dashboard
Accounts
Folders
Users
Groups
Audit
Sessions
Reports
Admin
All Users
Add
More
Administrator
admin_1@securden.com
Super Administrator
Anish Krishnan Sridhar
anish@securden.com
User
arry
User
Bala Bala
bala@securden.com
User
Bala Govind
sakthi@securden.com
Administrator
1 to 50 of 64
50
Details
Report
Concurrent Logins
Directly shared folder(s) details
Showing 1 to 23 of 23
25
Folder Name
Folder Description
Manage Folder
Add Accounts to Folder
View Folder
API Test
Cisco Routers
Client Services
Databases
File Server
Internal
IT Infrastructure


Password Vault for Enterprises
Search Accounts
Dashboard
Accounts
Folders
Users
Groups
Audit
Sessions
Reports
Admin
All Users
Add
More
Administrator
admin_1@securden.com
Super Administrator
Anish Krishnan Sridhar
anish@securden.com
User
arry
User
Bala Bala
bala@securden.com
User
Bala Govind
sakthi@securden.com
Administrator
1 to 50 of 64
50
Details
Report
Concurrent Logins
Group shared folder(s) details
Showing 1 to 25 of 37
25
Folder Name
Folder Description
Group Name
Manage Folder
Add Accounts to Folder
View Folder
API Test
Securden Admins
Cisco Routers
Administrators
Cisco Routers
Securden Admins
Client Services
Databases
Administrators
Databases
Securden Admins
Databases
Storage Replica Adm...

To export the user specific report, Navigate to **Users >> (select the required user account) >> Reports >> Export.**



You can also click on **Download as PDF** to directly download the report.

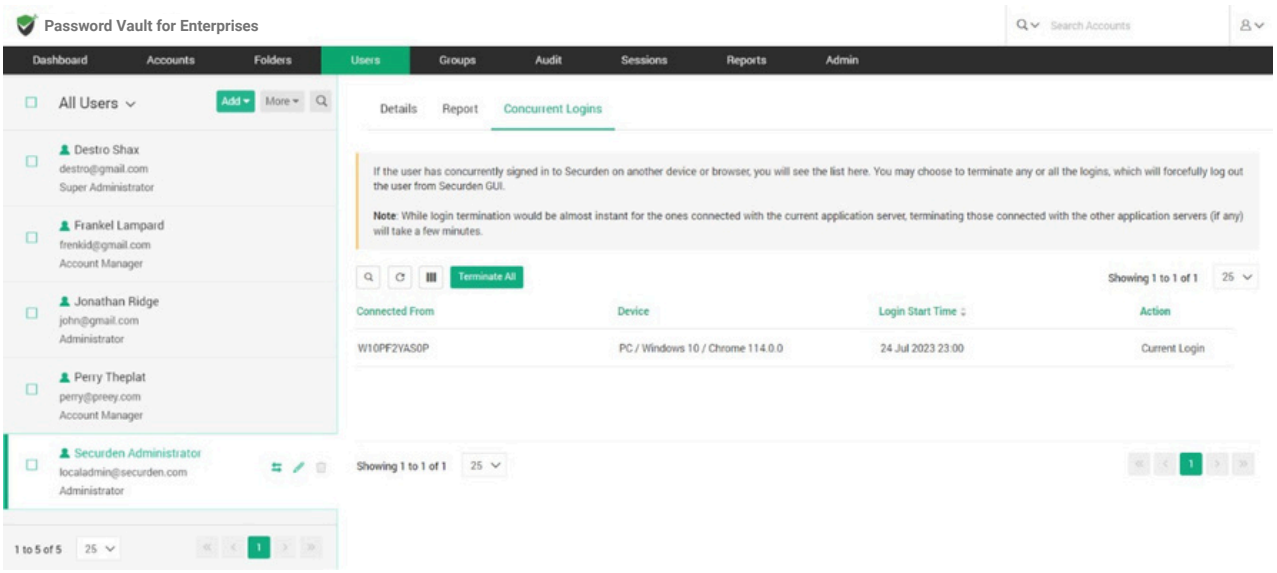
User Report can be exported in three different formats such as PDF, CSV, and XLSX.

Monitor Concurrent Logins

You can monitor the concurrent logins of each user.

For example, if a user has logged in to the Securden web interface through the web on multiple browsers, and also through mobile apps, the **Concurrent Logins** section lists out all the different logins.

You can review and even terminate any or all the logins, which will forcefully log out the user from Securden GUI.

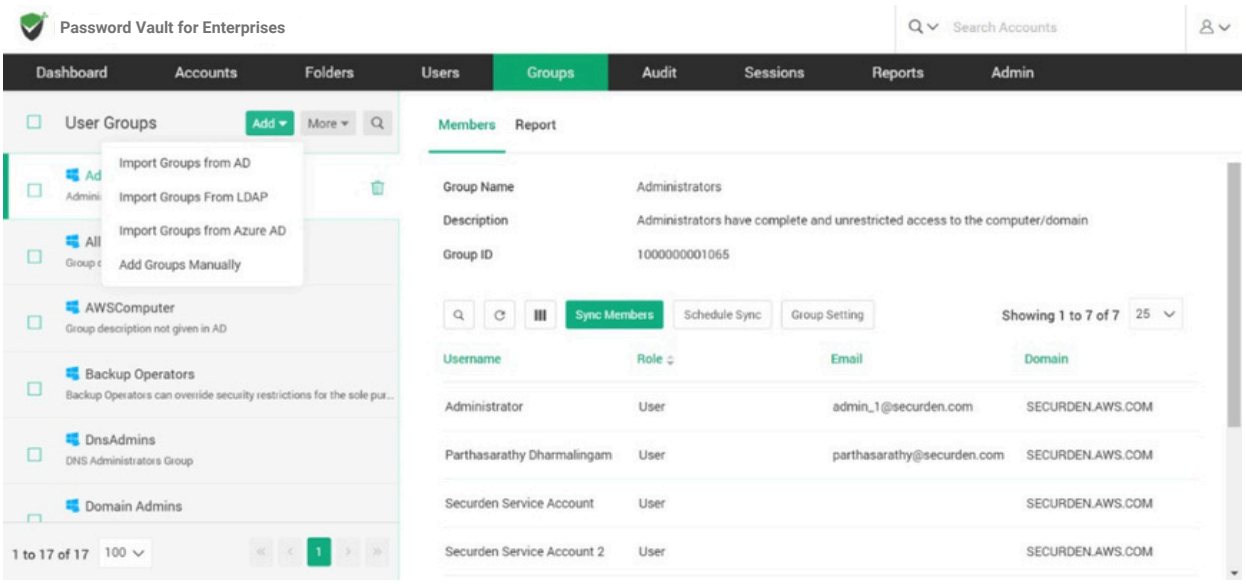


User Groups

You can organize the users in your organization as groups in Securden for efficient administration. You can even maintain the same team structure as in the organization. User groups help you carry out multiple operations for numerous users at the same time.
Adding groups can be done in the following ways:

- Import groups from AD
- Import groups from Azure AD
- Import groups from LDAP
- Add groups manually

Navigate to the **Groups** tab and click **Add** in the GUI to perform this step.

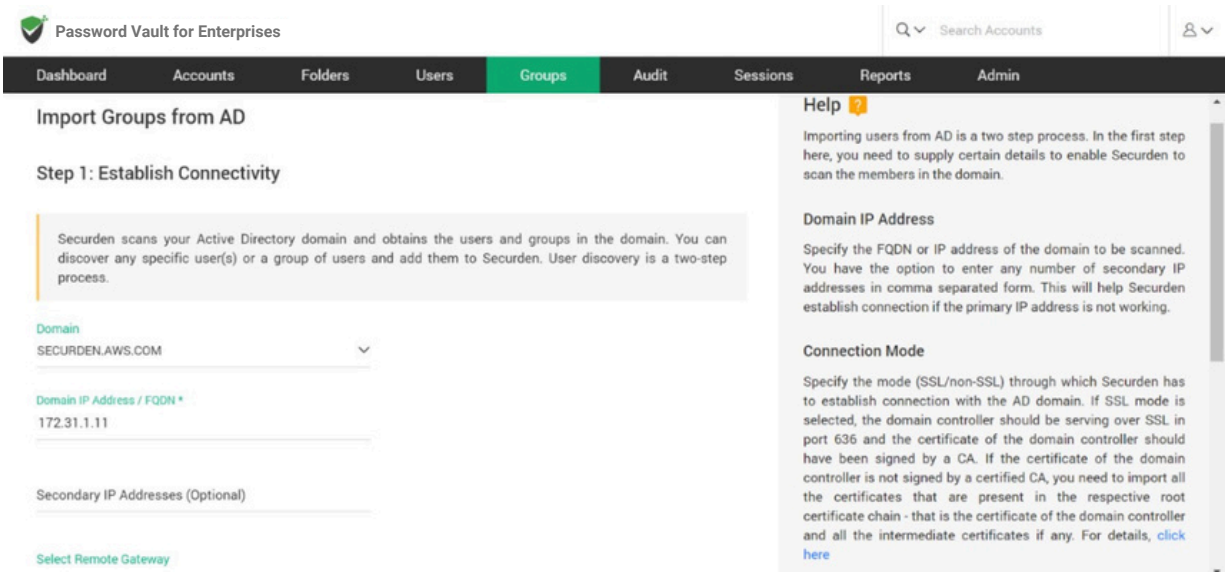


Import User Groups from AD

Securden scans your Active Directory domain and obtains the users and groups in the domain. You can discover any specific user(s) or a group of users and add them to Securden. User discovery is a two-step process.

Step 1: Establish Connectivity

This step requires you to provide certain details to enable Securden to scan members of the domain.



***Domain IP Address*:** Specify the FQDN or IP address of the domain controller to be scanned. You have the option to enter any number of secondary IP addresses (secondary domain controllers) in comma separated form. This will help Securden establish a connection if the primary is not accessible.

***Connection Mode*:** Specify the mode (SSL/non-SSL) through which Securden has to establish a connection with the AD domain.

If SSL mode is selected, the domain controller should be serving over SSL in port 636 and the certificate of the domain controller should have been signed by a CA.

If the certificate of the domain controller is not signed by a certified CA, you need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the domain controller and all the intermediate certificates if any.

You can follow the example given below to import the domain controller's certificate into the certificate store of the Securden server machine. However,

you may use any procedure that you would normally use to import the SSL certificates to the machine's certificate store.

- In the Securden server machine, launch Internet Explorer and navigate to **Tools >> Internet Options >> Content >> Certificates.**
- In the GUI that pops up, click **Install Certificate** and then choose **Local Machine** in the next step.
- Browse and locate the root certificate issued by the CA.
- Click **Next** and choose the option **Automatically select the certificate store based on the type of certificate** and install.
- Click **Import** again.
- Browse and locate the domain controller certificate.
- Click **Next** and choose the option **Automatically select the certificate store based on the type of certificate** and install.
- Apply the changes and close the wizard.
- Repeat the procedure to install other certificates in the root chain.

***Supply Administrator Credentials*:** You need to supply administrator credentials to enable Securden to scan the members in the domain. You may enter the username and password manually once and this will be stored in Securden for use during subsequent import attempts.
You can discover any group of users and add them to Securden.

Step 2: Go to Import

This step is to fetch the required user groups from the AD domain specified.

This GUI offers the flexibility to fetch user groups from OUs/Groups in bulk and even specific users, in a single step. That means, you can enter the names of the OU/Groups to be discovered in a single step. You can enter the discovery details in any combinations (OUs and Groups) as you wish.

To import OUs, select the OU tab.

1. Enter the OU name and select **Discover.**
2. You can also browse from the OU tree by clicking on the **Browse OU Tree and Select** option. You can select one or multiple OUs and select **Add.**
3. You can then verify your selection in the **Verify the Objects Selected for Discovery.**
4. You can then select the role for the OUs imported using the **Role in Securden** drop down.
5. Before selecting the import button, you can look into the additional settings which are explained below.
6. Select **Import.**

To import Groups, select the Groups tab.

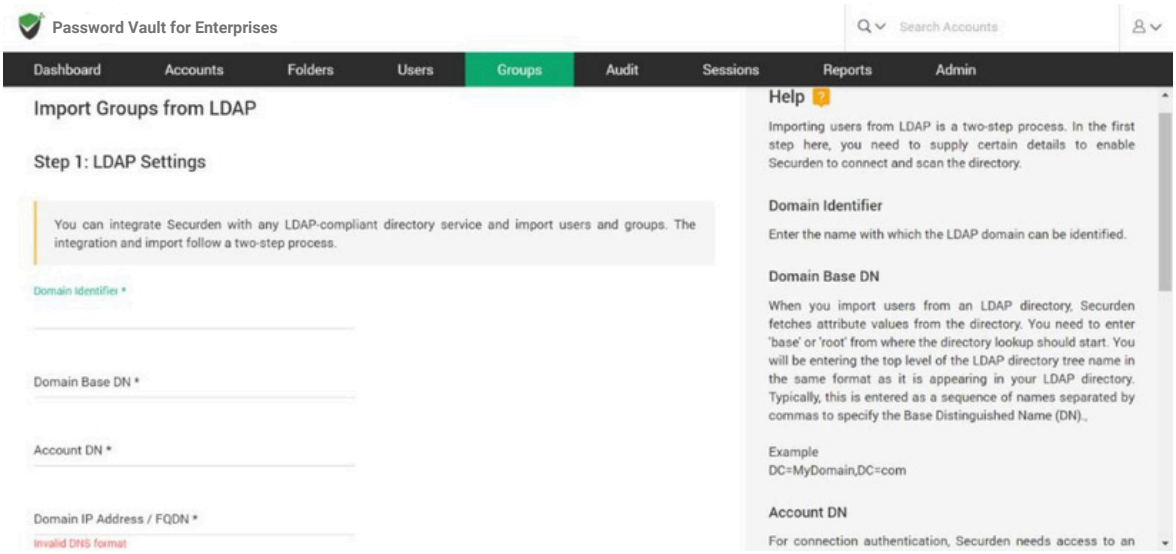
1. Enter the Group name and select **Discover.**
2. You can also browse by clicking on the **Browse Groups and Select** option. You can select one or multiple groups and select **Add.**
3. You can then verify your selection in the **Verify the Objects Selected for Discovery.**
4. You can then select the role for the OUs imported using the **Role in Securden** drop down.
5. Before selecting the import button, you can look into the additional settings which are explained below.
6. Select **Import.**

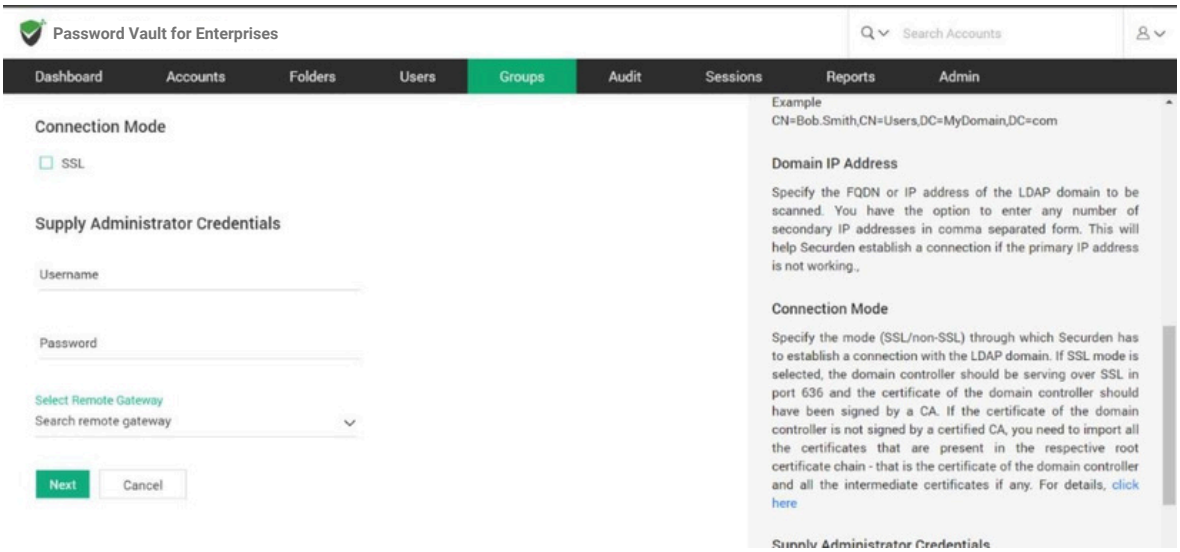
Advanced settings:

This option allows you to either include domain users of all subgroups to the group being imported or ignore the subgroups and import only the users of the first level group.

Import groups from LDAP

Importing user groups from LDAP is a two-step process. In the first step here, you need to supply certain details to enable Securden to connect and scan the directory.





Step 1: LDAP Settings

You can integrate Securden with any LDAP-compliant directory service and import user groups. In the GUI that opens, enter the following credentials to proceed with the integration.

Domain Identifier: Enter the name with which the LDAP domain can be identified.

Domain Base DN: When you import user groups from an LDAP directory, Securden fetches attribute values from the directory. You need to enter **base** or **root** from where the directory lookup should start. You will be entering the top level of the LDAP directory tree name in the same format as it is appearing in your LDAP directory. Typically, this is entered as a sequence of names separated by commas to specify the Base Distinguished Name (DN). Example DC=MyDomain,DC=com

Account DN: For connection authentication, Securden needs access to an LDAP account that has read access and is password-protected. You need to

enter the Account DN here. You may enter the account name and password in the last step.

Example

CN=Bob.Smith,CN=Users,DC=MyDomain,DC=com

Domain IP Address: Specify the FQDN or IP address of the LDAP domain to be scanned. You have the option to enter any number of secondary IP addresses in comma separated form. This will help Securden establish a connection if the primary IP address is not working.

Connection Mode: Specify the mode (SSL/non-SSL) through which Securden has to establish a connection with the LDAP domain.

- If SSL mode is selected, the domain controller should be serving over SSL in port 636 and the certificate of the domain controller should have been signed by a CA.
- If the certificate of the domain controller is not signed by a certified CA, you need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the domain controller and all the intermediate certificates if any.

Supply Administrator Credentials:

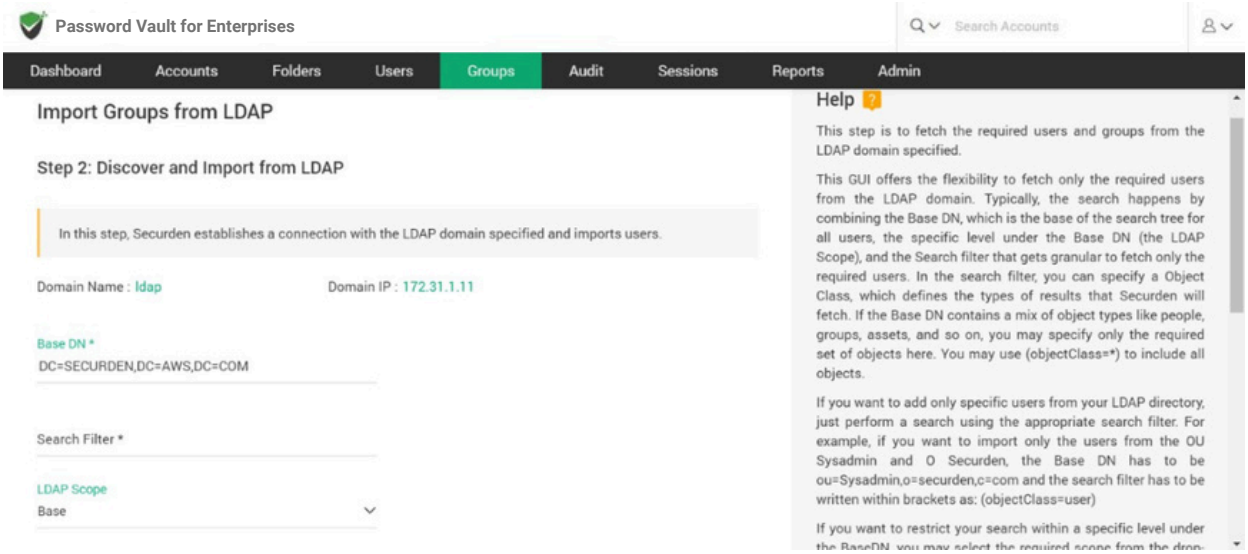
You need to supply administrator credentials so as to enable Securden to scan the members in the domain. You may enter the username and password manually once and this will be stored in Securden for use during subsequent import attempts. If the users belong to a different network than the Securden server, you can route the connection through a remote gateway. You can select the appropriate remote gateway

from the drop-down and the discovery will happen through the selected gateway.

Step 2: Discover and Import from LDAP

In this step, Securden establishes a connection with the LDAP domain specified and imports user groups.

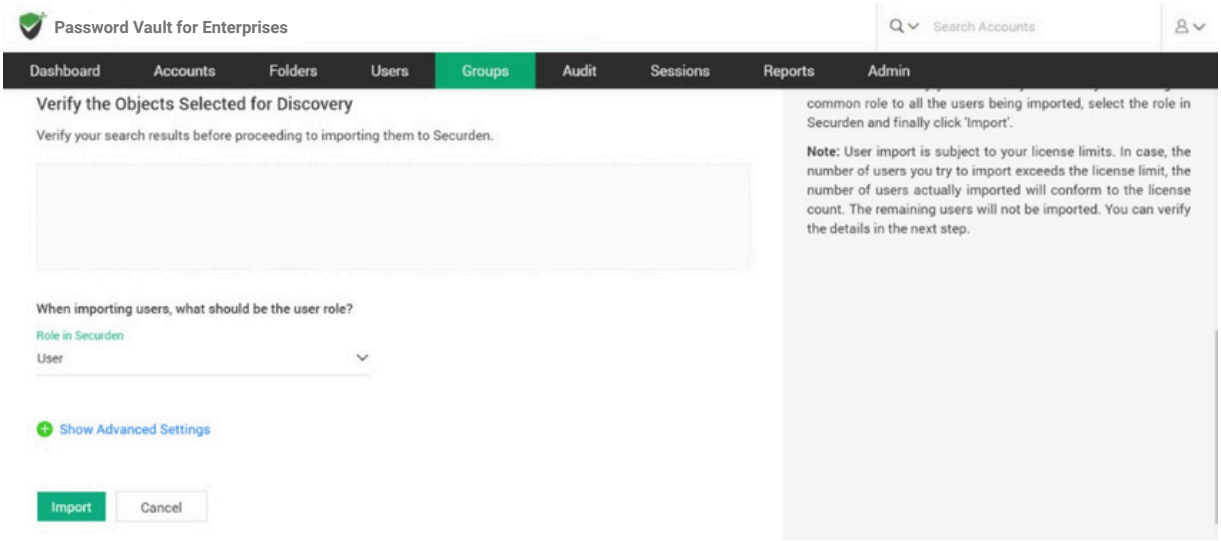
This GUI offers the flexibility to fetch only the required user groups from the LDAP domain.



- Typically, the search happens by combining the **Base DN**, which is the base of the search tree for all users, the specific level under the Base DN (the **LDAP Scope**), and the **Search Filter** that gets granular to fetch only the required users/user groups.

- In the search filter, you can specify an Object Class, which defines the types of results that Securden will fetch. If the Base DN contains a mix of object types like people, groups, assets, and so on, you may specify only the required set of objects here. You may use (objectClass=*) to include all objects.

- If you want to add only specific user groups from your LDAP directory, just perform a search using the appropriate search filter. For example, if you want to import only the groups from the OU Sysadmin and O Securden, the Base DN has to be ou=Sysadmin,o=securden,c=com and the search filter has to be written within brackets as: (objectClass=user).
- If you want to restrict your search to a specific level under the BaseDN, you may select the required scope from the drop-down.
- Click **Search**. Verify your discovery details under **Verify the Objects Selected for Discovery**. If you to assign a common role to all the users being imported, select the role in Securden and finally click **Import**.



***Advanced Settings*:**

This option allows you to either include domain users of all subgroups to the group being imported or ignore the subgroups and import only the users of the first level group.

Import from Azure AD

Securden allows you to import users from Azure AD. This is a two-step process. In the first step, you need to supply certain connectivity details to enable Securden to scan the members in the domain. This step requires integration with Azure AD and some configuration steps. For details, refer to ***Securden-Azure-AD-Guide.pdf***

Step 1: Establish Connectivity

Prerequisites:

Azure AD import requires internet connectivity. If your organization makes use of a proxy server to regulate internet traffic, you should have configured Proxy Server Settings (Admin >> General >> Proxy Server Settings).

In the GUI page that appears, enter the following details:

Tenant ID: Enter the Directory ID i.e., Your organization's ID with Azure AD.

Client ID: Enter the Client ID of the application.

Client Secret: This is the Secret Key created for Securden.

Step 2: Import Users

This step is to fetch the required users and groups from the AD domain specified.

This GUI offers the flexibility to fetch user groups from OUs/Groups in bulk and even specific users, in a single step. That means you can enter the names of the OU/Groups to be discovered in a single step. You can enter the discovery details in any combinations (OUs and Groups) as you wish.

To import OUs, select the OU tab

1. Enter the OU name and select **Discover.**
2. You can also browse from the OU tree by clicking on the **Browse OU Tree and Select** option. You can select one or multiple OUs and select **Add.**
3. You can then verify your selection in the **Verify the Objects Selected for Discovery.**
4. You can then select the role for the OUs imported using the **Role in Securden dropdown.**
5. Before selecting the import button, you can look into the additional settings which are explained below.
6. Select **Import**.

To import Groups, select the Groups tab

1. Enter the Group name and select **Discover.**
2. You can also browse from the OU tree by clicking on the **Browse Groups and Select** option. You can select one or multiple OUs and select **Add.**
3. You can then verify your selection in the **Verify the Objects Selected for Discovery.**
4. You can then select the role for the OUs imported using the **Role in Securden** dropdown.
5. Before selecting the import button, you can look into the additional settings which are explained below.
6. Select **Import.**

Advanced Settings:

This option allows you to either include domain users of all subgroups to the group being imported or ignore the subgroups and import only the users of the first level group.

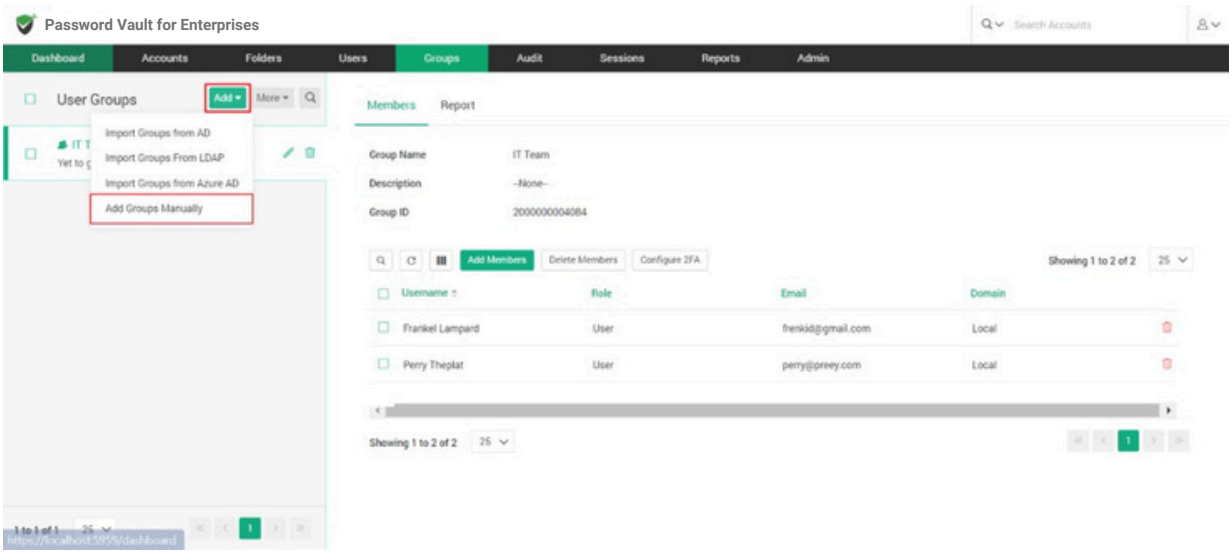
***User Groups to Import*:** You can import all or specific user groups to import, depending on your requirements. You can type in the names in the respective text fields in comma separated form.

***Configure Synchronization*:** Securden also allows Periodic Synchronization with AD. After you import the required user groups, you can configure periodic synchronization with AD. This helps you import the groups automatically. Click **Save** to save the domain details.

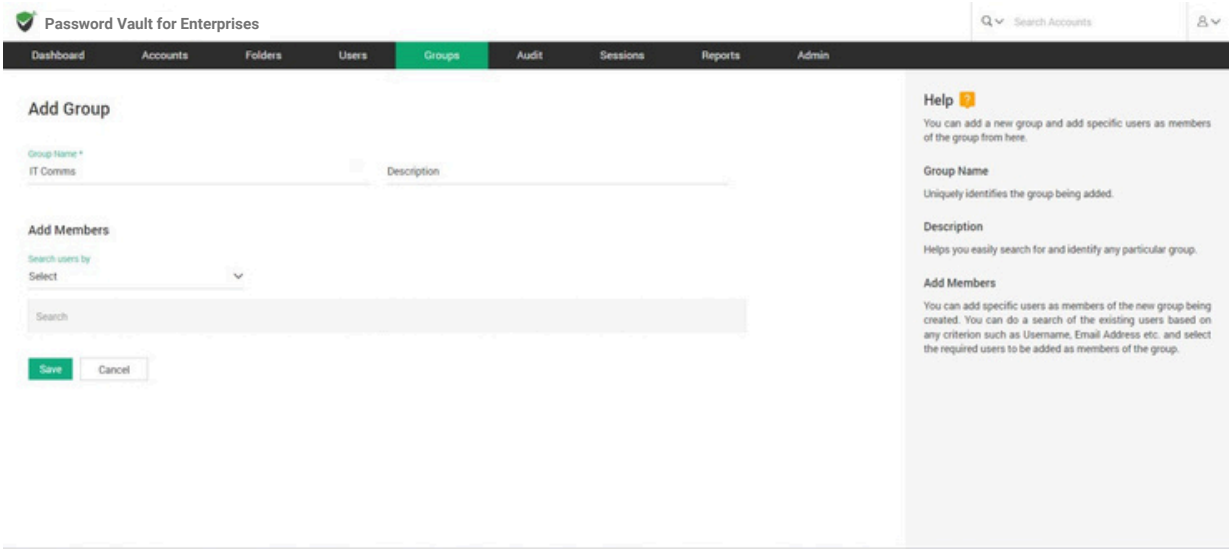
Add User Groups Manually

If you are not integrated with Active Directory or Azure AD, you can manually import user groups into Securden by following the steps given below.

To add user groups manually, navigate to **Groups >> Add >> Add Groups Manually**. You can add a new group and add specific users as members of the group from here.



In the GUI that opens, you have to provide the following details to create a new user group:

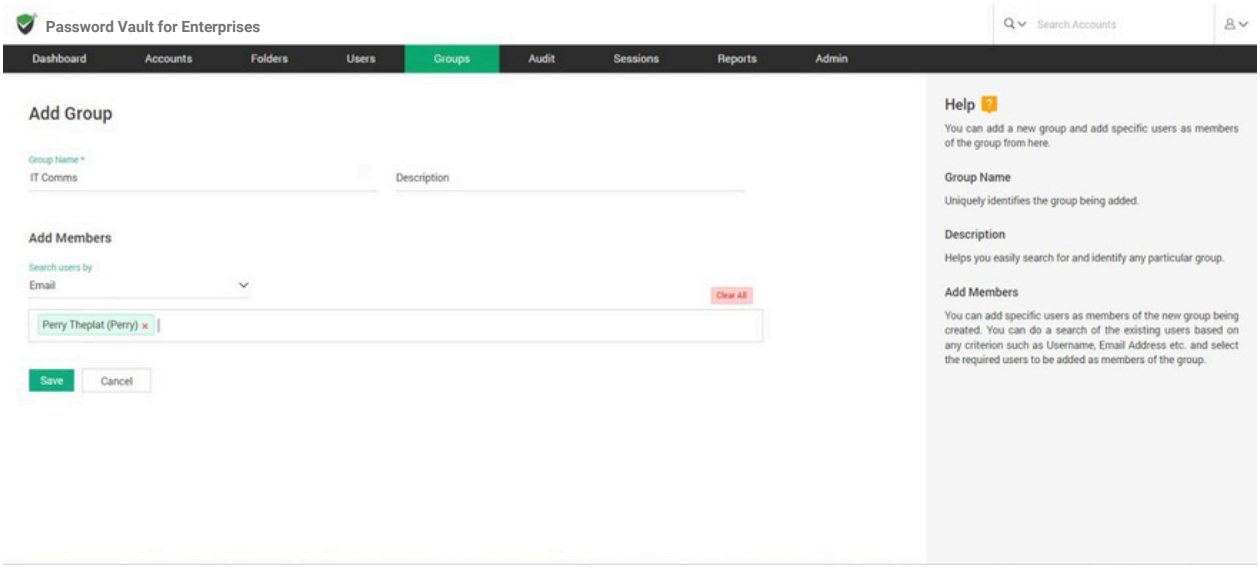


Group Name: Uniquely identifies the group being added.

Description: Helps you easily search for and identify any particular group.

Add Members: You can add specific users as members of the new group being created.

You can do a search of the existing users based on any criterion such as Username, Email, Role Name, etc., and select the required users to be added as members of the group.



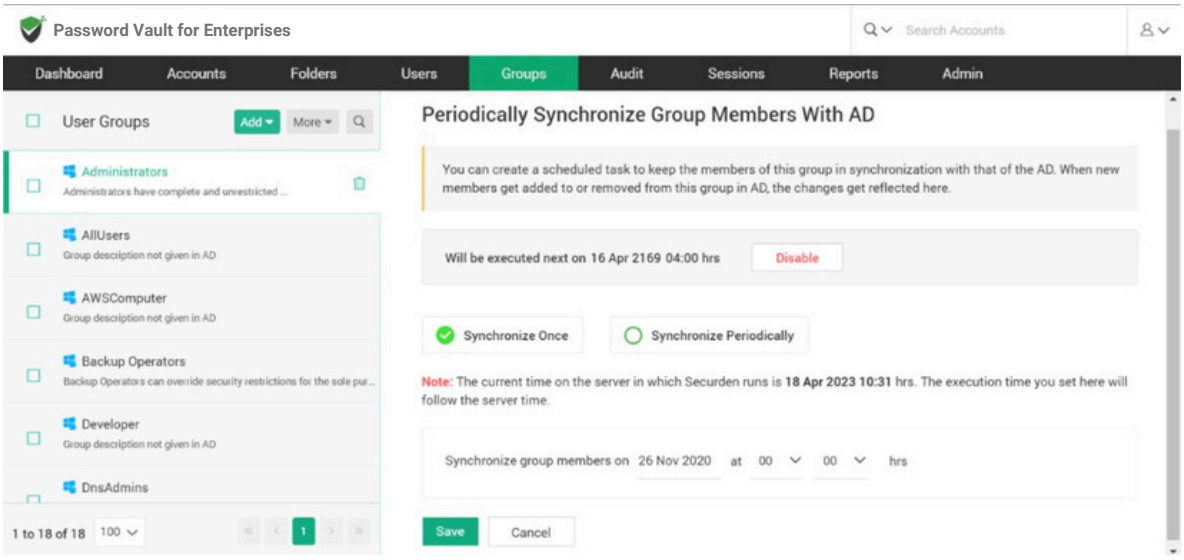
After providing these details, click on **Save** to create the user group.

Configure Periodic Synchronization of Groups

You can keep the members of this group in synchronization with that of the AD. When new members get added to or removed from this group in AD, the changes get reflected here without requiring any manual intervention on your part.

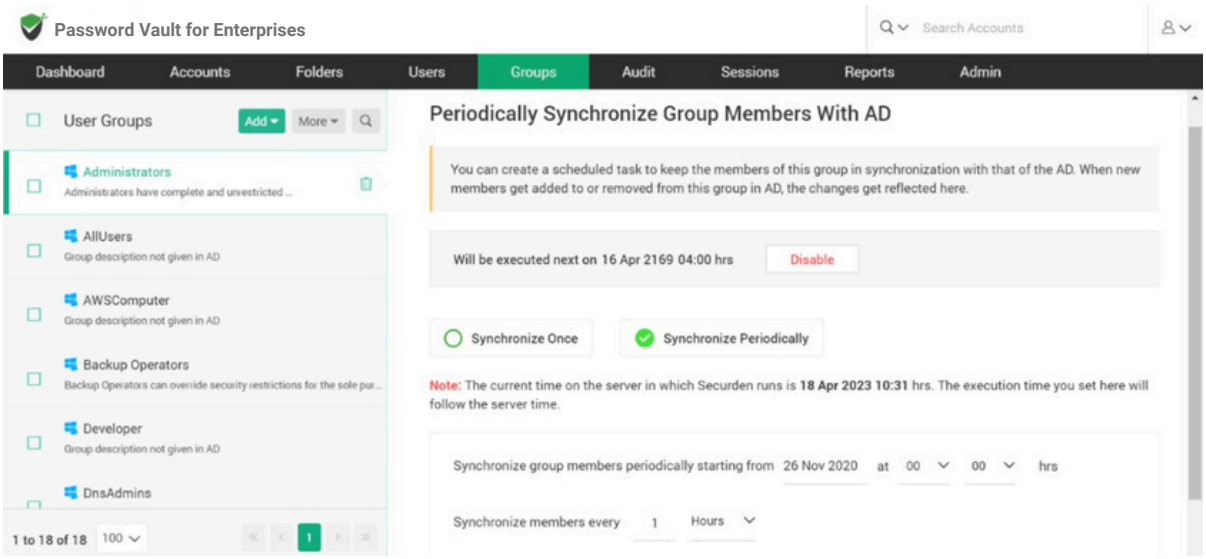
Navigate to **Groups >> Select the required group >> Members >> Schedule Sync** section in the GUI to perform this step.

You can either schedule the synchronization activity for a one-time run or create scheduled tasks to run periodically and ensure regular synchronization.



For periodic synchronization, you can choose the start time, and set the synchronization interval of your choice.

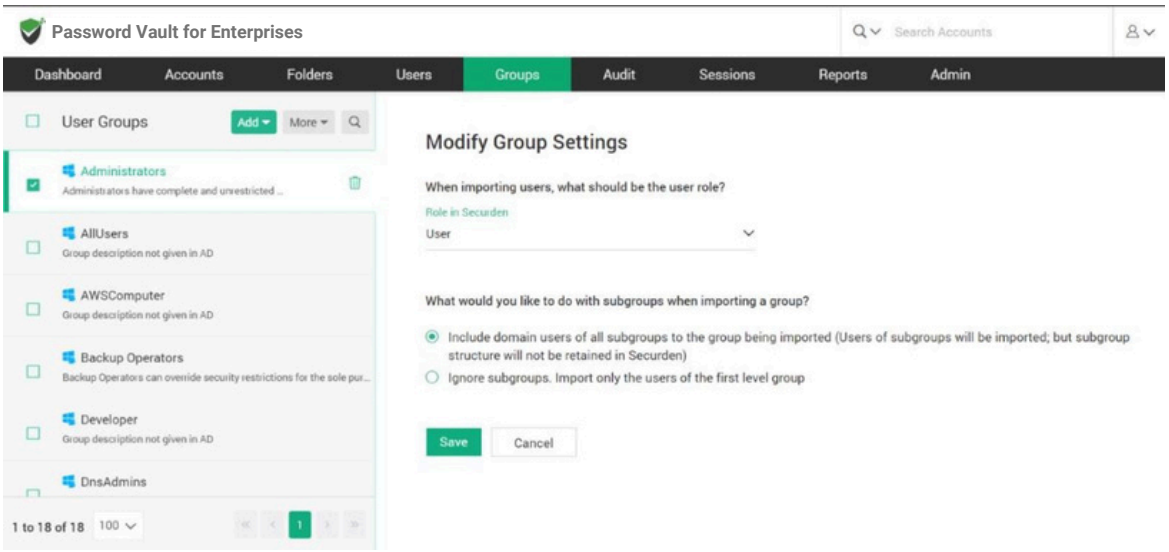
Once enabled, you can navigate to the **Schedule Sync** section as earlier to view the next planned schedule.



Group Settings

This option allows you to assign a role to the user groups being imported into Securden. This can be done by selecting a role under **Role in Securden**.

You also have the option to choose how the subgroups are to be assigned while importing. This means you can either choose to import domain groups of all subgroups or ignore them.



Explore Single Sign-On Options

Securden leverages SAML 2.0 to seamlessly integrate with SAML-compatible federated identity management solutions like Okta, G Suite, Microsoft ADFS, OneLogin, PingIdentity, Azure AD SSO, and others for Single Sign On.

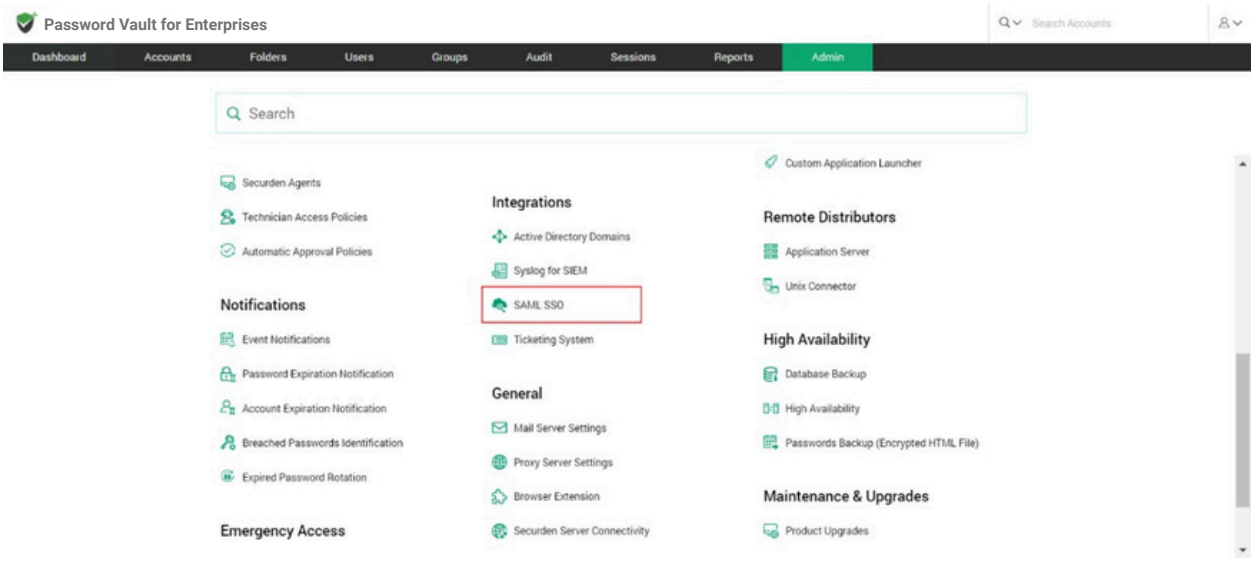
Securden serves as the SAML Service Provider (SP), and it integrates with SAML Identity Providers (IdP). Once this is done, users who log in to solutions like Okta (IdP) will be automatically logged in to Securden. The IdP and Securden exchange validation details are in the background.

Securden integrates with any SAML-based SSO solution. The integration process involves three steps:

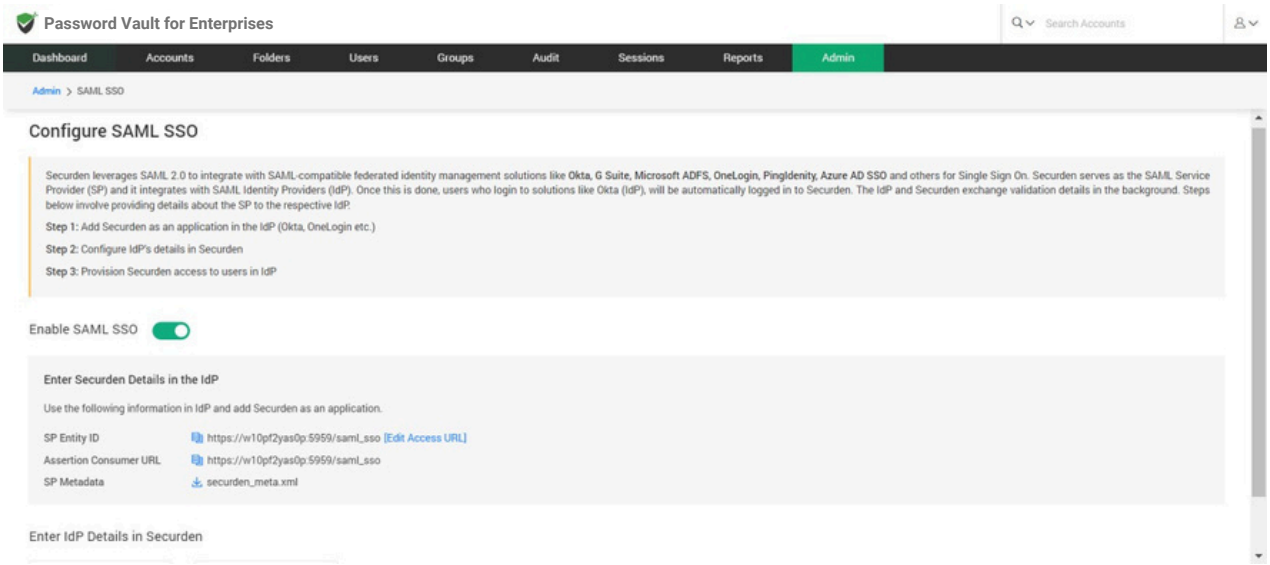
- Step 1: Add Securden as an application in the IdP (Okta, OneLogin, etc).
- Step 2: Configure IdP's details in Securden.
- Step 3: Provision access to Securden for your users in the IdP.

To start the integration, you would require certain details about Securden, which you can obtain from the product interface as explained below:

To configure SSO in Securden, navigate to **Admin >> Integrations >> SAML SSO.**



In the GUI that opens, **Enable SAML SSO** by setting the toggle to green



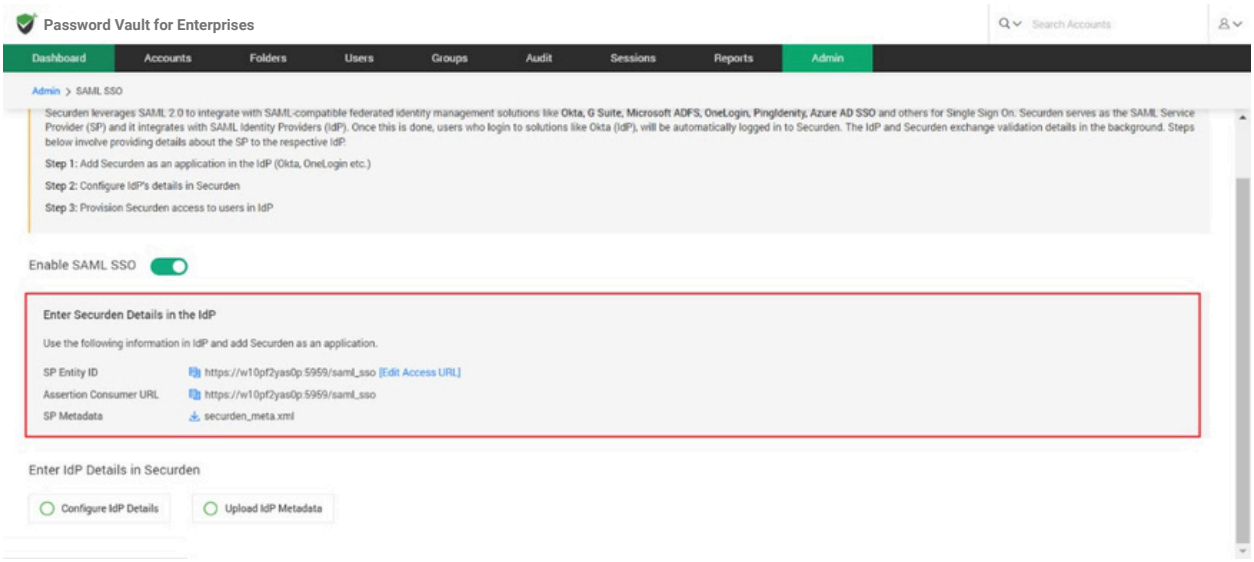
Step 1: Add Securden as an application in your SSO solution (known as the IdP).

You need to perform this step on your SSO solution.

For adding Securden as an application, you would typically require the following details. Securden is referred to as the ‘Service Provider’.

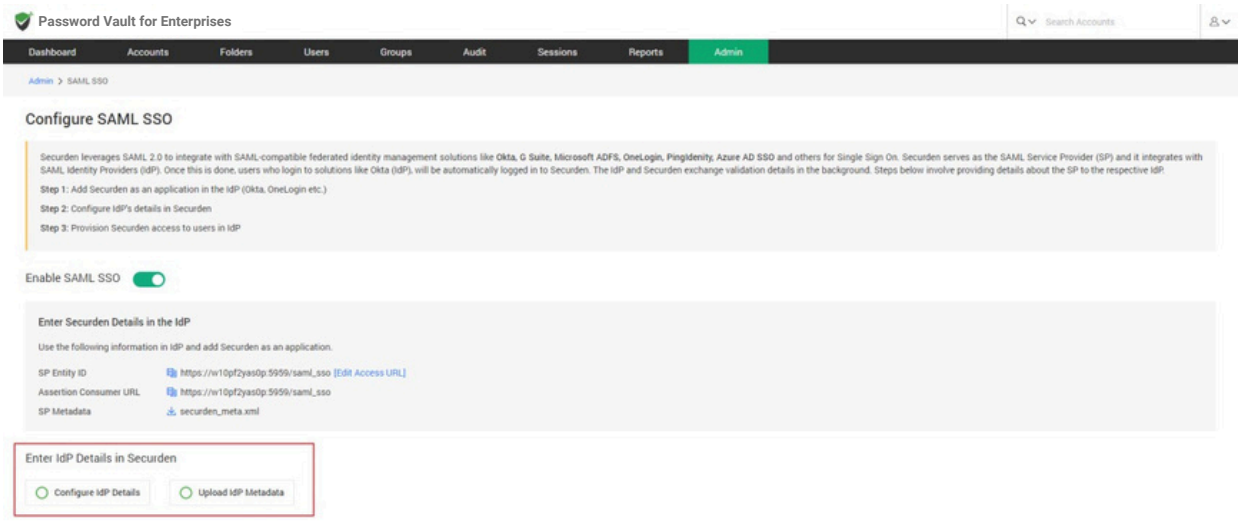
- Service Provider Entity ID
- Assertion Consumer URL
- Service Provider Metadata

All these details are available in the **Configure SAML SSO** page as shown below. You may readily copy this information using the icon provided beside each detail.



Step 2: Configure IdP's details in Securden

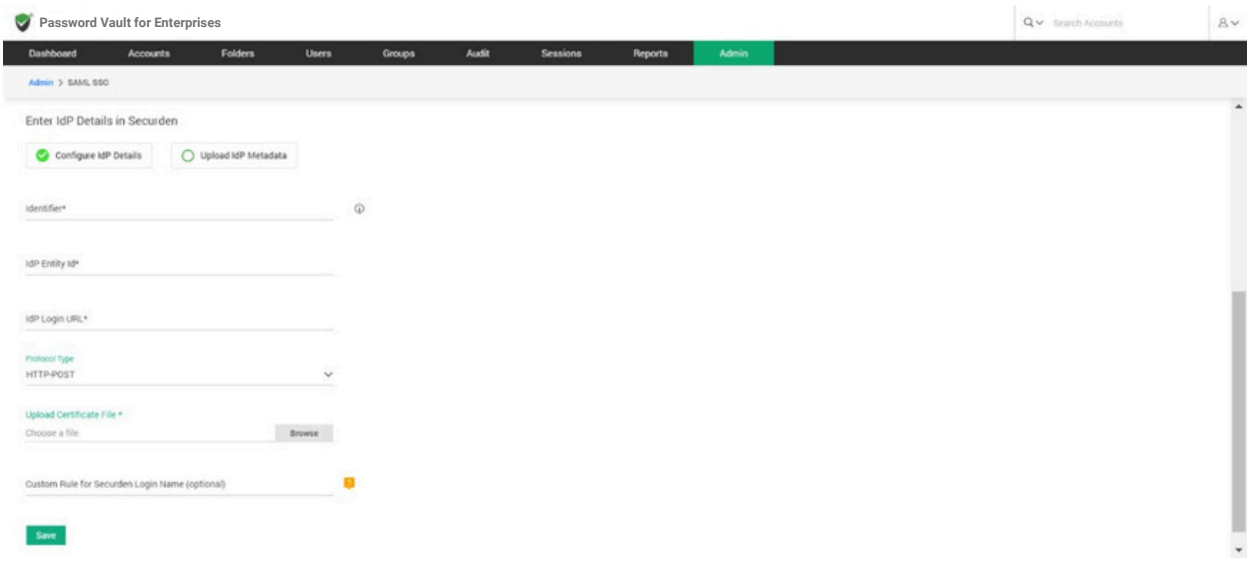
Once you have completed step 1 and added Securden as an application in your SSO solution, you would have certain details obtained from the IdP like IdP Entity ID, IdP login URL, and protocol type.



You have two options here from which you can select one that is best suited for you.

- Configure IdP Details (or)
- Upload IdP's Metadata file

If you select the option **Configure IdP Details**, enter the IdP details that you get once you complete step 1.



You need to enter the following information: **Identifier** – Enter an Identifier text that will appear on the Securden login screen to display the SSO option.

IdP Entity ID – You need to fetch the Entity ID from your IdP provider and enter it here.

IdP Login URL - Enter the URL used to login into your IdP portal. **PROTOCOL TYPE –** Select the type of protocol to use from the two available options.

- **HTTP-POST –** Select this if you wish to send data to the server.
- **HTTP-Redirect –** Select this if you want the server to redirect the response to your request.

Upload Certificate file – You can attach the certificate file that you have for your IdP.

Custom rule for Securden login - As part of the integration, one of the important aspects is the ‘login name’ format. The Identity Provider returns a login name, which Securden uses as the username for logging in to the application. If you want to map the name returned by the identity provider with a different name, you can create custom rules. Basically, you can make use of the following string functions to create custom rules to manipulate the login name returned by the identity provider. In the string function, login name denotes the name returned by the identity provider.

Step 3: Provision access to Securden for your users in the IdP

After completing the integration, remember to provision access to Securden to your users in the IdP.

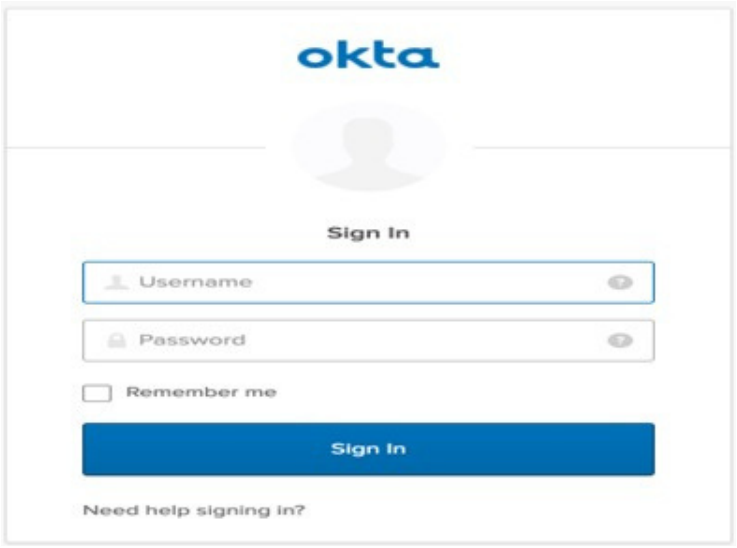
Configure Single Sign-On

The steps to configure Single sign on for various SSO providers have been elaborated below.

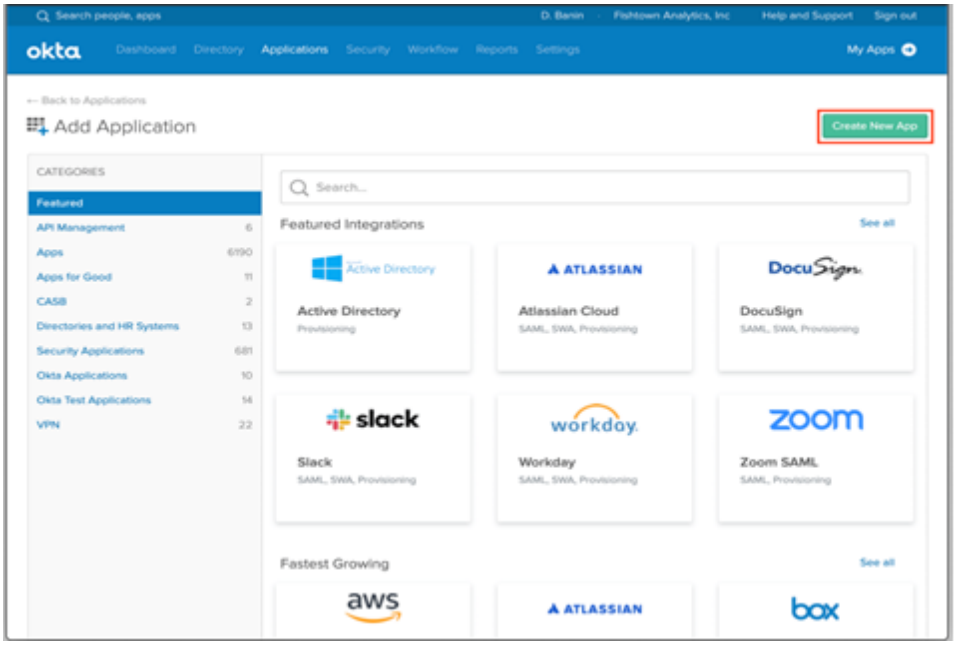
Configure Single Sign-On for Okta

To integrate Okta with Securden, you need to follow these steps:

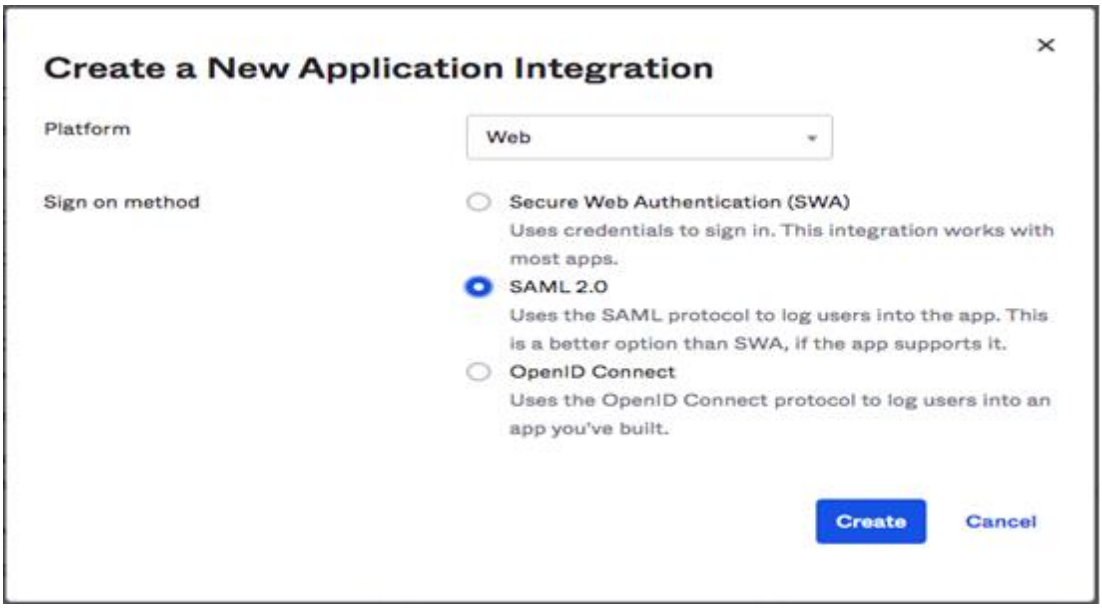
1. Log in to your Okta account using your admin credentials.



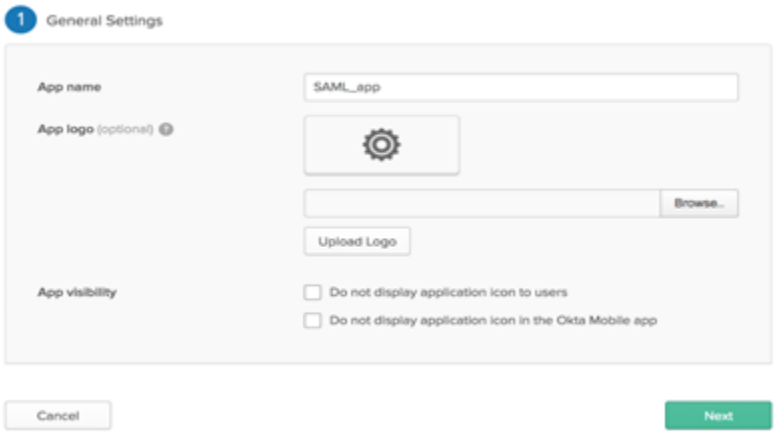
2. Navigate to **Applications >> Add Applications >> Create New App**.



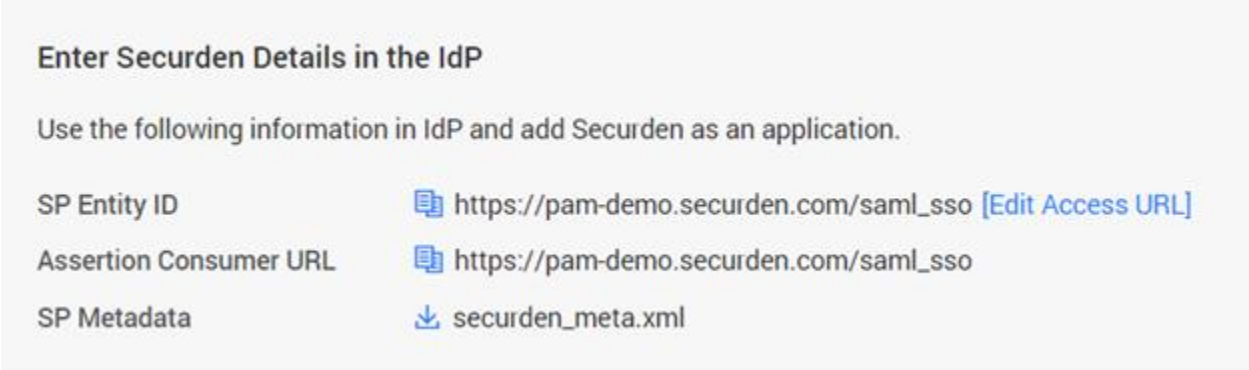
3. In the pop-up window, choose **SAML 2.0** as your sign-on method and click **Create**.



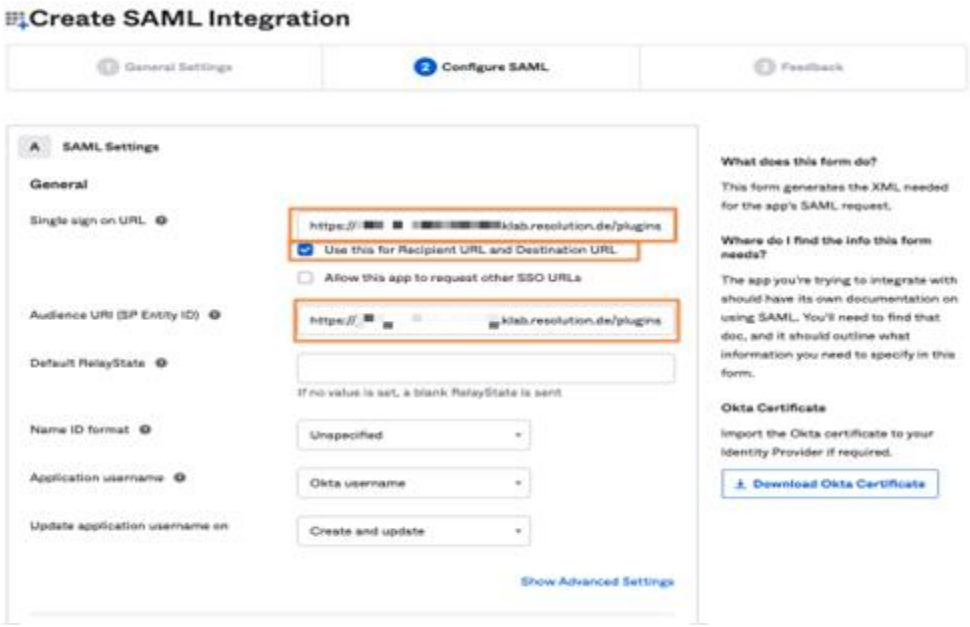
4. In the **Create SAML Integration** window, enter the application name, and if you want, you can add the application logo as well. Then, click on **Next**.



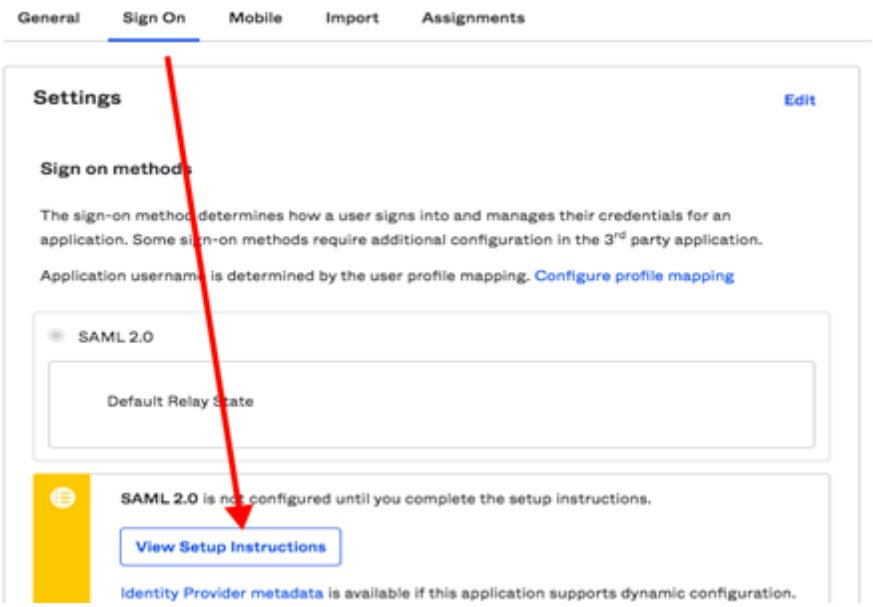
5. Here, you need to provide the Service Provider's, a.k.a. Securden's details for which you have to navigate to **Admin >> Integrations >> SAML SSO**. Use the provided details to integrate Securden with Okta.



6. Navigate to the Okta SAML settings page. Enter the Securden Service Provider details in Okta's **Configure SAML** settings page.



7. If you have used AD to import users, choose the **Custom** option for **Name ID Format**. Specify the following custom format: toUpperCase(substringBefore(substringAfter(user.email, "@"), ".")) + "\" + substringBefore(user.email, "@").
8. If you did not use AD for user import, you can choose the **Okta Username Prefix** option.
9. Click on the **Finish** button to complete the SAML creation process. Navigate to the **Sign On** tab and click on **View Setup Instructions** button.



10. Navigate to **Securden >> Admin >> Integrations >> SAML SSO**.

11. Click on the **Configure IdP Details** option to display the IdP options. Here, you need to enter details of your SAML IdP. You can add the details manually or choose to import them from the IdP Metadata file.

Configure Single Sign-On for Azure AD

To integrate Securden Login with Azure AD, you need to carry out the following steps:

1. Log in to your Microsoft Azure portal.
2. Click on the **App Registrations** from the left pane under **Manage**.
3. Click on the **+ New Registration** button on the top bar.
4. The registration page will load. Here, you need to provide the following information:

Name: Enter Securden Vault, or a name of your choice.

Choose supported account types - Accounts in this organizational directory only - Single tenant. Enter the Securden's Redirect URI.

5. Click on the **Register** button to complete the addition of Securden Vault

6. The newly registered Securden Vault's application will open up. Click on **Authentication** under **Manage** in the left pane. In the **Authentication** page, under **Advanced Settings,** enable **Allow Public Client Flows** by clicking on the **Yes** button.

7. Click on **API Permissions** under **Manage** in the left pane. In the **API Permissions** page, click on the **+Add a Permission** button.

8. A **Request API Permissions** window will pop up. Here, choose **Azure AD Directory Graph** under **Supported Legacy APIs**.

9. Click on **Delegated Permissions** and search for "read" in the **Select Permissions** search bar to populate relevant permissions. Select the

options Directory.Read.All, User.Read and click Add Permissions.

10. Now, click the **Grant Admin Consent** button under **Grant Consent**.

11. In the pop up that opens, click **Yes** to grant consent for the requested permissions.

12. You can now navigate to Securden Vault's interface to start importing users, after Securden Vault is registered with the relevant permissions in Azure AD.

Troubleshooting Tips

Issue:

"User not present" error while configuring Azure AD SSO integration.

Solution:

During authentication, we validate the value returned by the identity provider against the login name in Securden. When you import users from Azure AD, Securden checks the username as DomainName\loginname.

For this, you can change the custom rule for Securden login name in the SSO configuration page under "Admin>>SAML SSO>>Edit"

stringAppend('DOMAINNAME\', loginname)

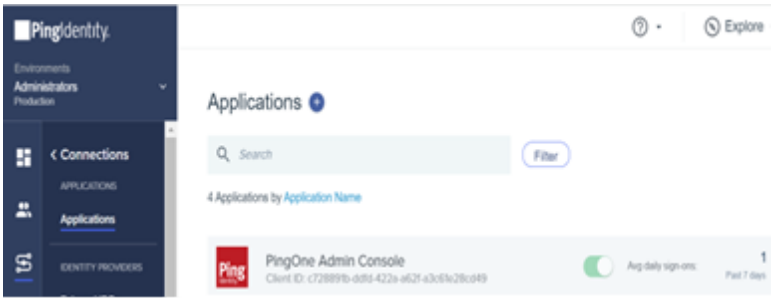
Example: stringAppend('SECURDENDEV\', loginname)

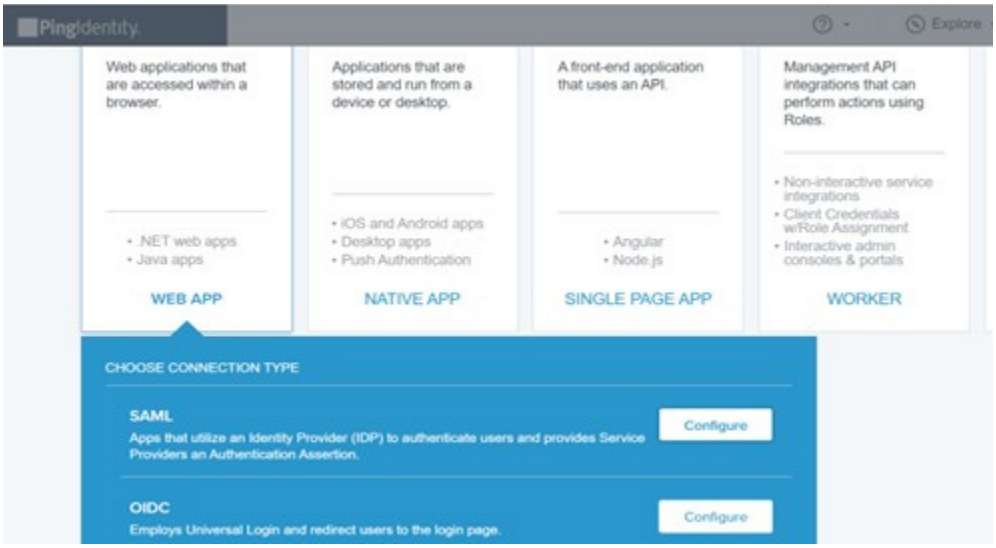
If an email is received from Identity Provider, the login name has to be stripped from the value:

stringAppend('DOMAINNAME\', substringBefore(loginname, '@')) For extracting username from email: substringBefore(loginname, '@')

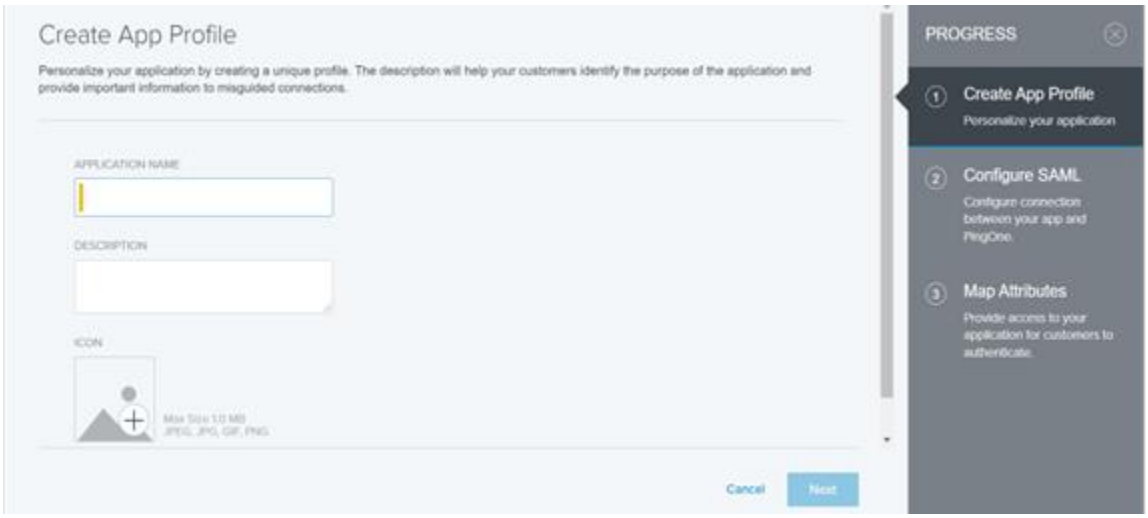
Configure Single Sign-On for Ping Identity

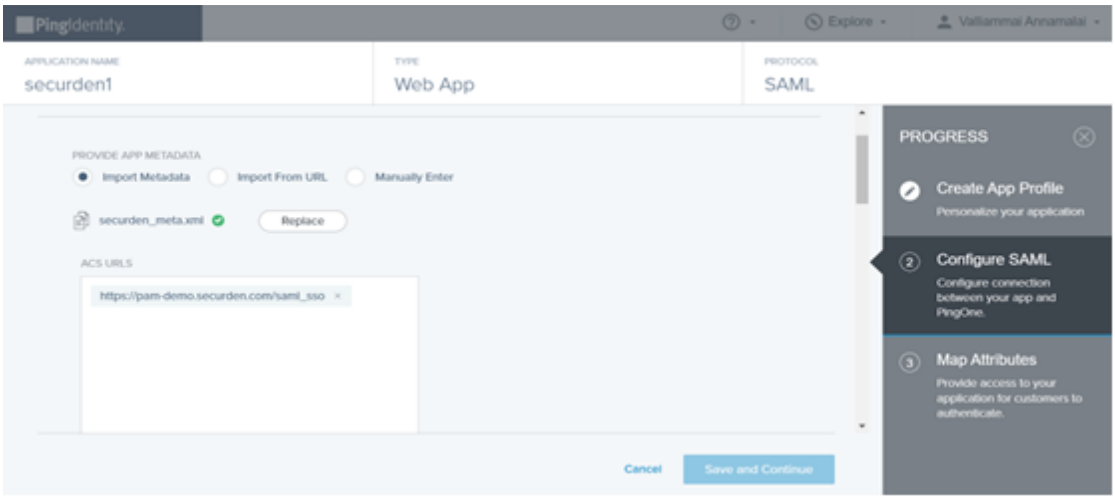
1. Login to your Ping Identity account.
2. Navigate to **Connections >> Applications +** and then click **Web App >> SAML.**



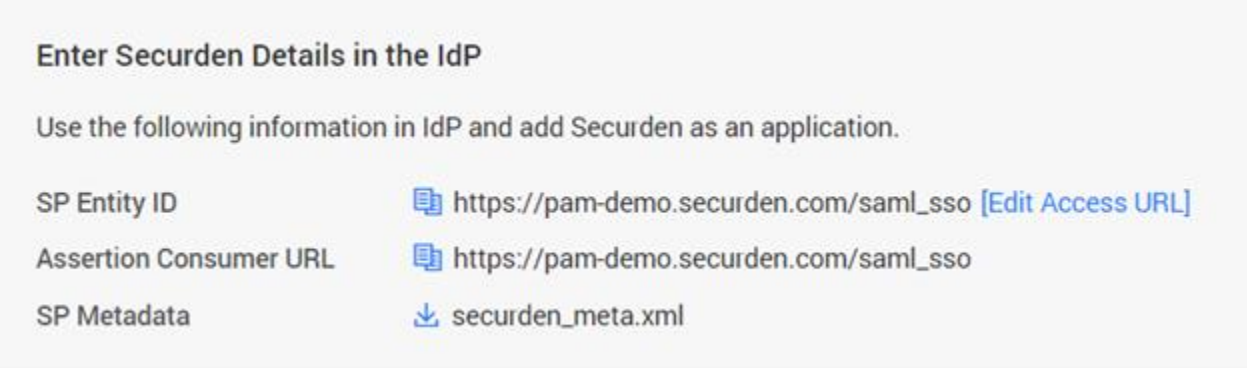


3. Create an App profile by personalizing your application with its name, description, and icon (optional). Then click on **Next.**





4. To configure connection between Securden and PingOne, you need to provide the Service Provider's, a.k.a. Securden's, details for which you have to navigate to **Admin >> Integrations >> SAML SSO**.

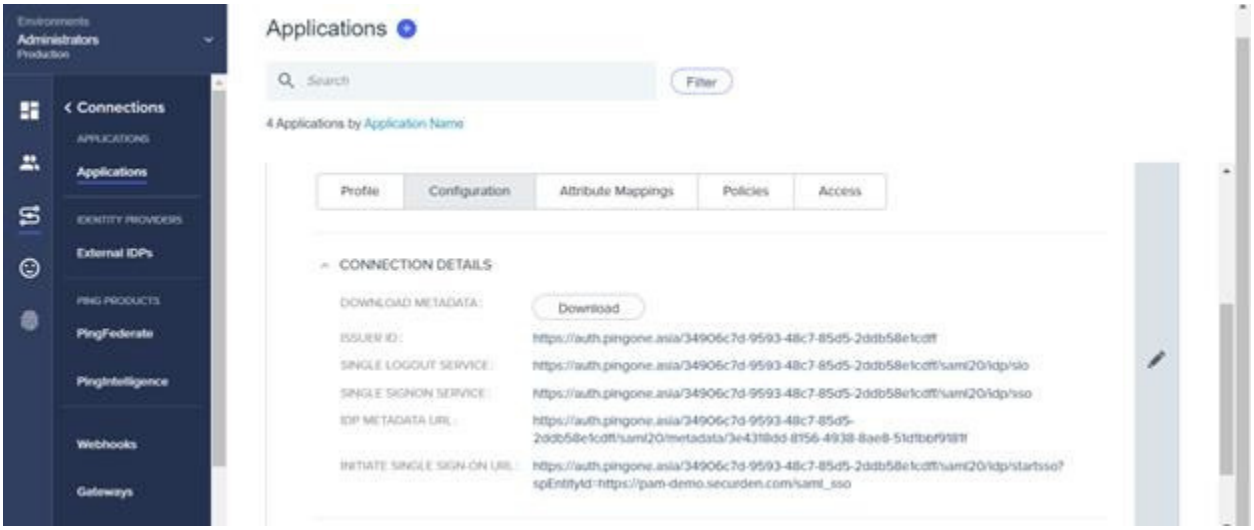


Use the provided details to integrate Securden with Ping Identity.

5. Map attributes to provide access to your application for customers to authenticate.

6. Click on the **Finish** button to complete the SAML creation process.

7. Navigate to **Applications >> Securden >> Configuration** and download metadata or copy the respective Issuer ID (Entity Id) and IDP metadata URL (Login URL).



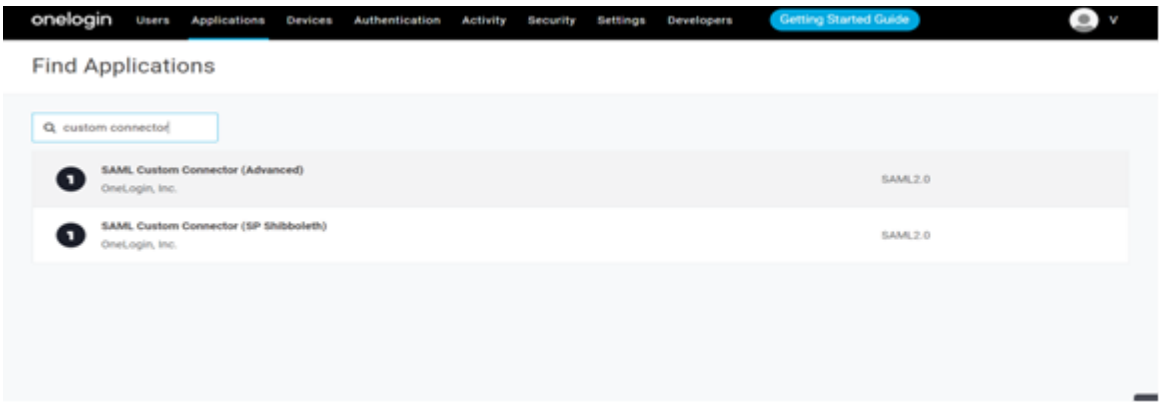
8. Navigate to **Securden >> Admin >> Integrations >> SAML SSO**.
   Click on the **Configure IdP Details** option to display the IdP options.

Here, you need to enter details of your SAML IdP. You can add the details manually or choose to import them from the IdP Metadata file.

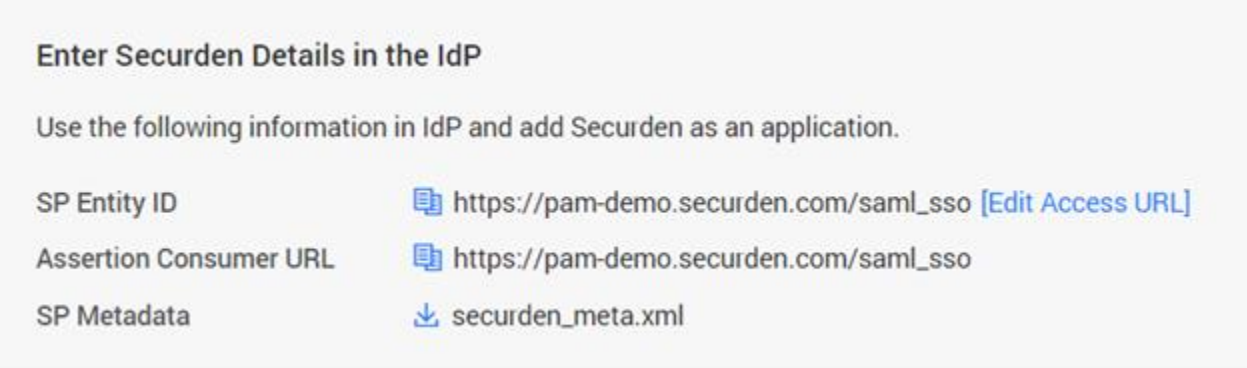
9. Click the **Save** button to complete the setup.
10. Navigate to Ping Identity, **Applications >> Securden >> Access** and follow the instructions in the GUI to assign Securden to your users. Select the required users and assign them the application.

Configure Single Sign-On for One Login

1. Navigate to **Applications >> Applications >> Add Apps** in the OneLogin administrator dashboard.

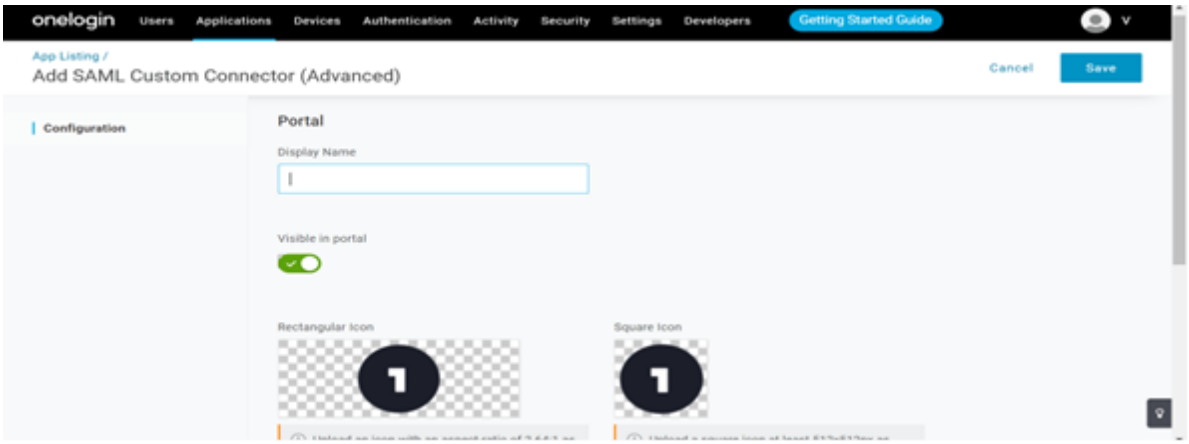


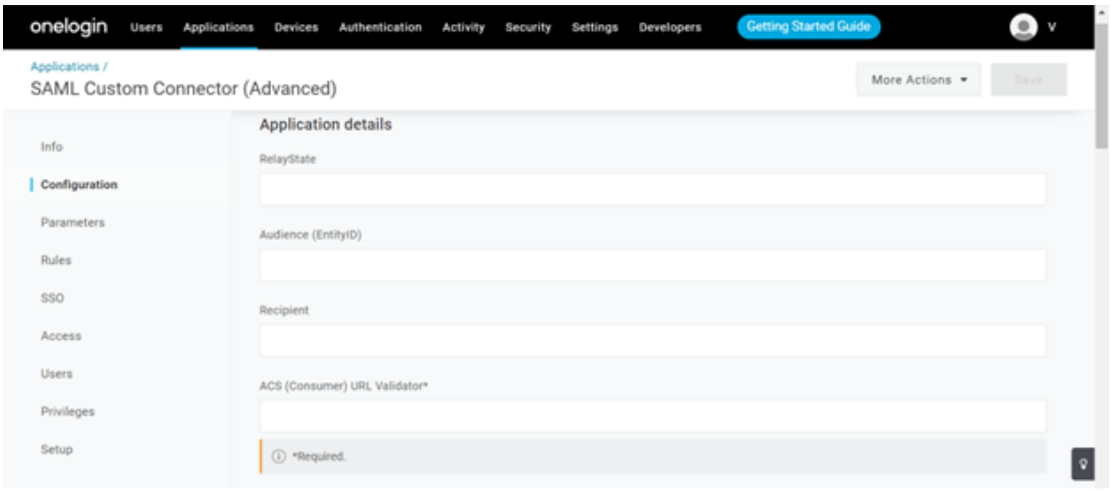
2. Search for **SAML Custom Connector (Advanced)** and select the first result from the search results.
3. Navigate to **Configurations** tab here, you need to provide the Service Provider's, a.k.a. Securden's details for which you have to navigate to **Admin >> Integrations >> SAML SSO**.

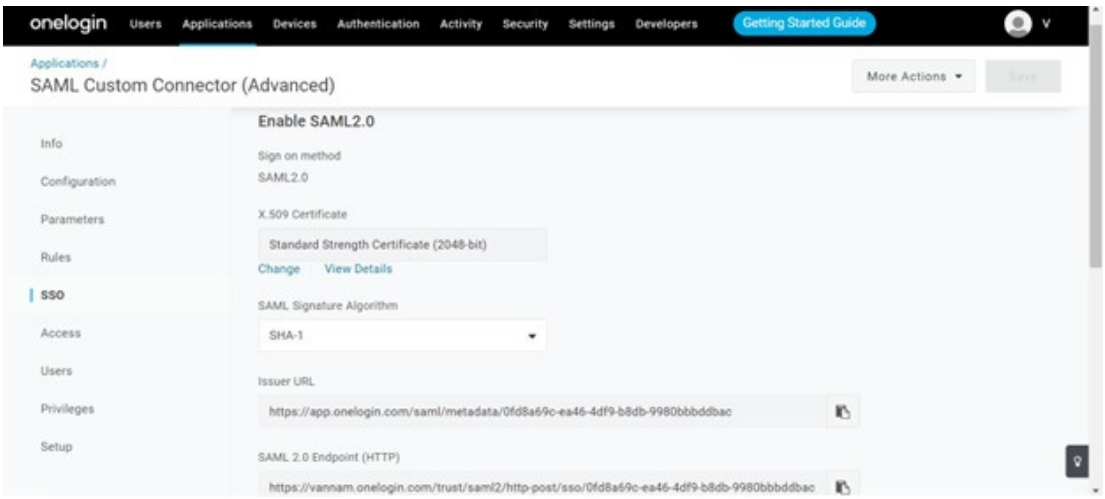


Use the provided details to integrate Securden with One Login.

4. Navigate to the **One Login Configurations** page. Enter the Securden Service Provider details in the configurations page.







5. Click on the **Save** button to complete the SAML creation process and navigate to **Securden >> Admin >> Integrations >> SAML SSO**.
6. Toggle the **Enable SAML SSO** switch on
   Click on the **Configure IdP Details** option to display the IdP options.
   Here, you need to enter details of your SAML IdP. You can add the details manually or choose to import them from the IdP Metadata file.
8. Click the **Save** button to complete the setup.

9. You can now assign Securden to your users. Navigate to **Applications >> SAML Custom Connector (Advanced) >> Users**. Select the required users and assign them the application.

Configure Single Sign-On for G-Suite

To integrate G-Suite with Securden, you need to follow these steps:

1. You need to possess a super administrator account to proceed further and open the Google Admin console.
2. From the Admin console Home page, go to **Apps >> Web and Mobile Apps**.
3. Click **Add App >> Add Custom SAML** app.
4. On the **App Details** page:
    a. Enter the name of the custom app (here Securden).
    b. (Optional) Upload an **app icon**. The app icon appears on the web and mobile apps list, the app settings page, and the app launcher. If you don't upload an icon, an icon is created using the first two letters of the app name.
5. Click **Continue**.
6. On the **Google Identity Provider** details page, get the setup information needed by the service provider using one of these options:
    a. Download the **IDP metadata**.
    b. Copy the **SSO URL** and **Entity ID** and download the **Certificate** (or SHA-256 fingerprint, if needed).
7. (Optional) In a separate browser tab or window, sign in to your service provider and enter the information you copied in Step 4 into the appropriate SSO configuration page, then return to the Admin console.
8. Click **Continue**.

9. In the **Service Provider Details** window, enter an **ACS URL, Entity ID, and Start URL** (if needed) for your custom app. These values are all provided by the service provider. **Note**: The ACS URL has to start with https://
10. The default **Name ID** is the primary email. Multi-value input is not supported.
11. Click **Continue**.
12. Under **Google Directory Attributes**, click the **Select Field** menu to choose a field name. Then, enter the corresponding attribute for your custom SAML app under **App Attributes**.
13. Click **Finish.**

Turn on your SAML App

1. Click **User Access**.
2. To turn on or off a service for everyone in your organization, click **On** for everyone or **Off** for everyone, and then click **Save**.
3. (Optional) To turn a service on or off for an organizational unit:
    - At the left, select the organizational unit.
    - Select On or Off.
    - Click **Override** to keep your setting if the service for the parent organizational unit is changed.
    - If Overridden is already set for the organizational unit, choose an option:

        Inherit—Reverts to the same setting as its parent.

        Save—Saves your new setting (even if the parent setting changes).
4. To turn on a service for a set of users across or within organizational units, select an access group.

5. Ensure that the email addresses your users use to sign in to the SAML app match the email addresses they use to sign in to your Google domain.

Configure Single Sign-On for Microsoft ADFS

Before configuring ADFS

- Register your Windows Server as a member of the existing domain.
- Log in to the ADFS server as a domain administrator.
- Ensure that the ADFS server has a valid certificate meant for it (ADFS).

Step 1: Install the ADFS role

1. Open Server **Manager >> Manage >> Add Roles and Features**. The **Add Roles and Features** wizard is launched.
2. On the **Before You Begin** page, click **Next.**
3. On the **Select Installation Type** page, select role-based or feature-based installation, and then click **Next.**
4. On the **Select Destination Server** page, click **Select a Server from the Server Pool** and click **Next**.
5. On the **Select Server Roles** page, select **Active Directory Federation Services** and click **Next**.
6. On the confirmation page, click **Install**. The wizard displays the installation progress.
7. Wait until the installation gets completed.

Step 2: Configure the Federation Server

1. Once the ADFS role is installed, click **Configure the federation service on this server** link.
2. On the **Welcome** page, select **Create the first federation server in a federation server farm** and click **Next**.
3. On the **Connect to Active Directory Domain Services** page, specify an account with domain administrator rights for the Active Directory domain that this system is connected to, and then click **Next**.
4. On the **Specify Service Properties** page, enter the following details before clicking **Next**:

a. Select the SSL certificate. The Federation Service Name will be automatically populated.

b. Enter a display name for **Federation Service Display Name**.

5. On the **Specify Service Account** page, select **Use an existing domain user account or Group Managed Service Account** and click **Next**.
6. On the **Specify Configuration Database** page, select **Create a database on this server using Windows Internal Database** and click **Next**.
7. On the **Pre-requisite Checks** page, verify if all prerequisite checks have been successfully completed and then click **Configure**.
8. Review the results and check whether the configuration has been completed successfully on the **Results** page.

Step 3: Configure ADFS to integrate with Securden

1. Open Server **Manager >> Tools >> ADFS Management**. The ADFS wizard is launched.
2. Expand to "**Relying Party Trusts**" and click "**Add Relying Party Trust".**
3. On the “**Add Relying Party Trusts**” wizard, click **Start.**
4. Launch Securden web interface (https://<Securden-Server- Hostname>:5454/), navigate to **Admin >> Integrations >> SAML SSO** and download the metadata file **- securden_metadata.xml.**
5. Go back to "**Add Relying Party Trusts**” Wizard. Under “**Select Data Source**”, select "**Import data about the relying party from a file**". Browse and select the "**securden_metadata.xml**", which you downloaded from Securden and click "**Next**".
6. In the “**Specify Display Name**” field, enter "**Securden**" and then click "**Next**" .
7. Choose "**I don't want to configure multifactor authentication settings for this relying party trust at this time**" and then click "**Next**".
8. Choose **Permit all users to access this relying party**.
9. Keep clicking **Next** until you reach the **Finish** screen.
10. Choose to open the **Edit Claim Rules dialog** before clicking Finish. This will launch the **Edit Claim Rules** window.
11. On the **Issuance Transform Rules** tab, click **Add Rule**.
12. Under **Select Rule Template**, set **Transform an incoming claim** as the rule template and click **Next**.
13. Choose **Windows account name** in **Incoming Claim Type** and **Name ID** in **Outgoing Claim Type** and then click Finish. Apply the claim rules in **Issuance Transform Rules** tab.
14. Navigate to **Endpoints**, and then to **MetaData Group**. Select the entry with type **Federation MetaData**.

15. Open a web browser and access the following URL path as in the entry "https://<ADFS-Server-Name>/<URL-Path>"

Example: (https://SEC-2K12.SECURDEN.LOCAL/FederationMetaData/2007-06/FederationMetaData.xml)

16. Launch Securden web client. Navigate to **Admin >> Integrations >> SAML SSO**. Enable **SAML SSO** and then upload the federation metadata.

Troubleshooting Tips:

Question / Issue - I have integrated with a SAML-compatible federal identity management solution but got an invalid user response when SSO feature was used. How to resolve this issue? **Steps to follow:**

1. The username format could be the cause of this issue. For authentication, we validate the value against the **Username** in Securden.
2. When you import users from AD, Securden maintains the username as **DomainName\username**. (When you add users locally instead of importing from AD, it will be just the username alone).
3. So, on the SSO configuration page, if you change the **Custom Rule for Securden Login** as below, the issue might be resolved:

   stringAppend('**DOMAINNAME**', loginname)

4. **Example**: stringAppend('**SECURDENDEV**', loginname)

5. In addition, there might be an email mismatch with username.
    a. If an email is received from SSO, the domain name has to be trimmed from the value: stringAppend('DOMAINNAME\', substringBefore(loginname, '@'))
    b. For extracting username from email:

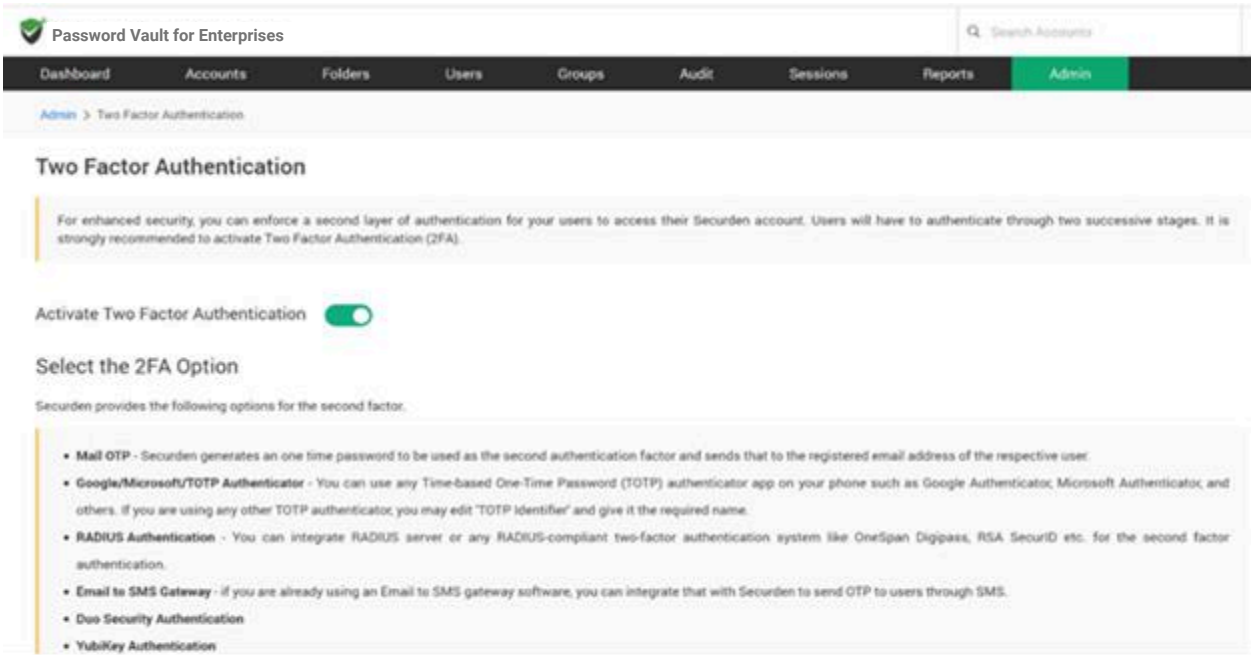
    substringBefore(loginname, '@')

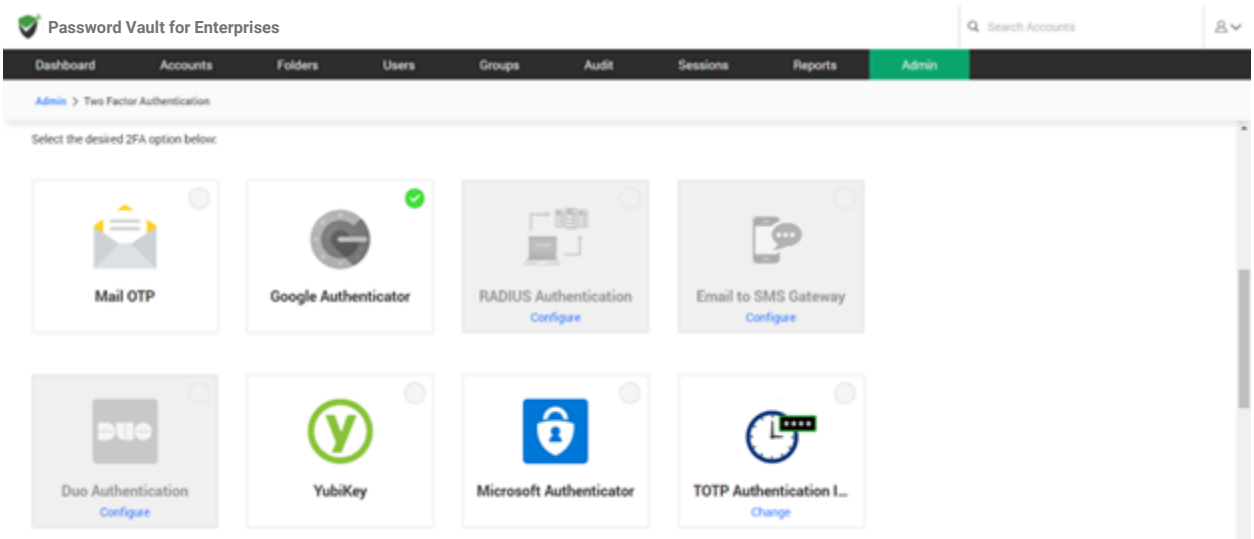
Section 4: Configuring Two Step Verification

Enforcing Two Factor Authentication (MFA)

For enhanced security, you can enforce the 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).

To Configure Two-Step Verification, Navigate to **Admin >> Authentication >> Two Factor Authentication** in the GUI to perform this step.





At present, Securden supports:

● **Mail OTP** - Securden generates a one-time password to be used as the second authentication factor and sends that to the registered email address of the respective user.

● **Google/Microsoft/TOTP Authenticator** - You can use any Time-based One-Time Password (TOTP) authenticator app on your phones such as Google Authenticator, Microsoft Authenticator, and others. If you are using any other TOTP authenticator, you may edit the '**TOTP Identifier**' and give it the required name.

● **RADIUS Authentication** - 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.

● **Email to SMS Gateway** - If you are already using an Email to SMS gateway software, you can integrate that with Securden to send OTP to users through SMS.

● **Duo Security Authentication –** If you have enrolled in Duo Security, you can easily integrate that with Securden and make use of the various authentication methods (security key, biometric authenticator, touch ID, web authentication, and more).

● **YubiKey Authentication –** You can also make use of a YubiKey as a second-factor authentication, which generates one-time passwords upon integration.

Mail OTP

In the case of Mail OTP 2FA, the user must first complete the first level of authentication, and then Securden will email a randomly generated password to the user. This password will only be available for the current session and will expire when the user logs out. The user has to enter the password to authenticate the second level and then they will have access to the Securden Vaultapplication.

To configure Mail OTP for 2FA:

1. Navigate to **Admin >> Authentication >> Two-Factor Authentication**
2. Select **Mail OTP** as your option and click **Confirm**.

Google Authenticator / Microsoft Authenticator / TOTP Authenticator

Google Authenticator provides a six-digit code to authenticate the second level of access for authentication. Microsoft Authenticator and TOTP Authenticator work the same way.

Prerequisites:

You need to install the Google Authenticator/Microsoft Authenticator/TOTP Authenticator app on your mobile phone or tab.

The app generates a six-digit number every 30 seconds and you receive the code instantaneously with the app.

To use Google/Microsoft Authenticator as your 2FA method,

1. Navigate to **Admin>>Authentication >> Two-Factor Authentication.**
2. Choose the option **Google Authenticator/Microsoft Authenticator/TOTP Authenticator.**
3. Click **Confirm**.

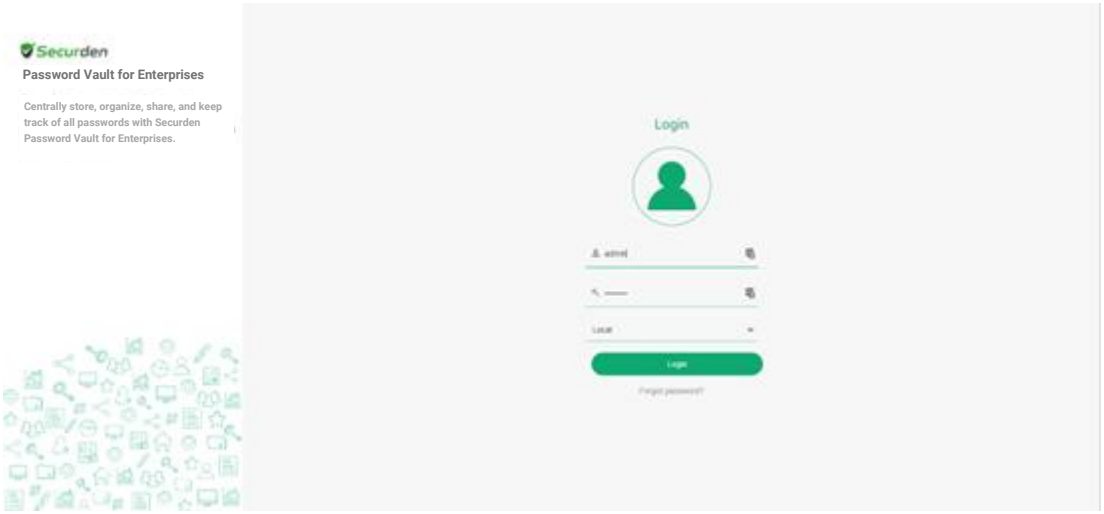
Yubikey

Yubico designed a physical authentication key called Yubikey, which can be integrated with Securden Password Vault for 2FA.

To integrate Yubikey with Securden,

1. Navigate to **Admin >> Authentication >> Two-Factor Authentication.**
    1. Click on **'Yubikey'.**
    2. Click **'Save'.**

4. To connect to Securden Vault after integrating it with Yubikey, you need to launch the Securden Vault's web interface first.



5. Enter your Securden credentials and complete the first level of authentication. Once it succeeds, you will be asked to enter the Yubikey OTP.

6. In the USB port of your computer, insert the Yubikey.
7. Before generating a one-time password, you need to decide which of the two slots, slot 1 or slot 2, of the YubiKey you're going to use for authentication throughout.

Slot 1: If you tap the YubiKey once, it generates a 44-character security key whose first 12 characters are unique to this slot. For every subsequent login through this slot, the first 12 characters remain the same and the rest of the 32 characters are randomized.

Slot 2: If you tap and hold the YubiKey for 2-5 seconds, it generates a 44-character security key whose first 12 characters are unique to this slot. For every subsequent login through this slot, the first 12 characters will remain the same and the rest of the 32 characters will be randomized.

8. Here is a sample output from a YubiKey where the button has been pressed three times.

- cccjgdwkdjkwjdkjwikjdkhhfgrtnnlgedjlftrbdeut
- cccjgjubuebduhubnjkedjkehijeiocjbnublfnrev
- cccjgjgkcbejnvchfkfhiiuunbtnvgihdfiktncvlhck

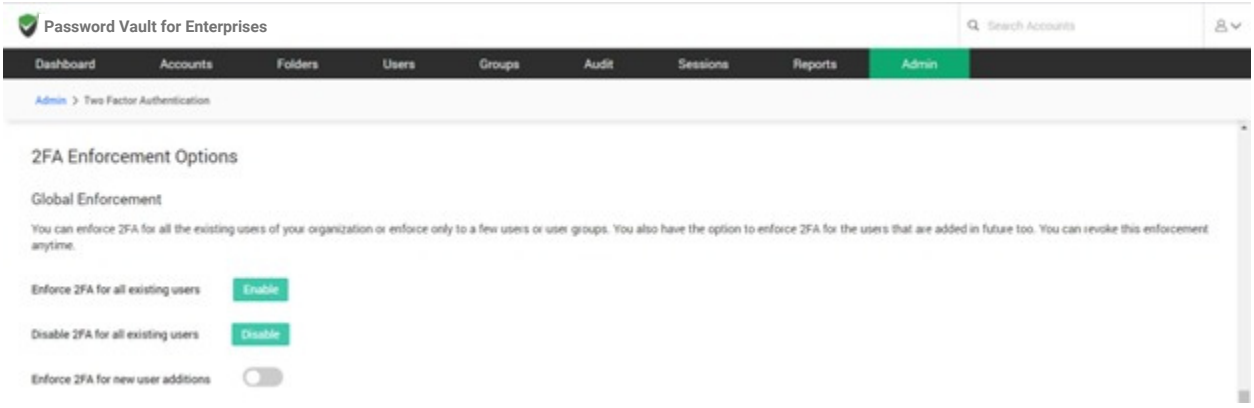
Note: By default, YubiKey generates slot 1 passcode for NFC configured mobile devices. You can set slot 2 passcodes as default by changing the setting from slot 1 to slot 2 using the Yubikey Personalization Tool.

9. Securden matches the 12-character key against your account in its database and verifies the same for the second level of authentication during future login attempts.

10. After submitting the YubiKey one-time password, click Register and Login.

Global 2FA Enforcement

Securden provides you with the option of enforcing the 2FA for all the users of the organization. You can also enable this feature for only the new users of your organization.

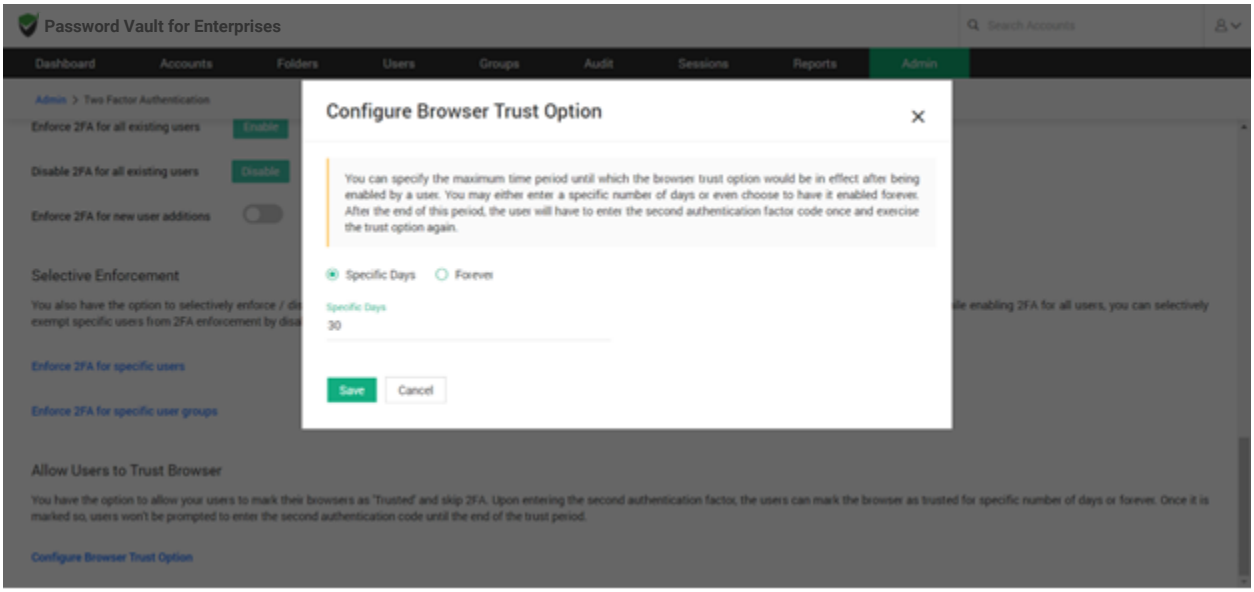


Selective 2FA Enforcement

You also have the option to selectively enforce/disable 2FA for specific users or user groups from **User (or) User Group >> More Actions >> Enable/Disable 2FA**. In addition, while enabling 2FA for all users, you can selectively exempt specific users from 2FA enforcement by disabling 2FA for them.

Allow Users to Trust Browser

You have the option to allow your users to mark their browsers as **Trusted** and skip 2FA. Upon entering the second authentication factor, the users can mark the browser as trusted for a specific number of days or forever. Once marked, users won't be prompted to enter the second authentication code until the end of the trust period.



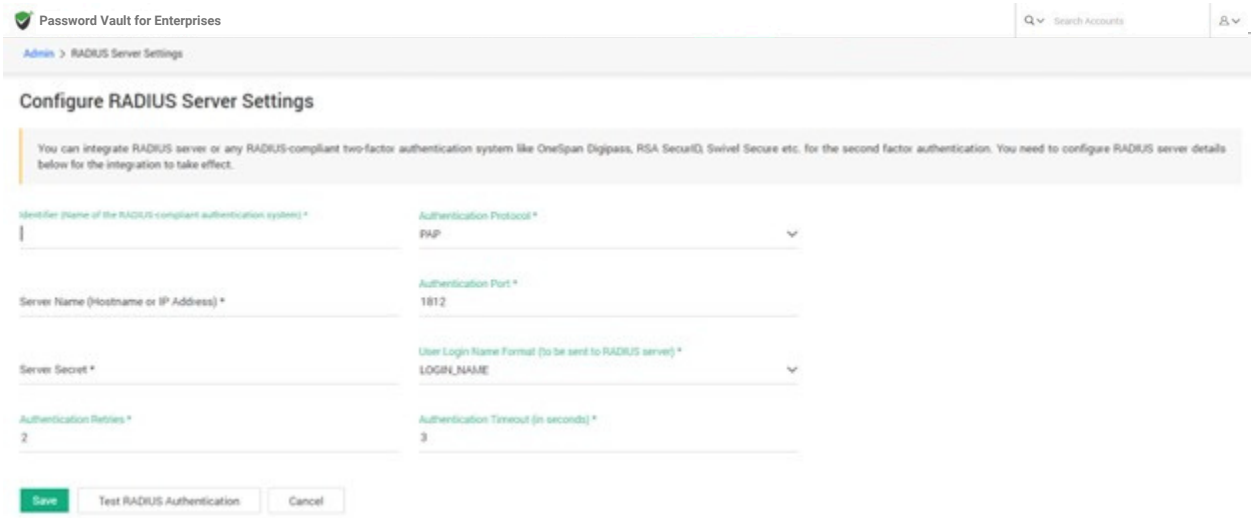
To enable this feature navigate to **Admin >> Two Factor Authentication >> Configure Browser Trust Option** link, and the pop-up box will appear. Here, you can specify the maximum period until which the browser trust option would be in effect after being enabled by a user. You may either enter a specific number of days or even choose to have it enabled forever. After the end of this period, the user will have to enter the second authentication factor code once and exercise the trust option again.

Radius Authentication

RADIUS Authentication can be integrated with Securden Vaultas a 2FA method.

To configure RADIUS authentication,

1. Navigate to **Admin >> Authentication >> Two-Factor Authentication.**
2. Click the configure option on **RADIUS Authentication**.
3. In the **RADIUS Server Settings** page that opens up, you need to enter the following details:
    a. Identifier - Name of the RADIUS-compliant system
    b. Servername - Hostname or IP Address
    c. Server Secret
    d. Authentication Retries
    e. Authentication Protocol (options are PAP, CHAP, MS-CHAP, MS-CHAPv2)
    f. Authentication Port
    g. User login format (to be sent to the RADIUS server): you can choose the format from the provided options or create your own format
    h. Authentication timeout (in seconds)
4. Once you have provided the required information, you can click **Save**.
5. You can also test the setup before saving it by clicking on the **Test RADIUS Authentication** button.



Email to SMS Gateway

As part of two-factor authentication, Securden integrates with Email to SMS gateway providers to send one-time passwords as SMS to the phone numbers of the users. You need to enter the country code for the phone numbers here. Also, ensure that all your users have phone numbers added in Securden. Otherwise, OTP cannot be sent as SMS.

To configure Email to SMS Gateway as an option,

1. Navigate to **Admin >> Authentication >> Two-Factor Authentication.**
2. Click on **Configure** on the **Email to SMS Gateway** option.
3. You need to provide the **Display Name** and the **SMS Service Provider Domain Name**. In case you want to prefix the country code of the users' numbers, you can check the **Prefix country code with phone numbers of all users** button.
4. Click on the **Save** button.

DUO Authentication

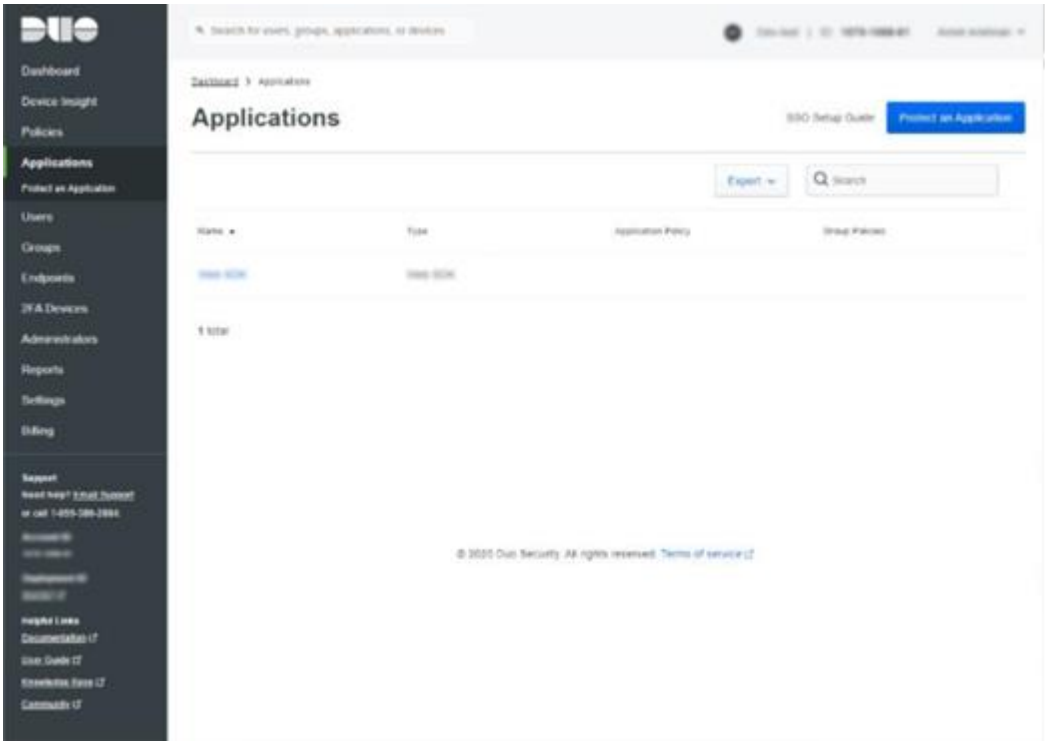
Securden integrates with Duo Security for two-factor authentication. Once configured, users will be enforced to authenticate through Duo for accessing the web interface.

Prerequisite: Before proceeding with the configuration steps below, you need to carry out a few steps at Duo Security to enable the integration with Securden. Once you complete the steps in Duo, you will get an integration key, secret key, and API hostname, which you need to supply below. After configuring this, remember to enable Duo Security authentication on the 2FA settings page.

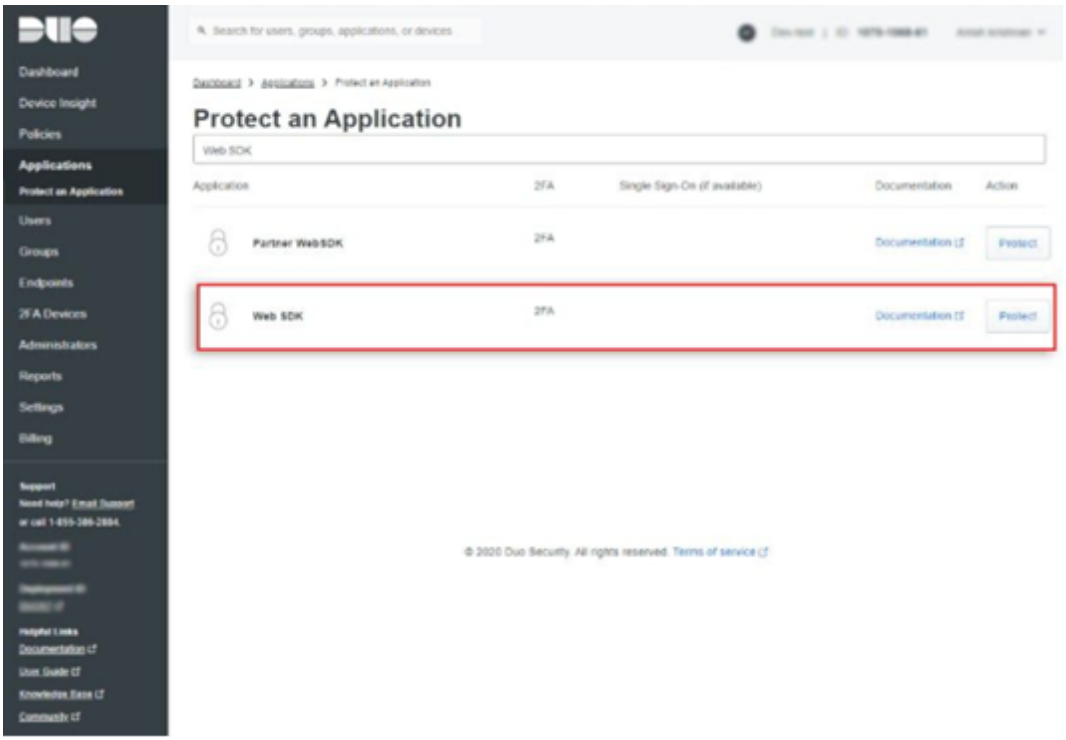
To enable Duo authentication in Securden, you need to carry out certain configuration steps in both Duo and Securden.

Step 1: Configurations in Duo

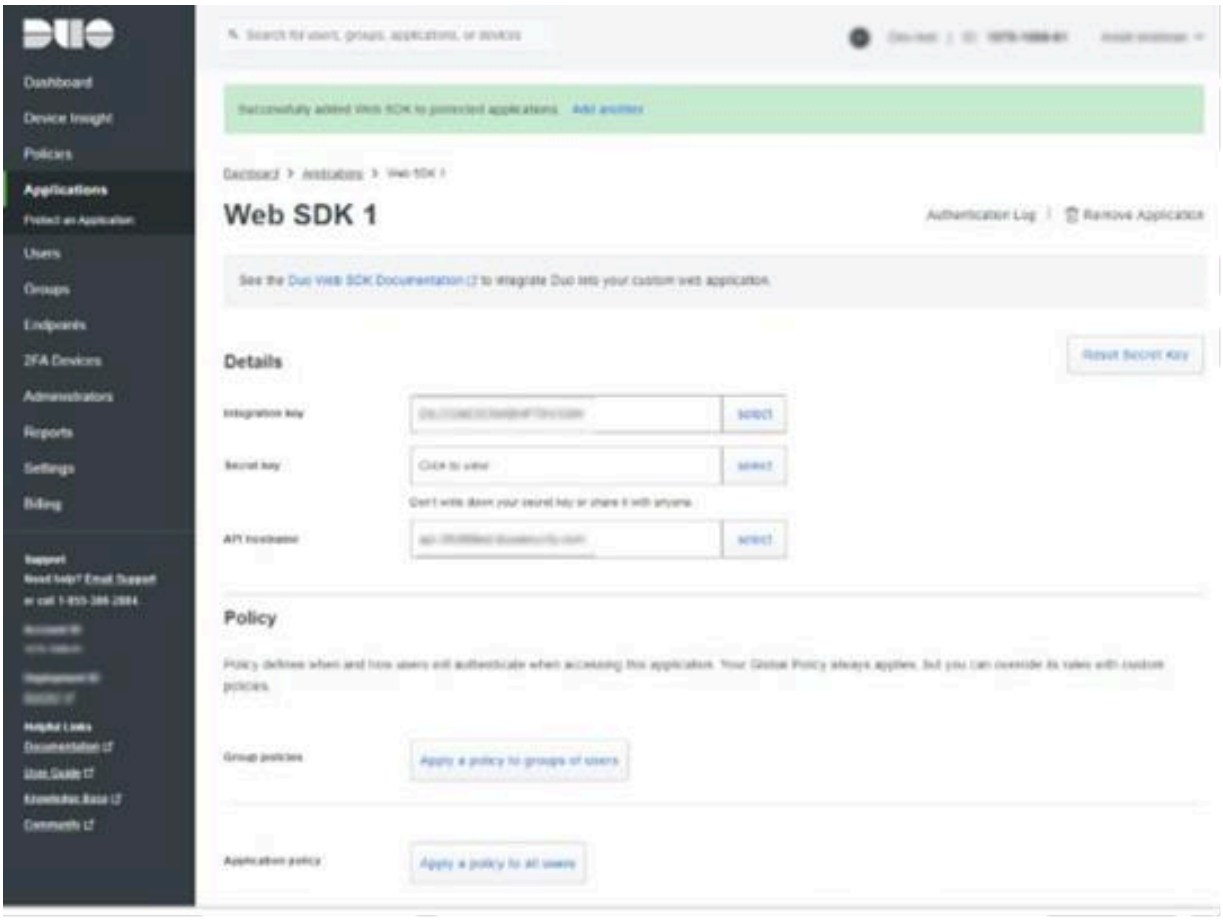
1. You should have an account with Duo and log into the Duo Admin Panel. Securden has to be added as a new application.
2. Click Applications in the left sidebar, and in the GUI that opens, click the **Protect an Application** button. Alternatively, you can click the **Protect an Application** submenu item in the left sidebar.



3. In the list of applications, search for **Web SDK**. Click the **Protect** button on the right to configure the application.



1. You will get your **integration key, secret key, and API hostname**. Copy these details. You will need these to complete your setup.



4. Finally, you need to create a policy to handle Duo enrollment scenarios in your organization for Securden. You may create a policy for Securden that takes effect for all users or use a Global Policy applicable to all your applications.

To handle the users who have not been enrolled to Duo yet, you have three options:

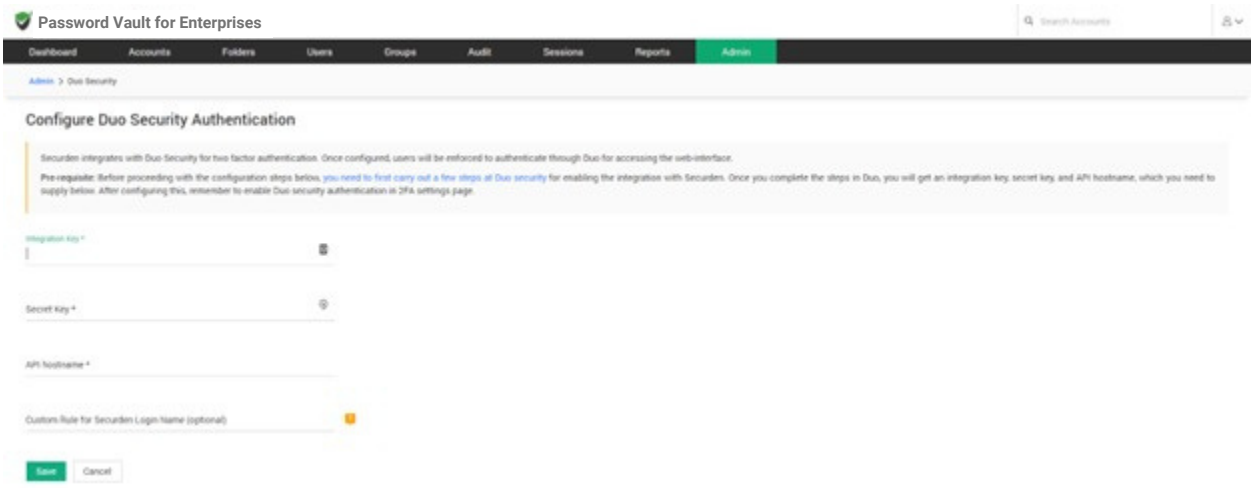
- **Require enrollment** - You can ask them to enroll in Duo. They will see an inline self-enrollment setup process after entering their username and password. (Users who are already enrolled in Duo are prompted to complete two-factor authentication).

● **Allow access** - You can grant access without Duo authentication to those who haven't enrolled with Duo. They will not be prompted to complete enrollment.

● **Deny access** - You can deny access to those who haven't enrolled with the duo. Users must be enrolled before attempting authentication.
The above steps complete the setup process in Duo.

Step 2: Configuration in Securden

1. In Securden GUI, navigate to **Admin >> Authentication >> Duo Security**. You will need to provide the integration key, secret key, and API hostname from the application in Duo security to Securden.

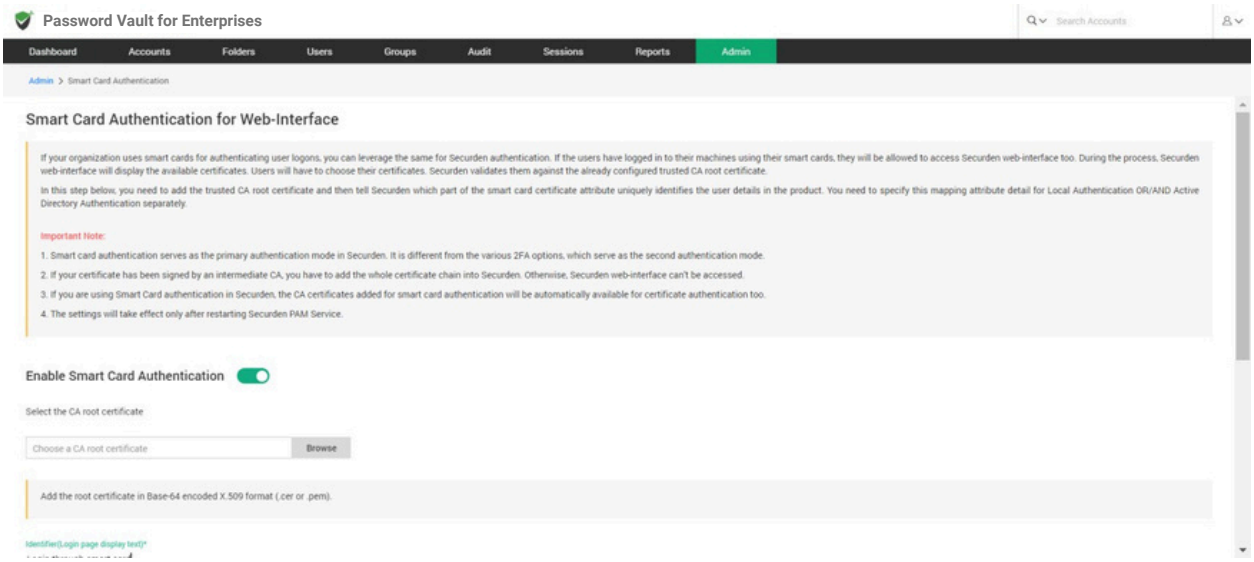


2. After entering the details, navigate to **Admin >> Authentication >> Two-factor Configuration** and select **Duo Security.**

3. Then Duo Security will now be used as the second-factor authentication for the users in Securden. The users may select two options for entering the second factor - to send push notifications to their mobile phones or to enter the code from the Duo mobile app.

Smart Card Authentication

If your organization uses smart cards for authenticating user logins, you can use the same for Securden authentication. If users have logged in to their machines using their smart cards, they will be allowed to access the Securden web interface too. During this process, the Securden web interface will display the available certificates and users will have to choose their certificates. Securden validates them against the already configured trusted CA root certificate.

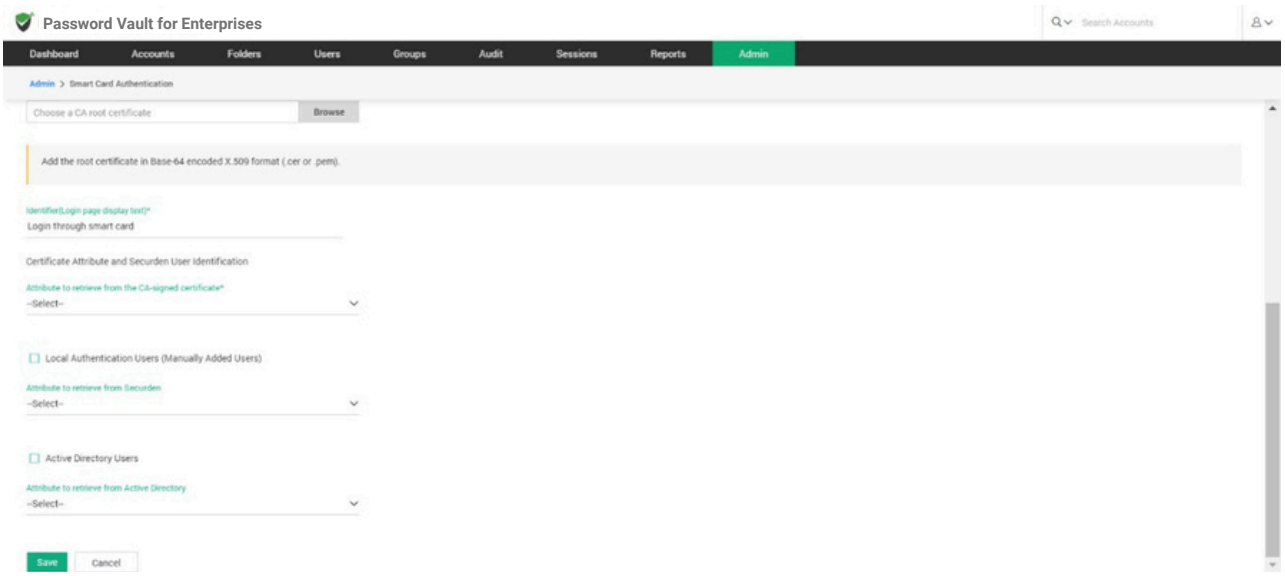


To Enable Smart Card Authentication:

1. Navigate to **Admin >> Authentication >> Smart Card Authentication.**
2. Toggle the **Enable Smart Card Authentication** to on.
3. Select the CA root certificate. You can do this by selecting the **Browse** button and selecting the certificate.
4. Select the **Identifier.**
5. From the certificate, select the attributes to be retrieved into Securden.
6. To enable Smart Card Authentication for local users, check the box and add the attribute.
7. Likewise, to enable Smart Card Authentication for Active Directory Users, check the box and add the attribute.
8. Click on **Save.**

In the above step, you need to add the trusted CA root certificate and then tell Securden which part of the smart card certificate attribute uniquely identifies the user details in the product. You need to specify this mapping

attribute detail separately for Local Authentication OR/AND Active Directory Authentication.



Note:

1. Smart card authentication serves as the primary authentication mode in Securden. It is different from the various 2FA options, which serve as the second authentication mode.
2. If your certificate has been signed by an intermediate CA, you have to add the whole certificate chain into Securden. Otherwise, the Securden web interface can't be accessed.
3. If you are using Smart Card authentication in Securden, the CA certificates added for smart card authentication will be automatically available for certificate authentication too.
4. The settings will take effect only after restarting Securden VaultService.

Troubleshooting Tips

Issue: 2FA code is not accepted in the UI.

Solution: The most probable reason for MFA not working is that the time on the mobile device is not synchronized. To troubleshoot this issue,

- Go to your phone Settings.
- Navigate to Date & Time settings.
- Turn ON Set Automatically (in iPhone) or Turn ON Use Network-Provided Time (in Android).
- Restart Google Authenticator / Microsoft Authenticator app.
- Now, try to login to Securden using the latest MFA code.

Section 5: Account Management

Securden provides a centralized credential vaulting facility in which you can add, remove, share, and monitor various privileged credentials that can be used to manage multiple privileged accounts in your organization. To manage the privileged credentials, you need to add them to the vault. You can add accounts from a file, manually add them to the vault, and import them from other password management solutions.

Adding Accounts

Once the users who are going to use Securden Vault are onboarded, the very first thing to do is add all the accounts for centralized management.

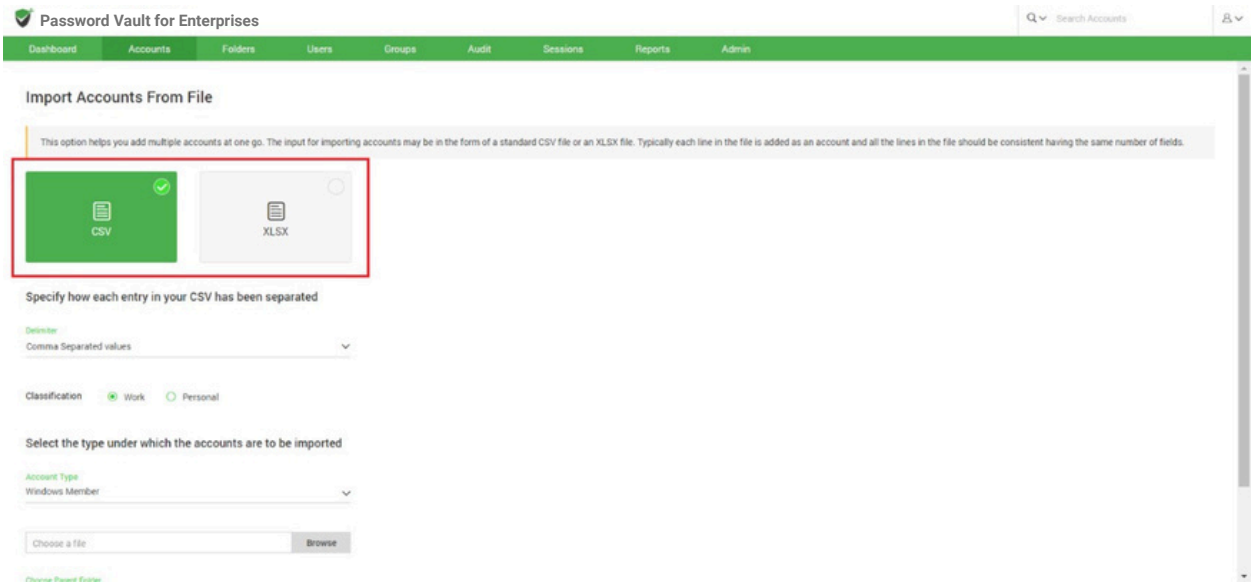
Importing Accounts from CSV/XLSX Files

If you have account credentials stored in spreadsheets or a text file, you can use the **Import from Files** option to add them to Securden at one go. The input for importing accounts may be in the form of a standard CSV file or an XLSX file. Typically, each line in the file is added as an account and all the lines in the file should be consistent having the same number of fields.

Formatting your File for Importing

Importing Accounts is very flexible in Securden. You can simply import the file you have exported from your current repository into Securden and then map the matching fields. For example, in a XLSX file, each row is considered a separate account and each column is considered as an account attribute. Similarly in a CSV file, each row is considered a separate account and each attribute is demarcated by a delimiter.

To import accounts from a file, navigate to **Accounts >> Add >> Import from File**



1. You need to select the type of file you want to import from.
2. If you select the file type **CSV**, you need to specify the delimiter used to separate different account attributes.
3. You need to select an account type that is suitable for all the accounts stored in the file. If such an account type doesn't exist, you need to

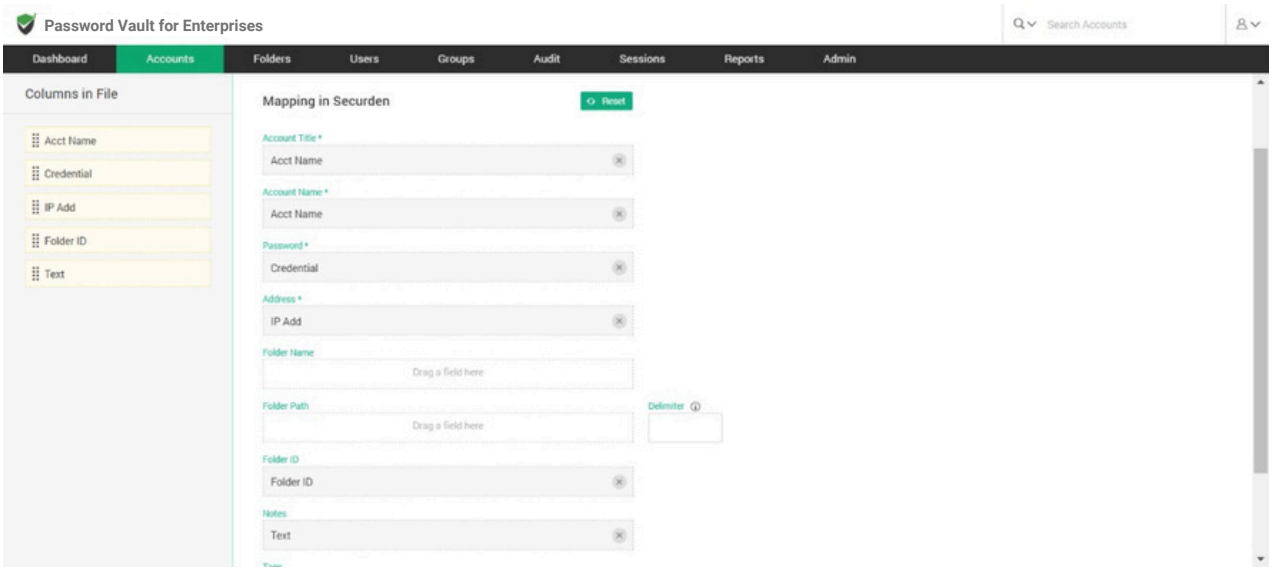
create a suitable account type for this purpose. Navigate to **Admin >> Account Management >>Account Types** to add a new account type.

4. Once the account type is finalized, you need to browse and select the file you want to upload. Click **Browse** and select the required file on your computer and click **Open**.
5. You need to select a parent folder to which the imported accounts will be added.
6. Click **Next**.

In the second step of the import, we provide the option to map the columns (attributes) in the input file to attributes in Securden.

Mapping

Mapping is the second step of import (refer to the screenshot below), you can map the columns (drag and drop from LHS to RHS).



For example, you can map

Acct Name -- > Account Title

Acct Name ---> Account Name

Credential --> Password

IP Add - -> URL

Hostname --> Hostname (additional field added by creating a new account type)

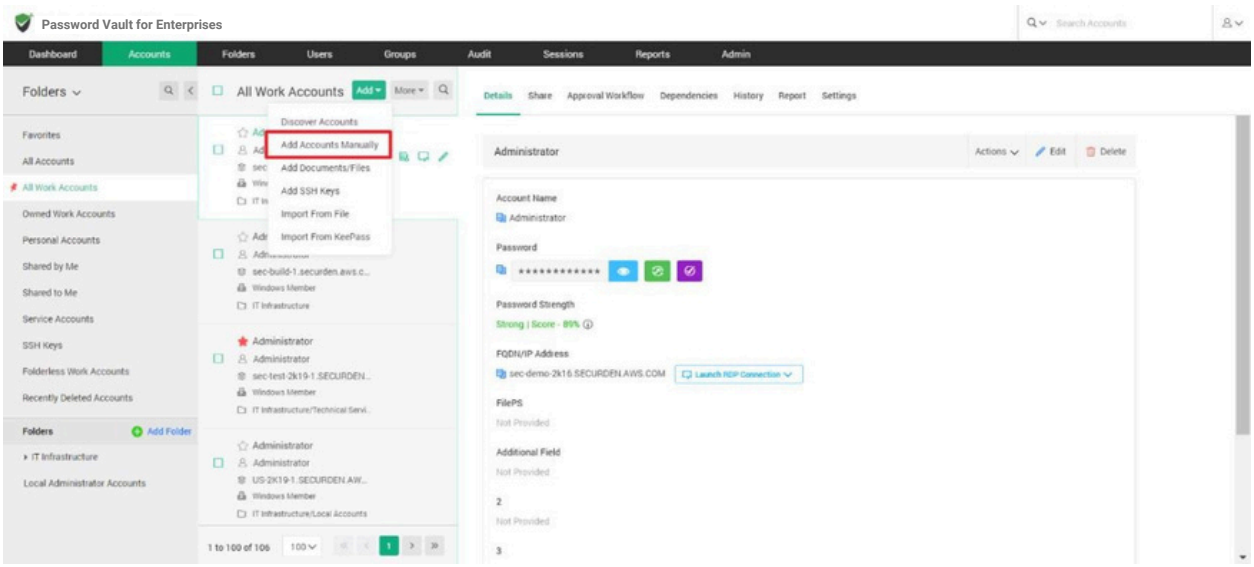
extra --> Extra (additional field added by creating a new account type)

grouping ---> Folders.

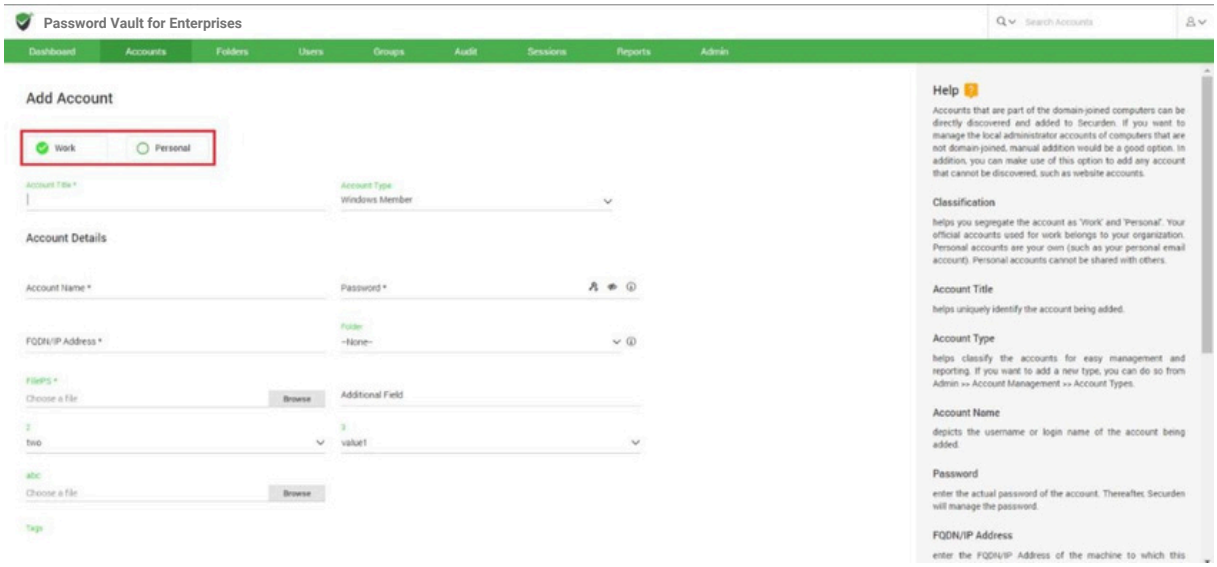
Adding Accounts Manually

You have the option to add accounts to the repository manually. Accounts associated with domain joined computers, servers, accounts, service accounts, organizational units (OUs), and groups, can be automatically discovered and added. Other accounts such as website accounts, files, etc. that cannot be discovered automatically can be added manually and managed with Securden.

To add an account manually, navigate to **Accounts >> Add >> Add Accounts Manually**



1. In the GUI that opens, you can fill in the fields and classify it either as a **Work** account or a **Personal** account.



Work Accounts

Your official accounts used for work can be added as work accounts. This account can be shared with other people in your organization.

Personal Accounts

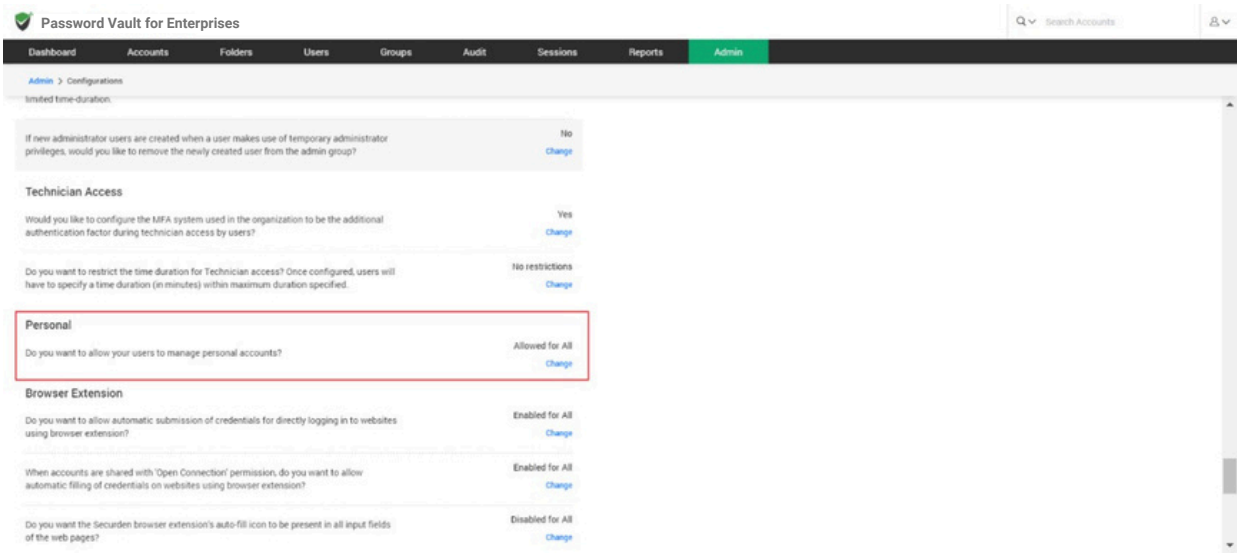
Personal accounts are your own accounts. Personal accounts can be health care accounts, email accounts, bank accounts, social security numbers etc.

Note:

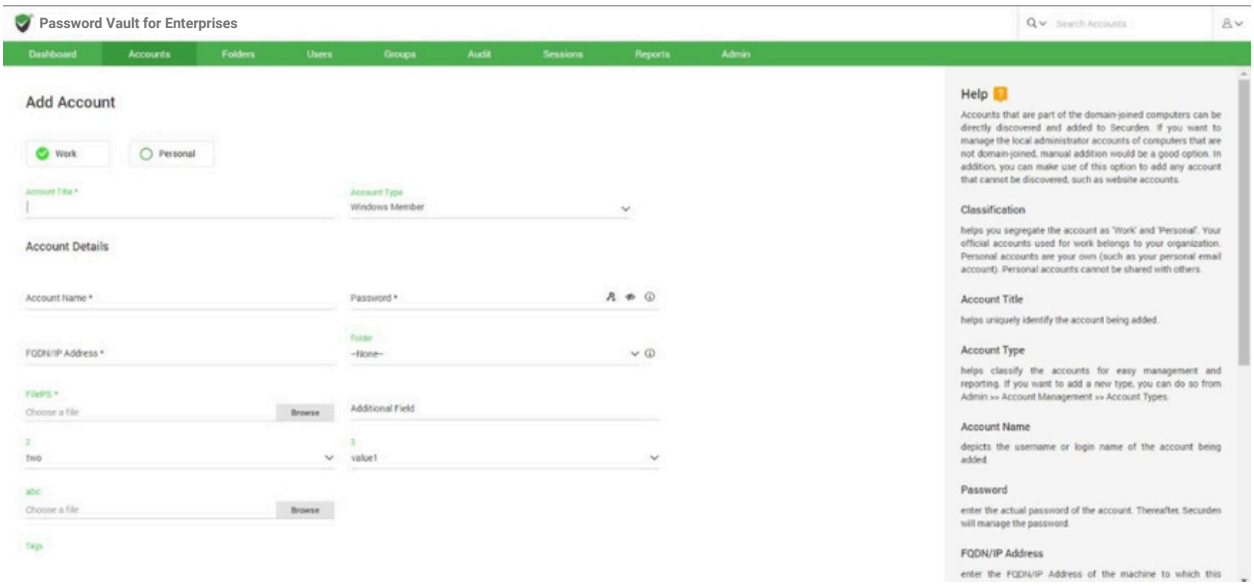
1) The primary differentiating factor between a work account and a personal account is that a personal account cannot be shared with another user in the organization.

2) Personal Accounts cannot be viewed by any other user. Even the most privileged role like the Super Administrator would not have the ability to view personal accounts belonging to individual users.

3) You may disable users from creating and storing personal accounts. Navigate to **Admin >> Configurations** to configure this option.



To add an account, select the type of account i.e., **Work** or **Personal**, and enter the required information:



- **Account Title:** The account title helps uniquely identify the account added, this makes it easier to add to folders and share with users as well.

- **Account Type:** You can select an existing account type added in Securden or choose to create a new account type for the account being created. This helps classify the accounts for easy management and reporting. If you want to add a new type, you can do so from **Admin >> Account Management >> Account Types**.

Note: The Account Type determines the different attributes that you will need to fill, this could vary from being a simple text field to a specific file attachment. The most general fields are covered below.

- **Account Name:** This depicts the username or login name of the account being added.
- **Password:** In this field you enter the actual password of the account. After doing so, Securden will take over the management of the password including periodic password resets if needed.

- **Folder**: If you want to add this account to a folder, you can select one of the existing folders in Securden or add a new folder by clicking on the **Add folder** option from the drop down.

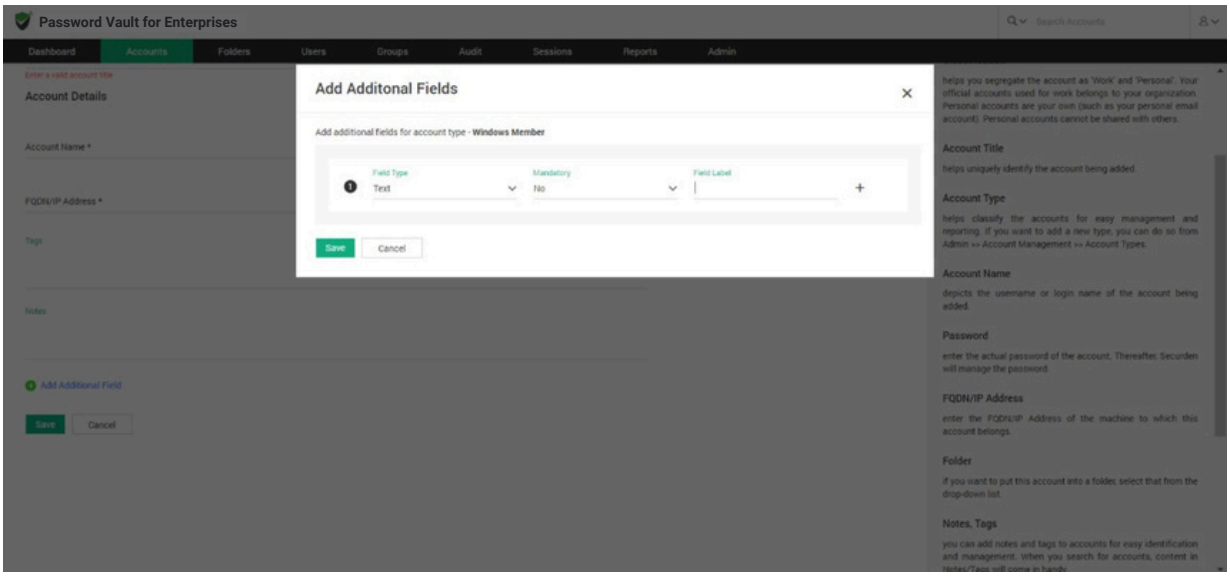
- **File:** You can browse and select a file from your computer to attach with the account.

- **Notes and Tags:** You can add notes and tags to accounts for easy identification and management. When you want to search for accounts, content in notes / tags will come in handy.

Adding Additional Fields:

You can add any number of additional fields for a selected account type. The fields you add for a particular account type will be displayed for all accounts belonging to this account type. Click on the **Add Additional Fields** to enter a text, password or file associated with the account.

- Choose a Field Type, either a text password or file.
- Choose whether the added field should be made mandatory for this account type.
- Enter a field label for easy identification.
- Use the '+' to add more Fields and '-' to remove extra fields.
- Once added, click **Save** to continue.



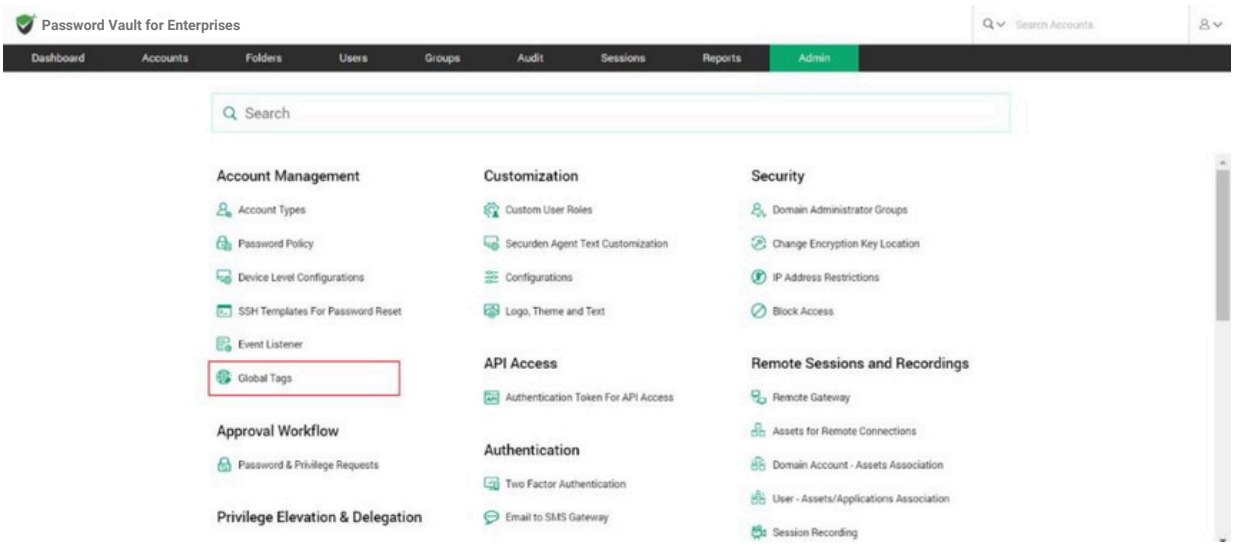
Once done with entering all the fields under Add Account click **Save** and your account will be added to Securden.

Global tags

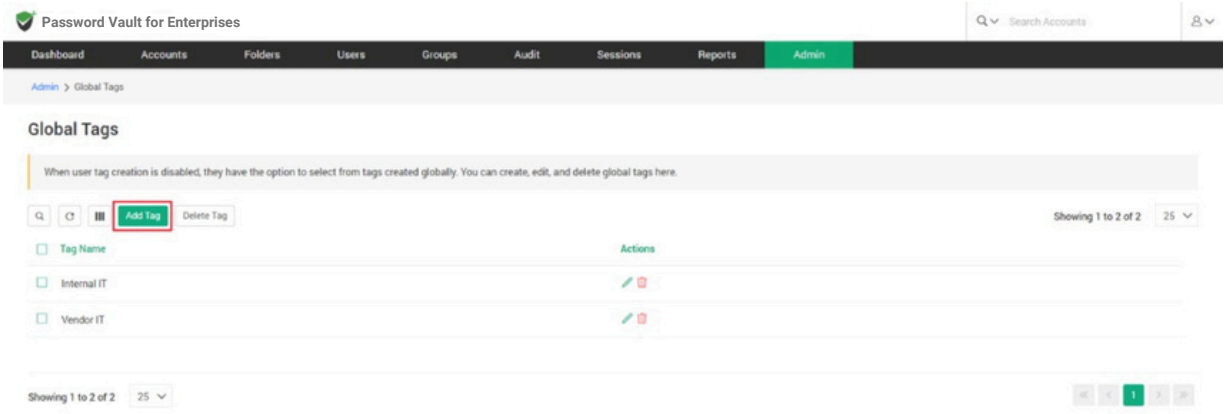
When user tag creation is disabled, they have the option to select from a list of globally available tags to associate with each account.

Administrators can create, edit, and delete global tags. All global tags created are listed here.

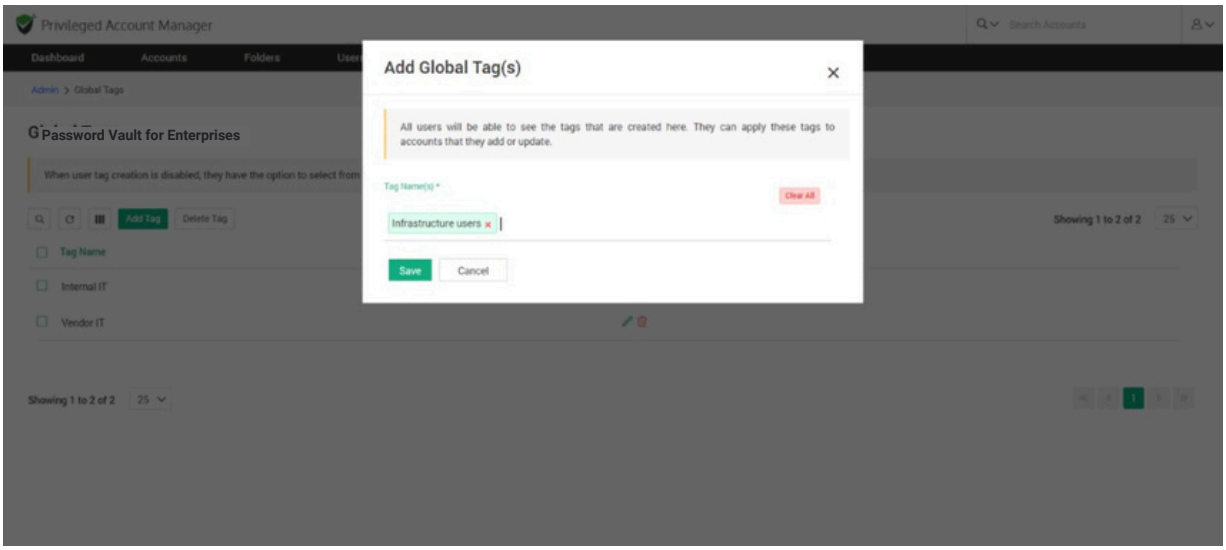
To configure Global tags , navigate to **Admin >> Account Management >> Global tags**.



To add a new global tag, click on '**Add Tag**'.



In the GUI that opens, you can select / create any number of tags and **Save** them in Securden.

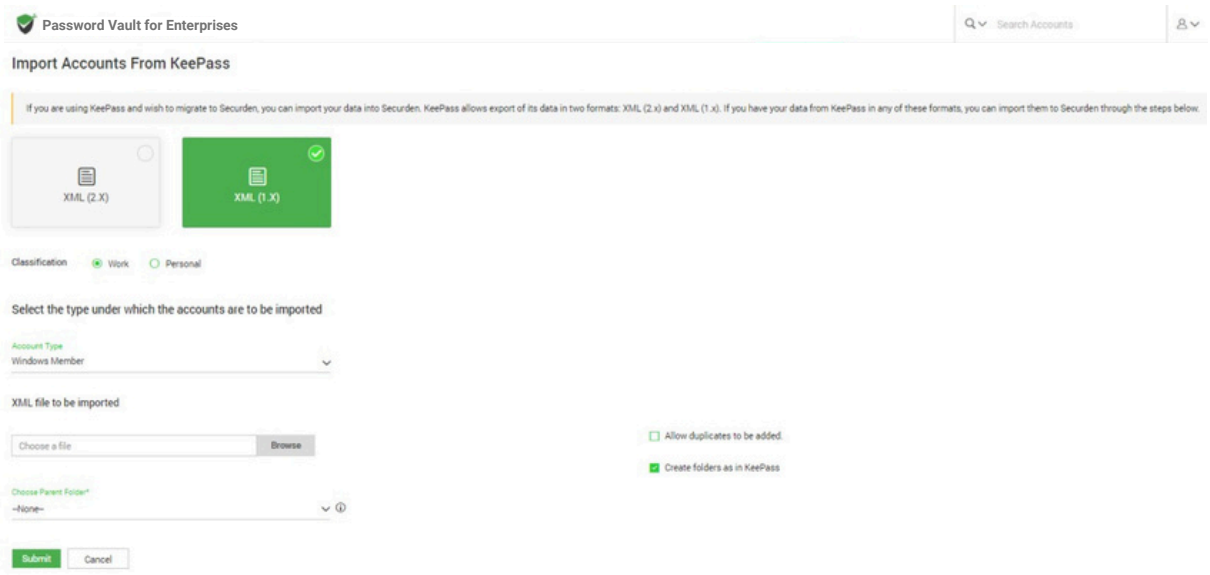


On configuring global tags, users can associate tags with accounts shared with them or owned by them. The globally created tags are displayed as a drop-down items when each account is created.

Importing accounts from KeePass

If you are using KeePass and migrating to Securden, you can import your data into Securden. KeePass allows the export of its data in two formats: XML (2.x) and XML (1.x). If you have your data from KeePass in any of these formats, you can import them to Securden using the steps below.

Navigate to **Accounts >> Add >> Import from KeePass** from the dropdown menu.

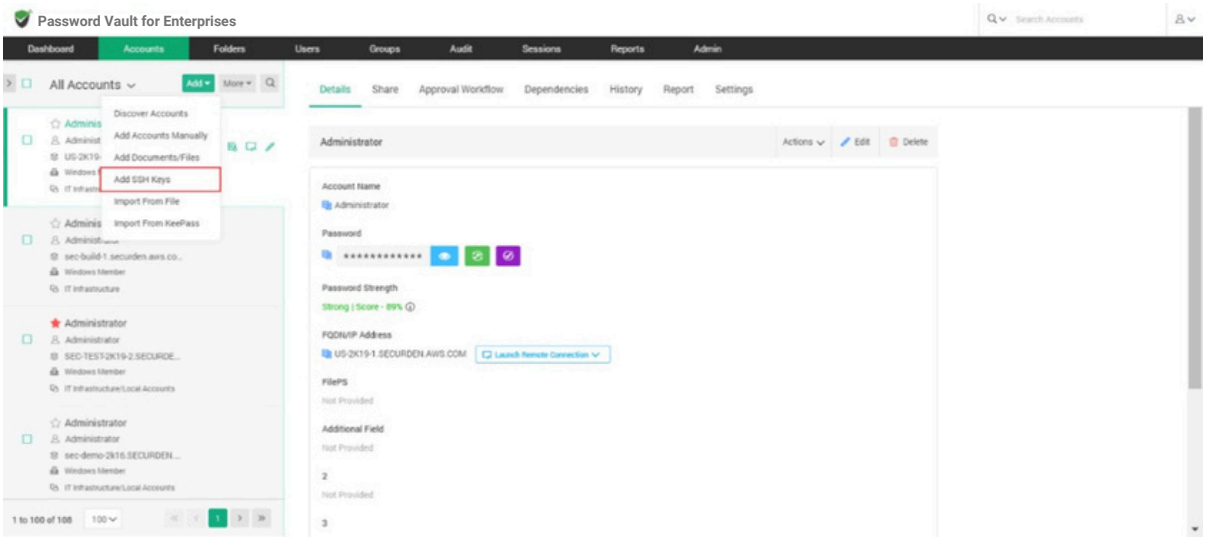


1. Select the appropriate file format.
2. Choose whether the accounts are Work or Personal.
3. Select the account type under which the accounts are to be imported.
4. Choose and upload the XML file.
5. When the checkbox **Create folders as in KeePass** is selected, the folder structure that was maintained in KeePass will be replicated in Securden.
6. Finally, choose the parent folder from the drop-down list and click **Submit.**

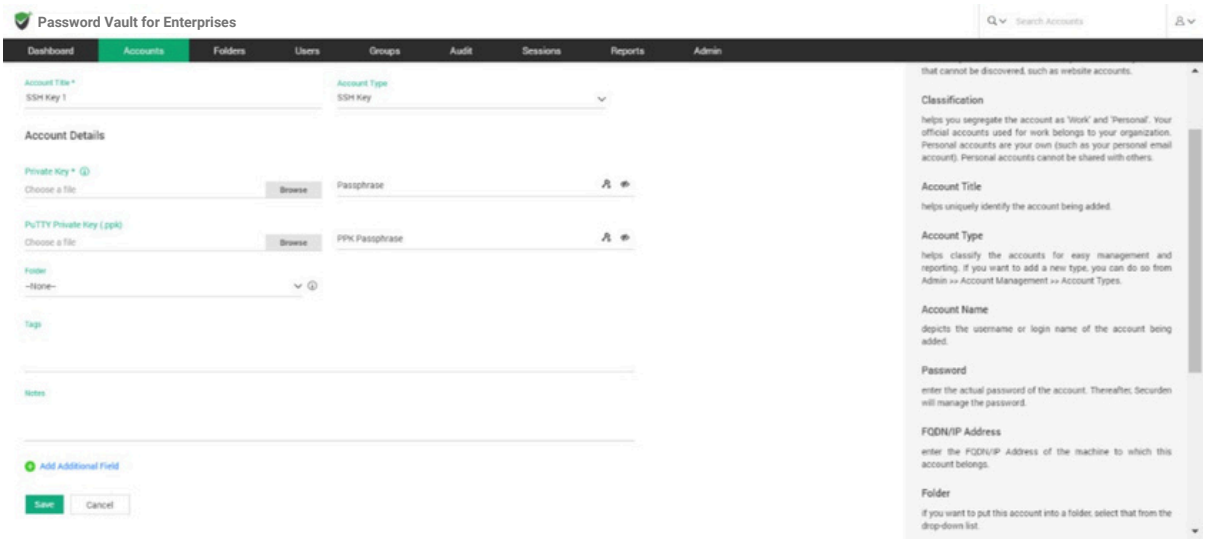
Add and Manage SSH Keys

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.

To add SSH keys, navigate to the **Accounts** tab and click on **Add** and select **Add SSH Keys** from the drop-down.



In the GUI that opens, enter the following details:



Account Title: Helps uniquely identify the account being added.

Account Type: The account type is set to default as SSH Key.

Account Details: Securden allows you to store the SSH keys along with the passphrase associated with them. There are two types of keys supported in Securden.

Private key - Private key slot accepts **.pem** files and is used to launch web based SSH/SQL connections. In case a .pem file is unavailable you may browse and upload a **.ppk** file, but this will only let you launch PuTTY connections.

PuTTY Private key - PuTTY Private key slot only accepts .ppk files and is used to launch putty connections.

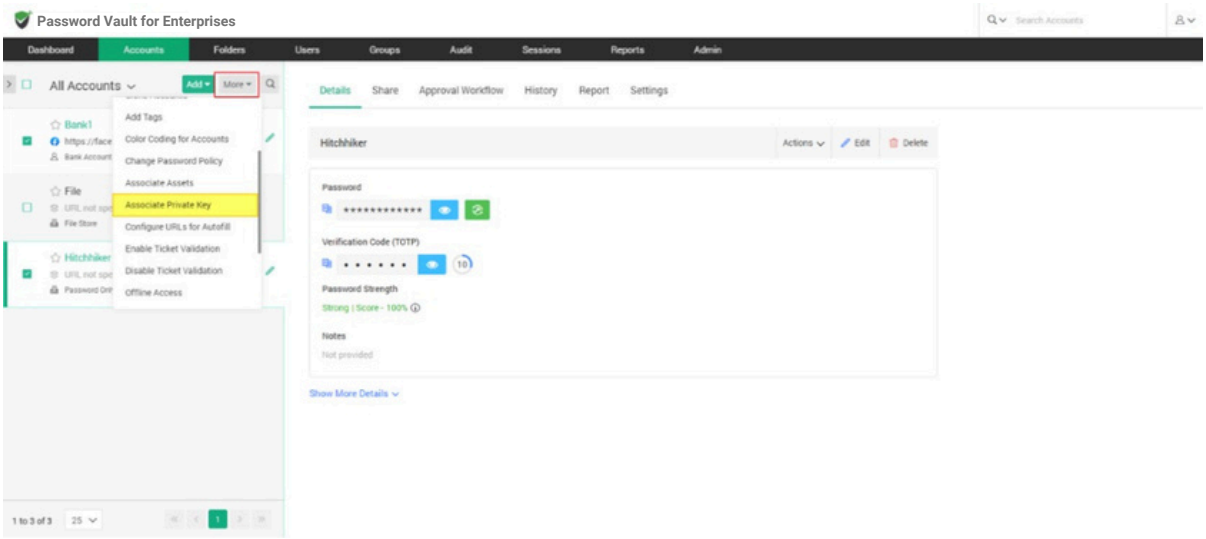
Folder: If you want to put this SSH Key account into a folder, select the required folder from the drop-down list.

Tags, notes: You can add notes and tags to the SSH Key for easy identification and management. When you search for keys, content in notes / tags will come in handy.

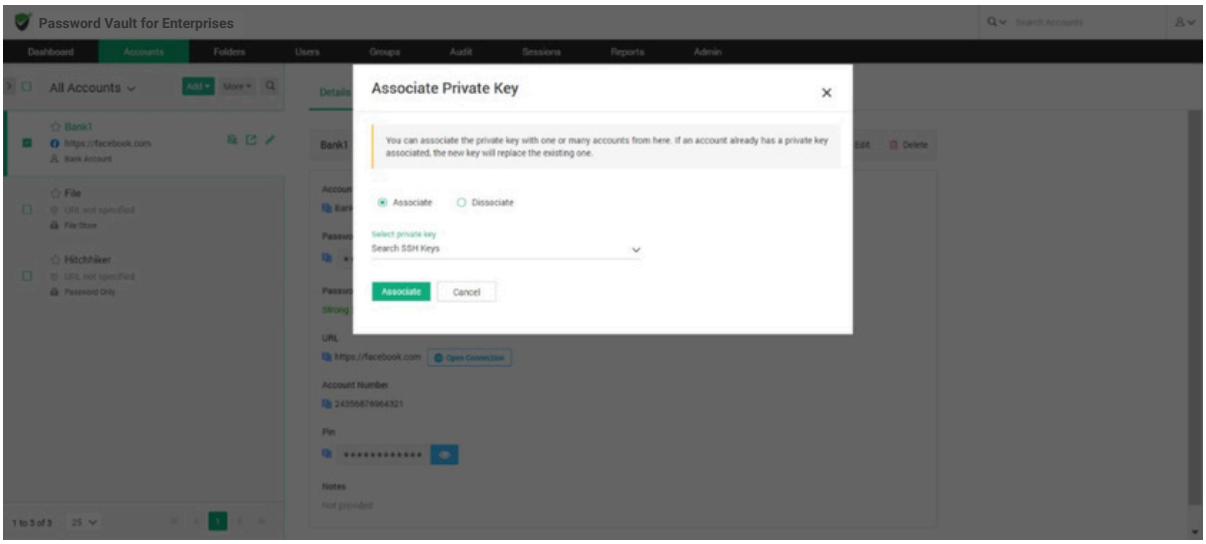
Once you enter all the details, click on **Save** to store the SSH Key.

Associating the SSH Keys to Accounts

After adding the keys, you can associate the key with the required accounts by navigating to **Accounts >> More >> Associate Private Key**.



Select **Associate** and then select the private key account from the drop down, click **Associate** once you have selected the key.

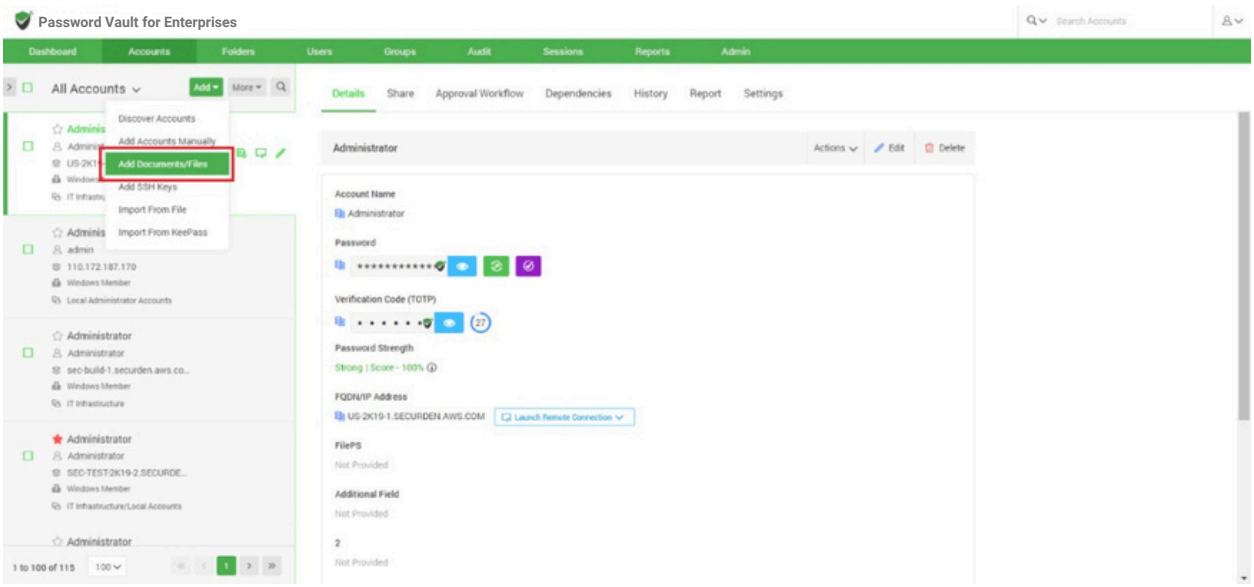


After associating the key, you can open direct connections with remote Unix devices using private key authentication.

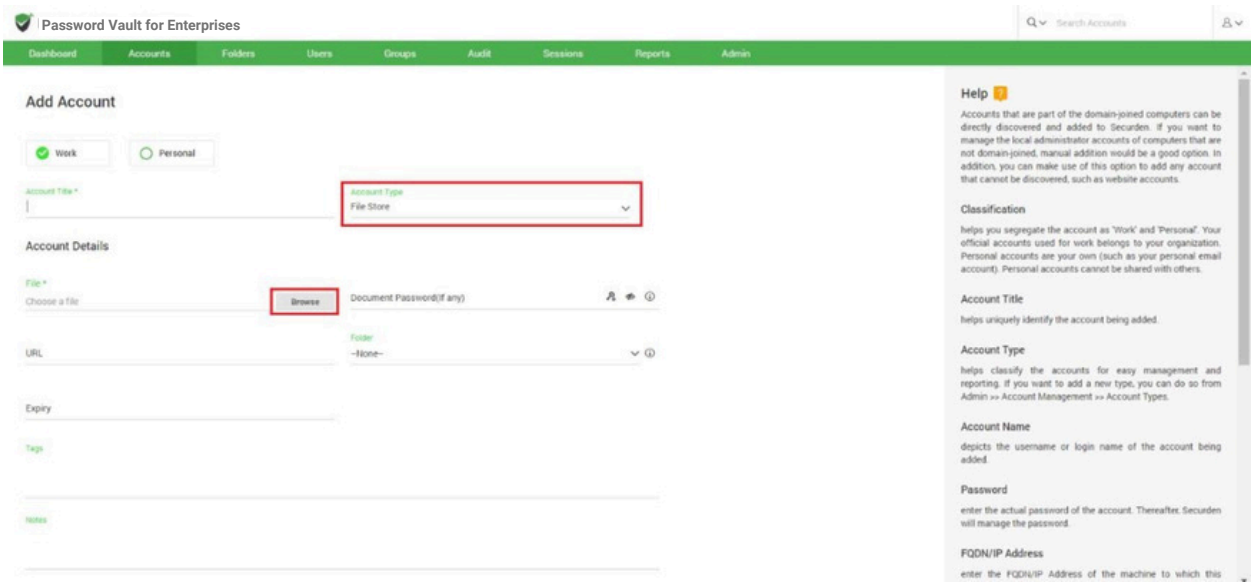
Add Documents / Files

In addition to passwords, you can also store and manage documents, files, images, license keys and others. You can either attach files along with an account or even store the documents individually.

Step 1: Navigate to **Accounts >> Add >> Add Documents / Files** in the GUI.



You can classify the file as **Work** or **Personal**



Step 2: Once you have classified the file as work or personal, you need to enter the following details:

Account Title: Provide a suitable title for identification purposes.

Account Type: This is set to the File Store type by default.

Browse: Select the required file from your device.

Document Password (if any): Enter the password if the file is locked from accessing.

Note: You can choose to generate a password. If you are generating a password here, you should manually configure the file to be password protected. While configuring, you should assign the password generated by Securden to the file.

Step 3: Add into a folder If you want to assign the file being added into an existing folder, you can select one from the drop-down. If you want to assign the file to a new folder, you can do so by clicking **Add Folder**.

Step 4: Add Additional Fields.

Once the details have been entered, if required, you can add additional fields by clicking **Add Additional Field**.

You have the option to add a text, password or a second file associated with the account.

- Choose a Field type, either a text, password or file.
- You have the option to make this additional field mandatory. If you
- want to enforce this field, select **Yes** from the drop-down.
- Enter a field label for easy identification.
- Use the '+' to add more Fields and '-' to remove extra fields.
- Once added, click **Save** to continue.

Once all the required fields under Add Accounts are filled, click **Save** and your file will be added to Securden.

Note: Files of any format up to the size of 25MB can be stored.

View Account Details, Passwords

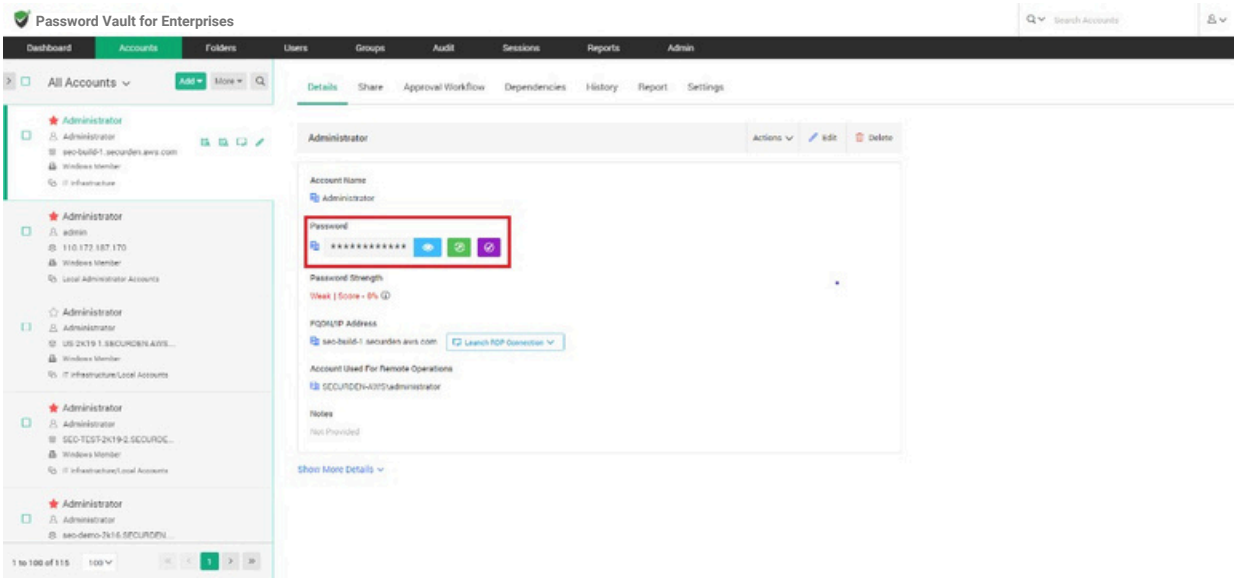
You can view the passwords of accounts, edit attributes, and access other information from **Accounts** tab in the GUI. Click the respective account title to view the details.

The basic details of an account are displayed on the right pane when you click on any account. This includes the account name, password, IP address and other security related information. The **Details** section provides a quick overview of the selected account in the inventory.

To view the passwords and other details of a specific account, navigate to Accounts tab and then click the Details tab on the right pane. Click the respective account title on the left pane, you will see the details like account name, password, and other attributes. You can also edit the account properties from the details section.

The primary information in the **Details** pane consists of:

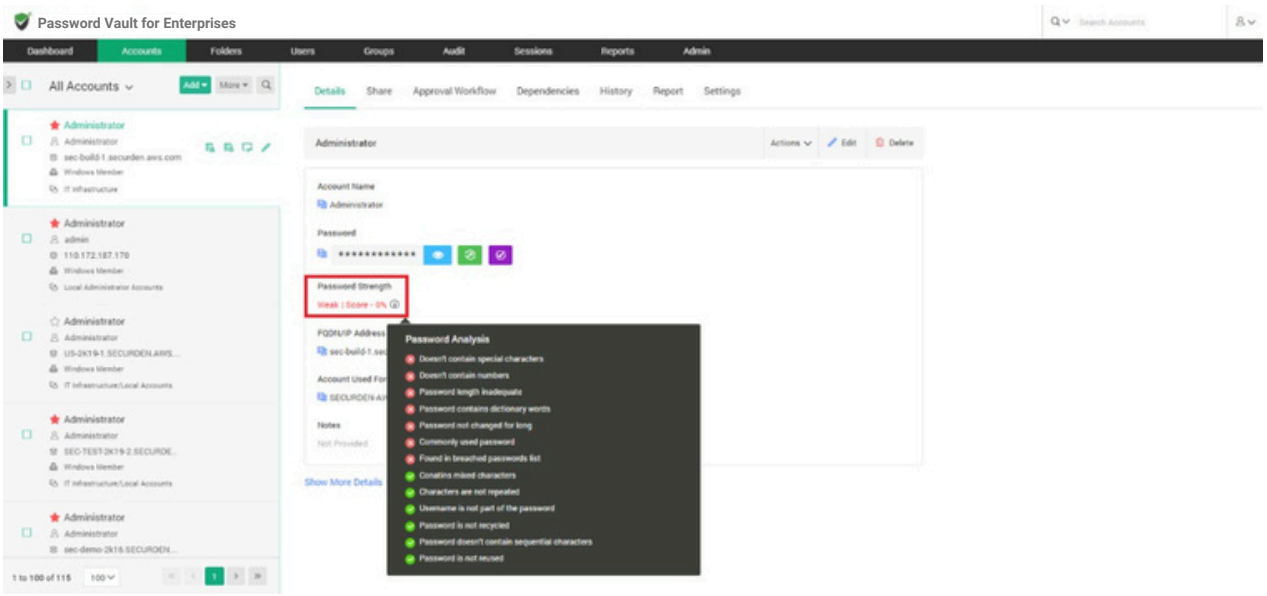
- Account Name
- Password - On the right side, next to the Password field, there are three options to Show/Hide Password, Change Password, and Verify Password.



Note: The password and all related fields will only be displayed if the user has all the required permissions.

1. To see the password and the strength score, the user must at least have **View** permission for the account.
2. To change the password, the user must at least have **Modify** permission for the account.

Password Strength - The password strength that is displayed is based on a set of predefined parameters defined in Securden.



Each of these parameters has a weightage assigned to it, based on which the password strength score is determined.

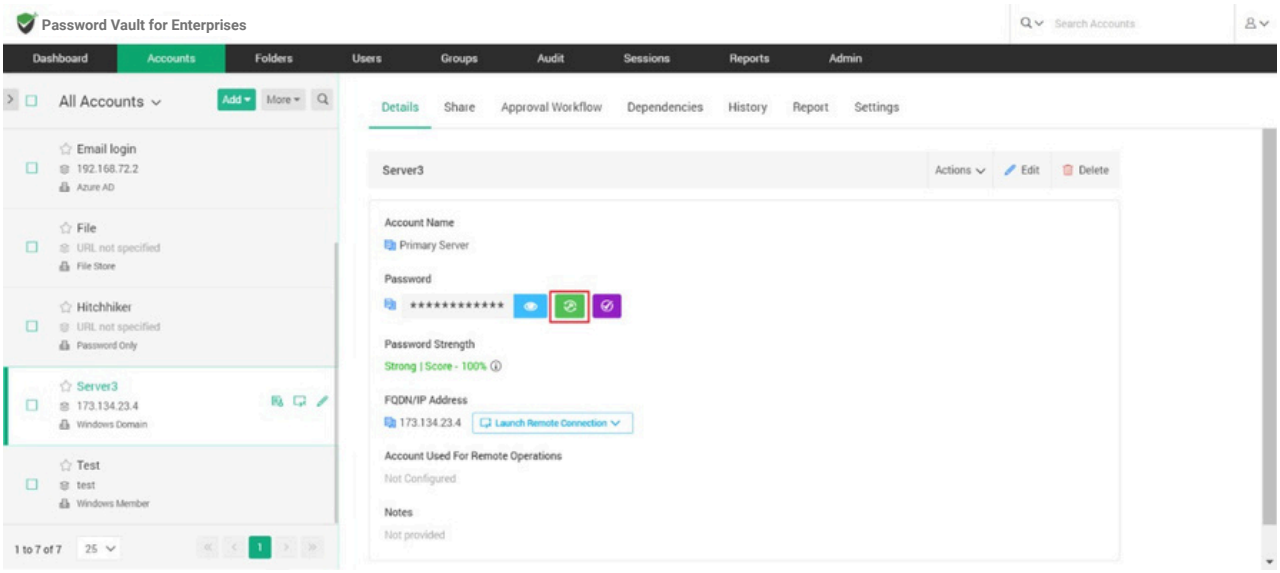
Note: This score is independent of the password policy assigned to the account.

Password Management Operations

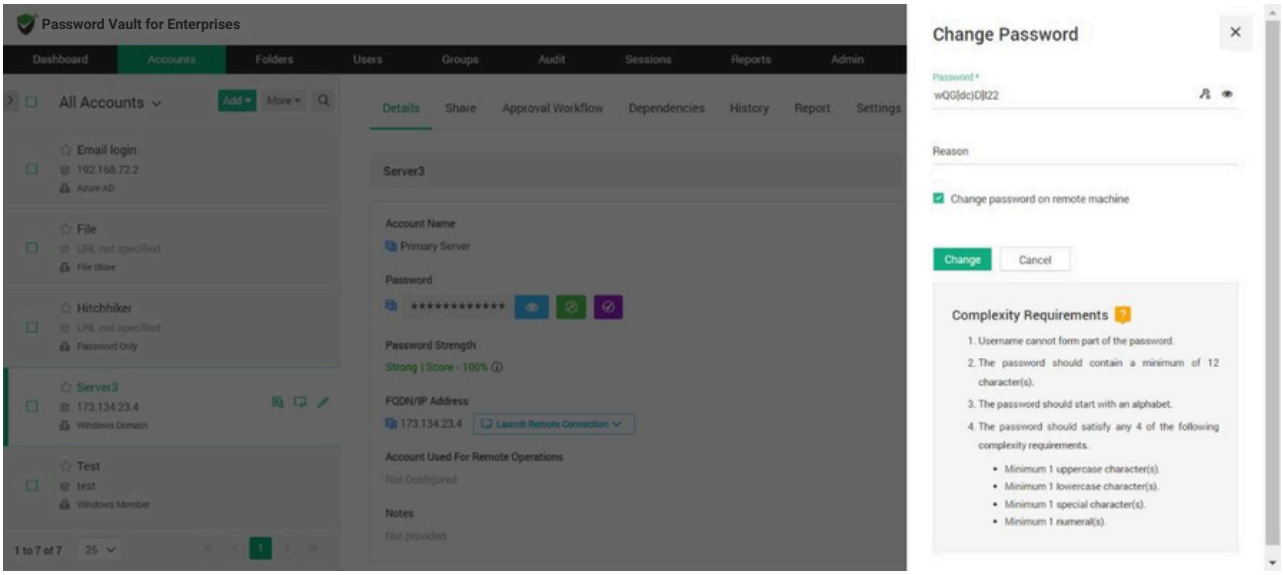
Change Password

You can change the password of an account locally in Securden by navigating to the **Accounts** tab and selecting the account from the left panel whose

password needs to be changed. On the right panel under the **Details** section, on the right side of the **Password** field there are three options to Show/Hide Password, Change, and Verify the password. Click on the **Change** password icon, a **Change Password** window opens.



There you can enter a new password manually or use the password generator to generate a strong password. You also need to justify the action by entering a reason. Clicking on the **Change** button will change the password within Securden.



The new password being created must satisfy the complexity requirements so that the strength and robustness of the password is ensured.

Note: The password complexity rules are set under the **Password Policy** navigating to **Admin >> Password Policy**

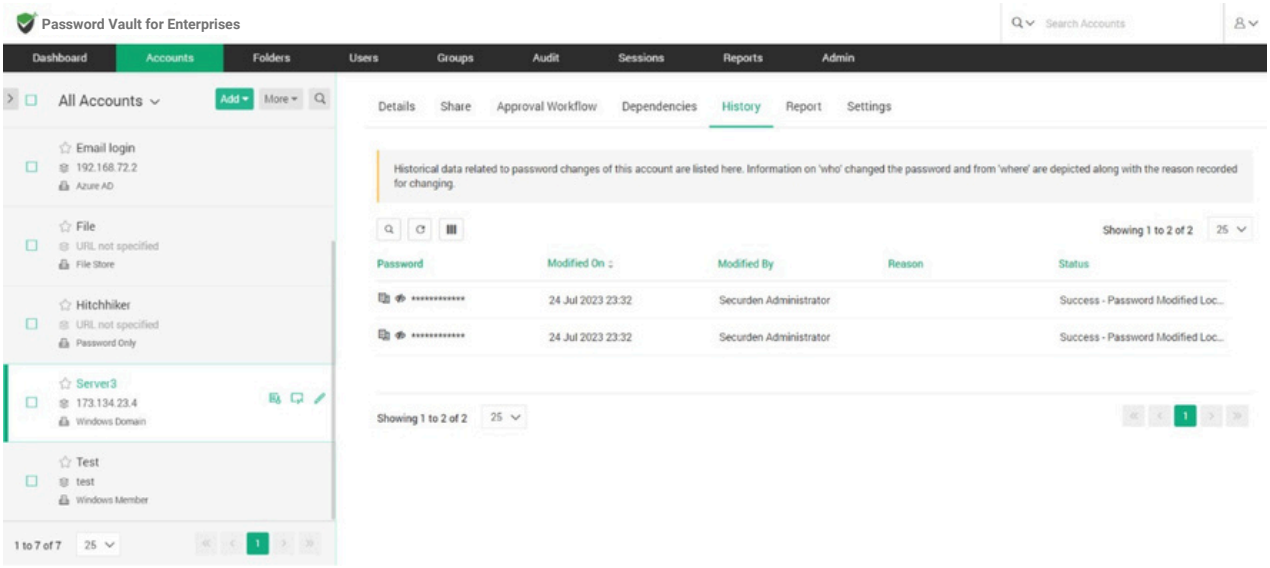
While resetting the passwords, you can take the help of Securden's password generator, which helps generate strong passwords. (**Generate password** is located beside the eye icon).

Note:

Changing the password on the remote machine is available only in **Enterprise PAM Edition** of Securden Password Vault.

Password History

You can view all the password changes performed on a particular account from this section of the GUI. This section details the information related to **who** changed the password, **when** was the password changed, and the reason for the change. Additionally, you can also perform a filter and search for historical password changes based on attributes such as Modified On, Modified By, and Reason.



Note: The historical data related to password changes of an account are stored indefinitely.

Launching Remote Connections

Most organizations give staff, independent contractors, and third-party vendors remote administrative access to IT assets. If this access is not monitored, it opens the door for malicious insiders and outside attackers to

exploit it. Furthermore, enabling direct remote access between end-user computers and the targeted IT assets might propagate security vulnerabilities.

One of the important capabilities of Securden is automatically launching connections to remote computers and devices without disclosing the underlying passwords. You can open direct remote connections with Windows, Linux, and Mac devices from Securden's GUI. This feature helps you can grant your remote workforce, including IT administrators, and third-party technicians secured administrative access to internal IT assets that are kept behind corporate firewalls.

Establishing Remote connections: Securden supports a variety of remote connections to IT assets running on different platforms. The following connections are supported.

Web-based and native connections:

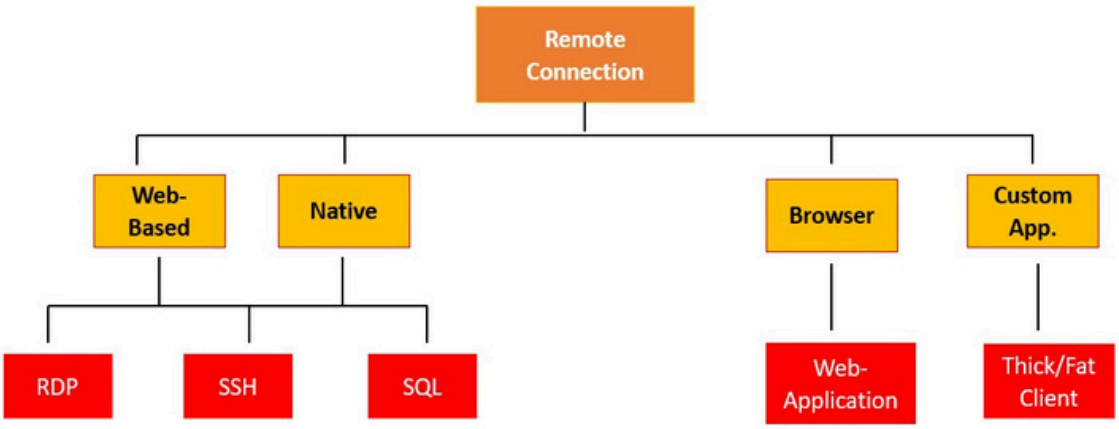
- RDP for establishing connection with Windows devices.
- SSH for establishing connection with Linux devices.
- SQL for establishing connection with Oracle and SQL database servers.

Brower-based connections

- You have the option to launch web-applications directly from the Vault interface. The target web-application will be launched on a browser window and credentials will be injected directly by the Securden browser extension.

Connections to thick clients

- Securden lets you self-support connections to any thick client application through **Custom Application Launchers**. To establish connections to applications like DBVisualizer, Toad, ERP solutions, Zoom, Skype, etc., you need to create a launcher profile listing the actions along with the sequence in which they must be performed on the application.



Web-Based Connections

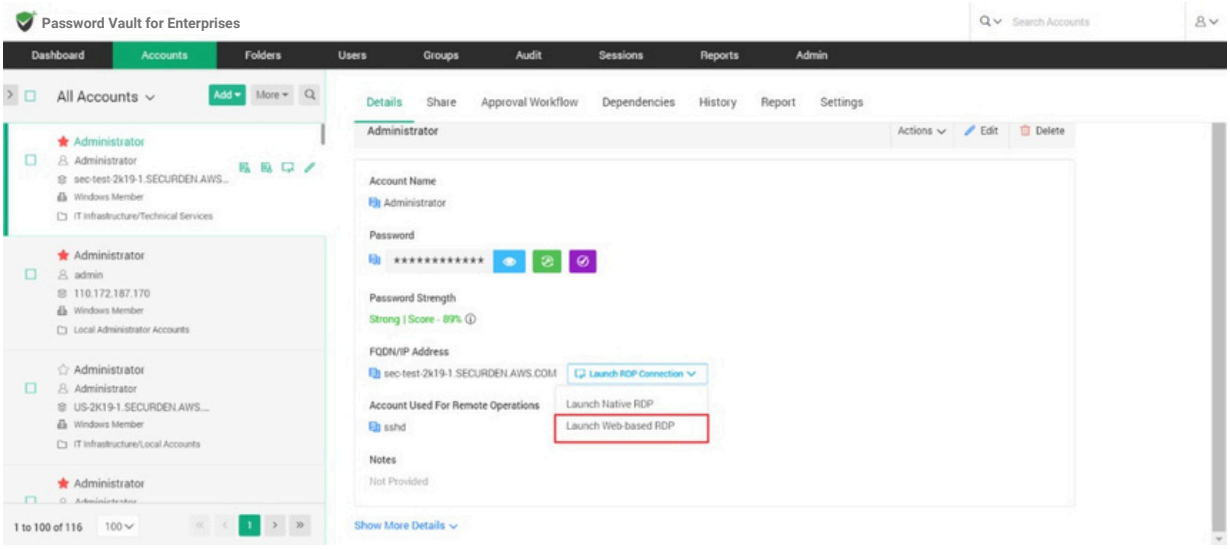
Users can launch connections using a web-browser without installing anything on their machines. There are no prerequisites for this option.

The web-based connections use the Securden server as the starting point to launch connections to the target device. The target machine must be in the operability range to successfully launch web connections. In web-based

connections, certain operations like file transfer, and audio and video recording are not supported.

Note: Prior to launching a remote Windows RDP session connection, you need to configure either a domain or a local account that users can use to authenticate and launch the session using the remote host.

To launch web-based RDP, SSH, and SQL connections, select the required account and click **Launch RDP/SSH/SQL Connection** and then choose the web-based option. After selecting the required option, a small popup window will appear.



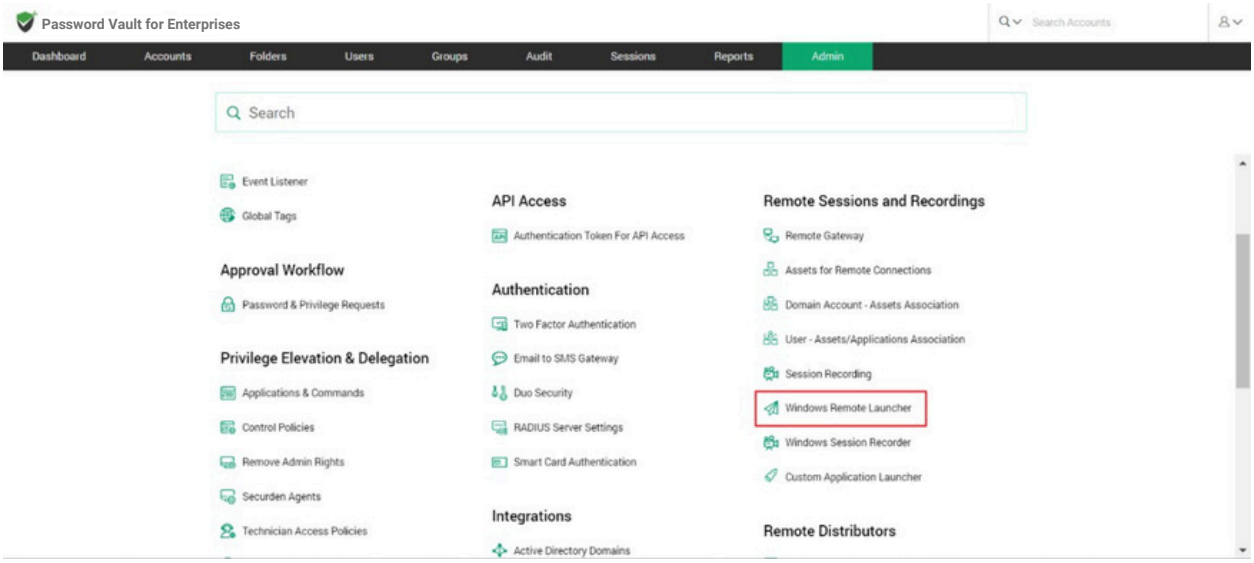
Here you can choose the asset you wish to connect to or specify the name. After you select the required asset, click **Connect** to launch the connection.

Using Native Client Applications

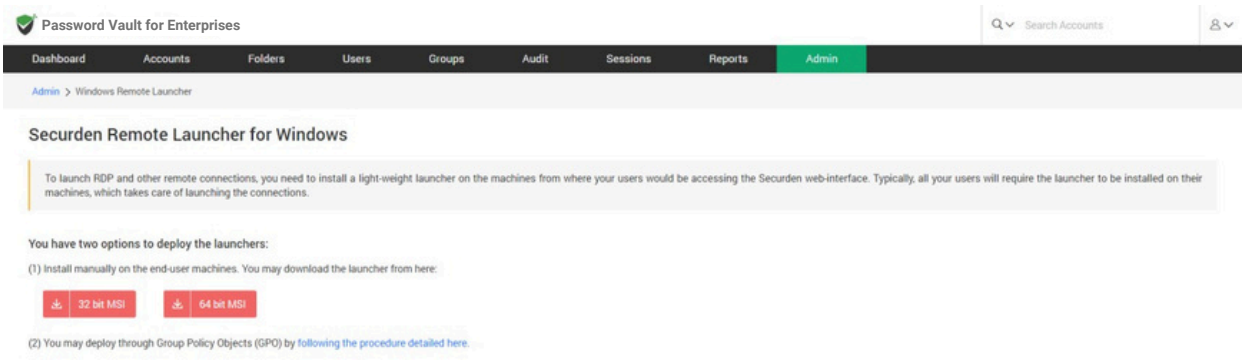
To use native client applications for RDP, SSH (PuTTY, SecureCRT etc.); SQL, a lightweight launcher application must be installed in all the end-user machines.

Installing Windows Remote Launcher for launching Native RDP connections

To launch a Native RDP connection, you need to install a lightweight launcher called **Securden Remote Launcher** on all the machines from which you would be connecting to the Securden web interface. The launcher can be downloaded and installed from **Admin >> Windows Remote Launcher**.

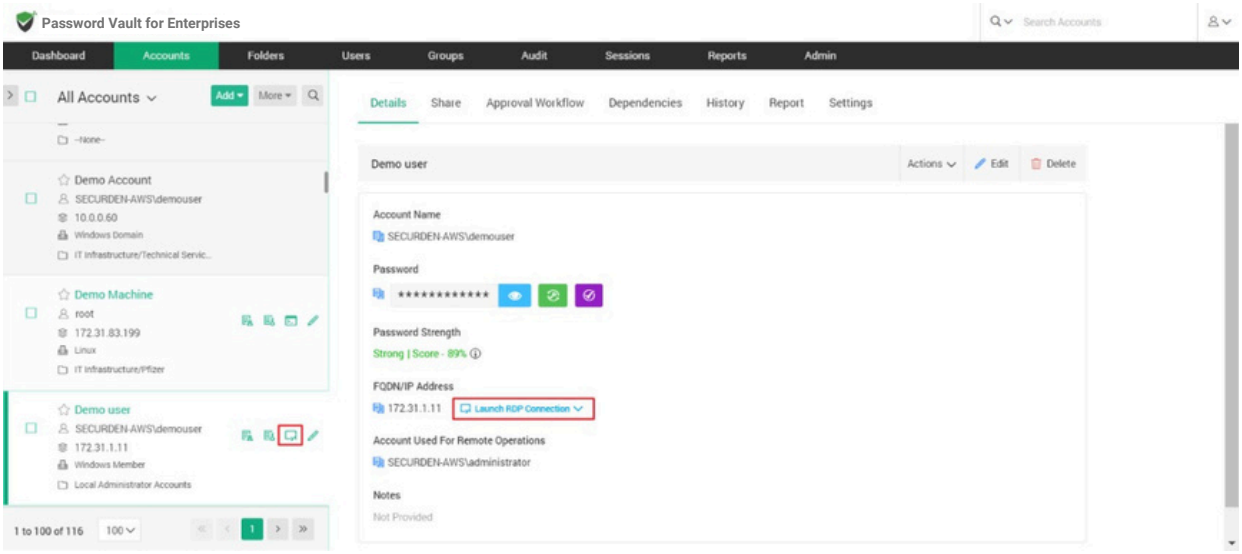


In the GUI that opens, you can follow the instructions provided to install the **Windows Remote Launcher**.



Launching Native RDP connections

RDP connections are mainly used to access Windows-based machines and network devices. Navigate to the 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. Alternatively, you can click the drop-down menu named **Launch RDP Connection** from within the Account to launch a connection.

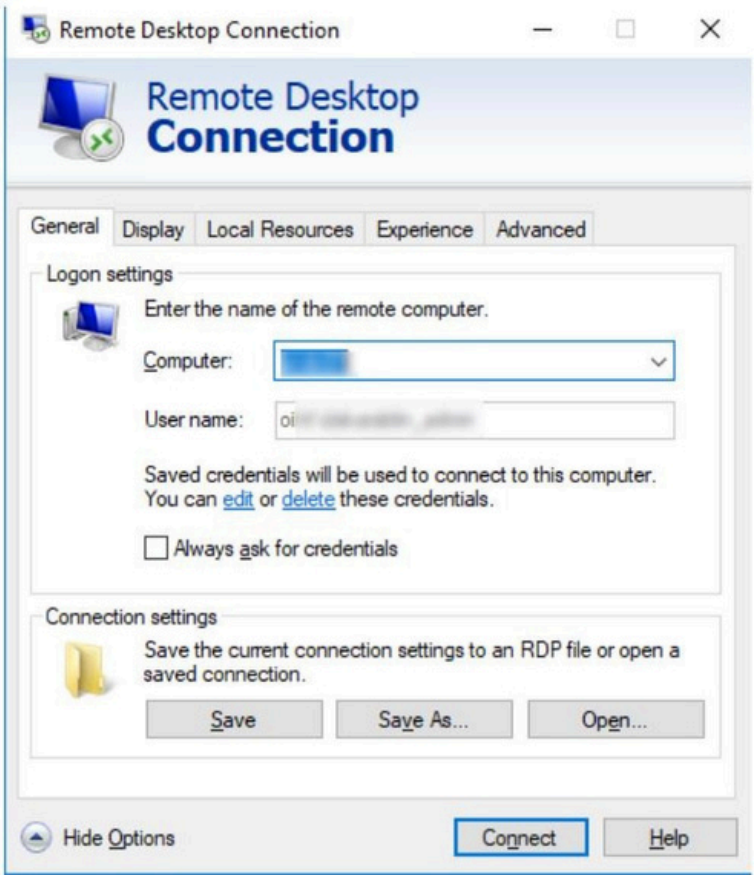


Native RDP Connections: Troubleshooting Checklist

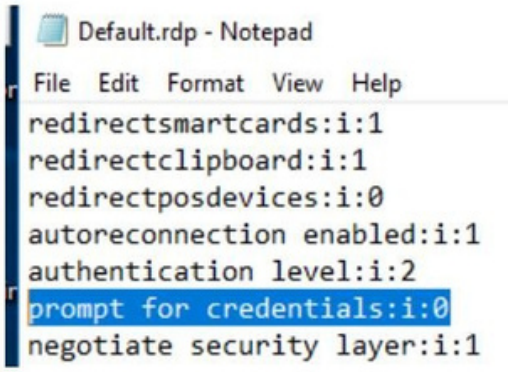
Securden Remote Launcher makes use of MSTSC for invoking remote desktop sessions. The following is a compilation of some of the settings that need to be checked to ensure proper working of RDP sessions. These settings are to be checked on the client machine from which native RDP connections are launched.

Settings to be checked in mstsc app:

Click **Show Options** in the RDP connection window and look for the checkbox **Always ask for credentials**. This option should remain unselected. Ensure this, close the mstsc application and then try launching the connection through Securden.



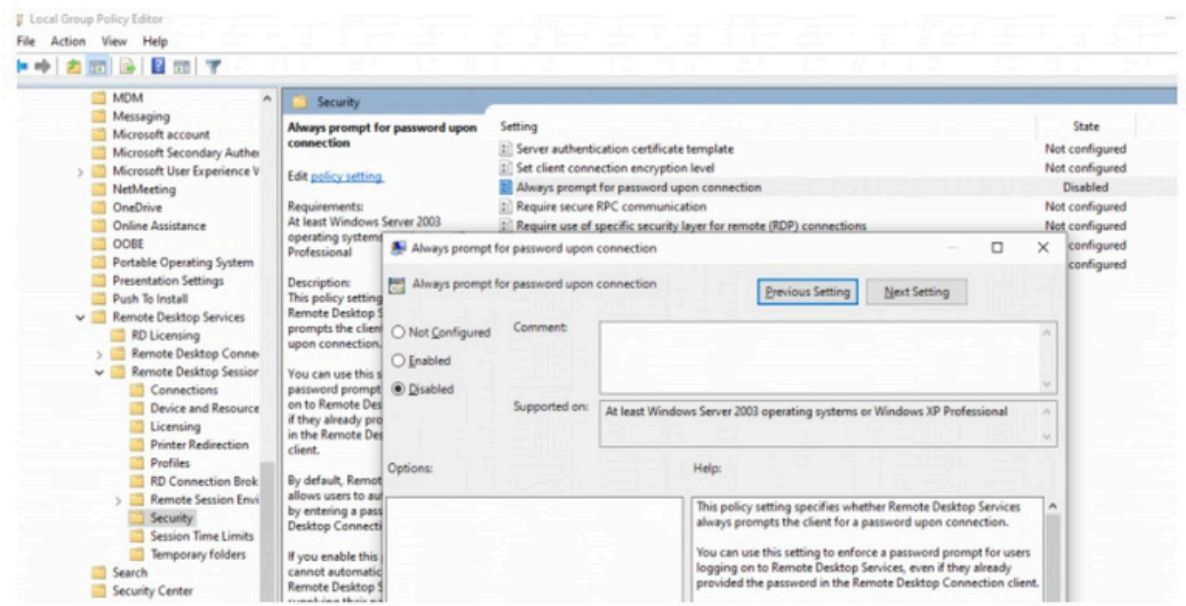
Changes in Default.rdp file - Navigate to the **Documents** (My Documents) folder and look for the **Default.rdp** file in that folder. If the file is present, look for **prompt for credentials: i:1** and change that to **prompt for credentials:i:0**. Save the changes and then try launching the RDP session through Securden.



Group Policy: Always prompt for password upon connection

1. Open **Run** command and open gpedit.msc or gpmc.msc depending on your need.

2. Navigate to **Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Security**. Look for the policy named **Always prompt for password upon connection**.



3. Double-click the policy and **disable** it.

4. Save the changes.

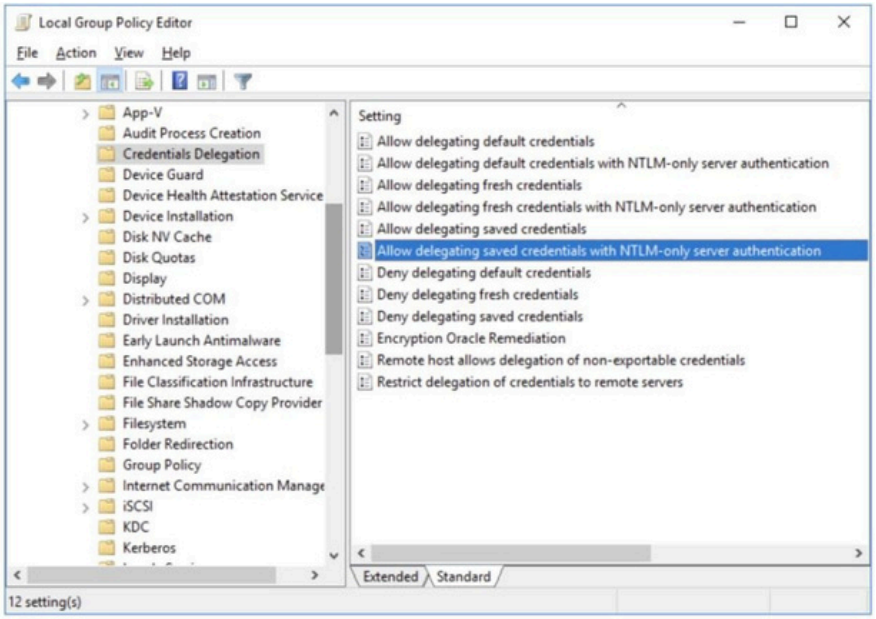
5. If a domain level policy is to be updated, you need to additionally run the command gpupdate/force in the command prompt as an administrator.

Group Policy: Allow delegating saved credentials with NTLM-only server authentication

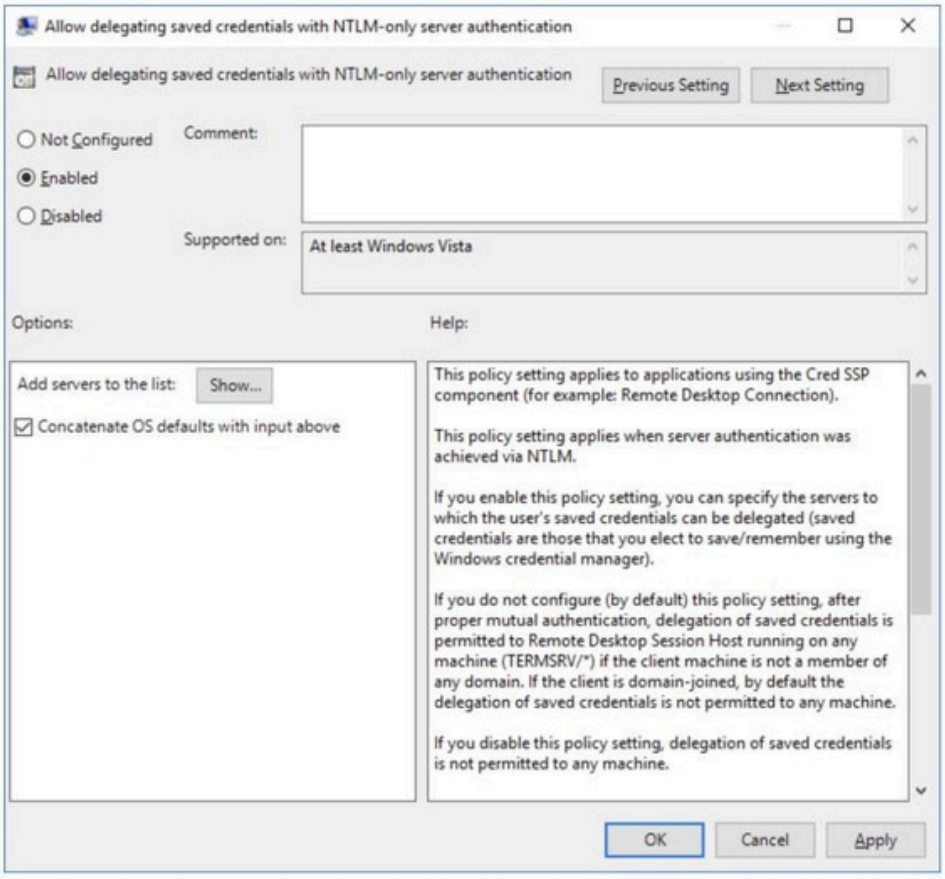
174

1. Open **Run** command and open gpedit.msc or gpmc.msc depending on your need.

2. Go to **Computer Configuration >> Administrative Templates >> System >> Credentials Delegation**. Look for the policy named **Allow delegating saved credentials with NTLM-only server authentication.**



2. Double-click the policy and **enable** it.



3. Click the **Show**... button and specify the list of remote computers (servers) that are allowed to use saved credentials when accessed over RDP. The list of remote computers must be specified in the following format:

A. **TERMSRV/server1** — allow to use a saved credentials to access a specific computer/server over RDP;
B. **TERMSRV/*.securden.com** — allow to establish RDP connection with saved credentials to all computers in the securden.com domain;

C. **TERMSRV/*** — allow you to use a saved password to connect to any remote computer.

5. Save the changes.

6. If domain level policy is to be updated, you need to additionally run the command gpupdate /force in the administrator command prompt.

Group Policy: Deny delegation saved credentials

1. Open **Run** command and type gpedit.msc or gpmc.msc depending on your need.
2. Go to **Computer Configuration >> Administrative Templates >> System >> Credential Delegation**. Look for the policy named **Deny delegation saved credentials**.

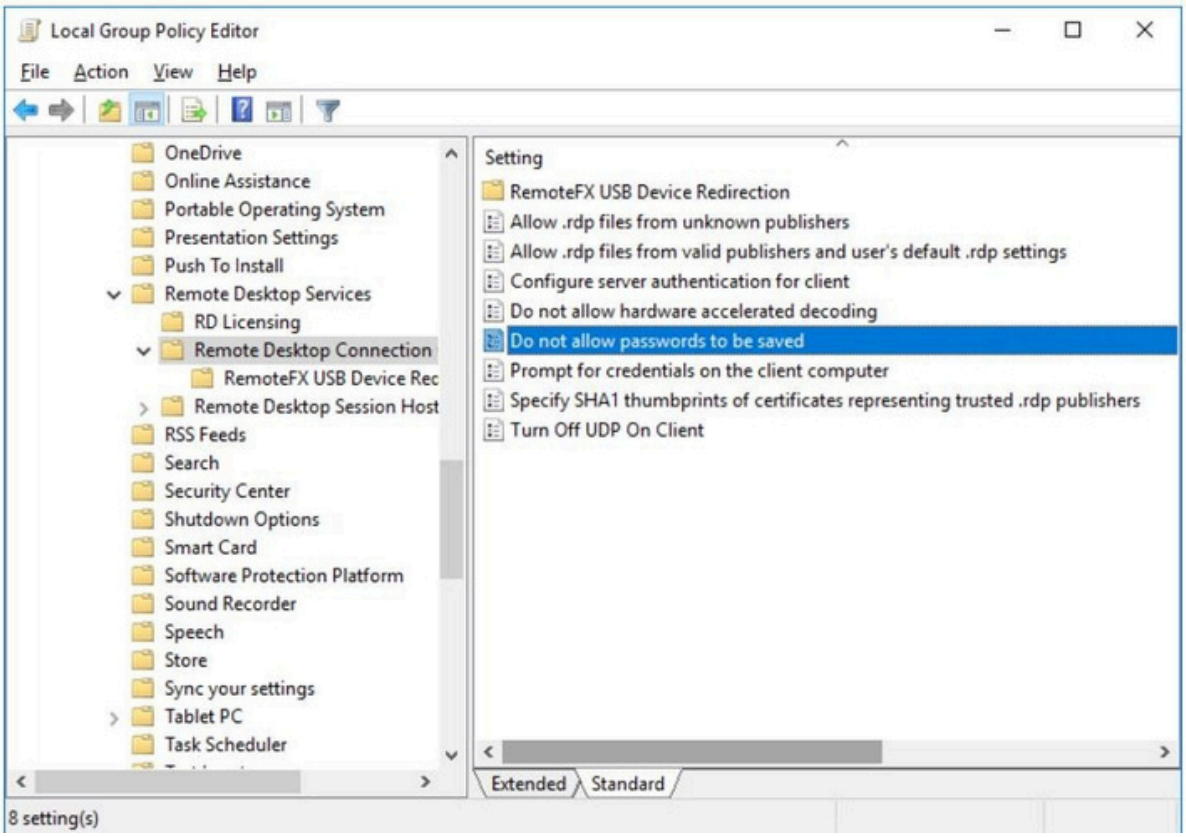
3. Double-click the policy and **disable** it.

4. Save the changes.

5. If domain level policy is to be updated, you need to additionally run the command gpupdate /force in the administrator command prompt.

Group Policy: Do not allow passwords to be saved

1. Open **Run** command and type gpedit.msc or gpmc.msc depending on your need.
2. Go to **Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Connection Client**. Find the policy named **Don’t allow passwords to be saved**.



3. Double-click the policy. **Disable** it.

4. Save the changes.

5. If domain level policy is updated, you need to additionally run the command gpupdate /force in the administrator command prompt.

Group Policy: Network Access: Do not allow storage of passwords and credentials for network authentication

1. Open **Run** command and type gpedit.msc or gpmc.msc depending on your need.
2. Go to **Computer Configuration >> Windows Settings >> Security Settings >> Local Policies >> Security Options**. Look for the policy

named **Network Access: Do not allow storage of passwords and credentials for network authentication**.

3. Double-click the policy and **disable** it.

4. Save the changes.

5. If domain level policy is to be updated, you need to additionally run the command gpupdate /force in the administrator command prompt.

Launching Native SSH connection

The Native SSH connection can be launched via:

- PuTTY
- SecureCRT etc.

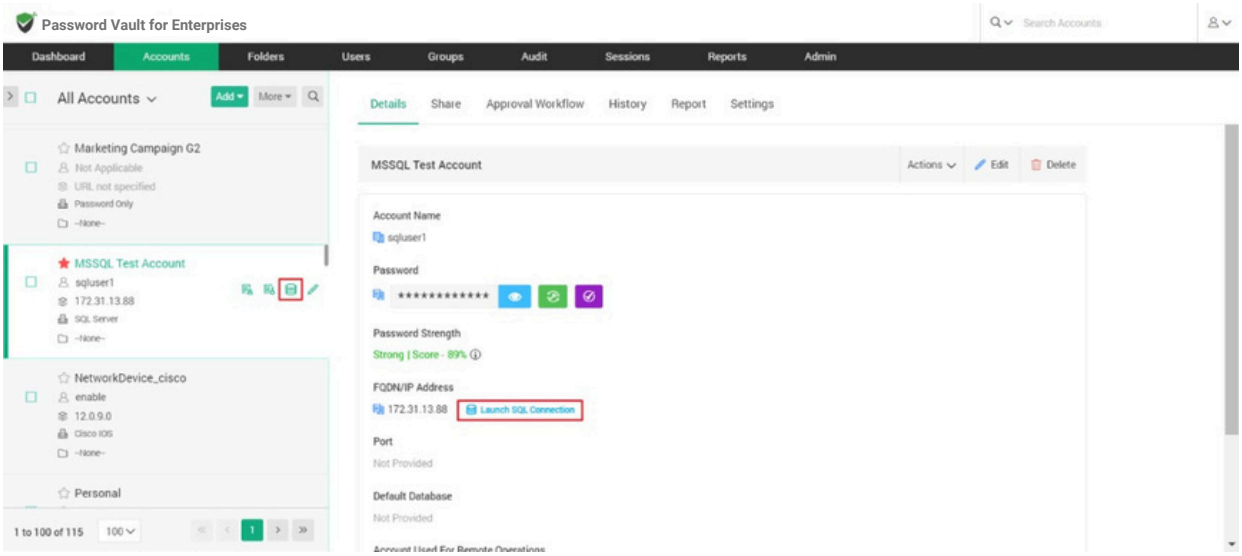
To launch PuTTY and SecureCRT connections you need the Securden Remote Launcher to be installed in the user's machine. The SSH connections are mainly used to connect to machines running Linux, Mac along with routers and other network devices.

Navigate to Accounts section in the GUI, click the required account, click the **Launch SSH Connection** icon appearing alongside the account information on the left-hand side. Alternatively, you can click the remote connection drop-down and launch a native SSH connection of your choice.

Launching Native SQL connections

The SQL connections can be launched to two types of databases, Oracle and MS SQL. All these connections are launched from the machines directly.

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 left-hand side. Alternatively, you can click the remote connection drop-down and launch a SQL connection.



Launching connections to thick application clients

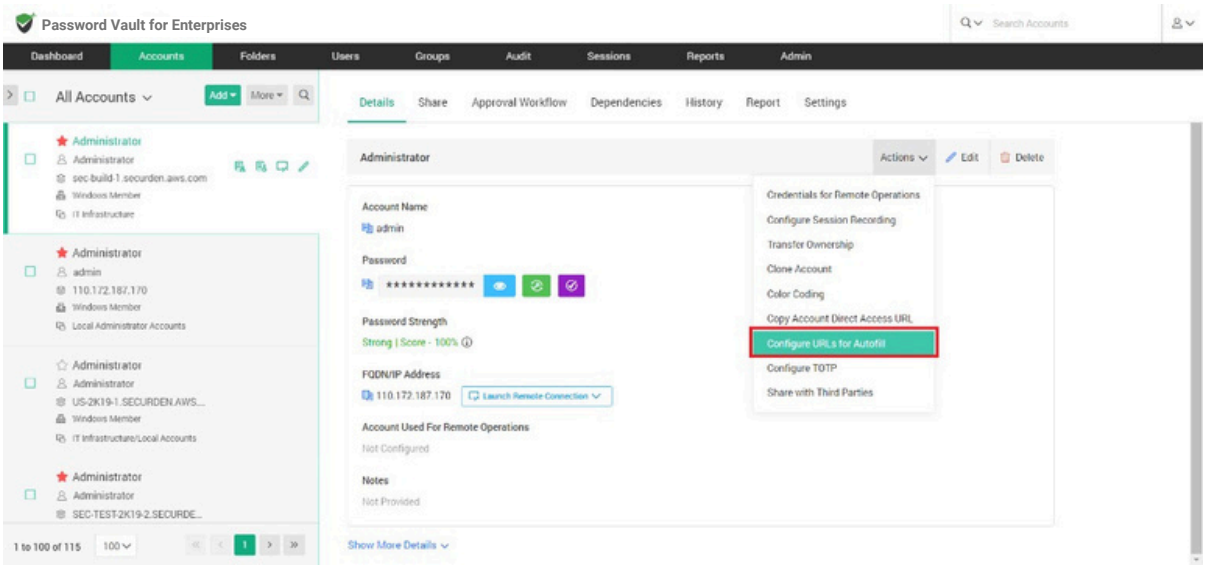
In addition to the default modes of launching web-based connections and through native clients, you can define custom application launchers to supply credentials and automatically launch any application, including thick application clients. Basically, you will be creating a profile for each such

application capturing the input fields as found in the target application. You can configure the profile with placeholders to replace the required values from Securden repository at the time of launching the connections. You need to navigate to **Admin >> Remote Sessions and Recordings >> Custom Application Launcher** and configure the profiles.

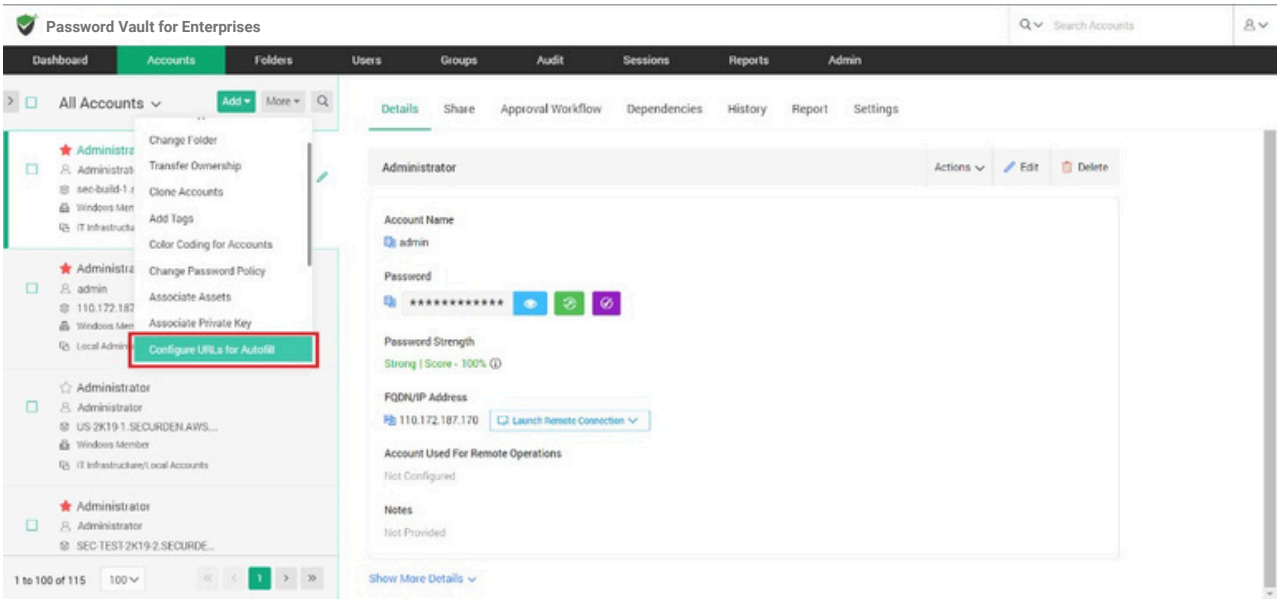
The custom application launcher is explained in detail further in the guide.

Configure URLs for Autofill

This feature lets you fill in the username and password automatically on websites and web applications. To add URLs on which you want to autofill username and password, navigate to **Accounts >> Actions >> Configure URLs for Autofill**.



Alternatively, if you want to add the same URL to multiple accounts at the same time, you may do so by selecting the required accounts from the accounts tab and navigating to **More >> Configure URLs for Autofill**.

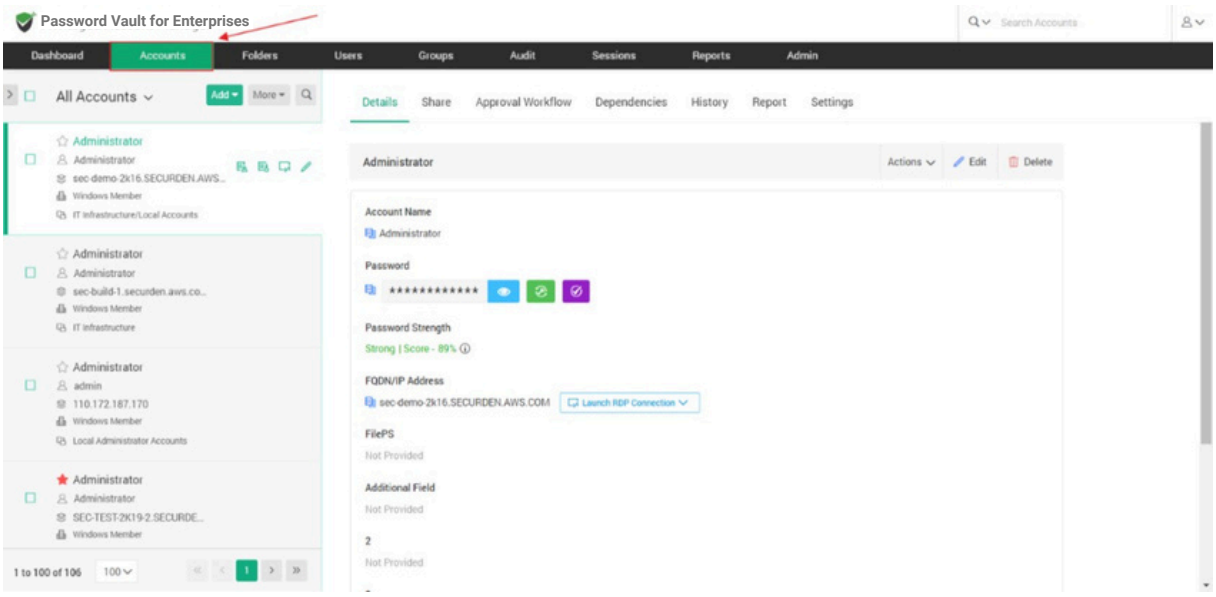


Securden browser extension helps you to autofill usernames and passwords on web applications and webpages. You can specify the URLs on which the username and password should be auto filled. When the user launches a connection to the web application / webpage, the Securden browser extension will auto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

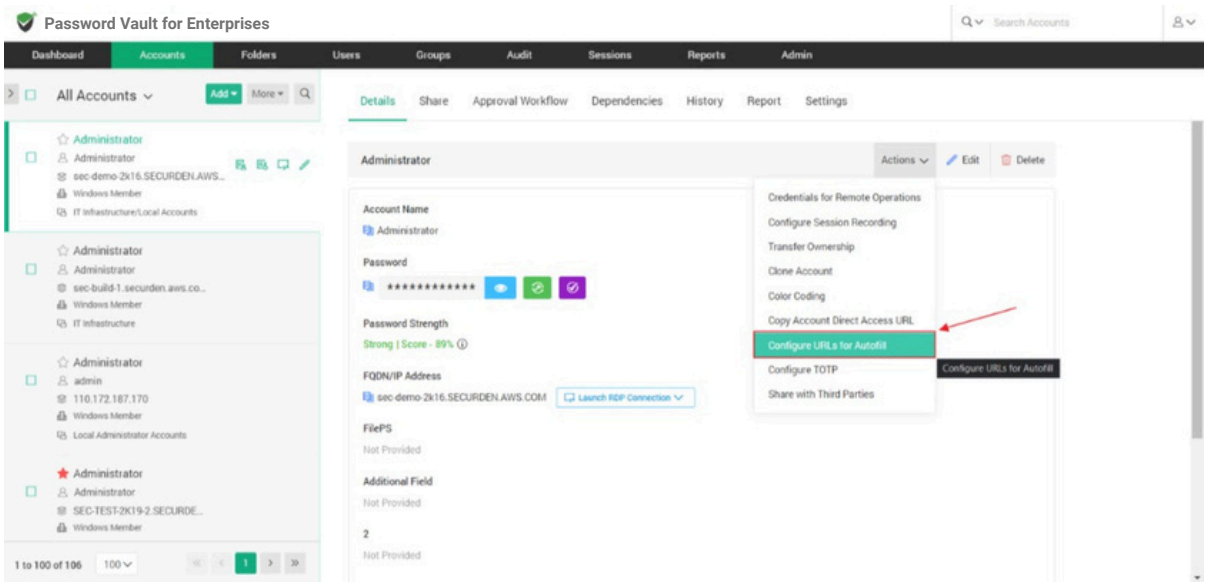
How to Add URLs to Accounts?

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

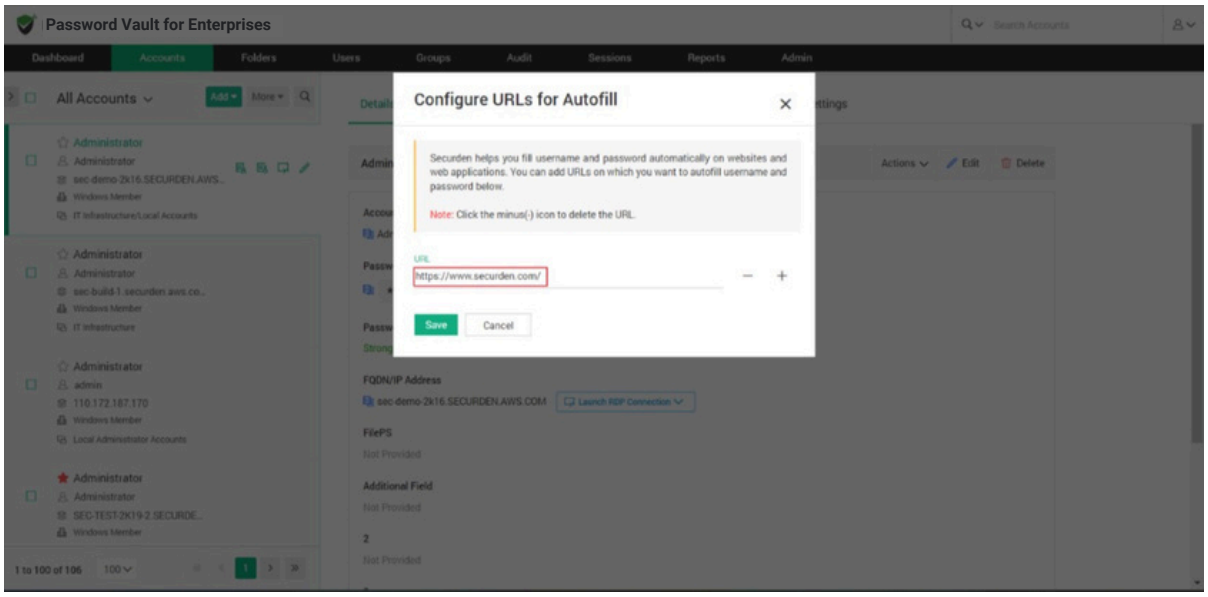
1. Navigate to Accounts tab and select the required account.



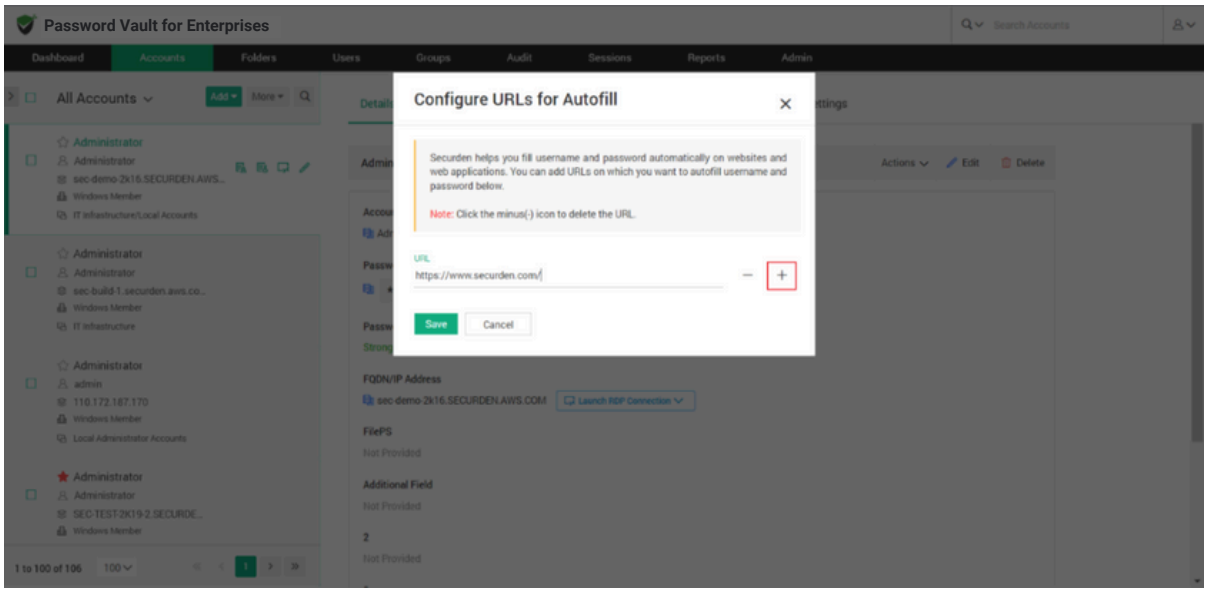
2. In the **Accounts** tab, navigate to **Actions >> Configure URLs for Autofill.**



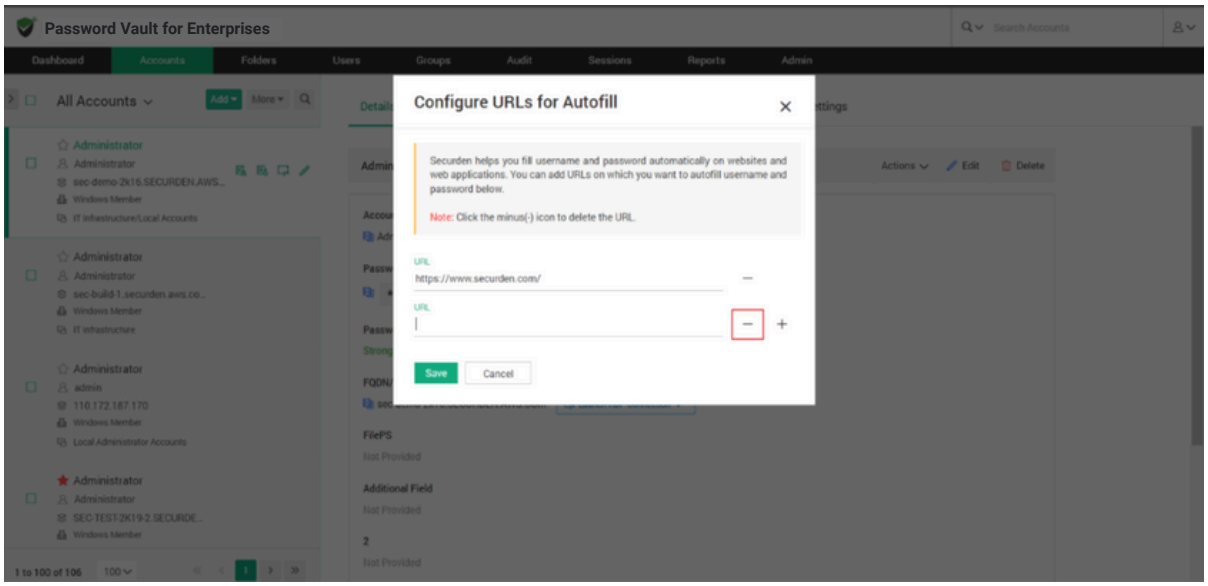
3. In the popup, you need to specify the URL on which username and password should be auto filled.



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.



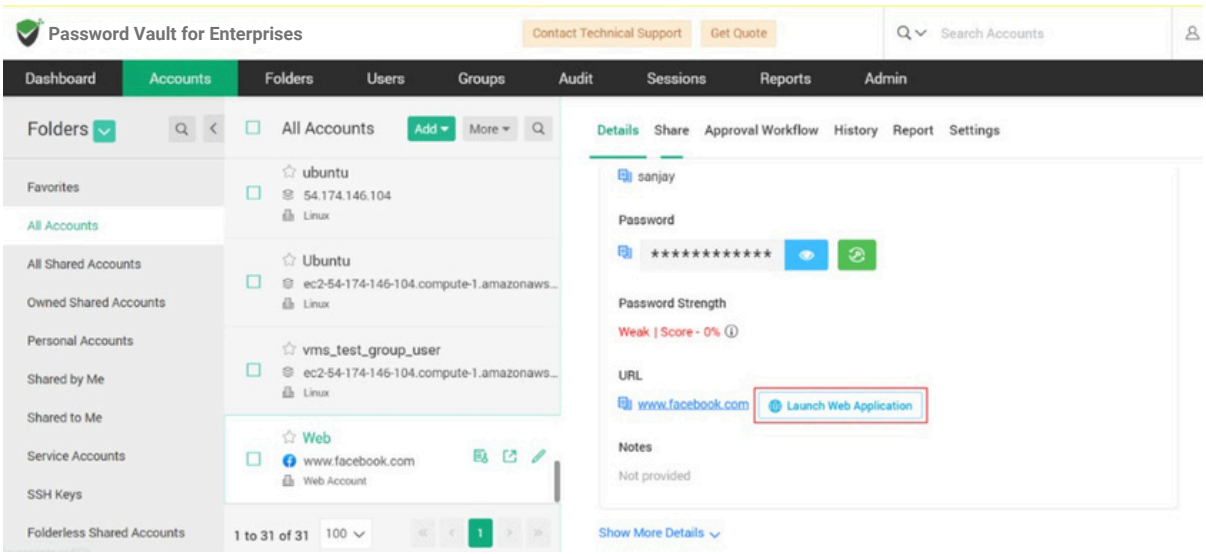
6. Once you have configured all the URLs you want, click **Save**.

How to auto fill credentials on the website?

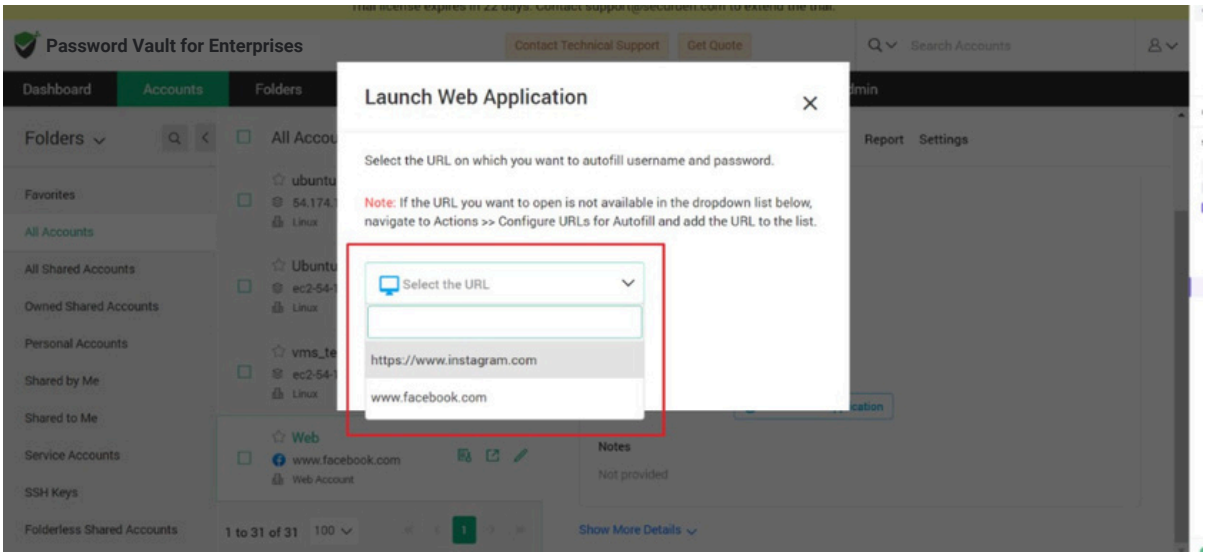
Note: You need to install the Securden Browser Extension on the required browser to be able to utilize the auto fill feature. To install the browser extension, navigate to **Admin >> General >> Browser Extension.**

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.

Managing Access Permissions

Share Accounts with Users / Groups

You can share an individual account with any user(s) and/or user group(s). To share a single account, navigate to **Accounts** section in the GUI, click the required account, click the **Share** tab.

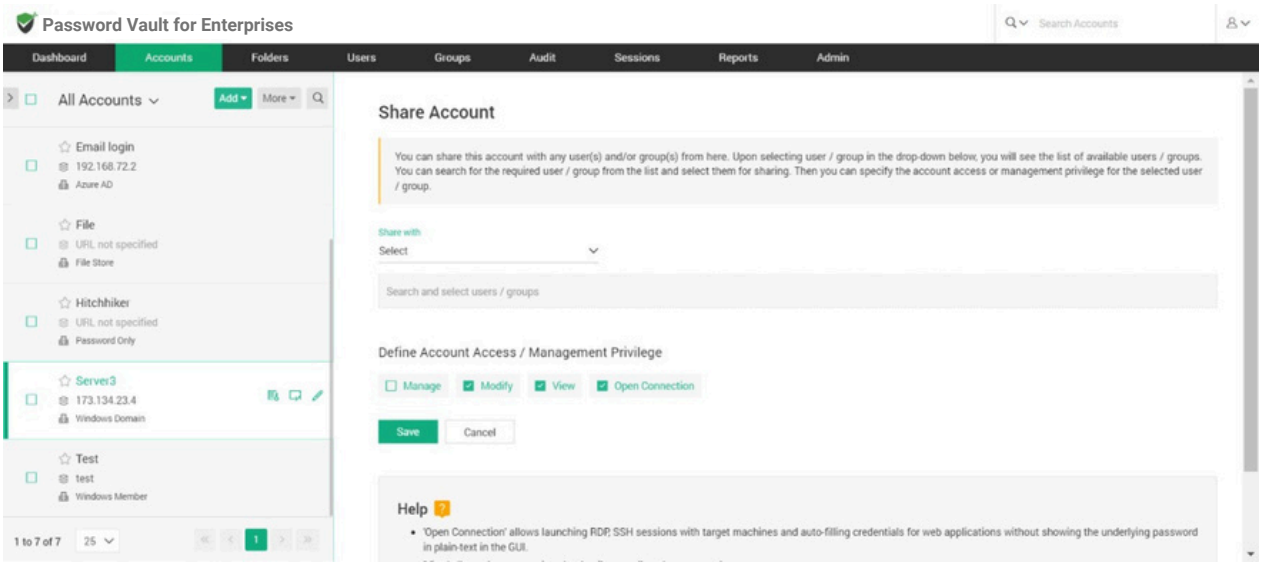
1. You can search and add the users and groups with whom the account must be shared.
2. You can search for either users or groups by selecting User or Group from the drop-down menu named **Share with**.
3. Then you need to choose the required users and groups from the dropdown list.
4. Once you select the users and groups, you need to select the level of access permission they get.

There are four permission levels with which you can share an account:

- **Open Connection** allows launching RDP, SSH sessions with target machines and auto-filling credentials for web applications without showing the underlying password in plain-text in the GUI.
- **View** allows the user to view the details as well as the password.
- **Modify** allows editing the password.
- **Manage** grants all privileges and is like concurrent ownership.

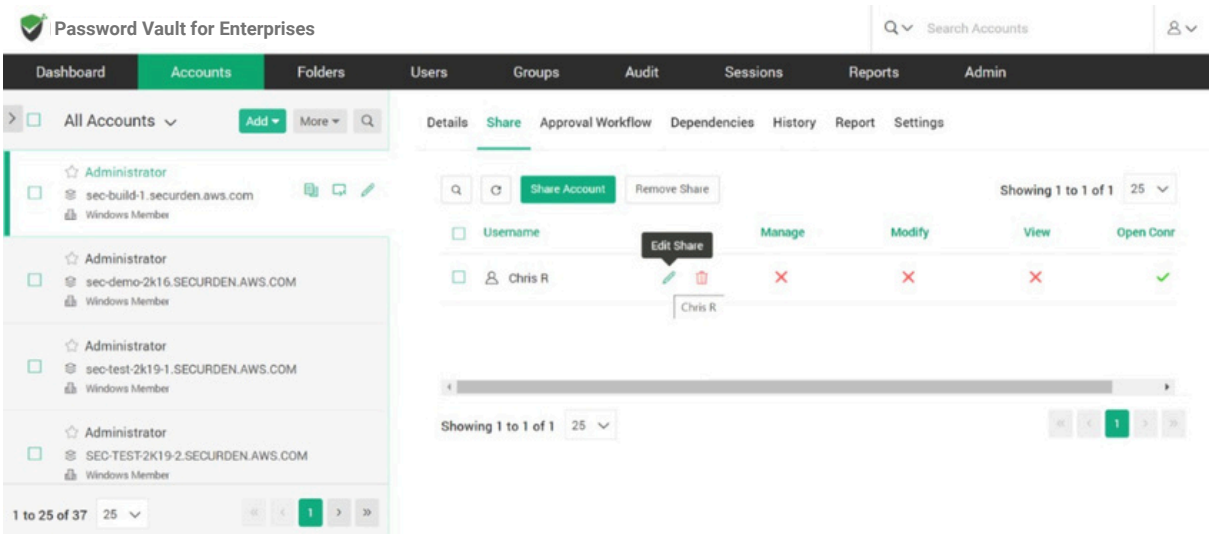
Launching Connections without revealing the Credentials

Securden provides the option to share accounts without disclosing the underlying passwords. You can grant such a permission by choosing **Open Connection** permission while sharing the account. In such cases, users will be able to launch direct connections with the computing resources without knowing the password.



How to modify share permissions?

The granular permissions granted to a user, or a group can be recast in the case of changes in work requirements. This step is a one click process to modify the allotted management privileges. Click on the **Share** tab in the right pane of the **Accounts** section.



Click on the **Username** and to the right of the field, click on the **Edit Share** option. In the window that opens, you can redefine the account access modes by selecting the required permission. Then click on the **Save** button.

How does Securden trace accounts shared at multiple levels?

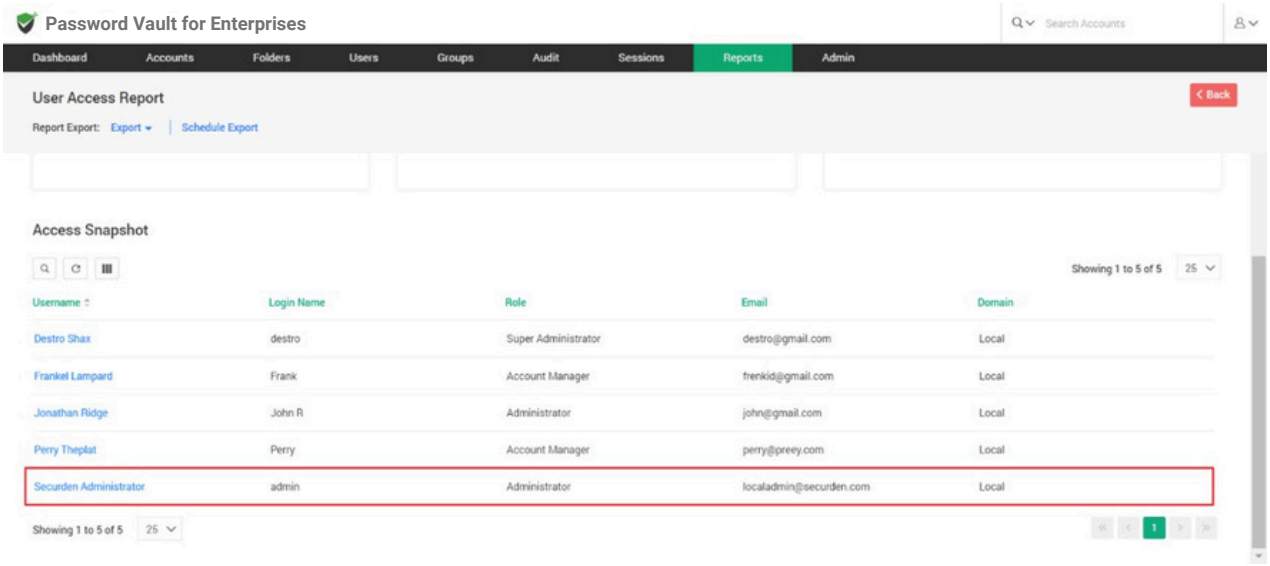
In some instances, an account might be shared to the same user at the user level and at the folder level. When an account is shared at multiple levels, Securden follows the principle of least privilege to assign the required account privilege to a user.

When sharing occurs at multiple levels, at times, you might want to check how the sharing has taken effect – what level of access is a user getting to an account.

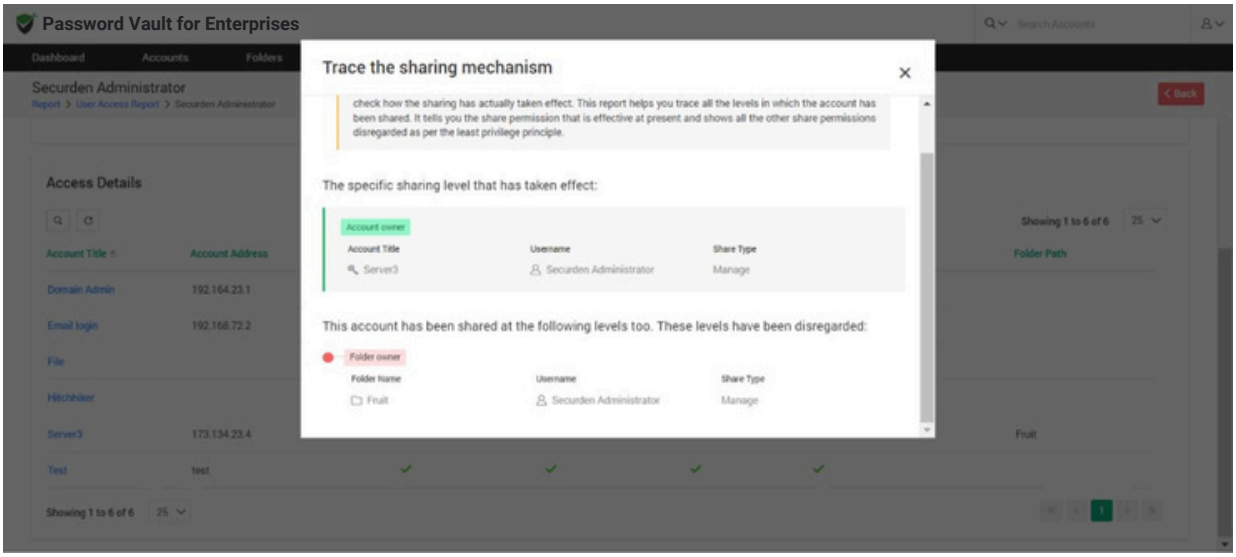
Securden provides a report that helps you trace all the levels in which the account has been shared. It tells you the share permission that is effective at present and shows all the other share permissions disregarded as per the least privilege principle.

You may use **Reports >> User Access Report** (OR) **Reports >> Account Access Report** for this purpose.

If you are taking a User Access Report, click the name of the user who has access to an account you want to verify.



Then click the required account name. You will see a pop-up that shows **Trace the sharing mechanism**.



It will tell you how the user is getting the access. Based on this finding, if needed, you would be able to take corrective action.

Synchronization of Groups in AD with Securden

Let us take an example to understand this feature in Securden. Consider the following scenario:

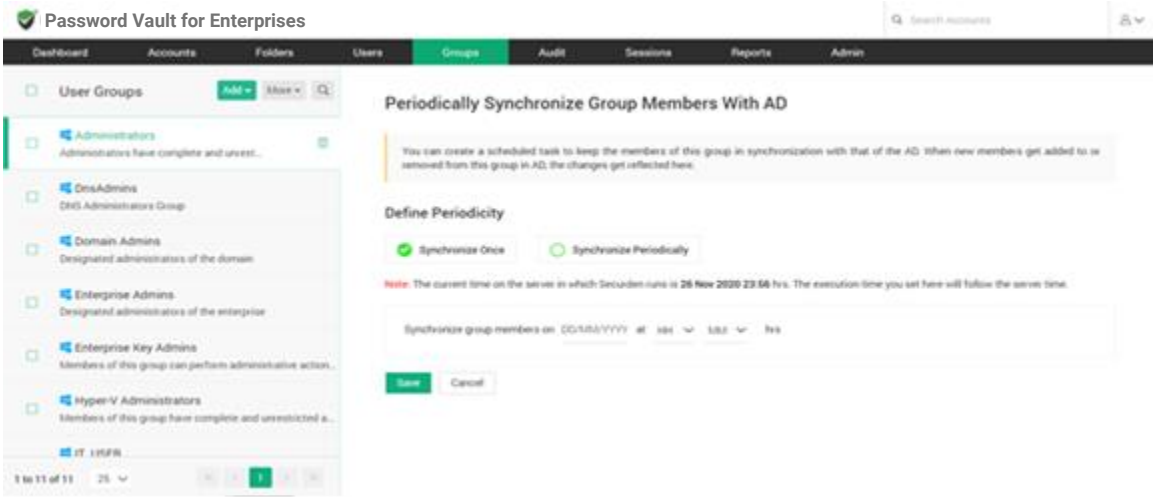
You have shared an account with a group imported from AD. The group originally has only 10 members. A new user is added to the group in AD and now the members total up to 11. Will the 11th member automatically get the access permissions associated with the group?

When a new member is added to a user group in Securden, they automatically gain access to all accounts/resources shared with the group. However, when the user is onboarded in AD and not explicitly added to the group, this cannot be achieved. To fix this, you need to configure periodic synchronization of groups with AD.

You can keep the members of this group in synchronization with that of the AD. When new members get added or removed from this group in AD, the changes get reflected in Securden without requiring any manual intervention.

Navigate to Groups >> Select the required group >> Members >> Schedule Sync section in the GUI to perform this step.

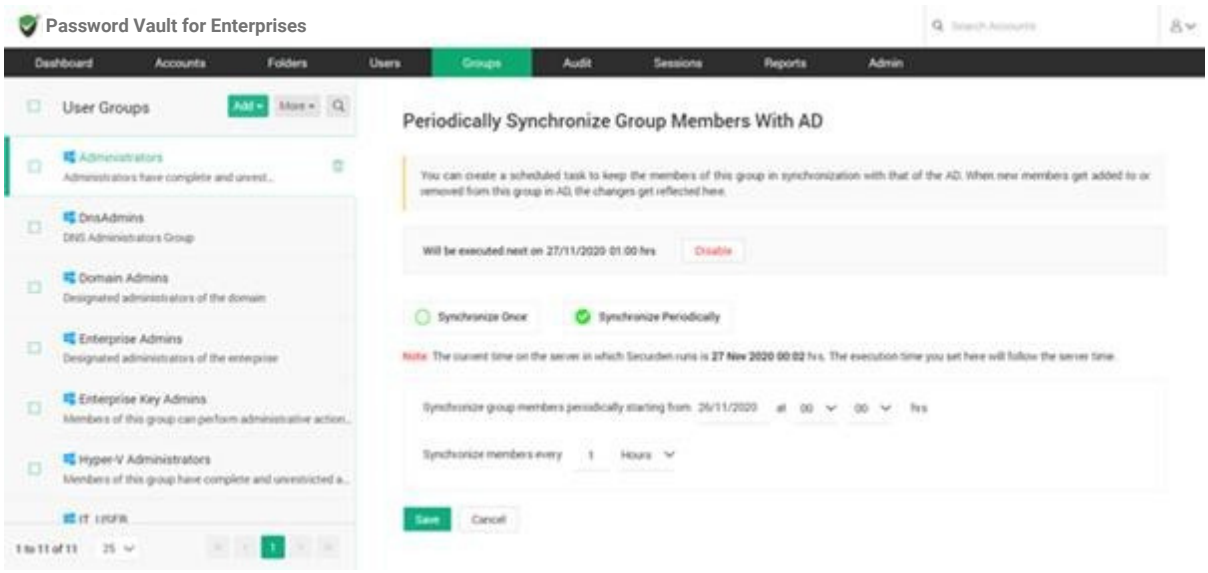
You can either schedule the synchronization activity for a one-time run or create scheduled tasks to run periodically and ensure regular synchronization.



For periodic synchronization, you can choose the start time, and set the synchronization interval.

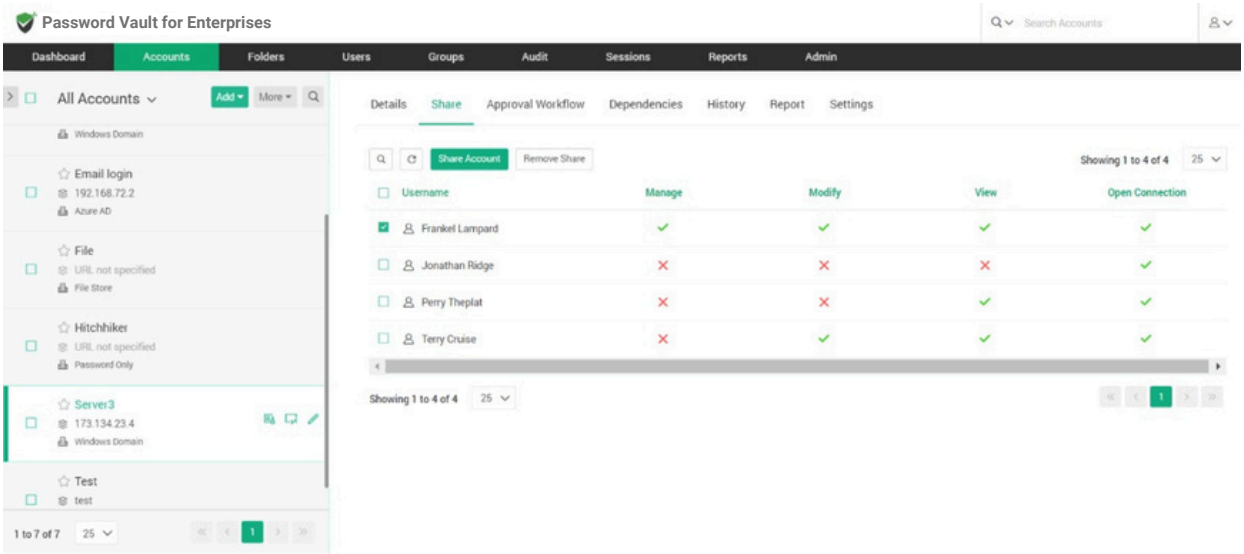
Once enabled, you can navigate to the **Schedule Sync** section to view the next planned schedule.

Once synchronization is configured, whenever a new member is added to a group in AD, the change will be automatically reflected in Securden. Subsequently, all access permissions associated with the group will be inherited by the user.



Remove Share Permission

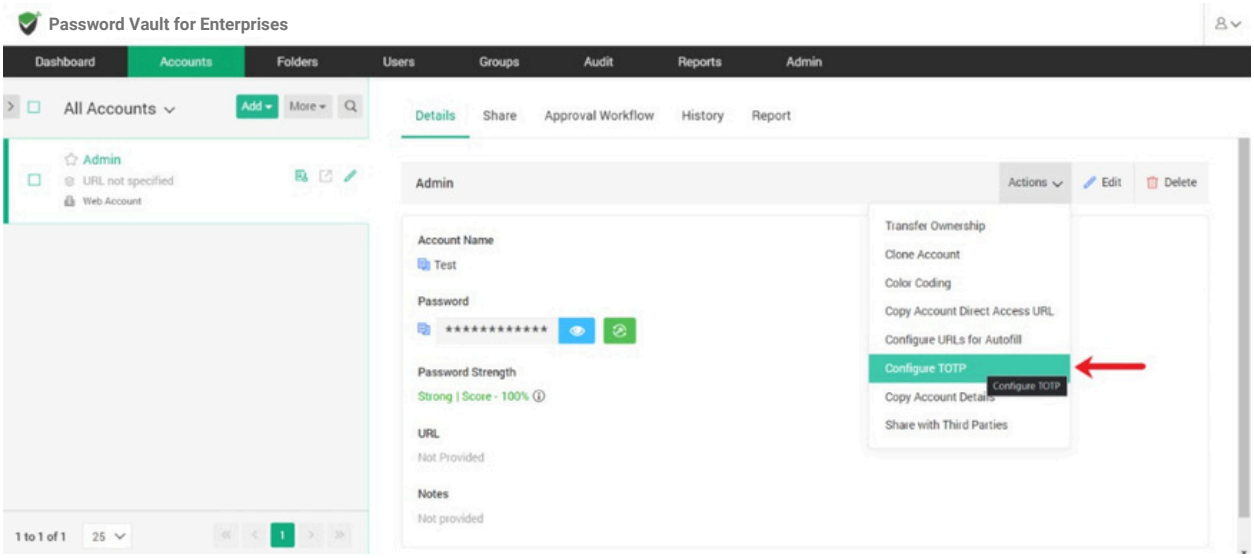
If you want to revoke the share permission from a user or group of users, navigate to the **Share** panel, select the users or groups for whom you want to terminate the account access, and then, click the **Remove Share** button.



Configuring Shared MFA Tokens

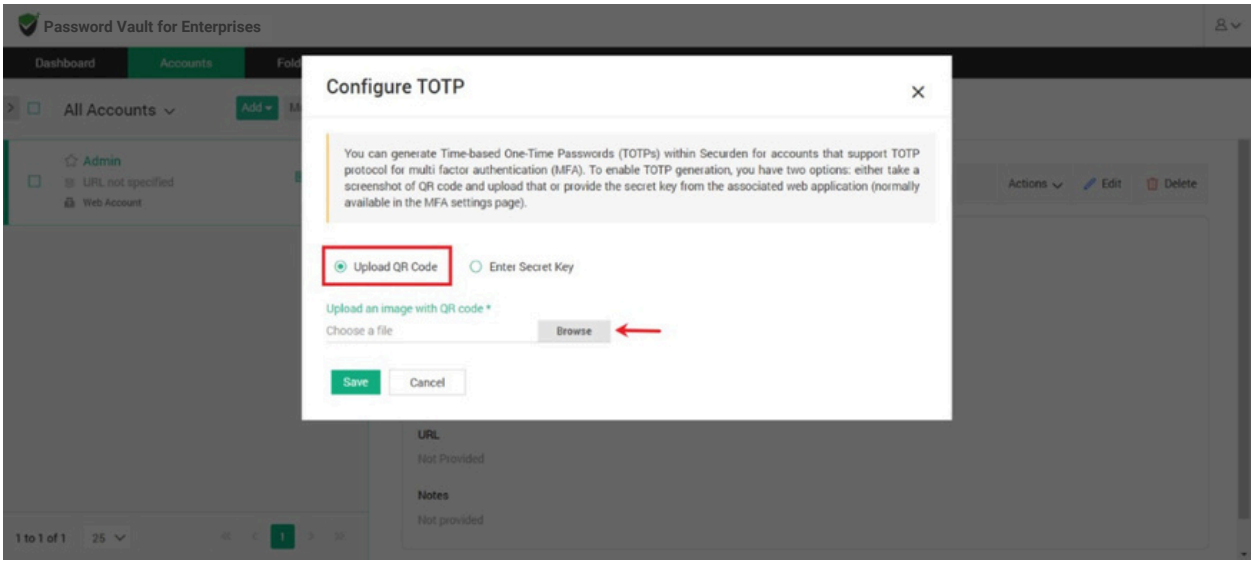
Securden readily integrates with TOTP-generating applications like Google Authenticator, Microsoft Authenticator, and others using either secret keys or QR codes. After integrating, the TOTP will be generated in the Securden interface.

You can share MFA-enabled accounts with users and they will be able to use the displayed TOTP for authentication. To configure TOTP generation in Securden, navigate to **Accounts >> Actions >> Configure TOTP**.

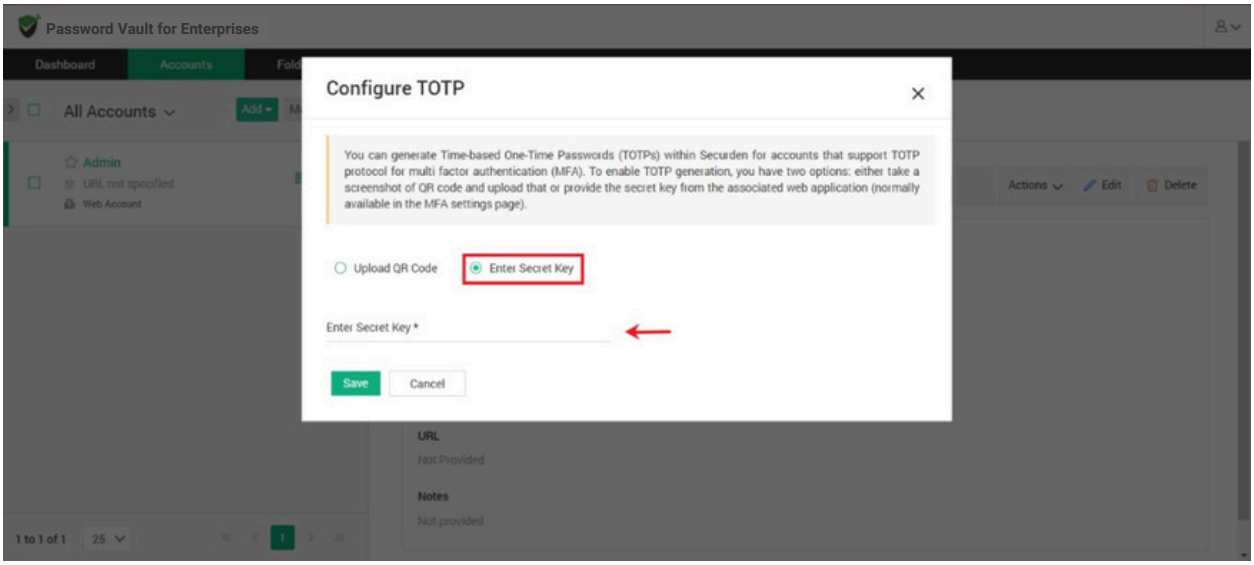


In the window that opens, you need to select between the two options available. You can configure TOTP generation by using either a QR code or the secret key from the MFA application.

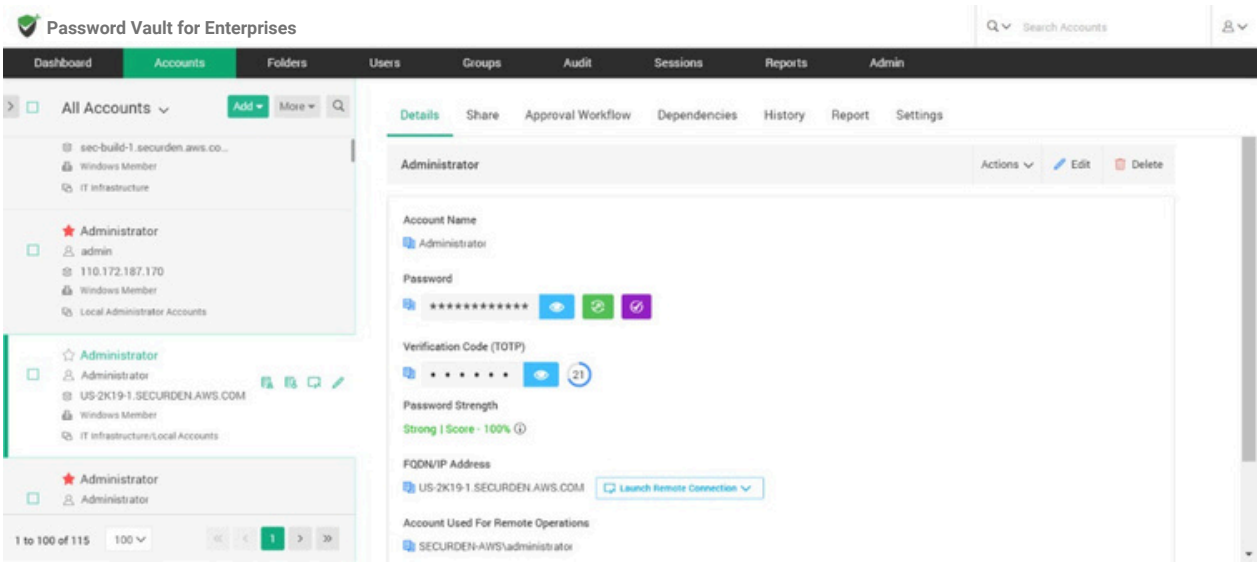
1. If you choose to use a QR code, you need to upload an image containing the QR code. Select **QR code** and click on **Browse**. Select and upload the required image. Click **Save**



2. If you choose to use a secret key, you need to find and obtain the secret key from the MFA app. Select **Enter Secret Key** and input the secret key. Click **Save**.



Once TOTP generation is configured, your TOTP will be generated and displayed in the accounts tab.



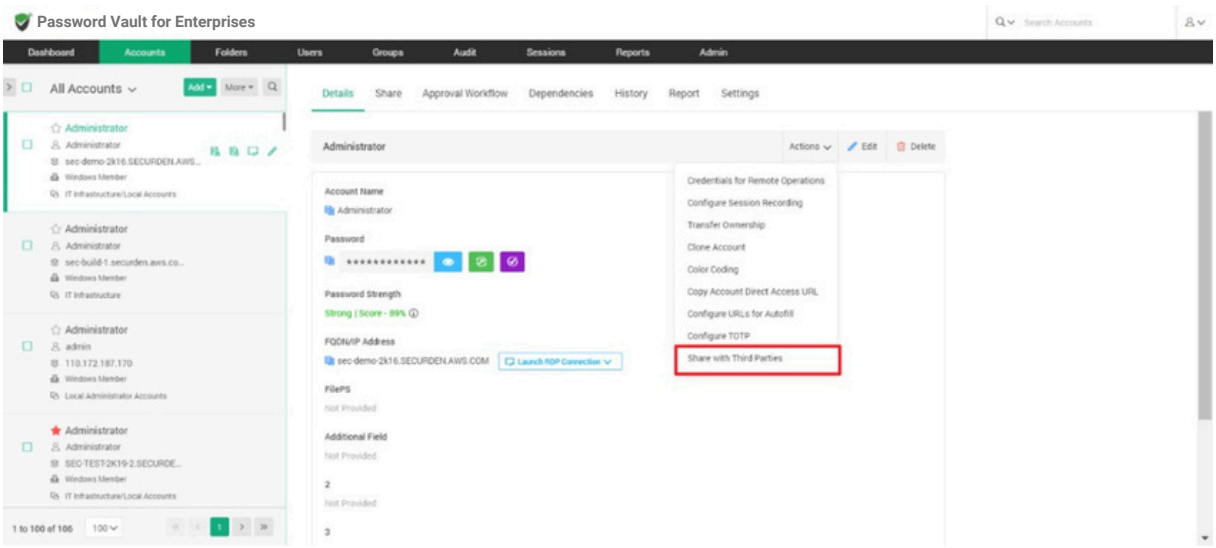
When you share the account with a user or a group, the associated TOTP will be shared alongside the credentials.

Share Accounts / Passwords with Third Parties

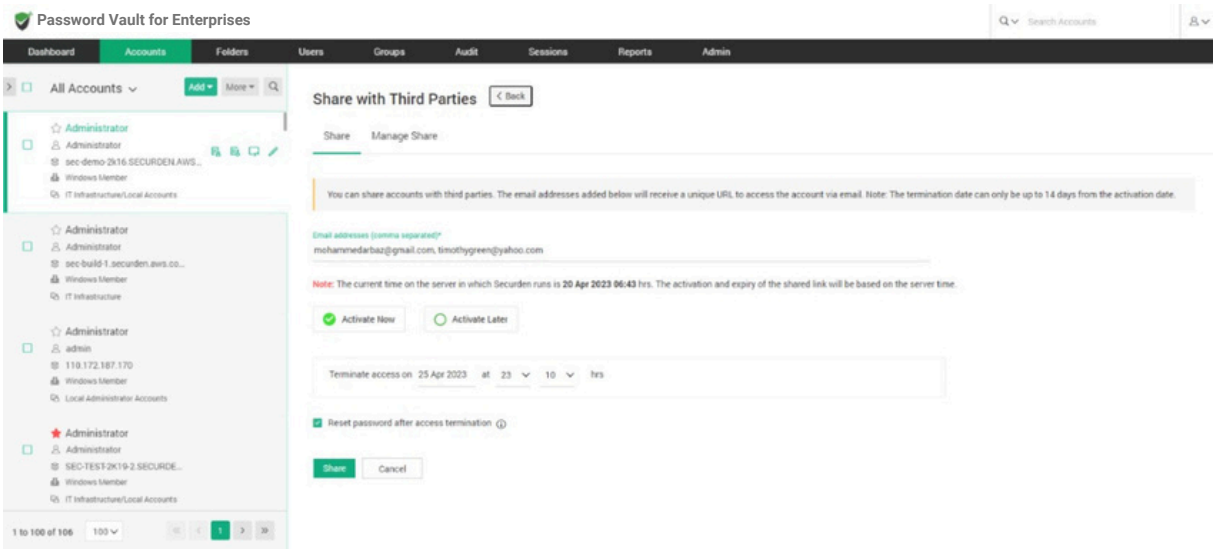
Any user in Securden can share accounts owned by them/shared with them to a third-party user outside the organization. They need the email addresses of the third parties who need access to the account.

Pre-requisite: 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 >> Actions >> Share with Third Parties**



This opens the GUI shown below:



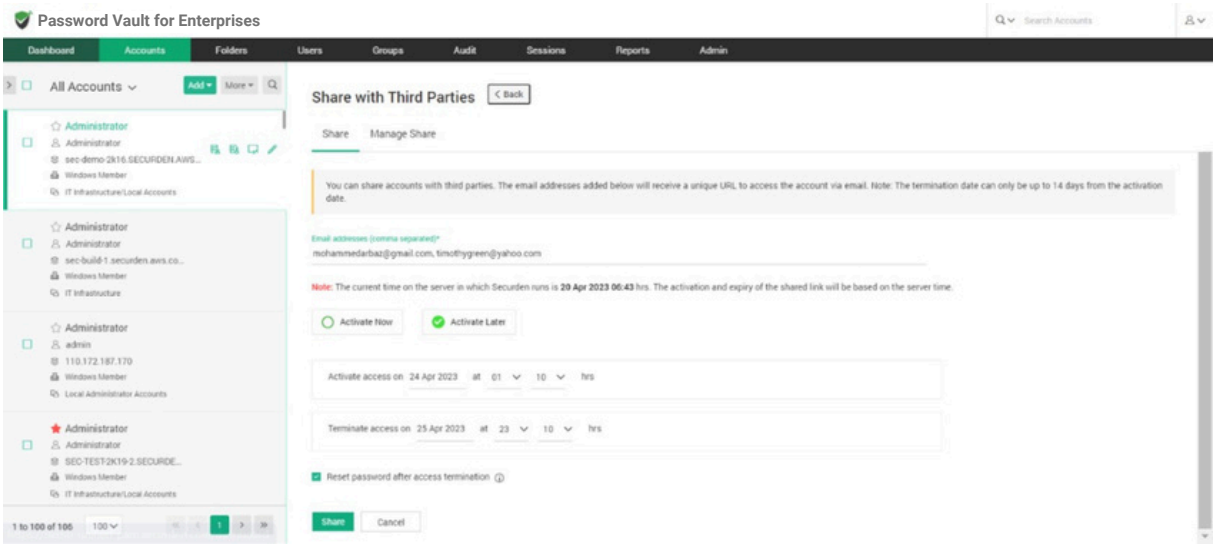
Each account is shared with an access timeframe to the third-party users. You need to specify the following details before sharing the account:

- **Email addresses:** You need to specify the email address of the third-party user. If you are sending this account to more than one

recipient, you must 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.

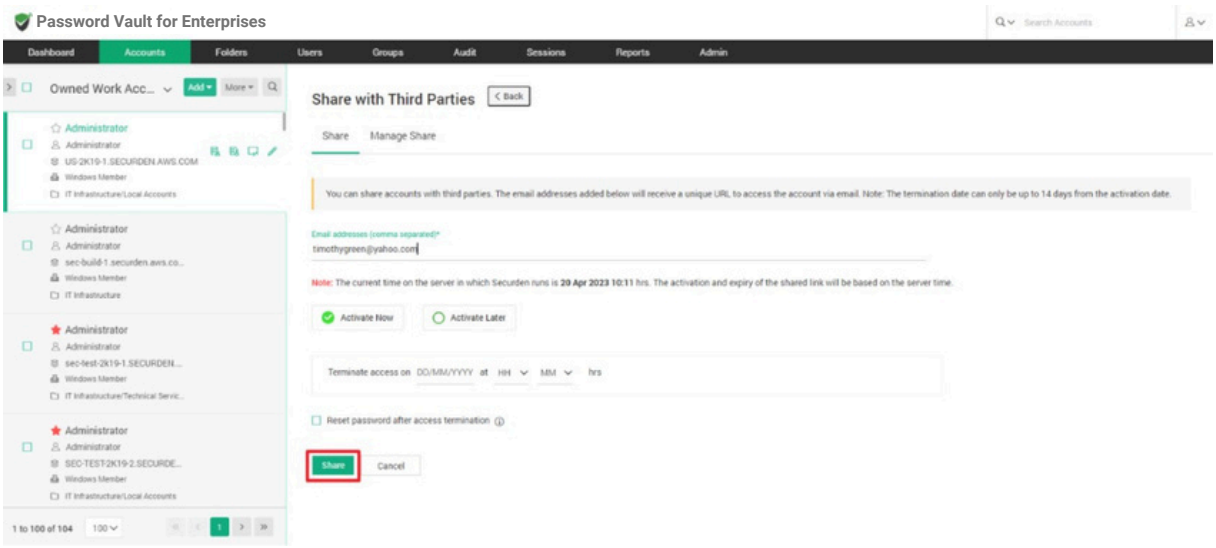
• **Activate Later:** You can select this option to allow the third party to access the account at a specified date and time.



• **Terminate access:** You must 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.

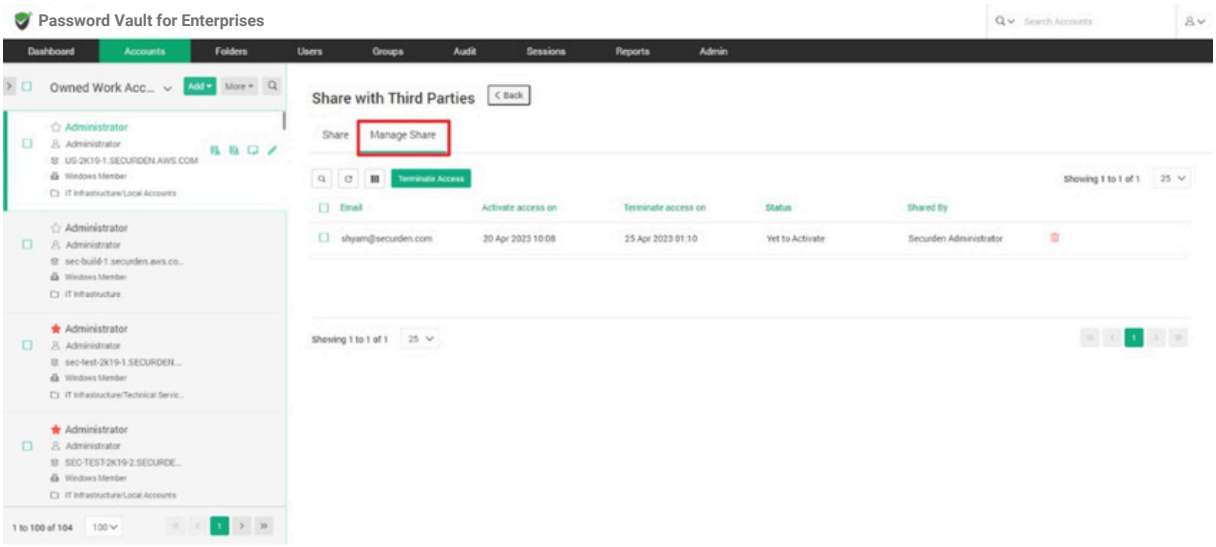
• **Reset password after access termination:** Enabling this checkbox will ensure that the password of the remote machine is changed after the third-party access is revoked.

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.



Terminating Third Party Access

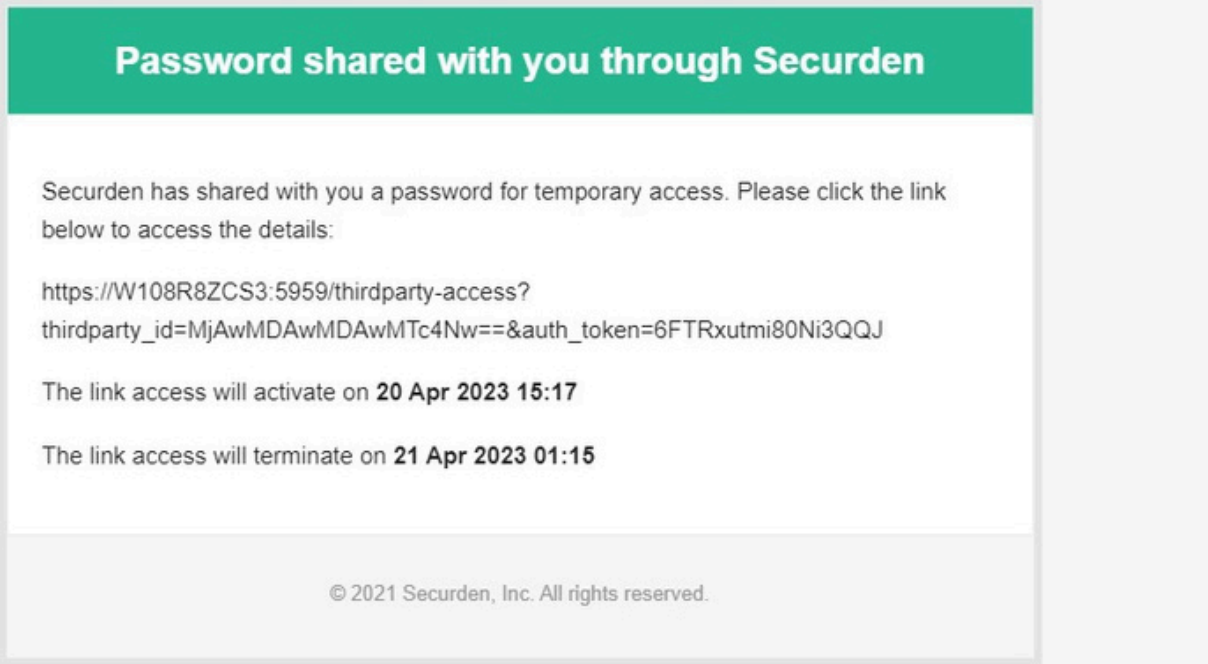
You can see which external users have shared access to this account from the Manage Share tab.



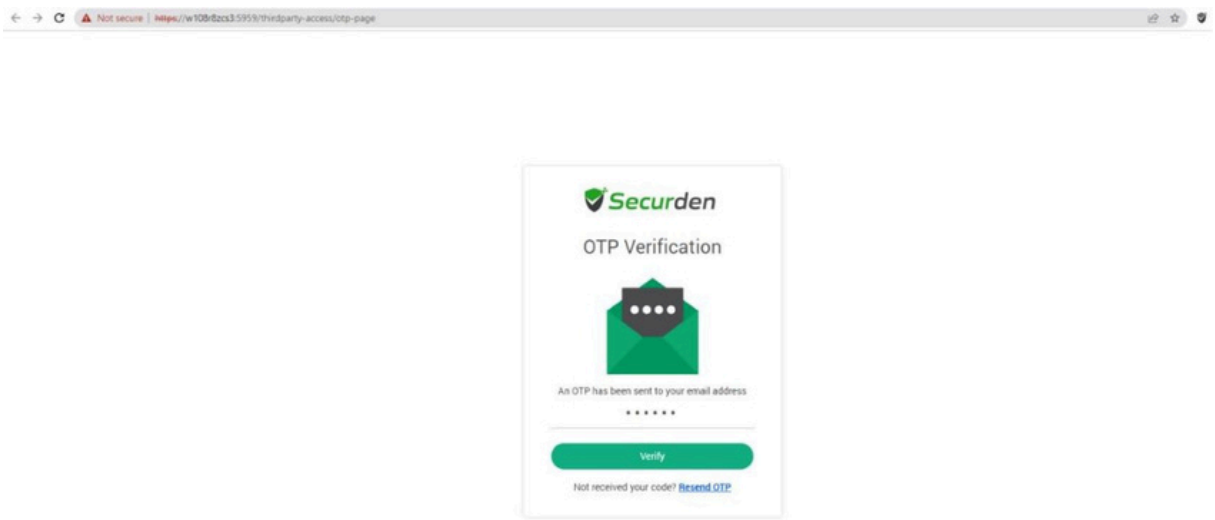
If required, you can select the email of the user and **Terminate Access** to the account. This will end their access regardless of the time-duration defined.

How external users access the shared account

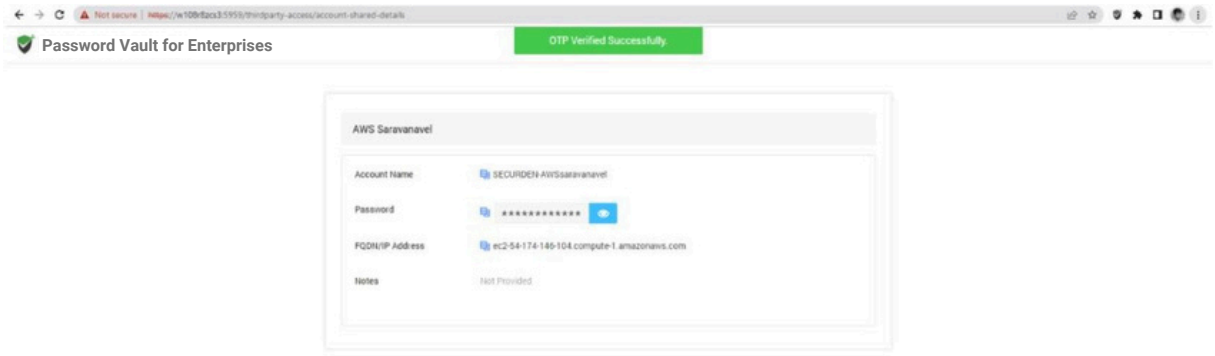
The external user who receives the shared account will find a link in their email id as shown below.



Upon 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.



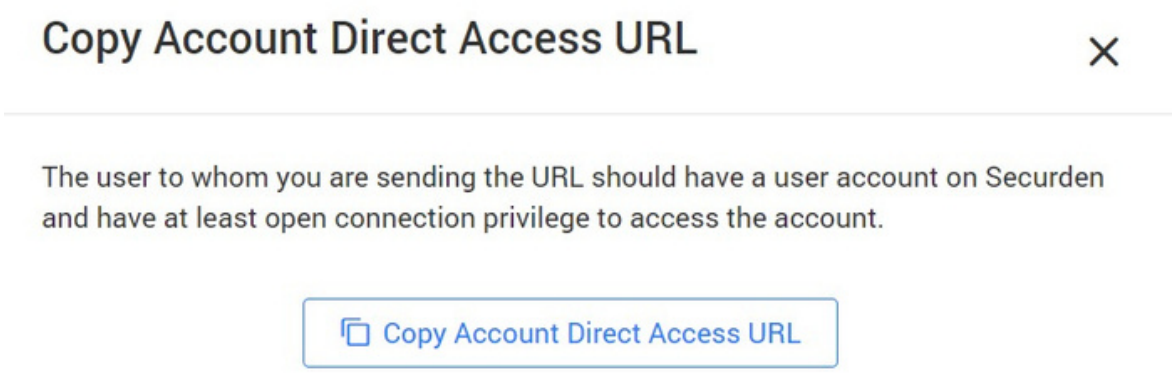
They can click the **View password (eye icon)** to see the hidden password.

When the duration of access expires, the account access is revoked, URL becomes invalid, and the password of the machine is reset.

Copy Account Direct Access URL

You can share the account to a user with a direct access URL. The user to whom you are sending the URL should have a user account on Securden and have at least an open connection privilege to access the account.

Navigate to **Accounts >> Details >> Actions >> Copy Account Direct URL**



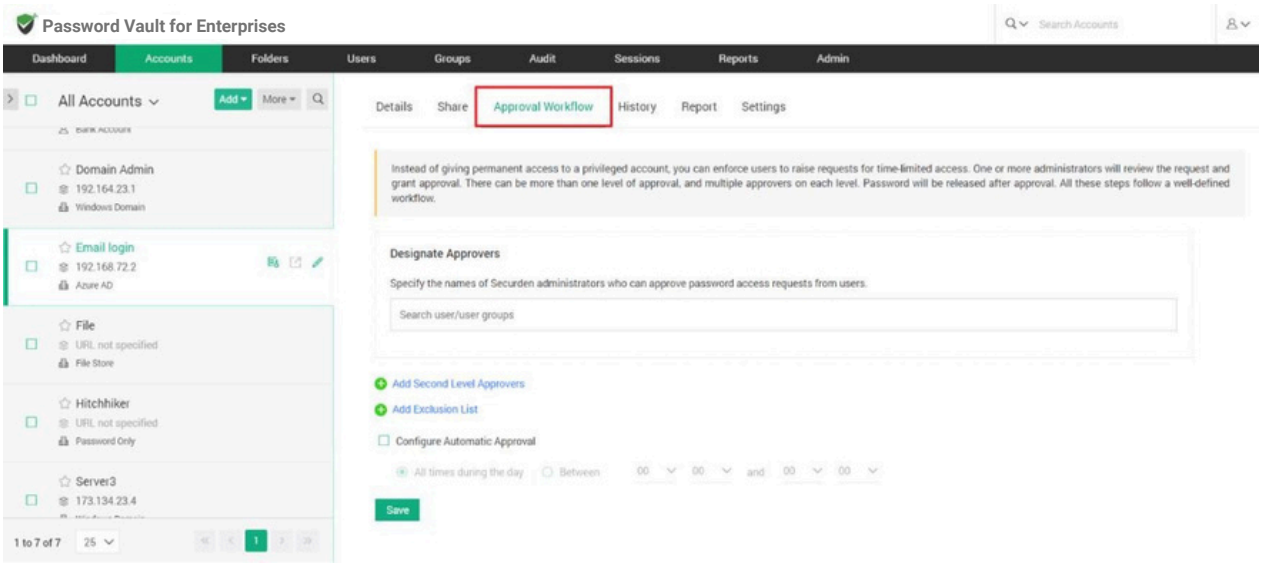
Just-in-time Access through Approval Workflows

You can establish an additional layer of security for sensitive accounts by enforcing your users to go through approval workflows. This also serves as 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** and 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, etc.

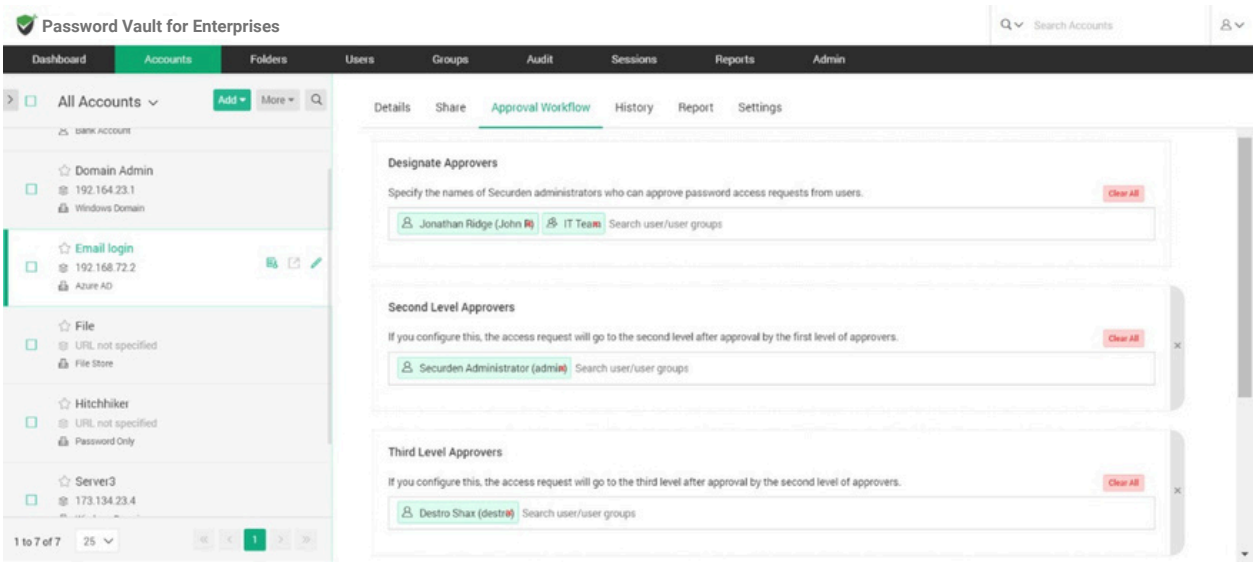
Configuring approval workflow

Navigate to the Accounts section in the GUI, click the required account, click the **Approval Workflow** tab in the right pane.



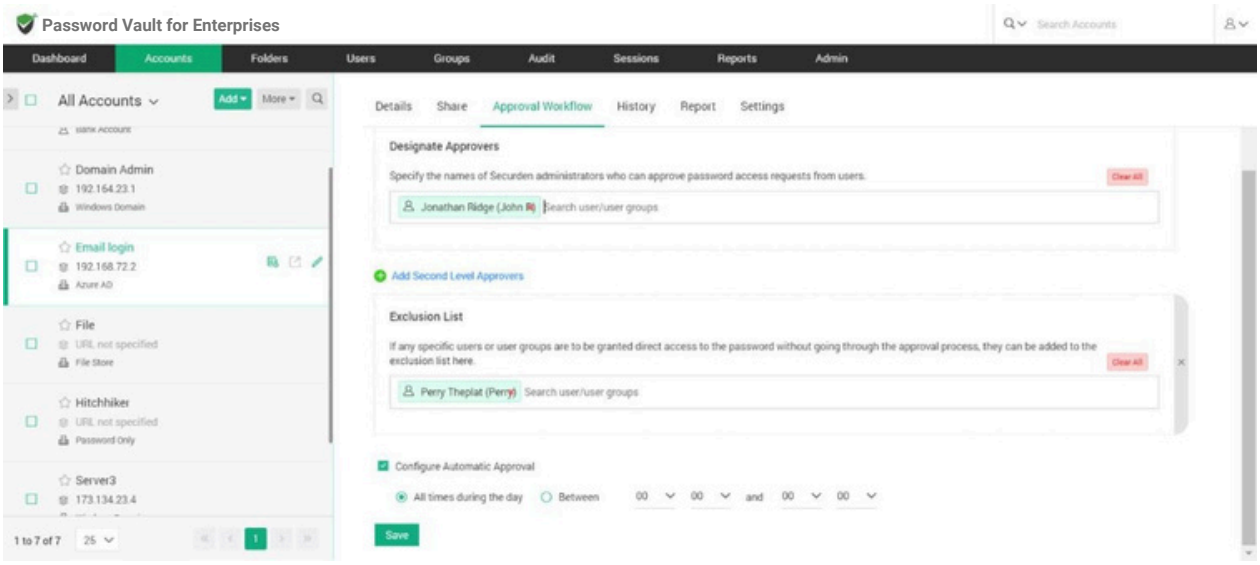
Designate Approvers

Securden lets you designate up to 3 levels of approvers for each account. You need to specify the names of the users/user groups who can approve the password requests for the selected account.



Exclusion List

If you wish to exclude certain users from going through the approval workflow to gain access to the account, you can specify the user/user group under the exclusion list. The added users will be granted direct access to the password.



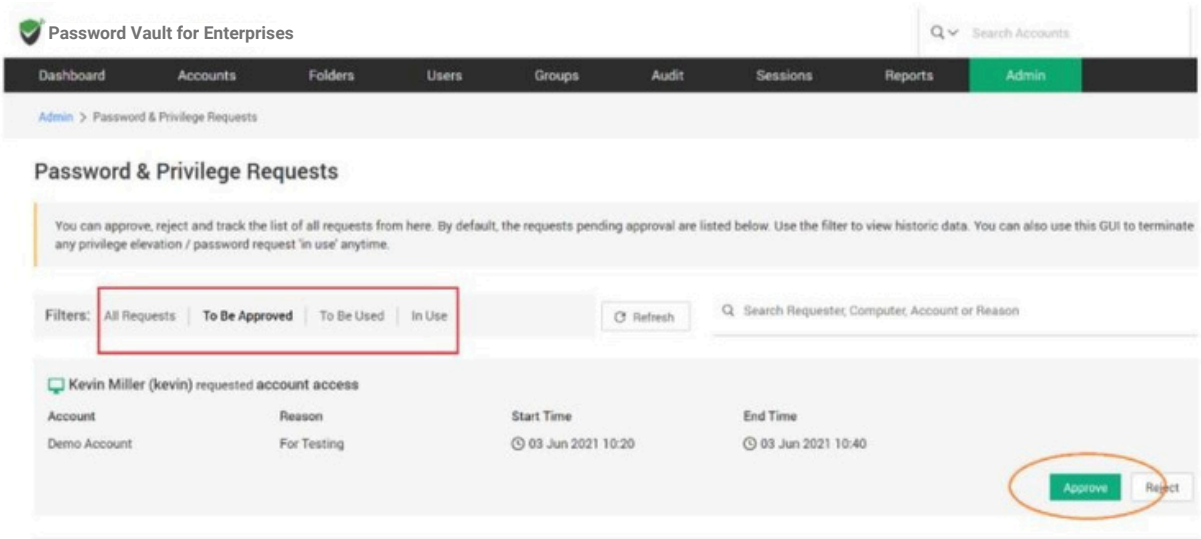
Configure Automatic Approval

If you have certain working hours where you want to allow users to get instant access to an account bypassing the approval workflow, automatic approval of access request can be configured. You may specify the time interval in which all access requests will be automatically approved.

Managing Access Requests

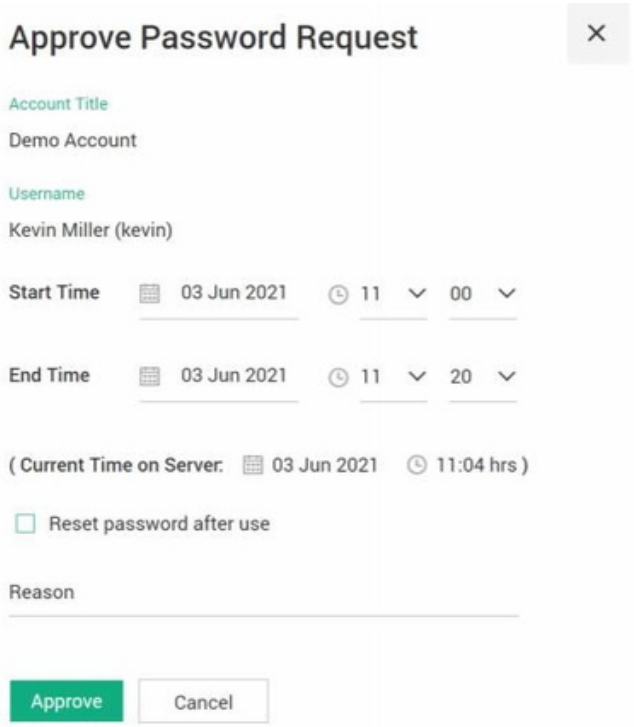
Navigate to **Admin >> Approval Workflow** section in the GUI. You will receive notifications through email when someone raises a request.

- Before verifying the request, you may also verify the justification provided by the requester. If it is satisfactory, you can go ahead and approve.



- When approving, you have the option to approve it **as it is** for the time duration requested by the user OR you can grant access at any time duration you deem fit. You may also record your comments in the **Reason** field for reference in the future.

- You also have the option to randomize the underlying password after use by the user by selecting the option **Reset Password After Use**.



- Once you approve the request, the entry moves to the **To Be Used** section. That means the user is yet to start using the access.
- Once the user starts using the access, the entry moves to the **In Use** section.
- Even after approving a request, you can still control and edit access parameters irrespective of the entry being in the **To Be Used** or **In Use** section.
- You can terminate ongoing access from the **In Use** section by clicking on the **Revoke Access** button.

Important Note:

• Once a user starts accessing the application after receiving approval, concurrent controls kick in. No other user, including the administrator, super administrator, and account owner, would be able to access the application until the access is surrendered or terminated, or expired. If another user attempts to access the account in use, they will see the message **In exclusive use by another user**.

- If the periodic password reset is configured for an account and at the time of the reset execution the account is used by a user, in this scenario the password reset task will not be executed for the account.

Accounts Report

This section details all the usage, access, and activities related to a particular account and depicted in the form of reports. The reports can be downloaded in the form of PDF, CSV, and XLSX.

Details that the report captures:

Password usage statistics - Data shown here includes password retrievals, remote connections launched and password auto-fills on websites.
Account usage statistics – The data in this report highlights the number of times the selected account has been used and by which user.
Access Details – A list of all the users who had accessed the account.

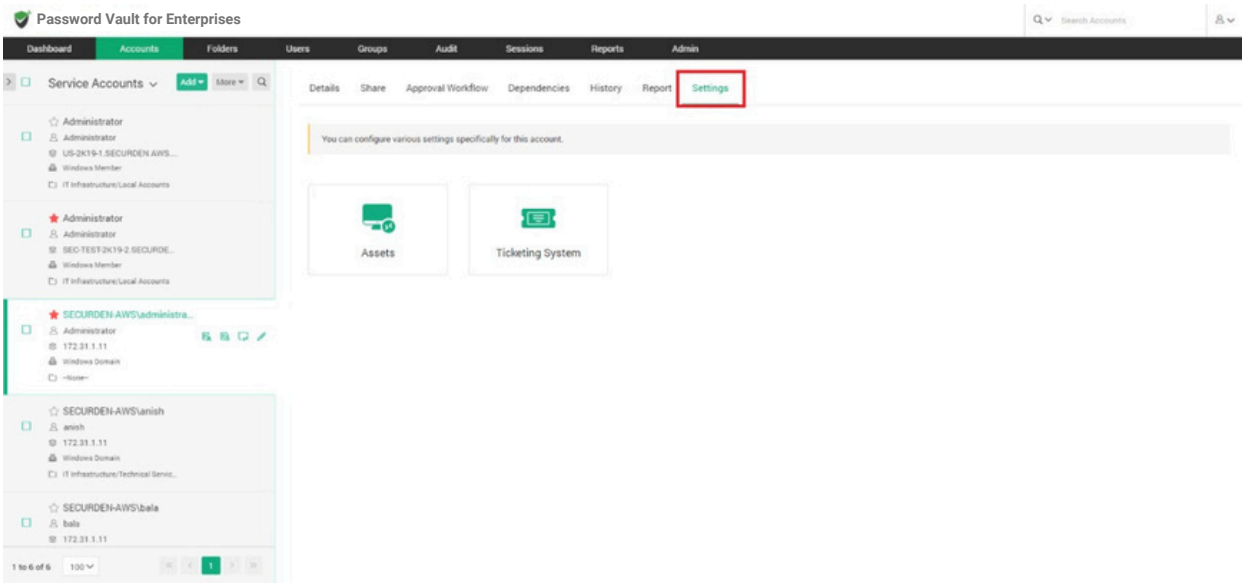
Account Activity – Lists out all the activities performed on the account by users.

Export Report – Export the account report in PDF, CSV, and XLSX file formats.

Note: If you choose to view a consolidate list of who has access to a particular account or activities performed on any particular account, navigate to **Reports >> Account Access or Reports >> Account Activity.** You will get a complete summary of all account related details and you can create a scheduled task to periodically export the report in PDF or CSV or XLSX format. The link to download the report will be emailed to the specified recipients.

Account Settings

This section lets you configure various settings specifically for an account.

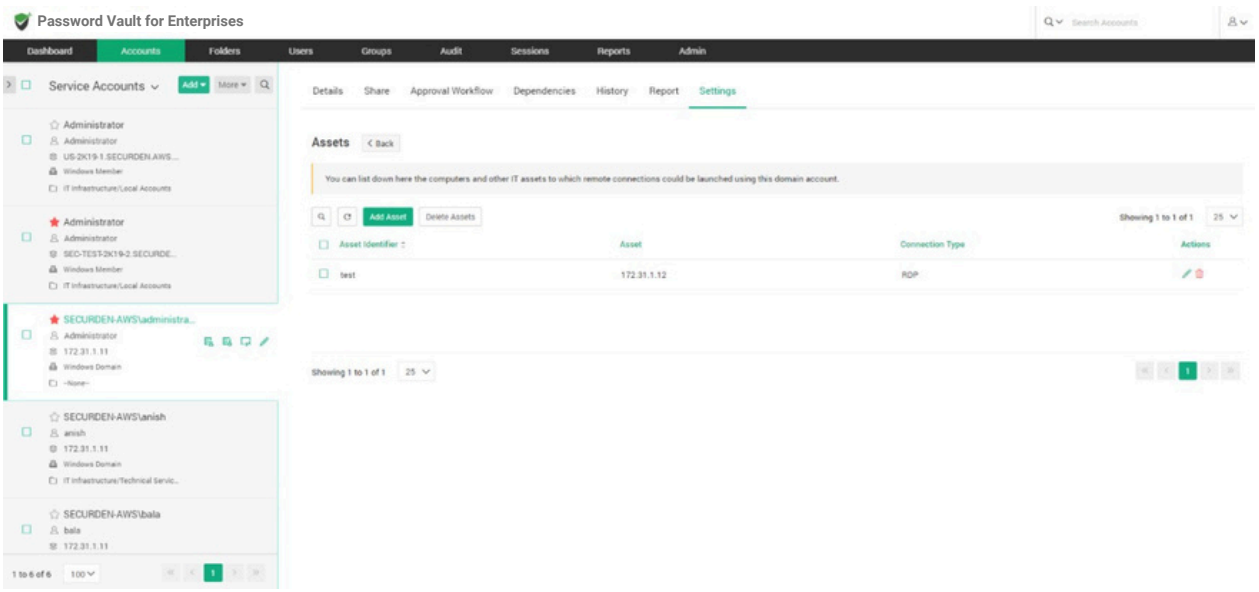


Assets

Lists down all the computers and other IT assets to which remote connections could be launched using this domain account.

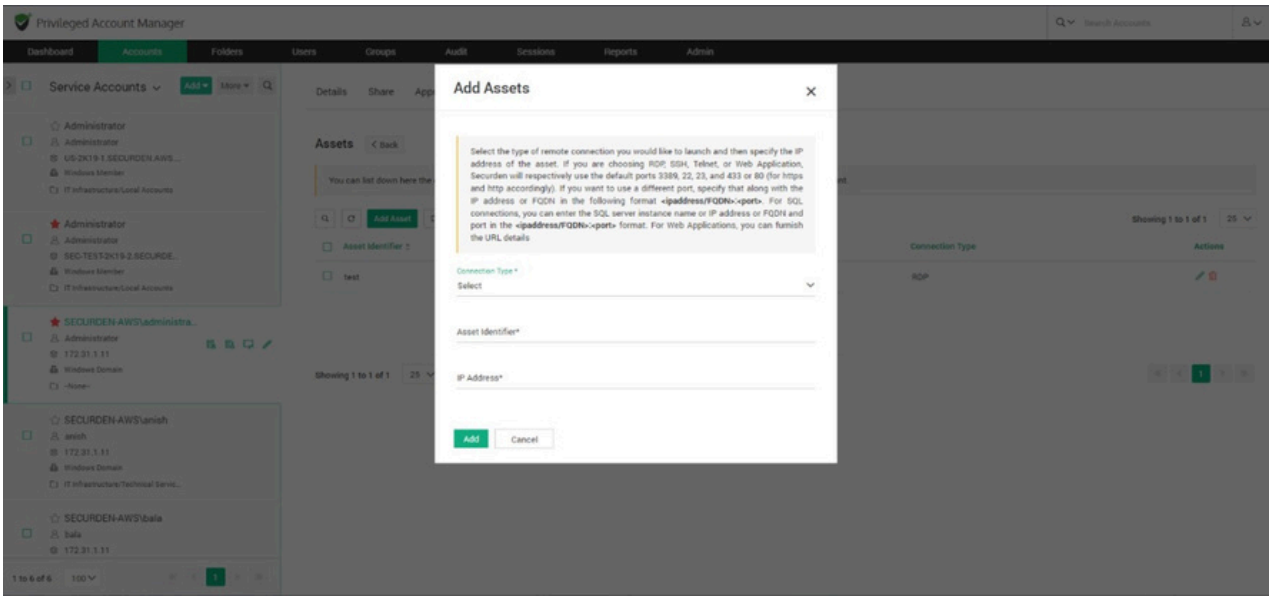
Select the account from the left-hand side of the UI. Navigate to **Settings >> Assets**.

You can add or delete assets from this part of the GUI.



Add Assets

Click on the **Add Asset** button. A small popup window will appear. You must provide the type of connection you want to launch to this asset (RDP, SQL, etc.) and its IP address.



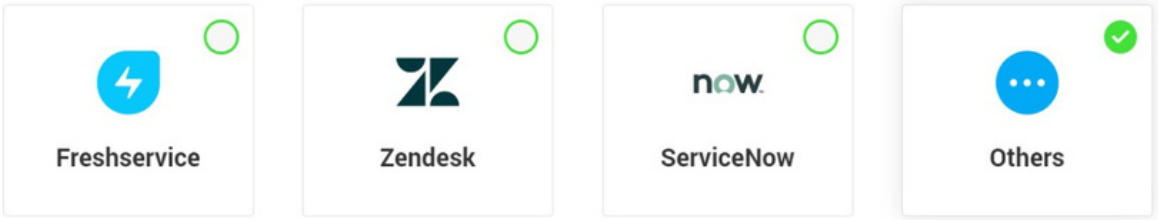
To add an asset, Select the type of remote connection you would like to launch and then specify the IP address of the asset. If you are choosing RDP, SSH, Telnet, or Web Application, Securden will respectively use the default ports 3389, 22, 23, and 433 or 80 (for https and http accordingly). If you want to use a different port, specify that along with the IP address or FQDN in the following format <ipaddress/FQDN>:<port>. For SQL connections, you can enter the SQL server instance name or IP address or FQDN and port in the <ipaddress/FQDN>:<port> format. For Web Applications, you can provide the URL details.

If you want to dissociate the asset from the domain account, you can select the asset and click on **Delete Assets**.

Enforcing Ticketing System Validation ENTERPRISE PAM

Securden integrates with web-based ticketing systems. The integration helps trace specific activities like password retrieval in Securden to corresponding

entries in the ticketing system. Securden validates the ticket ID provided by users either by matching the RegEx pattern of the ticket ID or directly accessing the ticketing system through API calls to see if there is a matching ticket found to be open. Out of the box, Securden integrates with Freshservice, Zendesk, and ServiceNow. However, you can integrate with any ticketing system through RegEx pattern validation.



Note: After configuring ticketing system here, you need to enable it at the account/folder level for the required accounts/folders.

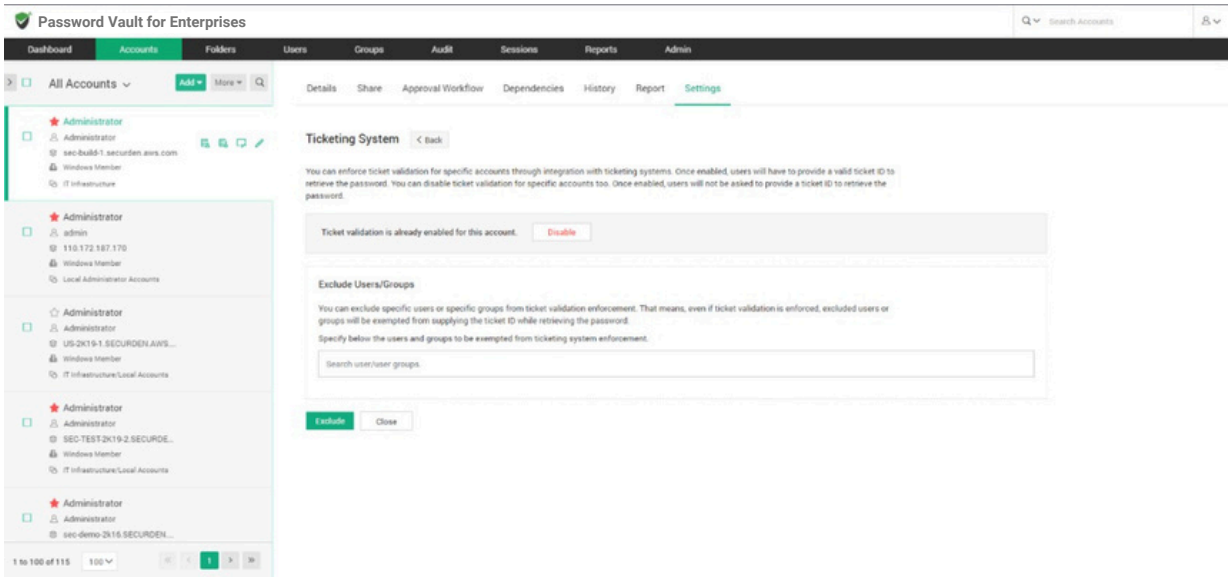
Enabling it at the account/folder level

You can enforce ticket validation for specific accounts through integration with ticketing systems. To enforce ticketing system validation, select the account from the left-hand side of the UI. Navigate to **Settings >> Ticketing System**.

Once enforced, users will have to provide a valid ticket ID to retrieve the password.

You can exclude specific users or specific groups from ticket validation enforcement. That means, even if ticket validation is enforced, excluded users

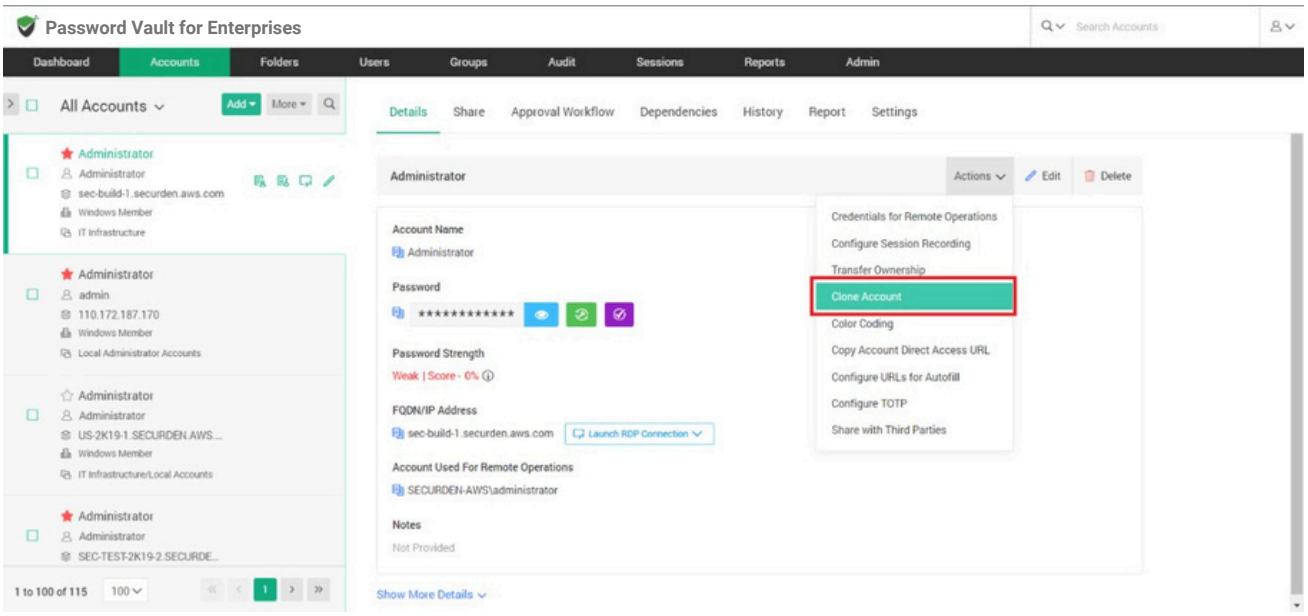
or groups will be exempted from supplying the ticket ID while retrieving the password.



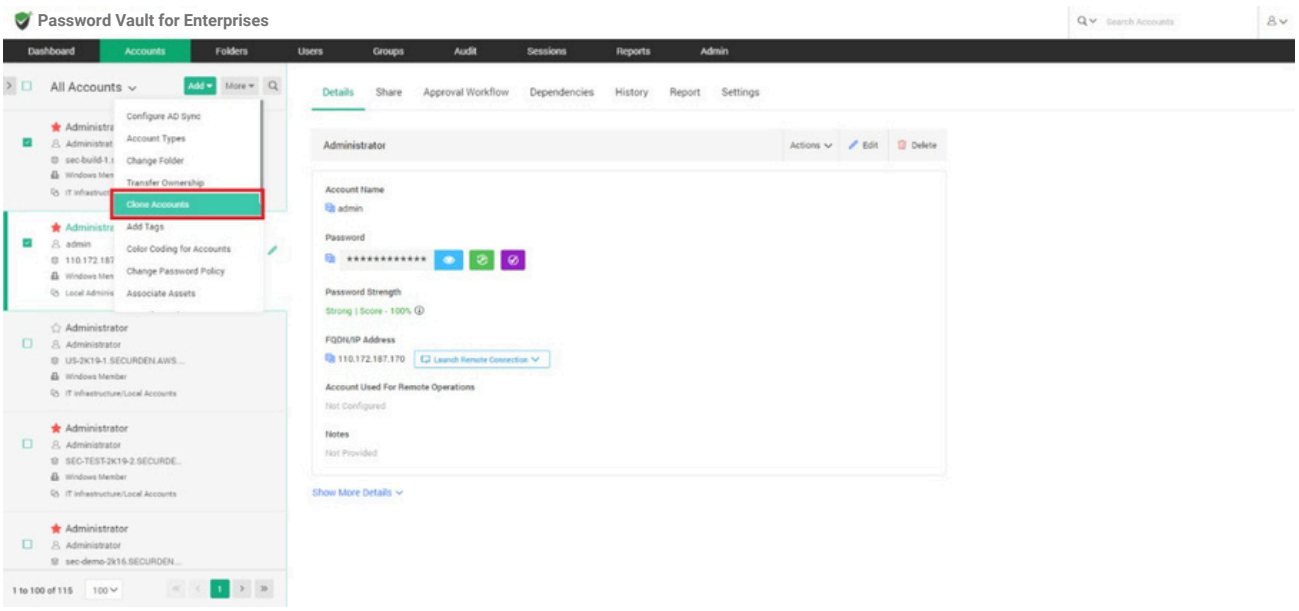
Account Actions

Clone Account

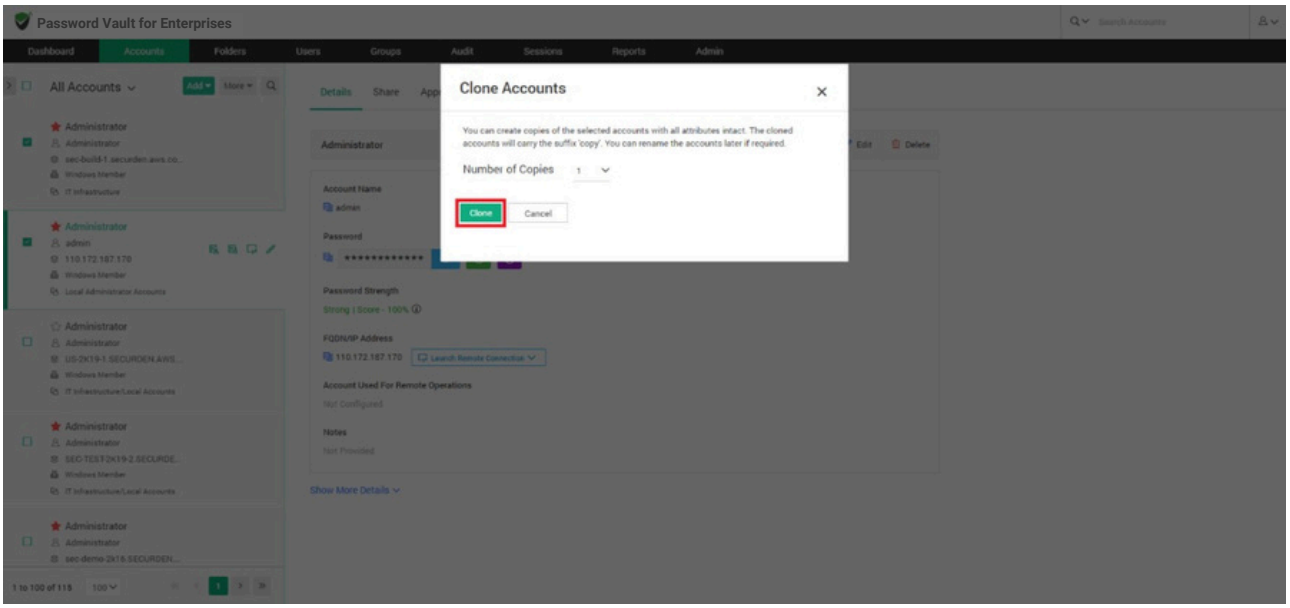
You can create copies of an account with all the attributes intact. The cloned accounts will carry the suffix “**copy”**. You can rename the accounts later if required. Multiple clones of the accounts with all the attributes intact can be created. Navigate to the account you want to clone. Select **Actions >> Clone Account.**



Alternatively, if you want to clone multiple accounts at once, you may select the required accounts and go to **More >> Clone Accounts**.

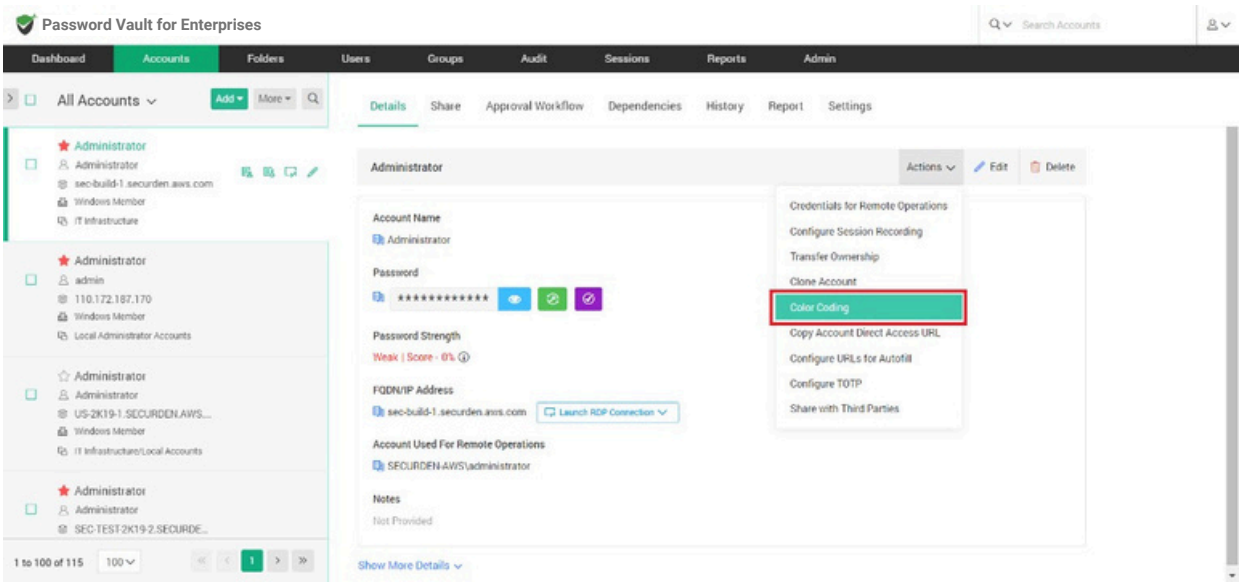


Select the number of copies you need from the drop-down list and click **Clone**.

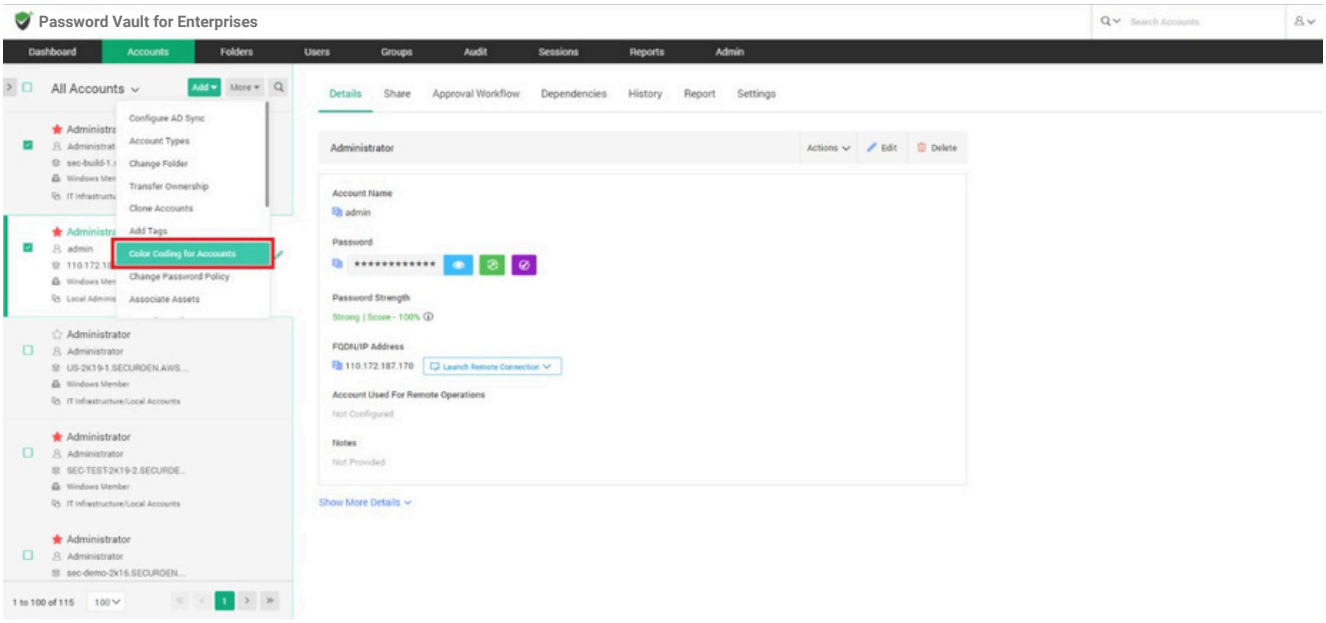


Color Coding

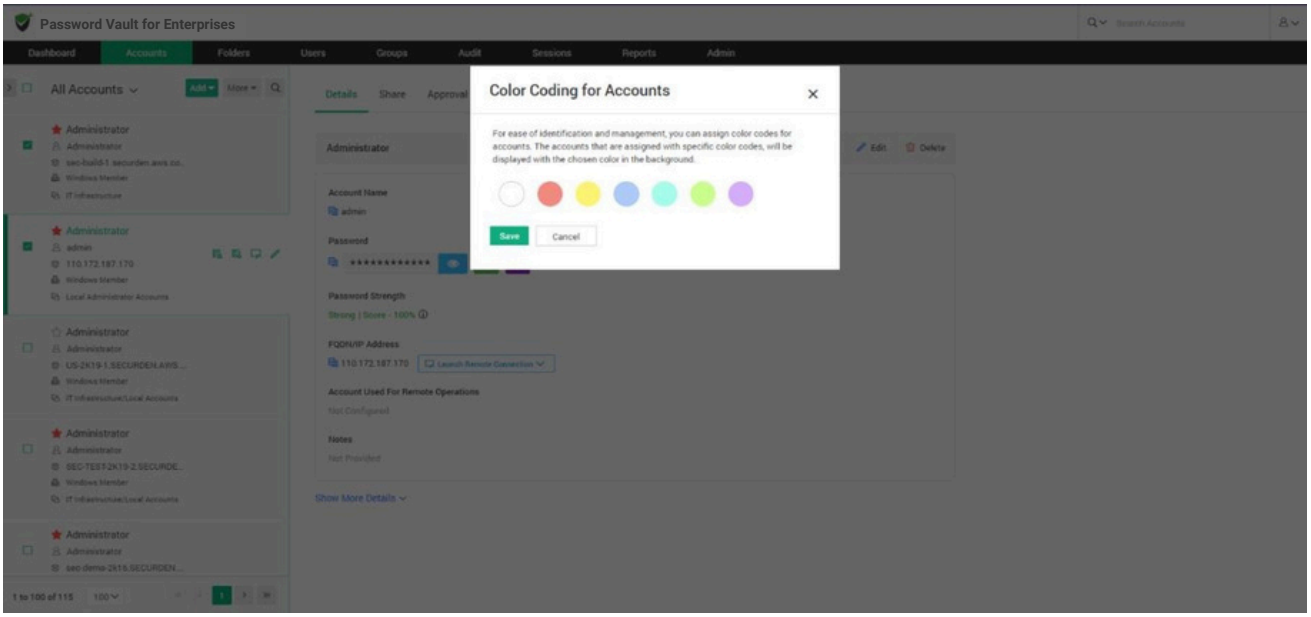
Designed for ease of identification and management, you can assign a color code for an account. Once a color is selected, the account will be displayed with the chosen color in the background. Select the account that you want to color code. Navigate to **Actions >> Color Coding.**



Alternatively, if you want to color code multiple accounts, you may select the required accounts and go to **More >> Color Coding for Accounts**.

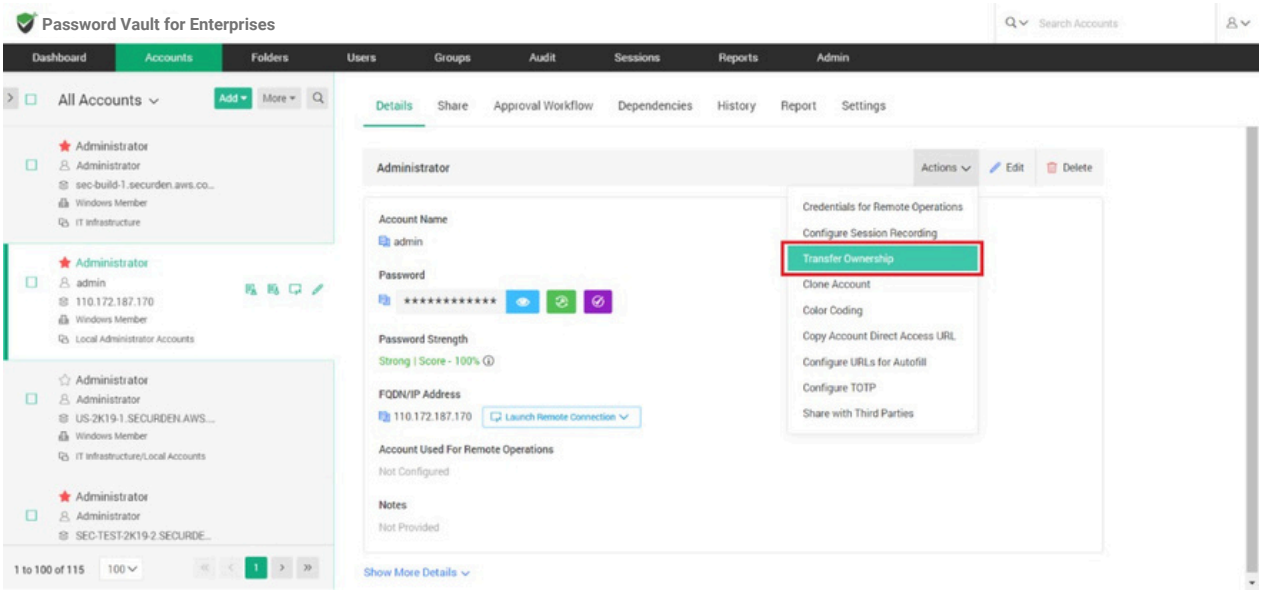


Select the desired color and click **Save**.

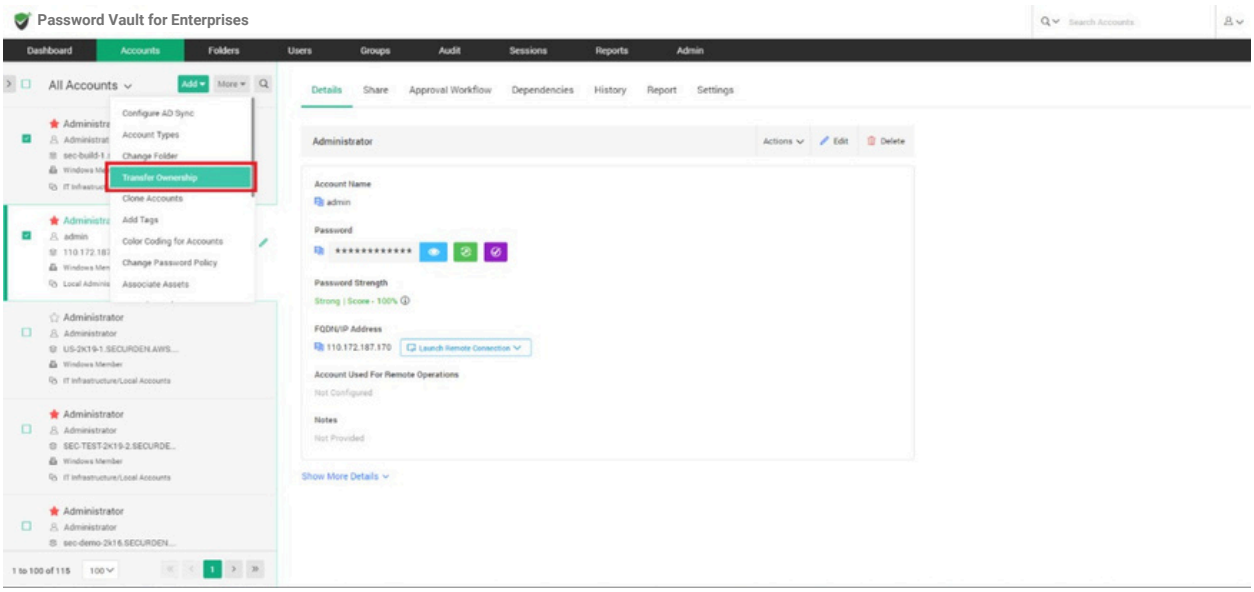


Transfer Ownership

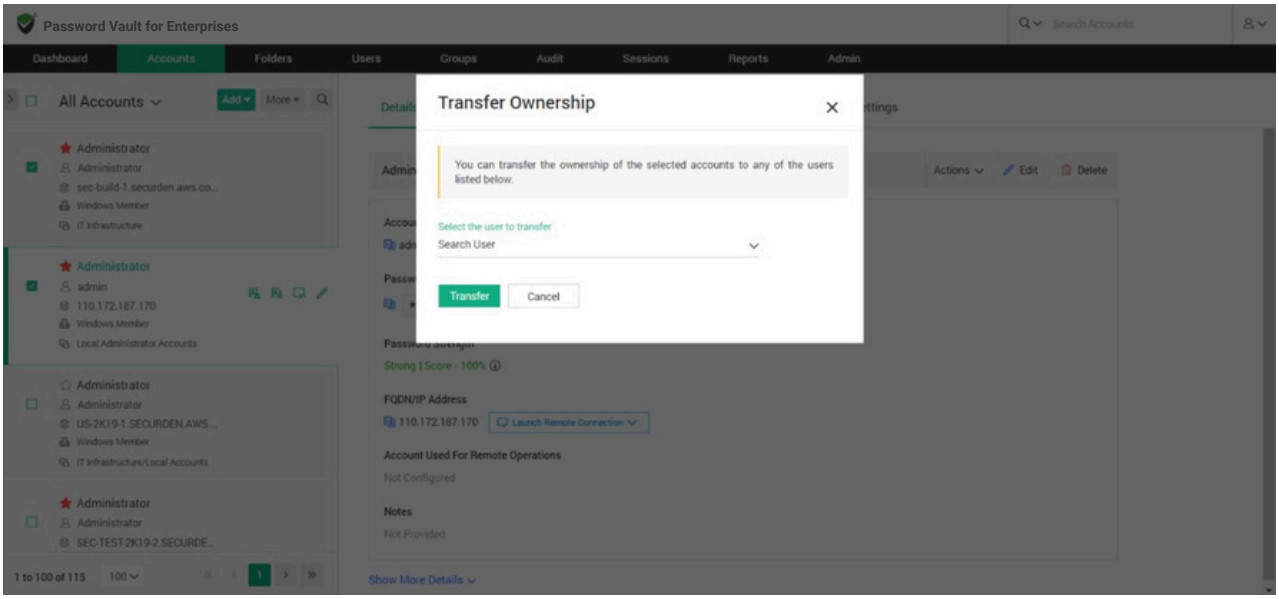
You can transfer the ownership of a particular account to any of the users in Securden. In such an event, the transferer will lose access to the accounts and folders already owned and the transferee will get complete ownership of those accounts and folders. Select the required accounts and navigate to **Actions >> Transfer Ownership**.



Alternatively, if you want to transfer ownership of multiple accounts, you can select the required accounts and navigate to **Accounts >> More >> Transfer Ownership**.



Select the user to whom the accounts need to be transferred and click **Transfer**.



Performing Operations on Multiple Accounts

You can perform various operations and customization on accounts stored in Securden. You have the option to perform operations on individual accounts or in bulk. If you would like to carry out operations on multiple accounts at once, you can navigate to **Accounts >> More** and do so.

Add and Manage Account Types

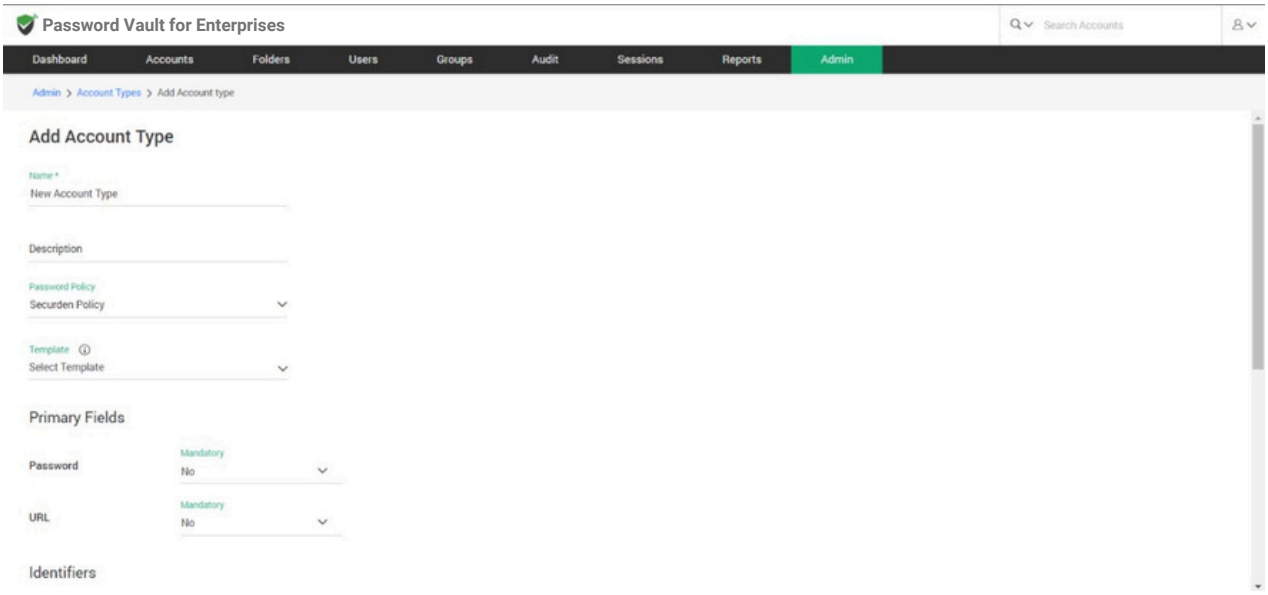
Account types help identify and classify the accounts being added in Securden. Proper classification comes in handy to carry out various operations such as sharing, remote password resets, reporting, etc. You can also use account types to define specific characteristics like fields for the accounts, specific password policies for the accounts belonging to that type, and so on. Super administrators, administrators, and account managers have the privilege to add custom types, edit and delete existing ones.

You need to define account types separately for **Work** and **Personal** type accounts. The procedure is the same for both.

Creating a new account type

To create a new account type, navigate to **Admin >> Account Management >> Account** Types. You need to select between **Work** and **Personal** type account and click **Add Account Type**. Enter a name for the new account type

being created. The name you enter here will uniquely identify the type. Adding a description to the type would help further in this aspect.



Associate a password policy

One of the most important aspects of Account Types is that password policies can only be associated at the account type level. You can create multiple password policies and associate them with different account types. The policy that is associated with an account type will take effect for all accounts that belong to the type.

You may choose from the list of already available policies or create a new policy. Alternatively, if any of the types don't require a password policy to be linked, you may choose the option **Don't link any policy**.

Associate a Template

Securden allows you to perform various remote operations such as password resets on devices. The product comes with certain predefined templates to carry out those operations on various types of devices.

In addition, you can create custom SSH templates to carry out remote password resets on devices that can be connected through SSH such as Linux devices, routers, server hardware, etc.

You can define a command or a sequence of commands to be used for carrying out the password reset activity in the form of a custom template. If the account type you are creating requires support for such remote operations, you may associate the required template in this step.

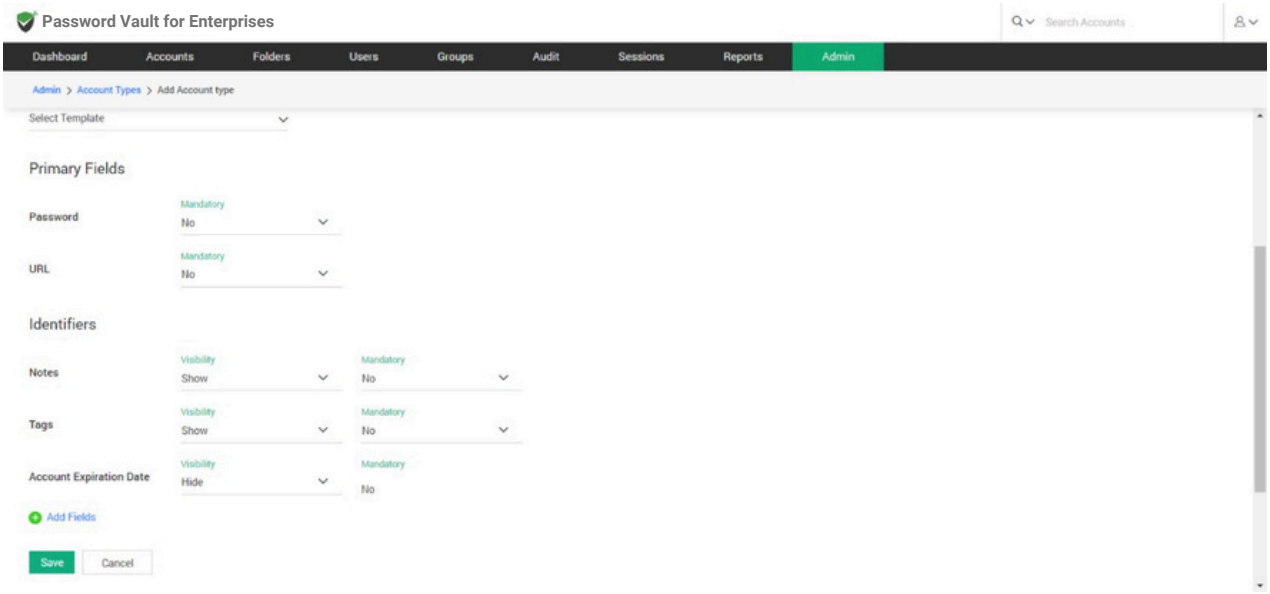
At present, templates can be associated only at the time of creating the account type. Templates can’t be associated while editing the type.

Define the Fields

Accounts in Securden contain various fields such as **Username**, **Password**, **URL** etc. Depending on the type of account, the fields will vary. You might even have some specific account types in your organization that require completely new fields and values. All such requirements can be met at the account types level.

You can define any number of fields required by this specific type and granularly specify if the fields are mandatory (requiring users to compulsorily

fill a value when adding accounts). You can also choose to hide certain default fields.



Primary Fields

The default **Password** and **URL** fields can't be hidden or deleted, but you can mark if they are to be made mandatory or not.

Identifiers: The **Notes**, **Tags**, and **Account Expiration Date** fields are optional. You can choose to **show** or **hide** any of these fields as required. When you choose to **show**, you can also mark if it has to be mandatory or not.

Additional Fields

You can create any number of customized additional fields as required. To create additional fields, click the **Add Fields** button. When creating additional fields, you have the option to specify the field type - Text,

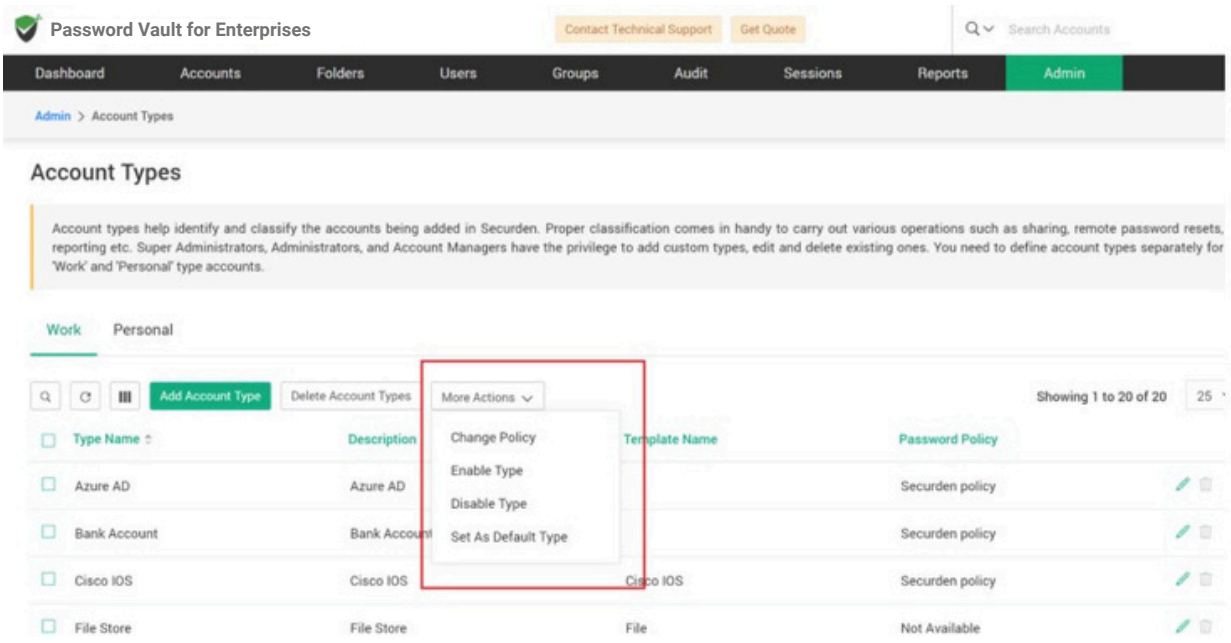
Password, or File Store. While **Text** represents a text field, **Password** helps mask the value from being displayed in plain text. **File Store** type allows you to browse and choose files.

Managing Account Types

You can manage the existing account types from **Admin >> Account Management >> Account Types** section. The management operations include changing the password policy association, setting any type as the default type, disable a type, enable a disabled policy, editing the nature of various fields, and so on.

From **Account Types >> More Actions** drop-down,

- You can quickly change the password policy association for any type
- Enable/disable a type. Among the system-defined account types, five types - Web Account, Bank Account, SSH Key, File Store, and License Key cannot be disabled. All other types can be disabled. When you disable a type, the same will not be available for choosing it during account addition.
- Set any type as the **Default Type** (the type which is set as the default type here will be the default selection of account type in the Add Accounts GUI for **Work** account types)

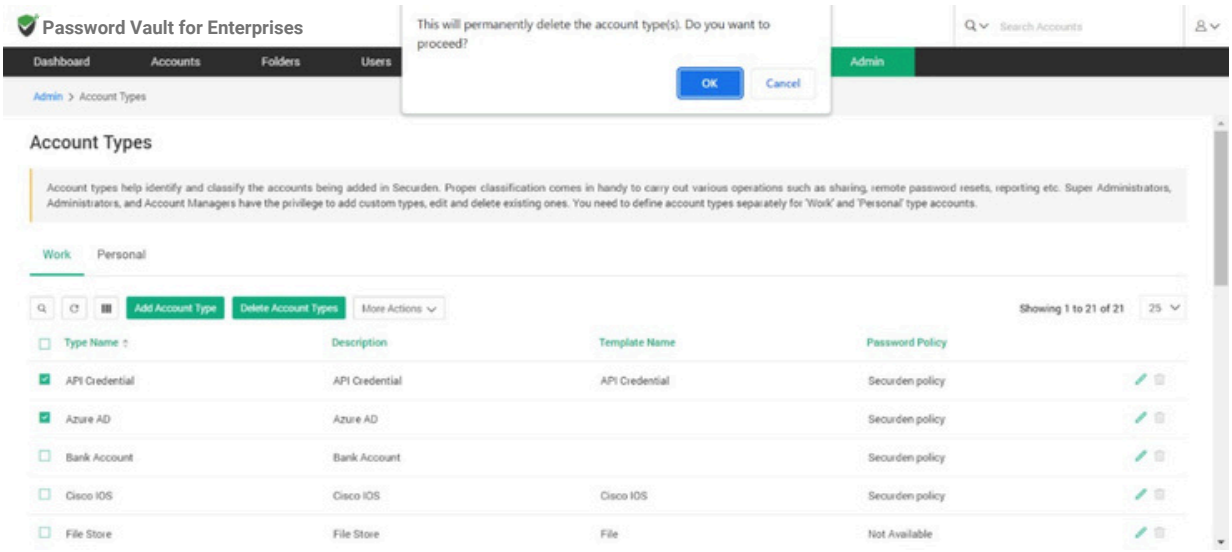


If you want to edit multiple attributes, you may use the **edit** icon present in the table.

Delete Account Types

You can delete any custom account types created. Select the types to be deleted and then click the button **Delete Account Types**.

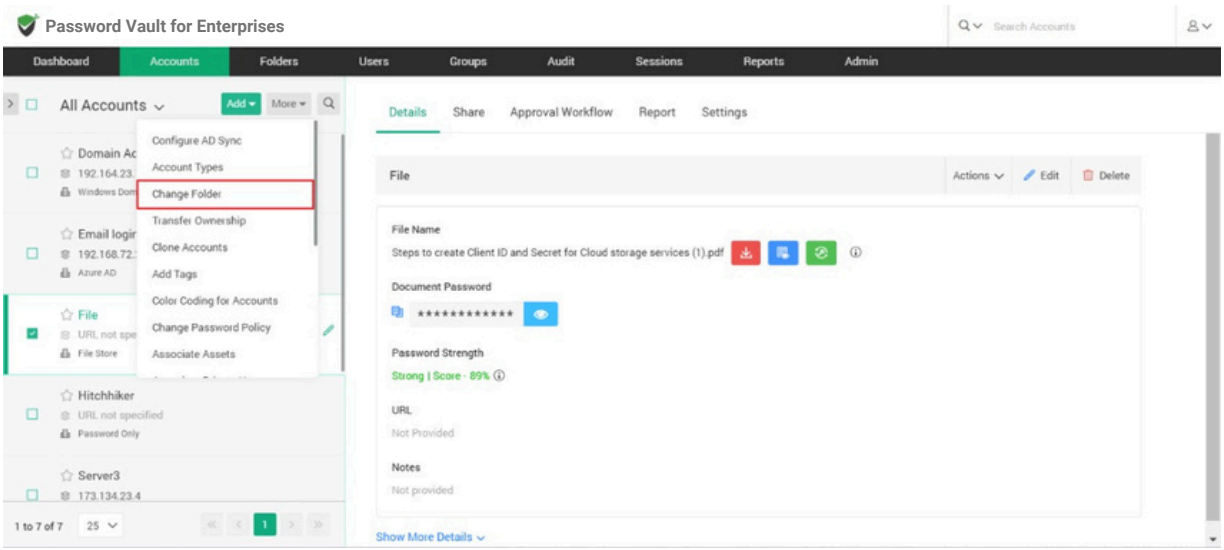
You can also click the **Delete** icon present at the RHS of each entry.



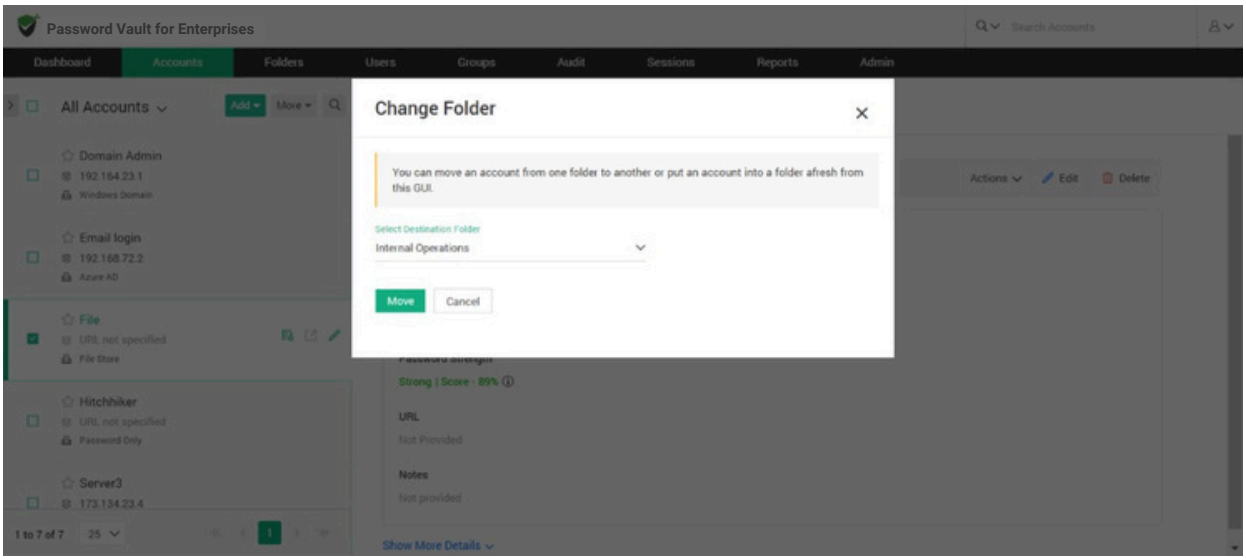
Note: If the account type you are trying to delete has accounts associated with it, you will not be able to delete it. You may either edit the respective accounts and associate them with a different account type and then delete the type or you can simply disable this account type and restrict any further addition of accounts to this type. The default system defined account types cannot be deleted. They can only be disabled.

Change Folder

You can move an account from one folder to another or put an account into a new folder. Select the account to be moved, click the **More** drop-down. Select the **Change Folder** option.

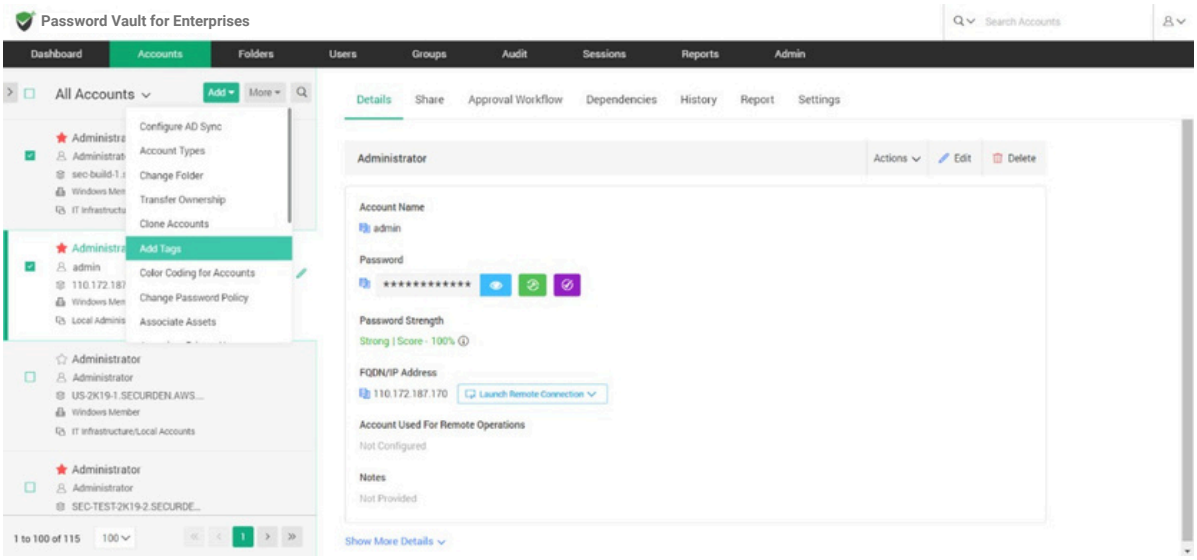


In the popup that opens, choose the folder to which the account(s) are to be moved, and then click **Move**.

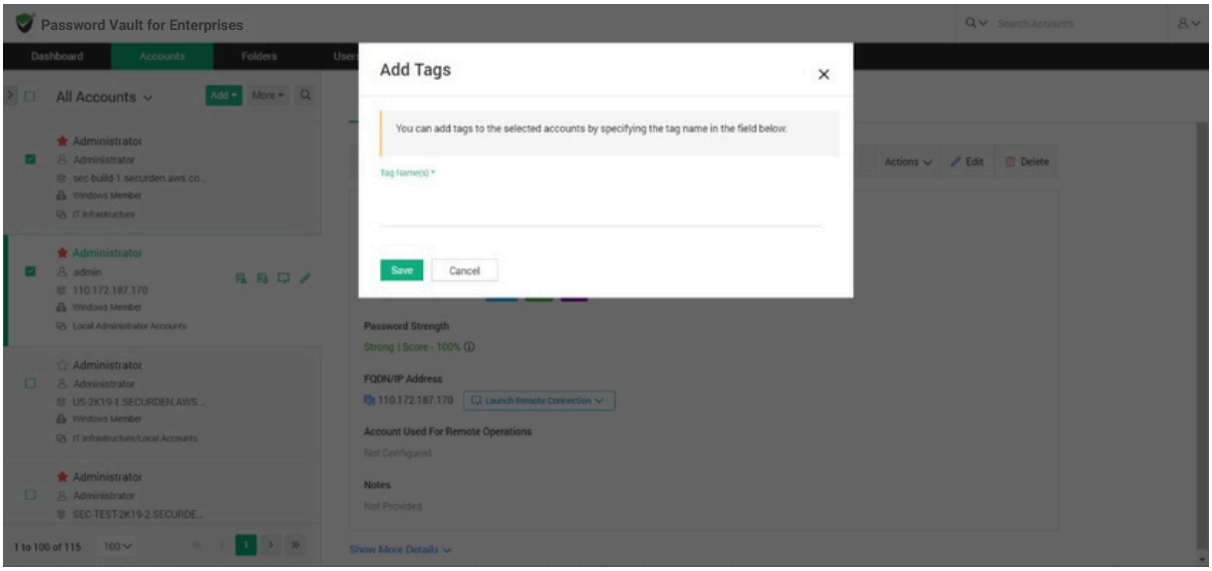


Add Tags

If you want to add any specific categorization to accounts in the form of a tag, you may do it by clicking on **Add Tags** under **More** drop-down in the **Accounts** section.

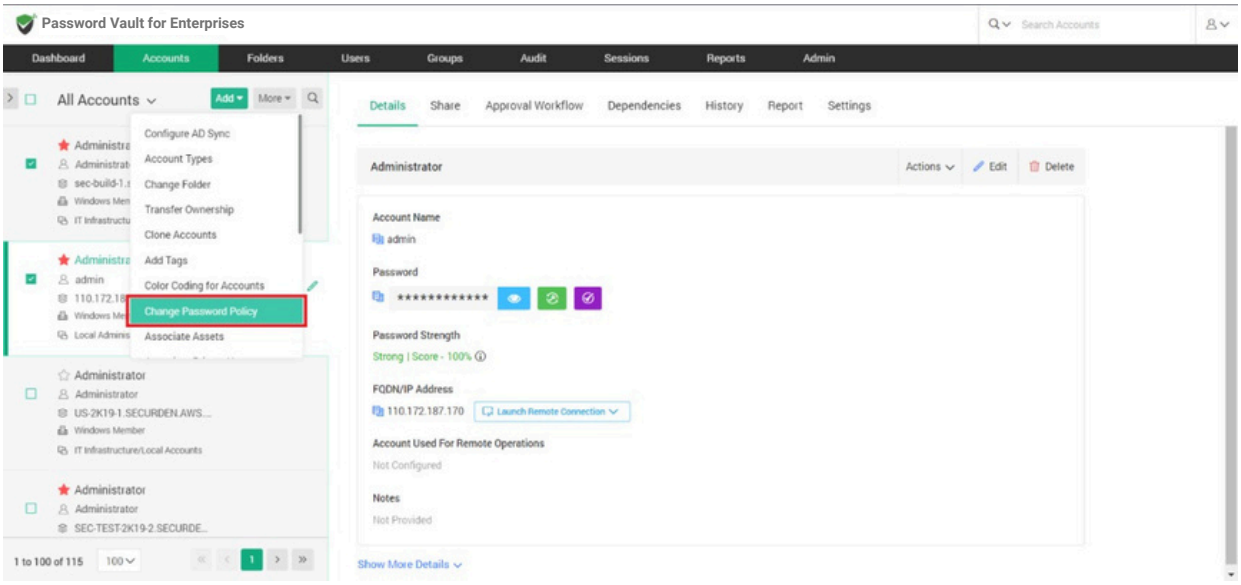


Select the account(s), enter the tag name(s), and click **Save**.

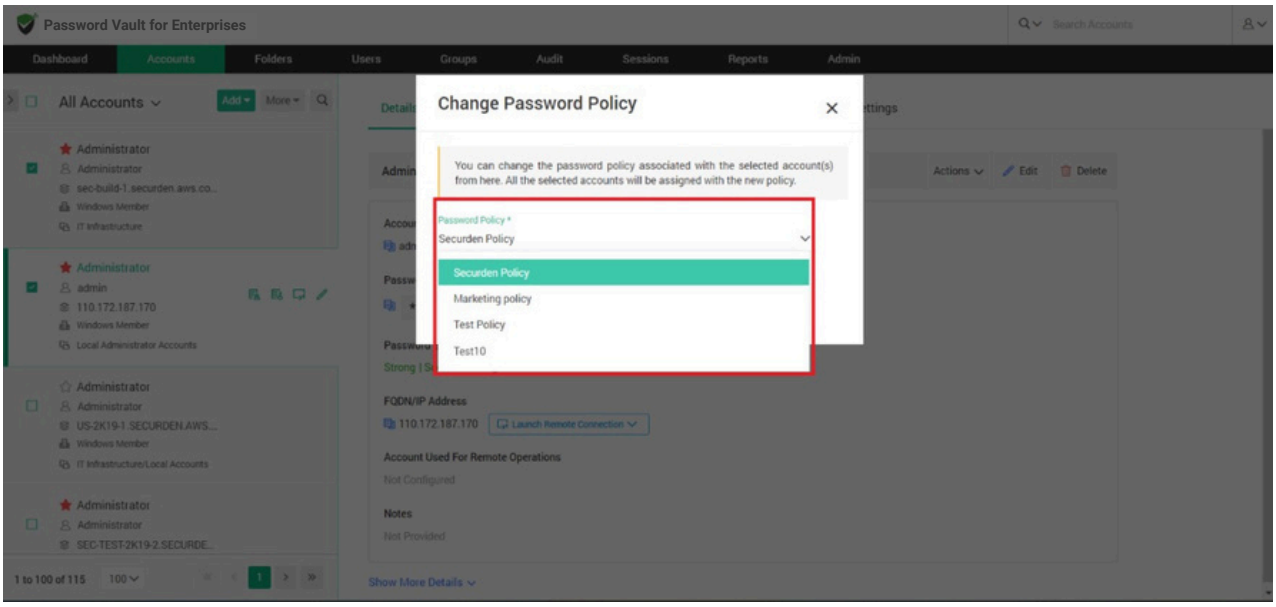


Change Password Policy

If you want to change the password policy for any specific account(s), you may change it by navigating to **Accounts >> More >> Change Password Policy**.

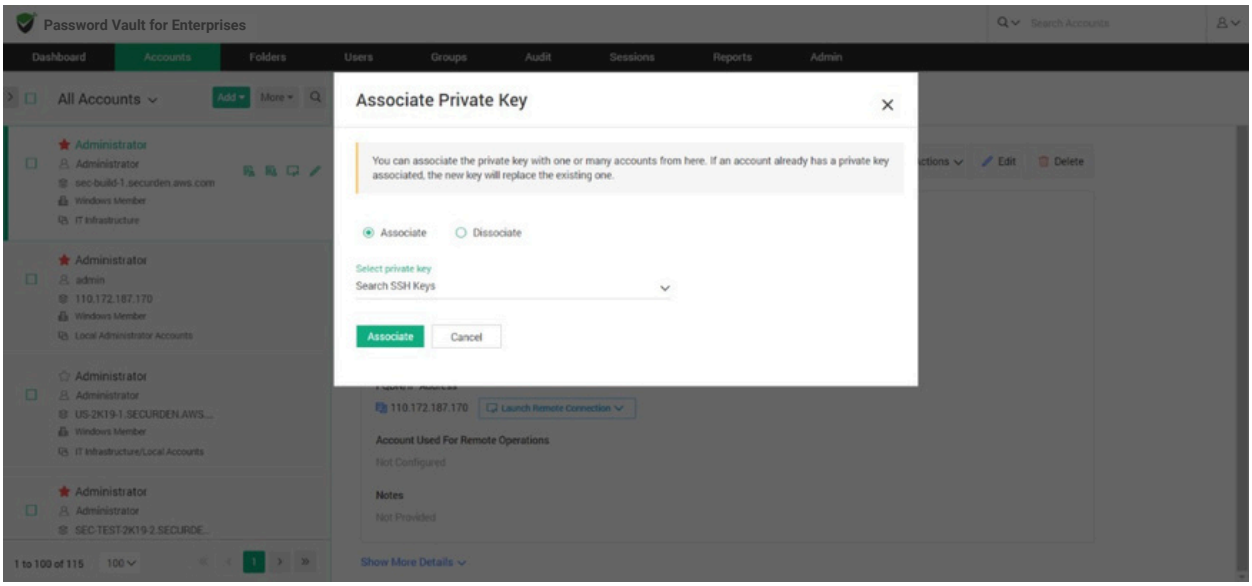


Select the account(s), click the option **Change Password Policy**, and then choose the policy to be applied from the drop-down. After selecting, click **Change Policy** to apply the policy to the account(s).



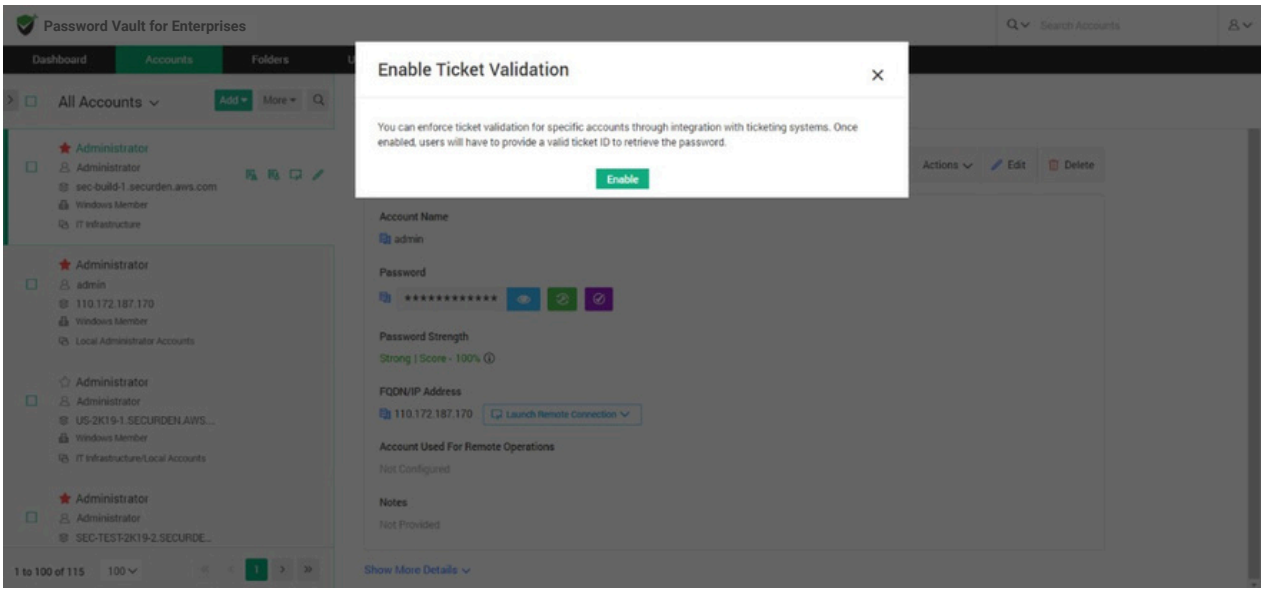
Associate Private Key

You can add an SSH key as an account and use that to launch connections to some other accounts. Navigate to **Accounts >> More >> Associate Private Key**. You can associate the private key with one or many accounts from this section. If an account already has a private key associated, the new key will replace the existing one. Select the key to be associated from the drop-down given and click **Associate**.



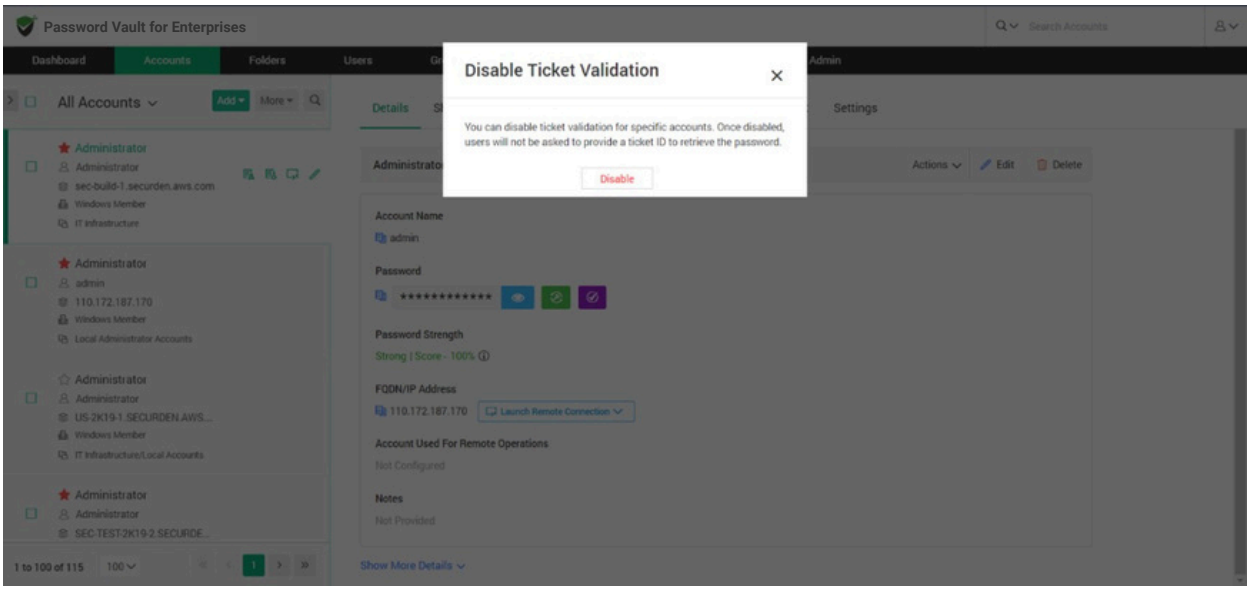
Enable Ticket Validation ENTERPRISE PAM

Securden integrates with web-based ticketing systems. The integration helps trace specific activities like password retrieval in Securden to corresponding entries in the ticketing system. You can enforce ticket validation for specific accounts through integration with ticketing systems. Once enabled, users will have to provide a valid ticket ID to retrieve the password. Select the accounts for which you want to enforce ticket ID validation. Navigate to **Accounts >> More >> Enable Ticket Validation** and click **Enable**.



Disable Ticket Validation ENTERPRISE PAM

Securden integrates with web-based ticketing systems. The integration helps trace specific activities like password retrieval in Securden to corresponding entries in the ticketing system. You can disable ticket validation for specific accounts. Once disabled, users will not be asked to provide a ticket ID to retrieve the password. Select the accounts for which you want to disable ticket ID validation. Navigate to **Accounts >> More >> Disable Ticket Validation** and click **Disable**.



Offline Access

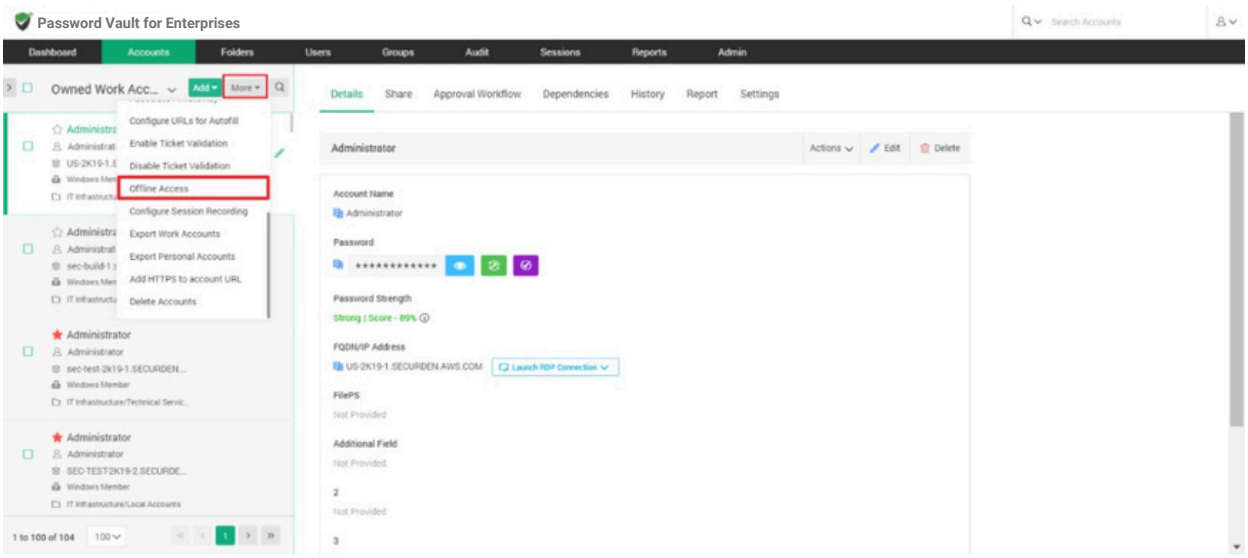
As an end user, you can access your accounts and passwords even when you go outside your network or don't have internet access. Securden provides the passwords in the form of an encrypted HTML copy for offline access. You can open this file in any web browser, and you will see the same interface as that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

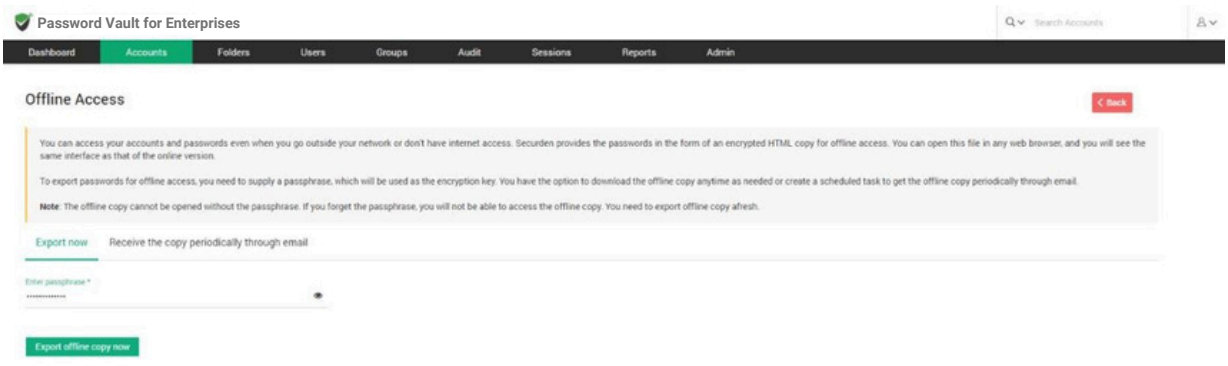
Note: The offline copy cannot be opened without the passphrase. If you forget the passphrase, you will not be able to access the offline copy. You need to export offline copy afresh.

End-users can save an offline copy of all the accounts they have access to.

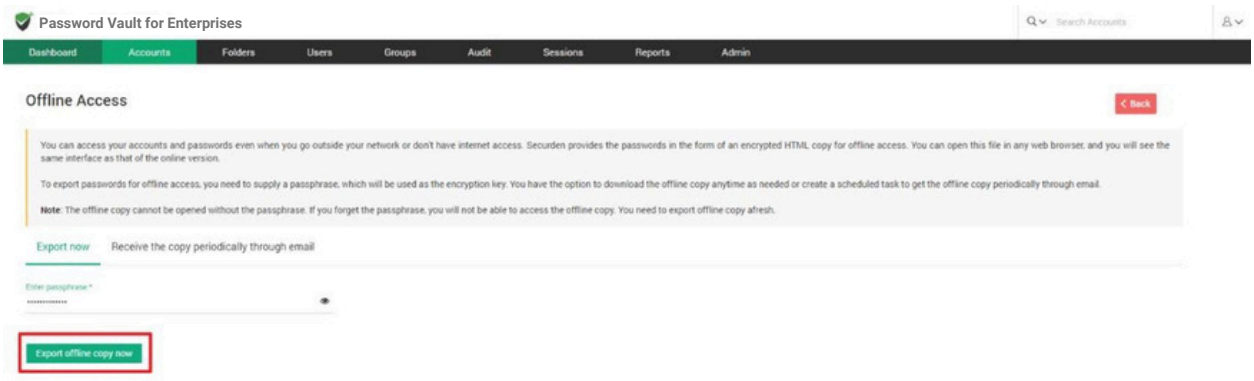
Users need to navigate to **Accounts >> More >> Offline Access.**



Users can export the account at once from the **Export now** tab, they need to enter a passphrase while exporting the 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**.

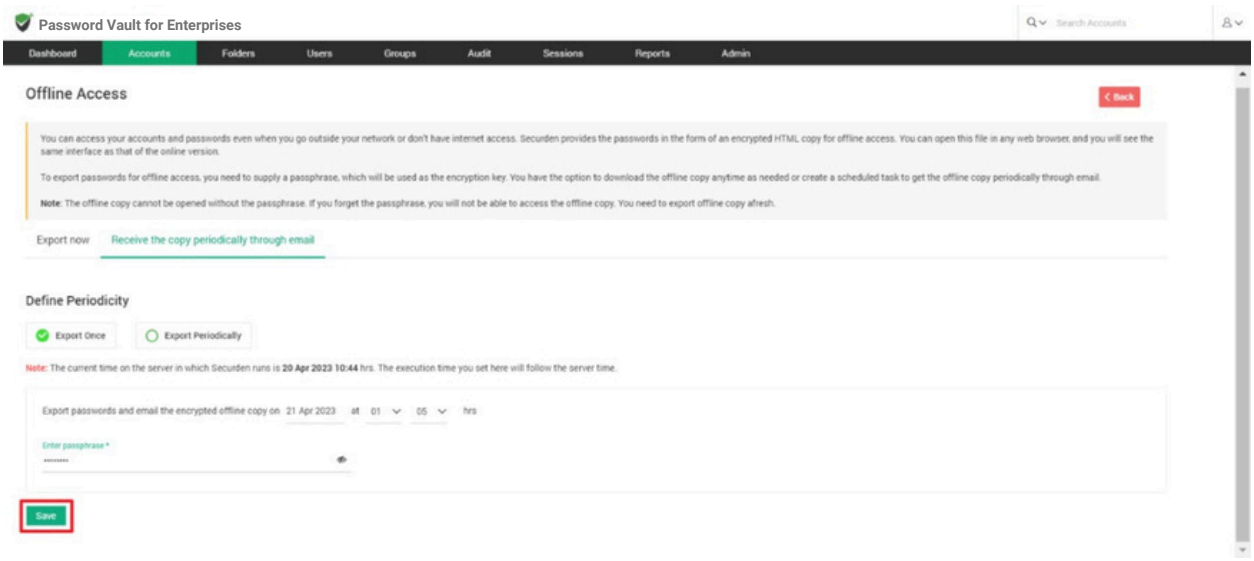


Receive the offline copy through email

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.

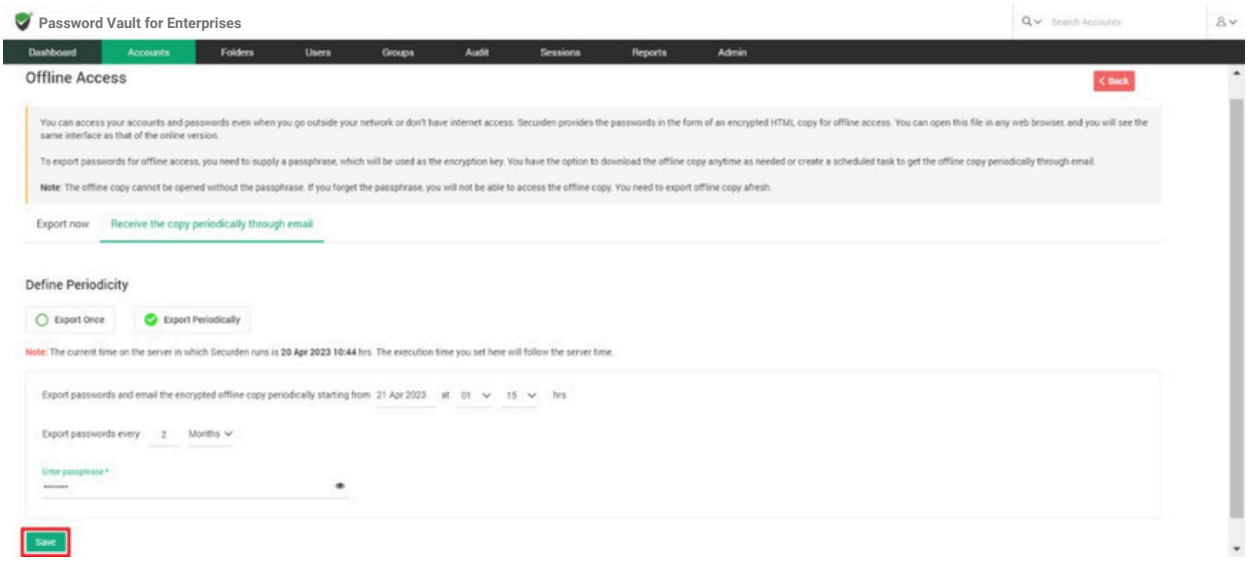
Once all the fields are selected, they can click **Save**.



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

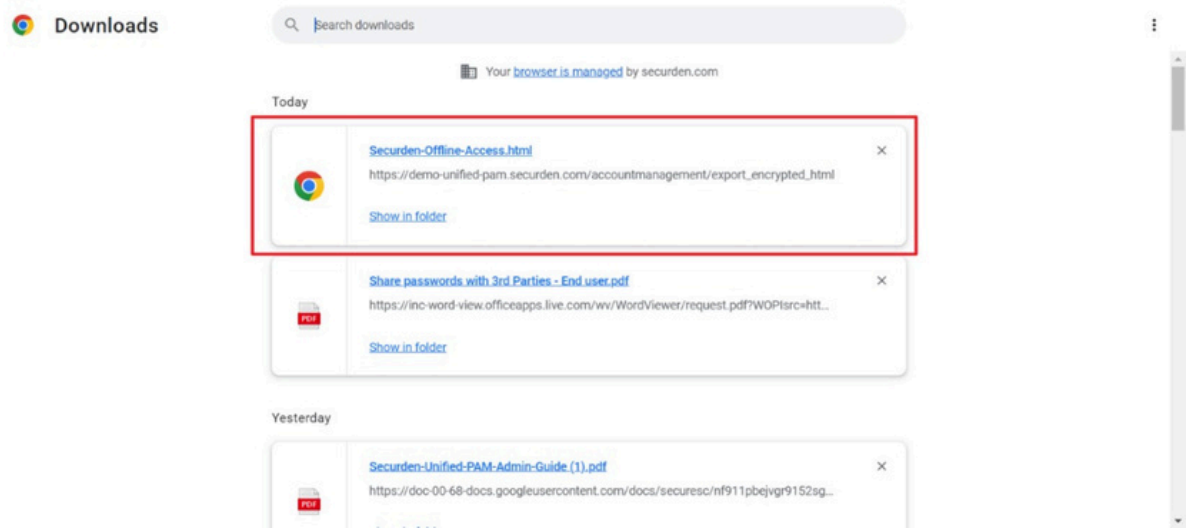
They then need to select the date and time at which they receive the first offline copy of passwords.

Users must then specify the periodicity at which they receive subsequent copies. This can be set as an interval of hours, days, or months.

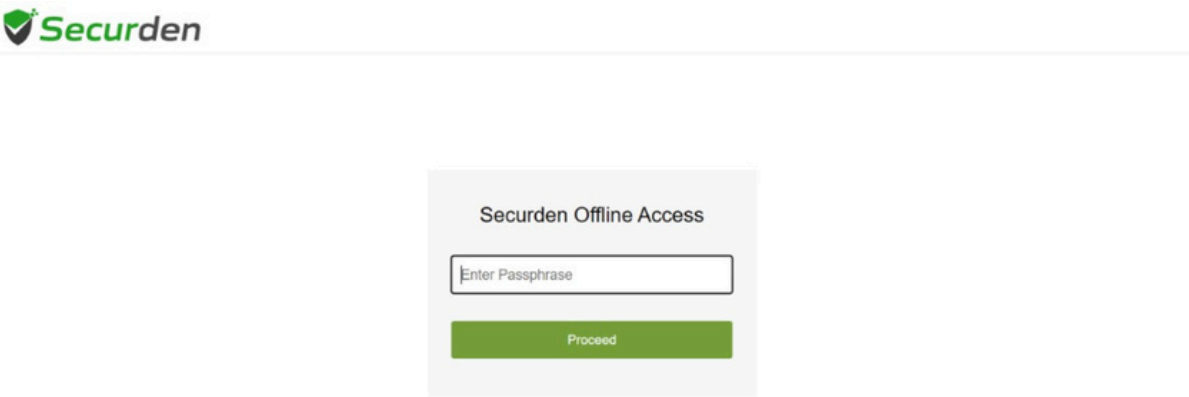


Once all the fields are selected, they can click **Save**.

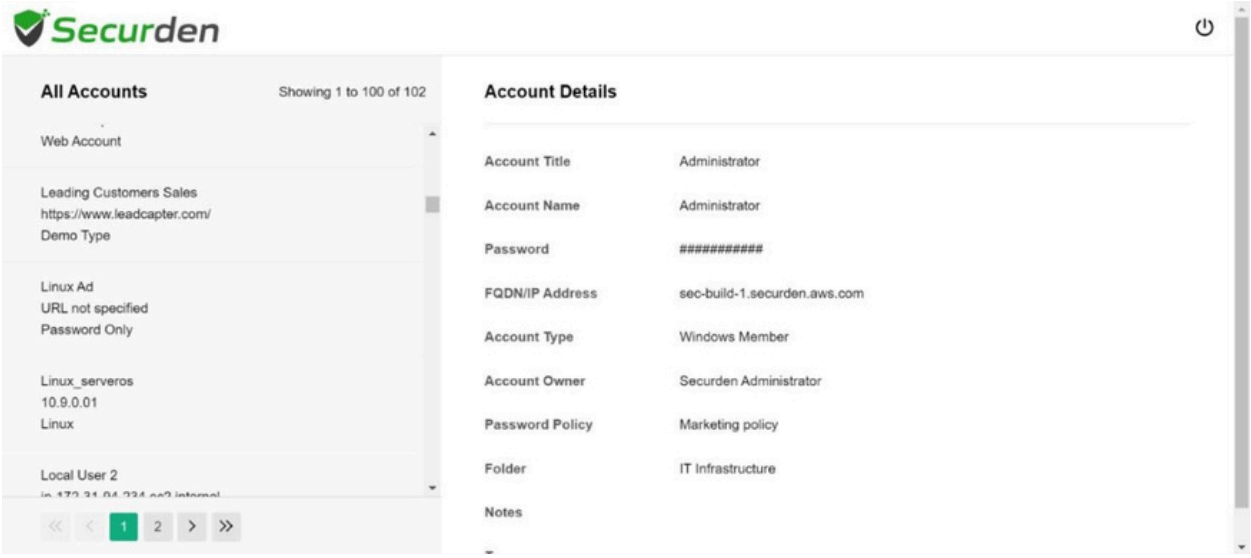
Users can access the downloaded HTML or access it from their email id.



To open the encrypted HTML file, users have to enter the passphrase that they keyed in on configuring offline access.

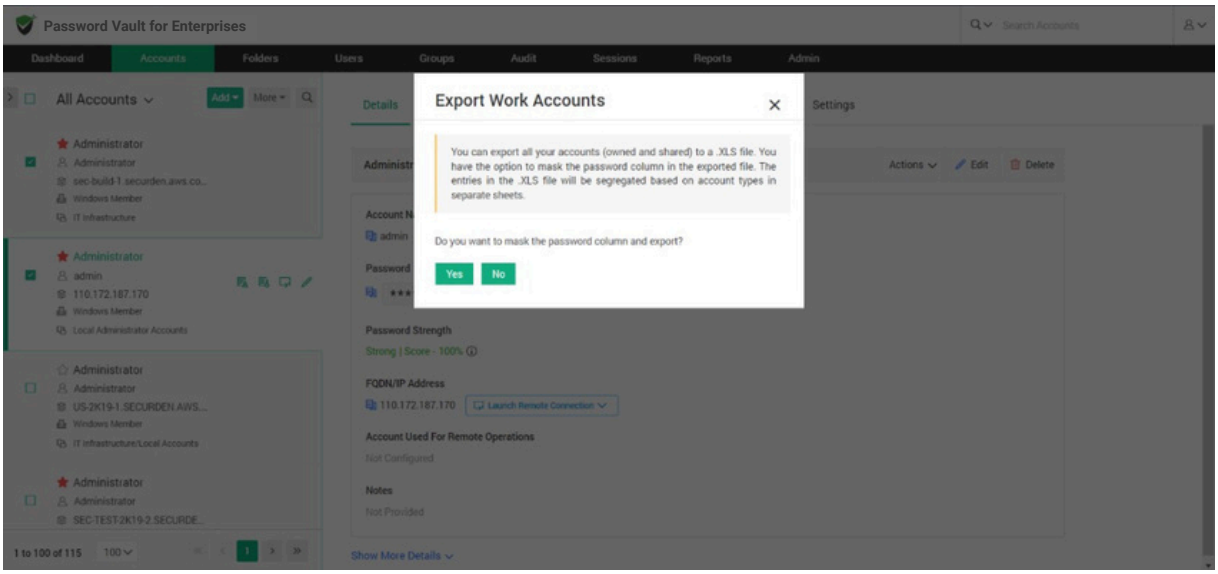


On successfully entering the passphrase, users can access all their passwords offline.



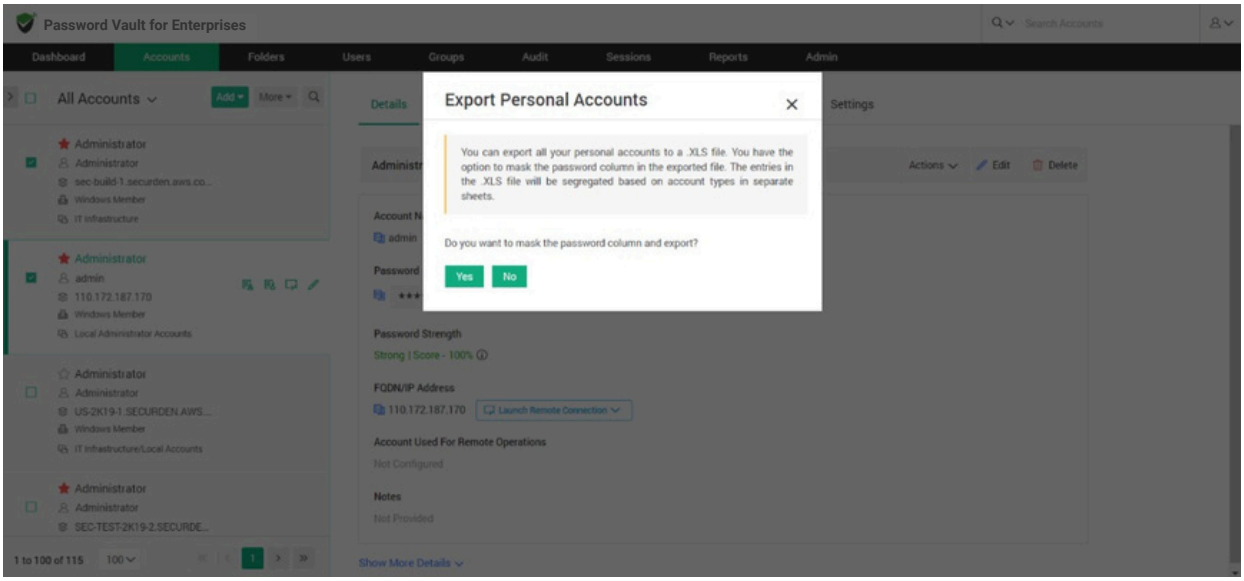
Export Work Accounts

You can export all your accounts (owned and shared) to an **XLSX** file. You have the option to mask the password column in the exported file. The entries in the XLSX file will be segregated based on account types in separate sheets. Navigate to **Accounts >> More >> Export Work Accounts**. Choose whether to mask the password column and export.



Export Personal Accounts

You can export all your personal accounts to an **XLSX** file. You have the option to mask the password column in the exported file. The entries in the XLSX file will be segregated based on account types in separate sheets. Navigate to **Accounts >> More >> Export Personal Accounts**. Click **Yes** to mask the password column and export.

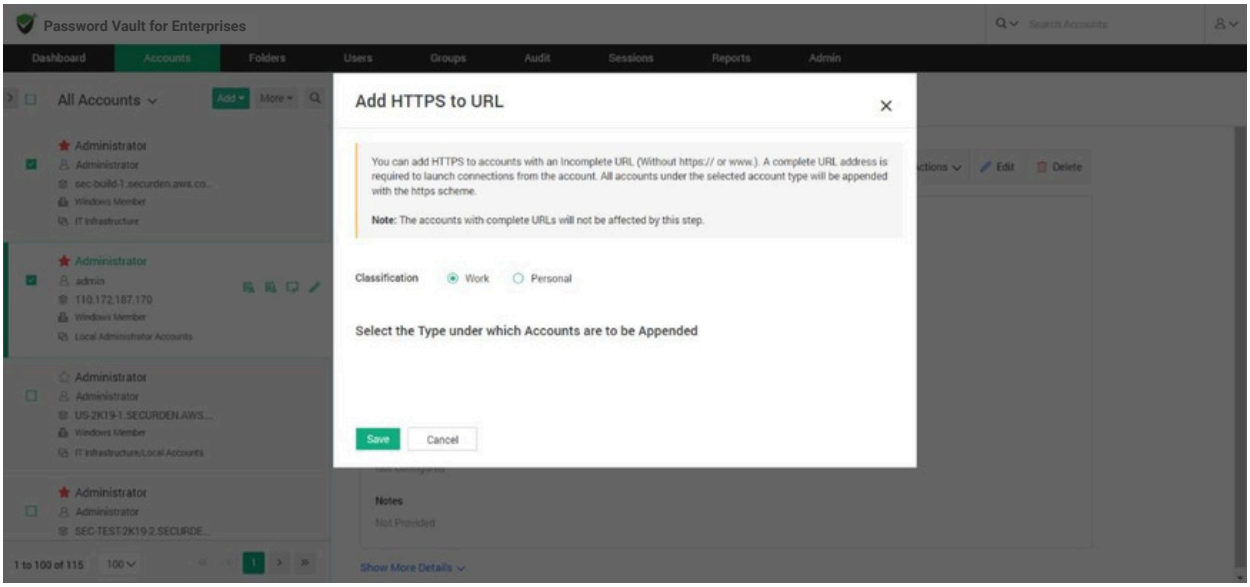


Add HTTPS to account URL

You can add HTTPS to accounts with an Incomplete URL (Without https:// or www.). A complete URL address is required to launch connections from the account. All accounts under the selected account type will be appended with the https scheme.

Note: The accounts with complete URLs will not be affected by this step.

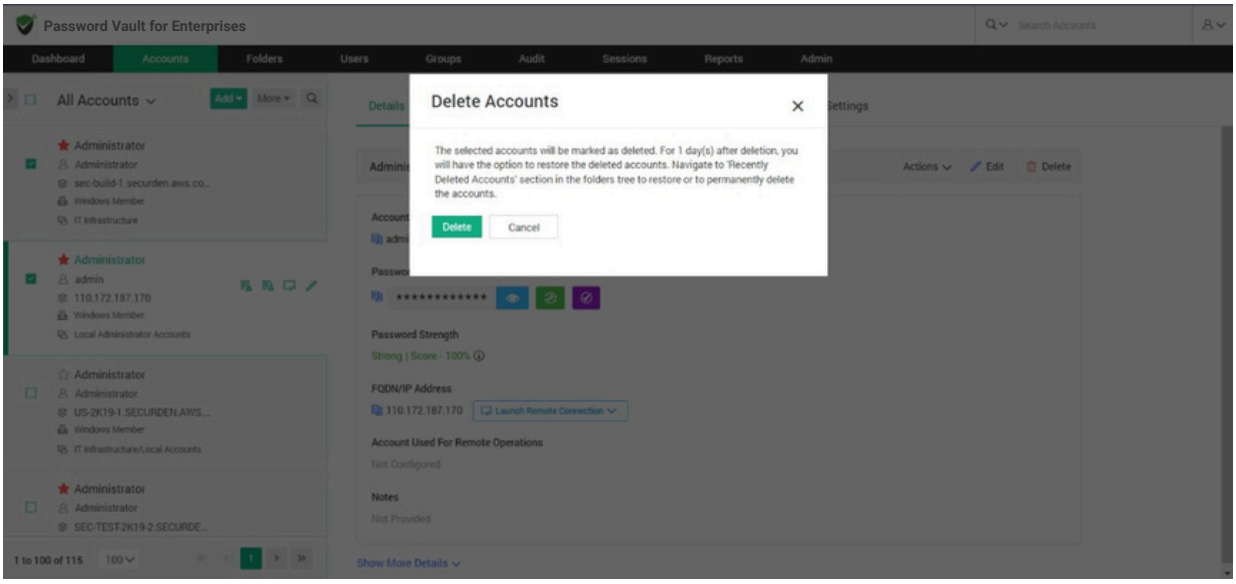
Navigate to **Accounts >> More >> Add HTTPS to the URL**. Select the classification of your accounts (Work or Personal) to which URLs are to be added, choose the account type from the drop-down given, and then click **Save**.



Delete Accounts

You can delete one or more accounts at once by navigating to **Accounts >> More >> Delete Accounts**. The selected accounts will be marked as deleted.

For 1 day(s) after deletion, you will have the option to restore the deleted accounts. Navigate to **Recently Deleted Accounts** section in the folders tree to restore or to permanently delete the accounts.



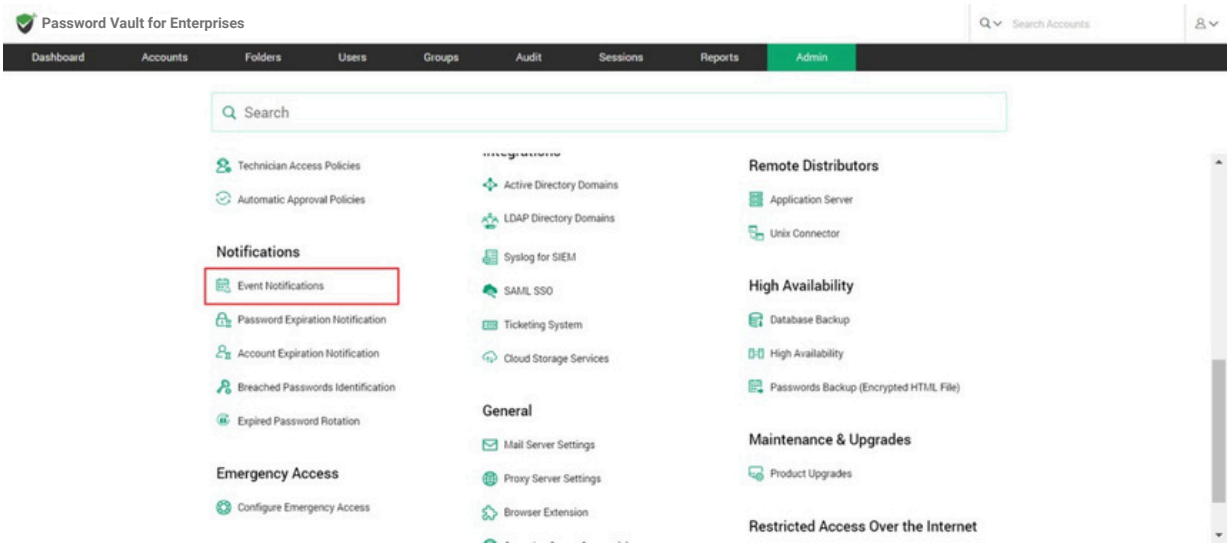
Section 5: Notifications

Event Notification

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.

Configure Event Notifications

Navigate to **Admin >> Notifications >> Event Notifications** to configure this feature.

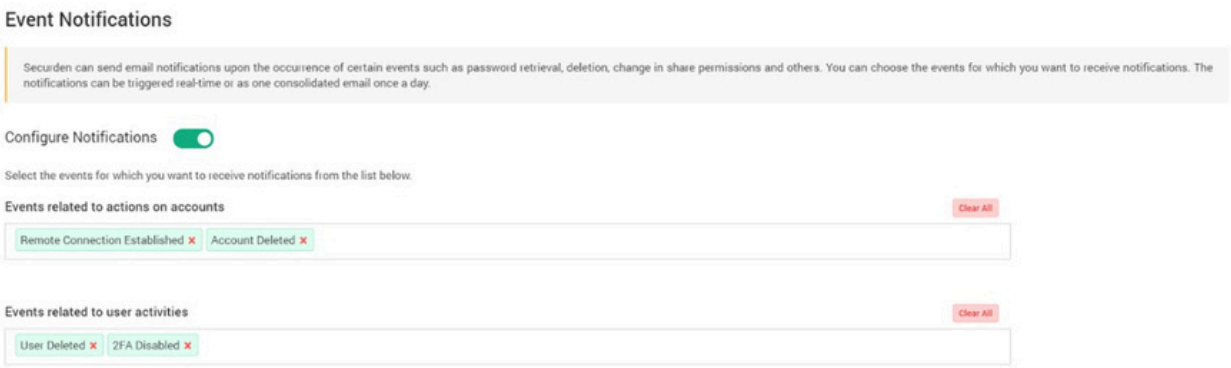


To enable notifications, you need to toggle the Configure Notifications button.

Selecting Events

You will see two fields named **Events related to actions on accounts** and **Events related to user activities**.

To add events that you want to get notifications for, click on **Select events** under **Events related to actions on accounts** or **Events related to user activities**. Select the events you want to get notified about from the list of events.



- The selected events are shown in a green box. Any of the selected events can be removed by clicking on the **X** present adjacent to the event. To clear all selected events, click on the **Clear all** button.

When do you want to get Notified?

You can choose to either get notified **As and when the events occur** or **As a consolidated email, once a day**. Specify your choice accordingly.

Who to Notify?

- You can trigger the notification upon the occurrence of the selected events to any specific user(s) or usergroup(s). You may even choose to trigger notifications for certain specific roles of users too - for example, ‘All Administrators’, ‘All Auditors’, etc.

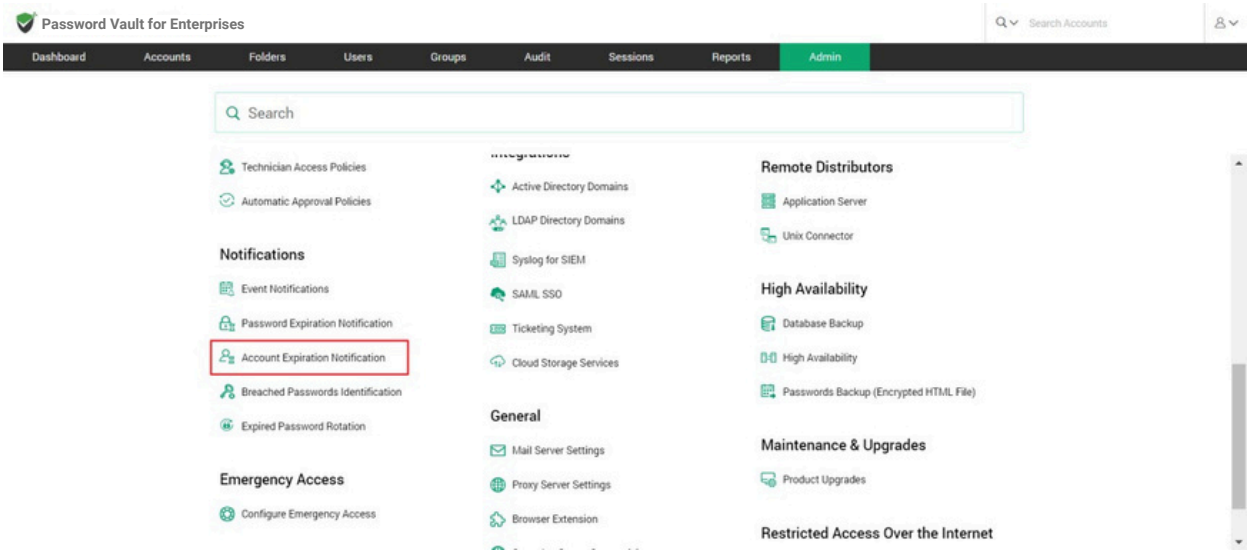
- You can also send notifications to people who are not registered users in Securden by specifying their email address in the box named **Others (specify email address)**

Account Expiration Notification

The expiration dates of licensing keys and certificates saved in Securden can be tracked. You can send email alerts a set number of days before the expiration date to act as a reminder. Administrators, auditors, owners of the respective accounts, and any specified users can receive notifications.

Configure Account Expiration Notification

Navigate to **Admin >> Notifications >> Account Expiration Notifications**.



Enable Expiration Notification to view the configuration options.

To Configure Account Expiration Notification, follow these steps.

The Notification Schedule

- You can configure Securden to send notifications on an impending account expiration. You can send notifications multiple times before the expiration date.
- You can add any number of Notifications by clicking on the '**+**' sign.
- Specify the number of days prior to the date of expiration a notification needs to be sent in each of the Notification schedules opened.

Who to Notify?

- You can trigger the notification upon the occurrence of the selected events to any specific user(s) or usergroup(s). You may even choose to trigger notifications for certain specific roles of users too - for example, 'All Administrators', 'All Auditors', etc.

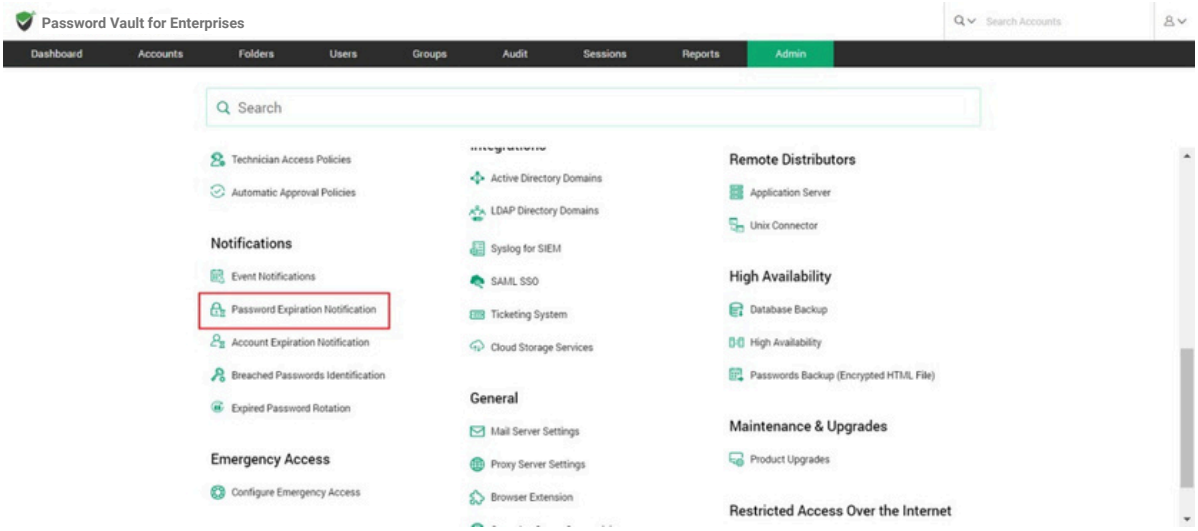
• You can also send notifications to people who are not registered users in Securden by specifying their email address in the box named **Others (specify email address)**.

Password Expiration Notification

You can send email notifications a specified number of days before the passwords expire to remind users to update their passwords. You can set up notifications to be sent any number of times before the password expires till it is reset. Administrators, auditors, owners of the respective accounts, and any specified users can all receive notifications.

Configuring Password Expiration Notification

Navigate to **Admin >> Notifications >> Password Expiration Notifications** to configure this feature.



Enable Expiration Notification to view the configuration options.

To Configure Password Expiration Notification, follow these steps

The Notification Schedule

- You can configure Securden to send notifications on an impending password expiration. You can send notifications multiple times before the expiration date.
- You can add any number of Notifications by clicking on the '**+**' sign and delete them by clicking on '**-**'.
- Specify the number of days prior to the date of expiration a notification needs to be sent in each of the Notification schedules opened.

Who to Notify?

- You can trigger the notification upon the occurrence of the selected events to any specific user(s) or usergroup(s). You may even choose to trigger notifications for certain specific roles of users too - for example, 'All Administrators', 'All Auditors', etc.
- You can also send notifications to people who are not registered users in Securden by specifying their email address in the box named **Others (specify email address)**.

Breached Password Identification

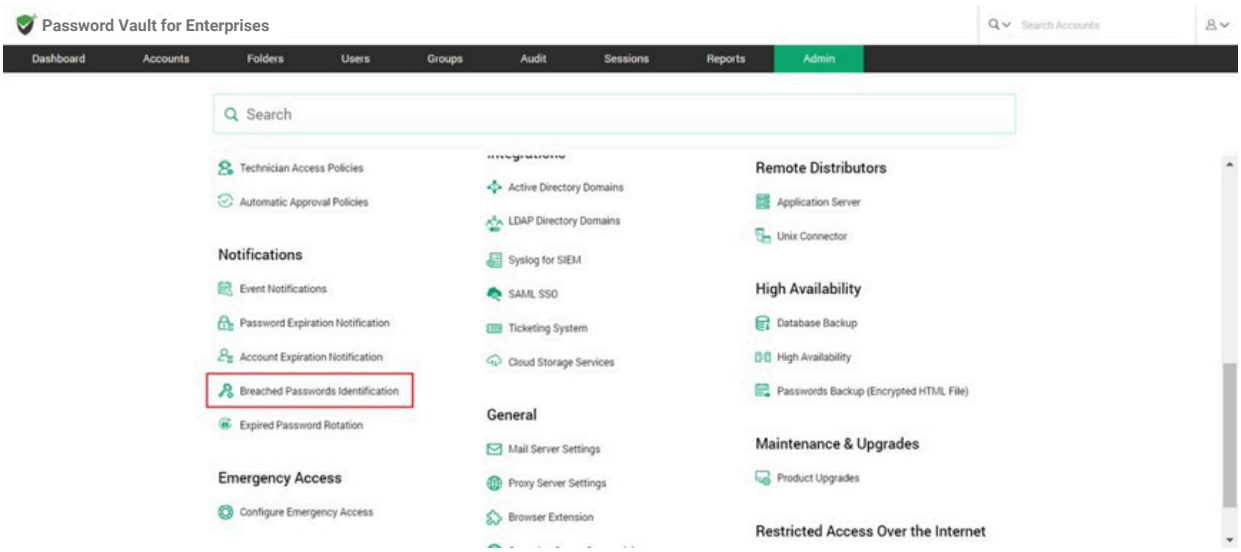
Passwords exposed in various data breaches worldwide are publicly available as a data dump. Many times, users are not aware when their passwords are exposed in credential spilling attacks. If a breached password is being used,

it may lead to a spate of cyberattacks. To prevent such incidents, Securden can periodically scan the dump and check if any of the passwords stored in the product matches with the passwords that have been exposed in known data breaches. You can configure how often Securden should check for breached passwords. Whenever usage of a breached password is detected, email alerts will be sent to administrators, auditors, respective account owners, and other specified users.

Important Note: In addition to periodic checks, Securden runs this check at the time of account addition and password change events provided the product is connected to the internet.

Configuring Breached Password Identification

Navigate to **Admin >> Notifications >> Breached Password Identification.**

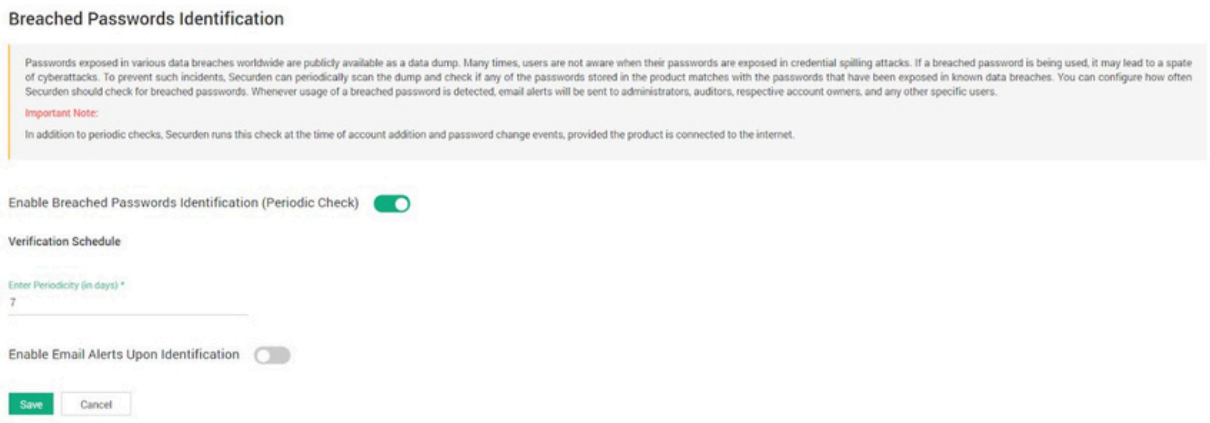


Enable breached password Identification to view the configuration options.

To configure Breached Password Identification, follow these steps.

Periodicity of checks

- You can specify the interval (in days) at which the breached passwords identification check is to be performed.
- You can get email notifications whenever a breached password is identified by enabling the **Enable Email Alerts Upon Identification** option.



Who to Notify?

Upon enabling email alerts, you can choose who receives the notification upon identification.

- You can trigger the notification upon the occurrence of the selected events to any specific user(s) or usergroup(s). You may even choose to trigger notifications for certain specific roles of users too - for example, ‘All Administrators’, ‘All Auditors’, etc.
- You can also send notifications to people who are not registered users in Securden by specifying their email address in the box named **Others (specify email address)**.

Expired Password Rotation ENTERPRISE PAM

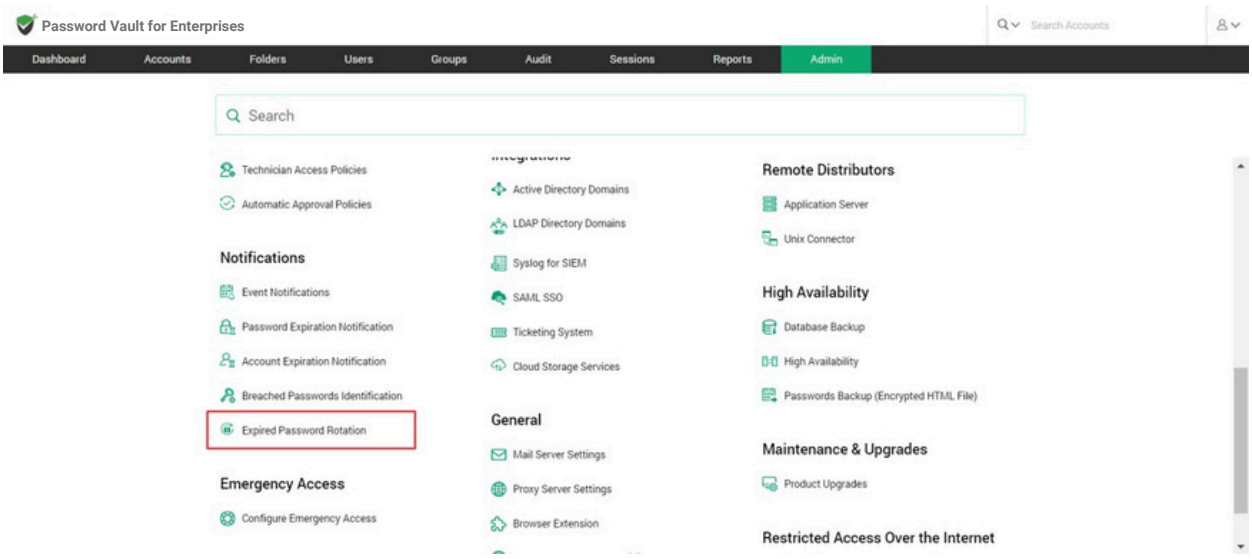
When passwords expire or are about to expire, Securden can automatically rotate them for accounts remote password reset is enabled. You can indicate the number of days until the password expires that the password rotation should be tried, as well as the number of attempts.

You don't have to change passwords manually anywhere because the new password is updated in both the end machine and the Securden database.

Important note: Only accounts for which remote access credentials have been provided can have password rotation configured. Go to **Admin >> Device Level Configurations** to set up remote credentials.

Configuring Password Rotation

Navigate to **Admin >> Notifications >> Expired Password Rotation**.



To be able to configure the settings, you need to enable the **Reset Passwords Upon Expiration** option.

You can configure Securden to carry out password changes either '**On Expiration Date** or a few days **Prior to Expiration** date.

If you choose **On Expiration Date**,

- You need to provide the frequency of password reset attempts, which can be as low as a minute.
- You should also specify the maximum number of attempts to be made to reset a password in **Number of retries**.
- You can choose to **Reset the already expired password**. Securden will try to reset the expired passwords at the time of configuration.

If you choose **Prior to Expiration**,

- You should specify how many days before the expiration date the reset attempts should be made.

- You need to provide the frequency of password reset attempts, which can be as low as a minute.
- You should also specify the maximum number of attempts to be made to reset a password in the field named **Number of retries**.
- You can choose to make reset attempts in accounts whose passwords are about to expire and the passwords that have already expired by clicking on the respective checkboxes.

Event Listener

Trigger automated follow-up actions upon the occurrence of specific events

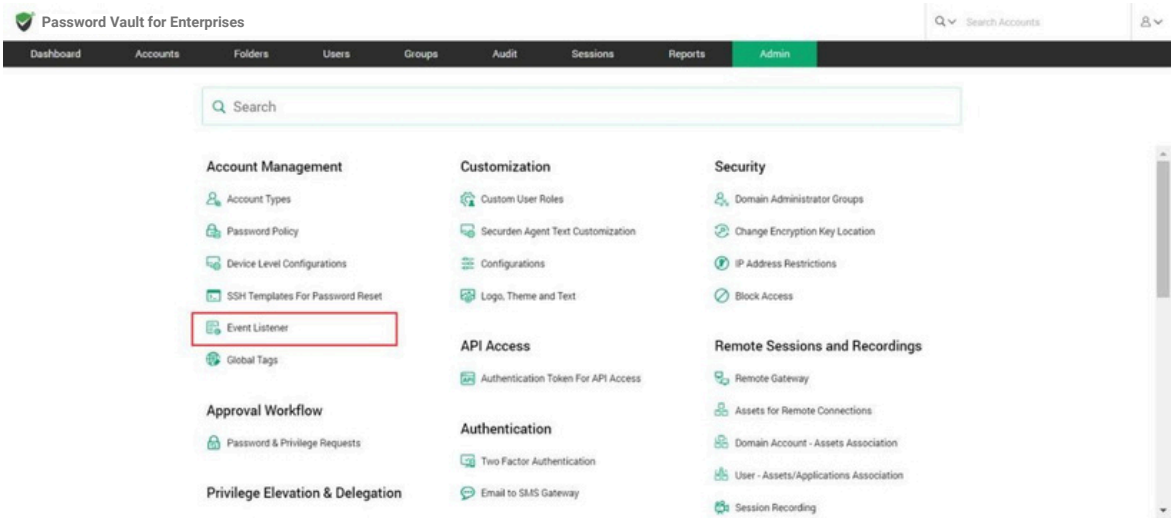
IT and DevOps often face the need to rapidly initiate a series of tasks upon the occurrence of certain events. Automation takes care of initiating the required tasks in a timely manner.

You can trigger the automated follow-up action(s) upon the occurrence of any specific event or a sequence of events in Securden. For example, when the password of an account is retrieved or changed, you can trigger a follow-up action automatically. Typically, Securden keeps listening for the event to occur and triggers the script defined by you to initiate the follow-up action.

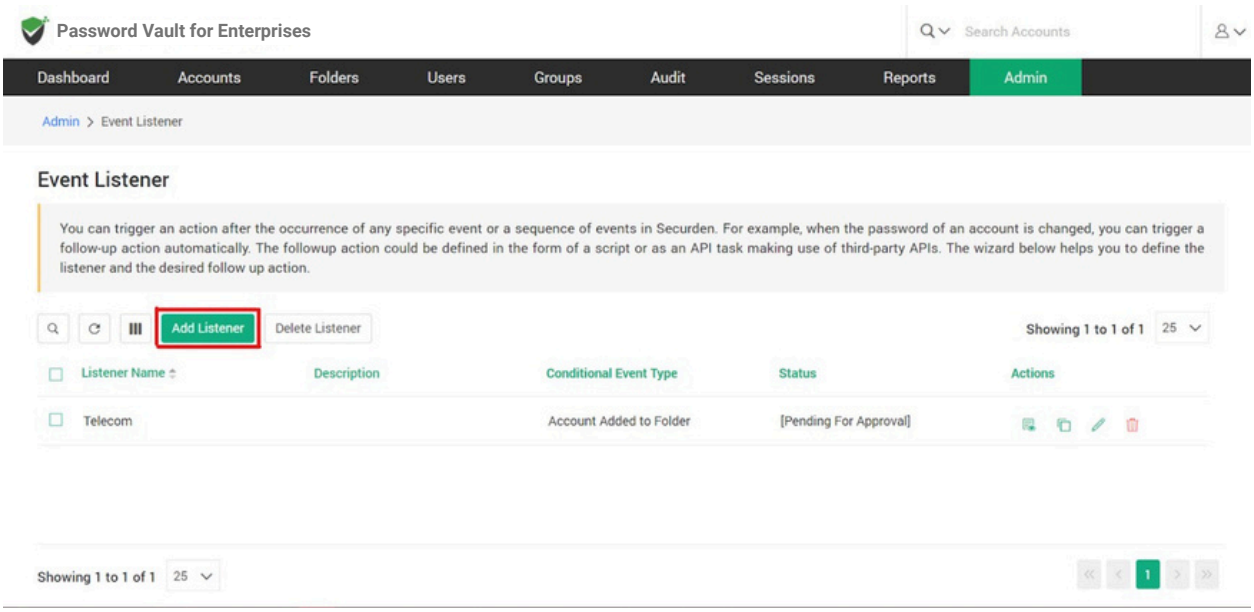
Creating the event listener

Creating the event listener involves configuring settings in Securden and defining the required follow-up action(s). Typically, you need to specify the conditional event (upon the occurrence of which you want to trigger the follow-up action), then the specific accounts in Securden that are to be considered for the conditional action.

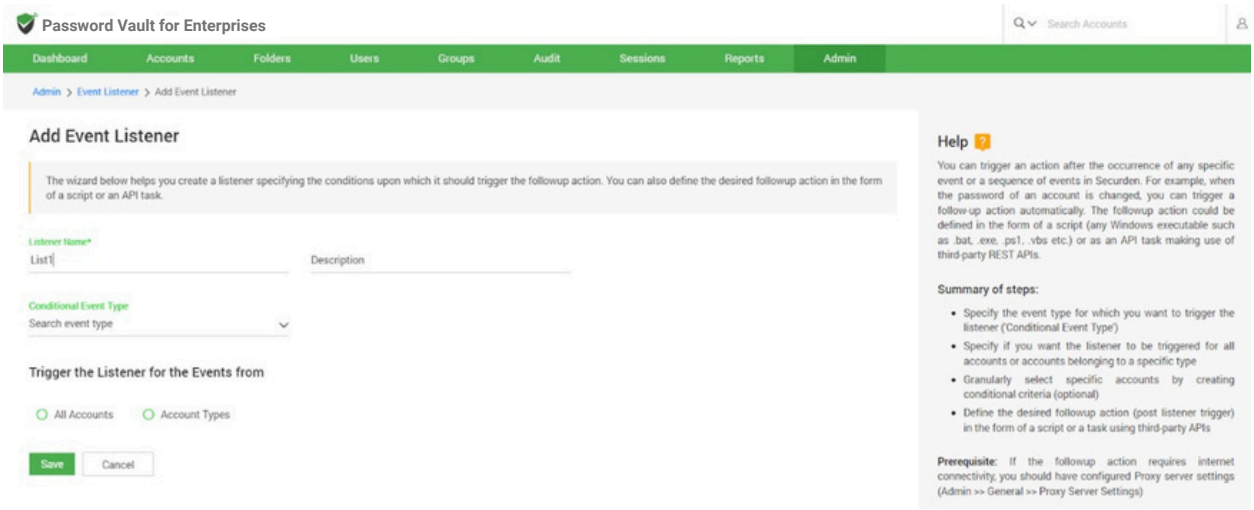
To configure or add an Event Listener, navigate to **Admin >> Account Management >> Event Listener**



To add an event trigger, click on **Add Listener.**

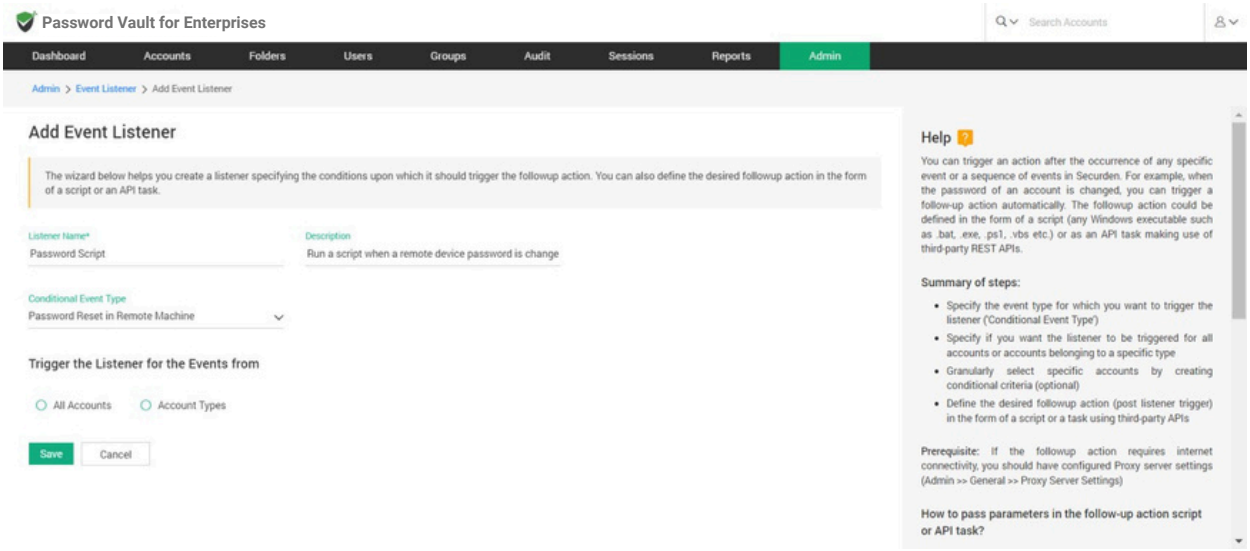


Clicking on **Add Listener** takes you to the settings GUI to add listener-related attributes.



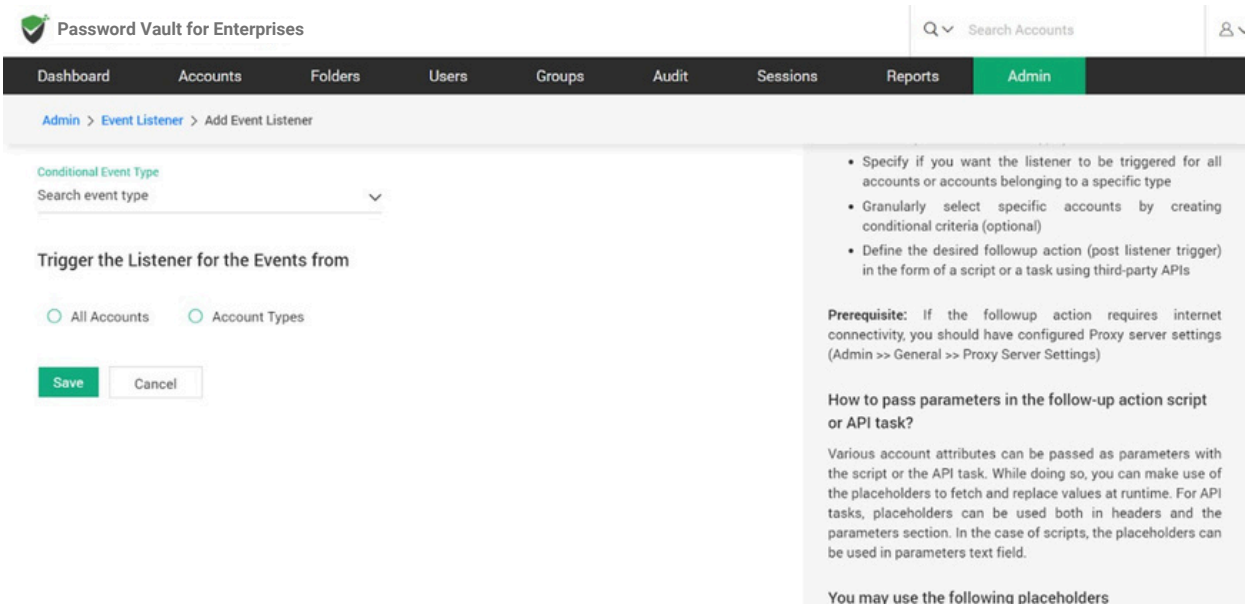
Provide a Name and description for the Listener

- **Listener name**: A listener name should be included for easy access on the listener lists page. This is done for quick identification.
- **Description**: A brief description of what the listener was created for or a general categorization of the listener can be given to have an overview of it.



Specify the event type to trigger the listener

The listener can be triggered for certain conditional event types. You can select the event type from the scroll list by clicking **Search event type.**



Some of the **conditional events** are Account Added, Account deleted, Account added to Folder, Account removed from Folder, Breached password identified, Password changed locally, Password reset in a remote machine, and Password retrieved.

Specify account types for listener to be triggered

You can choose an event listener to be triggered for activity in all accounts or for a specific account type like Linux, MAC, Windows Domain account, and others.

Click on **All Accounts** to trigger an event for all accounts.
Click on **Account Types** and select the type from the drop-down list.

Granularly select specific accounts

You can create granular conditions to trigger the listener only for a select list of accounts matching the criteria to suit your needs. You need to specify the account attributes needed or not needed as the selection criteria. To proceed with this step click on **Specify Attributes for Granular Selection.**

While selecting multiple attributes, you can choose between using the AND operator and the OR operator. Choosing AND will let you select all accounts that satisfy both conditions. Choosing OR will let you select all accounts that satisfy a minimum of one of the conditions.

You can choose the attributes you want to use as the criteria for selecting accounts from the drop-down list. The various options include **Account Title, Account Name, Address, Notes, Tags,** and **Folder Name.**

For each of the selected attributes, you can choose the condition from Equals, Contains, and Does Not Contain.

Specify the **Value** of the attribute chosen and choose the condition according to the rules below.

Condition:

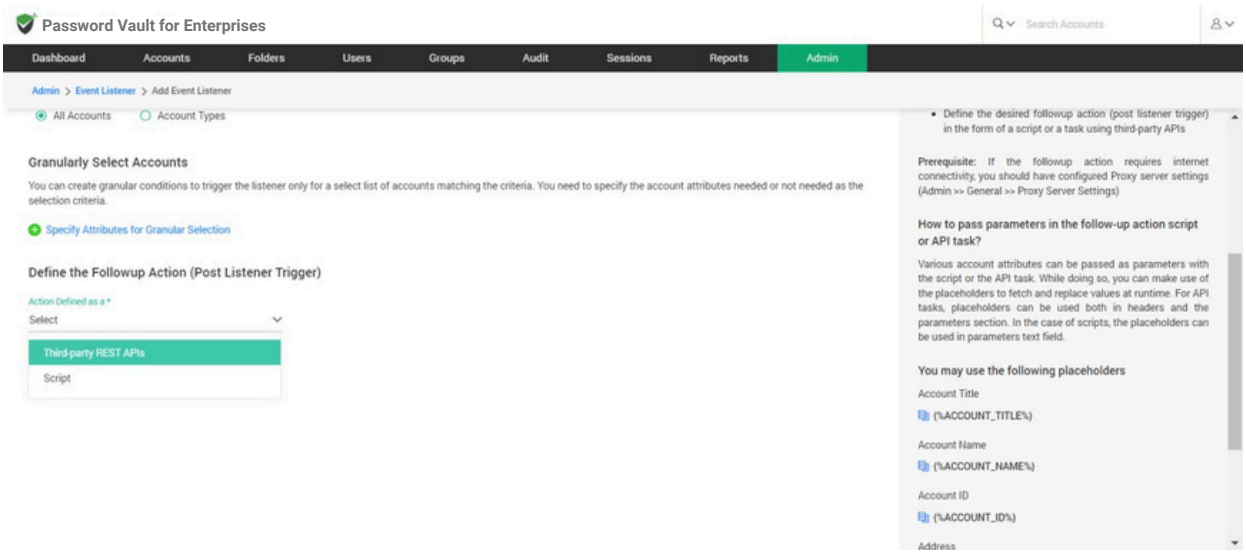
Equals mean the **Value** specified is an exact match to the account's attribute.
Contains mean the **Value** specified is a part of the account's attribute.
Does Not Contain means the **Value** specified is not a part of the account's attribute.

To add a criterion, you can click on **"+"** at the RHS.
To remove a criterion, you can click on **"-"** at the RHS.

Define the desired follow-up action

The follow-up action can be either in the form of a script or a task using third-party APIs.

Prerequisite: If the follow-up action requires internet connectivity, you should have configured Proxy server settings (Admin >> General >> Proxy Server Settings).



Setting up follow-up actions with a script

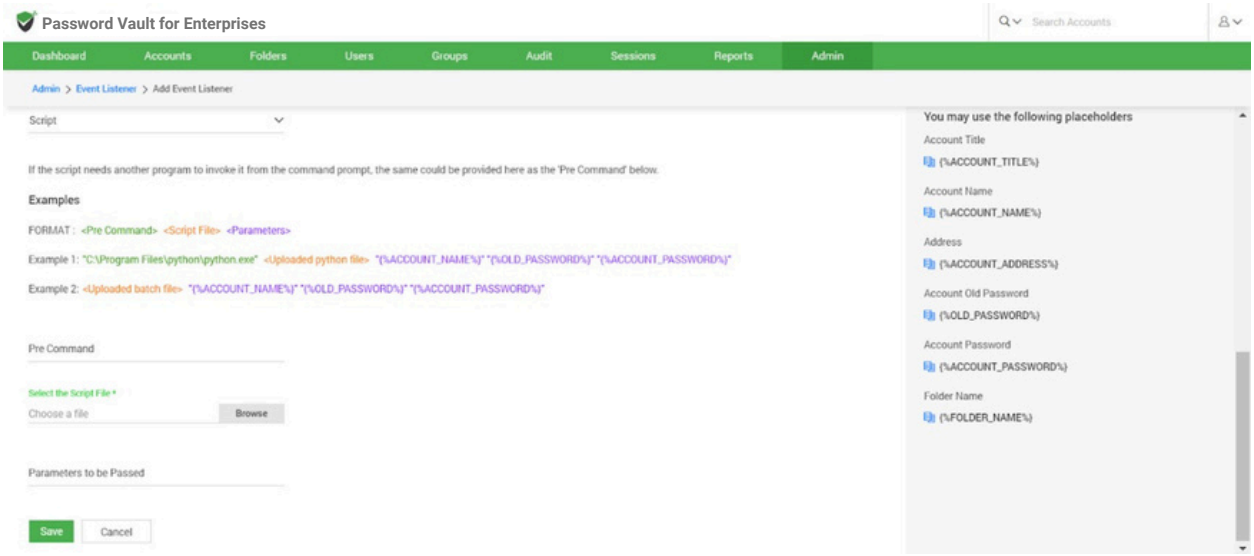
Summary of steps:

- Key in the **Pre-Command**: If the script needs another program to invoke it from the command prompt, the same could be provided here as the 'Pre Command'.
- Select the **Script file** from your computer.
- Choose the **Parameters to be Passed.**

FORMAT: <Pre Command> <Script File> <Parameters>

Pass parameters in the follow-up action Script/API task

Various account attributes can be passed as parameters with the script or the API task. While doing so, you can make use of the placeholders to fetch and replace values at runtime. For API tasks, placeholders can be used both in headers and the parameters section. In the case of scripts, the placeholders can be used in the parameters text field.



You may use the following placeholders:

- Account Title {%ACCOUNT_TITLE%}
- Account Name {%ACCOUNT_NAME%}
- Address {%ACCOUNT_ADDRESS%}
- Account Old Password {%OLD_PASSWORD%}

- Account Password {%ACCOUNT_PASSWORD%}
- Folder Name {%FOLDER_NAME%}
- Name of the account for remotely logging in to the IT asset {%REMOTE_LOGIN_ACCOUNT_NAME%}
- Password of the remote login account {%REMOTE_LOGIN_ACCOUNT_PASSWORD%}
- Name of the account that has privileges to do remote operation {%PRIVILEGED_ACCOUNT_NAME%}
- Password of the privileged account {%PRIVILEGED_ACCOUNT_PASSWORD%}

Setting up follow-up actions with a Third-party REST API

Select the request type from GET, PUT, POST, DELETE.

The four main HTTP methods (GET, PUT, POST, and DELETE) can be mapped to CRUD operations as follows:

GET retrieves the representation of the resource at a specified URL.
GET should have no side effects on the server.

PUT updates a resource at a specified URL. PUT can also be used to create a new resource at a specified URL, if the server allows clients to specify new URIs. For this tutorial, the API will not support creation through PUT.

POST creates a new resource. The server assigns the URL for the new object and returns this URL as part of the response message.

DELETE deletes a resource at a specified URL.

- Enter the Request URL where the request type will be applicable
- Choose to add Headers or API Parameters using **Add Headers** and **Add Parameters.**

To enter multiple Headers or Parameters use the **+** sign.
To remove a Header or Parameter use the **-** sign.

Enter the details of Name and Value for Headers and API parameters.

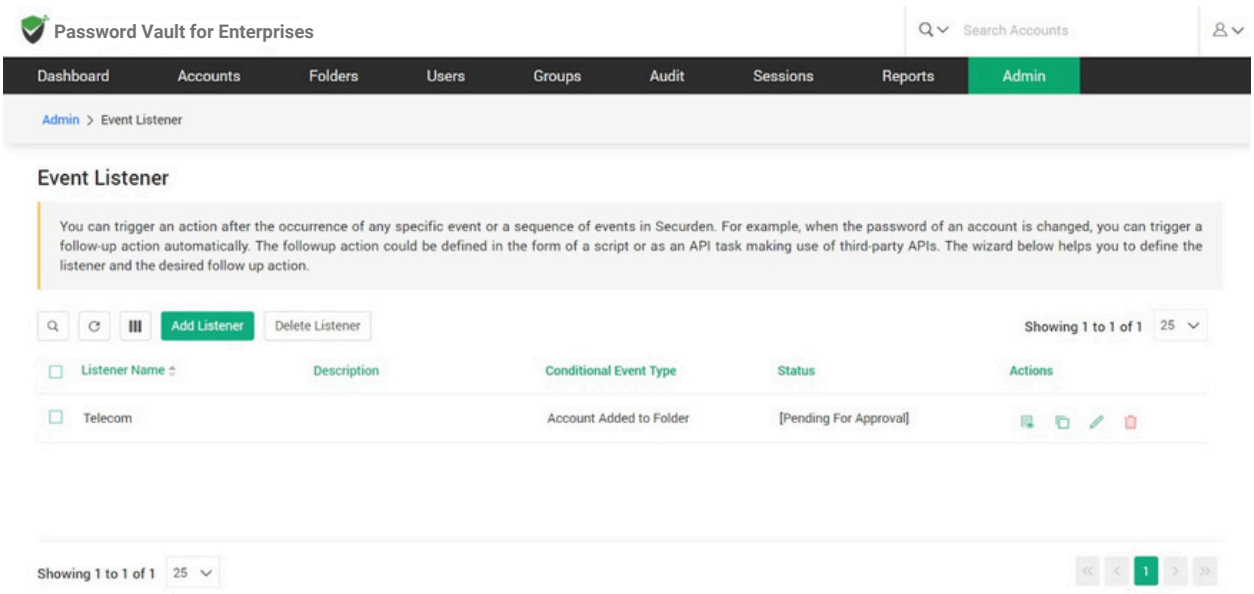
- API headers are like **an extra source of information for each API call you make** to represent the meta-data associated with an API request and response.

- API parameters are **the variable parts of a resource**. They determine the type of action you want to take on the resource. Each parameter has a name and value type.

Once all the fields have been filled, click on **Save**, if you wish to stop the listener configurations midway, simply click **Cancel.**

Event listener actions

You can configure event listeners added in Securden, you can choose to Delete, Edit, or Clone an event listener.



Delete a listener - To delete listeners, select them from the list and click **Delete Listener** OR delete them individually using the <**Red icon>** in **Actions.**

View Listener - gives you a brief of the Listener name, Event type, Trigger action, and Description. To access this, click on the **view icon.**

Clone Listener - To create a listener with similar details to an existing one, use the **clone icon**. This takes you to the Add listener configuration with all the pre-filled details of the clone, change the fields as needed and click **Save**.

Edit Listener - To edit a listener, click on the **edit icon**. This lets you change any field you have entered while adding the listener.

Section 6: API Access

APIs for Programmatic Access

Identities are present everywhere and in every piece of IT. Apart from the passwords, keys, and other credentials used by humans, every organization has to deal with a lot of machine identities, credentials embedded on scripts and applications, and so on. Securden provides APIs for programmatic access of the data stored in the product. Scripts, applications, and configuration files that require credentials can access the Securden database and fetch the data, thus eliminating the dangerous practice of hard-coding of credentials. API access is regulated through a token-based authentication mechanism.

To programmatically access an account through API, you need an URL and the Auth Token. The token can be a static one or dynamic and valid for a specified time duration or forever. The access can be restricted from specific IP addresses or FQDNs. Also, tokens can be applicable only for a specific list of operations.

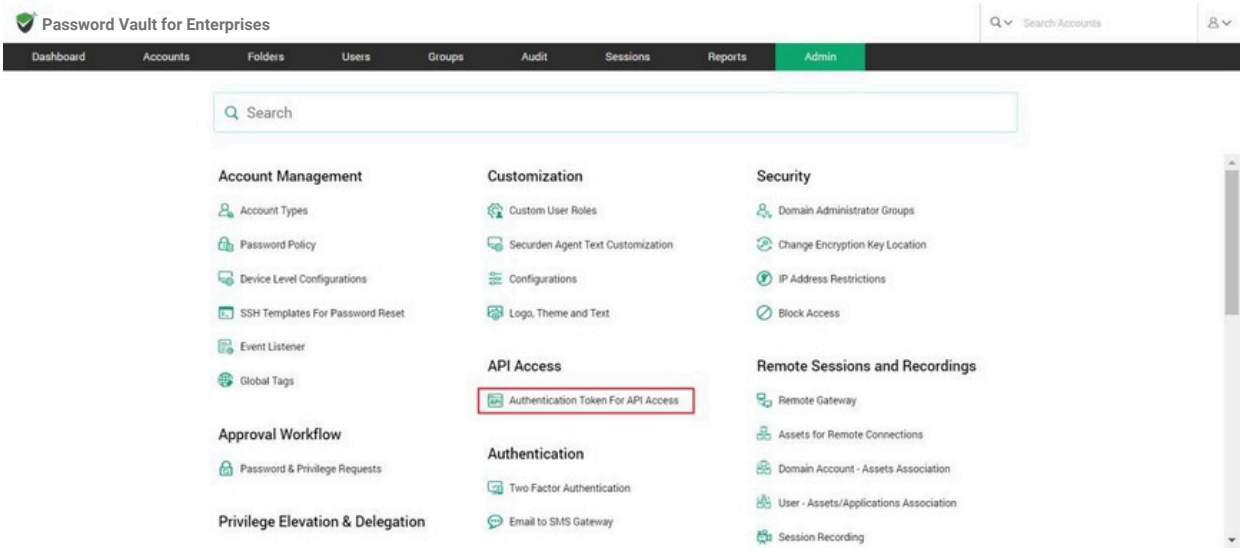
As mentioned above, you require two things for API access:

- Authentication token
- Access URL

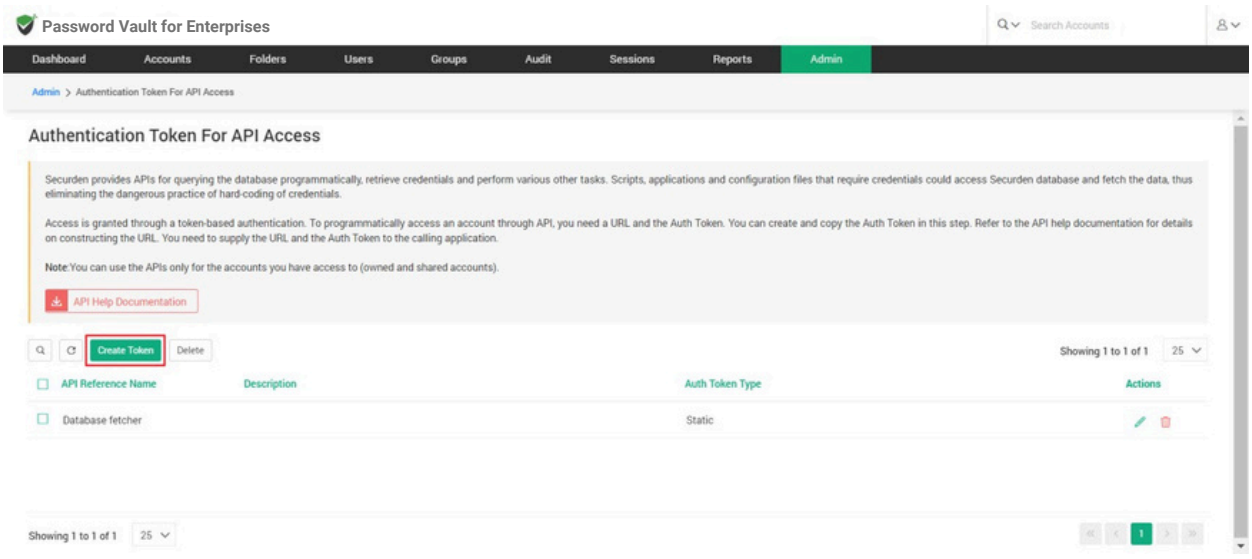
You need to create the authentication token in the GUI and then construct the URL referring to our API reference guide. You need to supply the URL and the Auth Token to the calling application.

How to create the authentication tokens for APIs?

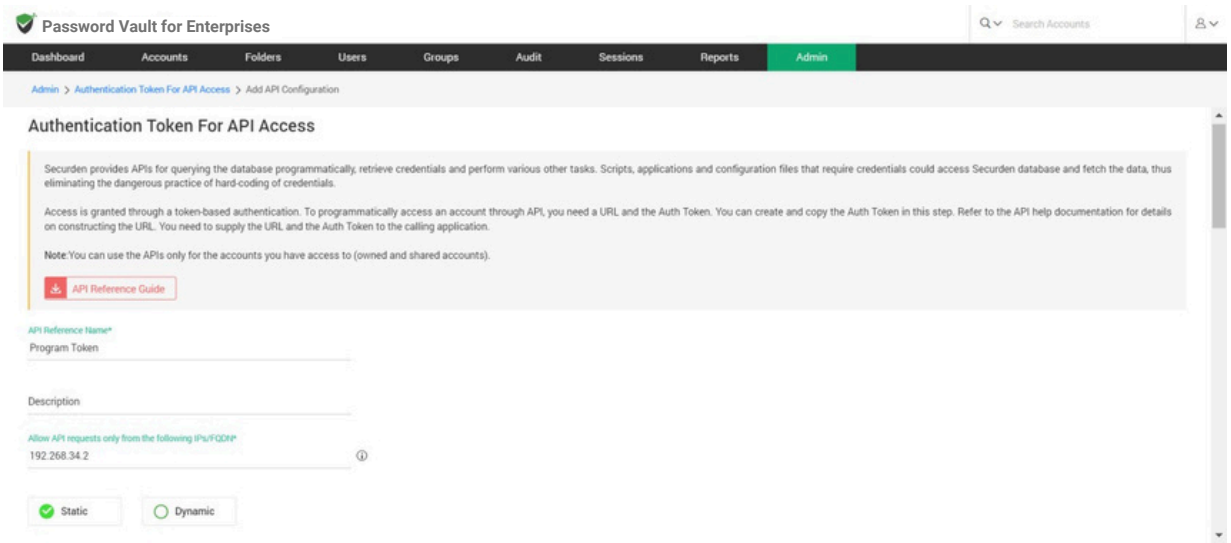
To create tokens for APIs, **navigate to Admin >> API Access >> Authentication Token for API Access** section.



In the GUI that opens, click the button **Create Token**.



In the GUI that opens, you need to enter the following information:



Token name and description

Enter a name for the token being created. This **API Reference Name** helps you uniquely identify the token when using it in APIs. A description will help in tracking the purpose of the token.

Token access restrictions

If you want to restrict the token usage only from specific IP addresses, you may enter the same in the field “Allow API requests from the following IPs/FQDN”.

You can enter individual IP addresses in comma separated form or an IP range or FQDNs or CIDR notations.

Examples:

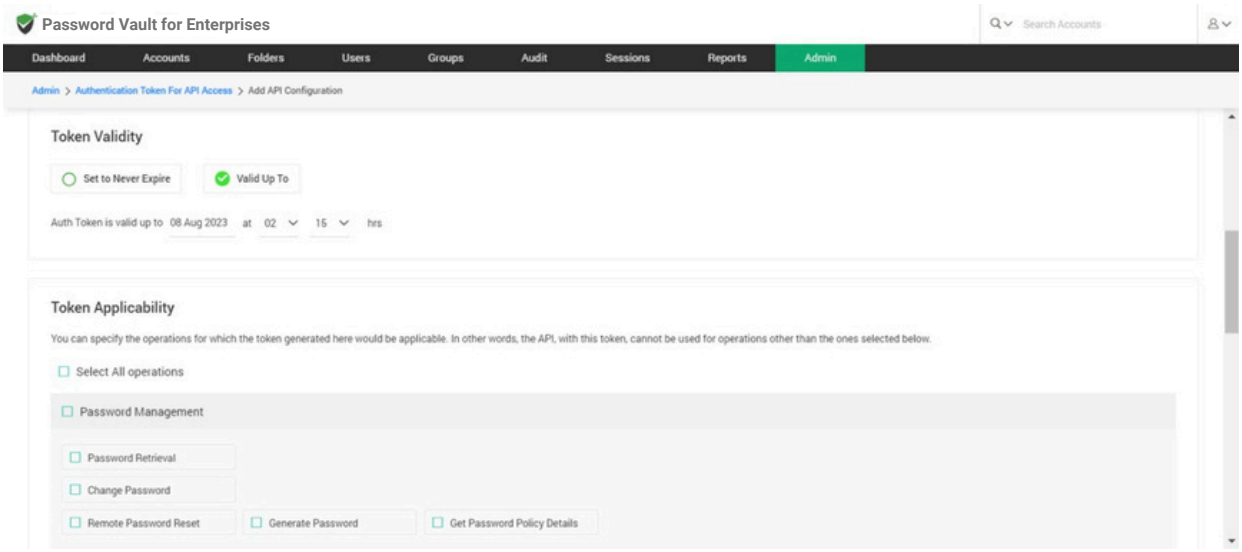
Specific IP Address: 191.224.1.22

IP Range: 224.1.1.10:224.1.2.1

CIDR Notation: 192.168.1.30/24

Token type

You can choose to create a static token or a dynamically changing one. Select your choice **Static** or **Dynamic** as required.

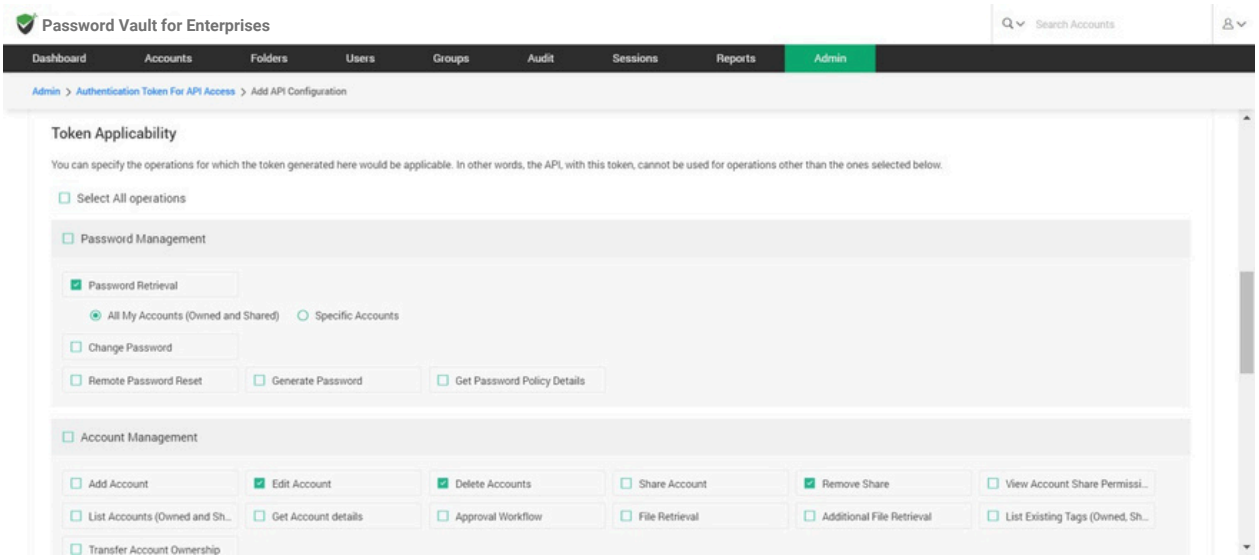


Token lifetime

You can also decide about the lifetime of the token being created. Static tokens can be created with a permanent validity **Set to Never Expire** or can be created to be valid for a predefined date and time. Select the option **Valid Upto** and set the validity date. Dynamic token will have a short lifespan in minutes.

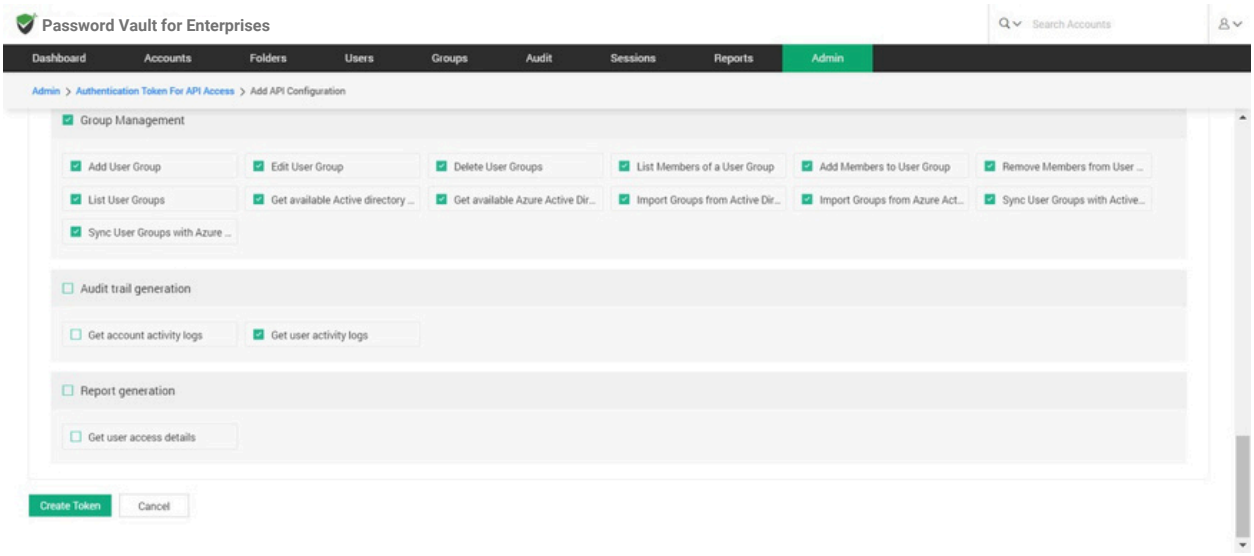
Token scope

You can define the scope of the token being created by restricting the operations for which the token generated here would be applicable. In other words, the API, with this token, cannot be used for operations other than the ones selected in scope. To define the scope, select the required operations under **Token Applicability**.

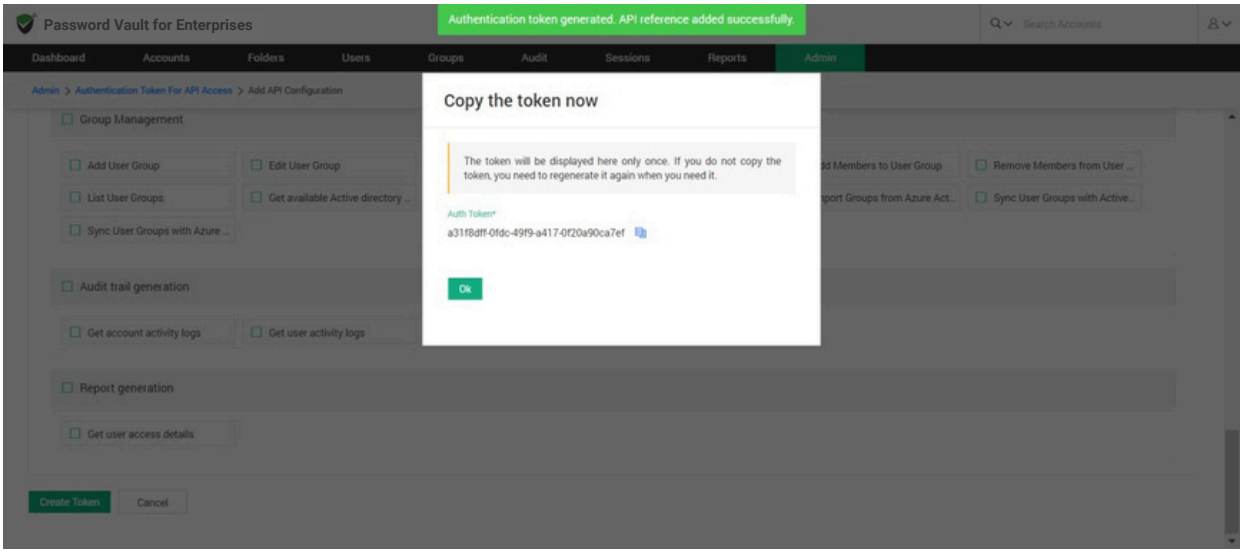


Create the token and copy the static token

After defining the scope, proceed to create the token.



If you have chosen the type **Static**, you will be prompted to copy the token to the clipboard. The token will be displayed only once and you can't refer to that again if you don't copy it.



Getting dynamic tokens Dynamic auth tokens can be obtained programmatically. Typically, you will obtain it as explained below. You will have to pass the credentials to access Securden as arguments.

GET /api/get_auth_token

Input data (arguments): login_name (String), password (String),

domain_name (Default authentication will be local)

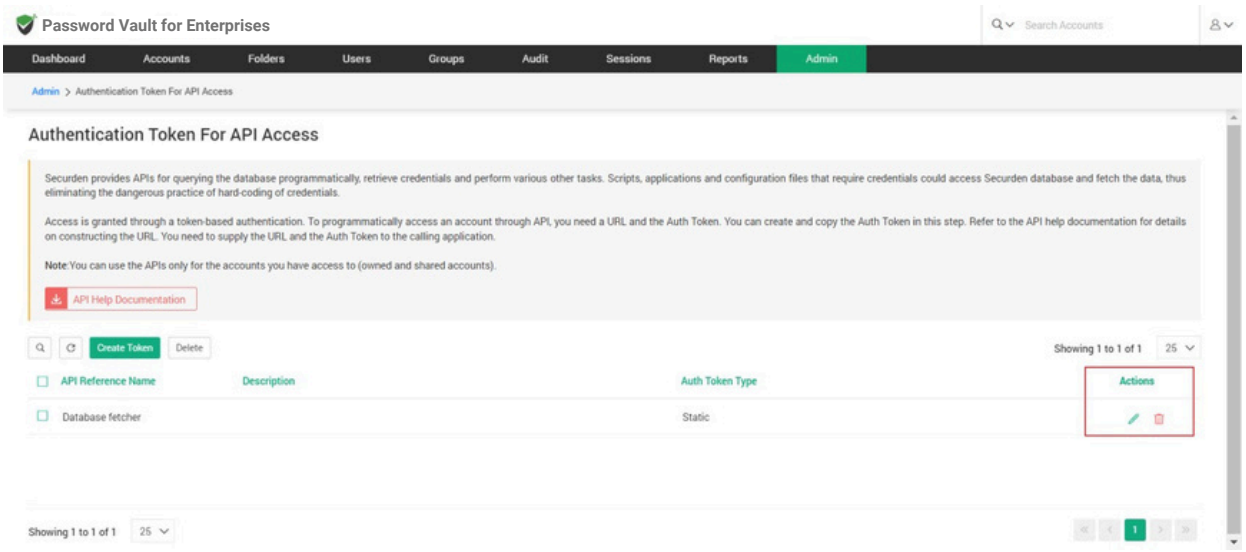
Example (if you are using Curl): curl -k -X GET

"https://vault.edmo.com/api/get_auth_token?login_name=admin&password

=admin&domain_name=xyz"

Edit, Delete, Update, Regenerate Tokens

You can use the **Actions** column on the APIs page to delete the tokens that are no longer needed. Similarly, you can edit the static tokens and extend their lifetime (validity period). In such cases, you will have to update and regenerate the token.



Token creation is the first step in API access. You need to construct the URL for use by applications, scripts, and configuration files.

Constructing the URL for API Access

To programmatically access an account through API, you need a URL with the Auth token. You have created the auth token through the steps detailed above. You can create the URL by following the steps detailed in the API Help Documentation present in **Admin >> API Access >> Authentication Token for APIs**. The documentation explain how the URL is to be constructed and the arguments to be passed for various operations.

Section 8: Folder Management

Organize Accounts with Folders

You can create folders and group **Accounts** for easy and efficient management. At any point of time, a specific account could be a member of only one folder. This means, an account cannot be a member of multiple folders. Grouping accounts into folders lets you perform actions like remote password resets for multiple accounts grouped in the folder at one go. You can also define a hierarchical structure with any number of folders and sub-folders.

You can add folders to Securden in two ways:

1. Add manually
2. Import from a file

Manually Adding Folders

Navigate to **Folders >> Add**. Provide the following details to create a folder.

Folder Name

You need to provide a name that uniquely identifies the folder. This name will appear on the left-hand side of the interface. The name will help you distinguish between folders while adding, deleting, and modifying accounts.

Description

You can also provide a description to further help classify the accounts for easy management.

Parent Folder

- If you want to create a stand-alone folder, leave this option as **--None--.**
- If you want to create a new subfolder to an existing folder, you should specify the existing parent folder by choosing the required folder from the drop-down list.

Inheritance of Share Permissions

- Once you select a parent folder, you will have the option to choose whether to inherit permissions from it or not . Select **Yes** if you want to inherit permissions. This means that the users and user groups having access to the parent folders will now have access to the subfolder with the same level of access permissions.
- Select **No** if you don't want the subfolder to inherit permissions granted to the parent folder.
- Choosing to inherit share permission will mean users who have shared access to the parent folder will now have access to the new folder with the same permissions (View/Modify/Manage). But, users with whom you

explicitly share the new folder will only obtain access permissions to the new folder.

- You can choose to switch inheritance **On** or **Off** anytime.

Notes

- You can add notes to a folder for classification, marking ownership, and sharing user guidelines.
- You can also add any miscellaneous remarks related to the folder and its content.

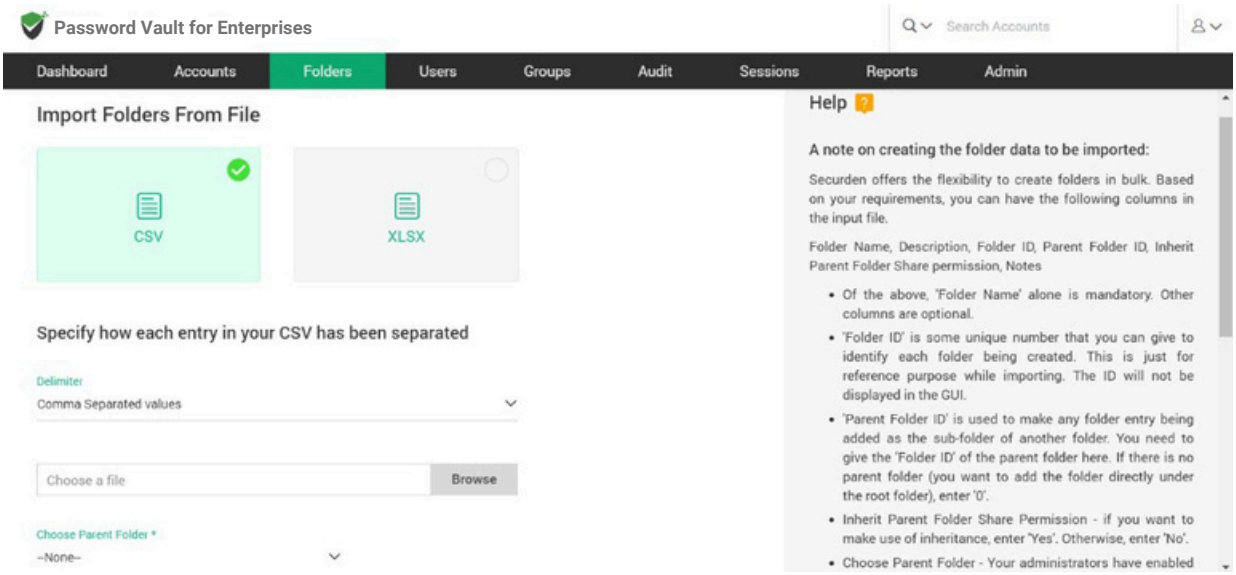
Add Accounts to the Folder

You can add accounts to the folder at the time of creation. An account could remain a member of one folder at a time. This means the same account cannot be added to multiple folders at the same time. Also, note that if inheritance mode is switched on, parent folders and the new folder will have the same share permission. That means, users who have access to the accounts stored in the parent folder(s), will get access to the accounts being added in this step.

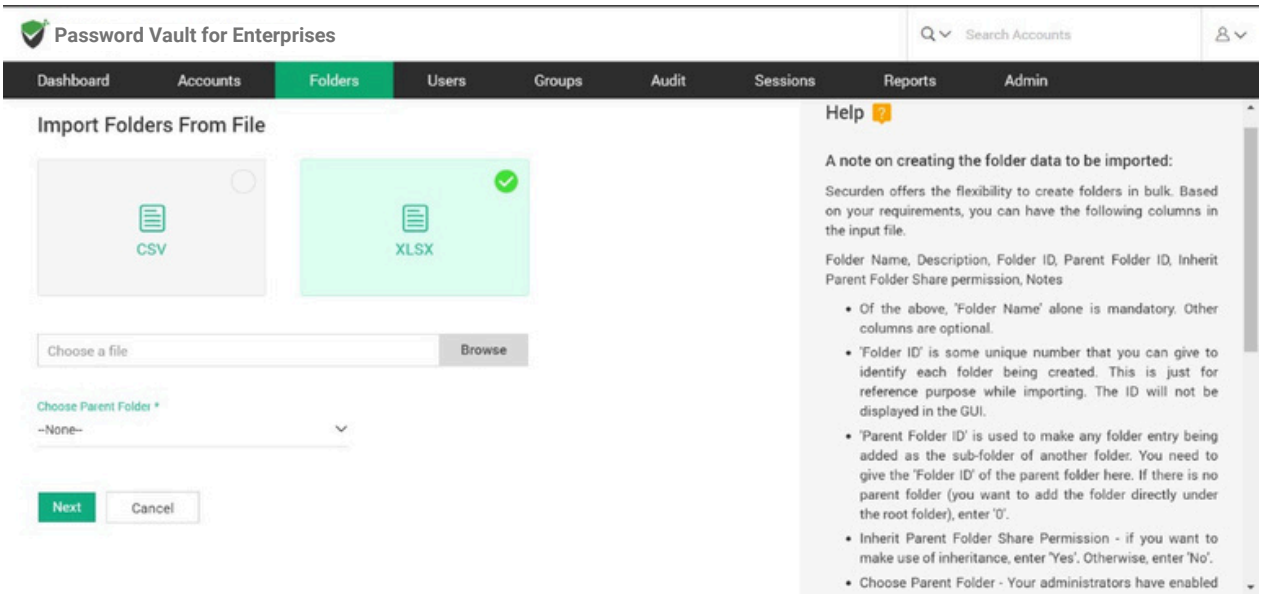
Import Folders from Files

In situations where multiple folders are to be added, you have the option to import them from a file.

Navigate to **Folders >> More >> Import Folders from Files**. You can either import folders from a CSV file or an Excel sheet.



- For CSV files, you need to specify how the values have been separated. You can choose between comma-separated values and tab-separated values. This is not required in the case of Excel Sheet (XLSX) files.



- Choose the file from your computer by clicking on **Browse**.

- If the imported folder is not a subfolder of a parent folder, leave the Parent Folder as **--None--**. If the folder is a subfolder, select the parent folder from the drop-down.

Note: If your administrators have enabled the configuration to enforce the selection of a parent folder while adding/editing a folder, you will only be able to import folders only as subfolders to folders for which you have **Manage** permission or to the folders you own.

A note on creating the folder data to be imported:

Based on your requirements, you can have the following columns in the input file.

Folder Name, Description, Folder ID, Parent Folder ID, Inherit Parent Folder Share permission, Notes

- Of the above, **Folder Name** is mandatory. Other columns are optional.

- **Folder ID** is an unique number that you can give to identify each folder being imported. This is just for reference purposes while importing. The ID will not be displayed in the GUI.

- **Parent Folder ID** is used to make any folder entry being added as the sub-folder of another folder. You need to give the **Folder ID** of the parent folder here. If there is no parent folder (you want to add the folder directly under the root folder), enter **0**.

- **Inherit Parent Folder Share Permission** - if you want to make use of inheritance, enter **Yes**. Otherwise, enter **No**.

Following are some sample entries:

IT Infrastructure, Description, 1,0, yes

Systems, Admin Team, 2, 1, yes

Windows, Tier 1 Team, 3, 2, yes

Linux, Tier 2 Team, 4, 2, no

This will create a folder structure as below:

IT Infrastructure

|

|__Systems

|

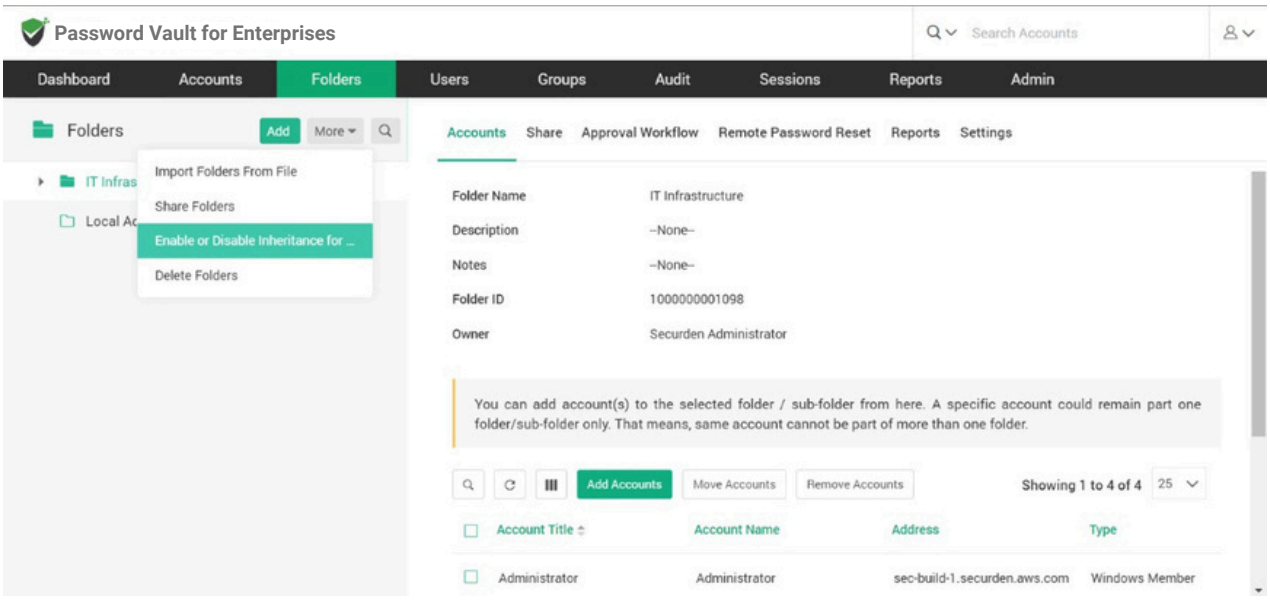
|__Windows

|

|__Linux

Enable and Disable Inheritance

You can enable and disable permission inheritance whenever you want. You can select multiple folders and configure inheritance permission by navigating to **Folders >> More >> Enable or disable Inheritance for Sub-Folders.**



You can also modify inheritance settings for a specific folder by navigating to **Folders >> Share**. This option is visible only when the selected folder is a sub-folder. This option is not valid for parent folders and stand-alone folders.

Quick Access Options

In addition to selecting a parent folder while adding a folder using manual method and when importing from files, you can also create subfolders from the quick access pane on the left side of the Folders GUI. If you hover the pointer over a folder, you will see two icons. One with the folder symbol and the other with a settings symbol.

1. The Folder icon represents **Add Sub Folder**.

2. The Settings icon has three different options. **Edit**, **Transfer Ownership,** and **Delete**.

Add Sub Folder

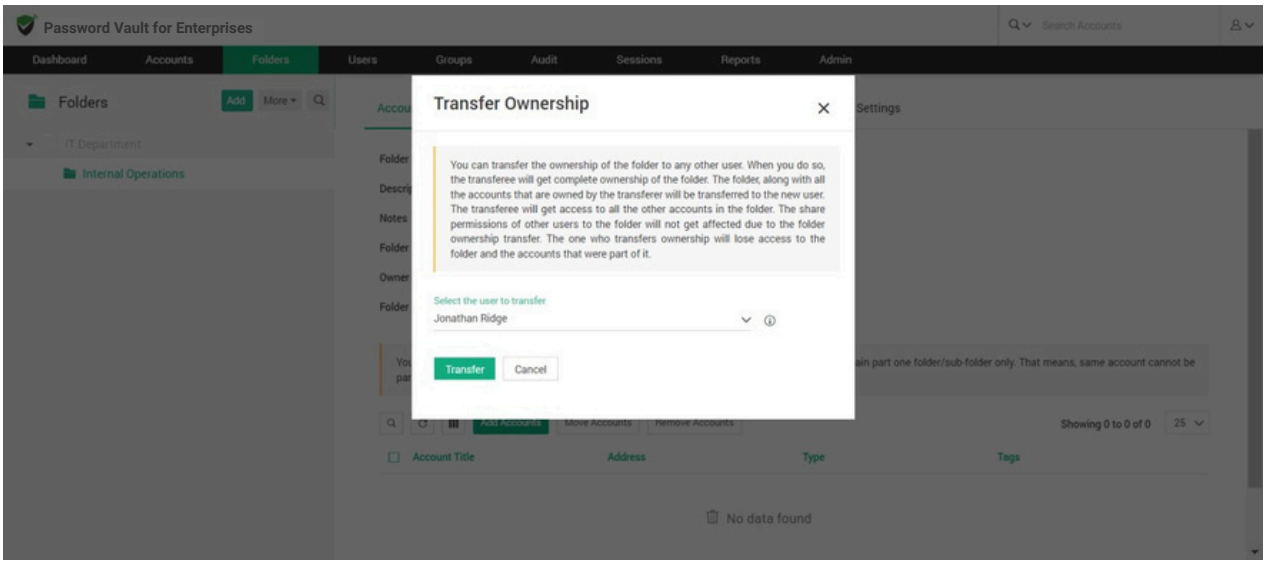
If you click the Folder icon, you will be redirected to the add folder page and the parent folder section will be auto-filled. You will still have to provide the other required information as mentioned in the **Manually Adding Folders** section.

Edit

In this section, you can alter the details of a folder while retaining the accounts added to it. All the details of a folder can be altered.
If a folder having subfolders is edited, the new details will be enforced to the subfolders automatically.

Transfer Ownership

You can transfer the ownership of an entire folder to another user instead of transferring the accounts one by one. In such an event, the Transferer will lose access to the accounts in the folder and the Transferee will get complete ownership of the accounts in the folder. The share permissions of other users will not be affected due to an ownership transfer.

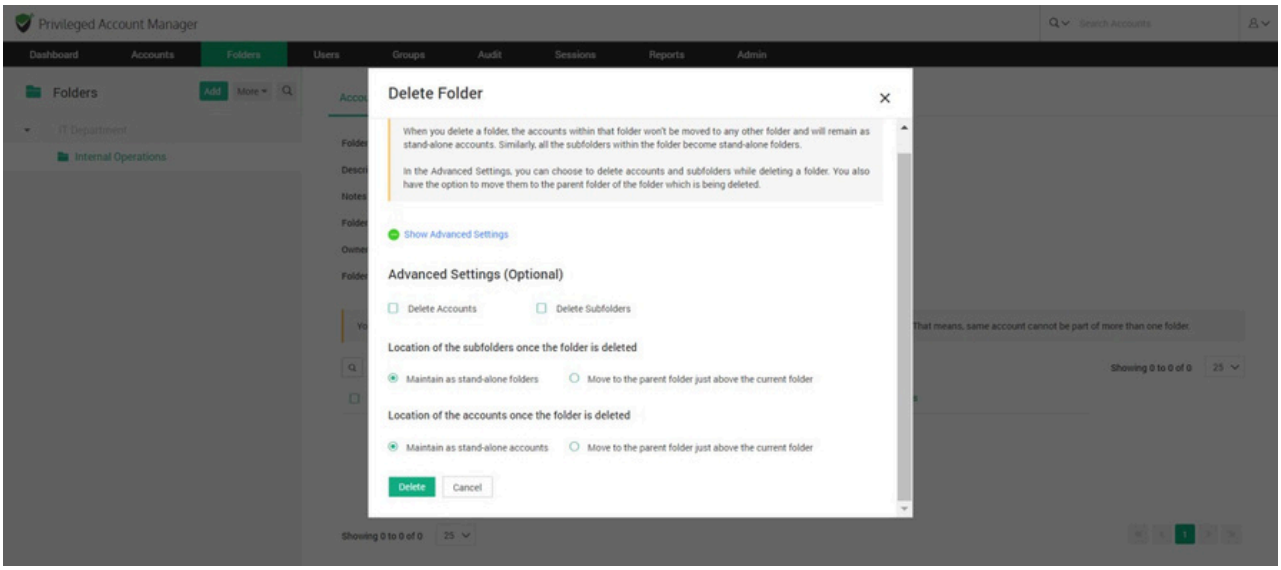


By default, Folders can only be transferred to Super Administrators, Administrators, and Account Managers. In the case of users with custom roles, the transferee should have add, edit, delete and share folder permissions.

To transfer the ownership of a folder, select the transferee from the list of users and click **Transfer**.

Delete

When you delete a folder, the accounts within that folder won't be moved to any other folder and will remain as stand-alone accounts. Similarly, all the subfolders within the folder become stand-alone folders.



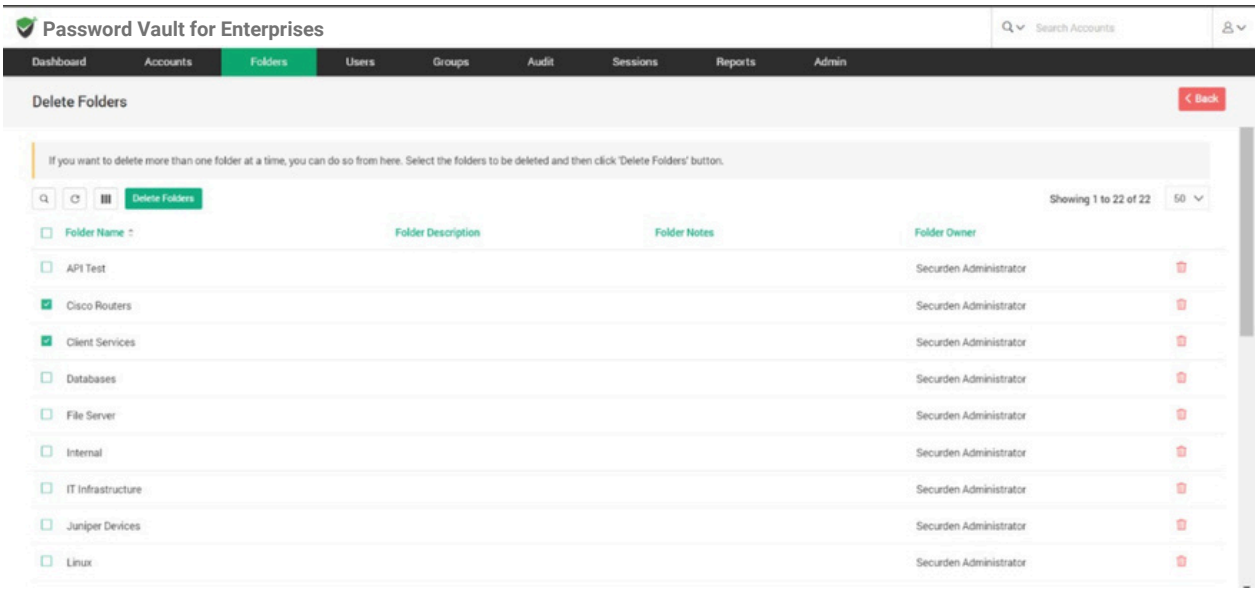
In Advanced Settings, you can choose to

1. Delete the accounts inside the Folder.
2. Delete SubFolders and subsequently delete the accounts in SubFolders.
   You can choose to maintain the folders and accounts as stand-alone or move them to the parent folder just above them in case you choose the accounts or the subfolders to not be deleted.

Deleting Multiple Folders

You can delete multiple folders at once. Navigate to **Folders >> More >> Delete Folders**.

Select the folders you want to delete and click **Delete Folders**.



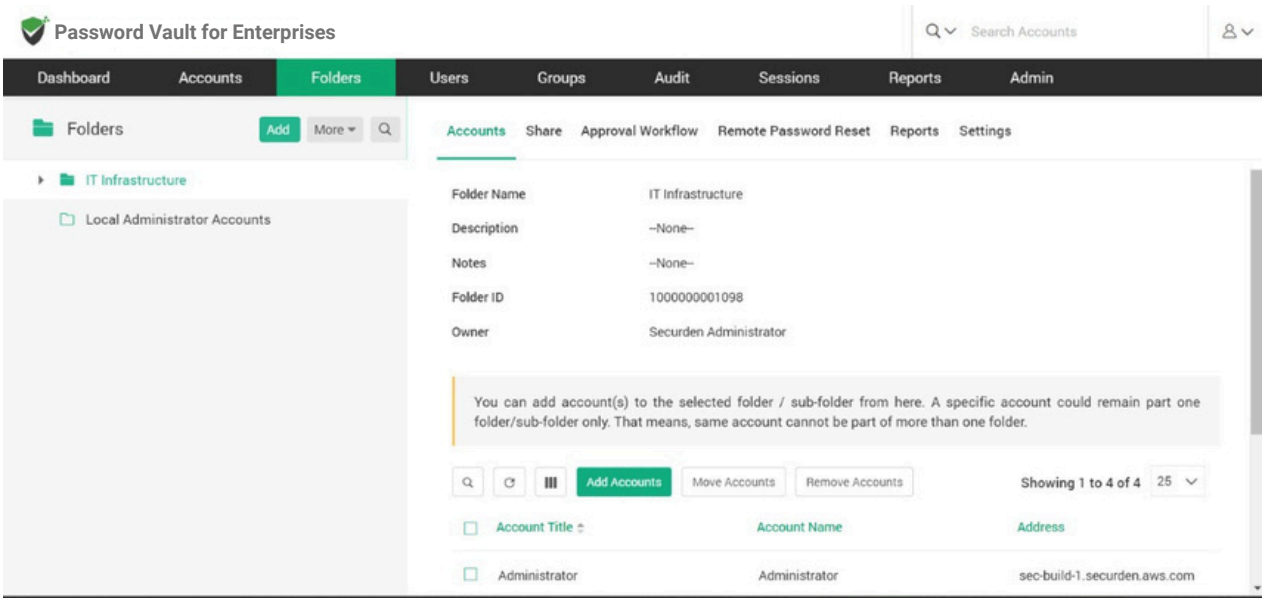
Manage Accounts in a Folder

You can add, search, move, and delete accounts by opening any folder for which you have **Manage** permission. An account can be a part of only one folder at any given time.

When you select a folder, the details such as the Folder Name, Description, Notes, Folder ID, and Owner (User name) will be displayed.

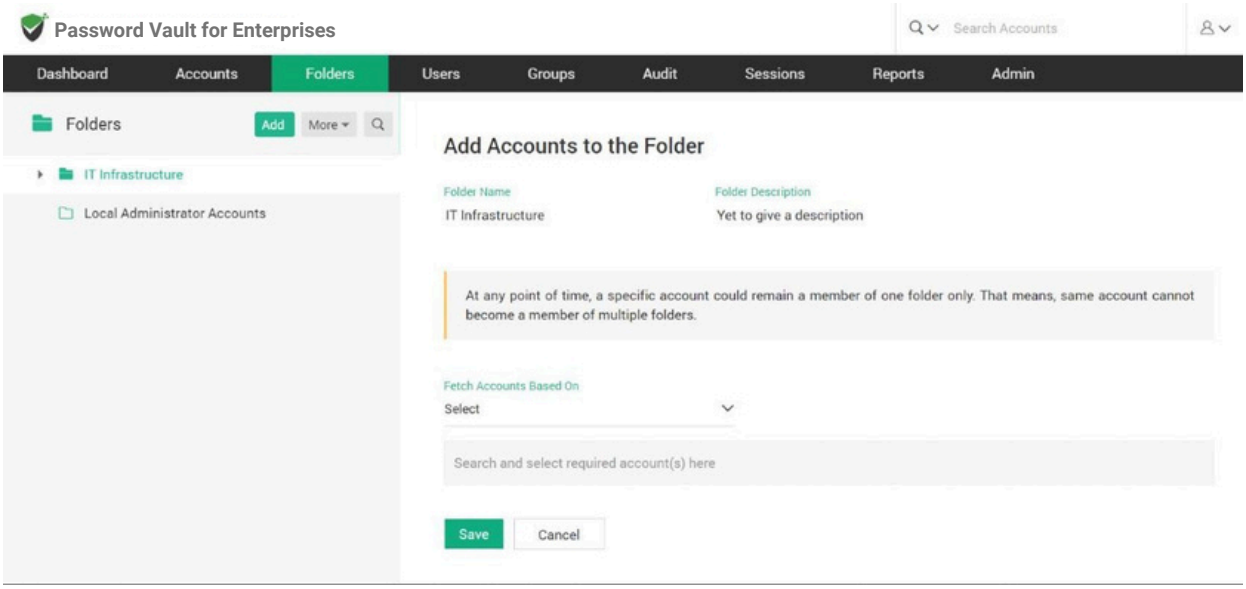
Below these details, the list of all accounts inside the folder will be displayed. The attributes of each account such as Account Title, Account Name, etc will be displayed. You can change which attribute to display by clicking on the **Column Chooser** icon.

You can view the list in batches of 25, 50, and 100 accounts at a time. To set the preferred batch size click on the drop-down button on the right-hand side of the Showing *x* to *y* of *y.*



Add Accounts

In addition to adding accounts at the time of folder creation, you can add accounts to a folder at any time. You can add accounts to a folder only if it is not already a part of another folder.



To add accounts to a folder,

1. Click on **Add Accounts**.

2. Here you can fetch a list of accounts based on any attribute such as Account Title, Account Name, DNS/IP address, Account Type, Notes, and Tags.

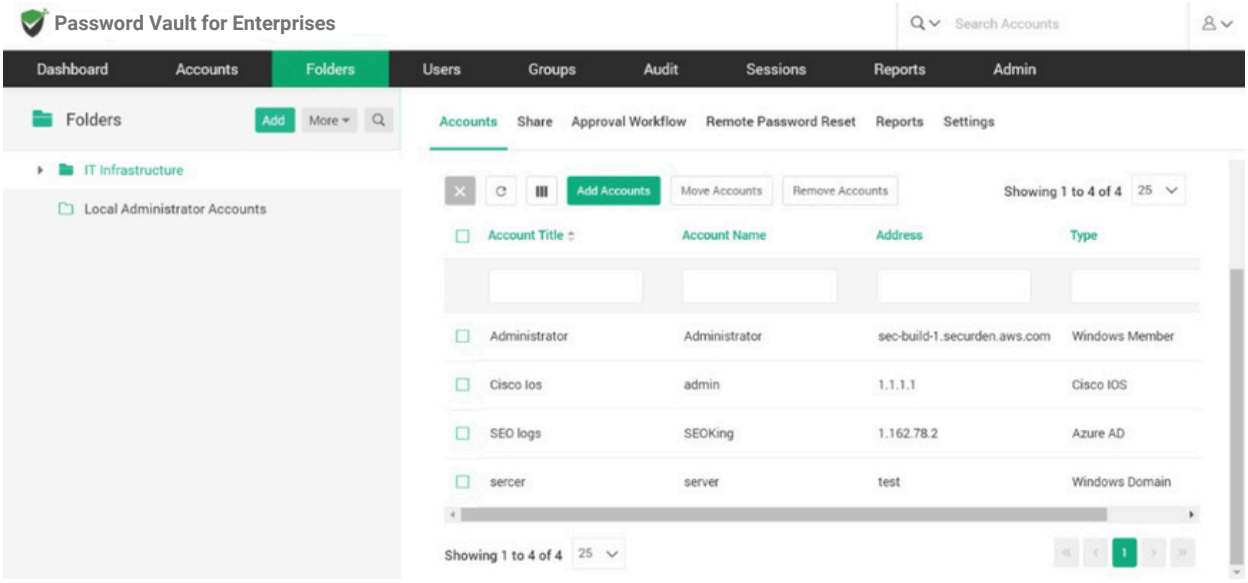
3. Once you select the attribute, Securden will fetch accounts and display the list of accounts based on its attribute. *For example, if you choose DNS/IP address as the attribute, Then a list of all accounts in this DNS/IP address will be displayed for you to select the required accounts..*

4. If you want to clear a selection, click on '**x**' of the selected account. If you want to clear all the selected accounts, click on '**Clear all**'.

5. Once the required accounts are selected, Click '**Save**'.

Search Accounts

You can search for accounts based on different attributes. This feature comes in handy when there are numerous accounts inside a folder.



To search for accounts,

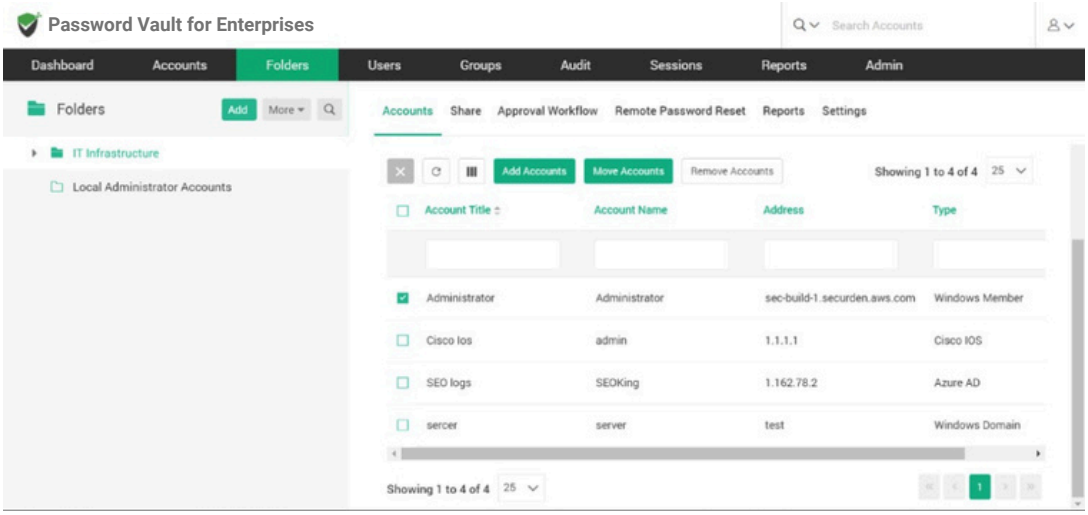
1. Click on the **Magnifying glass** icon present in Folders >> Accounts.
2. Give the input attribute(s) to search for.
3. From the list, you can select the accounts you want. If you want to select all accounts from the search result, click on the checkbox beside **Account Title**.

Move Accounts

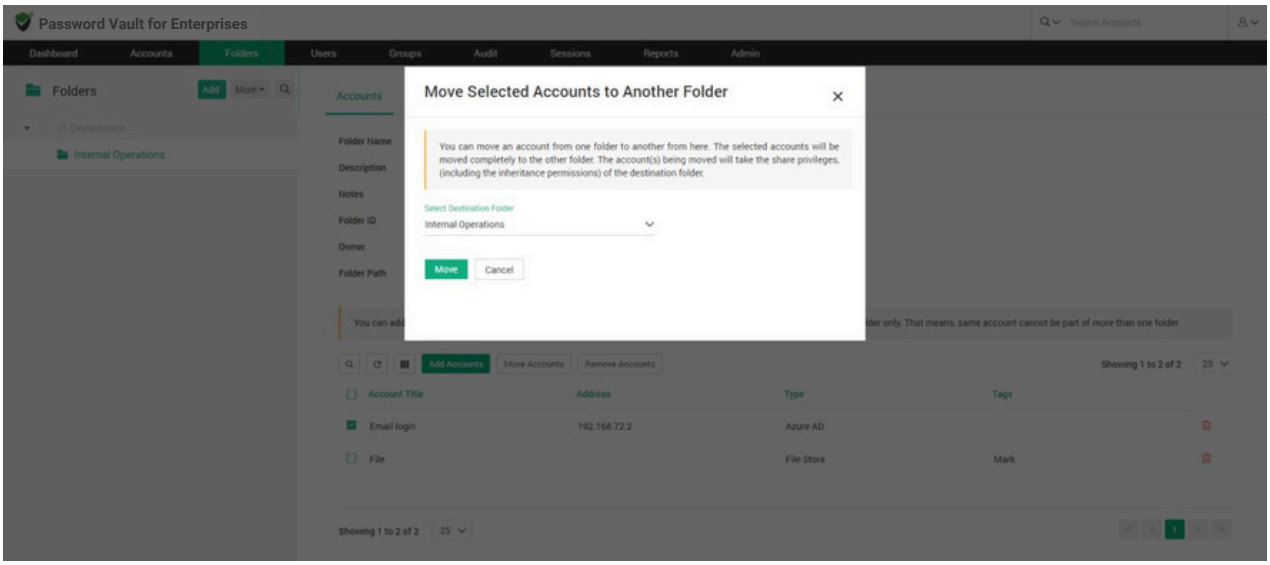
You can move accounts from one folder to another, however an account can only be a part of one folder at a time. The accounts being moved will have the same share permissions and the inheritance preferences of the destination folder.

To move accounts from one folder to another,

1. Open the folder in which the accounts are currently present.
2. Select the accounts you want to move.
3. Click on **Move Accounts**.



4. In the GUI that pops up, select the destination folder.
5. Click **Move**.

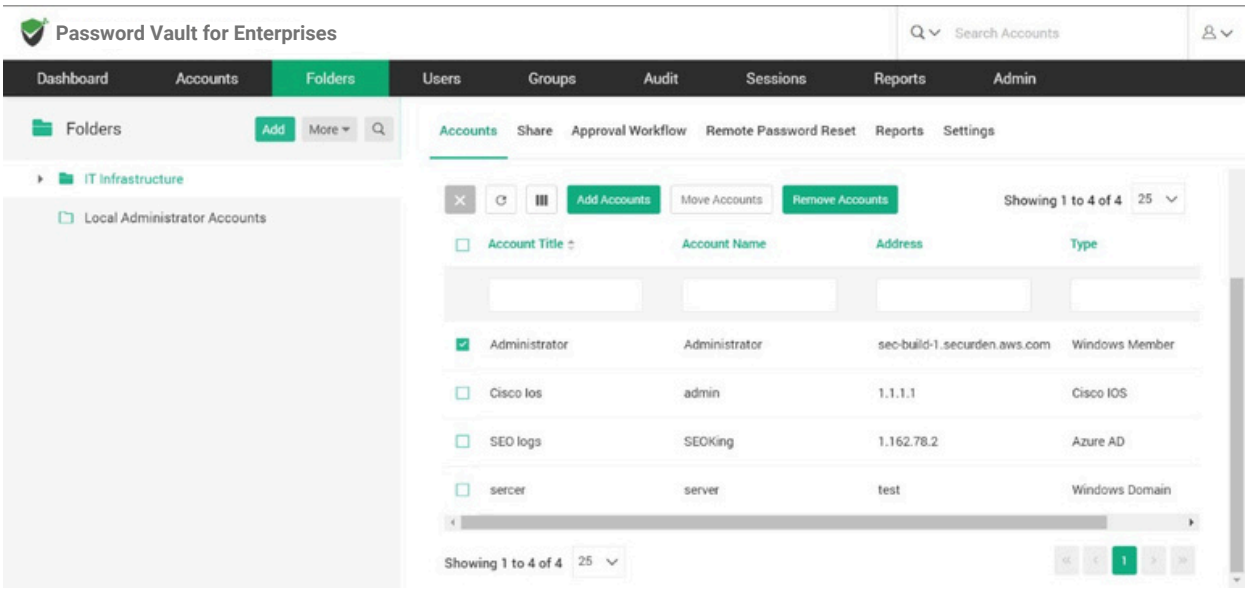


Remove Accounts

You can remove the accounts from a folder and make them stand-alone accounts.

To remove accounts from a folder,

1. Open the required folder.
2. Select the accounts you want to remove.
3. Click on **Remove Accounts**
4. In the confirmation window, Click **OK**



Share Folders

You can share multiple accounts at the same time by sharing a folder with Users and Groups. In addition to sharing accounts, you are also sharing the folder with well-defined privileges.

There are different folder management privileges and account management privileges in Securden. When you want to share a folder, you can select what privileges you want to grant to the users/groups with whom you want to share the folder.

Note: *When viewing the share settings of a sub-folder, the share permission settings will be displayed. You can turn inheritance of permissions On and Off as required from here.*

Folder Management Privileges

- 'View Folder Details' privilege allows the users/groups to simply view the folder properties. They are not allowed to modify anything.
- 'Add Accounts to Folder' privilege allows the users/groups to view the folder properties as well as add accounts to the folder.
- 'Manage Folder' privilege grants all permissions - view, modify properties, share the folder with others and add accounts.

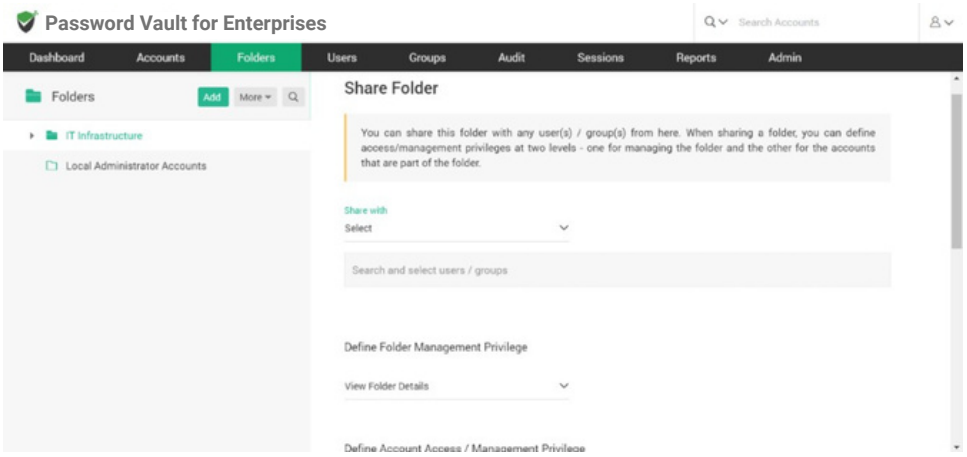
Account Access / Management Privileges

- 'Open Connection' allows launching RDP, SSH sessions with target machines, and auto-filling credentials for web applications without showing the underlying password in plain text in the GUI.
- 'View' allows the user to view the details as well as the password.
- 'Modify' allows editing the password.
- 'Manage' grants all privileges including subsequent share permissions.

To **Share** a Folder,

1. Navigate to **Folders >> <Folder Name> >> Share >> Share Folder.**
2. Select Users or Groups by clicking on the drop-down named **Share with.**
3. You can select the users/groups with whom you want to share by traversing the list from '**Search and Select Users/Groups**'. You can add multiple users and groups at the same time.

4. To remove a user/group from the selected list click on the x. If you want to clear all the selected users/groups, click on **Clear All**.

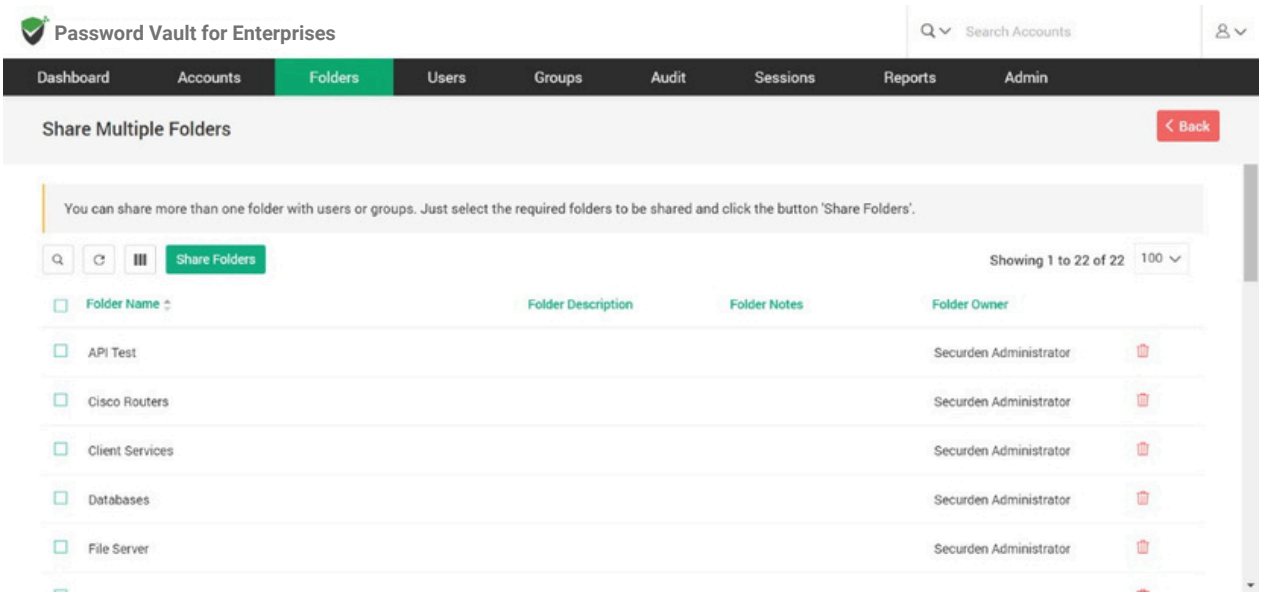


5. Define the folder management privileges and the account management privileges according to the definitions from above.

6. Click **Save**.

Share Multiple Folders

1. Navigate to **Folders >> More >> Share Folders**.
2. Select the folders you want to share.



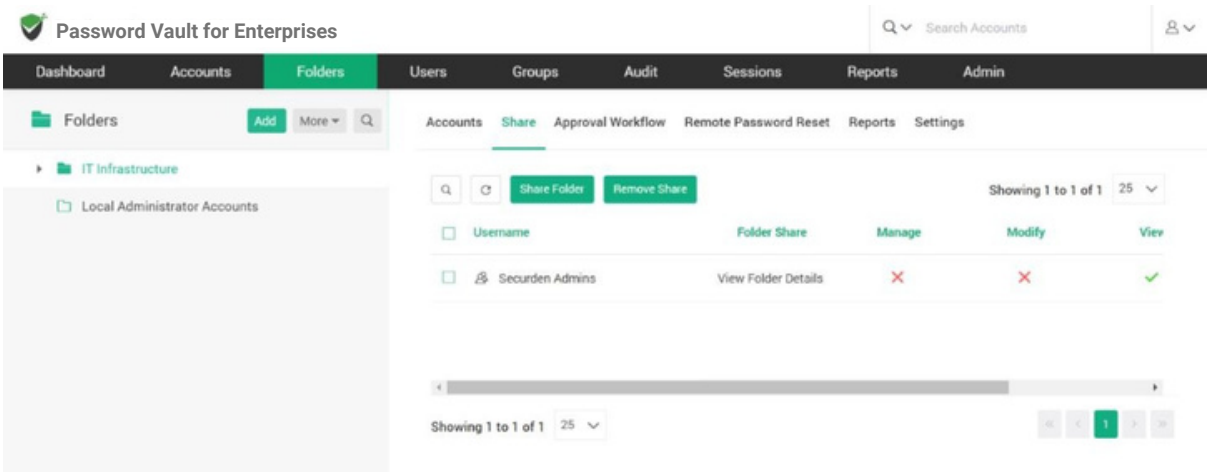
3. You can choose to not disturb existing shares and append the new share permissions wherever applicable. Doing so will imply that the share permissions can only be elevated. If a lower level of permission is selected, it will not take effect.

4. Define the folder and account management privileges by selecting the appropriate options. *To learn more about the different levels of permissions, refer to the sections above.*

Remove Share for a Folder

To **Remove** a Share, Navigate to **Folders >> Share.**

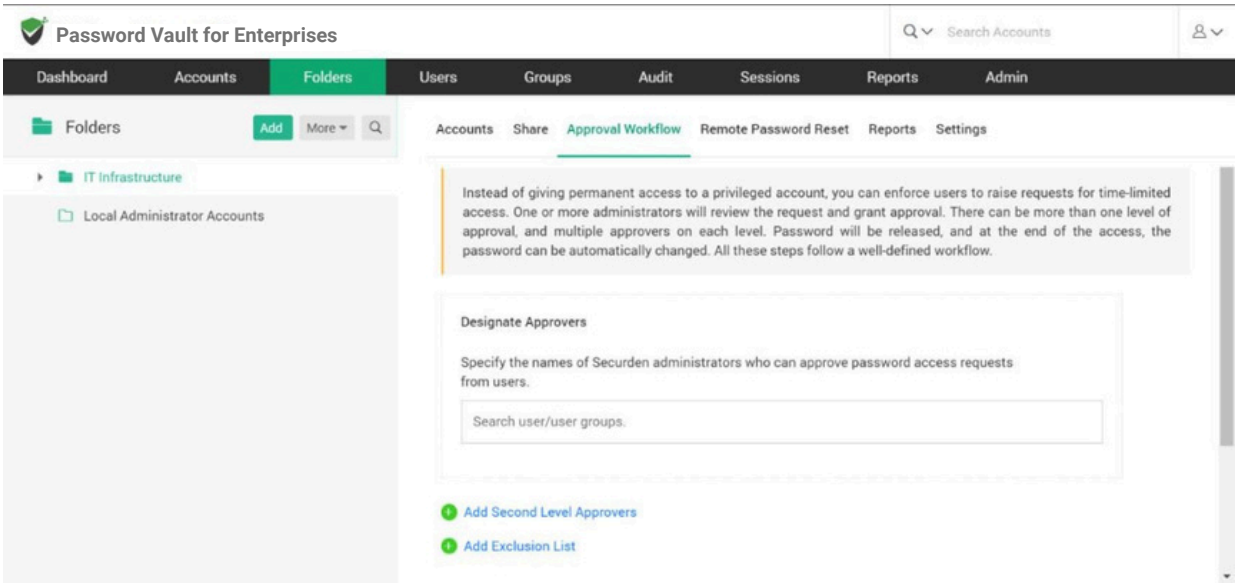
1. Select the user by clicking on the check box.
2. Click **Remove Share**.
3. Click OK on the confirmation dialog box.



Configure Approval Workflow for Folders

Instead of granting standing access to users, you can enforce just-in-time access at the folder level by using the approval workflow in Securden.

When users need access, they can place requests. One or more administrators will review before approving the request. There can be more than one level of approval with multiple approvers in each level. Upon approval, the password will be released. When the access ends, the password will be auto changed.



To **Designate Approvers**,

1. Navigate to **Folders >> Approval Workflow >> Designate Approvers.**
2. You can search for a specific user or a user group. You can select multiple users and user groups as approvers at the same time.
3. To remove a certain User or a User Group from the selection, click on x. To clear all selections, click **Clear All**.
4. To designate second level of approvers, click on **Add Second Level Approvers**. Follow steps 2 and 3 to designate the second-level approvers.

The request will reach the second-level approvers only after it is approved by the first-level approvers.

To designate subsequent levels of approvers, follow the same steps as above.

Exclusion List

You can grant direct access to passwords for any users or groups without going through the approval process, by adding them to the exclusion list.

To create an exclusion list,

1. Click on **Add Exclusion List**.

2. Search for the users/user groups and select the ones to be added to the list.
3. To remove a certain user or a user group from the selection, click on x.

   To clear all selections, click **Clear All**.

To automatically renew the passwords after the access is terminated, click on the checkbox named **Change Password After Use**.

In a situation where the approver(s) might not be available to approve requests, you can configure automatic approval of requests.

1. Click the checkbox named **Configure Automatic Approval**.
2. You can choose between approving requests throughout the day or between certain hours.

Click **Save**.

To Remove/Edit a designated approver after configuring approval workflow, you can click 'Edit' from **Folders >> Approval Workflow**.

To reset the configurations, you can click **Disable** from the same GUI.

Configure Automated, Periodic Remote Password Resets ENTERPRISE PAM

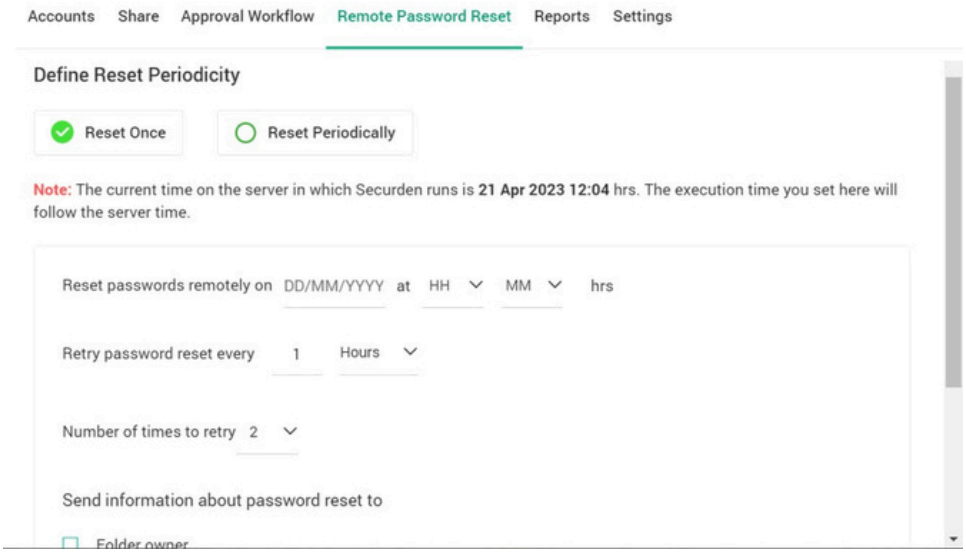
You can configure to reset the passwords of accounts contained in the folder by navigating to **Folders >> <Folder Name> >> Remote Password Reset**. There are two options to choose from when you schedule a password reset for a folder.

1. **Reset Once**
2. **Reset Periodically**

You can reset once on a specific date and time or you can configure a periodic reset to be taken in intervals as low as an hour.

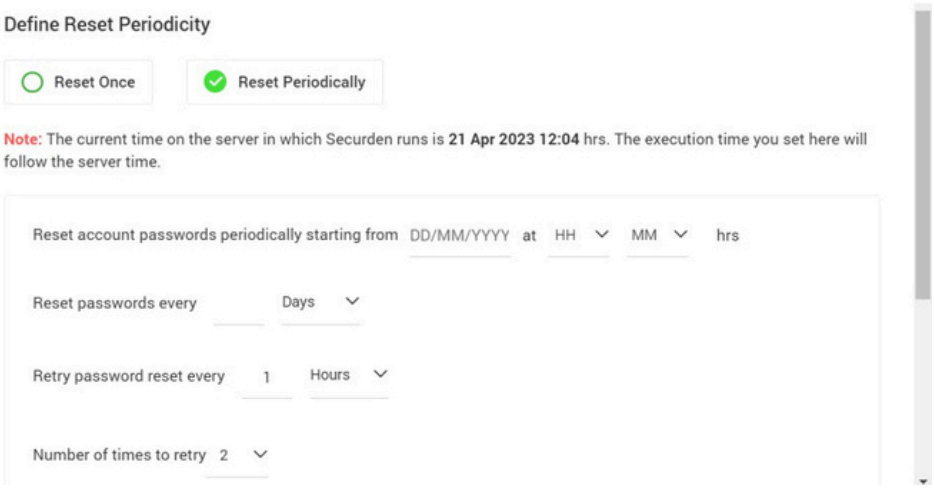
If you choose '**Reset Once**', follow the steps to schedule a backup

1. Specify the date of reset from the calendar by clicking on the date format text.
2. Specify the time of reset in the format [hh mm].
3. Specify how often to retry password reset.
4. Specify the maximum number of resets to be attempted.



If you choose '**Reset Periodically**', follow the steps to schedule backups

1. Specify the date of the first reset from the calendar by clicking on the date format text.
2. Specify the time of the first reset in the format [hh mm].
3. Specify the periodicity of password reset. You can configure a periodicity as low as an hour.
4. Specify the maximum number of resets to be attempted.



You can select options shown to notify the folder owner and the users with shared manage access. You can also include recipients to notify by specifying their email addresses in comma separated form.

To disable an already existing schedule, click on '**Disable**'. Click '**Save**'.

Troubleshooting Tips

1) **Issue:** Issue with Domain Admin accounts. The user has put them in a folder and has been using remote password reset functionality, but when it runs it shows the following error.

Error: Possible reasons:
(1) Invalid credentials.
(2) Remote connection privileges for this account could have been disabled on the remote computer.

Password on both side (Securden and AD) is the same and the user uses a domain admin account for remote.

Solution:

One possible reason could be that WMI connectivity might not be available. We use WMI protocol for password resets and verifications. By default, WMI remains disabled for all local users except for the built-in administrator accounts.

You may follow the steps below to enable WMI access on a specific Windows machine:
https://www.securden.com/documents/WMI-Access-for-All-Users.pdf

In case you wish to enable WMI on multiple machines, you may refer to the link below:
https://www.securden.com/documents/WMI-Access-For-All-Users-GPO.pdf

---

2) **Issue:**

I am trying to let local admin accounts from a PC, and I get an error "The username/password does not exist (or) the user does not have the remote launch or remote."

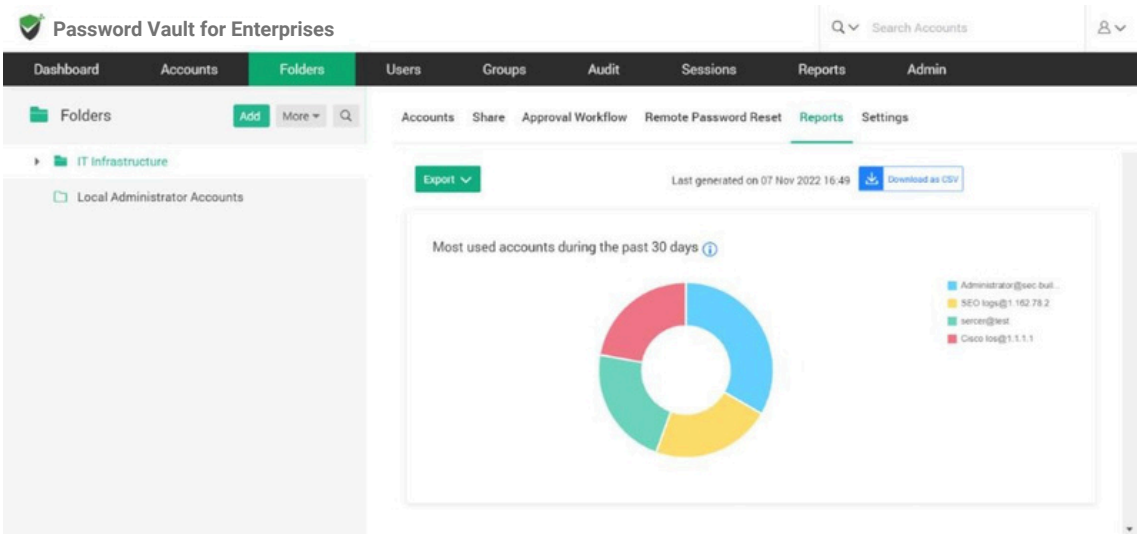
Solution: It might be an account permission issue. Try to re-run the discovery by providing a domain admin credential.

Navigate to Accounts >> Discover Accounts >> Windows. Click "Modify" >> Enter username and password

You can enter a domain admin credential and try to discover the computers again to fetch local accounts. If it still fails, please try disabling the firewall and check once again.

Folder Reports

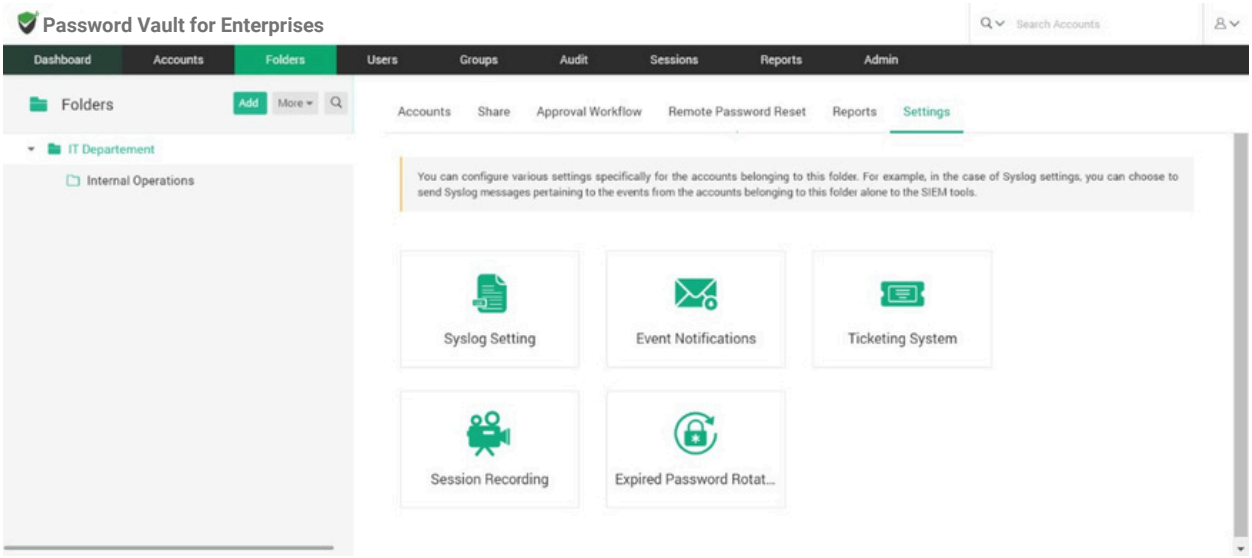
You can generate and view various actionable reports with the data specific to the selected folder.



You can view the most used accounts, most active users, accounts and activity trails of the selected folder.

Folder Settings

Certain settings such as session recording, syslog settings, etc., can be configured for accounts at a folder level in addition to being configured at an account level. For example, in the case of Syslog settings, you can choose to send Syslog messages pertaining to the events from the accounts belonging to this folder alone to the SIEM tools.



Syslog Settings

You can configure Syslog preferences for Folders. Navigate to **Folders >> Select a Folder >> Settings >> Syslog Settings**.

Pre-requisite: You need to configure the Syslog settings from **Admin >> Syslog for SIEM** to be able to access this folder level setting.

You can select the account related activities for which you want to maintain a Syslog.

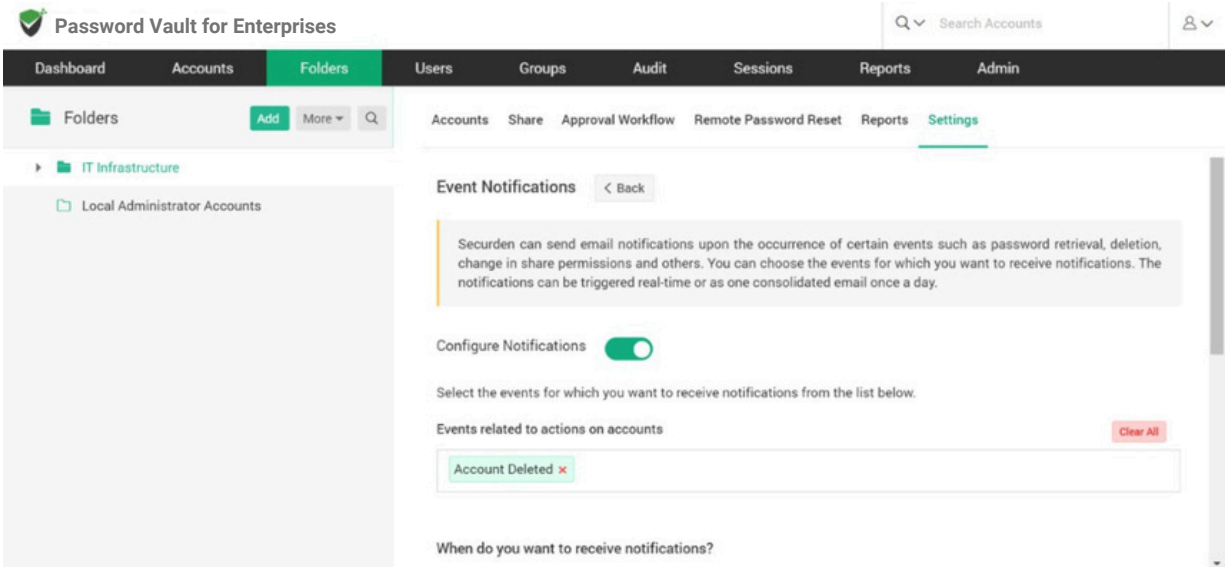
The folder-specific settings will get the preference over the global settings that were configured in **Admin >> Syslog for SIEM**.

Event Notification

When certain events occur, such as password recovery at the folder level, deletion, or changes in sharing permissions, Securden can send email notifications. You have the option of selecting which events you want to be notified about. The notifications can be sent out in real-time or as a consolidated email once a day.

Configuring Event Notifications

To start setting your preferences in receiving notifications, you need to toggle the Configure Notifications button. You will see a field named **Events related to actions on accounts**.



To add events, click on **Select Events** under **Events related to actions on accounts** and select the events you want to get notified about from the list.

The selected events will be shown in a green box and can be deselected by clicking on the **x** present adjacent to the event. To clear all selected events, click on the **Clear All** button.

When to Notify?

You can choose to either get notified **As and when the events occur** or **As a consolidated email, once a day**.

Who to Notify?

You can choose who receives notification emails by selecting the options in the checklist present under **Send Notifications to**. If you select **All Administrators**, users with **Administrator** or **Super Administrator** designation will be notified.
If you select **All Auditors**, the users with auditor role designated to them will be notified.

You can also configure to notify specific users or a group of users by selecting **Select Users/Groups**.

You can send notifications to people who are not registered users in Securden by specifying their email address in the box named **Others (specify email address)**. When more than one email address needs to be notified, separate the emails with a comma(**,**).

Click **Save**.

Ticketing System ENTERPRISE PAM

To use the ticketing system for a folder and its accounts, you need to configure the ticketing system from **Admin >> Ticketing System**.

Once the ticketing system has been configured, you can toggle this feature **On** for specific accounts and folders. Navigate to **Folders >> Settings >> Ticketing System** to toggle this feature **On** or **Off**.

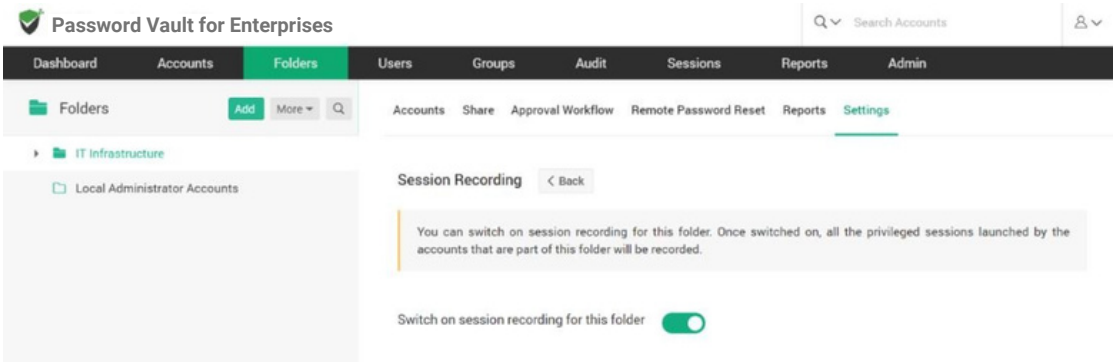
Exclusion List

You can exclude specific users or groups, with whom the folder is shared, from going through the ticket validation by including them in the exclusion list.

Session Recording at the Folder level ENTERPRISE PAM

You can switch ON the session recording feature at the folder level. Doing this records a video copy of remote sessions launched from all accounts that are a part of the folder.

Note: Switching this feature ON is a second step of configuring session recording in Securden. You need to configure preferences in **Admin >> Remote Sessions and Recordings >> Session Recording** before you can turn this feature ON for the folder of your choice.

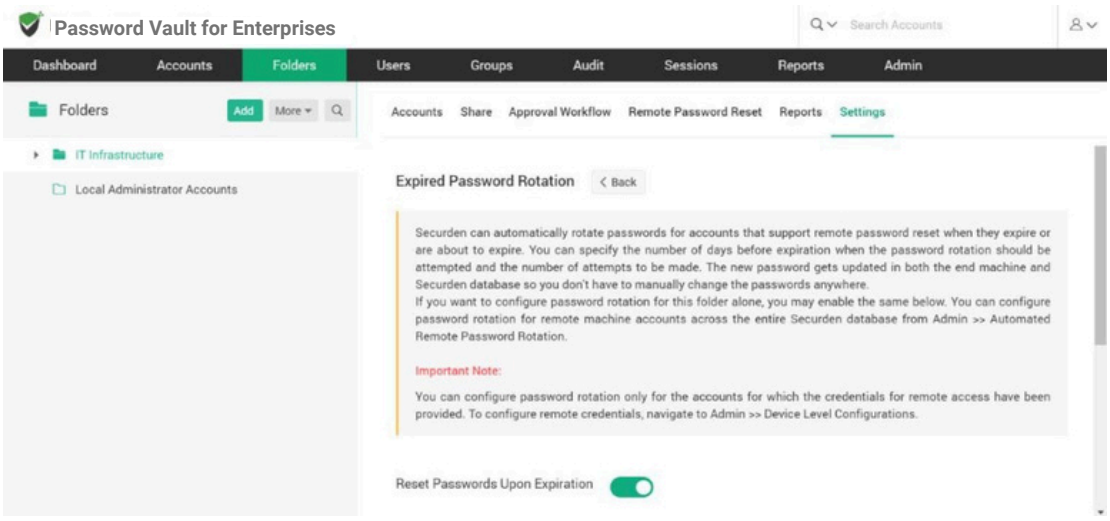


Expired Password Rotation ENTERPRISE PAM

When passwords expire or are about to expire, Securden can automatically rotate them for you without manual intervention. You can indicate the number of days until the password expires after which password rotation will be tried, as well as the number of attempts.

You don't have to change passwords manually anywhere because the new password is updated in both the end machine as well as the Securden database.

If you only want to configure password rotation for the accounts contained within a folder, you may do it from **Folders >> Settings >> Expired Password Rotation**.



You can set password rotation for remote machine accounts across the entire Securden database by navigating to **Admin >> Automated Remote Password Rotation**.

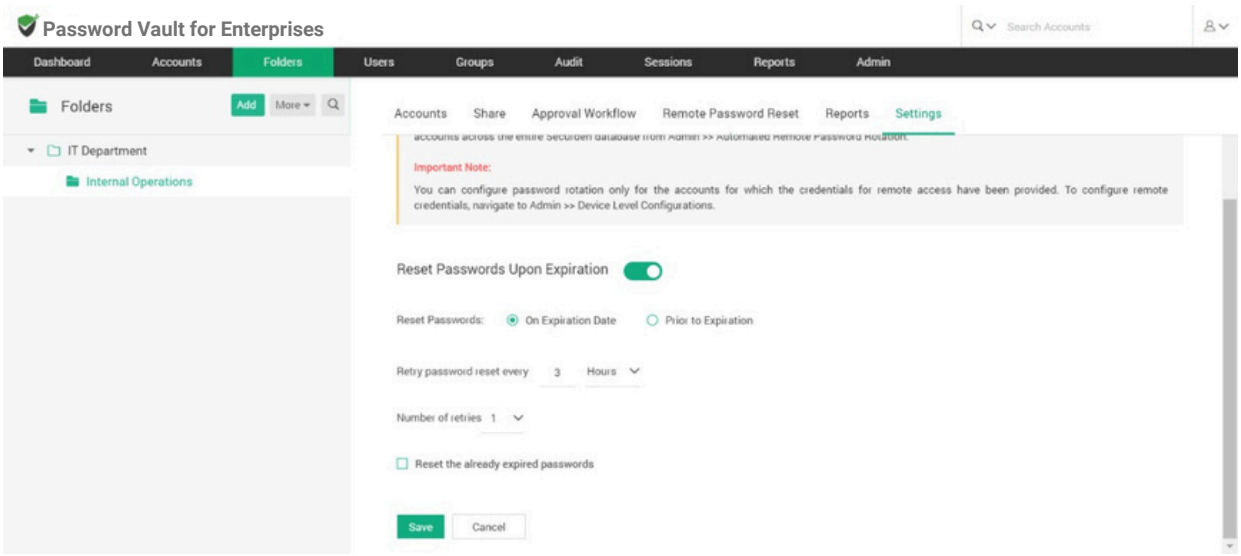
Important Note: You can configure password rotation only for the accounts for which the credentials for remote access have been provided. To configure remote credentials, navigate to **Admin >> Device Level Configurations.**

You can configure Securden to carry out password changes either **On Expiration Date** or a few days **Prior to Expiration** date.

If you choose **On Expiration Date**

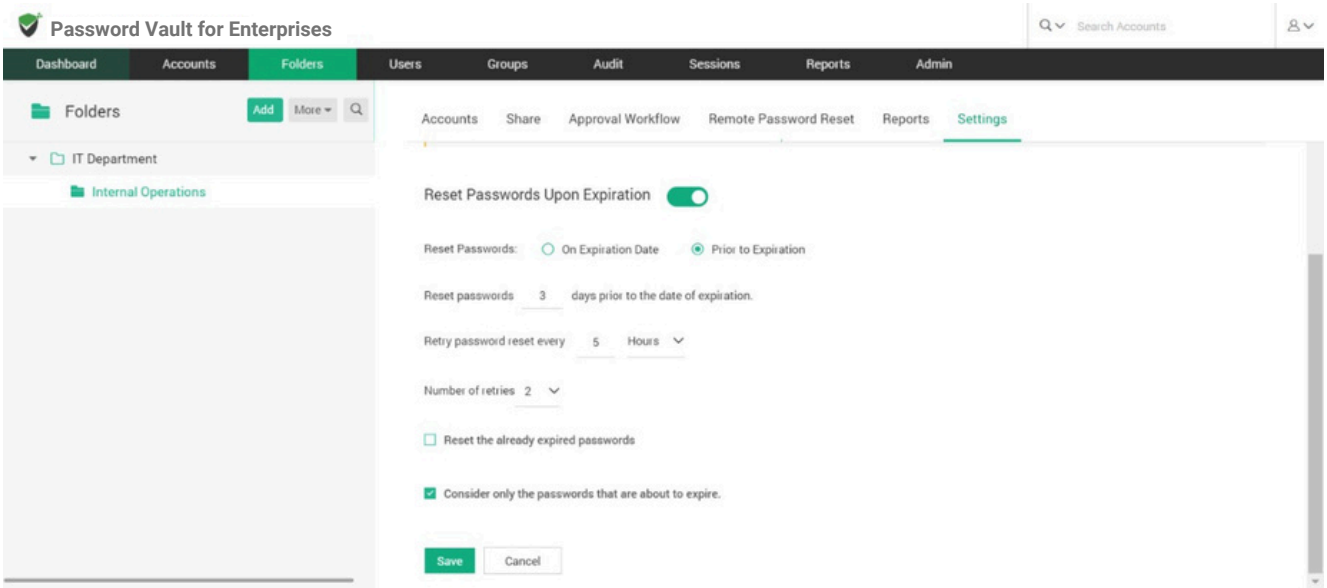
1. You need to provide the frequency of password reset, which can be as low as a minute.

2. You should also specify the maximum number of attempts to be made to reset a password in the field named '**Number of retries**'.
3. You can choose to '**Reset the already expired passwords**'. Securden will try to reset the expired passwords at the time of configuration.



If you choose **Prior to Expiration**,

1. You need to provide the frequency of password reset, which can be as low as a minute.
2. You should also specify the maximum number of attempts to be made to reset a password in the field named **Number of retries.**
3. You should specify how many days before the expiration date the reset attempts should be made.
4. You can choose to make reset attempts in accounts whose passwords are about to expire and the passwords that have already expired by clicking on the respective checkboxes.



Precedence of user-level privilege

When a user is part of a group, and if an account is shared with different levels of privileges with that group, and as well as the individual user, the privilege granted on the user-level will take precedence over the privilege granted on a group-level.

For example, let us say there is an account, user, and group named *Account1, UserA,* and *Group1* respectively.

Consider,

- UserA is a member of Group1
- Account1 is shared with 'Open Connection' permission individually to UserA
- Account1 is shared with **Modify** permission to Group1

Then, the UserA will only have **Open Connection** access to Account1, and not **Modify** access.

Precedence of least privilege

When an account / folder is shared with many groups with different privileges, and if same user is a member of all those groups, the user can access the account / folder only with the 'least level of privilege' given amongst the groups.

For example, let us say there is an account, folder, user, and groups named Account1, Folder1, UserA, Group1, and Group2 respectively.

Consider,

- UserA is a member of both Group1 and Group2.
- Account1 is shared with ‘Manage’ permission to Group1 and ‘Modify’ permission to Group2.

Now, the UserA will only have ‘Modify’ access over Account1, and not ‘Manage’ permission.

Precedence of account-level access over the folder-level

If a folder and an account has been shared with different levels of privileges to a user, and even if the same account is present within that folder, the user will still have account-level access over that folder and will not be able to access it with folder-level permission.
For example, let us say there is an account, folder, user, and groups named Account1, Folder1, UserA, Group1, and Group2 respectively.
Consider,

- Account1 is a part of Folder1.
- UserA is a part of both Group1 and Group2.
- Group1 has ‘Manage’ (folder-level) permission over Folder1, and Group2 has ‘View’ (account-level) permission over Account1, which is inside Folder1.

Now, the UserA will only have account-level ‘View’ access to Account1 and will not be able to access the account with folder-level ‘Manage’ access.

Section 9: Audits

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. activities capture the activities on the accounts. User activities capture the activities of the Users.

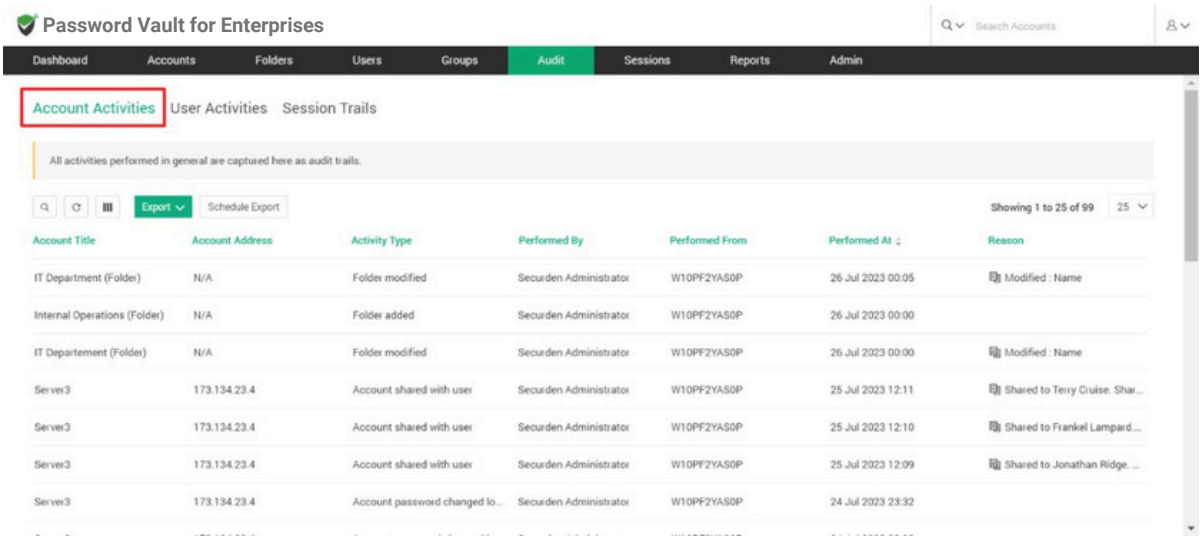
To view the audit trails, navigate to the ‘**Audit**’ tab in the GUI. The trails are classified into three categories:

- Account activities
- User activities
- Session activities

Account activities:

Account activities include all the activities related to the accounts that occur in Securden like changes in passwords account addition, deletion, modification and, so on. Activities across all accounts are recorded and can be tracked. It displays the dates and times that an account or file is handled, as well as the names of users who have retrieved, modified, or added it.

Navigate to **Audit >> Account Activities** to view account logs.



Filtering data from audit records:

You can acquire a concise report by filtering and viewing only the records that satisfy your criteria. To filter, click on the **Search** tab. You can search through the audit filter with the following labels:

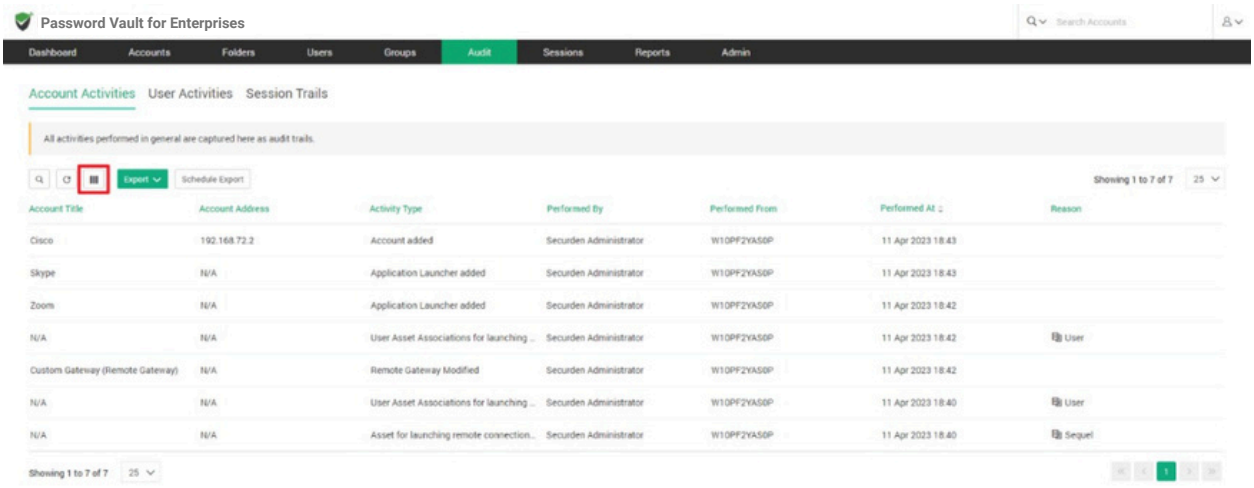
Parameter	**Description**
Performed by	The user who performed the operation.
Performed from	The name of the device where the operation was done.
Performed at	The time at which the operation took place.
Activity type	The type of action performed by the user.
Username	The name of the user who triggered the action.

Reason	The reason behind the particular activity is noted and displayed.
Account Title	The name of the account on which the user performed the activity.
Account address	The IP address of the device on which the account activity was performed.

For instance, If deletion of password occurs in a particular account and you want to see them, you can view them in the account activities and with the help of the available filters you can view the exact data you require.

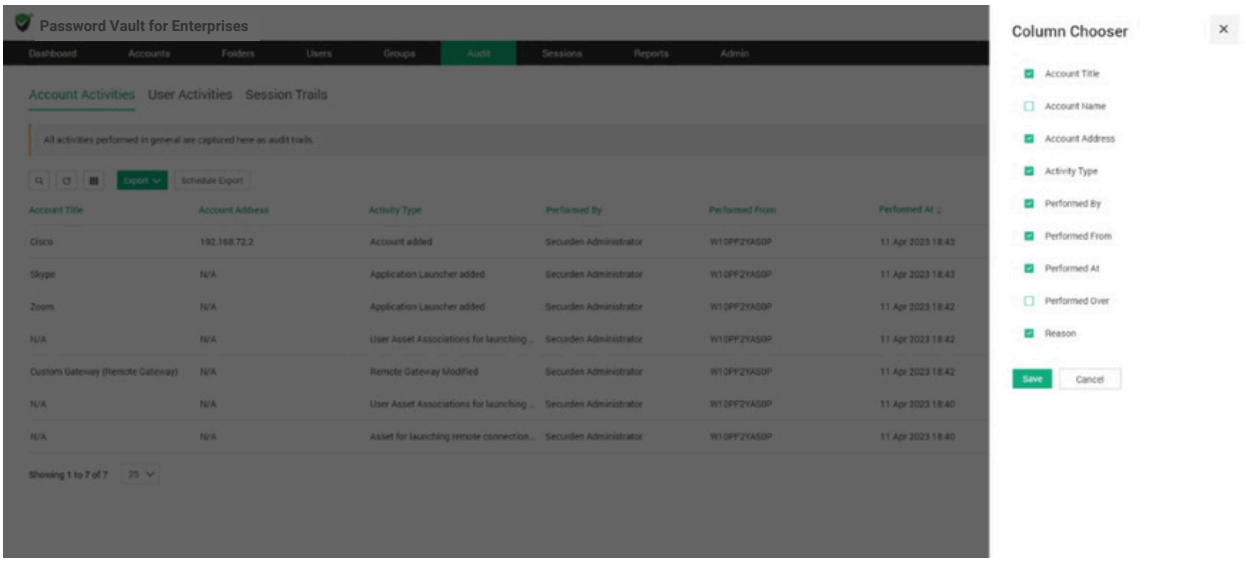
Column chooser:

You have the option to select which columns are displayed under account activitiy audits. Click the column chooser icon – shown below.

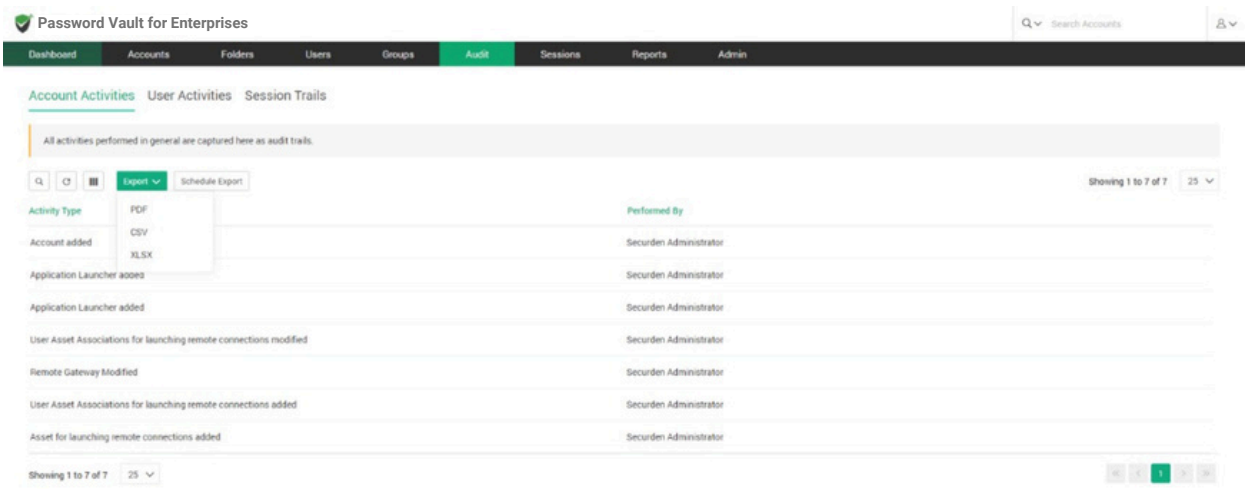


The search columns can display different label columns according to the requirements of the user. At a time, any six columns can be selected for

display from the following nine categories – **Account Title, Account Name, Account Address, Activity Type, Performed By, Performed From, Performed At, Performed Over, Reason.**



For instance, if you want to have a report solely consisting of activity type and who it was performed by, you can select those columns and download the report. An example screenshot is attached below:



Exporting the filtered data:

After the screening process of audit trails and securing the required audit, it can be exported for various investigation purposes. Navigate to the '**Export**' tab and select the required format.

There are three formats available and they are:

- PDF
- CSV
- XLSX

Click on the **Download as** to get the report to your system. The date and time at which the report was generated is also displayed.

Schedule Export of Account and User activities:

The exporting of audit data can be scheduled on a periodic basis or at once, in a time frame by selecting the required report format. To download the report, the link will be sent to the specified recipients. Navigate to the **Schedule Export** tab.

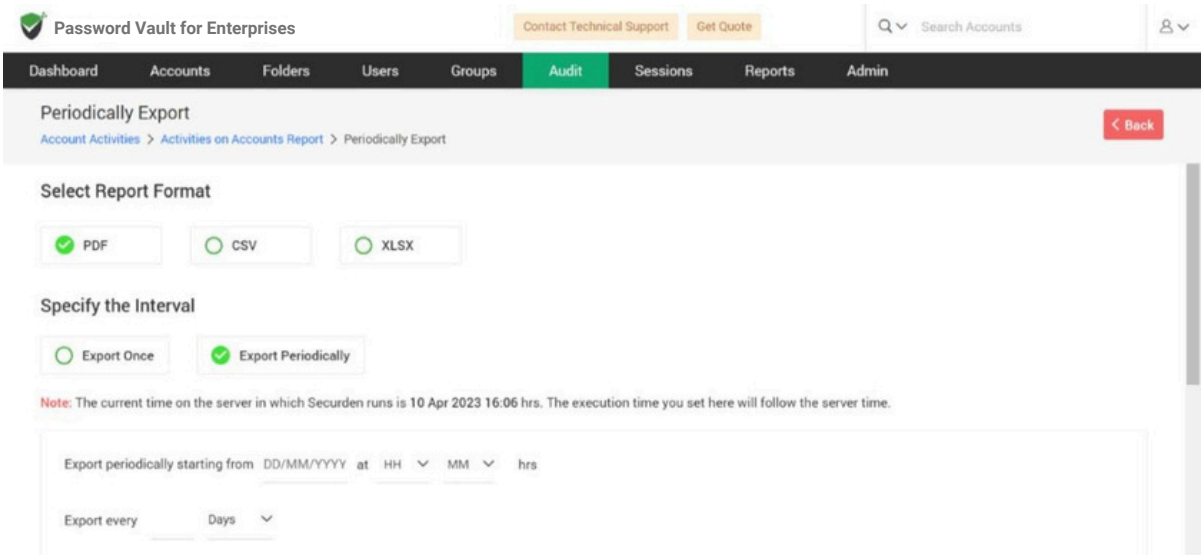
Firstly, the report format must be selected among the three options which are **PDF, CSV, XLSX**. Then the interval must be specified by choosing **Export Once** or **Export Periodically** according to the needs of the user.

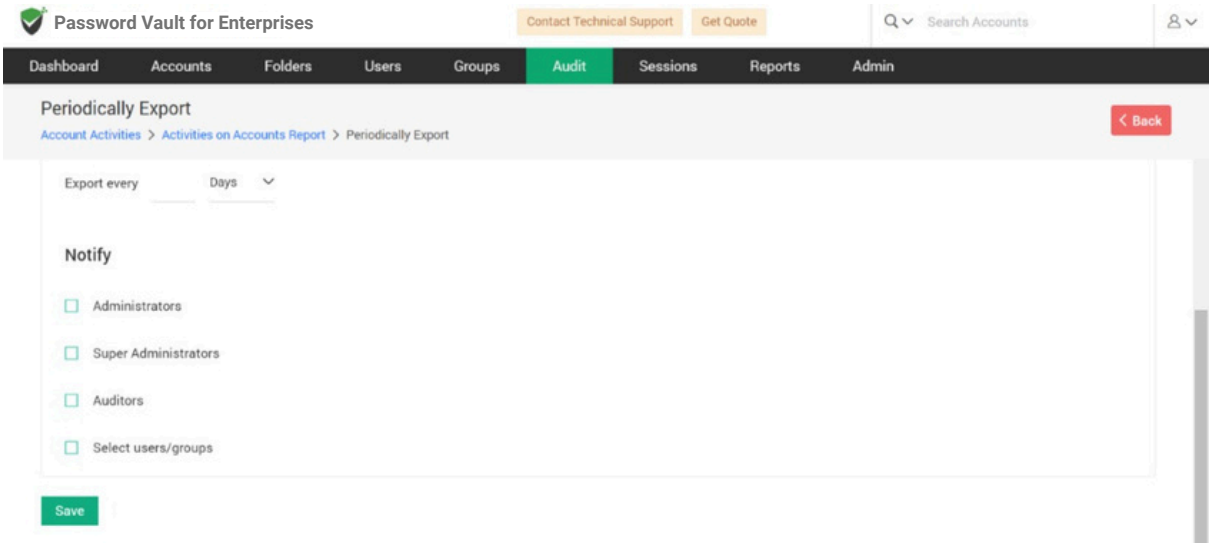
Note: The execution time you set will follow the current time indicated in the server in which Securden runs and the current timing along with the date is displayed.

The date and the timing of the export must be specified in the formats of DD/MM/YYYY and in the 24 hour format HH:MM respectively. The same can be notified to different levels of users:

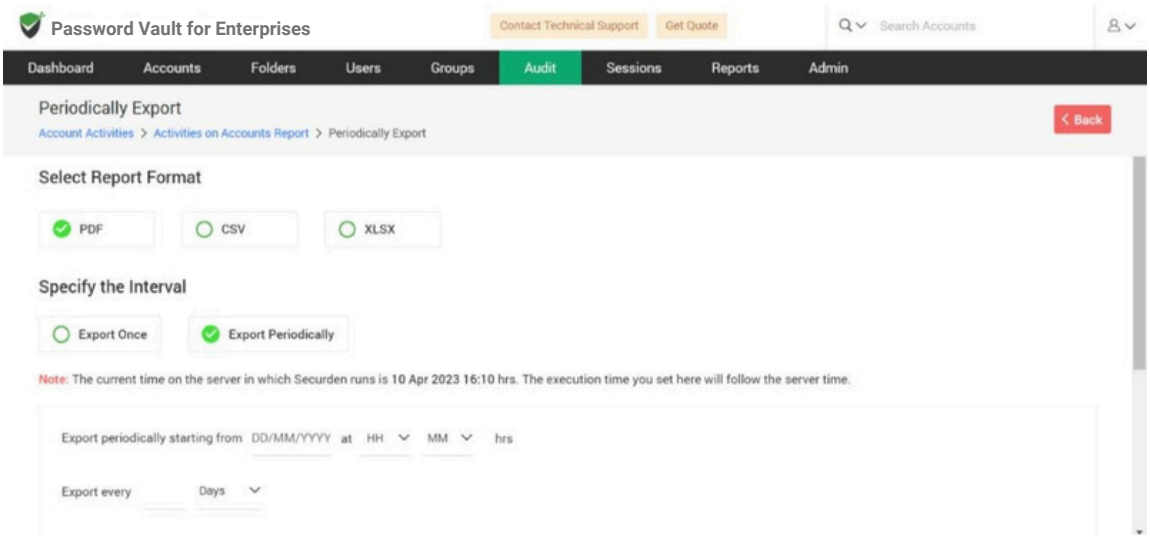
- Administrators
- Super Administrators
- Auditors
- Select users/groups

After selecting the recipients, click **Save**.





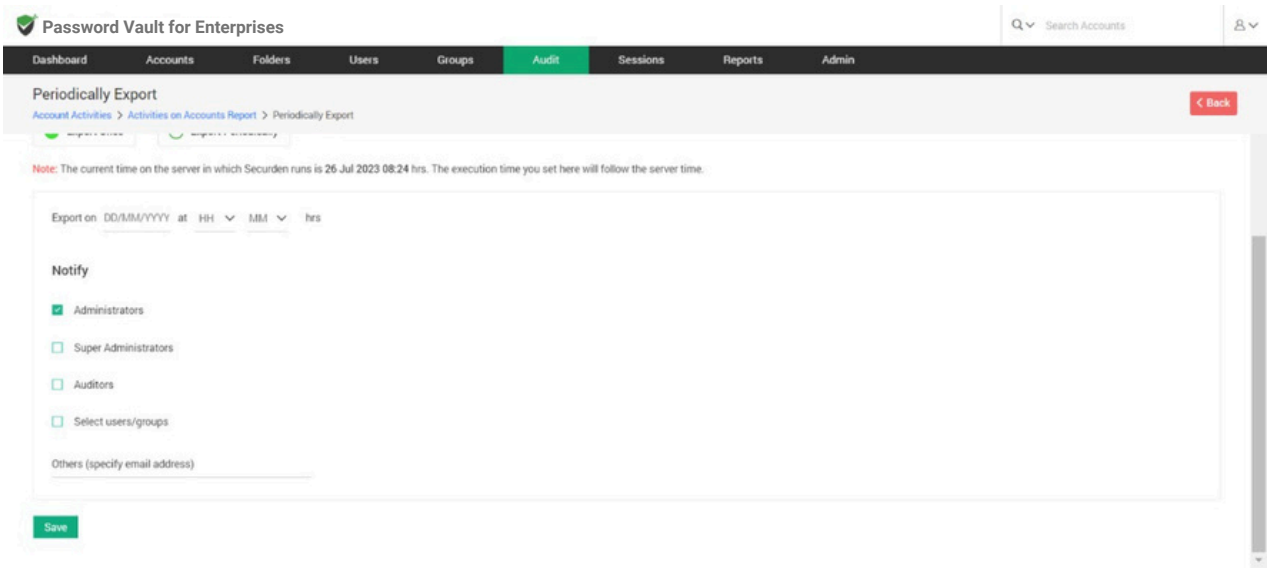
The only difference when you export periodically is that you need to specify the periodicity in terms of **Days, Months and Hours**.



For instance, If you want to avail the audit report in a CSV form you can easily export and download them. Also if you want them to be exported everyday at 10.00 AM, you can customize and schedule the time and get them exported in any format you expect.

Notify

Navigate to the **Schedule Export** tab and under that you can find the set of users, to whom the link will be sent to download certain reports. When we want to track specific audit events, then upon their occurrence we can notify the required users.

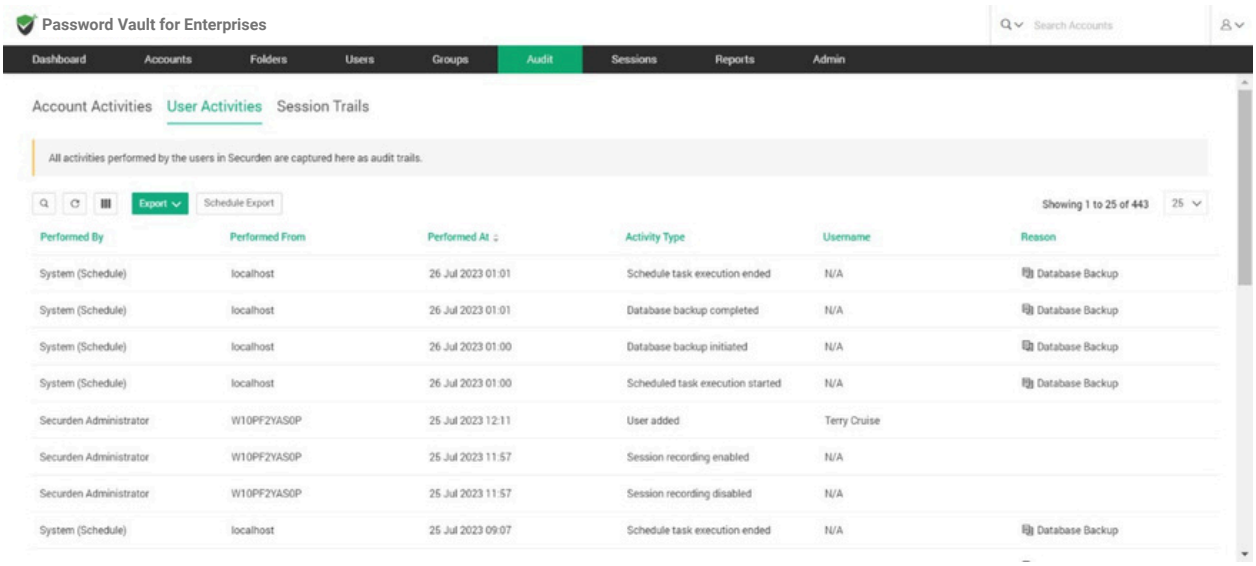


User activities

All the activities performed by the users in Securden are recorded as audit trails under User activities. The number of users in any organization varies from time-to-time. Some users may leave the organization but the activities they performed before leaving will get captured here and can be utilized if any information is needed.

For instance, If a user is leaving your organization, it is high-time the passwords accessed by him might be exposed. So, to avoid any such circumstances, Securden allows you to view the activities performed by a particular user and change them. To help ease that process, you can have a vareity of filters and search icon.

Navigate to **Audit >> User Activities**.



Click on the **Search** icon. Among the plethora of activities performed by each of the users, the search option helps to filtrate and acquire the relevant trails. To facilitate the search process, six different parameters are available.

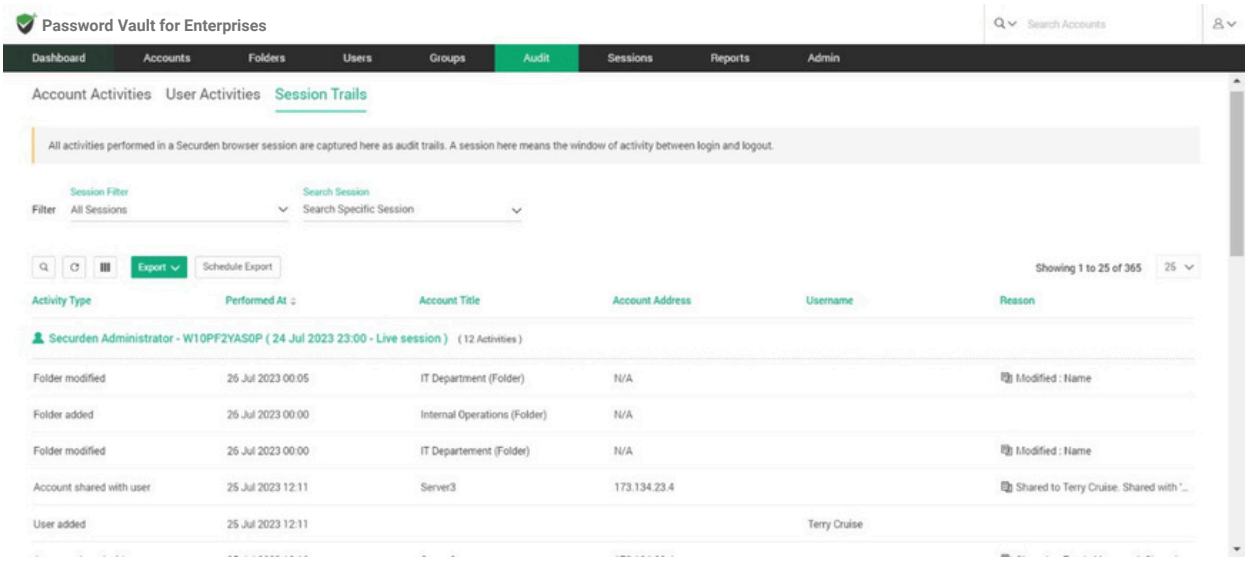
Parameter	**Description**
Performed by	The role of the user who performed the operation.
Performed from	The name of the device where the operation was done.
Performed at	The time at which the operation took place.
Activity type	The type of action performed by the user.
Username	The name of the user who triggered the action.
Reason	The reason behind the particular activity is noted and displayed.

Session Trails:

All activities performed in a Securden browser session are captured here as audit trails. A session here means the window of activity between login and logout. Every detailed activity from the beginning of the session to the ending is captured.

For instance, If you are an IT admin in your company and you want to know the reason for a particular password issue requested by your employee, you can easily reach out to session activities and view the session from the start to the end and find out the reason.

To get audits from session activities, navigate to **Audit >> User Activities**.



Filters in Session activities:

You have a couple of filters like **Session filter** and **search session** with which you can dil down the report and acquire the exact data you want. In **Session Filter**, you have

- All sessions
- Live sessions
- Concluded sessions

To filter out and search the exact audit data you require, click on the search icon. To facilitate the search process, six different parameters are available as seen abouve in the account and user activities.

Export and scheduled export:

You can also avail the export and schedule export option like the other audit tabs as explained above.

Event notification:

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. This is further explained in the admin section.

For instance, if you need to know all the addition and deletion activities performed by all users and accounts in your organization, you can choose to receive notifications for that particular event. You can also customize the time of receiving notifications like if you want them at the time of occurance or consolidated notification once in a day.

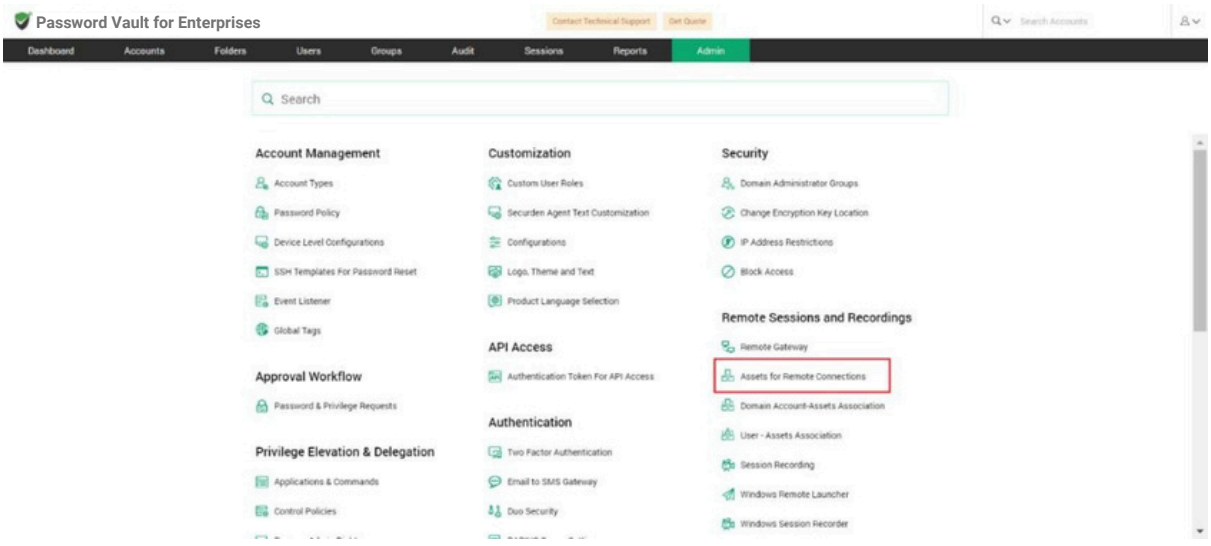
Add Assets for Remote Connections

Domain accounts are often used to remotely connect to computers and various other IT assets. Any domain account can be configured to remotely connect to multiple IT assets. In such scenarios, creating an association between the domain accounts and the list of IT assets it could connect to, becomes necessary.

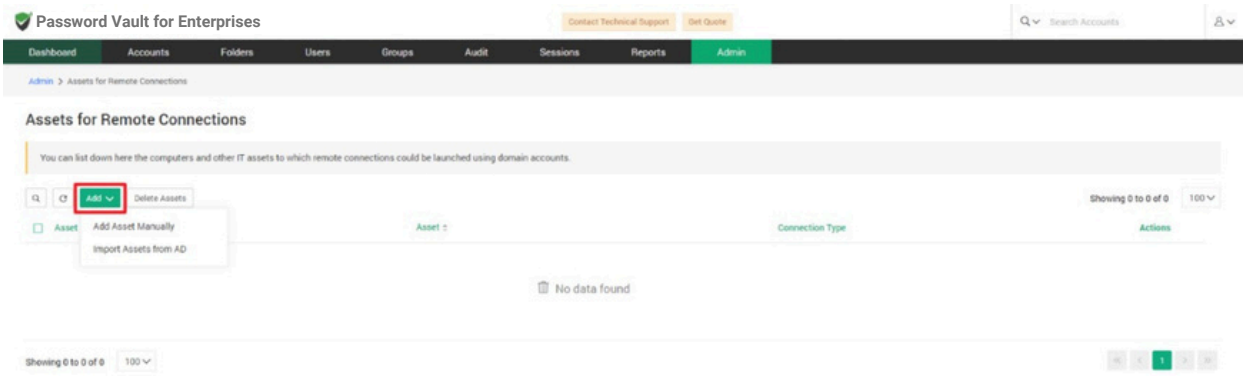
Prior to creating such an association, the IT assets are to be added to Securden. You may add all such computers and other IT assets in this section.

While adding the IT asset, you can specify how the device can be connected (RDP / SSH / SQL) and the device's connectivity details. As mentioned above, the assets added here need to be associated with the required domain accounts - that is, with specific users/user groups and accounts/folders in Securden.

To add the assets that are to be remotely accessed, navigate to **Admin >> Remote Sessions >> Assets for Remote Connections**.



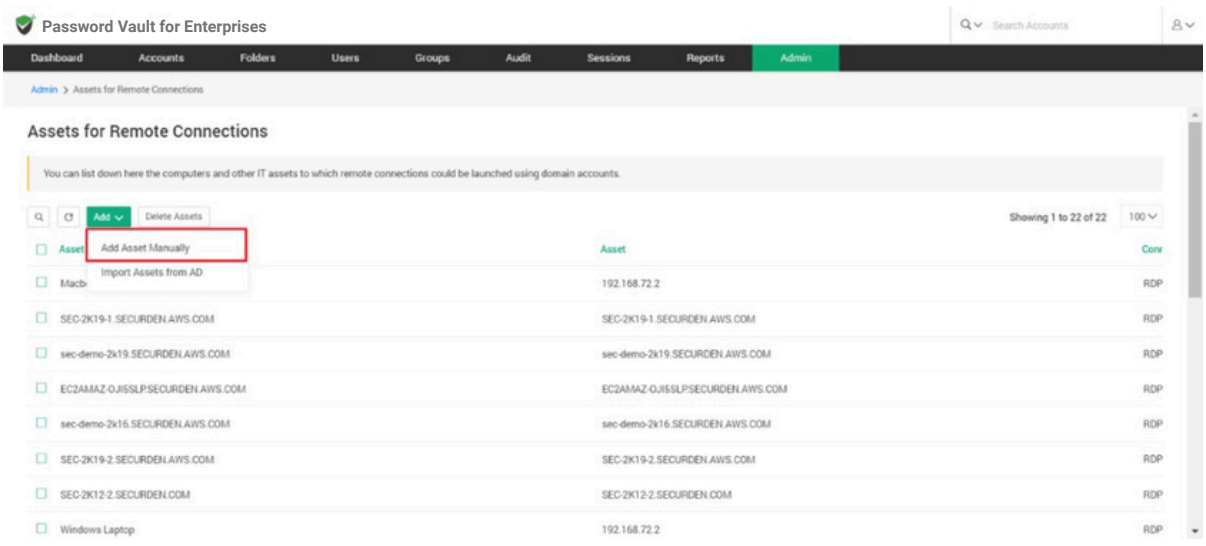
In the GUI that opens, click **Add**.



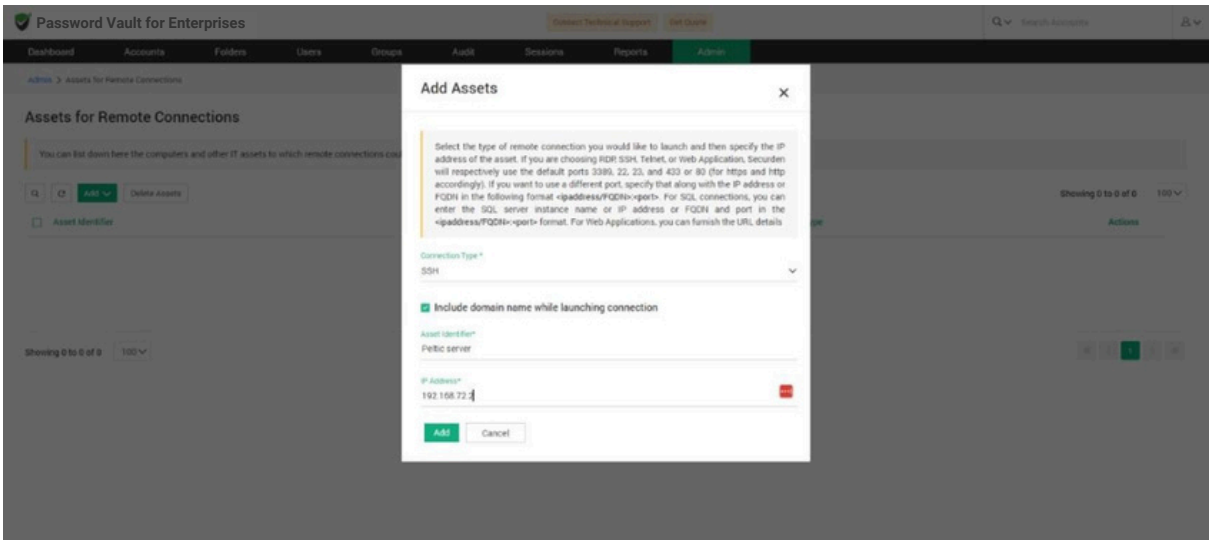
You have the option to either add assets manually by supplying the connectivity details or import them from your directory. Both options are elaborated below.

Add Assets Manually

You can add the required IT assets manually one at a time. Click on **Add Asset Manually.**



In the GUI that opens, you need to specify the attributes associated with the asset.



Provide the following attributes associated with the asset:

- **Connection type:** You can specify what type of connection the asset will be connected with from the options available in the drop-down.

If you choose RDP, SSH, or Telnet, Securden will use the default ports 3389, 22, and 23 respectively. If you want to use a different port, specify that along with the IP address in the following format <ipaddress>:<port>. For SQL connections, you can either enter the SQL server instance name or the IP address and port in <ipaddress>:<port> format.

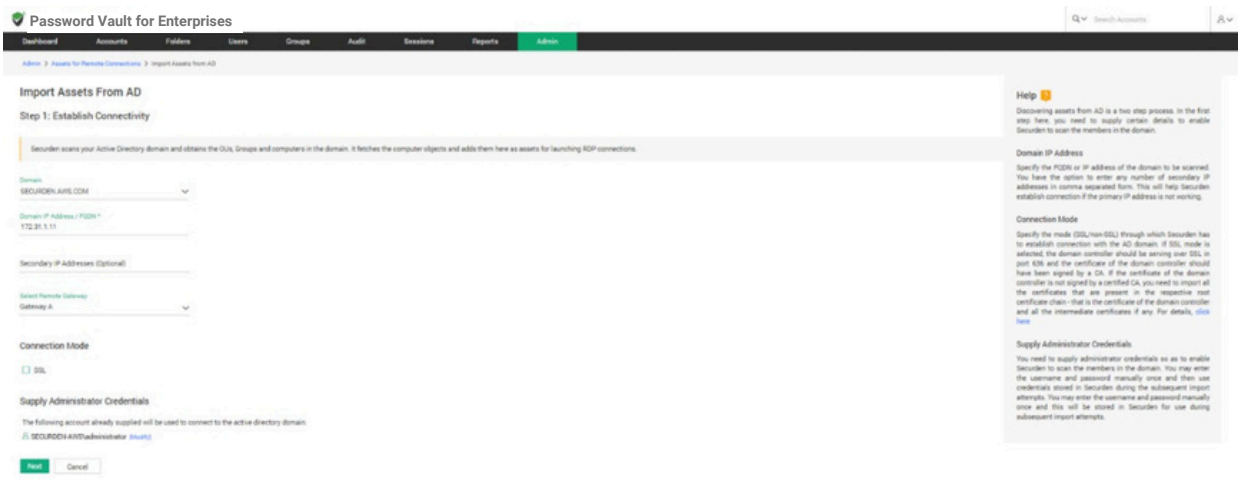
Note: For SSH connections, you have the additional option to include the domain name while launching a connection.

- **Asset Identifier:** Enter a name for the IT asset being added in this field. This helps in uniquely identifying the asset for launching remote connections.

- **IP address:** Finally, specify the IP address of the asset.

Import Assets from AD

The other option is to import the required IT assets from the Active Directory domain. You can import select devices, OUs, or Groups in any manner as needed. To import assets, click “**Import Assets from AD**”. The import is a two-step process.



Step 1: Establish connectivity

Securden scans your Active Directory domain and obtains the OUs, Groups and computers in the domain. It fetches the computer objects and adds them here as assets for launching RDP connections.

To establish connectivity with your domain you need to specify the following:

Domain: Select from an active directory domain added in securden

Domain IP address: Enter the IP address or the FQDN of the domain

Remote gateway (Optional): You can choose to route the connection with the domain using a remote gateway added in Securden. If you wish to add a new remote gateway, navigate to **Admin >> Remote Sessions and Recordings >> Remote Gateway**

Connection Mode: You can specify if you wish to connect securely using an SSL connection by clicking the checkbox.

Administrator Credentials: You need to supply the administrator credentials which will be used to connect to the domain and authenticate.

You can either enter the username and password of the account which will be used to connect to the domain, or alternatively select an account already added to Securden.

On completion, click **Next**

The page that appears will allow you to select the OUs/Groups/Computers from the domain. You can search and select the required assets and add them to Securden.

Once you complete the step 2 above, the imported IT assets will appear in the list on the page **Admin >> Remote Sessions and Recordings >> Assets for Remote Connections.**

As previously mentioned, the assets added here need to be associated with the required domain accounts. Typically, the asset is associated with specific users/user groups and accounts/folders in Securden.

This can be done from Admin >> Remote Sessions and Recordings >> Domain Account - Assets Association. Once the association is made, the asset will appear in the list of remote session launch options for the specific domain account for the specific users.

Domain Accounts - Asset Associations

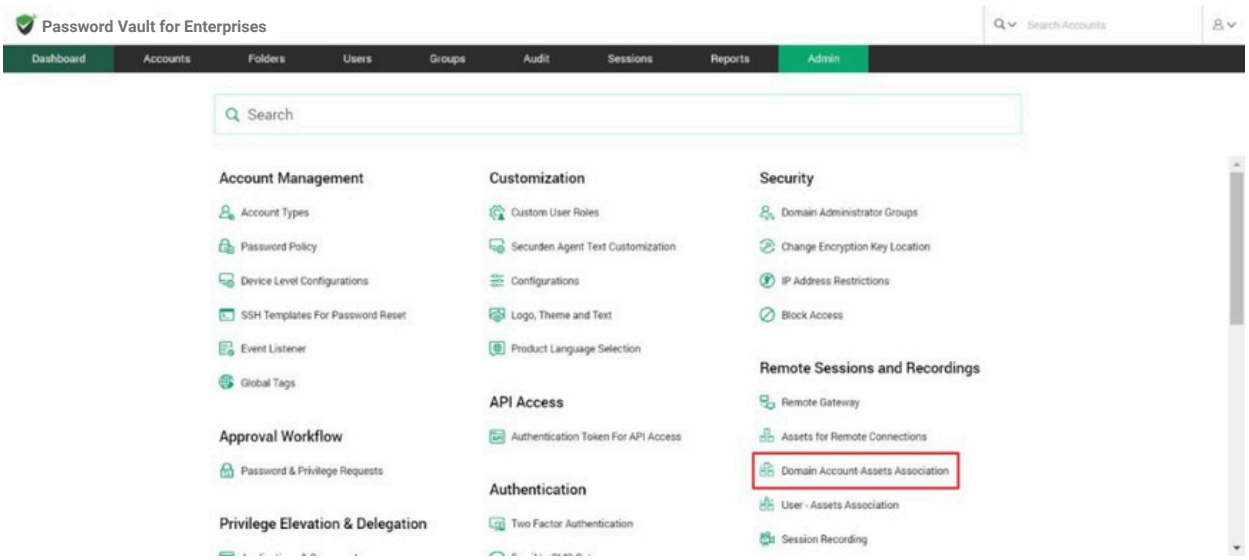
If any domain account is used to remotely connect to multiple IT assets, creating an association between the domain accounts and the list of IT assets it could connect to, becomes necessary.

Typically, an asset is associated with specific users/user groups and accounts/folders in Securden. That means, you will specify ‘who’ can launch a remote connection to ‘what’ asset using ‘which’ domain account.

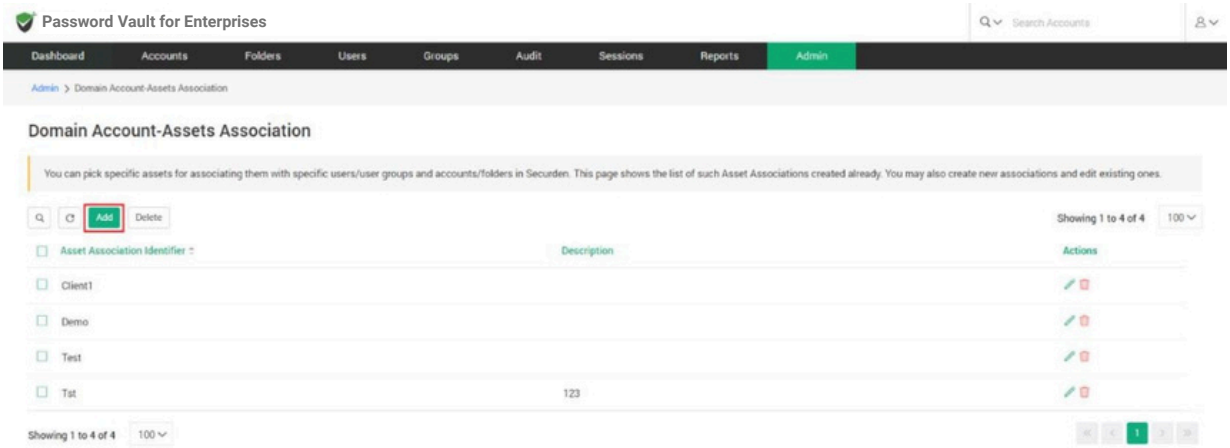
Once the association is made, the asset will appear in the list of remote session launch options for the specific domain account for the specific users. You can create any number of such associations from this section.

Adding Asset Associations

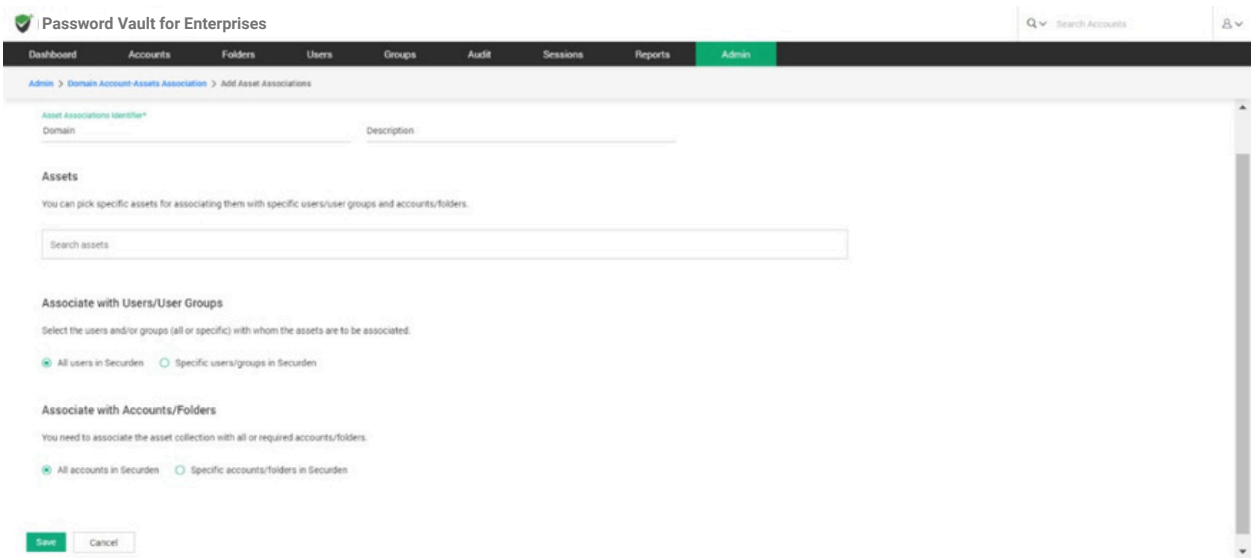
To add a new asset association configuration, navigate to **Admin >> Remote Sessions and Recordings >> Domain Account - Asset Association**



In the GUI that opens, all added domain-asset associations will be listed. You can choose to add a new association. Click on '**Add**'.



In the GUI that opens, you need to fill in certain attributes – like an identification name for the association etc.



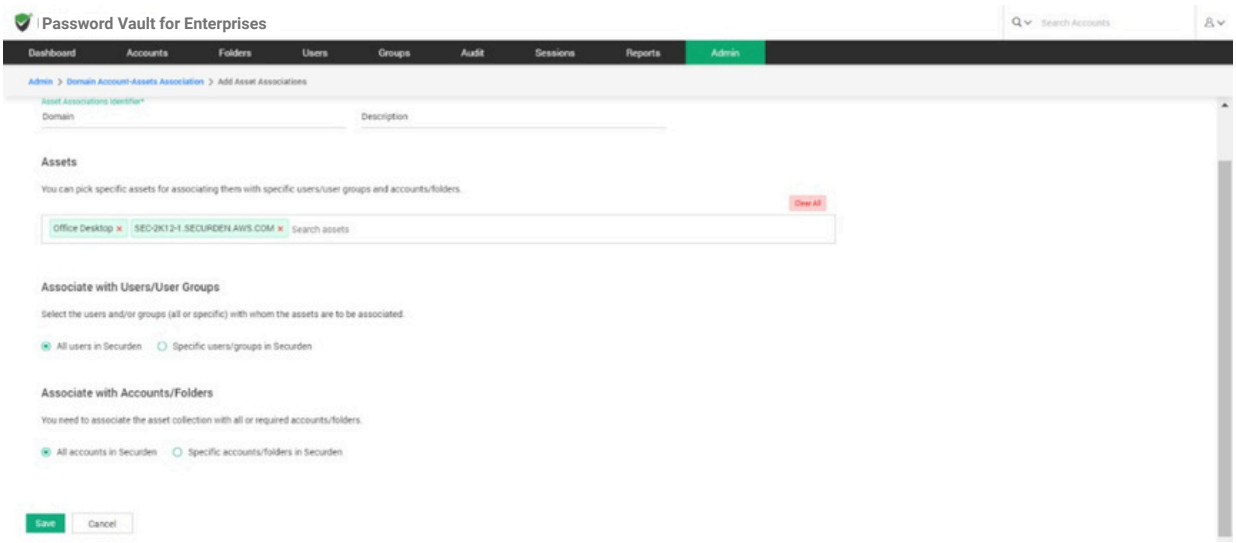
The fields to be filled are explained below:

Asset Association Identifier - Provide a name for the new mapping being created. The name you enter here helps uniquely identify the asset-account association.

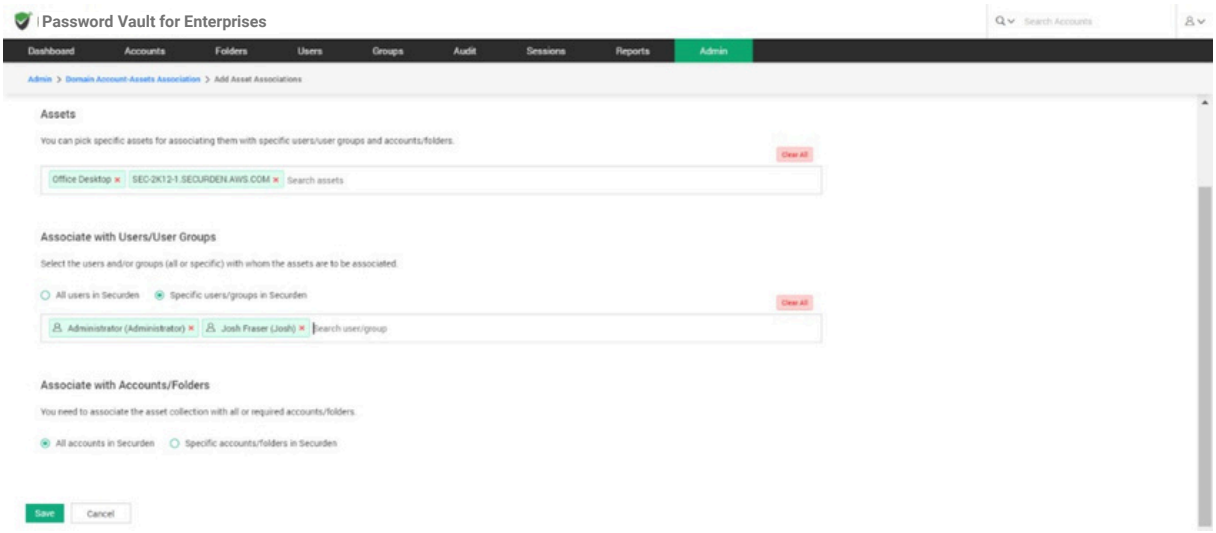
Description - Provide a Description for this association.

Select the Assets - You can pick one or more assets for associating them with specific users/user groups and accounts/folders.

Securden will display all the Assets that were already added in the drop-down list in the field under “Assets”. Search the drop-down and add the asset you want to associate with the Users/User groups and Accounts/Folders. You can select any number of assets.



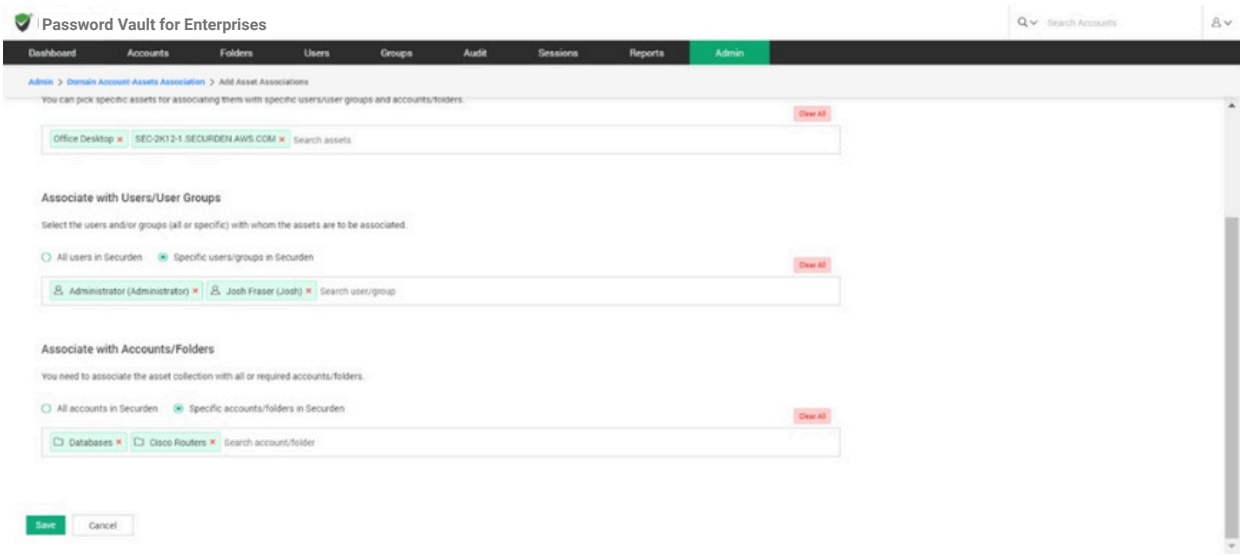
Associate with User/User Groups



You can choose to associate the selected assets with all the users and groups in Securden by selecting the option **All users in Securden.** You can also associate the assets with specific users and groups by selecting the option **Specific users / groups in Securden**.

If you select **Specific users / groups in Securden**, all the users and groups present in Securden will be displayed in the drop-down list. Search and add all the users and groups you want to associate with the selected assets.

Associate with Accounts / Folders

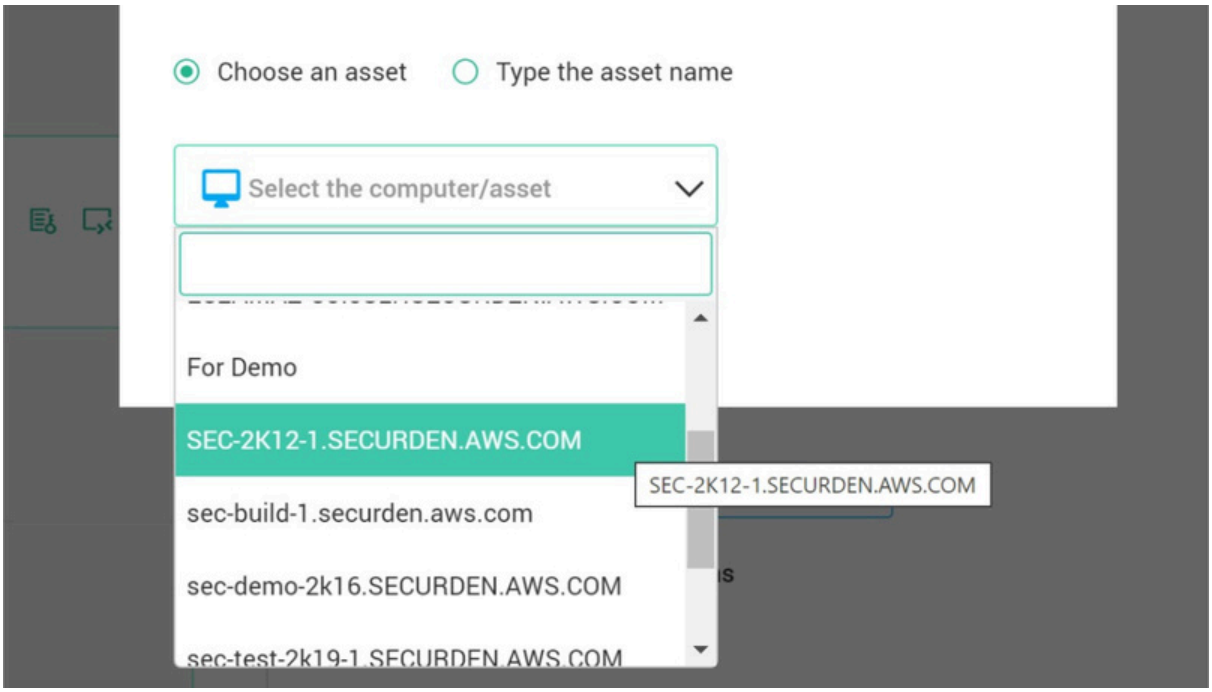


The final step in the association process is to link the assets and users/groups selected above with the required accounts/folders.

You can choose to associate the selected assets with all the accounts and folders in Securden by selecting the option **All accounts in Securden**. You can also associate the assets with specific accounts and folders by selecting the option **Specific Accounts / Folders in Securden**.

If you select **Specific accounts / folders in Securden**, all the accounts and folders present in Securden will be displayed in the drop-down list. Search and add all the accounts and folders you want to associate with the selected assets. Once you've associated the selected assets with users/accounts, click **Save**.

Once this association is completed, when launching a connection using a domain account, the associated asset will appear in the drop-down as shown below:

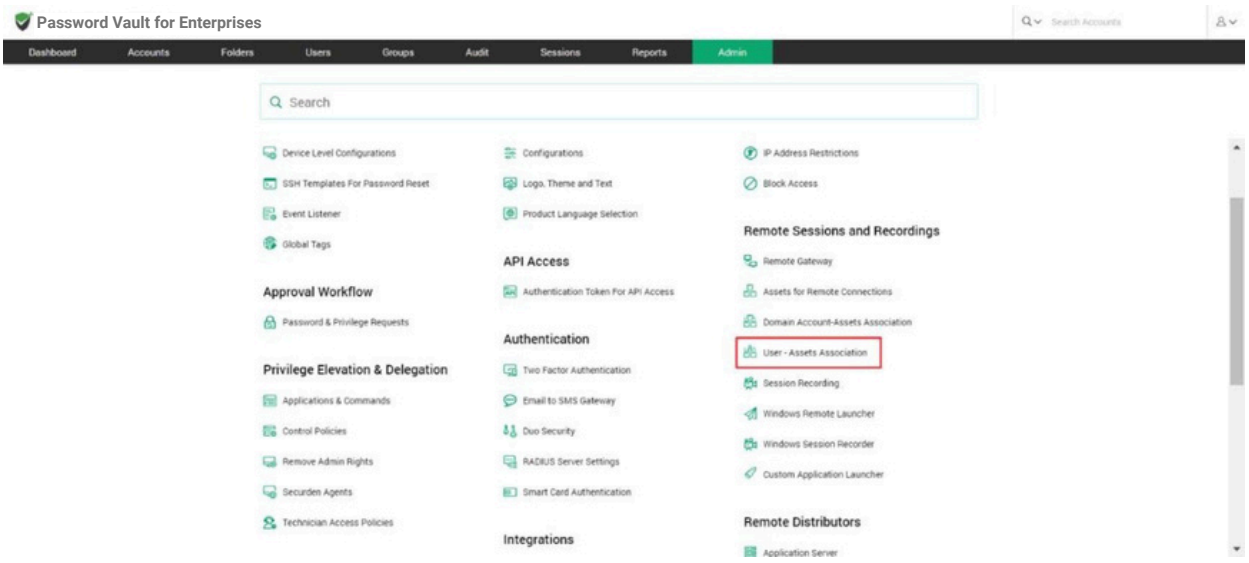


User – Assets / Application Association

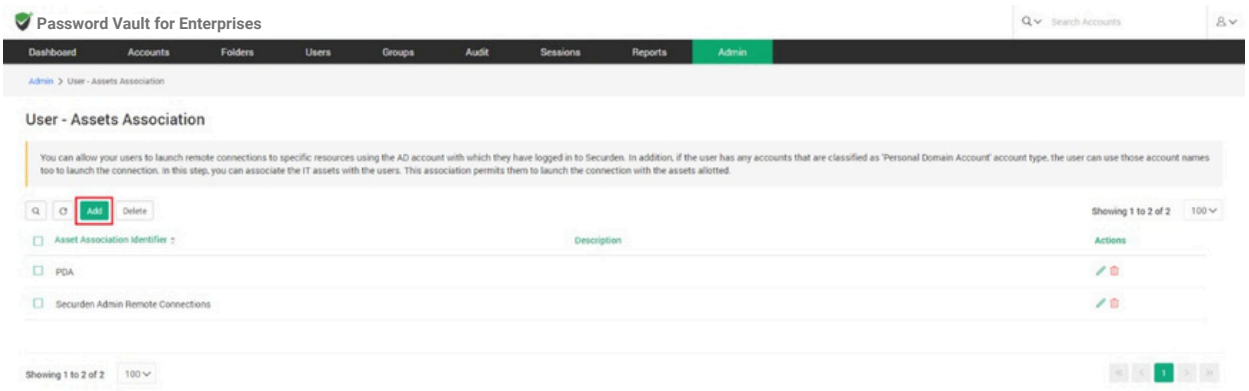
You can allow your users to launch remote connections to specific resources using the AD account with which they have logged in to Securden. In addition, if the user has any accounts that are classified as 'Personal Domain Account' account type, the user can use those account names too to launch the connection. In this step, you can associate the IT assets with the users. This association permits them to launch the connection with the assets allotted.

Additionally, you can also associate the applications with the users. This association permits them to launch the connection with the thick client applications allotted.

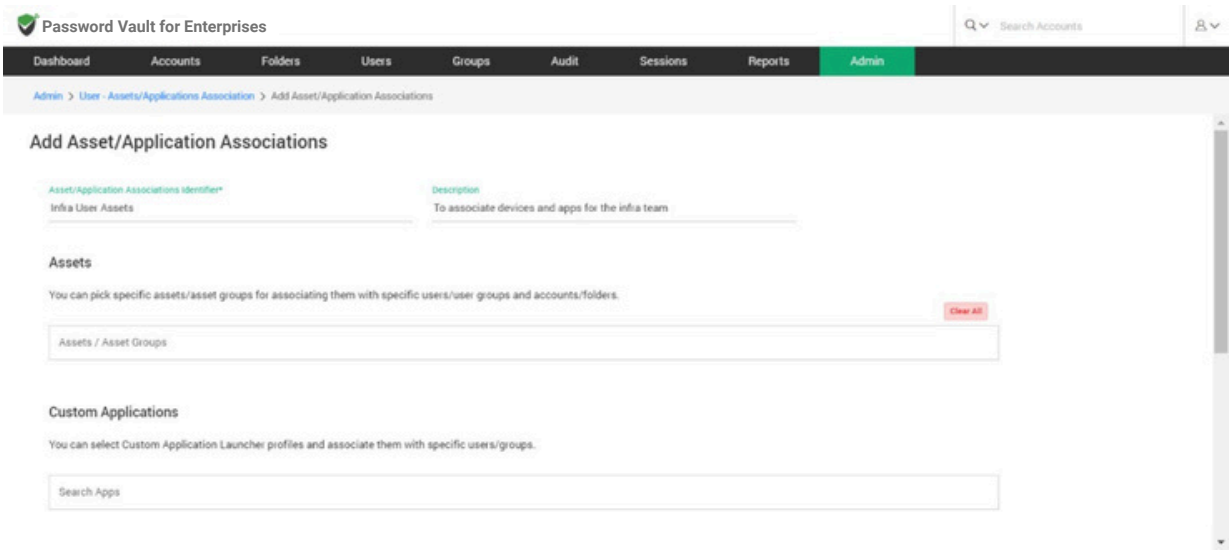
To associate assets/applications with users, navigate to **Admin >> Remote Sessions and Recordings >> User – Assets/Applications Association**



In the GUI that opens, click on **Add** to add a new user-asset/app association.



In the page that opens, you can associate assets with users the same way assets were associated with domain accounts.



You need to enter the following details on the page:

Asset Association Identifier - Provide a name for the new mapping being created. The name you enter here helps uniquely identify the asset-account association.

Description - Provide a Description for this association.

Select the Assets - You can pick one or more assets for associating them with specific users/user groups and accounts / folders.

Securden will display all the Assets that were already added in the drop-down list in the field under **Assets.** Search the drop-down and add the asset you want to associate with the Users/User groups and Accounts/Folders. You can select any number of assets.

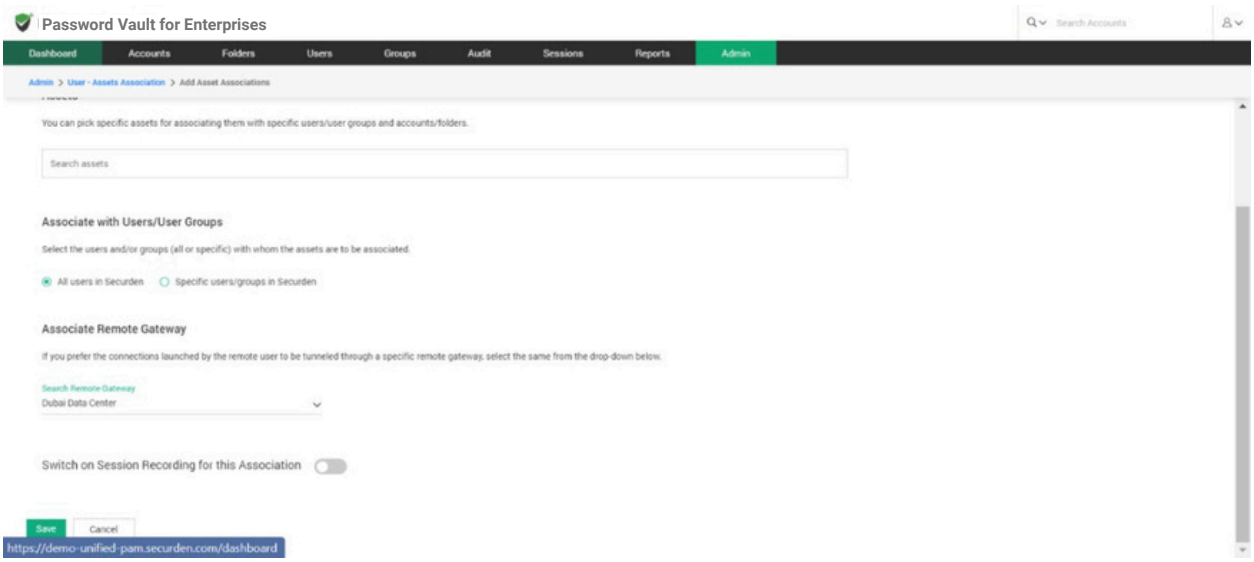
Select the Custom Applications - You can pick one or more custom applications for associating them with specific users/user groups and accounts / folders.

Pre-requisite: You should have added custom app launcher profiles under **Admin >> Remote sessions and recordings >> Custom application launcher.**

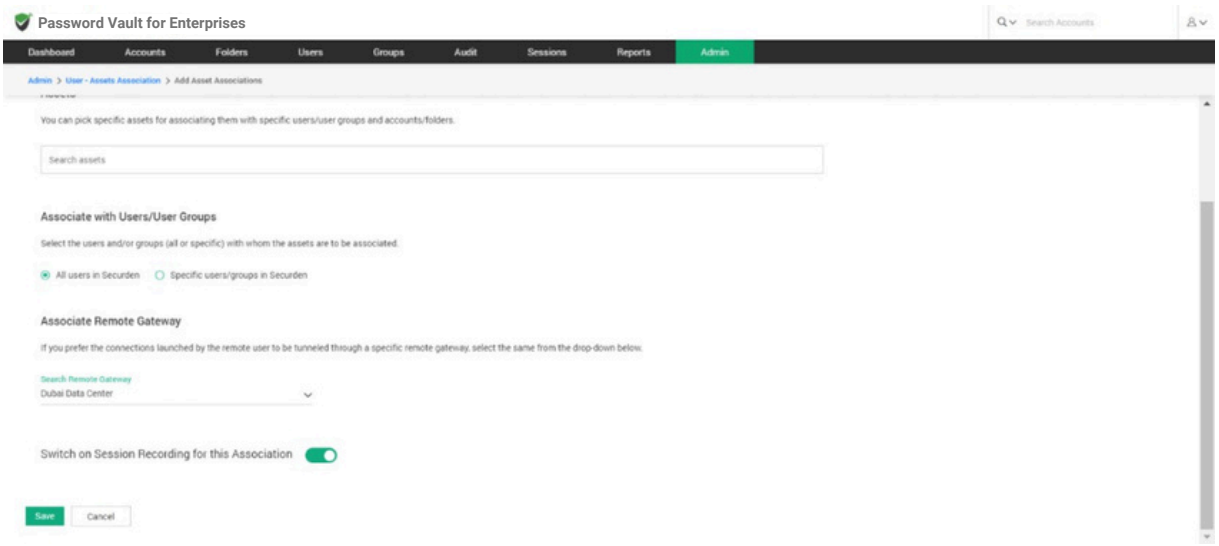
Search the drop-down and add the application you want to associate with the Users / User groups and Accounts / Folders. You can select any number of custom applications.

Associate a remote gateway ENTERPRISE PAM

You can choose to tunnel the connections launched by the remote user through a specific remote gateway, select the same from the drop-down on the page.



You have the option to record all the sessions launched using the associated remote gateway by the selected users. Enable the switch if you wish to do so.



On filling all the fields, click **Save**.

Custom Application Launcher

Securden facilitates launching connections with remote IT assets and applications. In addition to the default modes of launching web-based connections and through native clients, you can define custom application launchers to supply/autofill credentials and automatically launch any application, including thick application clients.

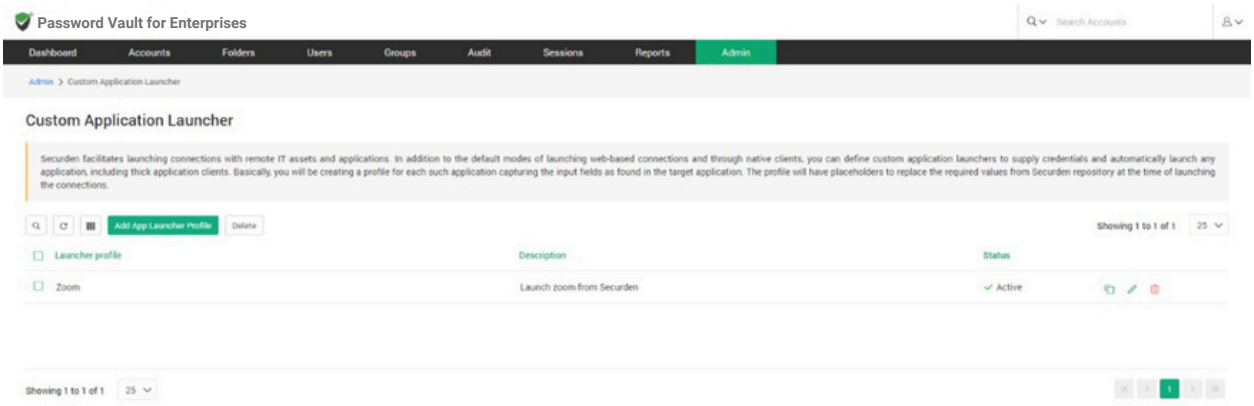
Creating a custom launcher basically involves creating a profile for each such application capturing the input fields as found in the target application. The profile will have placeholders to replace the required values from Securden repository at the time of launching the connections.

To create/configure the application launcher profile, navigate to **Admin >> Remote Sessions and Recordings >> Custom Application Launcher.**

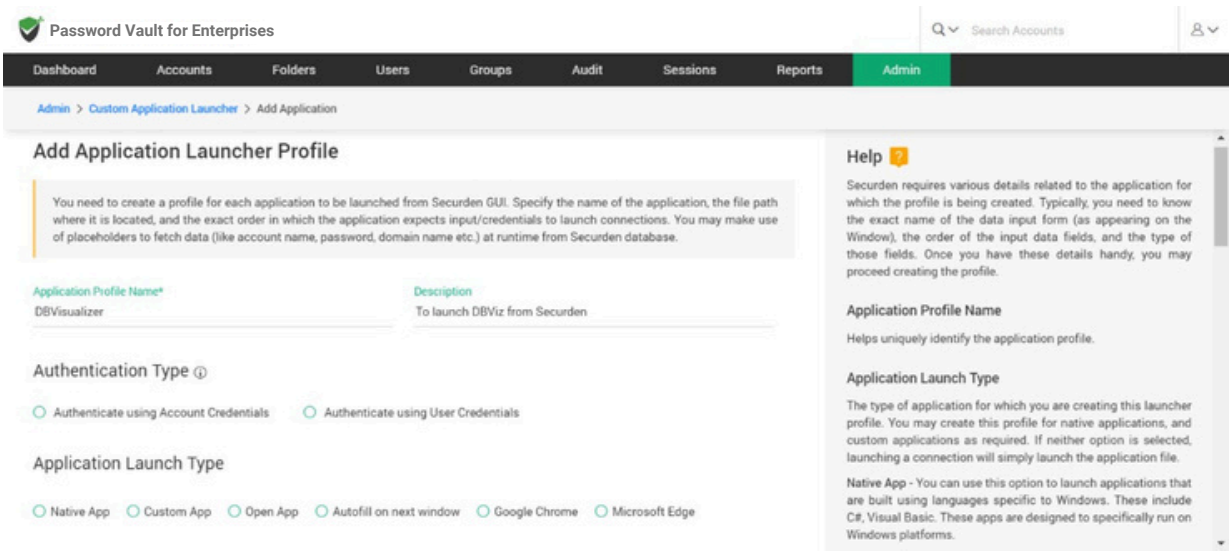
In the page that opens, you can create new app launcher profiles or configure existing launcher profiles.

Create an app launcher profile

To create a new application launcher profile, click on **Add App Launcher Profile**.



Securden requires various details related to the application for which the profile is being created. Typically, you need to know the exact name of the data input form (as appearing on the Window), the order of the input data fields, and the type of those fields. Once you have these details in hand, you may proceed to create the profile.



In the GUI that opens, the following fields need to be filled:

Application Profile Name: The name that you enter here helps you uniquely identify the application profile being created. This name will appear on the remote connection launching section in Securden. Your users will identify the launch option through this name.

Description (Optional): A brief of the app launcher for a quick overview, this could explain the purpose of this launcher profile.

Authentication Type

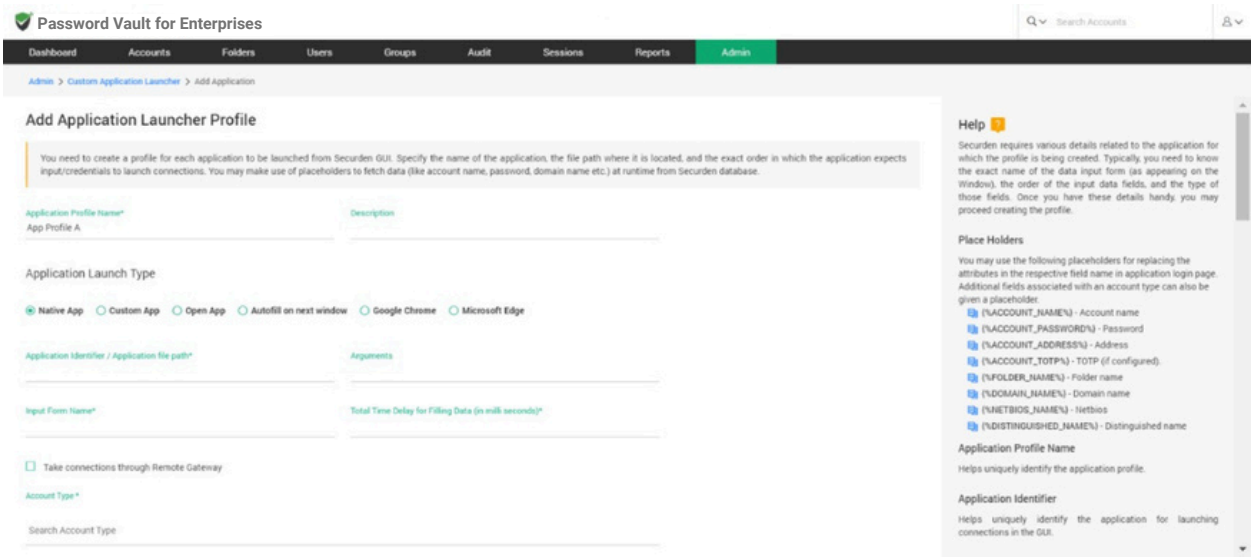
- Authenticate using Account Credentials

If you select this option, you need to specify the account types for which this custom application launcher profile is applicable. Once the profile is created, it will be automatically added to the list of available connections for all accounts of the selected type and the account credentials will be used for authentication

- Authenticate using User Credentials

Once the application launcher profile is created, it should be associated with the required users. Credentials of the associated user will be used for authentication. To associate the profile, navigate to **Admin >> Remote Sessions and Recordings >> User - Assets/Applications Association**

Once you have filled these fields, you need to select an **Application Launch Type**



This is the type of application for which you are creating this launcher profile. You may create this profile for native applications, custom applications or explore other options as required.

- **Native Applications:** Generally, Windows applications possessing one or more drop-downs, text-boxes, password fields and action buttons are called native applications in Securden. Securden can easily identify the fields of native windows apps. If you are familiar with the exact values the fields in your application would hold, you may select the option **Native Apps**. SQL server studio is a typical example of a native app.

- **Custom Applications:** Applications that have a more complex field pattern can be classified as custom applications. Zoom, Skype, any other app/web-app are examples of custom applications.

• **Open Application:** If you wish to simply launch/open an application without needing to input credentials and other fields in it, you may select the option **Open App**.

• **Autofill on next window:** If you want to autofill credentials on active applications, you can select the checkbox Autofill in the next active application. Although, while launching a connection using this method, applications will not be launched. Instead, Securden will autofill credentials in the next active application window (the window that opens when you press Alt+Tab). You need to ensure that the appropriate window is manually launched beforehand and is the next active window.

Important Note: The autofill option simply changes the input focus to the next active application regardless of its type and autofill the credentials. For example, if the next active application happens to be a notepad, it will autofill the credentials there too. So, exercise care in selecting this option. If you are granting access with 'Open Connection' permission to an account, enabling this option may result in auto-filling credentials (in plain text) on any application and might potentially reveal the credentials.

• **Google Chrome/Microsoft Edge:** If you wish to launch a chrome or edge browser you can select this option. Securden auto-fills the fields known for the Chrome/Edge profile so you can fill the rest with ease.

Application Identifier/Application file path: This is an important configuration parameter. You need to specify the name of the custom application you want to launch (for example, test.exe. The application should be in the system path) OR the exact file path of the application (for example, C:\example\testapp.exe). This application should be available on all the client machines from which users would try to launch the application from Securden.

Arguments (Optional): If the application requires any arguments to be passed for launch, you may enter the same here. For example, some applications might require IP addresses to launch the application. In such cases, you may pass the required value as an argument as shown below:

/h {%ACCOUNT_ADDRESS%}

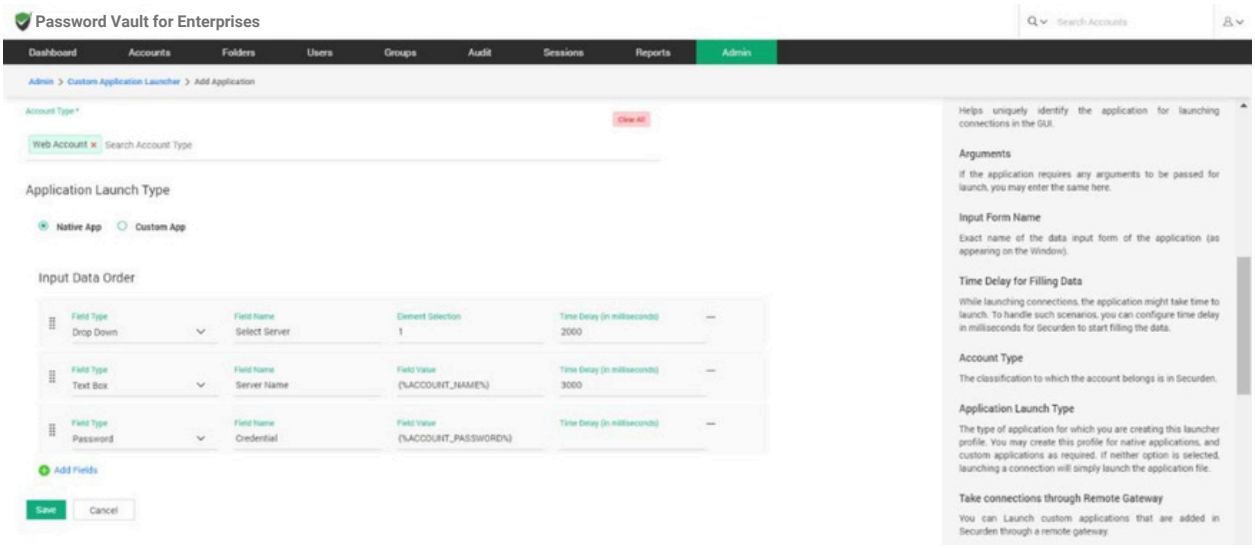
Input form name: Exact name of the data input form of the application (as appearing on the Window)

Time Delay for Filling Data: While launching connections, the application might take time to launch. To handle such scenarios, you can configure time delay in milliseconds for Securden to start filling the data.

Account Type: This represents the **Account Type** in Securden. The custom profile being created, will be applicable only for the selected account type.

Creating a native app launcher profile

Native app launcher profiles will require you to fill in the order of input data fields and enter the field value. Each input action has to be defined according to the order in which they will be filled.



The steps to follow while entering each input action is as follows:

- Firstly, select the field type – this can either be a text field, a button, a password or a drop-down.
- Then, enter the name of the field that appears on the application.
- Specify Field Value and Select Element

If the field type in your application form is of the type **Drop Down** you will have to take care of **Element Selection**.

Element Selection for drop-down allows you to select the entries from the drop-down. If you enter the element value as ‘0’, the first entry in the drop down will be selected. 1 will choose the second entry and so on.

If the field type in yourapplication form is of the type **Text-box** you will have to take care of **Specify Value**.

In the case of text fields, you can specify the value to be filled in for the specific input field. It could be the account name, password, or any other value. When specifying the value, you have the option to use placeholders as explained below.

The values for the placeholders will be taken by Securden at runtime:
You may use placeholders for replacing the attributes in the respective field name in application login page.

{%ACCOUNT_NAME%} - to be replaced with the respective “Account name” at runtime

{%ACCOUNT_PASSWORD%} - to be replaced with the account’s password at runtime

{%ACCOUNT_ADDRESS%} - to be replaced with the respective account’s “IP Address” at runtime

{%ACCOUNT_TOTP%} - to be replaced with the respective account TOTP token at runtime (if configured)

{%DOMAIN_NAME%} - to be replaced with the domain name of the mentioned account

{%NETBIOS_NAME%} - to be replaced with the NetBIOS name of the account mentioned.

- Specify **Time delay**

Wherever you want Securden to wait for a few milliseconds before filling the respective data while launching the application, you may add **Time Delay** in milliseconds.

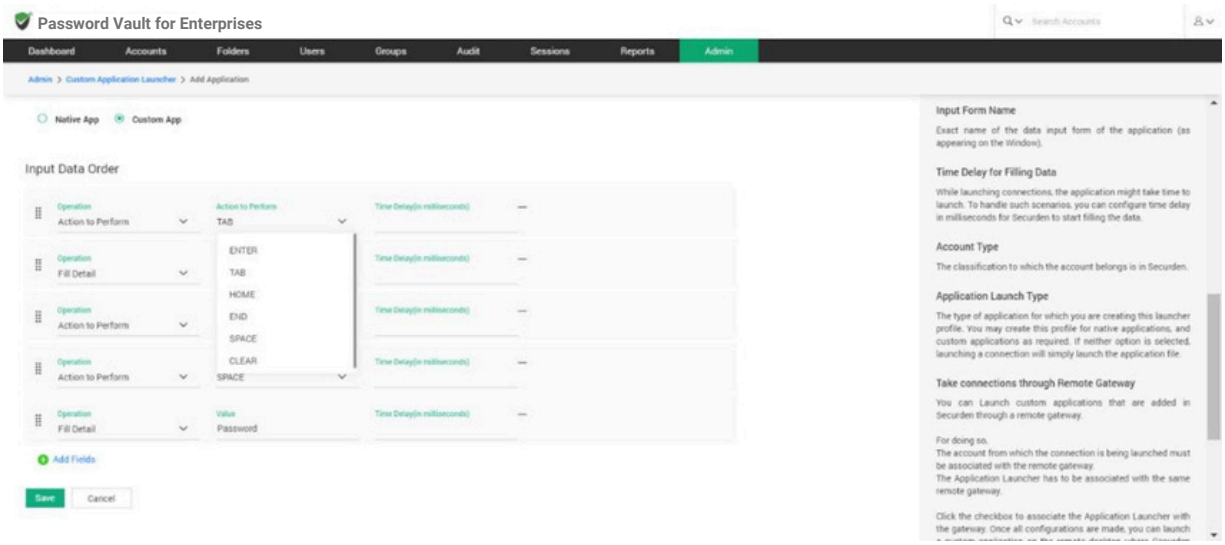
Once you have defined the Input Data Order, click **Save** to add the native app launcher profile in Securden. The native application can now be directly launched from Securden.

Creating a custom app launcher profile

Custom app launcher profiles require you to fill in the order of input data fields and enter the field value, similar to the native app launcher. Each input action has to be placed according to the order in which they will be filled in the application.

The steps to follow while entering the input data order is as follows:

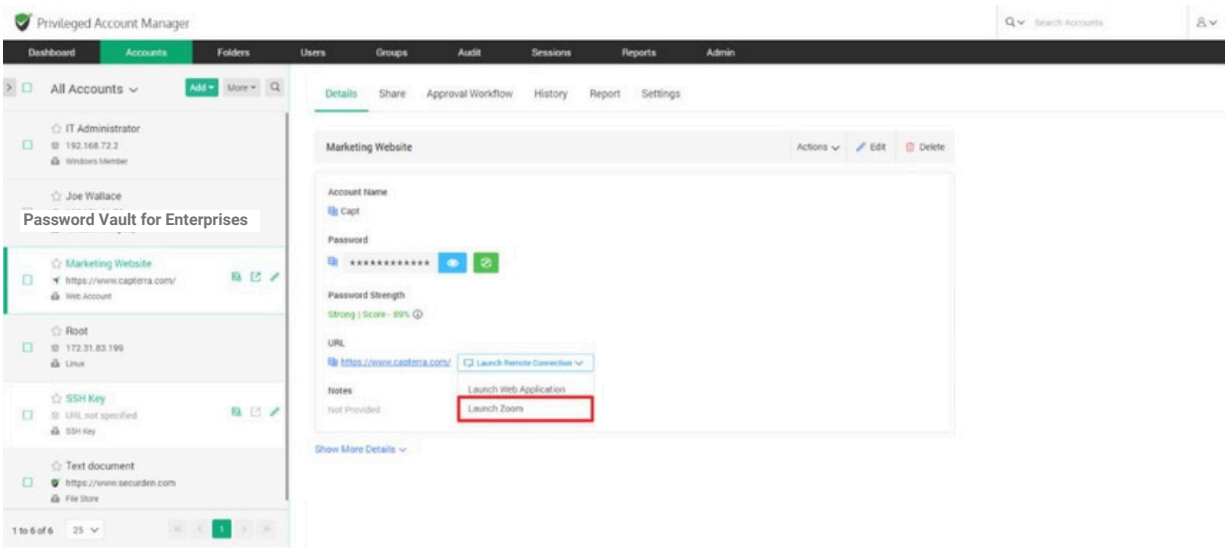
- Firstly, select the **Action to Perform -** This lets you perform actions like clicking TAB, ENTER, SPACE etc. on the application.
- Then select the **Fill Detail** operation and specify the value that will be filled in after the selected action is performed.
- Repeat the input actions in the order that they will be carried out.



You have to carry out these steps for each input action added to the launcher. Once you have defined the Input Data Order, click **Save** to add the custom app launcher profile in Securden. The custom application can now be directly launched from Securden.

Launching Remote Connections Using the Custom Launcher

Once you create the app launcher profile, the custom app launcher will be available in the remote access drop-down for accounts with the specified account type.

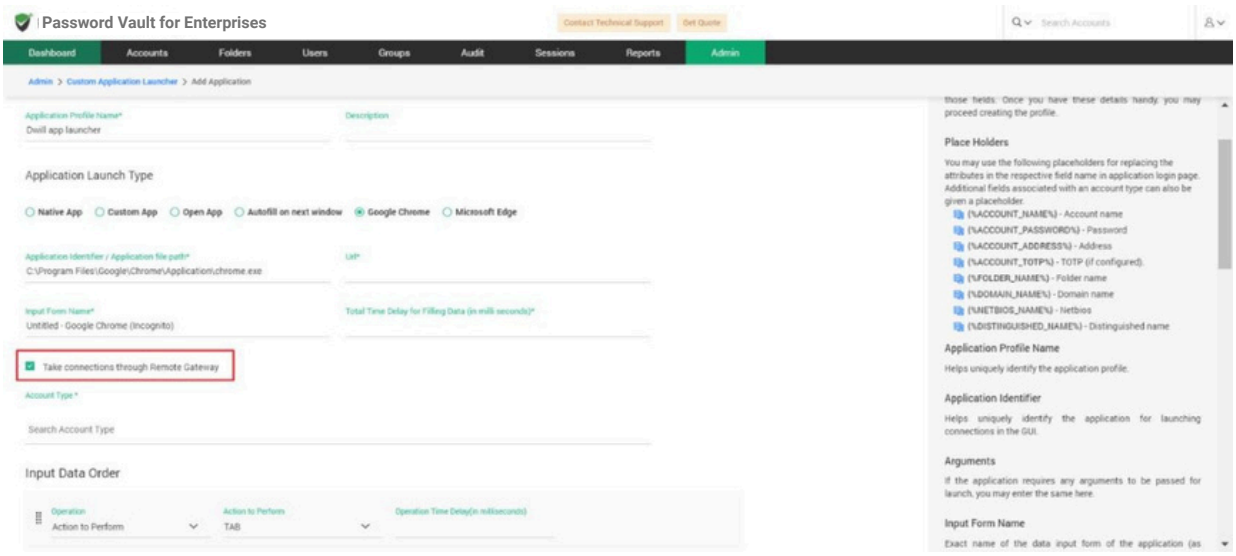


You can click that and directly launch the connection.

Take connections through Remote Gateway ENTERPRISE PAM

You can launch custom applications that are added in Securden through a remote gateway. As a pre-requisite, the account from which the connection is being launched must be associated with a remote gateway.

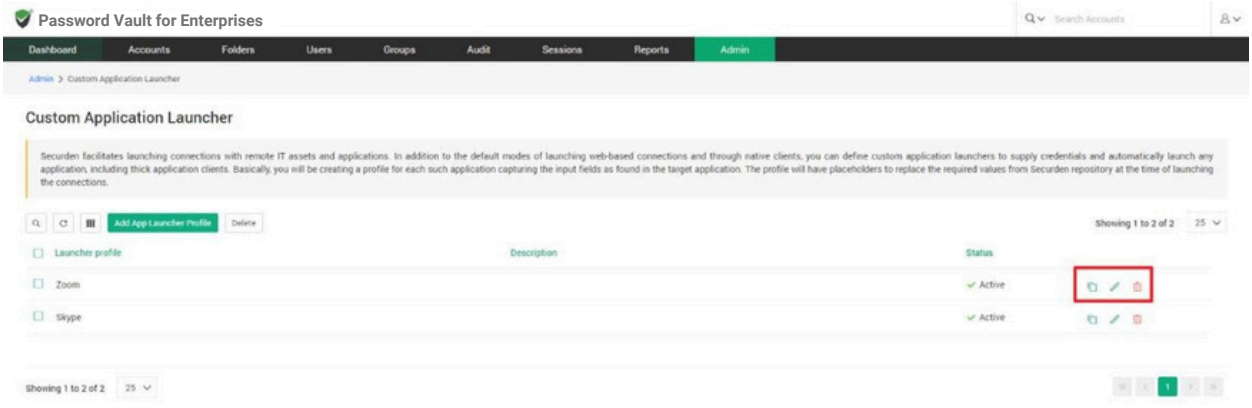
Click the checkbox **Take connections through the remote gateway**.



Once all configurations are made, you can launch the custom application through the remote gateway. You can create a Remote Gateway from **Admin >> Remote Sessions and Recordings >> Remote Gateway**

Configure an existing app launcher profile

You have the option to clone, edit, or delete a previously created app launcher profile. This can be done using the action buttons highlighted below.



Section 10: Customization

Customize Password Vault

You can customize Securden Password Vault to suit your organization's unique needs. Securden allows you to create custom user roles, granularly switch on and switch off certain features, add your company logo, modify the text appearing at certain places, select the display language of product interface, and so on. Navigate to **Admin >> Customization** section to check the various customization options.

Configurations

Securden lets you comprehensively enable, disable, and configure all the features that are part of the solution. You can make necessary modifications to the required features from the **Configurations tab** available under **Admin >> Customization**.

Defaults selection

When importing users from AD or file, what should be the default role?

While importing users from the Active directory, you can assign role to the users. You have the option to select which role users are imported with. When you click change, it shows the list of default roles and custom roles available.

You can choose from the list of roles. The users which gets imported after changing the role will acquire that role.

While importing user groups from AD/Azure AD, do you want to configure automatic synchronization with Securden groups?

You can automatically synchronize the user groups in Securden with that of Active Directory. Automatic synchronization is applicable only for the user groups imported after saving this configuration. When users are added or deleted in AD, the same gets reflected here. You can also define the synchronization interval.

When you click change, a GUI with two options ‘Configure’ and ‘No’ appears. When you select No, automatic synchronization will be disabled. If you select ‘Configure’

A GUI named ‘Configure Automatic Group Synchronization’ appears. You can customize the time interval with which the synchronization should happen. After selecting the time interval click on ‘**Save**’ to see the changes.

When synchronizing user groups with AD in Securden, do you want to remove the users (from the group) who remain disabled in AD? If you select 'No' for this option, the disabled users in AD will only be disabled in Securden too. They will not be be removed from the respective group.

Securden allows you to remove the imported users who are disabled in the Active directory. If you don’t want them to be removed you can just disable them. When you click change, a GUI with two options Yes and No appears. If you select Yes, the disabled users in the Active Directory will be removed. If you select No, the disabled users in AD will only be disabled in Securden too. They will not be removed from the respective groups.

Do you want to receive an email alert on the remaining user license count (when you can add less than 5 users)?

Securden allows up to 5 free users. You have the option to receive email alert on the remaining user license when the added user count is less than 5.
When you click change, a confirmation box will appear saying Yes and No. You'll receive email alerts if you select Yes and if you select No, it will be disabled.

Do you want to enable hotkeys?

Hotkeys here are nothing but the shortcut keys used inside the Securden UI. Securden has many hotkeys like ctrl+shift+U for copying account name, ctrl+shift+P for copying password, ctrl+shift+S for opening advanced search etc.

When you click change, a list with options like **Enable for all, Disable for all** and **Customize** appears. You can enable hotkeys for a custom list of users by selecting customize. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added below.

You can enable hotkeys for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added below.

Do you want to send email alerts to users on user addition?

Securden sends email alerts to the users upon adding them. It is not mandatory. If you want to disable it, you can do it in the configuration section.

When you click change, it comes with the dropdown that says **Yes** and **No.** If you want to send email alerts, you can select **Yes** and if you don't want you can select **No.**

Do you want to send email alerts when users are added in specific roles?

Securden has the flexibility to send email alerts to specific roles. It is totally customizable.

When you click change, it shows options like No and Customize. You can choose from the options given. If you don't want to send email, you can select No. If you want to customize, you can select customize and make the required customization from the respective section.

Do you want to include the username of the creator and the time of creation as a footer in PDF reports?

Securden allows you to generate reports in the form of PDF. You have the option to include the username of the creator and the time of creation as a footer in PDF reports.

When you click change, a GUI with two options Yes and No appears. If you want to include the details in PDF, you can select Yes. If you don't want to include the details, you can select No.

Password Policy

Would you like to enforce password policy during account addition and local password resets?

Securden allows you to enforce password policy during account addition and local password resets.

When you click change, a GUI with two options Yes and No appears. If you select Yes, password policy will be enforced and if you click No, it will not be enforced.

You can enforce complexity rules for the passphrase to be used for offline access. Select a password policy to be enforced for that purpose.

Securden allows you to create and enforce the complexity rules for passphrase to be used for offline access. You have the option to specify and enforce an existing password policy for the passphrase used to encrypt the offline copy.

When you click change, a GUI named ‘Change Password Policy for Offline Access’ appears. You have to enter password policy by clicking the drop- down and click ‘**Change policy**’ to enforce them.

RESTful API

Do you want to allow API access for all users?

Securden allows you to have API access for all users. You can disable it for all and also customize it as desired. All these can be done in the **Admin>>Configurations section**.

When you click change, a dialog box with four options ‘Allow for all’, ‘Deny for all’, ‘Deny for Users & Auditors’ and ‘Customize’ appears. When you select ‘Allow for all’, all users will be allowed access and if you select ‘Deny for all’,

all users will be denied from using API access. If you select ‘Deny for Users & Auditors’, only the Users & Auditors will be denied. If you select customize,

You can enable API access for a custom list of users. If you select 'Allow', this configuration will be applicable only to the users/groups added below. If you select 'Deny', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

Account Management

Do you want to enforce folder selection while adding/editing accounts?

Securden allows you to enforce folder selection while adding/editing accounts. You have the option to enable/disable/customize the folder selection. When you click change, a confirmation box with three options Enable for all, Disable for all and Customize appears. If you select enable for all, the folder selection will be enforced for all the users and if you select disable for all it will be disabled for all the users.

If you select customize, you can enforce folder selection while adding / editing accounts for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added.

Do you want to display the account details page in expanded form by default?

Securden allows you to display the account details page in expanded form by default. You can enable display of account details page in expanded form for a custom list of users.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', It will be displayed for all users. If you select 'Disable for all', it will not be displayed for anyone. If you select Customize,

You can enable display of account details page in expanded form for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users / groups added below. If you select 'Disable', this configuration will be applicable to all users / groups except the ones added.

Do you want to enforce users to provide reason while retrieving passwords?

Securden allows you to enforce users to provide reason while retrieving passwords. If you don’t want to enforce it for all the users and you want to customize it for specific users/Groups, you can go ahead and do it.

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, all users will be providing reasons while retrieving passwords and if you select ‘Disable for all’, this option will be disabled. If you select ‘Customize’,

You can enforce providing reason while retrieving passwords for a custom list of users . If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added.

Do you want to enforce users to provide reason while launching remote connections using the remote launch icon

Securden allows you to enforce users to provide reason while launching remote connections using the remote launch icon. You can disable it and also can customize it for specific Users/Groups.

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, it will be enforced for all the users and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’,

You can enforce providing reason while launching remote connections via the remote launch button for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Finally click ‘**save**’ to show changes.

Do you want to enforce users to provide reason while changing password?

Securden allows users to provide reason while changing passwords. You can disable it for all the users and also can customize it for specific Users/Groups..

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, it will be enforced for all the users and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears

You can enforce providing reason while changing passwords for a custom list of users . If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click ‘**Save**’ to show changes.

Do you want to enforce users to provide a reason while deleting accounts and folders?

Securden allows users to provide a reason while deleting accounts and folders.
You can disable it for all the users and also can customize it for specific Users / Groups.

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, it will be enforced for all the users and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears

You can enforce a custom list of users to provide a reason while deleting accounts and folders. If you select ‘Enable’, this configuration will be applicable only to the users / groups added below. If you select ‘Disable’, this configuration will be applicable to all users / groups except the ones added. Click ‘**Save**’ to show changes.

Do you want to allow concurrent access to an account for multiple users as part of approval workflow? If this is allowed, the account owner also will be able to view the password and launch a concurrent remote connection with the device even when another user is using the password.

Do you want to display Recently Deleted Accounts by default?

Securden allows users to display Recently Deleted Accounts by default. You can disable it for all the users and also can customize it for specific Users/Groups. When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, it will be enforced for all the users and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears

You can set password change as a default when logging into remote machines.. If you select 'Allow', this configuration will be applicable only to the users/groups added below. If you select 'Deny', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

Do you want to restrict the time duration for password access requests as a part of 'Approval Workflow'? Once configured, users will have to specify a time duration (in minutes) within the maximum duration specified

Securden allows an option to restrict the time duration for password access requests as a part of 'Approval Workflow'.

When you click change, a GUI 'Configure Maximum Time Duration for Password Access' appears. If you want to restrict time limit, select 'Restrict Time Duration' you can specify the upper limit (in minutes) within which users can request access for password and if you don't want, you can select 'No restriction'. Click **Save** changes.

Do you want to deny account addition permission (work accounts) to the users with roles 'User' and 'Auditor'?

Securden have the option to deny account addition permission (work accounts) to the users with roles 'User' and 'Auditor'.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, users with roles 'Users' and 'Auditors' will be denied account addition permission and if you select No, users will not have any such restrictions.

Do you want to allow users with the roles 'User' and 'Auditor' to import accounts from files?

Securden allows users with the roles ‘Users’ and ‘Auditor’ to import accounts from files. If you don’t want you can just disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, users with roles ‘Users’ and ‘Auditors’ will be allowed to import accounts from files and if you select No, users will not have any such permissions.

Do you want to allow users with roles 'User' and 'Auditor' to edit the details of accounts that are shared to them with ‘Manage’ privilege?

Securden allows users with the roles ‘Users’ and ‘Auditor’ to edit the details of accounts that are shared to them with ‘Manage’ privilege. If you don’t want you can just disable it.

When you click change, a confirmation box will appear saying Yes and No.If you click Yes, users with roles ‘Users’ and ‘Auditors’ will be allowed to edit the details of accounts that are shared to them with ‘Manage’ privilege and if you select No, users will not have any such permissions.

Do you want to allow users (irrespective of the role) to view the 'Password History' of accounts if the share permissions allow them to view passwords?

Securden allows users (irrespective of the role) to view the 'Password History' of accounts if the share permissions allow them to view passwords. If you don’t want you can just disable it.

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, it will be enforced for all the users and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears.

You can allow a custom list of users to view 'Password History' of accounts if they already have view permission. If you select 'Allow', this configuration will be applicable only to the users / groups added below. If you select 'Deny', this configuration will be applicable to all users / groups except the ones added.

Click ‘**save**’ to show changes.

Do you want to deny account sharing permission to the users with the roles ‘User’ and ‘Auditor’?

Securden have the option to deny account sharing permission to the users with roles ‘User’ and ‘Auditor’. If you don’t want you can just disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, users with roles ‘Users’ and ‘Auditors’ will be denied account sharing permission to the users with the roles ‘User’ and ‘Auditor’ and if you select No, users will not have any such restrictions.

Do you want to enforce selection of a parent folder while adding / editing folders?

Securden allows you to enforce selection of a parent folder while adding / editing folders. If you don’t want you can disable it.

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, it will be enforced for all the users and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears.

You can enforce parent folder selection while adding/editing folders for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added.

Click ‘**save’** to show changes.

During folder creation, do you want to enable 'permissions inheritance from parent folders' by default?

Securden allows you to enable ‘permissions inheritance from parent folders’ by default during folder creation. If you don’t want you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, ‘permission inheritance from parent folders’ will be enabled by default during folder creation and if you select No, it will be disabled.

Do you want to enforce 'permissions inheritance from parent folders', while creating or editing a folder?

Securden allows you to enable ‘permissions inheritance from parent folders’ while creating or editing a folder. If you don’t want you can disable it.

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, it will be enforced for all the users and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears.

You can enforce parent folder inheritance for specific users/groups. You can do this by selecting the list of users/groups and enable/disable parent folder inheritance. Click ‘**save’** to show changes.

Do you want to restrict users with roles 'User' and 'Auditor' from deleting the accounts owned by them?

Securden have the option to restrict users with roles ‘User’ and ‘Auditor’ from deleting the accounts owned be them. If you don’t want you can just disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, users with roles ‘User’ and ‘Auditor’ will be restricted from deleting the accounts and if you select No, it will be disabled.

Upon clicking a folder in the 'Accounts' list view, do you want to show the accounts belonging to its sub-folders?

Securden have the option to show the accounts belonging to its sub-folders upon clicking a folder in the ‘Accounts’ list view. If you don’t want you can just disable it.

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, it will be enforced for all the users and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears.

You can enable viewing of accounts belonging to the sub-folders while clicking a folder in the 'Accounts' list view a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click ‘**save**’ to show changes.

Do you want to show the folders tree in collapsed mode on the 'Folders' tab?

Securden have the option to show the folders tree in collapsed mode on the ‘Folders’ tab. If you don’t want you can just disable it.

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, it will be enabled for all the users and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears.

You can apply this setting for specific users or a group alone. Select the names of users and groups here. If you select 'Enable', this configuration will be applicable only to the users/groups added. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click ‘**save**’ to show changes.

Do you want to show the folders tree structure in 'Accounts' view in compact form collapsing the entries by default?

Securden have the option to show the folders tree structure in ‘Accounts’ view in compact form collapsing the entries by default. If you don’t want you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, the folders tree structure in ‘accounts’ view in compact form collapsing the entries by default will be shown and if you select No, it will be disabled.

Do you want to allow users to add multiple accounts with the same account title?

Securden allows users to add multiple accounts with the same account title. If you don’t want, you can just disable it.

When you click change, a confirmation box will appear saying Yes and No.
If you click Yes, users can add multiple accounts with the same account title and if you select No, it will be disabled.

How long (in days) would you like to keep the recently deleted accounts before permanently deleting them?

Securden allows an option to keep the recently deleted accounts before permanently deleting them for a period of time. You can specify the time period (in days).

When you click change, a GUI appears ‘Recently Deleted Accounts Restoration’. You can specify the maximum number of days the recently deleted accounts to be kept for recovery. During this time window, you will have the option to recover. After that, the accounts will be permanently deleted. At last, click ‘**save**’ to show changes.

Do you want the system default folders to be shown on the Accounts page?

Securden have the option to show the system default folders on the Accounts page. If you don’t want.

When you click change, a dialog box with two options ‘Yes’ and ‘Customize’ appears. If you select Yes, the system default folders will be shown on the Accounts page and if you select Customize, a GUI appears

The list of default system folders is shown below. Select the ones that you want to see on the 'Accounts' page. The greyed-out items in the list cannot be disabled.

When searching for folders, do you want to include sub-folders in the search result?

Securden have the option to include sub-folders in the search result when searching for folders. If you don’t want, you can disable it. When you click change, a confirmation box will appear saying Yes and No. If you click Yes, sub-folders will be included in the search result when searching for folders and if you select No, it will be disabled.

Do you want allow your users to create their own tags while adding or editing work accounts?

Securden allows your users to create their own tags while adding or editing work accounts. If you don’t want, you can disable it.

When you click change, a dialog box with three options ‘Allow for all’, ‘Deny for all’ and ‘Customize’ appears. If you select ‘Allow for all’, users will be allowed to create their own tags while adding or editing work accounts and if

you select ‘Deny for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears.

You can enable or disable specific users/groups from creating custom tags. Disabled users/groups will only be able to utilize existing tags while creating/editing accounts. Click ‘**save**’ to show changes.

Do you want to customize the account details displayed in the 'Accounts' list view?

Securden allows you to customize the account details displayed in the ‘Accounts’ list view. If you don’t want, you can disable it or even customize it. This can be done in the **Admin >> Configurations section**.

When you click change, a dialog box with two options ‘No’ and ‘Customize’ appears. If you select ‘No’, the account details cannot be customized in the ‘Accounts’ list view. If you select ‘Customize’, a GUI appears.

You have the option to select/deselect the account details displayed in the 'Accounts' list. The Account Title is displayed by default and cannot be disabled. Click ‘**save**’ to show changes.

Do you want to display the account title shown on the web interface in multiple lines?

Securden allows you to display the account title shown on the web interface in multiple lines. If you don’t want to display, you can just disable it.

When you click change, a confirmation box will appear saying Yes and No.

If you click Yes, the account title shown on the web interface will be displayed in multiple lines and if you select No, it will be disabled.

Remote Connections

When launching remote connections using a domain account, a list of FQDN/IP addresses will be displayed to which you can connect. Do you want to show the address of the domain account in the list?

Securden have the option to show the address of the domain account in the list. When launching remote connections using a domain account, a list of FQDN/IP addresses will be displayed to which you can connect. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No.
If you select Yes, the address of the list will be shown in the list and if you want to disable it, you can select No.

When launching remote connections with specific addresses (FQDN/IP Address) using a domain account, do you want to display the list of permitted account addresses a user has access to?

Securden allows you to display the list of permitted account addresses a user has access to, When launching remote connections with specific addresses (FQDN/IP Address) using a domain account. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you select Yes, the list of permitted account addresses a user has access to will be displayed and if you want to disable it, you can select No.

When launching remote connections using a domain account, do you want to allow users to type the name of IT asset to be connected?

Securden allows users to type the name of IT asset to be connected when launching remote connections using a domain account. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you select Yes, users will be allowed to type the name of IT asset to be connected and if you want to disable it, you can select No.

Do you want to allow remote Telnet connections? When the Telnet window is opened, Securden fills the credentials (password might get printed on the command window). Telnet protocol has its inherent security limitations that have limited its usefulness in environments where the network cannot be fully trusted. The use of Telnet over the public internet should be avoided as it carries the risk of eavesdropping. Allow this only after carefully considering the security aspects.

Securden has the option to allow remote Telnet connections. If you don't want, you can disable it.

Do you want to disable any type of remote connections available in Securden?

Securden has the option to allow remote Telnet connections. If you don't want, you can disable it.

When you click change, a dialog box with two options ‘No’ and ‘Customize’ appears. If you select ‘No’, the option to disable any type of remote connections available will be denied. If you select ‘Customize’, a GUI appears.

Securden supports various protocols for launching remote connections. You may enable or disable any protocol as needed. Every connection type listed below is enabled by default, except Windows Telnet & Putty Telnet connections.

To disable a protocol, unselect it from the list below.

If you select to have Telnet connections, you need to additionally enable Telnet connections from Admin >> Customization >> Configurations >> Remote Connections. You can select up to five details to be shown in the details list.

Export Accounts

Do you want to allow your users to export their work accounts as .xlsx file?

Securden allows your users to export their work accounts as .xlsx file. If you don’t want, you can disable it or even customize it.

When you click change, a dialog box with three options ‘Allow for all’, ‘Deny for all’ and ‘Customize’ appears. If you select ‘Allow for all’, users will be allowed to export their work accounts as .xlsx file and if you select ‘Deny for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears.

You can allow a custom list of users to export their work accounts as .xlsx file. If you select 'Allow', this configuration will be applicable only to the users / groups added below. If you select 'Deny', this configuration will be applicable to all users/groups except the ones added. Click ‘**save’** to show changes.

Do you want to allow your users to export their personal accounts as .xlsx file?

Securden allows your users to export their personal accounts as .xlsx file. If you don't want, you can disable it or even customize it.

When you click change, a dialog box with three options 'Allow for all', 'Deny for all' and 'Customize' appears. If you select 'Allow for all', users will be allowed to export their personal accounts as .xlsx file and if you select 'Deny for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can allow a custom list of users to export their personal accounts as .xlsx file. If you select 'Allow', this configuration will be applicable only to the users/groups added below. If you select 'Deny', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

Do you wish to conceal the password column when users export their work accounts as .xlsx file?

Securden have the option to conceal the password column when users export their work accounts as .xlsx file. If you don't want, you can disable it or you can even customize it

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', the password column will be concealed when users export their work accounts as .xlxs file and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can conceal the password column while exporting work accounts as .xlsx file for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click ‘**save**’ to show changes.

Do you want to allow offline access for your users? If allowed, they will be able to download their data as an encrypted HTML file.

Securden have the option to allow offline access for your users. If allowed, they will be able to download their data as an encrypted HTML file. If you don’t want, you can disable it and you can even customize it.

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, your users will

be allowed offline access and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears.

You can allow offline access for a custom list of users. If you select 'Allow', this configuration will be applicable only to the users/groups added below. If you select 'Deny', this configuration will be applicable to all users/groups except the ones added. Click ‘**save’** to show changes.

Do you want to send a notification email to all approvers when a request is approved or rejected by a designated approver?

Securden have an option to send a notification email to all approvers when a request is approved or rejected by a designated approver. If you don’t want, you can disable it When you click change, a confirmation box will appear saying Yes and No.

Securden have an option to send a notification email to all approvers when a request is approved or rejected by a designated approver. If you don’t want, you can disable it When you click change, a confirmation box will appear saying Yes and No.

If you select Yes, notification email will be sent to all approvers and if you don’t want, you can select No.

Securden has the option to enable/disable the Securden Agent to be upgraded automatically. If you don’t want, you can disable it.

Personal

Do you want to allow your users to manage personal accounts?

Securden allows your users to manage personal accounts. If you don’t want, you can disable it or even customize it.

When you click change, a dialog box with three options ‘Allow for all’, ‘Deny for all’ and ‘Customize’ appears. If you select ‘Allow for all’, users will be allowed to export their personal accounts as .xlsx file and if you select ‘Deny for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears.

You can allow a custom list of users to manage personal accounts. If you select 'Allow', this configuration will be applicable only to the users / groups added below. If you select 'Deny', this configuration will be applicable to all users / groups except the ones added. Click ‘save’ to show changes.

Browser Extension

Do you want to allow automatic submission of credentials for directly logging in to websites using browser extension?

Securden allows your users to export their personal accounts as .xlsx file. If you don’t want, you can disable it or even customize it.

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, the password column will be concealed when users export their work accounts as .xlxs file and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears.

When accounts are shared with 'Open Connection' permission, do you want to allow automatic filling of credentials on websites using browser extension?

Securden allows automatic filling of credentials on websites using browser extension when accounts are shared with ‘Open Connection’ permission. If you don’t want, you can disable it or even customize it. This can be done in the **Admin >> Configurations section.**

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, automatic filling of credentials on websites using browser extension will be allowed and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears.

You can enable automatic filling of credentials on websites using browser extension when accounts are shared with 'Open Connection' permission for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click ‘**save’** to show changes.

Do you want the Securden browser extension's auto-fill icon to be present in all input fields of the web pages?

Securden allows browser extension’s auto-fill icon to be present in all input fields of the web pages. If you don’t want, you can disable it or even customize it.

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, Securden’s browser extension’s auto-fill icon will be present in all input fields of the web pages for all Users/Groups and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears.

You can enable Securden autofill icon to be filled in all input fields on websites. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click ‘**save’** to show changes.

Mobile App

Do you want to enable MFA for Securden mobile application?

Securden allows you to enable Multi Factor Authentication for Securden mobile application. You can disable it or you can also customize it for specific Users/Groups.

When you click change, a dialog box with three options ‘Enable for all’, ‘Disable for all’ and ‘Customize’ appears. If you select ‘Enable for all’, it will be enforced for all the users and if you select ‘Disable for all’, it will be denied for all the users. If you select ‘Customize’, a GUI appears

You can enable MFA for Securden mobile application for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click ‘**Save**’ to show changes.

General

Do you want to check the Active Directory port before initializing the connection with the AD? If yes, specify the time duration in seconds after which the check times out.

Securden provides an option to check the Active Directory port before initializing the connection with the AD. You can specify the time duration in seconds after which the check times out. If you don’t want, you can disable it or even customize it.

When you click change, a GUI appears. In that, you can specify the time duration (in seconds) within which a response from the Active Directory domain controller is expected. Click '**save'** to show changes.

Do you want to run password verification schedule everyday?

Securden have an option to run password verification schedule everyday. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No.

If you click Yes, the option to run password verification schedule everyday will be enabled and if you select No, it will be disabled.

Do you want to disable local authentication in Securden? In case, you choose not to allow local authentication, no local user will be able to login into Securden.

Securden have an option to disable local authentication. In case, you choose not to allow local authentication, no local user will be able to login into Securden. If you don't want, you can disable it or even customize it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, the option to disable local authentication will be enabled and if you select No, it will be disabled.

Do you want to display 'forgot password' option in Securden login GUI? In case, you choose not to allow this, no one in your organization, including the super administrator will see 'forgot password' link.

Securden allows an option to display ‘forgot password’ in Securden login GUI. In case, you choose not to allow this, no one in your organization, including the super administrator will see 'forgot password' link. If you don’t want, you can disable it or even customize it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, the option to display ‘forgot password’ in Securden login GUI will be enabled and if you select No, it will be disabled.

Do you want to customize the footer section for emails generated by Securden?

Securden allows you to customize the footer section for emails generated. If you don’t want, you can disable it or even customize it.

When you click change, a GUI appears. In that You have the option to modify the footer section in emails generated by Securden. You can customize the existing copyright text and the footer message. Click ‘**save’** to show changes.

How long should the web session be active (in minutes) when things are idle?

Securden allows you to specify the maximum time (in minutes) should the web session be kept active when things are idle. You have the option to keep the session active indefinitely too.

When you click change, a GUI named ‘Change Inactivity Timeout’ appears. In that, you can choose ‘Keep Active Indefinitely’ if you want to keep the session alive or choose ‘Specify Session Timeout’ if you want to customize the maximum time. You have the option to logout the session on closing the browser. You can select the checkbox if you want to enable it. Click ‘**save**’ in the end.

What should be the default date and time display format?

You can define the specific format in which the date and time should be displayed in the GUI. There is a list of various time and date formats available and you can choose from it.

When you click change, a GUI with a list of date and time display format appears. You can choose the desired format from the list. Click ‘**save**’ to show changes.

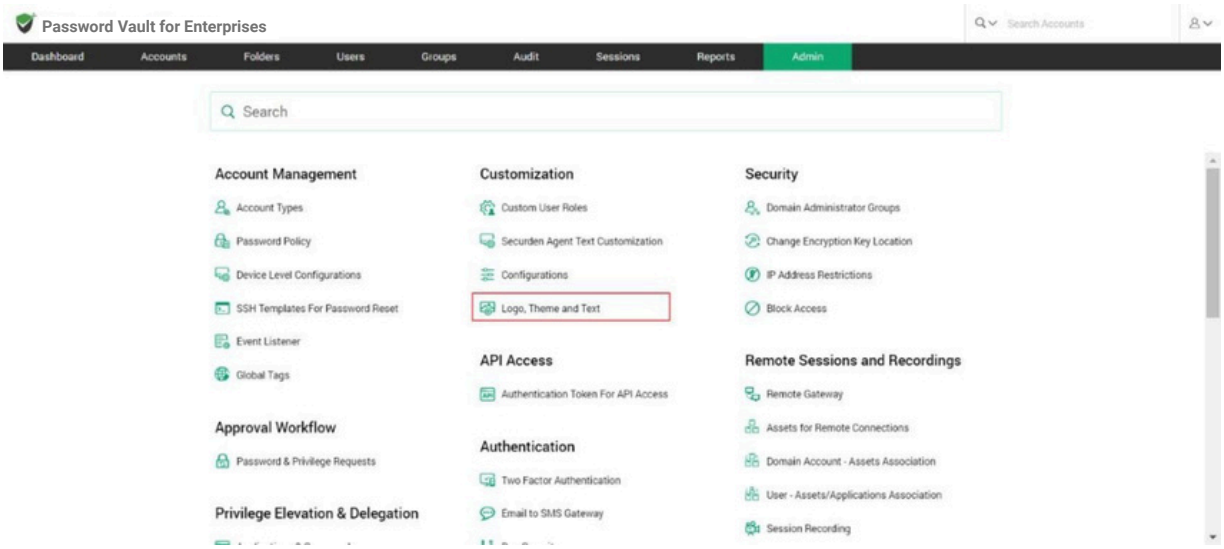
Do you want to disable the Super Administrator role?

Securden has 5 pre-defined user roles which includes user, auditor, account manager, administrator and super administrator. Super administrator is a kind of break glass account. They will not have any access control. They will be able to just view all the data stored in the application. If you don’t want a super administrator role, you can disable it.

When you click change, a dialog box comes up with two options ‘enable’ and ‘disable’. If you want a super administrator role you can click enable and if you don’t want, you can disable it.

Changing the Logo, Theme, and Text

You can replace the Securden logo that appears in the login page and throughout the GUI with your own logo. Navigate to **Admin >> Customization >> Logo, Theme and Text.**

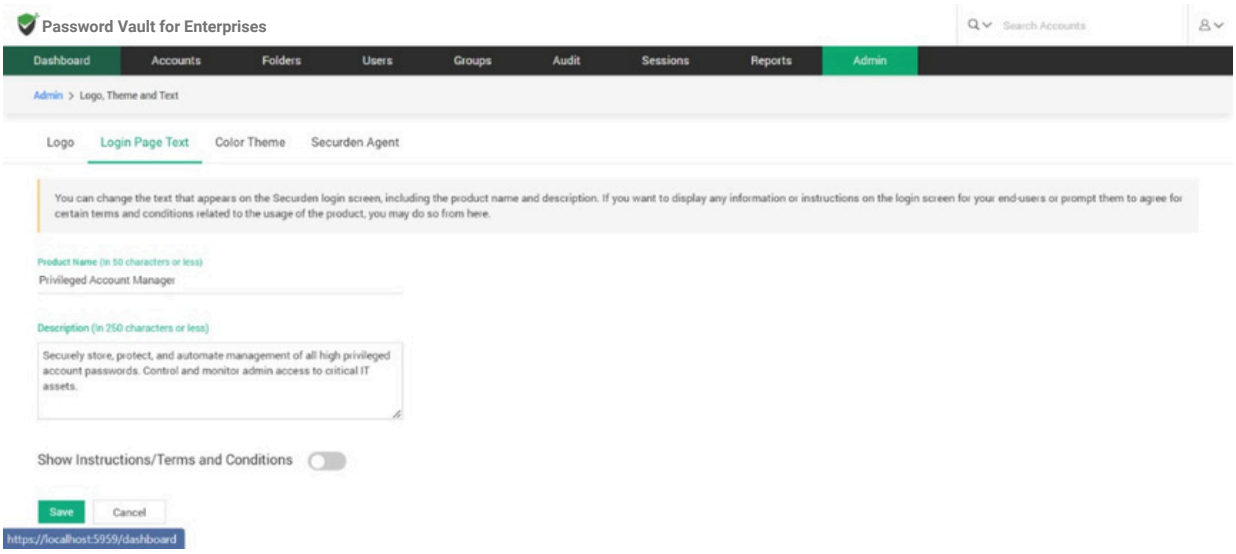


Click on Logo and you can upload your logo which will replace the Securden logo that appears throughout the GUI. The logo can be uploaded in the PNG or JPG format.

Login Page Text

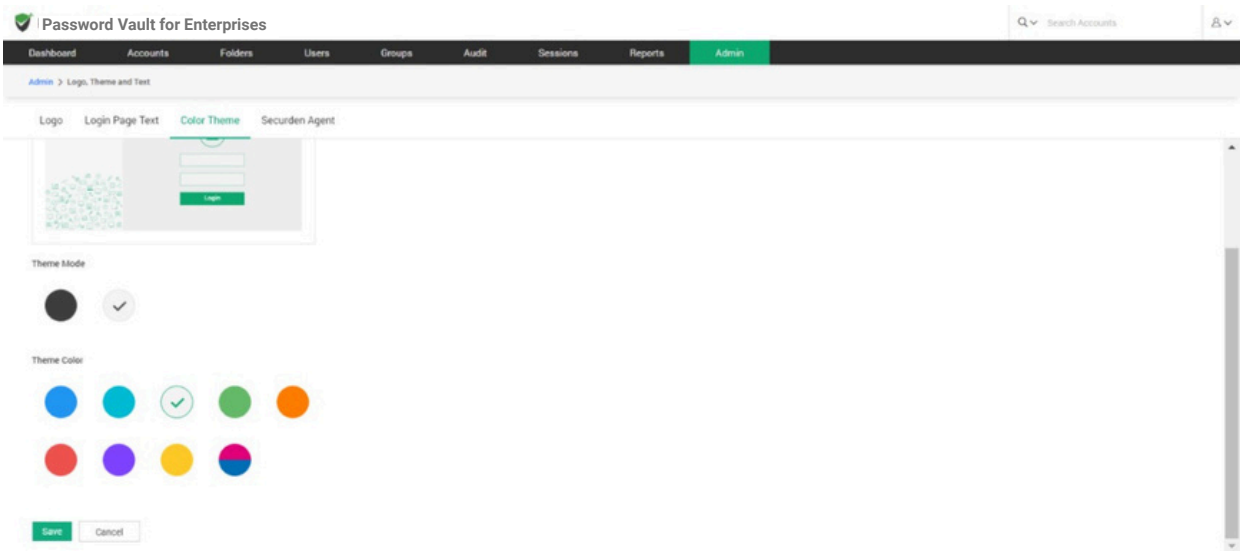
You can change the text that appears on the Securden login screen, including the product name and description. If you want to display any information or instructions on the login screen for your end-users or prompt them to agree to certain terms and conditions related to the usage of the product, you may do so here.

Click the **Admin >> Customization >> Logo, Theme and Text >> Login Page Text.**



Color Theme

By default, Securden web interface follows the green color theme. You may change it and assign a different color theme by selecting a color below. The theme you set here will be the default theme for your organization and take effect for all users. However, end users can overwrite this and can choose a theme of their choice for their own views. If any of your users have already changed their theme, the change you make here will not take effect for them.



Click on **Admin >> Customization >> Logo, Theme and Text >> Color Theme**

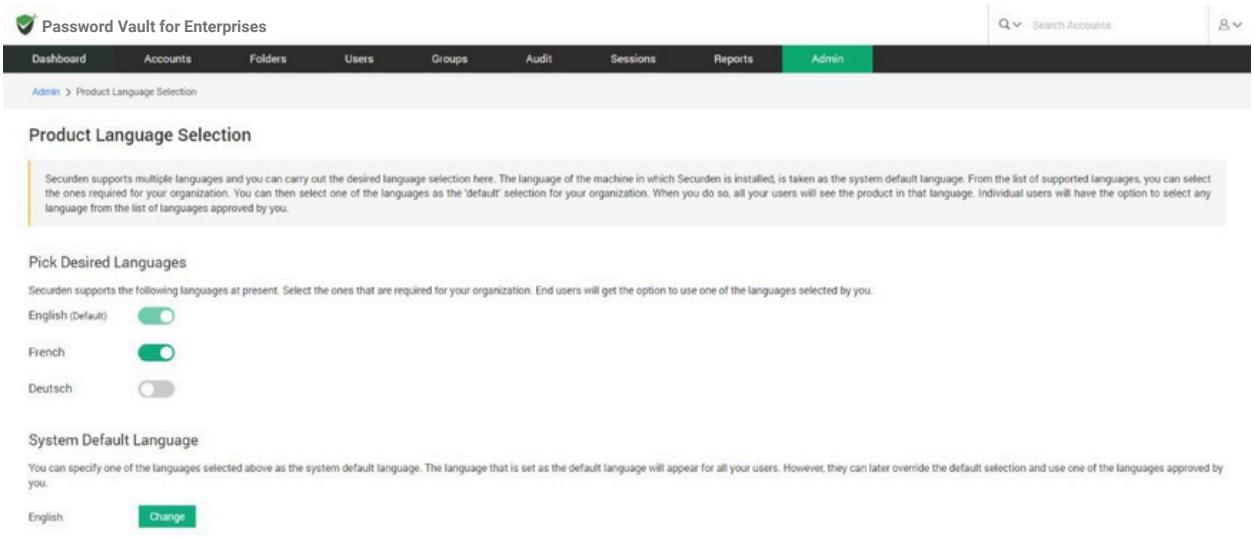
After selecting the theme mode and theme color, click on the Save button. “Product color theme changed successfully” will be displayed on top of the screen after it is saved.

Product Language Selection

Securden supports multiple languages, and you can select the desired language here. The language of the machine in which Securden is installed is taken as the system default language. From the list of supported languages, you can select the ones required for your organization. You can then select one of the languages as the 'default' selection for your organization. When you do so, all your users will see the product in that language. Individual users

will have the option to select any language from the list of languages approved by you.

Navigate to **Admin>> Customizations >> Product Language Selection**.



The screen will display the languages that are currently supported by Securden. You will have to select the language from Pick Desired Languages according to your organization's requirements. Once the desired language is enabled, a message "Language Activated Successfully" will be displayed on top of the screen. When you disable any language, it will display the message - **Language deactivated successfully**. End users will get the option to use one of the languages selected by you.

The languages available and supported by Securden at present are:

- English
- French
- Deutsch

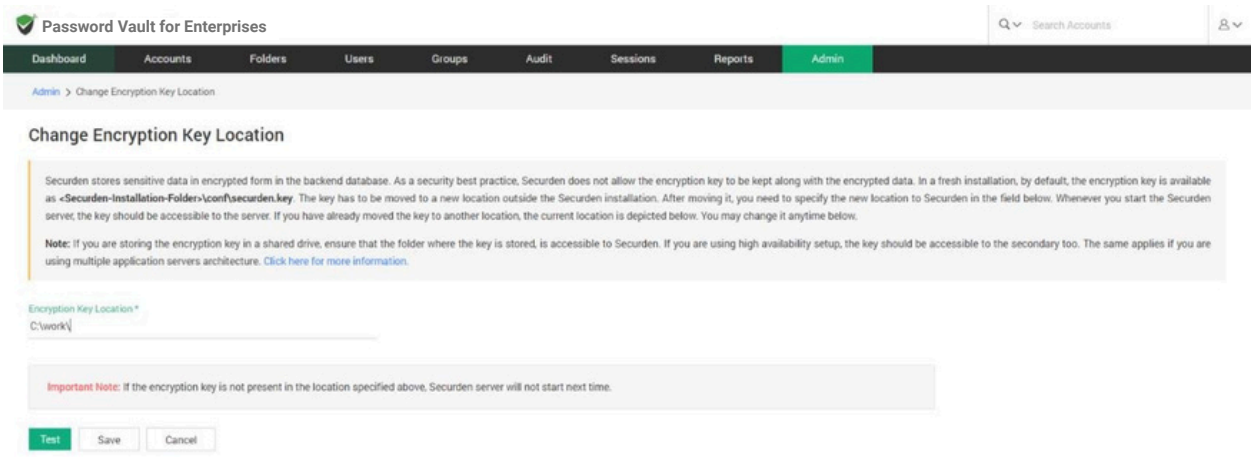
Then you can specify one of the languages selected above as the System Default Language. The language selected as default here will appear for all your users. However, they can later override the default selection and use one of the languages approved by you.

Section 11: Security Settings

You can carry out certain security settings to protect the Securden installation and control access to the interface.

Change the Encryption Key Location

Every installation of Securden is protected with a unique encryption key. By default, this encryption key is located at <securden installation folder>/conf/securden.key for evaluation purposes. Securden doesn't allow the encryption key and the encrypted data to reside in the same location to ensure security. Hence, the key has to be moved outside the Securden installation folder.



When deploying the product to production, Securden enforces moving the key out of the installation folder. The encryption key is essential to start the Securden server. If the key is not present in the new location, Securden server won't start. After moving the key to some other secure location, you need to specify the new location as explained below:

To specify the new location,

1. Navigate to **Admin >> Security >> Change Key location.**

2. Specify the location.

3. Click 'Test' to check whether the key is found in the specified location.

4. If the floating screen states "Securden encryption key not found in the path specified", check if the key is found in the new location.

5. If the encryption key was found in the specified location, A floating screen will appear containing a message stating **Encryption key found in the path specified**.

6. Click **Save**.

Note: If the server fails to start, you can view the current location of the encryption key by opening the Securden_key.location file using any text editor. This file is located at <Securden Installation folder>/conf/Securden_key.location.

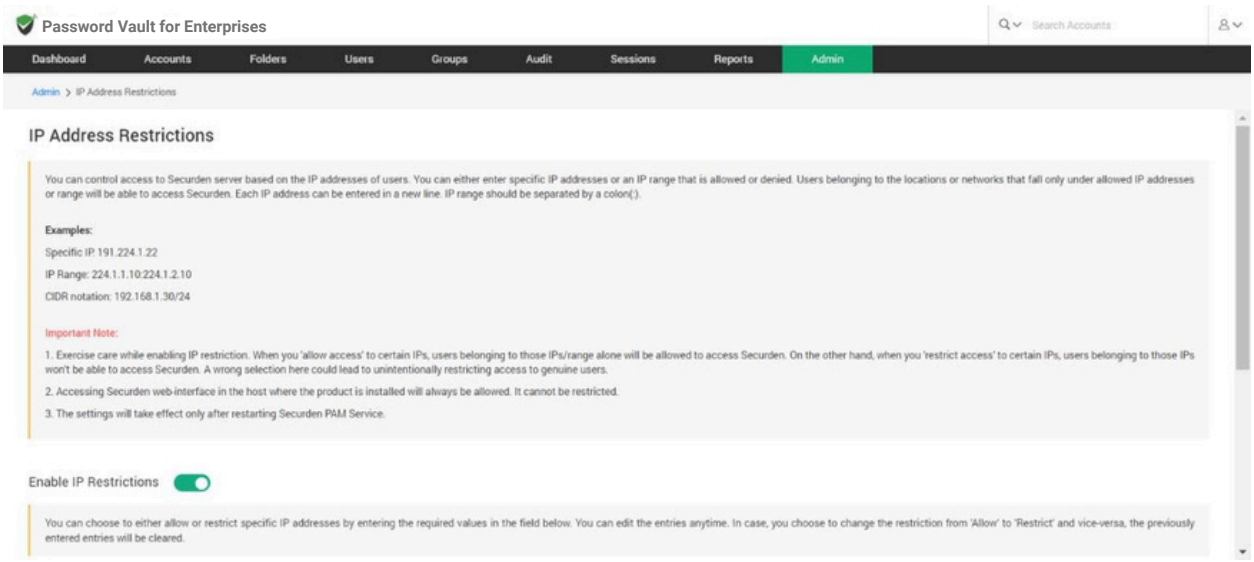
You need to have the encryption key in the location specified in this file for the Securden server to start.

IP Address Restriction

Securden gives you the option to control and restrict access to Securden Server based on the user's IP address. You can either enter specific IP addresses or an IP range that is allowed or denied. Users belonging to the locations or networks that fall only under allowed IP addresses or range will be able to access Securden.

Enable IP Restrictions

To Enable IP Restrictions, navigate to **Admin >> Security >> IP Address Restrictions >> Enable IP Restrictions** and move the toggle **Enable IP Restrictions** to green.



Here you choose either to allow access or to restrict access.

Enter one or multiple IP addresses. Each IP address can be entered in a new line. IP range should be separated by a colon (:).

Examples:

Specific IP: 191.224.1.22

IP Range: 224.1.1.10:224.1.2.10

CIDR notation: 192.168.1.30/24

Note:

• Exercise care while enabling IP restriction. When you allow access toc ertain IPs, users belonging to those IPs/ranges alone will be allowed to access Securden. On the other hand, when you restrict access to certain IPs, users belonging to those IPs won't be able to access Securden. A wrong selection here could lead to unintentionally restricting access to genuine users.

• Accessing the Securden web interface in the host where the product is installed will always be allowed. It cannot be restricted.

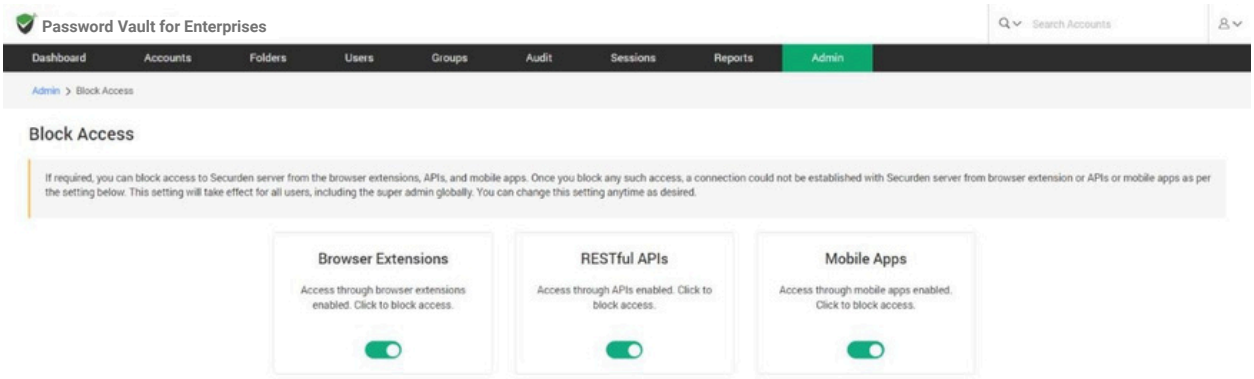
Finally, click **Save**. The settings will take effect only after restarting Securden VaultService.

Block Access through API, Extensions, Mobile Apps

Securden allows you to block and filter access to its server from extensions, API, and mobile applications. Once you block any such access, a connection

could not be established with the Securden server from browser extension or APIs or mobile apps as per the setting below. This setting will take effect for all users, including the super admin globally. You can change this setting anytime as desired.

To block access, navigate to **Admin >> Security >> Block Access**.



You can block access through browser extensions, APIs, or mobile apps by moving the green toggle to red.

You can change this setting anytime as required

Section 12: Emergency Access Settings

Configure Emergency Access

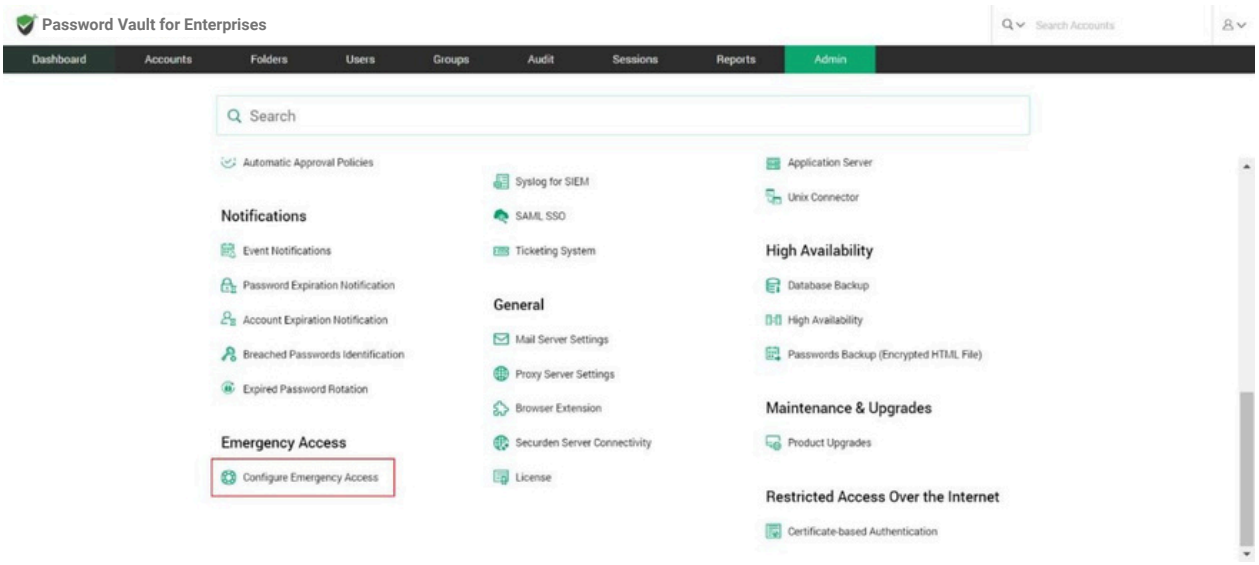
Emergency access, as the name implies, is used in highly critical and urgent situations. For instance, imagine the scenario when an administrator who has access to an IT resource is away and your team requires immediate access to the device. The emergency access feature helps in this scenario to gain access in a hassle-free manner with a well-defined workflow.

How does emergency access work?

You can enable a designated list of users as ‘Emergency Access Users’ allowing them to access all passwords (work accounts) stored in Securden, breaking the usual access controls during emergency situations. When an emergency access requirement arises, any of the designated users will first declare emergency and get access after the predefined mandatory waiting period. In the meantime, all administrators will be notified of the situation.

Configuring emergency access

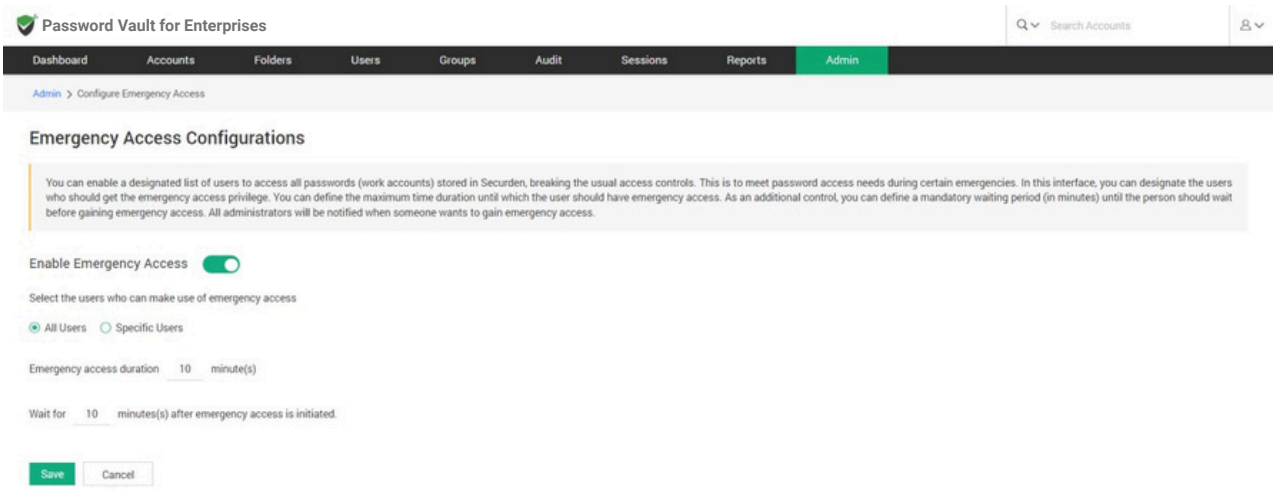
To configure emergency access, navigate to **Admin >> Emergency Access >> Configure Emergency Access**.



In the GUI that opens, 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.

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.

Move the toggle **Enable Emergency Access** to turn on emergency access. You will see two options namely, **All users** and **Specific users**. As the name itself implies, **All users** option grants the emergency access privilege to all the users. On the other hand, if you want to grant the privilege only to certain specific users or groups of users, you need to choose the option **Specific users**.



When you choose the **Specific users**, you need to select the users or groups from the list. You can define the maximum duration up to which a user can avail emergency access. Specify the duration in minutes. As a security best practice, to guard against any possible misuse of the provision, you can enforce a mandatory waiting period for anyone to gain access after **breaking the glass**. During this window, notifications will go to all administrators, who can revoke access if any suspicious motive is found. You can define the waiting time in minutes. After configuring these values, click **Save**.

The above steps complete the emergency access configuration. The configuration done by one administrator has to be approved by another administrator. The approval can be done from the same page in the GUI. When another administrator logs in, the link to approve or reject the request will be visible as shown below.

How to initiate emergency access?

When an emergency access requirement arises, the designated user(s) can initiate the access from **Admin >> Emergency Access >> Initiate**

Emergency Access. In the GUI that opens, the user has to justify why emergency access is needed. As per the emergency access configuration, the user will get access.

Disaster Recovery Settings

Database Backup

To ensure uninterrupted access to passwords even in the unlikely event of a disaster, you can take a backup of the entire database and store it in a secure location. If something goes wrong with the existing installation, you can do a quick recovery of data. Backup can be taken anytime on-demand and at periodic intervals by creating a scheduled task.

Configuring Backup

To configure database backup, navigate to **Admin >> High Availability >> Database Backup** section in the GUI. There are two options to choose from when scheduling a backup. You can choose to take a backup once whenever required or at periodic intervals. If you want to take a backup instantly, you can click on **Backup Now**. If you choose **Take Backup Once**, follow the steps below:

1. Select the date and time when you want to take backup once.
2. If needed, change the backup destination from its default location by providing the destination folder path. When the backup file is to be stored in another machine, you can specify the network path to that destination.
3. Specify the maximum number of backups to be retained in that

location. For example, if you specify this as 5, only the most recent 5 backup copies will be retained. Click **Save**

If you choose Take Backup Periodically', follow the steps below to create a scheduled task:

1. Choose the date and time of the first backup.
2. Thereafter, you can schedule backups on an hourly, daily, weekly, and monthly basis. Choose an option between 'Hours', 'Days', 'Weeks', and 'Months' from the drop-down menu. Specify the number of hours/days/weeks/months in the adjacent space.
3. If needed, change the backup destination from its default location by providing the destination folder path. When the backup file is to be stored in another machine, you can specify the network path to that destination.
4. Specify the maximum number of backups to be retained in that location. For example, if you specify this as 5, only the most recent 5 backup copies will be retained.
5. Click **Save**

Disabling the Database Backup

You can use the disable option to delete an already existing backup schedule along with its configurations.

Important Note: Every installation has a randomly generated, unique encryption key, using which sensitive data are encrypted and stored in the database. By default, the encryption key is located at <Securden-Installation-Folder>/conf/securden.key. Securden doesn't allow the encryption key and encrypted data to reside together. It has to be moved to some other location. When you start the Securden server, the key should be available in the path specified every time. Otherwise, the server won't start, and you won't be able to access the passwords.

This encryption key is needed to restore the data from the backup copy. If you don't have the encryption key, data cannot be restored. Ensure that you have a copy of the encryption key for disaster recovery.

Steps for Data Recovery

In the event of a disaster, you can restore the data and the configurations from a backup file.

Important Note: The backup data is encrypted using the same encryption key as the original. For data restoration, Securden requires access to the encryption key.

Ensure the key is available at the location specified in the current (new) installation of Securden. By default, the encryption key is located at <Securden-Installation-Folder>/conf/securden.key.

You can also identify the current location of the encryption key by navigating to **Admin >> Security >> Change encryption key location**, and hovering

the pointer over the "i" icon (or) Open the file named Securden_key.location using a text editor. This file can be found at <Securden installation folder>/conf/Securden_key.location

To Recover the backed-up data, follow the steps below

- Install Securden in a new machine without disturbing the existing installation.
- Stop the Securden server. >> Open services.msc >> Navigate to Securden Vault Service. >> Stop the service.
- Open Command Prompt by clicking on 'Run as Administrator'.
- Navigate to <Securden-Installation-Folder>/bin.

● In the cmd window, use the following command. >> RestoreDatabase.exe <enter the full path of the backup file>

Example:RestoreDatabase.exe C:\ProgramFiles\Securden\Password_Vault\exports\PostgreSQL_Backups\Securden_postgresql_ db_backup_2019-05-22-11-48-22.zip

Start Securden Vault service from services.msc. (You can safely ignore the other service named Securden Web Service, which is automatically taken care of).

Backup of Passwords as an Encrypted HTML File

As an additional backup option, super administrators can take a backup of all passwords in the form of an encrypted HTML file. These HTML files can be opened using a web browser. A passphrase has to be provided at the time of configuring the schedule. This passphrase will be used as the encryption key. Whenever the file has to be opened, the passphrase has to be supplied. The passphrase is not stored anywhere.

The encrypted HTML file contains work accounts only. The personal accounts of the users cannot be backed up. As mentioned above, only super administrators can create the schedule. Administrators can view the schedules created by a super administrator.

To configure backup of passwords as an encrypted HTML file, navigate to **Admin >> High Availability >> Password Backup** (Encrypted HTML file). You will see options to configure backup once or periodically. You can also specify the location where the encrypted HTML file should be stored and in the case of periodic backup, how many copies to be retained. If you specify 5, the most recent five backfiles will be retained.

Section 13: High Availability

[High Availability configuration steps are also available as separate guides for the default PostgreSQL as the backend database and optional MS SQL server as the backend separately. You may refer to them if needed.]

Configure High Availability

Securden comes with High availability architecture to ensure uninterrupted and a reliable supply of credentials. Configuring High Availability (with PostgreSQL database as the backend) To configure high availability in Securden Password Vault, 2 or more servers have to be deployed.

1. Primary server with bundled PostgreSQL database.
2. One secondary standby server with bundled PostgreSQL database.
3. One more application server without a database (optional).

Securden uses an active-active approach to high availability support. A primary server and a secondary server will be active at the same time and will have their own databases. In the event of a primary server going down, users can connect to the secondary standby server. Additionally, any number of application servers can be deployed for load distribution. Two types of secondary servers can be deployed and both have different use cases. You may choose one of the options below:

Case 1: Automatic failover with active standby. When the secondary server is deployed as a standby server, the database will be replicated and periodically synchronized with the primary server database. You will be able to enable automatic failover only when one of the secondary servers deployed is of this type. Only one such server can be deployed and it has to be deployed in the same subnet as the primary server for the automatic failover to work.

Case 2: Load distribution using application servers without database. You can also deploy a secondary server as an application server without a database. The secondary server will only have the securden application installed and not a database. Since there is no separate database other than the one in the primary server, automatic failover will not be possible. This type of secondary server is useful when you need to deploy more than one secondary server. It is mainly used for load distribution by ensuring no single server bears too much demand and reduces application response time for users.

Notes

1. For automatic failover to work, the database port (5858) of the standby server must be accessible from the primary application server. Also, ensure that the standby server is in the same subnet as that of the primary server.

2. The primary and secondary servers must be running the same version of Securden. Navigate to User Details (User icon at the top right corner) >> About >> Version to check the current product version. Contact Securden Support if you need any assistance.

Pre-requisites: A primary server with Vault up and running and using the bundled PostgreSQL database. Refer to our installation guide to install the application.

Summary of Steps

Step 1: Setting up a secondary server

Step 2: Configuring High Availability in the primary server.

Step 3: Downloading and Transferring the high availability package.

Step 4: Configuring the Secondary server.

Step 5: Verifying the high availability setup

Step 1: Setting up a Secondary Server

1. Identify a machine that would act as a secondary server. Consider the current Securden Password Vault installation as the primary server.

2. Install Securden Password Vault on the chosen machine. Refer to our installation guide if you need help with the installation process.

Note: Make sure both the machines are running the same version of Securden Password Vault.

Navigate to User Details (On the top right corner) >> About >> Versionto check for the current product version. Contact Securden Support for any Assistance.

Step 2: Configuring HA in the primary server

1. Navigate to Admin>> High Availability in the GUI of Securden Password Vault in the primary server.

2. Click the ‘Configure Secondary Application Server’ button and enter the following details regarding the secondary server.

Server Identifier - Provide a name that helps identify the secondary application server.

Address - hostname/ IP address of the machine where the secondary server instance has been installed.

Secondary Type - Two types of secondary servers can be deployed:
Application server without database and Standby Server. Select **Standby** and click **Save**.

STEP 3: Downloading and deploying the high availability package

1. Once the details of the secondary server have been saved, a pop-up with the title ‘Download and Deploy the High Availability Package’ will appear in which you will have an option to download the package as a zip file.

You can also download the package from the main High Availability GUI too. Navigate to **Admin >> High Availability >> High Availability**. In this GUI you will have the download option right next to the secondary server in the server list.

2. Transfer the downloaded zip file to the secondary server.

STEP 4: Configuring the secondary server

1. Stop the server if it is running. Open windows service manager (run services.msc) and stop Securden Vault Service.

2. Put the High availability package under the “<Securden Installation folder(Secondary)>/bin” directory.

3. Open Command Prompt with administrator privileges and navigate to the “< Securden Installation folder(Secondary)>/bin” directory. Then execute the following command: ApplyHAPackage.exe-<Secondary server Identifier>.zip

4. Securden secondary server shares the same encryption key as the primary server. Ensure the location of securden.key as mentioned in “<Securdensecondary installation folder>/conf/securden_key.location” is accessible from the secondary server. (You can open securden_key.location with any text editor)

5. Start the service again on the secondary server. To start the service, open Windows service manager (run services.msc) and start Securden Vault service. Securden High availability setup is now ready.

STEP 5: Verifying High availability

1. Navigate to admin>>High availability in the GUI of the primary server.

2. Check the status column for the secondary server. If the status shows “Running”, It means high availability is available working properly.

Deploying additional secondary application servers without DB (Optional)

You can deploy any number of secondary application servers without database. You need to deploy additional servers only if you need to distribute the load between multiple servers. To deploy additional secondary application servers without database, follow Step 1 through Step 5 again and except for “Standby” as secondary type in Step 2, select “App server without DB”

Troubleshooting Tip

Status column for the secondary shows “Data sync in progress” for a long time or **Data replication to standby stopped.**

Solution

This issue can occur when the database port (5858) of the primary server is not accessible from the secondary standby server or vice-versa. Run the following Telnet commands to verify these connections:

In secondary server: Telnet <primary server address> 5858
In primary server: Telnet <secondary server address> 5858

If these two connections are not working, you should be able to resolve it by creating an inbound firewall rule to allow access to the database port in both primary and secondary standby servers.

To add an inbound rule,

1. Open “Windows Defender Firewall with Advanced security”

2. Go to Inbound Rules and select New Rule. Add the following rule.

3. Rule Type: Port

4. Protocols and Port: TCP, 5858

5. Action: Allow the connection

6. Profile: Domain, Private, Public

7. Name(Example): TCP5858

8. Click Finish

Configuring High availability with MS SQL Server as the Backend Database

To configure High availability in Securden Password Vault you will need two or more application servers and a database server with MS SQL server installed. Securden enables the configuration of multiple application servers for high availability. You can configure any number of application servers as a measure to ensure high availability. In the event of the primary server going down, Users can connect to a secondary server.

To provide high availability for the Database, you need to set up your MS SQL server database with SQL clustering or AlwaysOn High availability groups.

Prerequisites: A primary server with Securden Password Vault and MS SQL database should be installed and kept running. Refer to our Installation guide to install the application. You can refer to the **Optional: Change Backend database to MS SQL server** section in the document to set up an MS SQL Server as the backend database.

Summary of Steps

Step 1 Setting up a secondary server

Step 2 Configuring High Availability in the primary server.

Step 3 Downloading and Transferring the high availability package.

Step 4 Configuring the Secondary server.

Step 5 Verifying the high availability setup

STEP 1: Setting up a Secondary Server

1. Identify a machine that would act as a secondary server. Consider the current Securden Vault installation as the primary server. 2. Install Securden Password Vault on the chosen machine. Refer to the installation guide if you need help with the installation process.

Note: Make sure both the machines are running the same version of Securden Vault. Navigate to User Details (On the top right corner) >> About >> Version to check for the current product version. Contact Securden Support for any assistance.

STEP 2: Configuring HA in the Primary Server

1. Navigate to Admin>> High Availability in the GUI of Securden Password Vault in the primary server.

2. Click the ‘Configure Secondary Application Server’ button and enter the following details regarding the secondary server.

a. Server Identifier - Provide a name that helps identify the secondary application server.

b. Address - hostname/ IP address of the machine where the secondary server instance has been installed.

STEP 3: Downloading and Transferring the Download Package

1. Once the details of the secondary server have been saved, a pop-up with the title **Download and Deploy the High Availability Package** will appear in which you will have an option to download the package as a zip file.

You can also download the package from the main High Availability GUI too. Navigate to Admin >> High Availability >> High availability. In this GUI you will have the download option right next to the secondary server in the server list.

2. Transfer the downloaded zip file to the secondary server.

STEP 4: Configuring the secondary server

1. Stop the server if it is running. Open windows service manager (run services.msc) and stop Securden Vault Service.
2. Put the High availability package under the “<Securden Installation folder(Secondary)>/bin” directory.
3. Open Command Prompt with administrator privileges and navigate to the “< Securden Installation folder(Secondary)>/bin” directory. Then execute the following command: ApplyHAPackage.exe-<Secondary server Identifier>.zip
4. Securden secondary server shares the same encryption key as the primary server. Ensure the location of securden.key as mentioned in “<Securden secondary installation folder>/conf/securden_key.location” is accessible from the secondary server. (You can open securden_key.location with any text editor)

5. Start the service again on the secondary server. To start the service, open Windows service manager (run services.msc) and start Securden Vaultservice. Securden High availability setup is now ready.

STEP 5: Verifying High availability

1. Navigate to admin >> High availability in the GUI of the primary server.

2. Check the status column for the secondary server. If the status shows “Running”, It means high availability is available working properly.

Troubleshooting Tips

Issue: The secondary server fails to start after startup.

Solution 1:

Make sure both the machines are running the same version of Securden Password Vault. Navigate to User Details (On the top right corner) >> About >> Version to check for the current product version. Contact Securden Support for any Assistance.

Solution 2:

Verify the location of the encryption key in the secondary server. Whenever Securden is run, the key should be accessible to the server. Otherwise, the server won’t start. Securden secondary server shares the same encryption key as the primary server. Ensure the location of securden.key as mentioned in “<Securden secondary installation folder>/conf/securden_key.location” is accessible from the secondary server. (You can open securden_key.location with any text editor)

Solution 3:

Database port (1433) of MS SQL and web server port (5959) should be accessible from the secondary server. Run the following telnet commands in your secondary server to verify the connections

Telnet <database server address> 1433

Telnet <primary server address> 5959

If any of the ports are inaccessible, you can resolve it by creating an inbound firewall rule for that particular port in the primary server or the database server.

To add an inbound rule,

1. Open “Windows Defender Firewall with Advanced security”
2. Go to Inbound Rules and select New Rule. Add the following rule.
3. Rule Type: Port
4. Protocols and Port: TCP,<Port Number>
5. Action: Allow the connection
6. Profile: Domain, Private, Public
7. Name(Example): TCP5959
8. Click **Finish**

Section 14: Reports

Securden Password Vault provides comprehensive reports for detailed insights on password management and user activities. The easy-to-understand graphs and tables display activity status and summaries related to password management.

Click the **Reports** tab and select your preferred report to proceed. The reports are broadly classified into four categories namely:

1. Standard Reports
2. Concise Reports
3. Password Security Analysis
4. Exported Reports

Standard Reports

Insights related to accounts stored

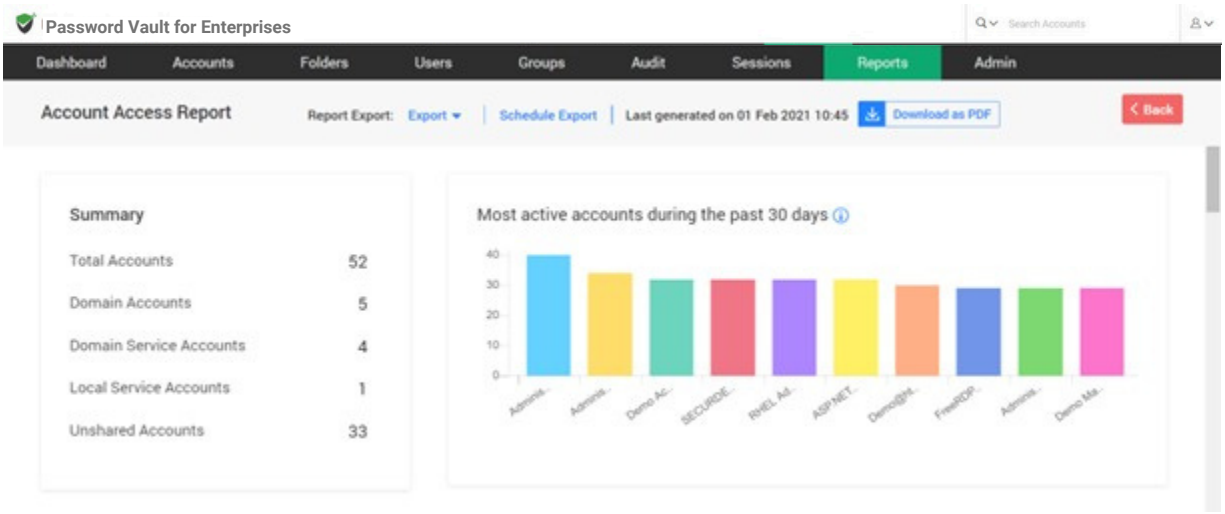
Account Access Report

To access this report, navigate to **Reports >> Standard Reports >> Account Access**. The account access report shows '**who**' are all linked to a

particular account along with '**how**' many of them share that account. The various access entitlements given to the shared users are also displayed.

In the Summary, the number of accounts are displayed categorically and on the other side the bar-graph further highlights the most active accounts during a month. The data shown in the graph includes password retrievals, remote connections launched and password auto-fills on websites.

When you click on any bar on the graph, it specifies the account address, account title and their level of usage.



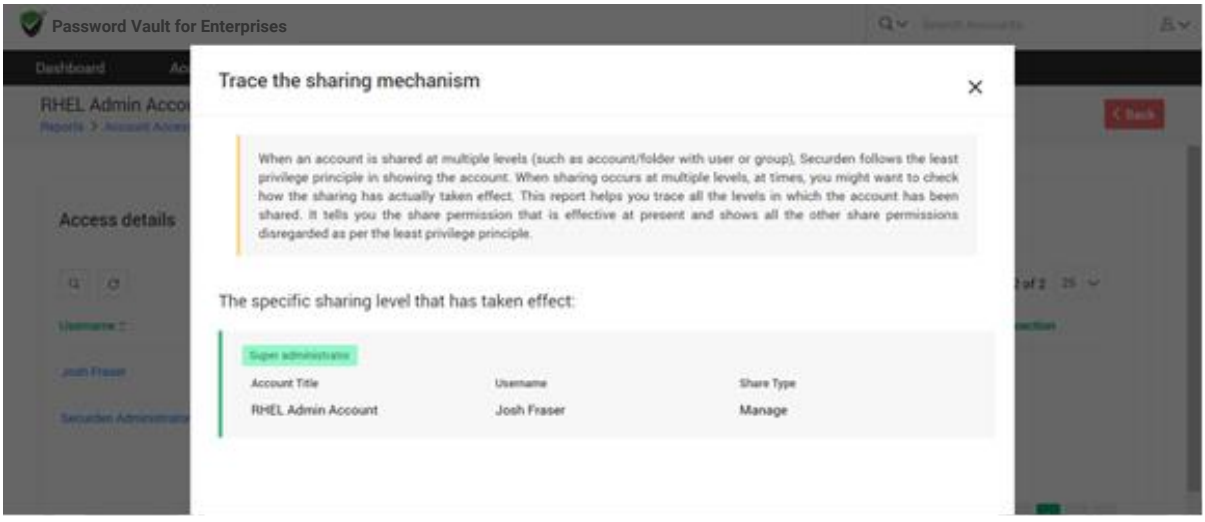
Trace accounts/folders shared with users or groups

From the Access Snapshot, you get the list of accounts present in the product. Once you click on a particular account, you get the details of users who have access for that account. When an account is shared at multiple levels (such as

account / folder with user or group), Securden follows the least privilege principle in showing the account.

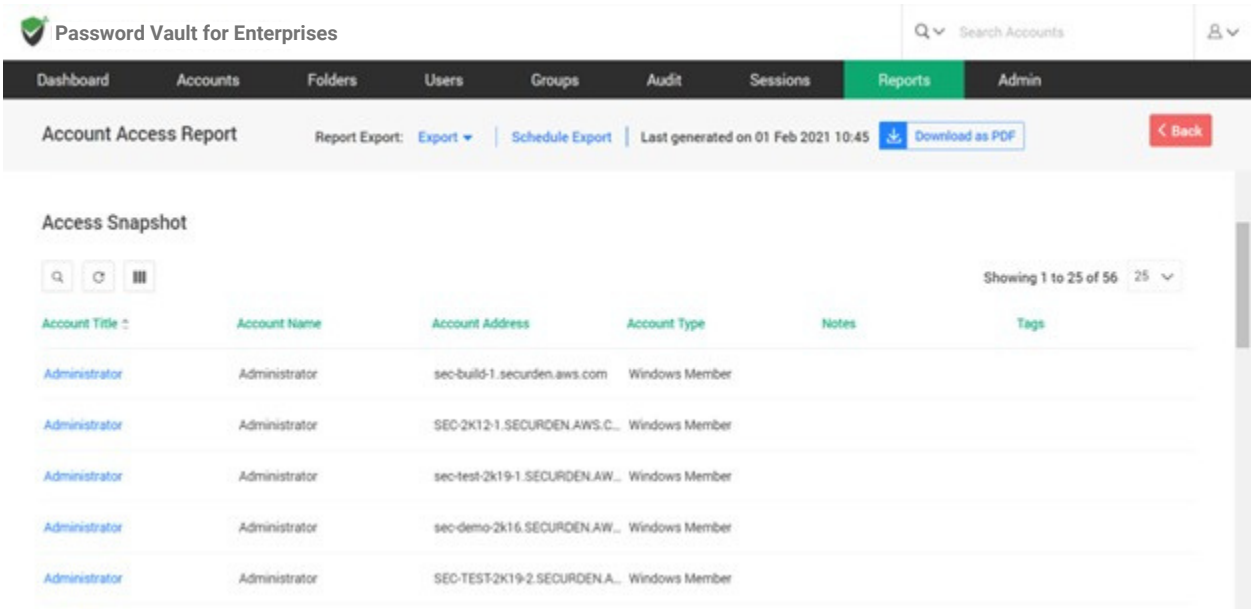
When sharing occurs at multiple levels, at times, you might want to check how the sharing has actually taken effect - how a user is getting access to an account. Account Access Report helps you trace all the levels in which the account has been shared. It tells you the share permission that is effective at present and shows all the other share permissions disregarded as per the least privilege principle.

You may use **Reports >> Account Access Report** for this purpose. Based on this finding, you would be able to take corrective action in case of any deviations.



Access Snapshot

When you click on the **Account title**, the page navigates to the **Access details** screen. The access details screen shows the modes of privileges assigned to the user; **Manage, Modify, View and Open Connection**.

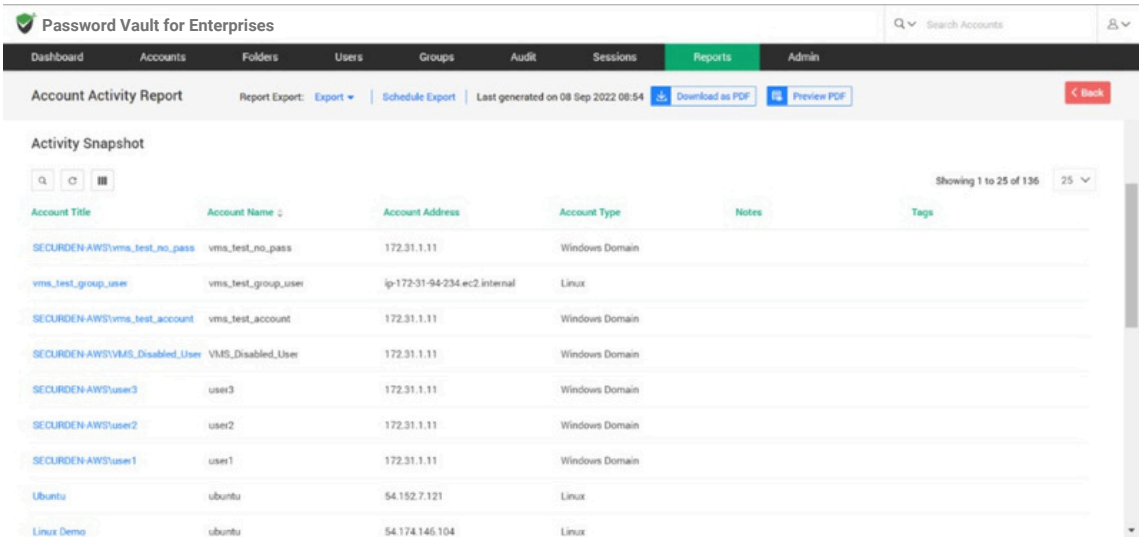


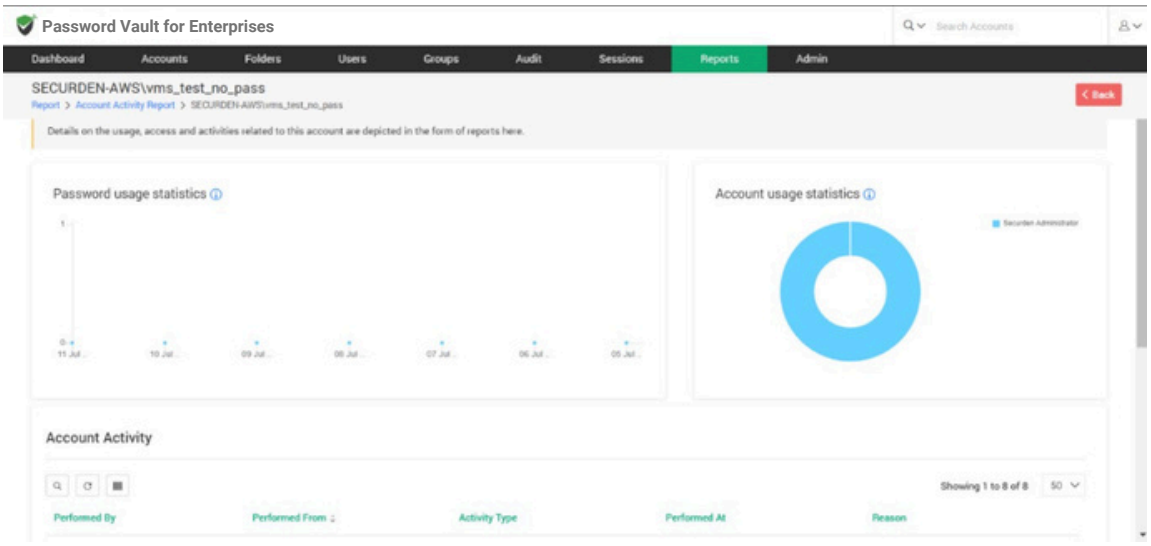
Account Activity Report

To access this report, navigate to **Reports >> Standard Reports >> Account Activity**. The report indicates about the activities performed on any particular account. The screen displays a graph that shows account access during the past week and a piechart that specifies the type distribution. The type distribution throws light upon the number of activities performed on the account.

The Activity Snapshot, through the search filter, enables you to view the string of activities performed on the accounts in a brief manner.

Once you click on an account, you will get a detailed report on the usage, access, and activities related to that account. The screen shows Password usage statistics and Account usage statistics from which you can see details about password retrievals, remote connections launched, and password auto- fills on websites. Account Activity displays the details of users who have carried out activities on the account, along with the reasons involved.





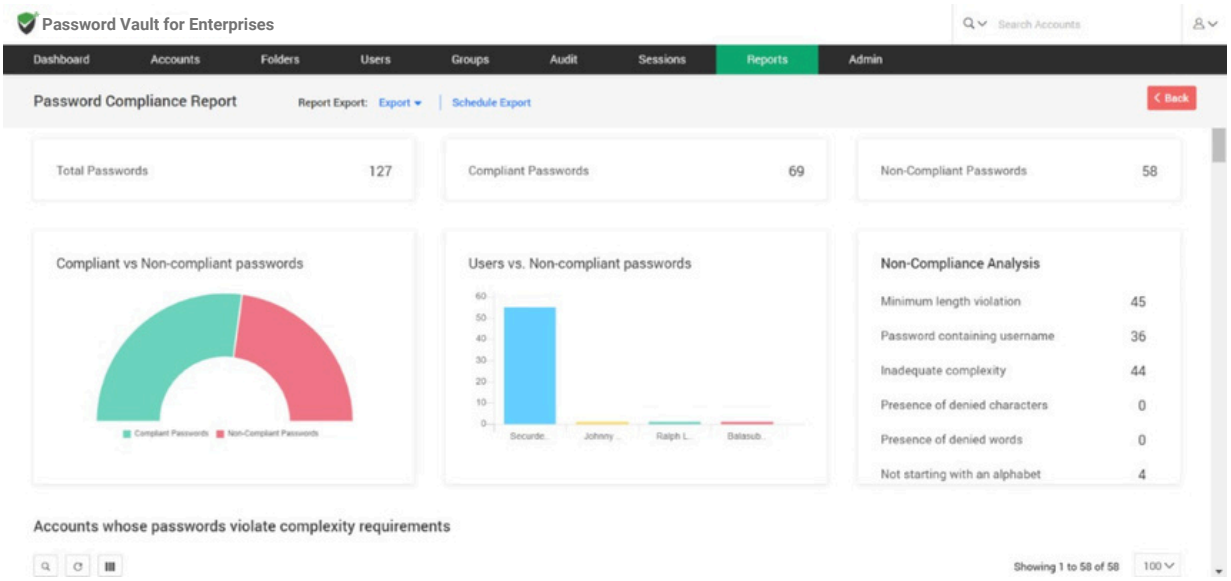
Password Compliance Report

To access this report, navigate to **Reports >> Standard Reports >> Password Compliance**.

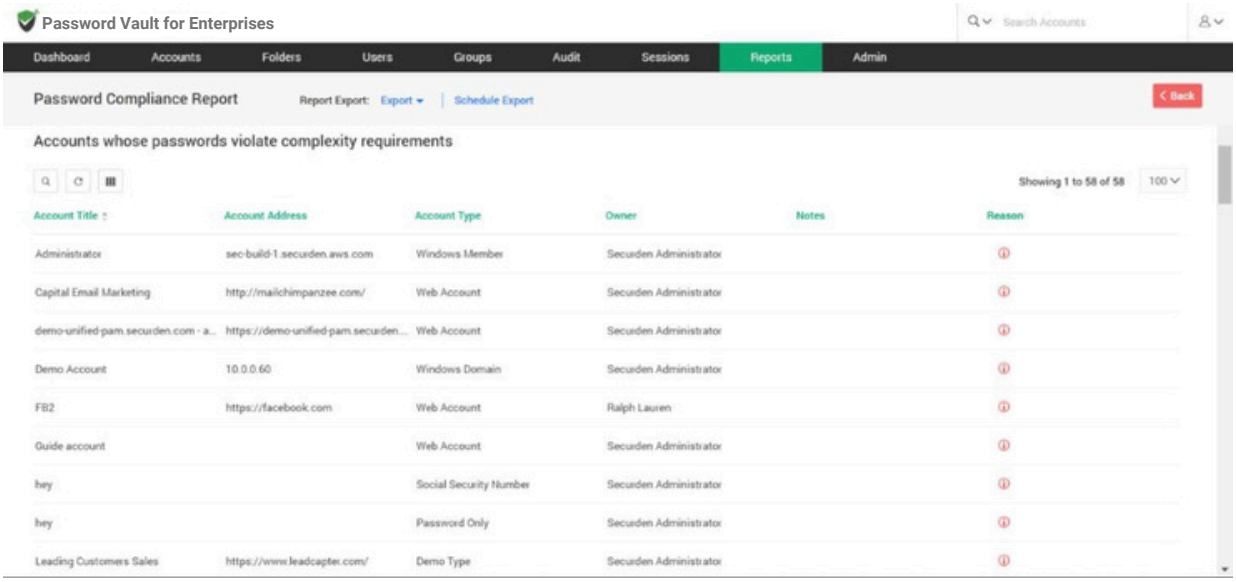
The passwords that do not comply with the IT policy of the organization are reported. Securden aids in checking the passwords of the account with the respective password policies and represents the compliance status in the report. Accounts which are excluded from any policy are not included in the report.

The report showcases the summary which includes the number of passwords in the three categories namely, **Total Passwords, Compliant Passwords, and Non-Compliant Passwords.**

The bar graphs and pie charts show us the comparison between Compliant and Non-compliant passwords, Users and Non-compliant passwords respectively. The Non-compliance analysis further lists the policies which are deviated in the password generated. The search filter enables users to locate the accounts whose passwords violated the complexity requirements. The complexity requirements that were not satisfied by the account are displayed in the reason column.

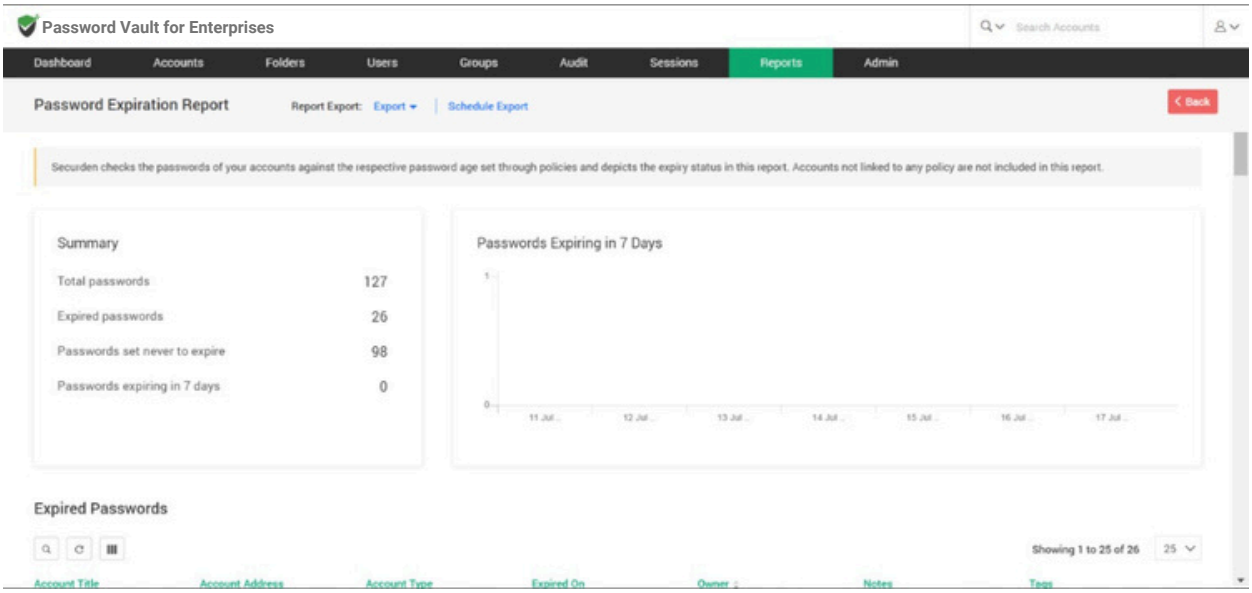


The expiration dates can be noted for the accounts from the Compliant passwords table.



Password Expiry Report

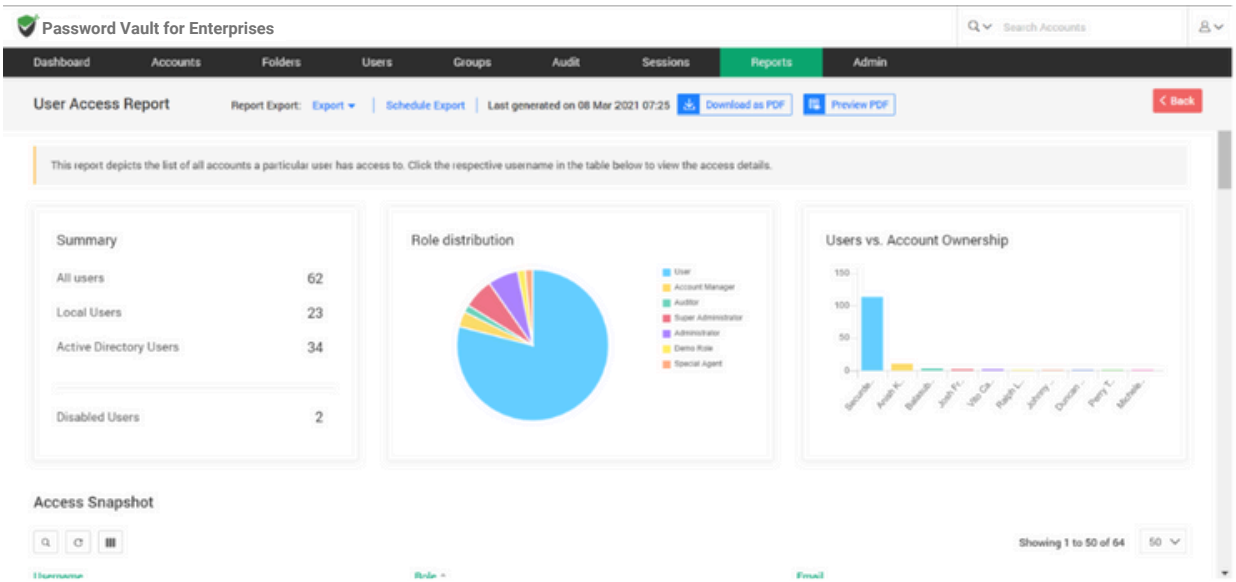
To access this report, navigate to **Reports >> Standard Reports >> Password Expiry.** Securden checks the passwords of your accounts against the respective password age set through policies and depicts the expiry status in this report. Accounts not linked to any policy are not included in this report. The graph in the GUI gives the update on passwords expiring in seven days. The three sets of tables, **Expired Passwords, Passwords that will expire in seven days, Passwords set never to expire** give information about account details along with expiration dates and notes if any.

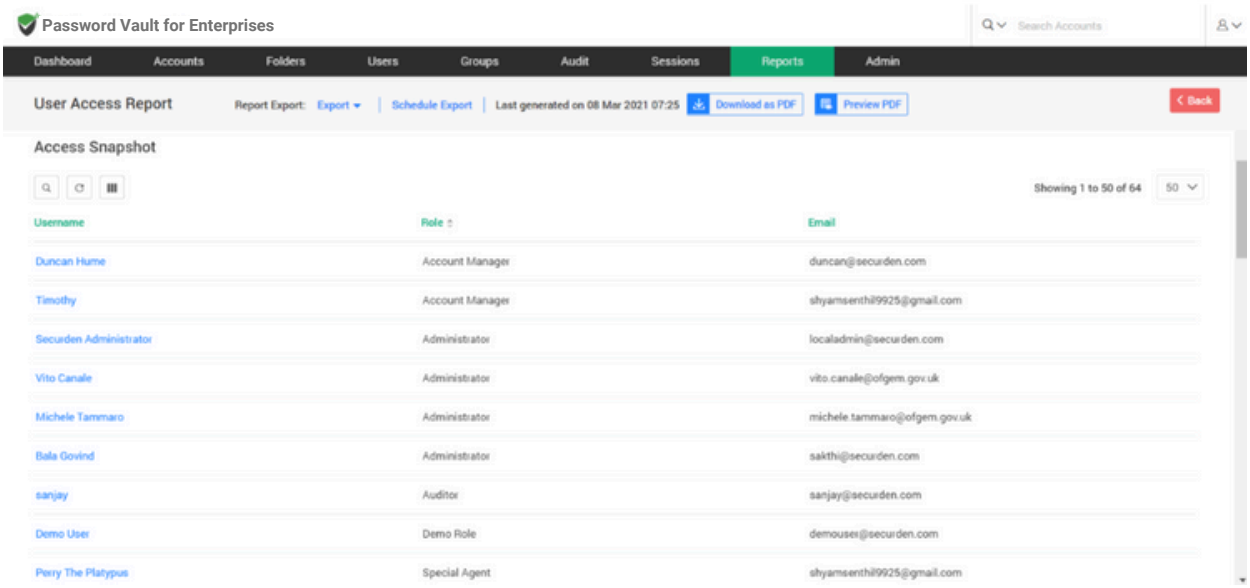


Analysis of user access and activities in Securden

User Access Report

To access this report, navigate to **Reports >> Standard Reports >> User Access**. The '**User Access Report**' provides you organization-wide information on the list of access entitlements for a specific user. You can select any user and view the information. The user access report is the inverse version of Account Access reports.

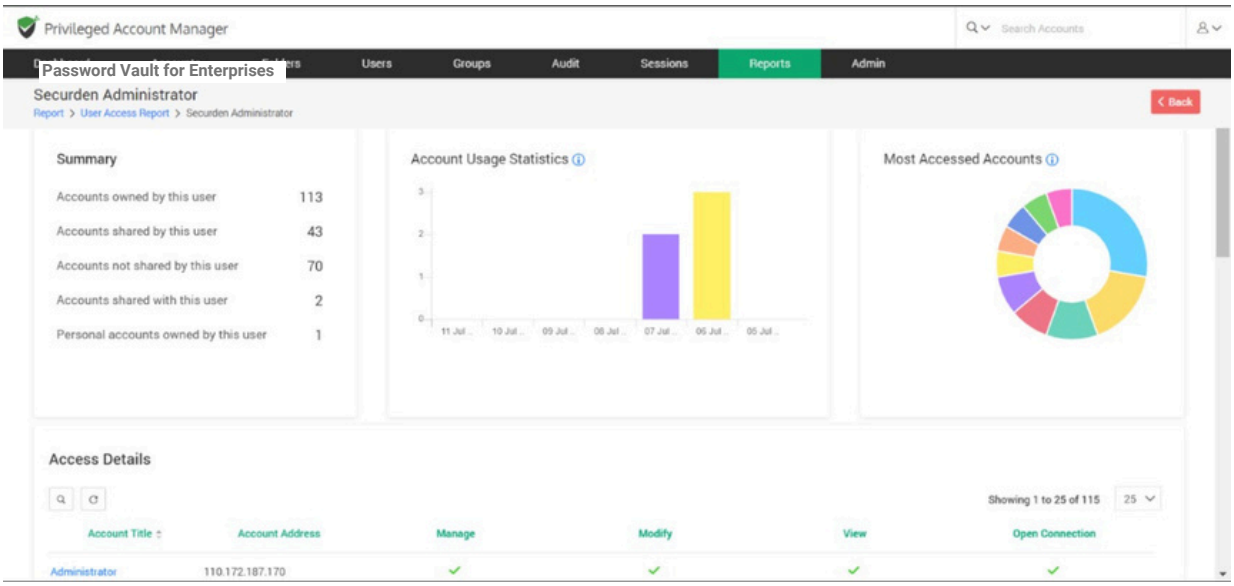




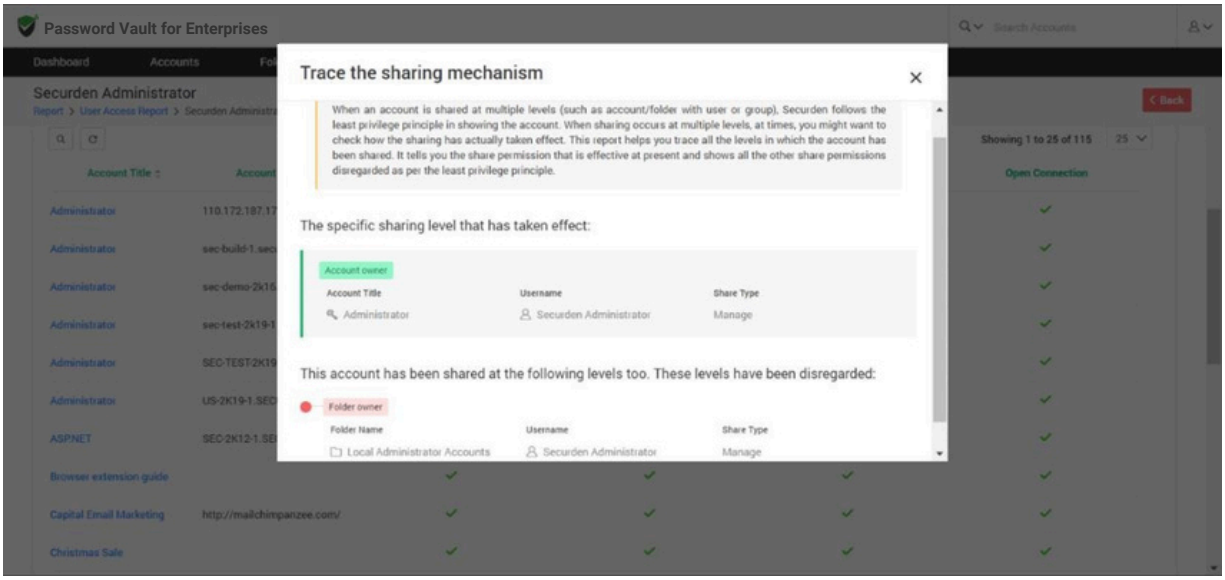
How is the user getting access to an account?

When an account is shared at multiple levels (such as account/folder with user or group), Securden follows the least privilege principle in showing the account. When sharing occurs at multiple levels, at times, you might want to check how the sharing has actually taken effect - how a user is getting access to an account.

You may use **Reports >> User Access Report** for this purpose. Under the **Access Snapshot**, you get the details of users along with the accounts they have access to. Once you click on a username, you will be directed to a page that shows account usage statistics, and access details of that user. If you are taking a User Access Report, click the name of the user (listed under Access Snapshot) who has access to an account you want to verify. Then click the required account name under Access Details

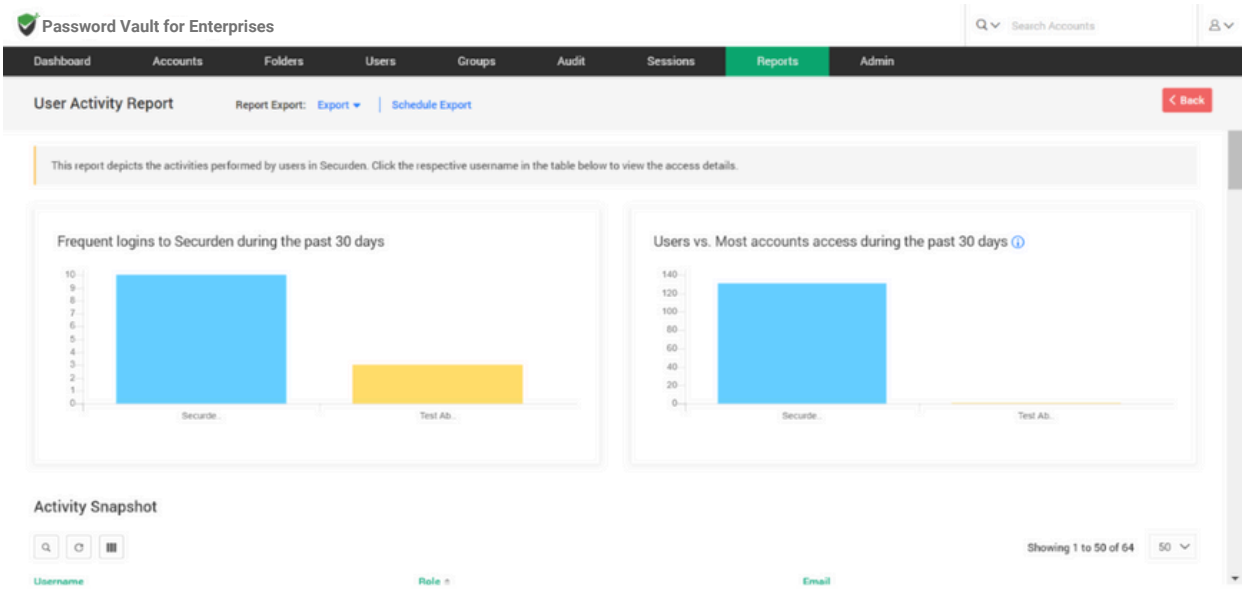


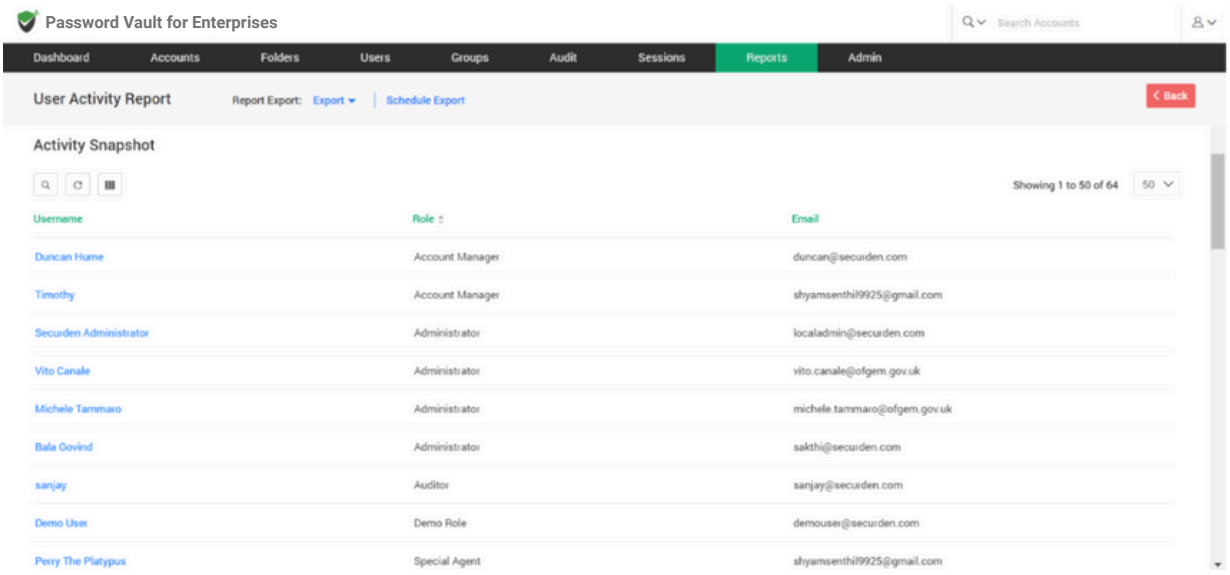
You will see a pop-up that shows **Trace the sharing mechanism**. It shows details regarding the account's access. Based on this finding, you would be able to take corrective action in case of any discrepancy.



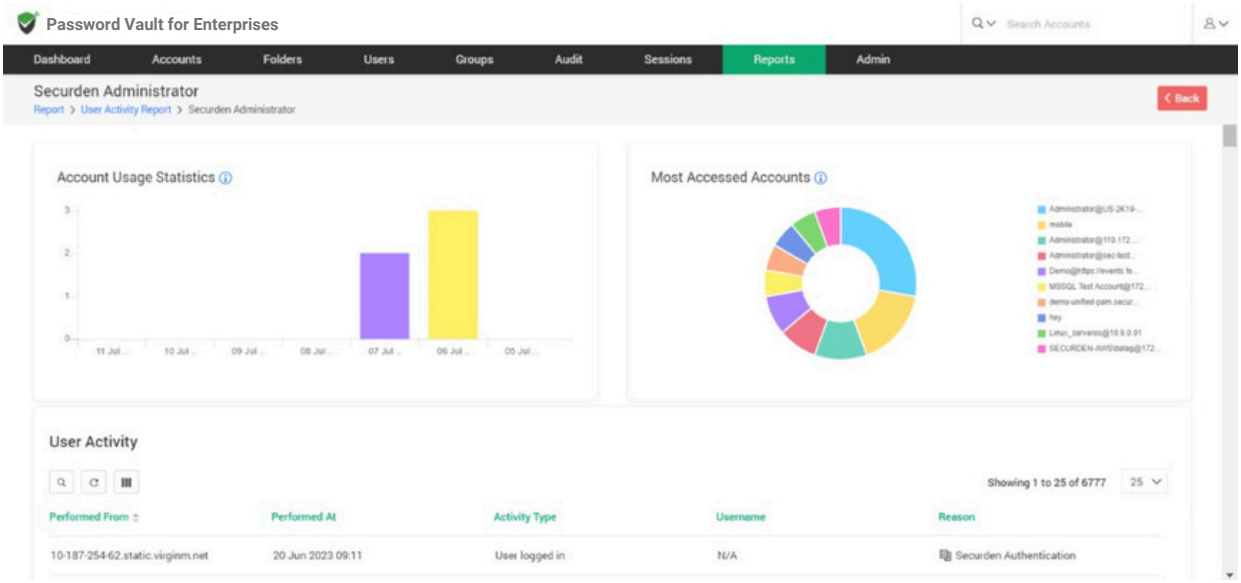
User Activities Report

To access this report, navigate to **Reports >> Standard Reports >> User Activity**. The User Activity Report depicts the activities performed by users in Securden. Click the respective username in the activity snapshot table to view the access details. The two bar graphs in the GUI display the frequent logins and usage of accounts during a 30-day time period. The **Activity Snapshot** further gives us more details about the user, their role along with their email id.



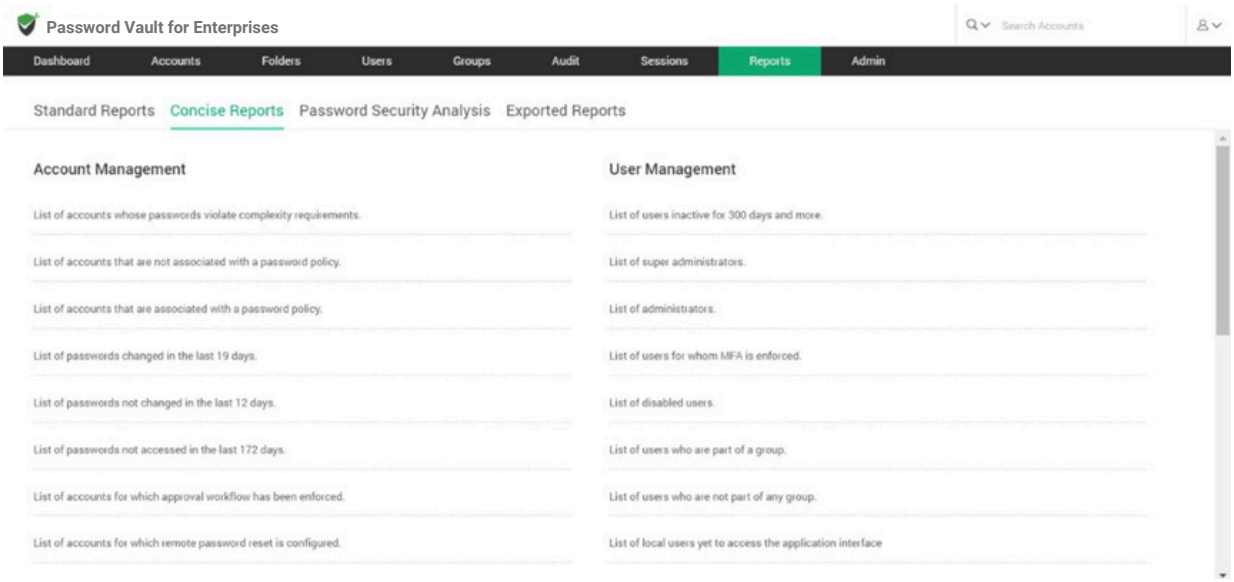


To get a user activity report, click on a username present under Activity Snapshot, and then you will be directed to a page that displays account usage statistics, user activity, account activity, groups that the user belongs to, directly shared folders, and group shared folders to that particular user.



Concise Reports

Concise Reports provide you ‘to the point’ information on specific topics. For example, if you want to know the list of passwords that were changed during the past X number of days, the concise reports will get you the details quickly.



Concise reports consists of different categories:

Account Management

The account management section deals with the list of accounts and password related matters. This includes violation of password complexity requirements, password policies and expiry duration etc.,

User Management

The user management section deals with the list of many user activities. This includes inactive users, super admins, disabled users, users part of group and those who are not part of any groups.

My Accounts

This section deals with the list of accounts:

1. Owned by you
2. Shared by you
3. Shared with you

Folder Management The folder management section deals with a list of folders owned, shared by you, not shared with anyone and also folders for which approval workflow has been enforced.

My Folders

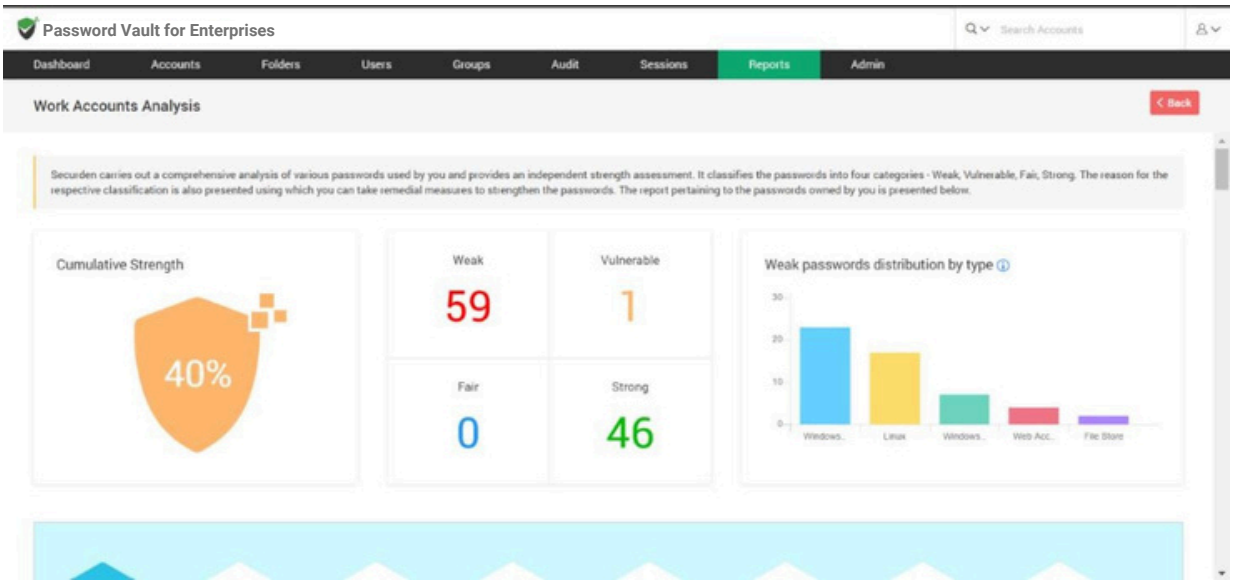
This section deals with a list of folders:

1. Owned by you
2. Shared by you
3. Shared with you

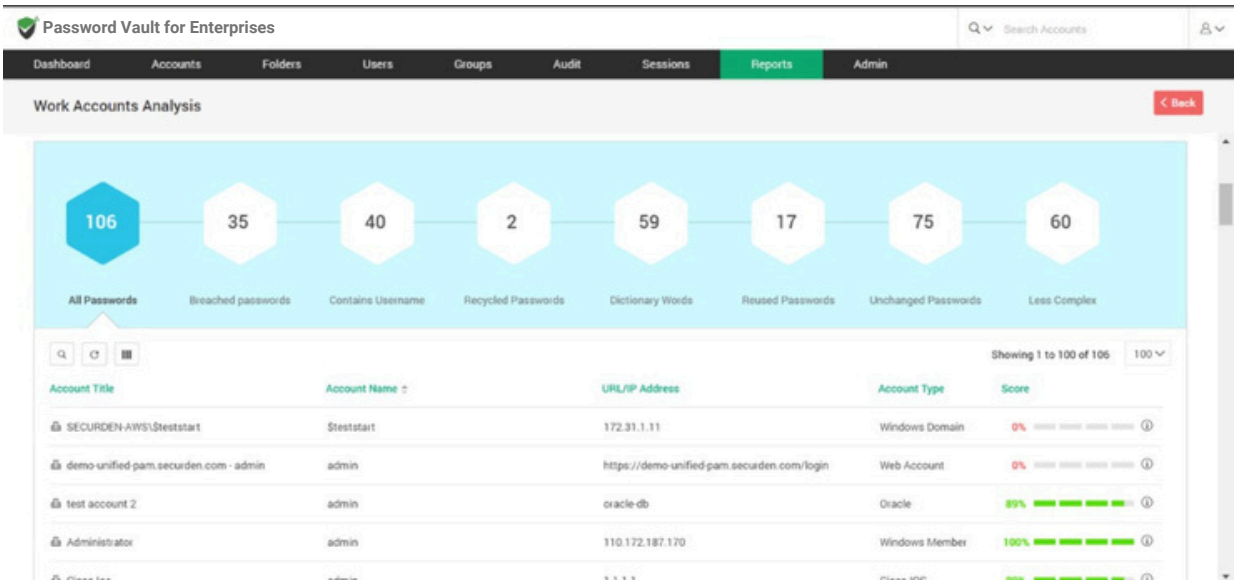
Password Security Analysis

Work Account Analysis

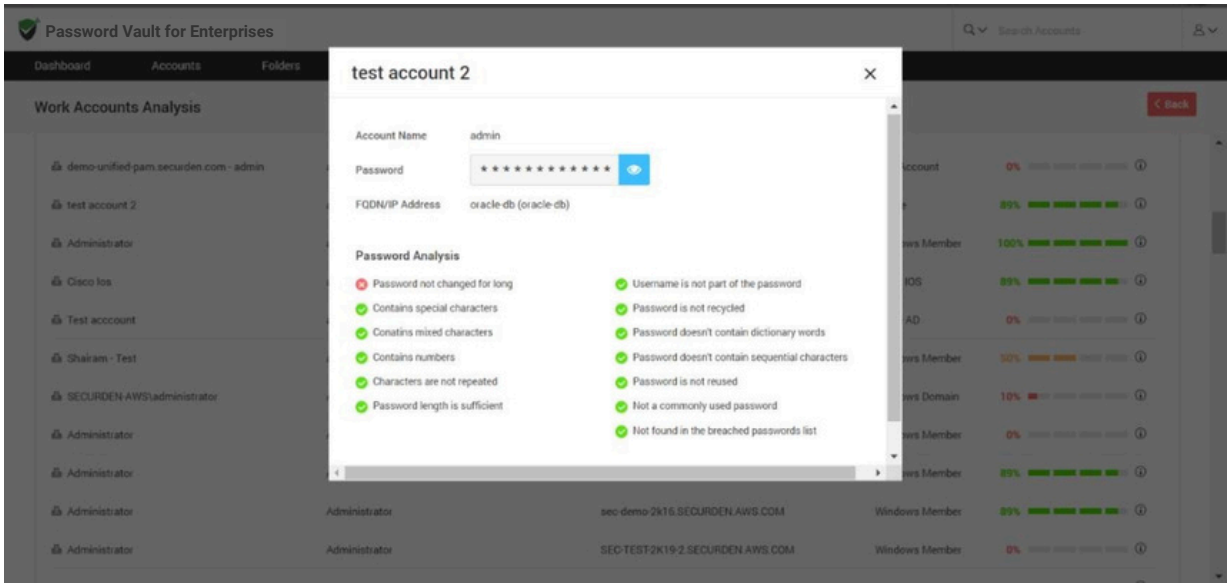
To access this report, navigate to **Reports >> Password Security Analysis >> Work Accounts Analysis**. Securden carries out a comprehensive analysis of various passwords used by you and provides an independent strength assessment. It classifies the passwords into four categories - Weak, Vulnerable, Fair, Strong. The reason for the respective classification is also presented, using which you can take remedial measures to strengthen the passwords. The report pertaining to the passwords owned by you will be presented on the screen.



The cumulative strength password indicates the overall strength of the various passwords in terms of the percentage. The bar graph of weak passwords distribution by type depicts a quick summary of the weak passwords belonging to different account types. The types that have the most number of weak passwords are also displayed on the screen.



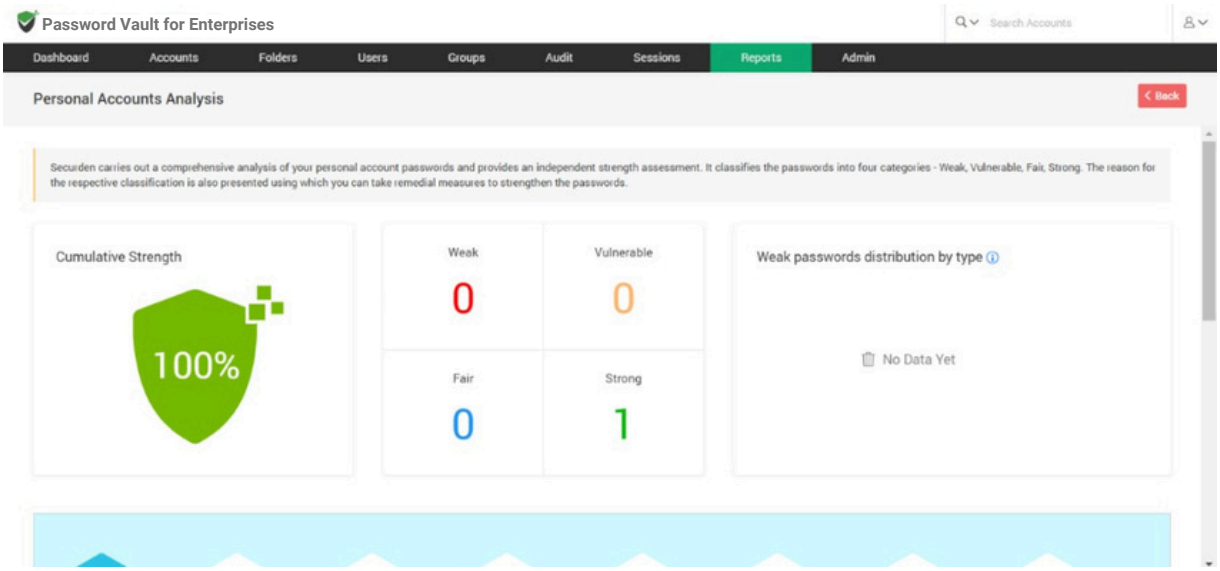
The hexagons display the category of password (such as breached passwords, less complex passwords, reused passwords, etc.,) and show the table with account details and strength score of the password (in percentage). The score column further tells us which criterias have been satisfied by that password and gives a detailed password analysis for each account.



Personal Account Analysis

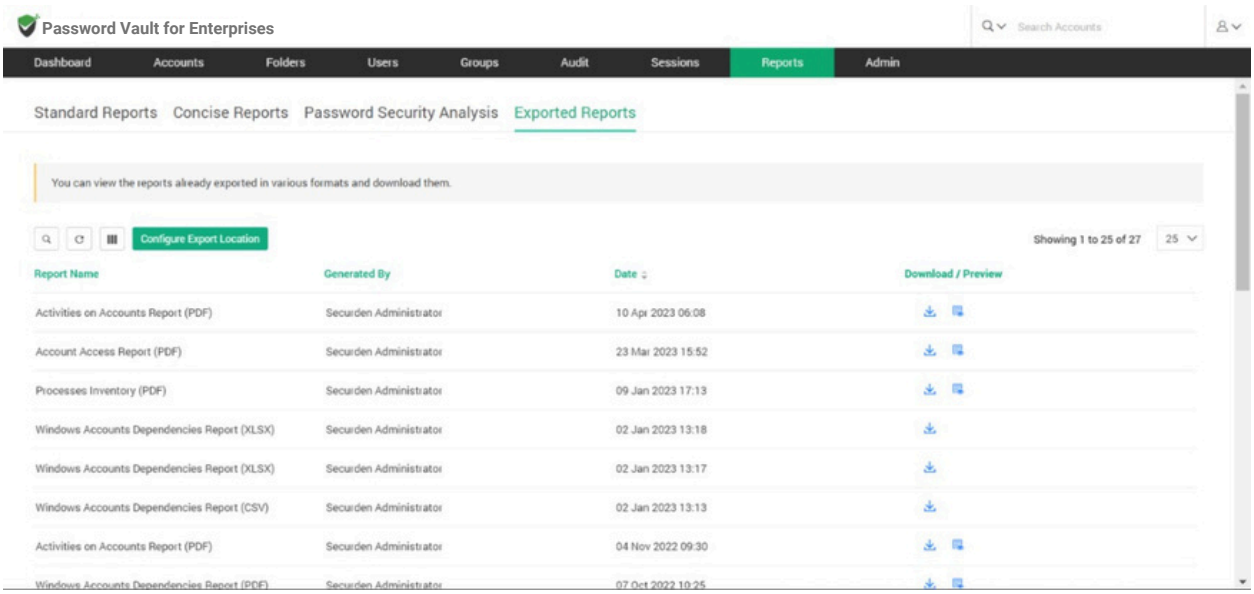
To access this report, navigate to **Reports >> Password Security Analysis >> Personal Accounts Analysis**.

This report keeps track of the personal account passwords and provides an analysis about the activities performed with those accounts.



Exported Reports

To access these reports, navigate to **Reports >> Exported Reports**. You can view the reports already exported in various formats and download them. The different types of reports which were already exported are displayed here along with the date of download and the user who generated it. Click on **Configure Export Location** to change the location for the exported reports.



Section 15: Miscellaneous

Change Database

If you want to change the backend database to MS SQL Server, 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 Vault ervice** 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 Vault 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

Store Encryption Keys on Securosys HSM

You can configure an HSM device and store the Securden encryption key for additional security. HSM is an encrypted, security-hardened device used for storing, generating, and rotating encryption keys. You need to provide certain details of your HSM device and configure it before storing the Securden encryption key in your HSM device.

Prerequisite: You need to take a backup of your entire database along with the encryption key before starting the HSM configuration process.

Step 1: Stopping the Securden Vaultservice on Primary and Secondary servers

Navigate to services.msc and **Stop** the **Securden Vault service**. If you have configured secondary application servers in your organization, you need to stop the Securden Vaultservice on all the secondary servers.

Step 2: Configuring the HSM

Navigate to <Securden installation folder>/bin and locate **ConfigureHSM.exe.**

Open **ConfigureHSM.exe** and provide the following details:

1. **HSM Provider Name**: The name of your HSM provider. You can select Securosys from the drop-down menu.
2. **DLL File Path**: Securden integrates with your HSM provider through their **primus.dll** file. You need to specify the location of this file in this field.
3. **HSM Slot ID**: The partition in which the Securden encryption key should be stored.
4. **HSM Slot Password**: The credential required for accessing the HSM and storing the encryption key in the slot mentioned above.
5. **Encryption Key Label**: The name with which the Securden encryption key should be stored in the HSM.

Once the required details are provided, click **Configure**.

Important:

After configuring the HSM,

1. The entire database will be decrypted using your current key and encrypted using a new key which is stored in your HSM.

2. You need to take a fresh backup of your database since your previous backup copies cannot be restored, since the encryption key is different.

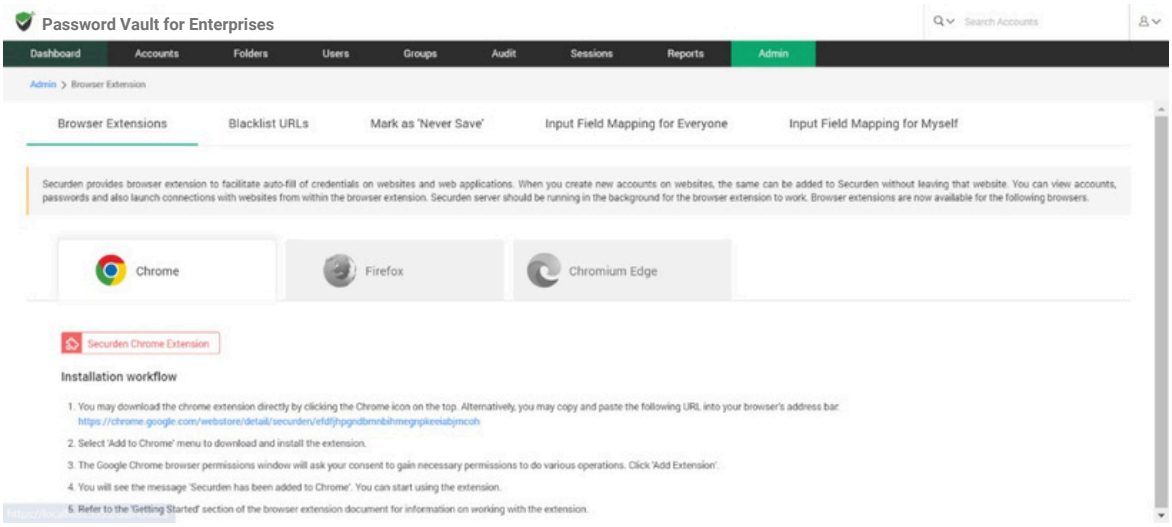
3. If you had configured secondary servers of any type before configuring the HSM, they would not work as intended after the process is completed. This is because of the encryption key mismatch between the primary server and the secondary server. You need to re-configure all secondary servers (Remote distributors and high availability servers) and deploy the application server package once again.

4. Securden primary and secondary servers share the same HSM keys. You need to ensure that HSM keys (hsm_1.key, hsm__2.key, and hsm_3.key) are located in the default (Securden\conf) folder.

Browser Extensions

Securden provides browser extensions 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 server should be running in the background for the browser extension to work. Extensions are available for Chrome, Firefox, and Chromium-based Edge browsers.

Navigate to **Admin >> General >> Browser Extensions** to download the extensions.



The steps to install different browser extensions are given below:

Chrome

● You may download the chrome extension directly from the GUI. Alternatively, you may copy and paste the following URL into your browser's address bar:

https://chrome.google.com/webstore/detail/securden/efdfjhpgndbmnbihmegnpkeeiabjmcoh

● Select the 'Add to Chrome' menu to download and install the extension.

● The Google Chrome browser permissions window will ask for your consent to gain the necessary permissions to do various operations. Click Add Extension.

● You will see the message 'Securden has been added to Chrome'. You can start using the extension.

Firefox

● You may download the chrome extension directly from the GUI. Alternatively, you may copy and paste the following URL into your browser's address bar: https://addons.mozilla.org/enUS/firefox/addon/securden/

● Click the 'Add to Firefox' menu to download and install the extension.

● The Mozilla Firefox browser permissions window will ask for your consent to gain the necessary permissions to do various operations. Click 'Add'.

● You will see the message 'Securden has been added to Firefox'. You can start using the extension.

Chromium Edge

● You may download the chrome extension directly from the GUI. Alternatively, you may copy and paste the following URL into your browser's address bar: Securden - Chrome Web Store (google.com)

● Select the 'Add to Chrome' menu to download and install the extension.

● The Chromium Edge browser permissions window will ask for your consent to gain the necessary permissions to do various operations. Click 'Add Extension'.

● You will see the message 'Securden has been added'. You can start using the extension.

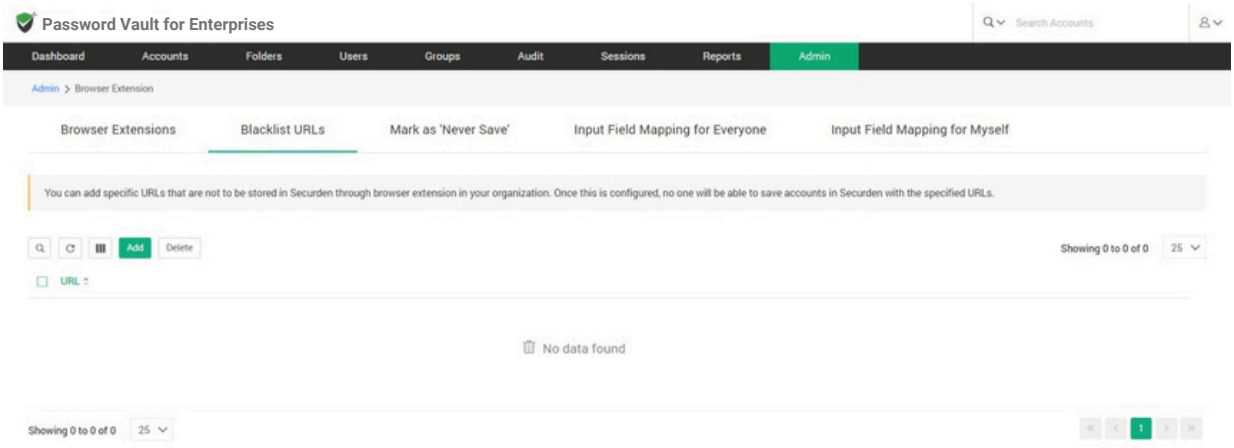
In addition to installing browser extensions, you can do certain configurations related to the usage of the extensions.

Blacklist URLs

Once you install the extension, whenever you create a new account/password on a website, it usually prompts you to add the accounts to Securden inventory. There might be requirements where you wouldn't need certain accounts to be added to Securden. You can handle such scenarios through the blacklist URLs option.

This option Securden allows you to add (and delete) specific URLs that are not to be stored in Securden through the browser extension in your organization.

Navigate to **Admin >> General >> Browser Extension >> Blacklist URLs** page and click the **Add** button.

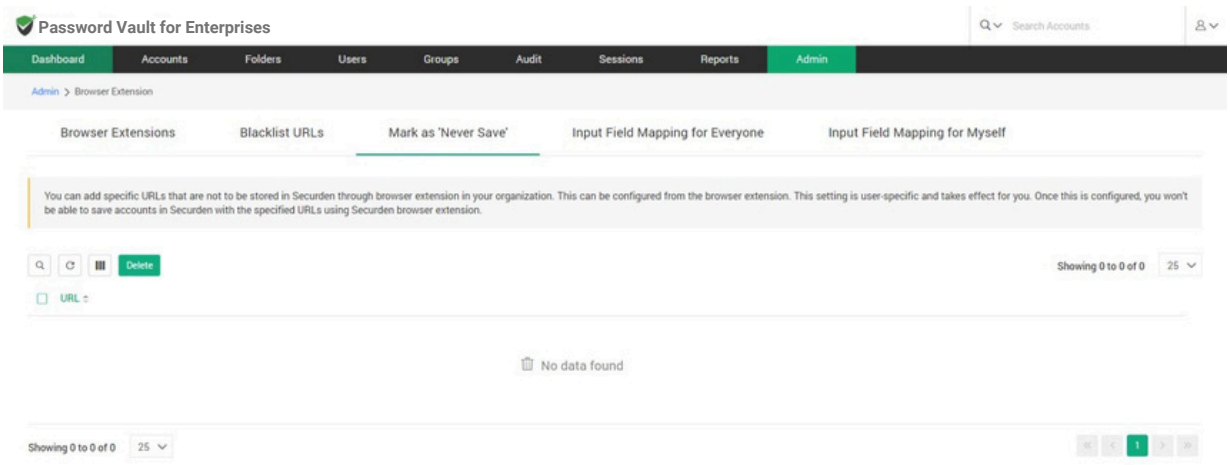


Once this is configured, no one will be able to save accounts in Securden with the specified URLs.

Mark as Never Save

This feature is similar to the Blacklist URL option and allows you to define specific URLs that are not to be stored in Securden through the browser extension. While the Blacklist URLs option takes effect globally across the organization for all users, the ‘Never Save’ option is user-specific and doesn’t affect the entire organization.
Typically, the URLs that are marked not to be saved in Securden (setting you will see in the extension) will be listed on this page.

Navigate to **Admin >> General >> Browser Extension >> Never Save** page to manage such URLs.



You can add specific URLs that are not to be stored in Securden through browser extension in your organization. This can be configured from the browser extension. This setting is user-specific and takes effect for you. Once this is configured, you won't be able to save accounts in Securden with the specified URLs using Securden browser extension.

Moving Securden Installation from One Machine to Another

If you want to move the Securden installation from one machine to another (for example, moving a test setup to production), you may follow the steps below:

Prerequisite: Securden installation is guarded by a unique encryption key. When you move the installation, you need to take care of the key as well. The new installation would require the key. By default, the encryption key is available as <Securden-Installation-Folder>\conf\securden.key.

In production instances, we enforce changing the key location. If you have changed it from **Admin >> Security >> Change Encryption Key** Location, you need to ensure that the key is present in the location specified.

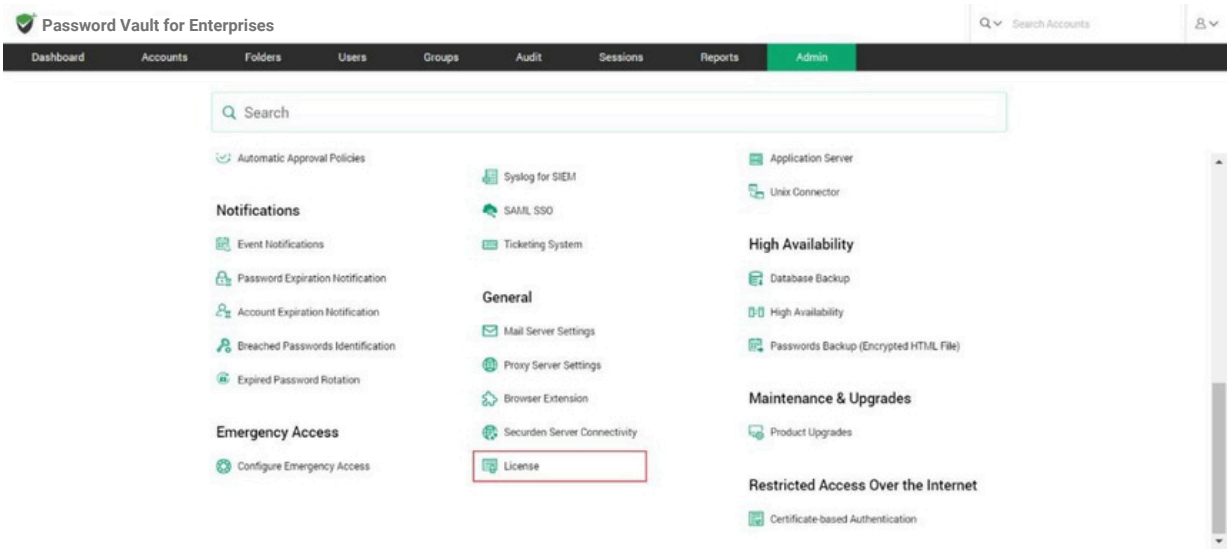
To move Securden from one server to another follow the steps below.

- Stop the "Securden Vault Service" from services.msc
- Copy the entire Securden installation folder
- Paste it on the new server
- Open a command prompt, run with admin privileges, and navigate to **<Securden Installation Folder>/Password_Vault bin folder**

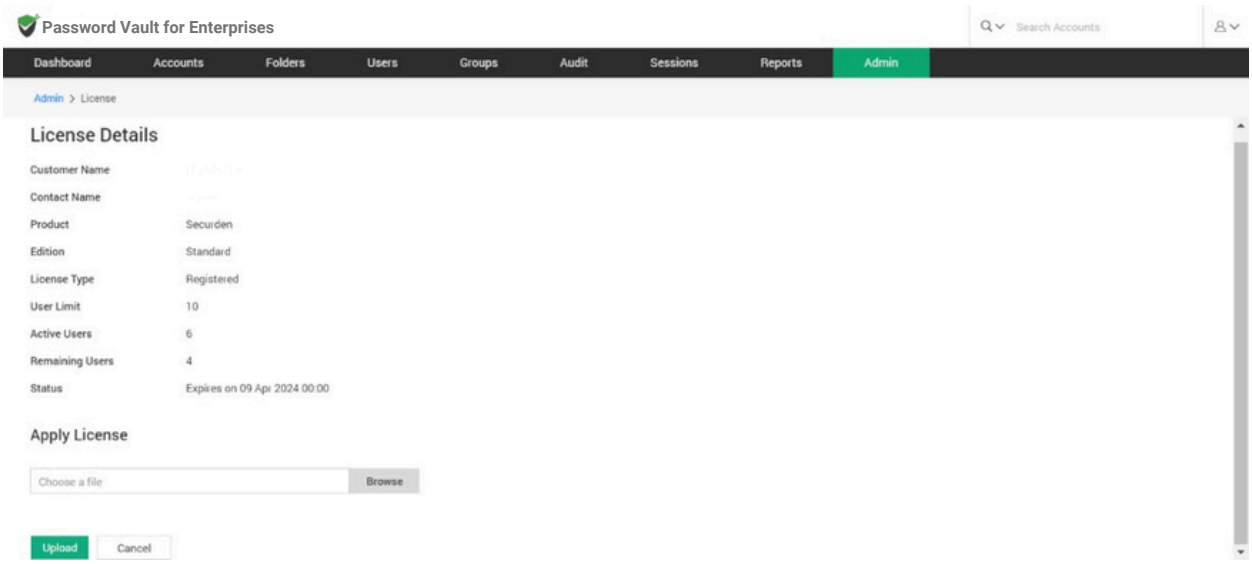
- Execute the command SecurdenServiceInstaller.exe install
- Start the "Securden Vault Service" from services.msc

Section 15: Product License Key

You can apply the Securden license key and get information about the existing license from **Admin >> General >> License** section.



In the License details page, the following details are displayed:



Customer Name: The name of the organization for which the product is licensed

Contact Name: Contact person within the company

Product: The name of the product purchased from Securden.

Edition: Product edition name

License Type: This indicates if you are a registered user or if you are using the trial version.

User Limit: The number of users that can be onboarded into Securden.

Active Users: The number of users that are currently onboarded into the solution.

Remaining Users: The number of users who can be added into Securden.

Addons: Product addons, if any.

Status: The number of days until expiration is displayed here. To add a new license, you can use the browse button to search for that license and upload the same