Securden

Unified PAM

User Guide

User Guide

Introduction

This guide provides the essential information for the end users to get started with Securden PAM. It throws light on what operations you can perform and how efficiently you can use the product.

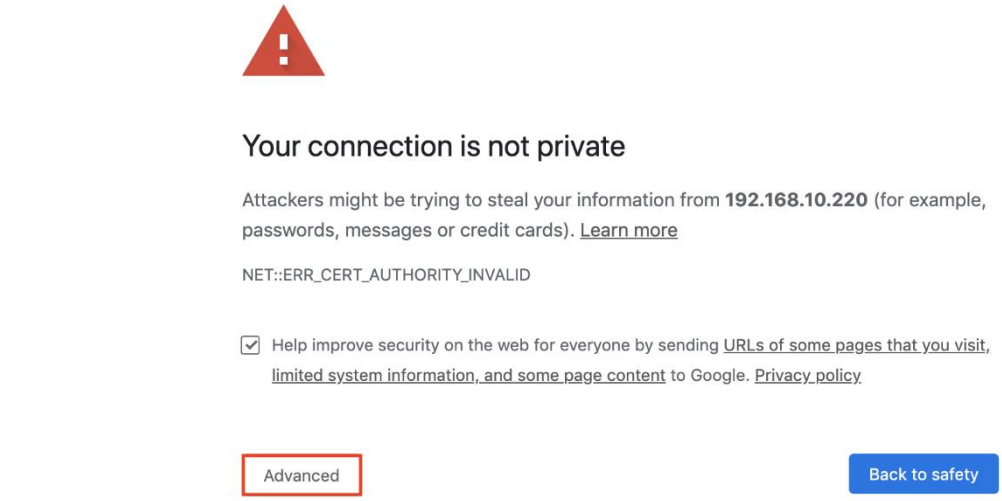
Accessing the Web-interface

Your administrator would have provided you with the URL to connect to the web interface, which typically looks like **https://<Hostname or IP address of Securden server>:5959**.

To access web interface,

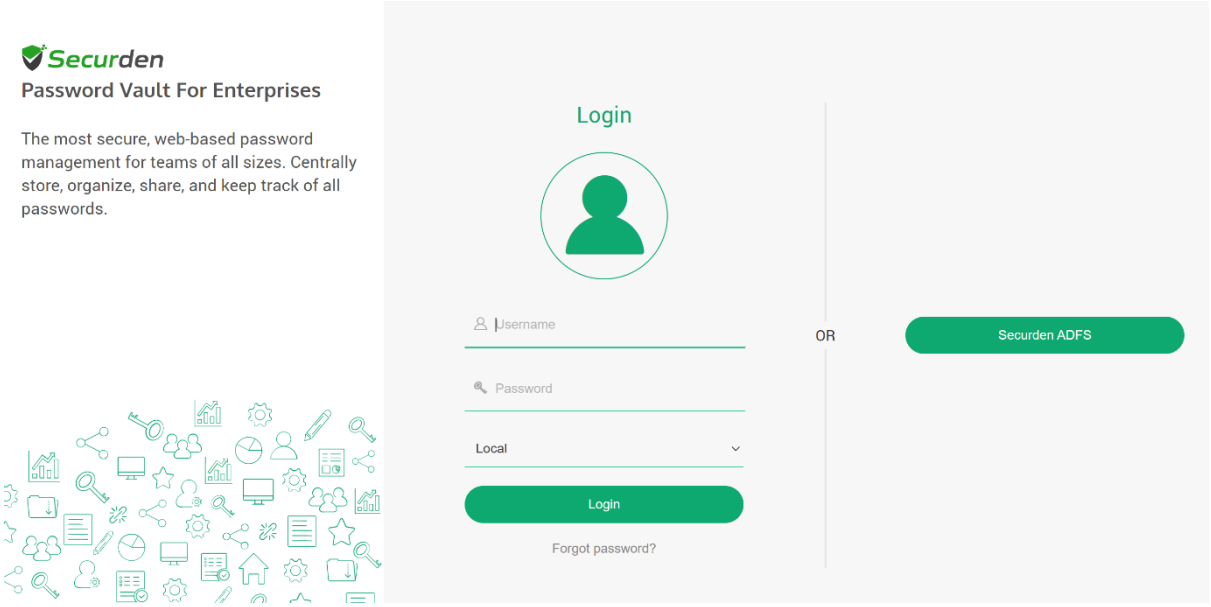
- Open any browser and type the URL. It is typically in this format: **https://<Hostname or IP address of Securden server>:5959**
- During this process, you might see warning messages displayed by the browsers. This message appears because Securden comes bundled with a self-signed certificate. (If your 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'.



Logging in to Securden

Securden supports various authentication options, including Active Directory authentication, native local authentication of the application, and different Single Sign-On options. Your administrator would have informed you about the authentication mode.



- Choose the appropriate one on the login screen
- If your administrator has enforced two-factor authentication, you will have to enter a verification code

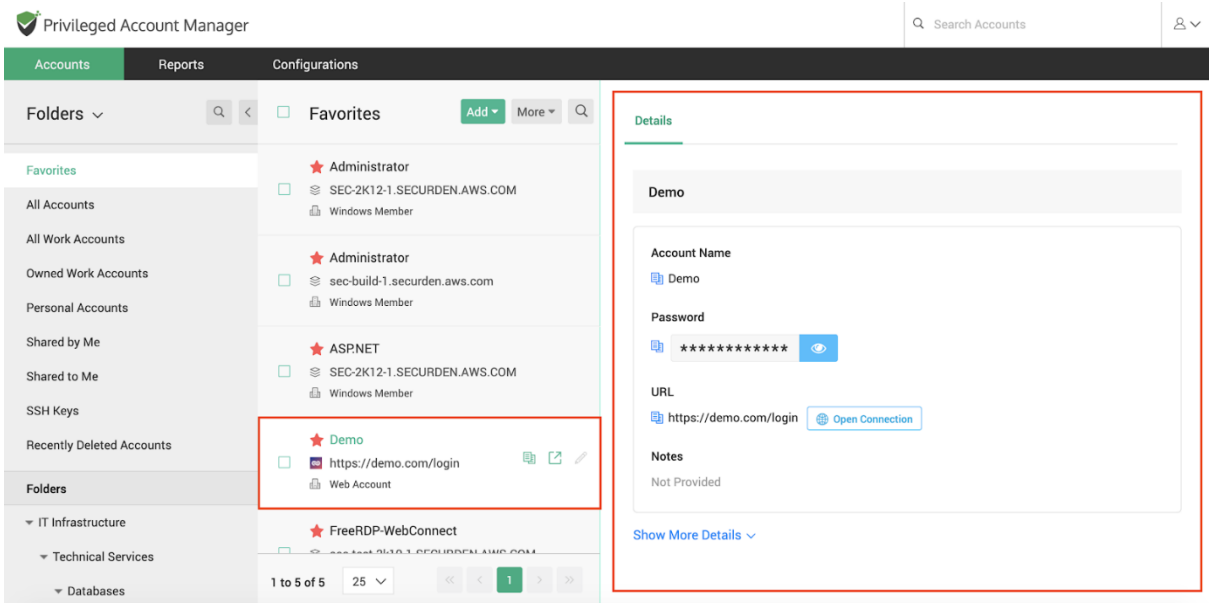
Working with the Interface

Upon logging in to the web interface, you will see different tabs based on the permissions granted. All password management-related operations are performed from the '**Accounts**' tab.

The Accounts Tab

View the account details and passwords allotted to you

Any login information (username and password) stored in Securden is referred to as an account. You will see the list of such accounts you have access to in the 'Accounts' tab.



You can click the required account and view the details on the RHS. If you have been provided with permission to view the password of that particular account, you can view that by clicking the 'Eye' icon. Otherwise, the password will not be displayed. For

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

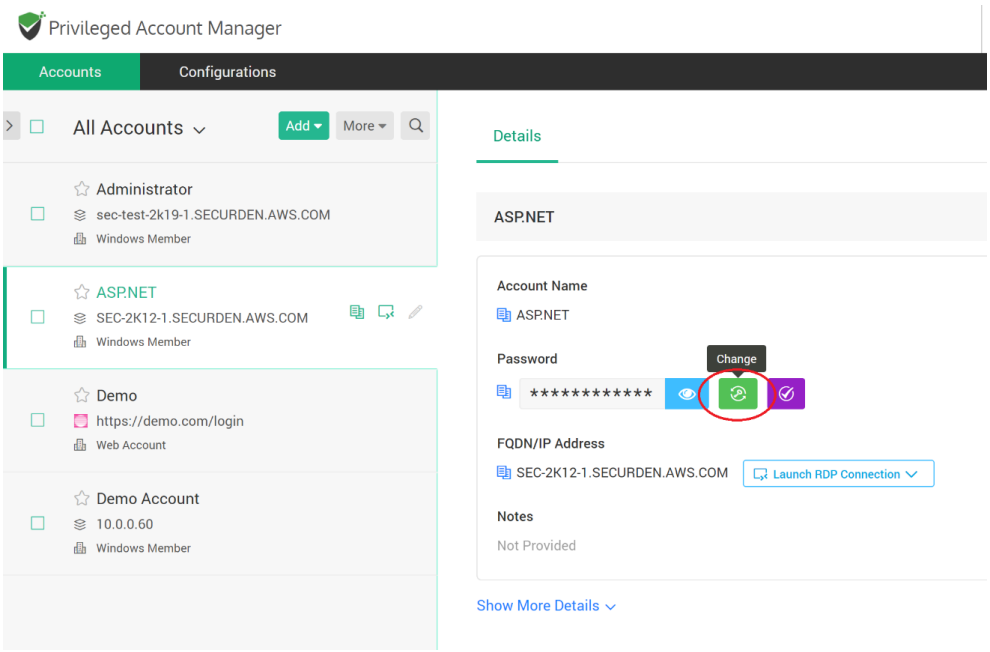
The bottom of the 'Details' section provides more information about the other attributes of the account. In addition, security-related information such as account creation time, ownership details, last access, and modification details are also displayed. Click '**Show More Details**' link to view these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

Copy Credentials

To copy the username or password to the clipboard, click the **Copy** button located on the left side of the respective 'Account Name' or 'Password' field.

Change Password

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



helps generate strong passwords. When you select the option "Change the password on remote machine", the new password will be applied on the remote device too. In addition, you may have to justify why you are changing the password by mentioning the reason. The reason you enter here is captured in the audit trail.

Verify Password

To verify if the password stored in Securden is in synchronization with the remote device,

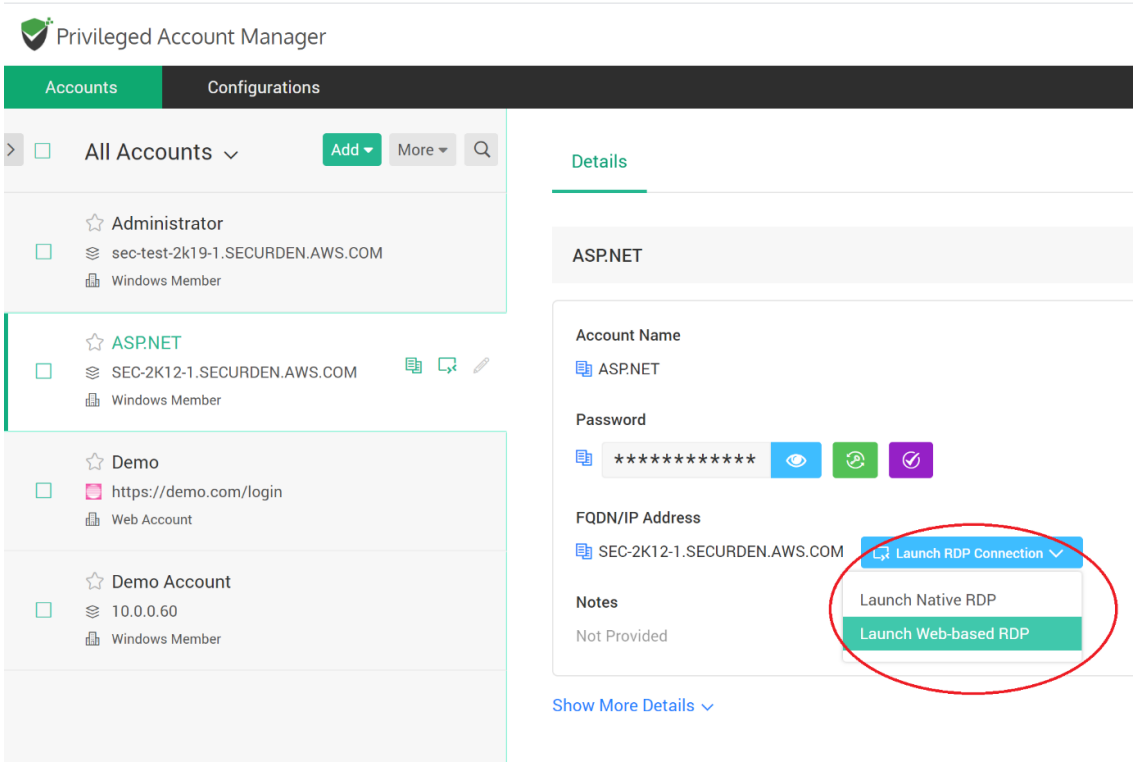
- Navigate to **Accounts** section in the GUI, **click the required account,** click the '**Verify**' button in the right pane next to the account password and then follow the instructions in the GUI.

Launching Remote Connections
(RDP, SSH, SQL, Website Connections)

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

Web-based Connections

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



To launch web-based RDP, SSH connections, select the required account, click "**Launch RDP Connection**" or "**Launch SSH Connection**" and then choose the web-based option.

Using Native Client Applications

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

Launcher for RDP Connections

As mentioned above, to launch RDP connections, you need to install a lightweight launcher called '**Securden Remote Launcher**' on all the machines from which you would be connecting to Securden web interface. The launcher can be downloaded and installed from **Configurations >> Remote Sessions >> Windows Remote Launcher**.

To launch RDP connection,

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

To launch SSH connections,

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

To launch SQL connections,

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

Auto-fill Credentials on Websites

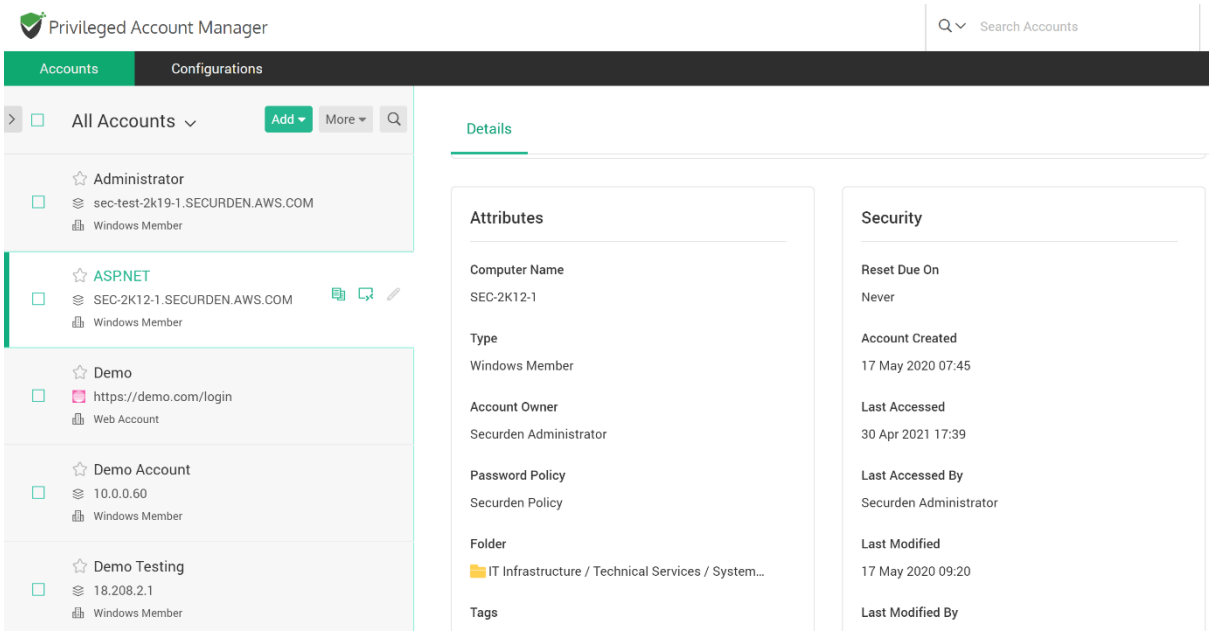
Pre-requisite: Securden provides browser extensions to facilitate auto-fill of credentials on websites and web applications. Securden browser extensions are now available for Chrome, Firefox, and Edge. You can install the browser extensions from the **Configurations >> General >> Browser Extensions** section In the GUI. The installation instructions and how to work with the extensions are available in this document. (Auto-fill will not work if the browser extension is not installed).

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

View Account Details

When you click "**Show More Details**" in the 'Details' section of an account, you will see the various attributes of the account. Most of these attributes are self-explanatory. The "Account ID" attribute denotes the unique id of the account, which can be used in API calls.

If you have the permission, you will also see security-related information of the account too.



In the **Attributes** section, the details shown include:

- **Account Type**: The internal classification of the particular account.
- **Owner:** The user who created the account. If the one who created the account had transferred the ownership, the field displays the current owner.
- **Password Policy:** The password policy (complexity rules) associated with the account by your administrator.
- **Folder:** Accounts can be grouped to form a folder. This field shows the folder to which the account belongs.
- **Tags:** Accounts are associated with various tags that come in handy to identify and locate the accounts quickly.
- **Account ID:** Unique id that helps identify an account. The IDs can be used in API calls for programmatic access.

Security Attributes

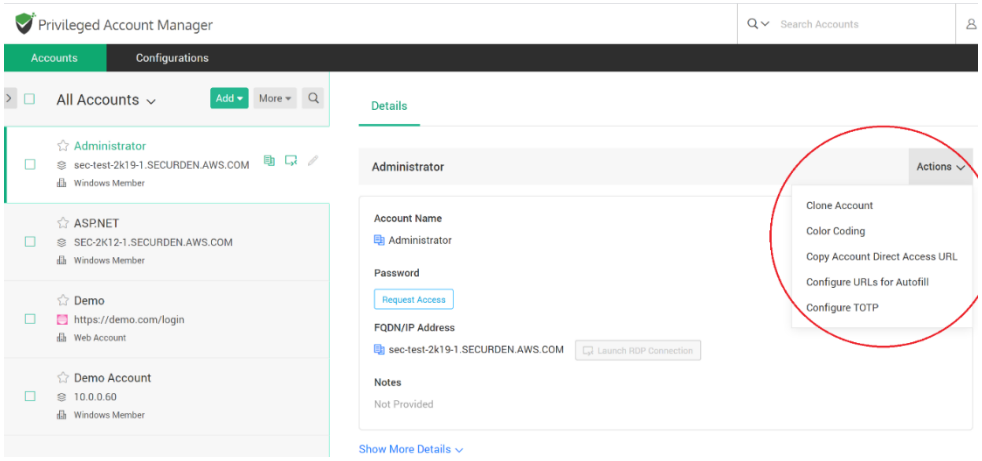
This section will be visible only if you have been permitted to view these details.

- **Reset Due On**: If the password policy associated with the account specifies a 'password age' or if it mandates resetting the passwords at periodic intervals, the due date for changing the password is displayed here.

- **Account Created:** Shows the date the account was created on.
- **Last Accessed:** The date when the account was last accessed.
- **Last Accessed By:** The name of the user who last accessed the account.
- **Last Modified**: If the password had been modified, this attribute shows the date on which it was last modified.
- **Last Modified By:** Shows the name of the user who last modified the password.

Account Actions

Based on the permission granted to you for each account, you will be able to perform one or more actions on the accounts as explained below.



Clone Accounts

Cloning an account means creating a copy of the account with all the attributes intact. You can modify some of the values in the fields and save the cloned account as a new account. This saves you from manually entering data when you have to add accounts with similar information. The cloned accounts will carry the suffix 'copy' in the name. To clone accounts, follow these steps:

- Select the account(s) you want to clone and navigate to **Details >> Actions >> Clone Account.**

- Select the number of copies you want to create and click 'Clone' to create a copy of the accounts

Color Coding

For ease of identification and management, you can assign color codes for accounts. The accounts that are assigned with specific color codes will be displayed with the chosen color in the background. To color code accounts, follow these steps:

- Select the account for which you want to associate a color code and navigate to **Details >> Actions >> Color Coding.**
- Select the desired color and click 'Save' to make changes
- The color-coding is account-specific. That means, if the account is shared with multiple users, the latest color associated by any of the users takes effect.

Copy Direct Access URL

When you are logged in to Securden, you can directly access any particular account using the account-specific URL. Of course, the access requires successful authentication and permission to view the account. The URLs should start with HTTP or HTTPs. You can copy the URL and use it to have quick access to the account. To copy the account, follow these steps:

- Select the account for which you want to create a direct access URL and navigate to **Details >> Actions >> Copy Direct Access URL.**

Configure URLs for Autofill

As mentioned earlier, Securden (through browser extensions) enables auto-filling usernames and passwords on websites. Sometimes, an account can have multiple URLs. You can configure all such exact URLs here and Securden takes care of the auto-filling.

- Select the account for which you want to configure URLs and navigate to **Details >> Actions >> Configure URLs for Autofilling.**

Configure TOTP

For shared accounts that require a Time-based One-time Password (TOTP) as the second authentication factor, you can configure the same here so that all those who have access to the account will also have access to the TOTP too.

- Select the account for which you want to configure TOTP and navigate to **Details >> Actions >> Configure TOTP.**
- From your MFA settings page, either take a screenshot of QR code and upload that or provide the secret key associated with the web application
- Once this is done, the respective TOTP will be available with the account details.

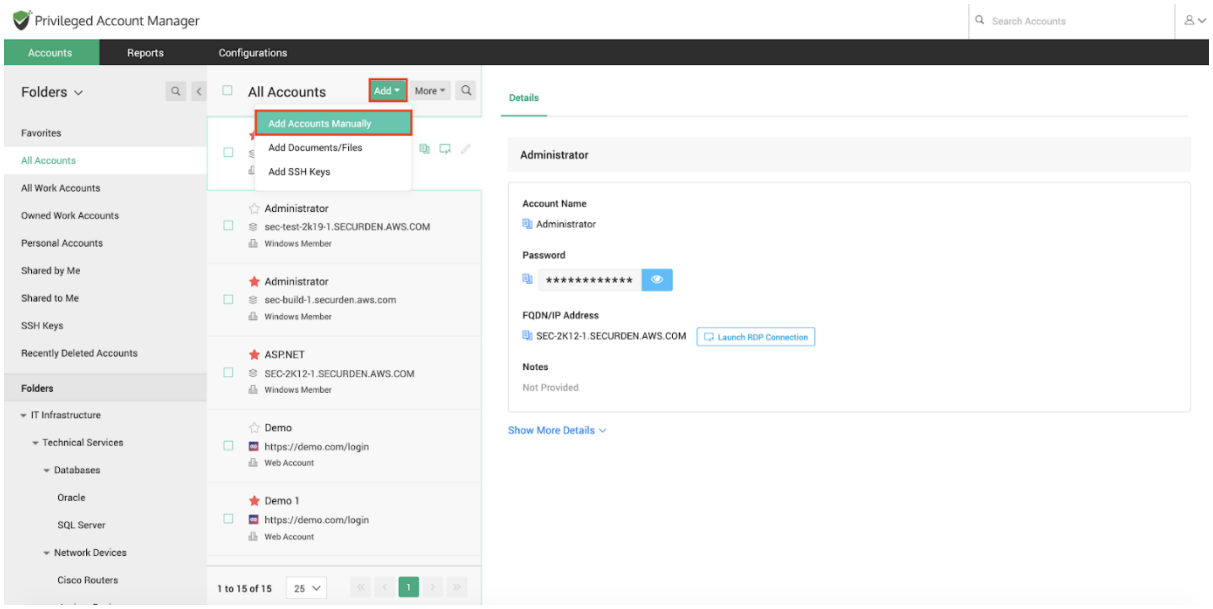
Add Accounts

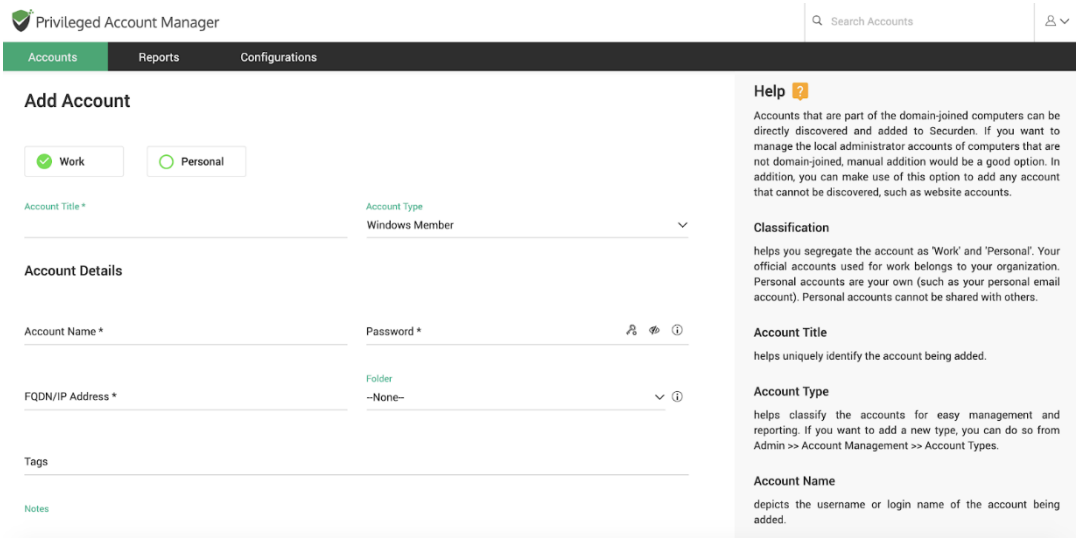
If you have permission to add accounts, you can do that in two ways. Either you can add accounts manually or import them from a file. Securden classifies accounts as 'work' and 'personal'. Depending on your organization's specific requirements, your administrator will permit adding both 'Work' and 'Personal' accounts or anyone or neither. Accounts classified as 'Personal' are purely personal to you, and no one else can see them. Personal accounts cannot be shared with others. Whereas, when you add work accounts, you can share them with other users.

Adding accounts manually

To add accounts manually, navigate to **Accounts >> Add >> Add Accounts Manually**. While adding accounts, select the appropriate account type. You can add descriptions, tags, and notes for easy identification.

Note: When you add Windows accounts manually, ensure that you choose 'Windows Domain' as the type for domain accounts and 'Windows Member' for local accounts.





Add Documents, Files

In addition to storing passwords, you can also store and manage documents, files, images, license keys, etc. You can either attach files along with any account or even store the documents individually. Navigate to **Accounts >> Add >> Add Documents/Files** in the GUI to perform this step. While adding documents, the account type will be set as 'File Store' by default. You can add descriptions, tags, and notes for easy identification.

Import Accounts

If you are already using another password manager or keeping your passwords on spreadsheets, you can import accounts from a standard CSV or XLSX file. Navigate to **Accounts >> Add >> Import From File** to perform this.

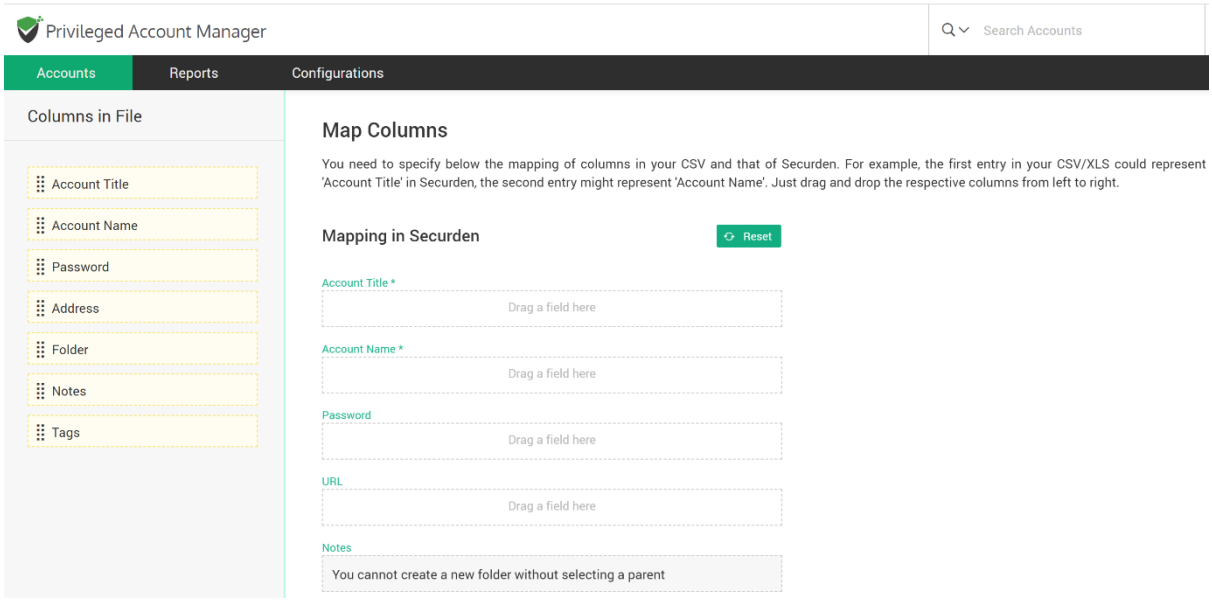
File Format

Accounts import is very flexible in Securden. You can simply import the file you have exported from your current repository into Securden. Typically, each line in the file is added as an account. In the second step of accounts import, you can **map the columns** in the input file and those of in Securden. So, the format of the import file doesn't have a major role.

Steps to import

- Navigate to **Accounts >> Add** and select "**Import From File**" option.
- Browse and select the file
- Click '**Next**'. In the second step of the import, we provide the option to **map the columns** in the input file and that of Securden.

Mapping



In 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 Name --> Account Title, UserName ---> Account Name, Password --> Password, URL --> URL, Hostname --> Hostname (created as additional field), extra --> extra (created as additional field), grouping ---> Folders.

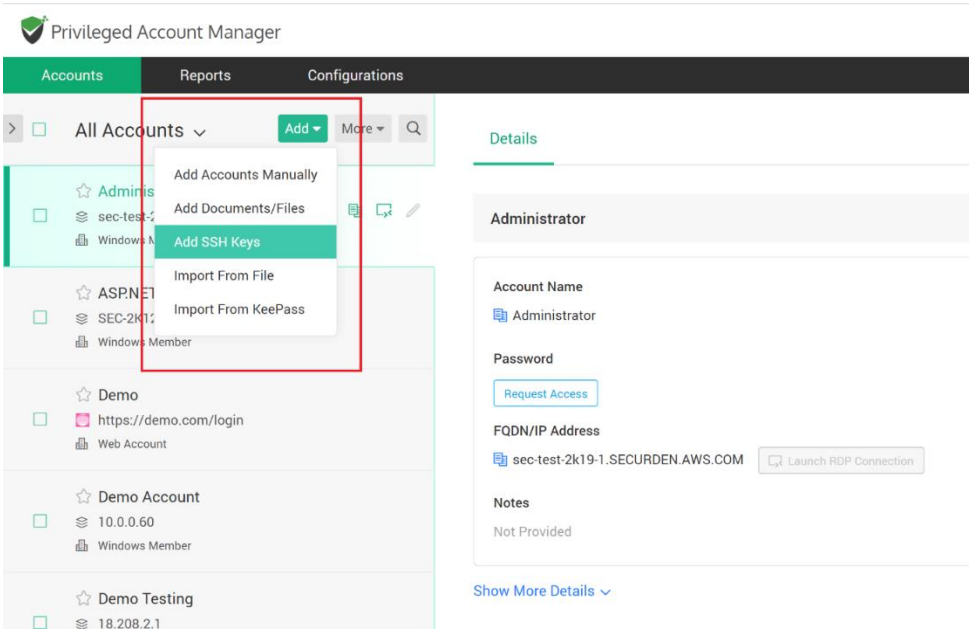
Taking Care of Additional Fields

To include the additional fields that are present in your file into Securden, either you can create a new account type (this is similar to a template) or edit an existing account type. This can be done only by the administrators. You will have to ask your administrator to add/edit.

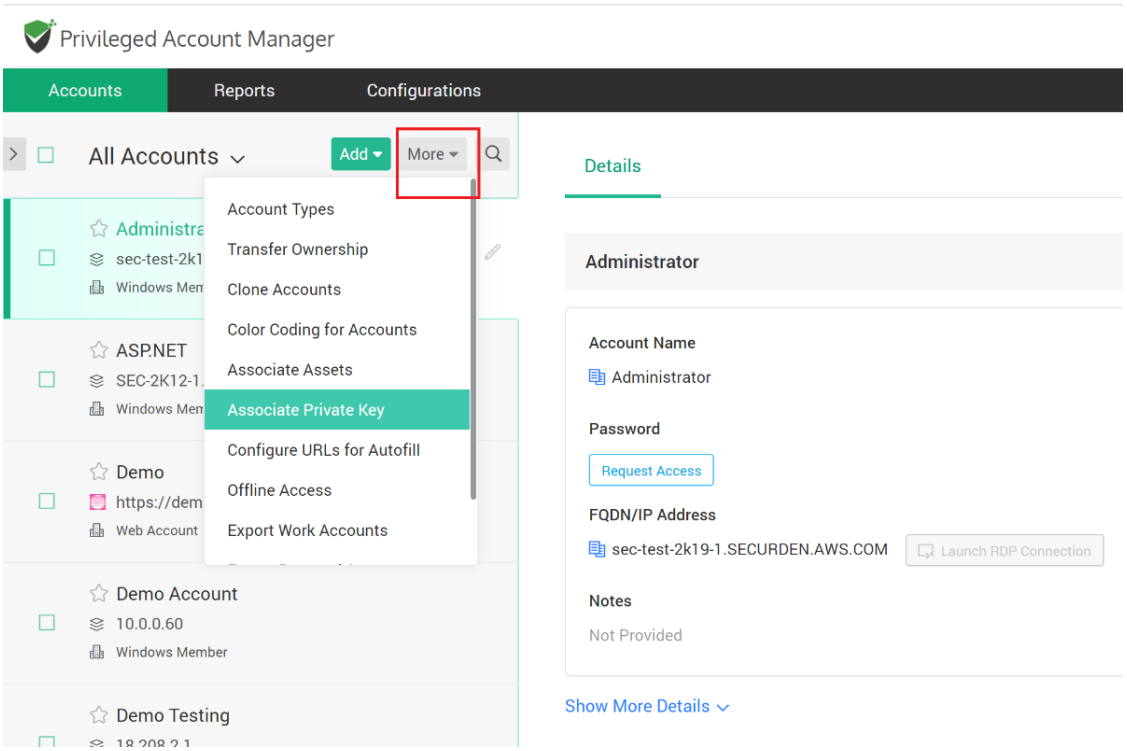
Add and Manage SSH Keys

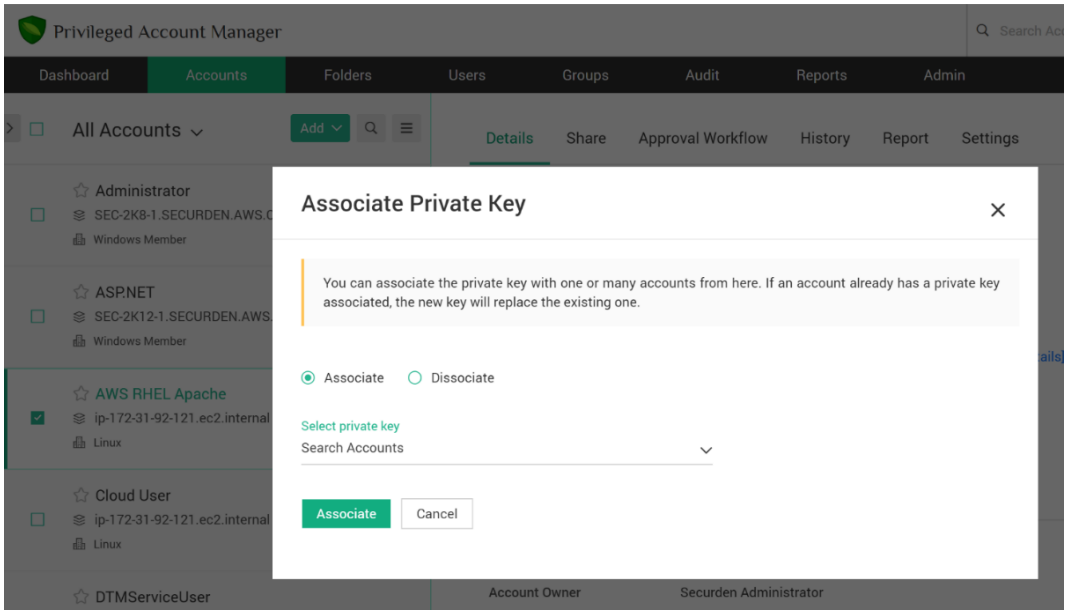
In addition to storing passwords, you can also store and manage SSH keys. The provision for managing SSH keys helps you store the keys securely, track their usage, and associate them with required Unix devices for authentication and remote access.

Navigate to **Accounts >> Add >> Add SSH Keys** in the GUI to perform this step.



After adding the keys, you can associate the required key with the required account by clicking '**Associate Private Key**' option in '**More**' (next to the 'Add' button in 'Accounts' tab). After associating the key, you can open direct connections with remote Unix devices using private key authentication.



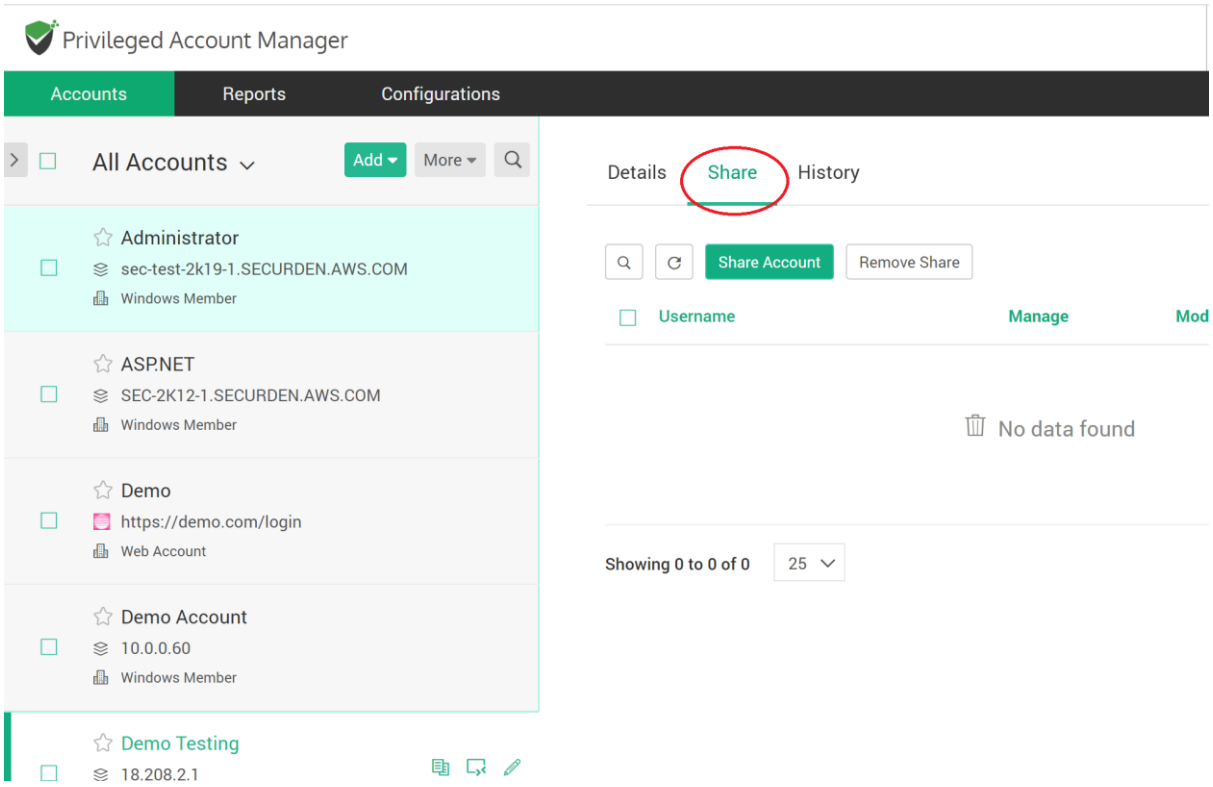


Sharing Your Work Accounts

You can share any work account **created by you/owned by you** with other users or groups with granular permissions.

How to share an account?

- Select the desired account you want to share
- On the RHS of the interface, click the 'Share' option and then click the 'Share Account' button



- You can share the account with users and/or groups. After selecting user/groups, you can search and select the user/group with whom you want to share the account.
- Then choose one of the four sharing permissions:

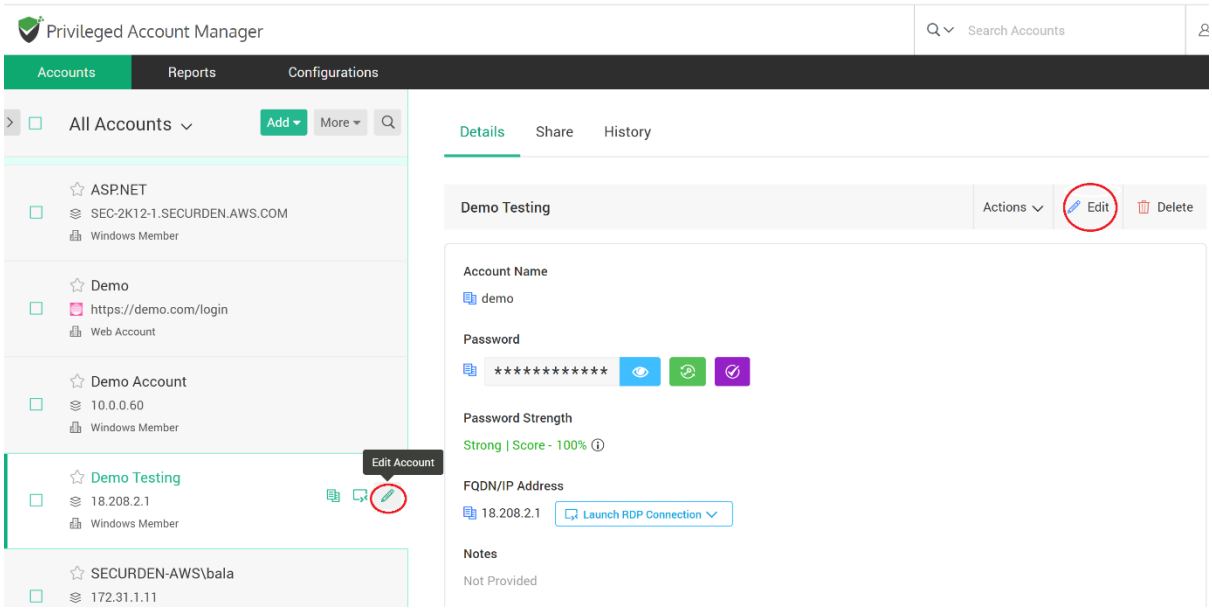
- **'Open Connection'** allows launching RDP, SSH sessions with target machines, and auto-filling credentials for web applications without showing the underlying password in plain text in the GUI
- **'View'** allows the user to view the details as well as the password
- **'Modify'** allows editing the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

- Finally, click "Save".

If you want to remove share at any time, you may visit the same "Share" section in the GUI.

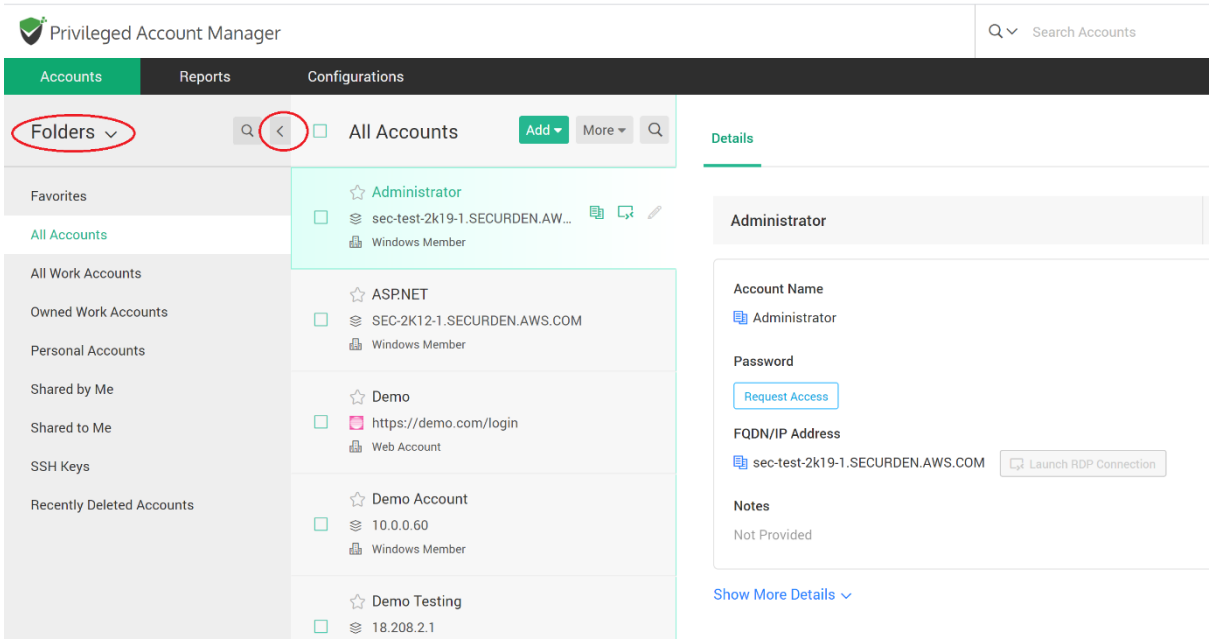
Edit Accounts

You will be able to edit the attributes of the account that you own. The **Edit Account** icon on the LHS or the **Edit** button on the RHS will enable you to edit the account's various attributes such as Account Title, Type, Name, URL, Folder, Tags, and Notes.

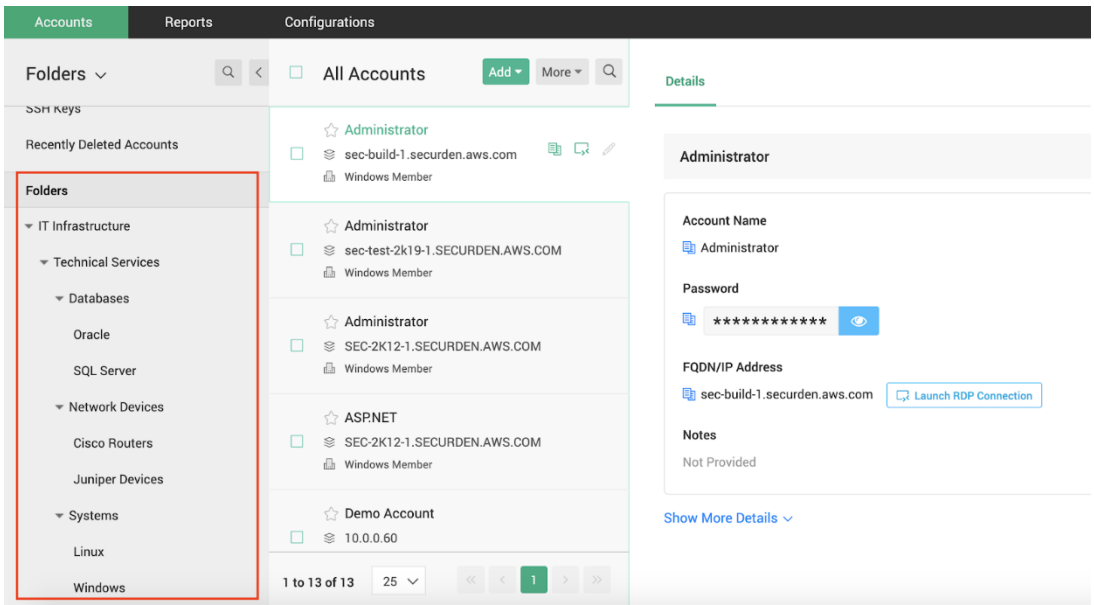


Folders

The accounts in Securden can be grouped and organized as 'Folders'. You can view the folders already created. Click the '>' icon on the LHS and you will see the folder tree.



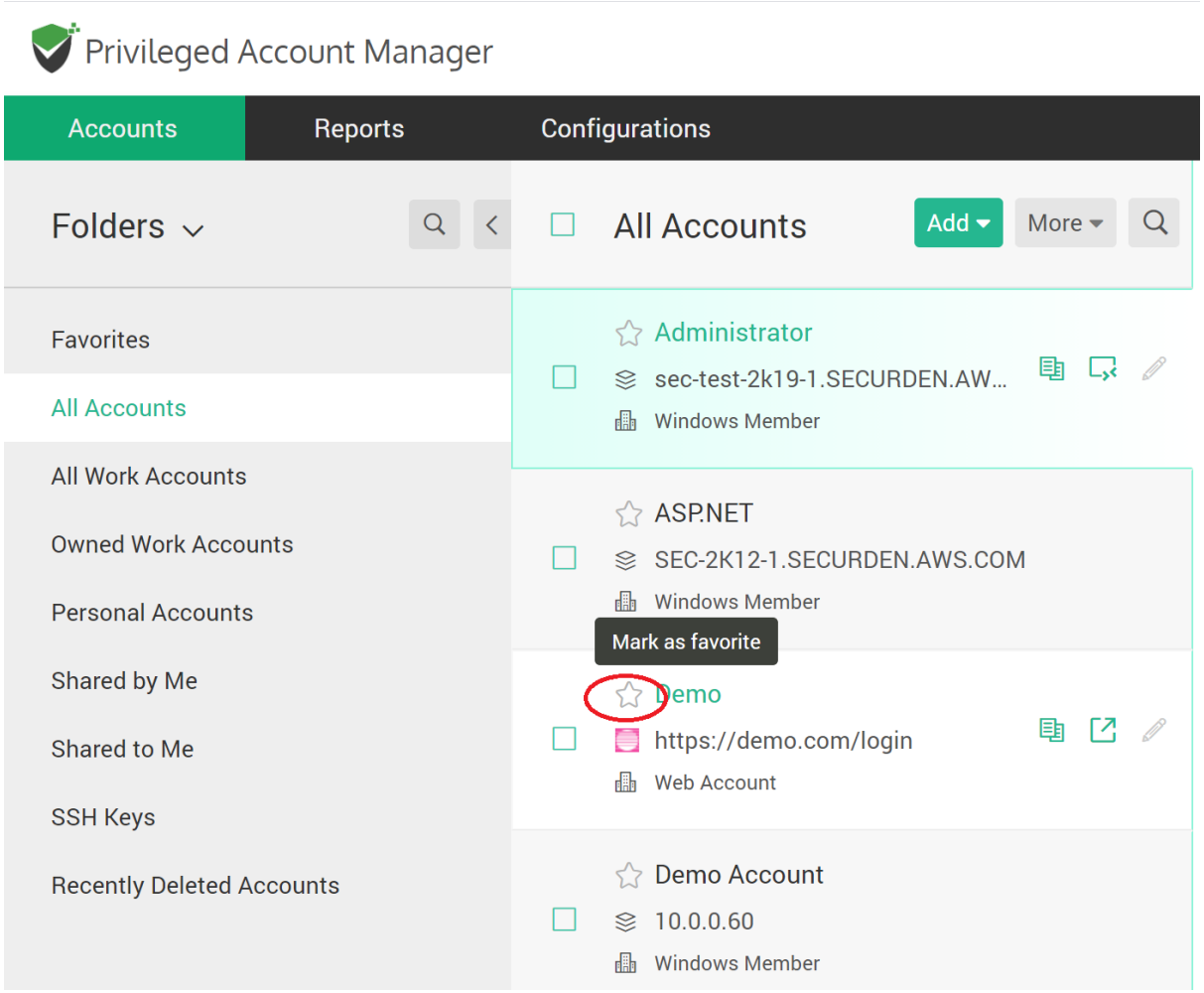
Folder Tree Navigation



The list of folders available are displayed by default on the LHS bottom portion of the 'Accounts' window. Click any folder name to view the accounts in that folder.

Mark Accounts as Favorites

You can label any number of accounts that you would frequently be using as "favorites" for quick access. You can click the star icon near the account name to mark an account as a favorite. You can find all accounts that are labeled as favorite in the 'Favorite' quick link on the LHS.



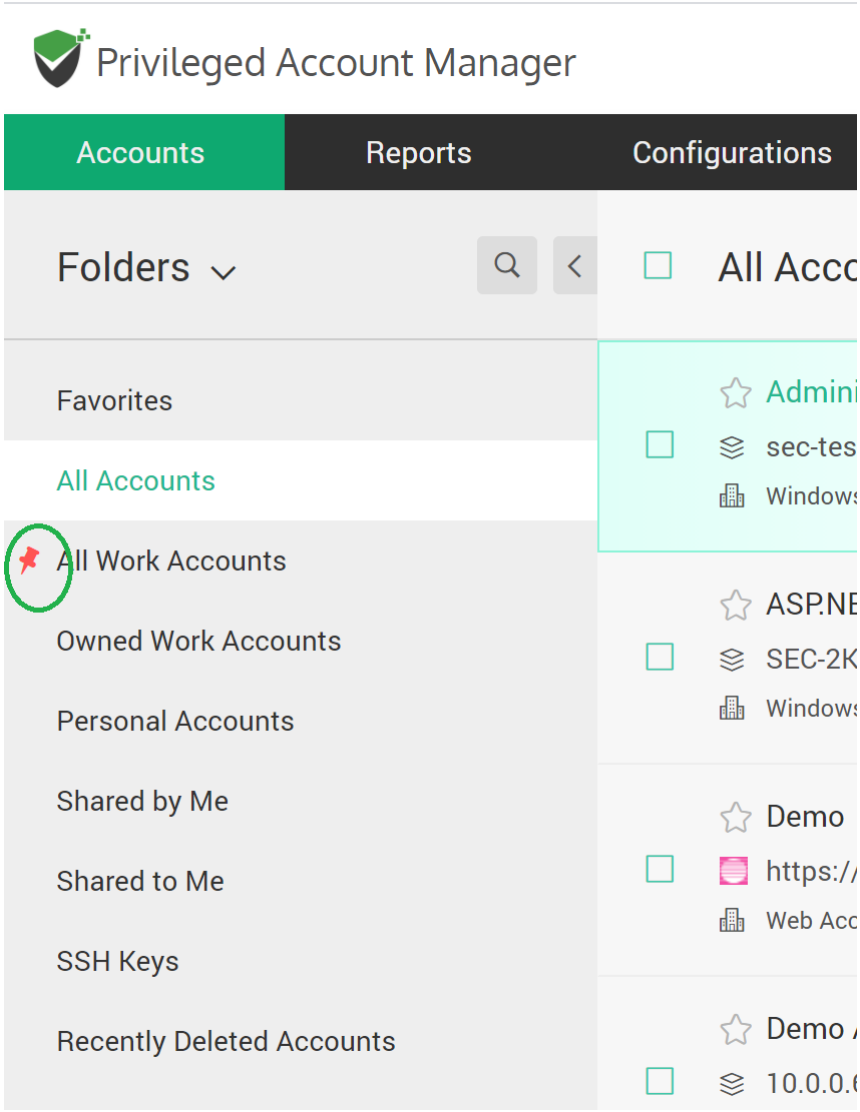
Explore Navigation Options in the LHS

The tree on the LHS contains the following other entries too

- **All Work Accounts:** All the accounts (owned and shared) that have been classified as 'Work' Accounts are displayed.
- **Owned Work Accounts:** All the work accounts you have created are displayed.
- **Personal Accounts:** All the accounts that are marked 'Personal' by you are displayed.
- **Shared by Me:** All the accounts that you have shared with other users/groups are displayed.
- **Shared with Me:** All the accounts that others have shared with you are displayed.
- **SSH Keys:** The accounts with SSH Keys are displayed.
- **Recently Deleted Accounts:** Any account that you delete will be available in this folder for one day, after which the account will be permanently deleted. In case you want to restore your account, you can navigate to this folder, select the account you would like to restore, and click the Restore button to restore it.

Pin Entries

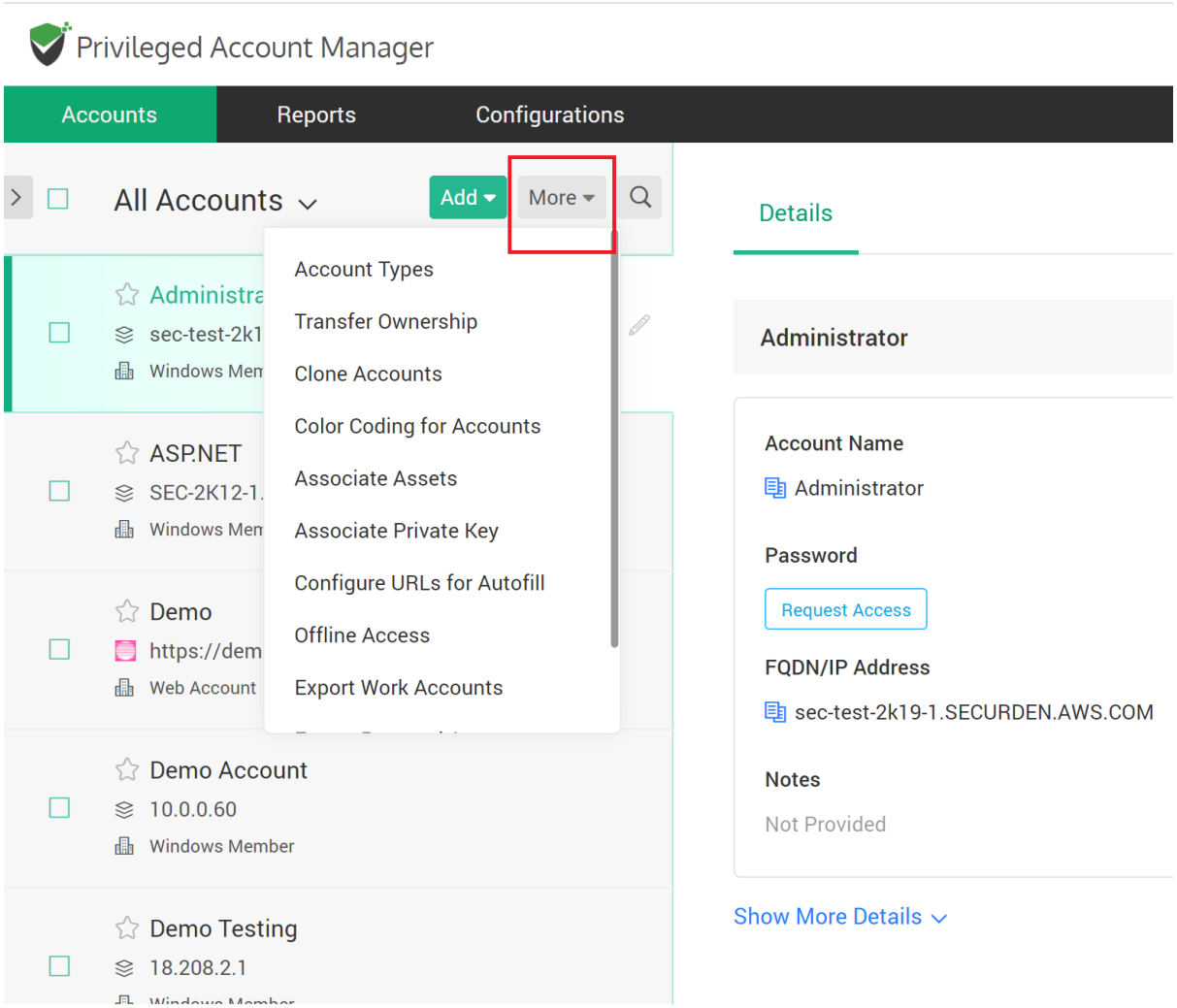
You can pin any entry on the LHS so that the pinned entries will always be visible on top. This will come in handy when you have a large number of folders. To pin an entry, click the 'Pin' icon beside the required entry.



More Actions on Accounts

The **'More' drop-down** in the 'Accounts' tab (next to the 'Add' button) contains a good number of features such as the provision to transferring ownership of accounts, creating clones of existing accounts, establishing color coding for easy identification, associating SSH private keys, exporting data for offline access, provision to delete accounts and a lot more. Navigate to **Accounts >> More** in the GUI to explore these features.

We have covered information about some of these actions in the preceding sections. The additional features are explained below.



Account Types

Account types help identify and classify the accounts being added in Securden. Proper classification comes in handy to carry out various operations such as sharing, reporting etc. Super Administrators, Administrators, and Account Managers have the privilege to add custom types, edit and delete existing ones.

When creating your own account types, you can define the fields needed for that type and decide if certain fields should be marked as 'mandatory', if any field holds default values, and so on. You can create account types for storing personal accounts only. These types will not be listed when you add work accounts.

Navigate to **Accounts >> More >> Account Types** to create new account types and to manage existing ones.

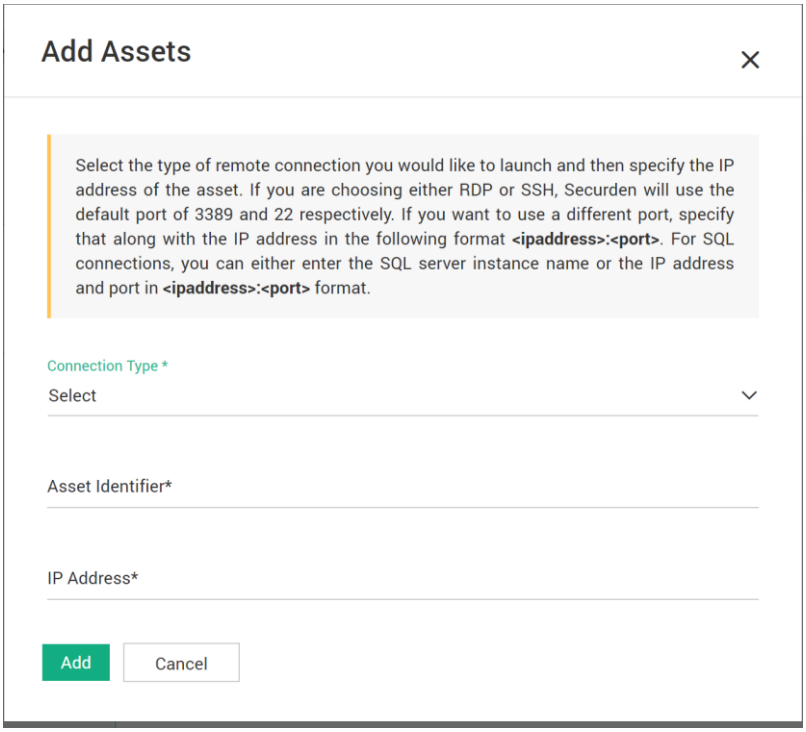
Transfer Ownership

You can transfer any account owned by you to any other user. After transferring ownership, you can't access those accounts. You will not be able to transfer the ownership of shared accounts. To transfer ownership, follow these steps:

- Select the account and navigate to **More >> Transfer ownership**
- Select the user to whom you want to transfer ownership and click 'Transfer'

Associate Assets

Asset refers to Windows machines, Linux machines, and MS SQL instances linked to a windows domain account. You can establish remote connections with assets without adding them as accounts. You have to associate them with the respective windows domain account. When you are launching the remote connection, the associated assets will be listed. To associate assets to a windows domain account, follow these steps:



- Select the account and navigate to **More >> Associate Assets**
- Select the type of remote connection you would like to launch
- Specify a that uniquely identifies the asset being added
- Then specify the IP address or DNS address of the assets. If you are going to add multiple assets at a time, then enter IP addresses or DNS addresses of assets in comma separated form.
- The default port for RDP is 3389 and SSH is 22
    - 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
      For example, 192.168.1.1:1234
- Then click 'Add' to complete the process

Associate Private Key

This feature can be used to associate an SSH key with a Unix device. After associating the key with a Unix device account, you can remotely access that device using private key authentication. You can also replace an old key with a new private key from here. To associate private key, follow these steps:

- Select the account(s) and navigate to **More >> Associate private key**
- Select the operation you want to carry out (Associate or Disassociate)
- If you select 'Associate', then all the SSH Key accounts will be listed and select the SSH key from the list.
- If you want to dissociate an already associated key, click ' Disassociate'.

Offline Access

If your administrator has permitted this option, you will be able to 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.

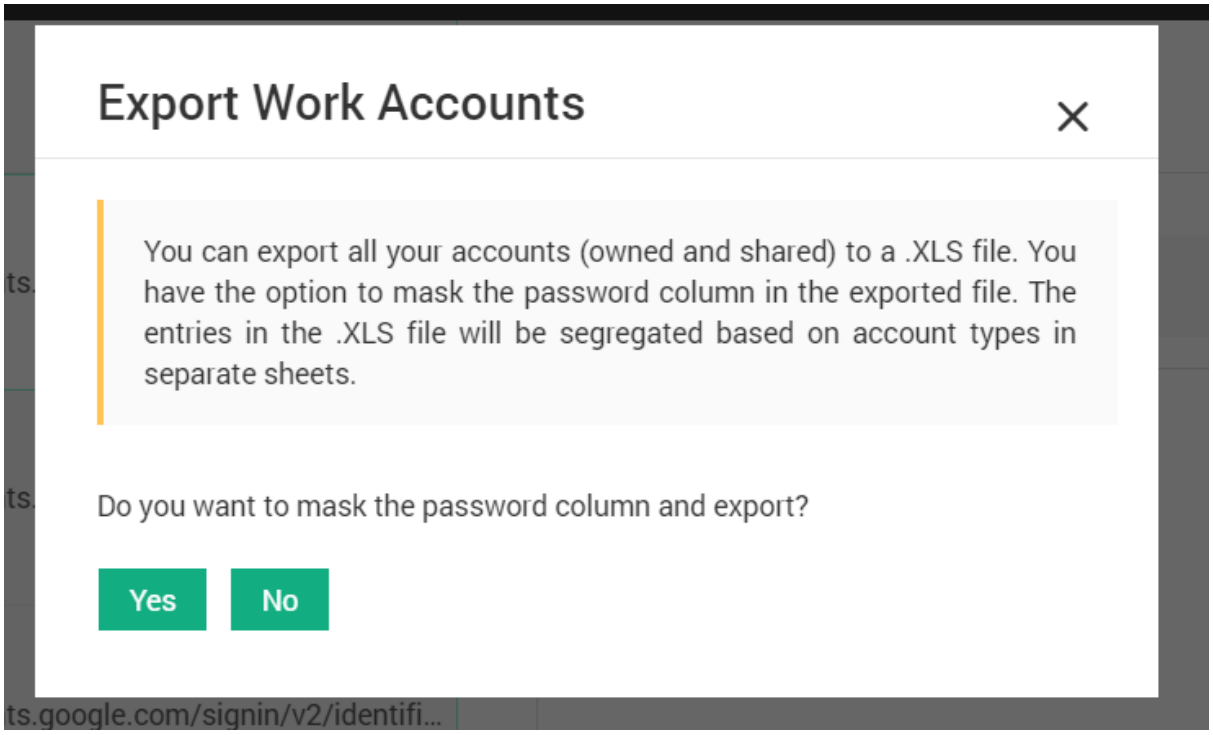
To export passwords for offline access, you need to supply a passphrase, which will be used as the encryption key. You have the option to download the offline copy anytime as needed or create a scheduled task to get the offline copy periodically through email. You can download the offline copy using this option unless your administrator restricts this option for end-users. To export an offline copy, follow these steps:

- Navigate to **More >> Offline Access** and click 'Export Now' tab
- Add a passphrase and Click 'Export offline copy now.'
- Also, you have the option to get the offline copy to your email. The accounts will be exported and sent to your email. You can get the copy for once as well as periodically through email. You have to configure it using 'Receive the copy periodically through email' tab. Enter the required details and click 'Save'.

Export Work Accounts

If you have the permission to export accounts, you can export all your work accounts you have access to as a spreadsheet. When doing so, you have the option to mask the password column in the exported file. The entries in the exported file will be segregated based on account types in separate sheets. You will not be able to use this feature if your administrator has disabled the option of exporting work accounts for end-users. Also, the password column will be masked automatically if your administrator has enabled the option of password concealing. To export work accounts, follow these steps:

- Navigate to **More >> Export Work Accounts**
- If you click 'Yes', then work accounts will be exported with all passwords masked. Otherwise, work accounts will be exported without masking the passwords.



Export Personal Accounts

You can export all your personal accounts to a Microsoft Excel file. You have the option to mask the password column in the exported file. The entries in the excel sheet will be segregated based on account types in separate sheets. To export personal accounts, follow these steps:

- To export work accounts, navigate to **More >> Export Personal Accounts**
- If you click 'Yes', then personal accounts will be exported as a Microsoft Excel file with all passwords masked. Otherwise, personal accounts will be exported with passwords in plain-text.

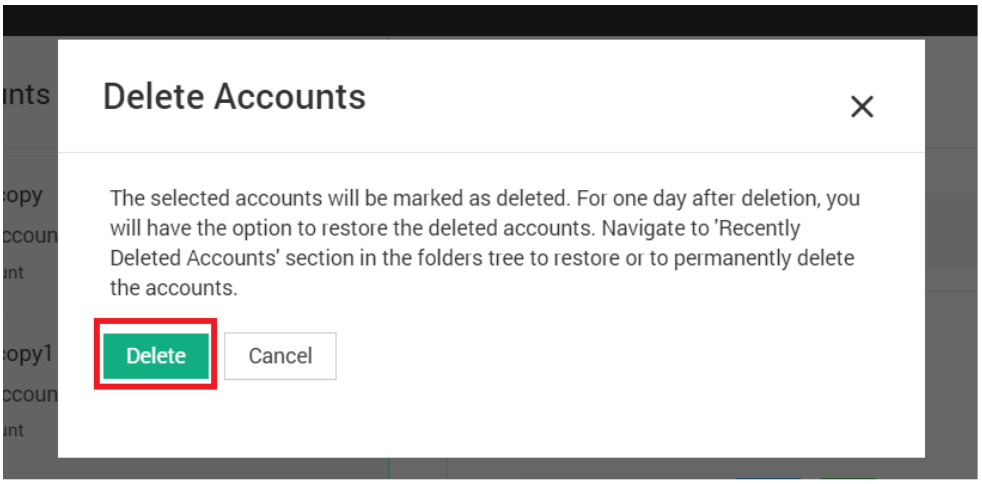
Delete Accounts

Using this option, you can delete the accounts that are owned by you (work and personal accounts). You cannot delete the shared accounts. Select the accounts that you

want to delete. If your administrator hasn't permitted deletion, you can't delete accounts.

To delete accounts, follow these steps:

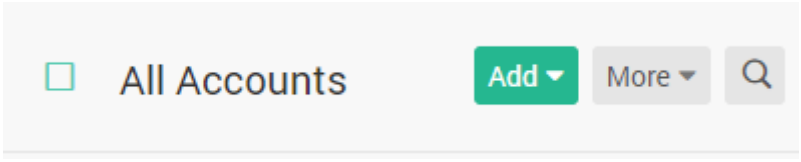
- Navigate to **More >> Delete Accounts** and click 'Delete Accounts'
- Click 'Delete' to remove selected accounts



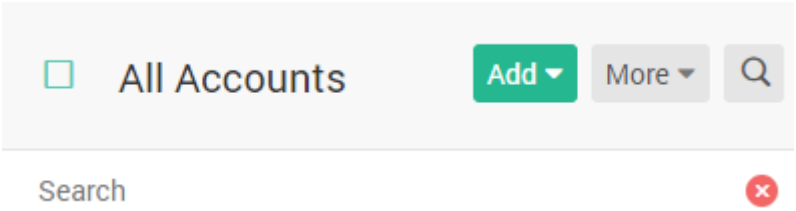
Search for Accounts

Basic Search

In the Accounts tab, you can search to locate any required account. You may use various attributes to search for the accounts using the **Search** icon.

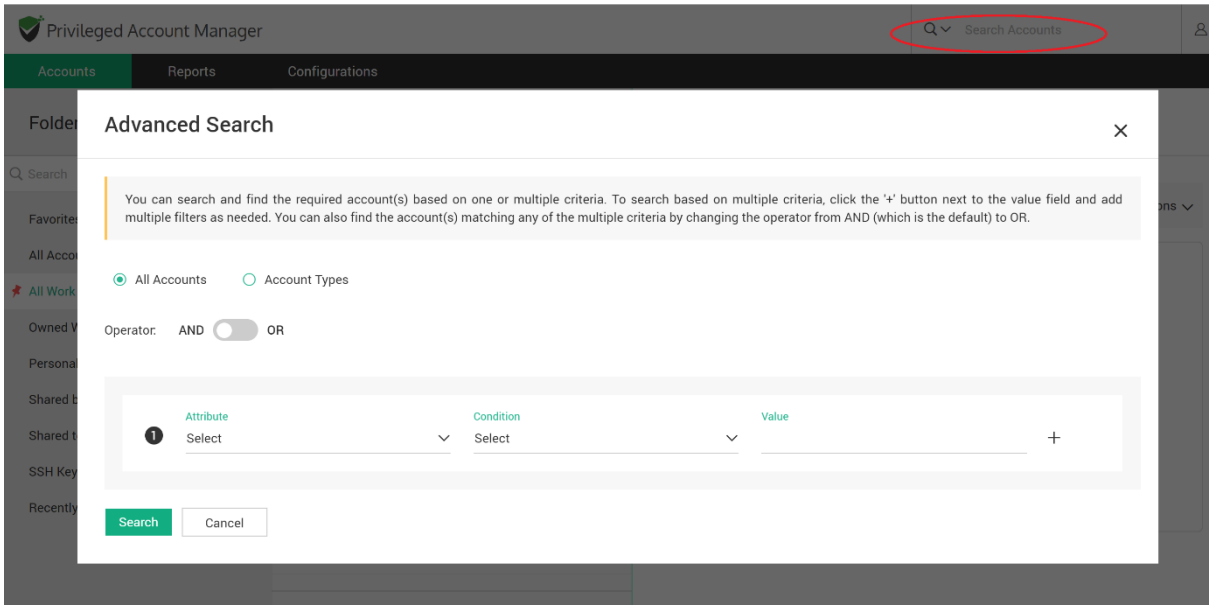


After you click on the search button, the search bar will appear below it.



Advanced Search

Advanced search involves searching and finding the required account(s) based on one or multiple criteria. Use the search field available on the top RHS for advanced search.



In the GUI that opens, to search based on multiple criteria, click the '+' button next to the value field and add multiple filters as needed. You can also find the account(s) matching any of the multiple criteria by changing the operator from AND (which is the default) to OR.

Note: The attributes that are available for filtering are determined by the account type. When you select an account type, you will find all the attributes related to that particular account type in the dropdown list. For example, an SQL server account will

have attributes like “Instance Name or IP address”, “Port”, and “Default Database”; a web account will have attributes like “URL”.

Reports

Securden carries out a comprehensive security analysis of the passwords owned by you and provides an independent strength assessment. It also ascertains if any stored passwords are found in the list of compromised passwords in various cyberattacks and provides timely alerts.

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.

Configurations

In the configurations tab, you will see the following options.

General

- **Change Password**: You can change your Securden login password here. This is applicable only for the local accounts. If you are using Active Directory authentication, the AD credentials cannot be changed from here.
- **Browser Extension:** You will find instructions for installing browser extensions here.
- **Mark as ‘Never Save’:** You can add specific URLs that are not to be stored in Securden through browser extension. When you create a new password for such websites, Securden browser extension will not prompt saving the password.

Windows Remote Launcher

- To launch RDP and other remote connections, you need to install a lightweight launcher on the machines from where Securden web interface is accessed.
- You can download the launcher from here.

Browser Extensions

Securden browser extension facilitates the auto-filling 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. Browser extensions are now available for Google Chrome, Mozilla Firefox, and Microsoft Chromium Edge browsers. The installation instructions and how to work with the extensions are available in this document.