



Help Document

Unified PAM

Mobile Application →



Index

1. Introduction.....	03
2. Getting Started.....	03
• Application Overview	
• Installation and Authentication	
3. Home Screen.....	07
4. Accounts.....	13
• Favorites	
• All Accounts	
• All Work Accounts	
• Owned Work Accounts	
• Personal Accounts	
• Shared by Me	
• Shared to Me	
• Service Accounts	
• SSH Keys	
• Folderless Work Accounts	
• Locked Accounts	
5. Access Request Approval Workflow.....	29
6. Settings.....	34
• Biometric Authentication	
• Theme	
• Offline Access	
7. Miscellaneous.....	45

Introduction

The Securden mobile application for Unified PAM is now available for both Android and iOS mobile operating systems. It enables IT administrators track, monitor, and manage privileged access on the go. Users can raise privileged access requests, configure multi-factor authentication and view the status of access requests from their mobile phones. This document provides an overview of the installation process and the features of Unified PAM available through the mobile application.

Getting Started



Application Overview

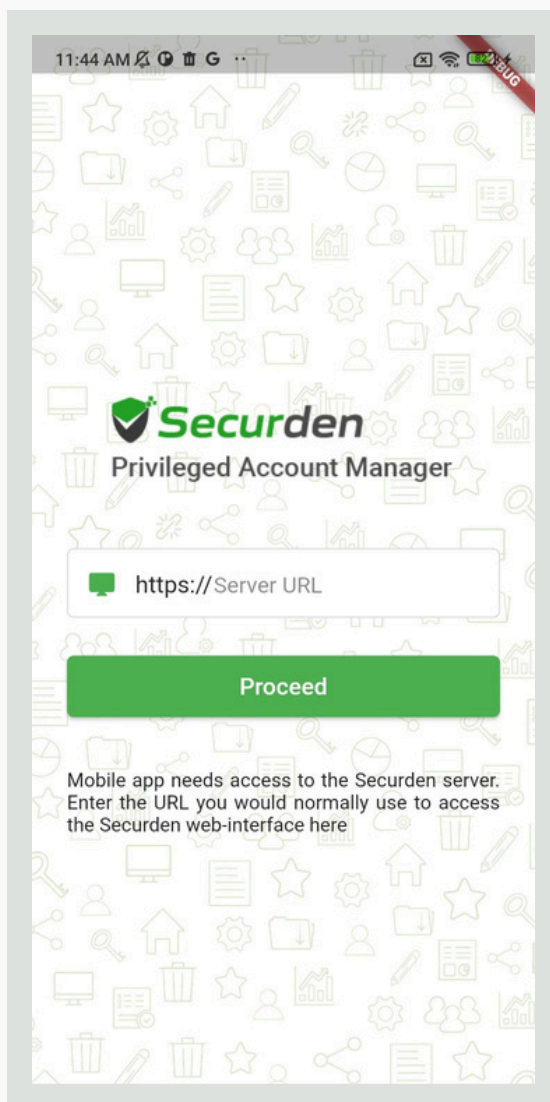
The Securden mobile application for Unified PAM is tailored for Android and iOS devices. Listed below are the hardware and software requirements for the installation of the app. The application size varies with each new update.

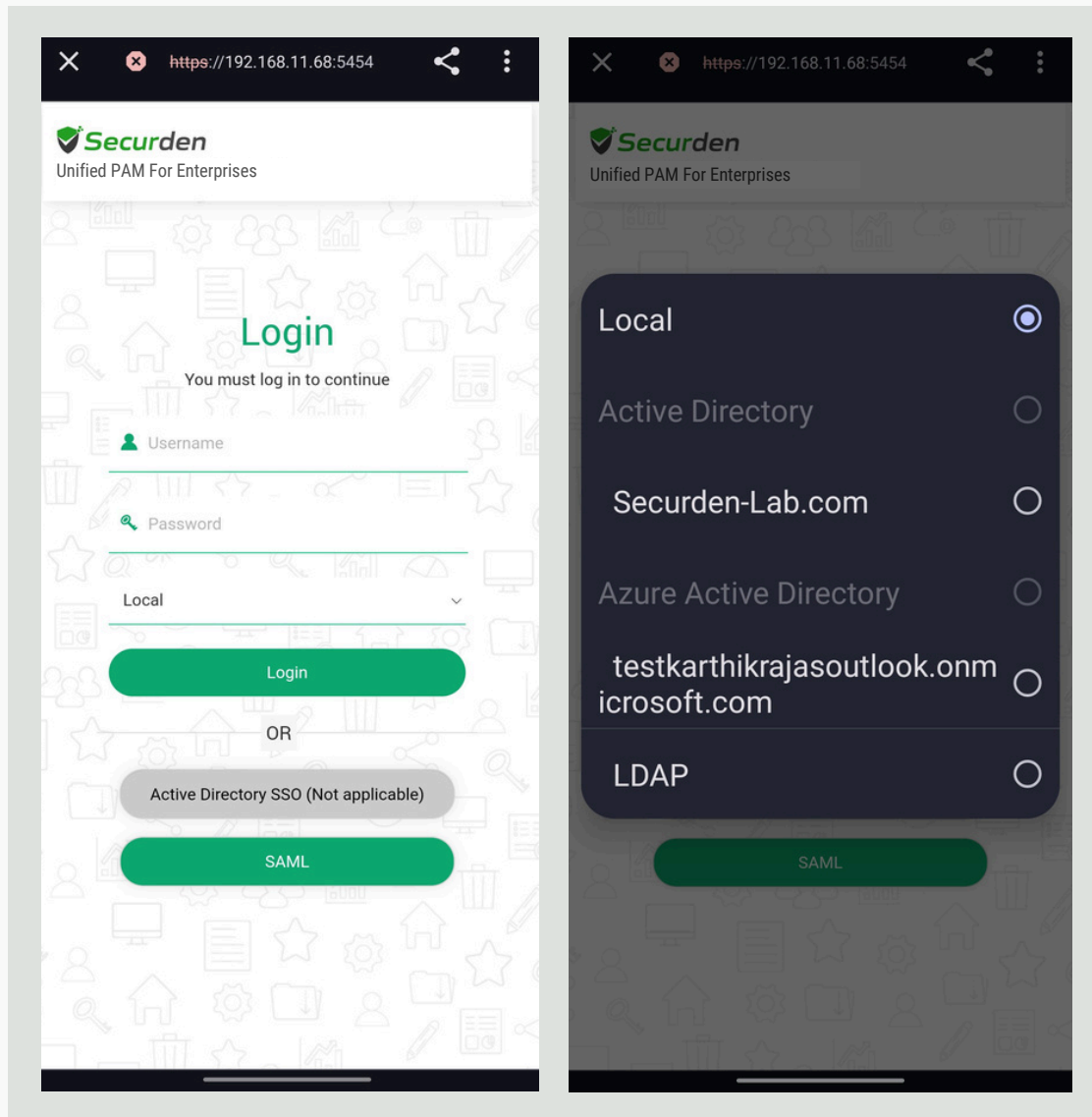
Supported Devices	All Android and iOS Devices
Compatibility	Android requires version 4.4 and above. iOS requires version 12 and above.
Language Supported	English

Installation and Authentication

1. For the Android mobile application, go to Google Play Store and search for **Securden PAM**. For the iOS application, visit the App Store and search for **Securden PAM**.
2. Download the application and install it on your mobile.
3. After installing, enter the URL of the Securden server along with the port details in order to establish connectivity between the app and the web server. The URL will typically be in this format: <https://customer-unified-pam.com:5959>

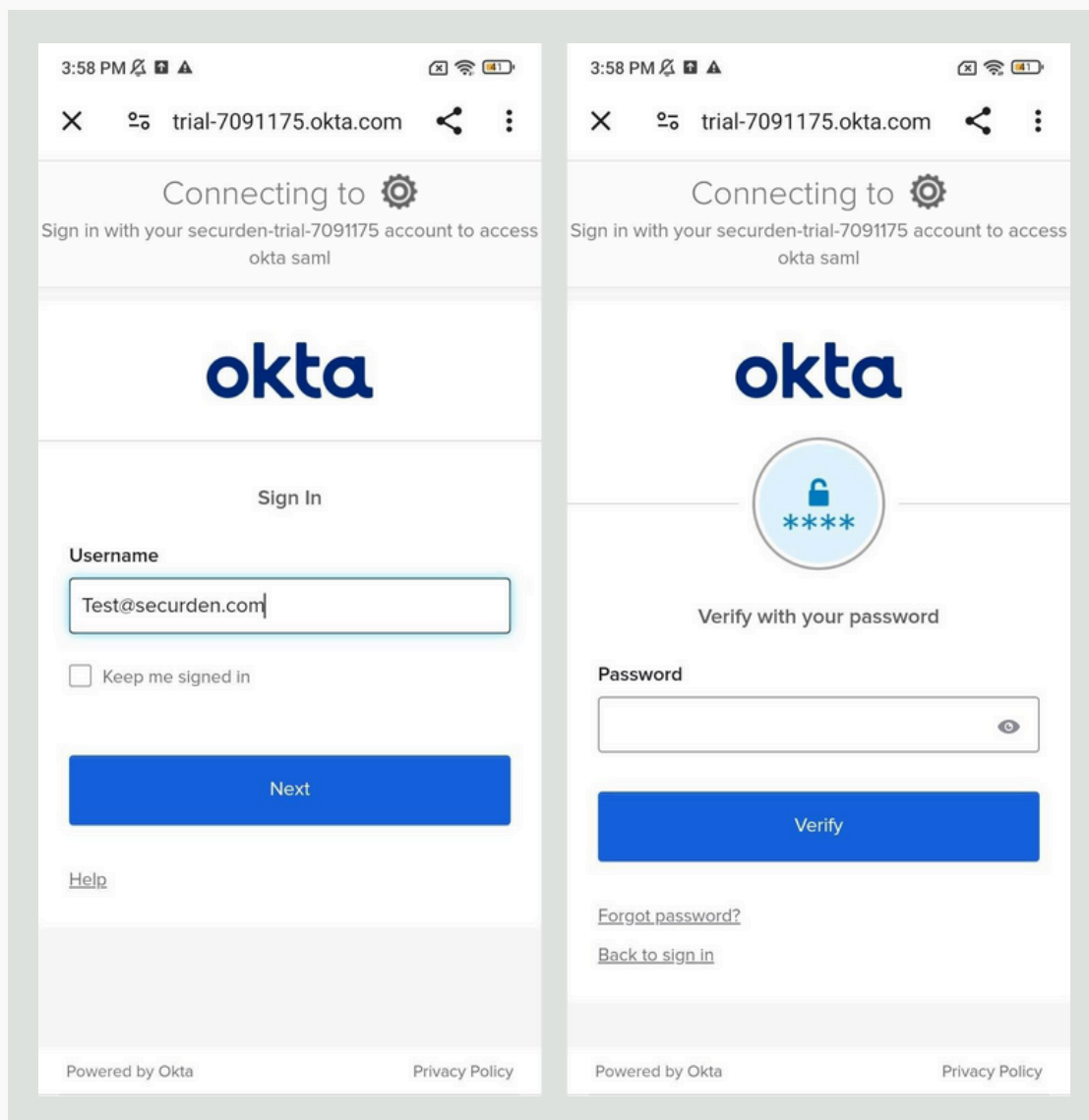
Once connectivity is established between the mobile app and the web server, you need to provide your Unified PAM login credentials to access your account. The mobile application offers various authentication methods, including Securden's native authentication, Active Directory / Azure AD / LDAP integration, and SAML.





To log in using Active Directory/LDAP credentials, choose your domain name from the dropdown list.

If SAML is enabled on your Securden server, a browser window will open within the application, where you will have to log in with the SAML credentials.



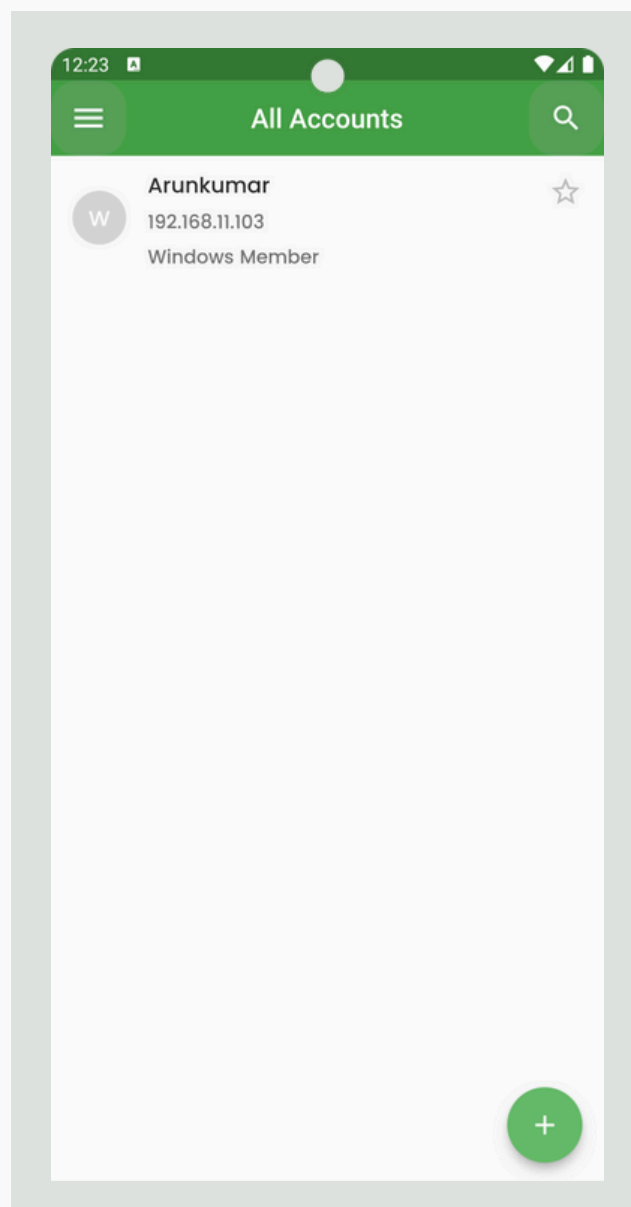
Once you log into the application using one of the above techniques, you will be taken to the home screen of the application.

Home Screen



The home screen displays a list of all accounts within the application, along with the option to add new accounts.

Once you log into your account successfully, you will see all the accounts on the home screen. When logging in as an administrator, you gain access to view all accounts within the mobile application. Whereas if you're logging in as a user, you get access to those accounts owned by you and those that are shared with you. You have the option to designate accounts as favorites by clicking on the star icon located next to the account name.



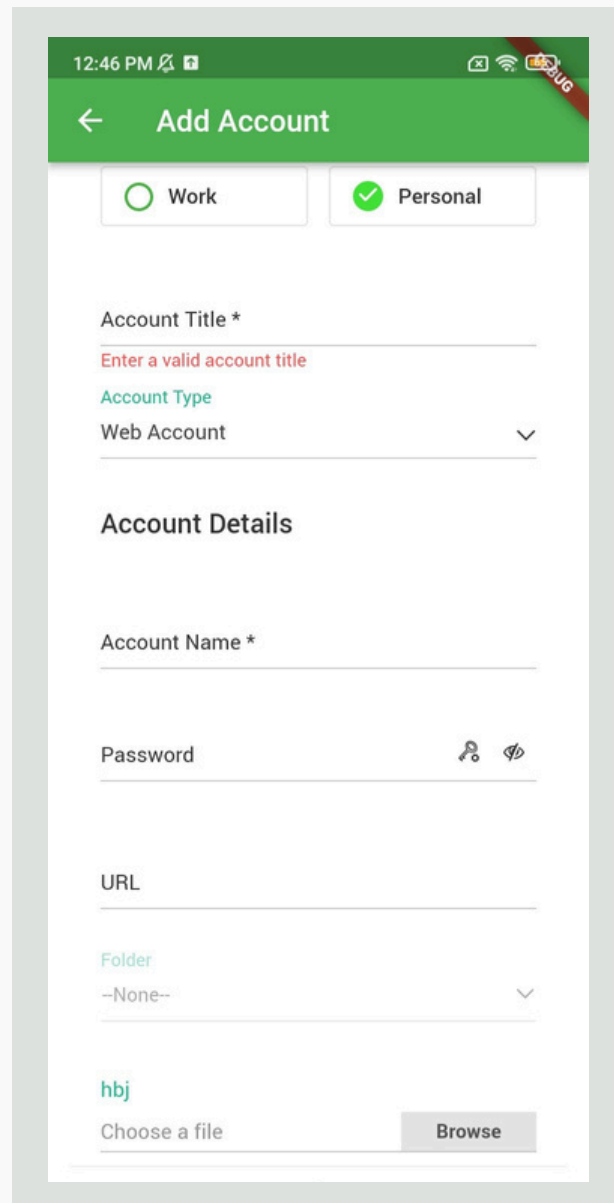
Adding Accounts

To add accounts, simply click on the '+' icon situated in the lower right corner. This action will take you to the account addition page, where you will need to input the necessary details of the account you want to add.

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.

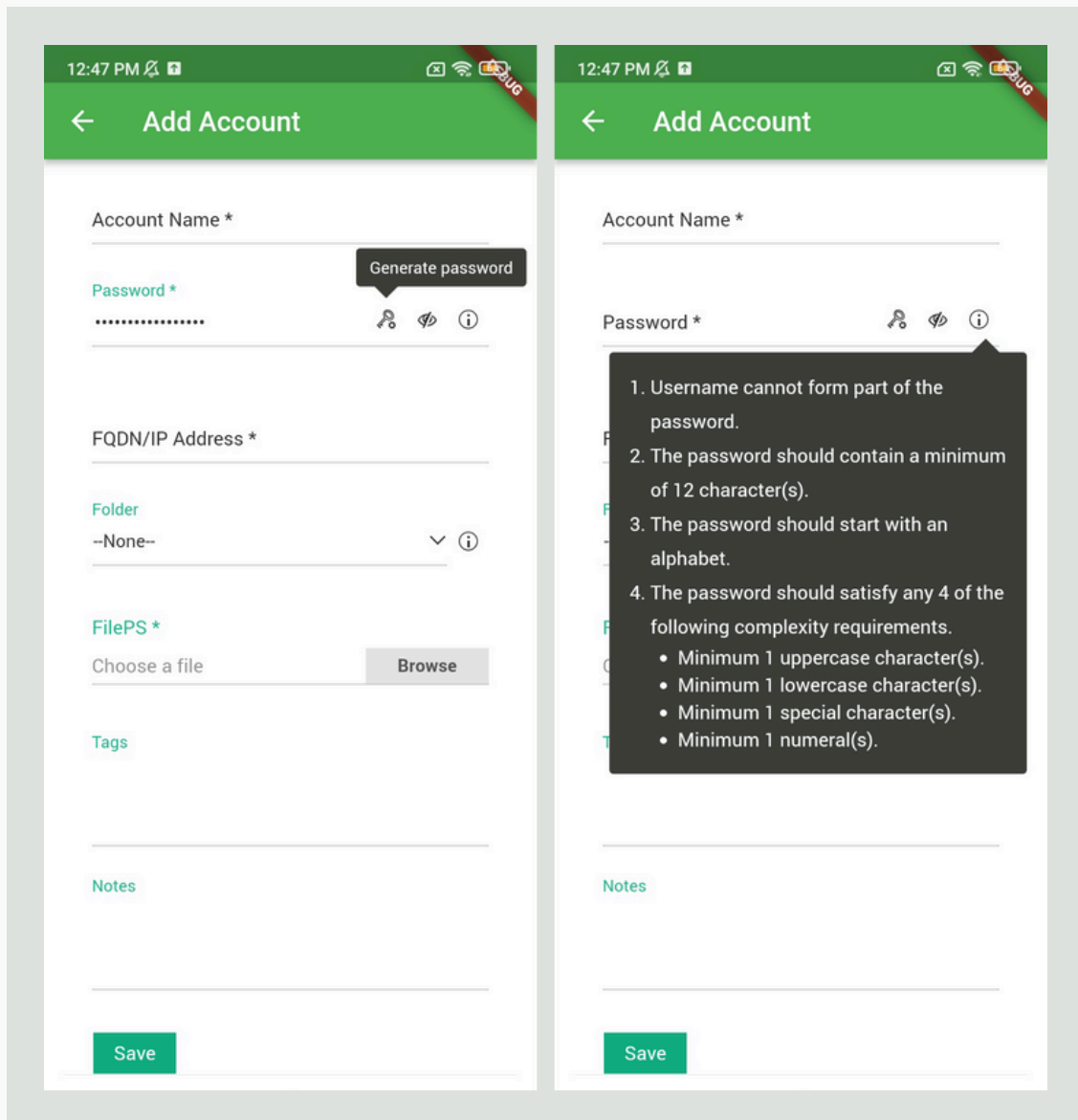
The image displays two side-by-side screenshots of the 'Add Account' mobile application interface. Both screens feature a green header with a back arrow and the title 'Add Account'. The left screenshot shows the 'Work' account type selected, with fields for 'Account Title', 'Account Type' (Windows Member), 'Account Details' (Account Name, Password, FQDN/IP Address, Folder, Tags), and a 'Save' button. The right screenshot shows the 'Personal' account type selected, with fields for 'Account Name', 'Password', 'FQDN/IP Address', 'Folder', 'Tags', 'Notes', and a 'Save' button.



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 password of the account if it already exists or create a new one. Once done, you have the option to set up automatic password rotation and scheduled password resets for the established password using Securden.

Select the 'generate password' icon within the password field to automatically create a password that adheres to the complexity requirements and password policies specified for the respective account. Click on the information icon within the password field to view the complexity requirements designated for that account.



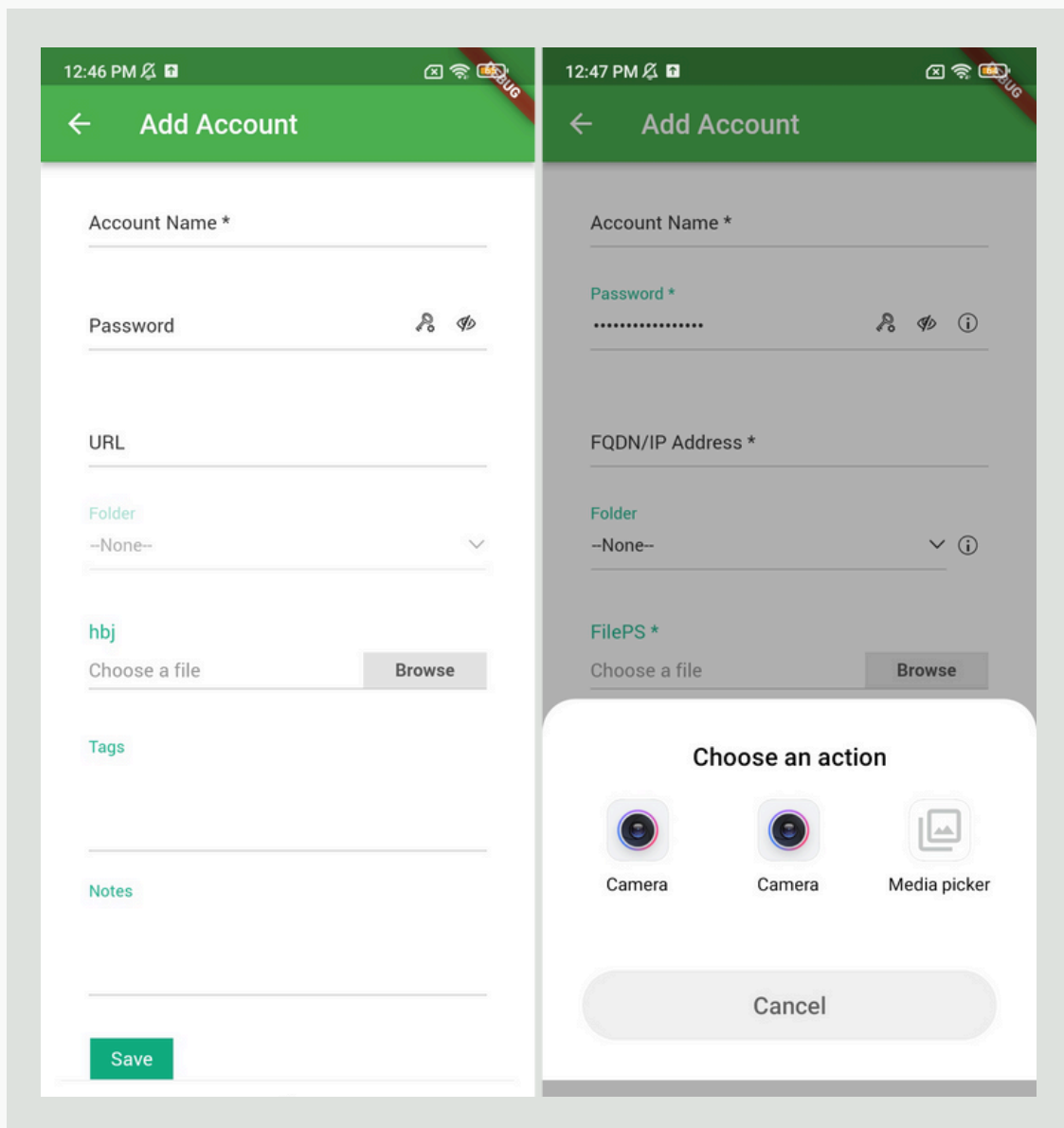
- **Folder:** If you want to add this account to a folder, you can select one of the existing folders in Securden or add a new folder by clicking on the Add folder option from the drop down.

Note: Folders that are shared to the users with 'view' permission are either not shown or shown disabled in the dropdown for adding accounts.

The screenshot shows the 'Add Account' screen in the Securden mobile application. At the top, there is a green header with a back arrow and the title 'Add Account'. Below the header, the form contains several input fields: 'Account Name *', 'Password *' (with icons for password management), and 'FQDN/IP Address *'. A dropdown menu for 'Folder' is open, showing '-None--' and a tooltip that reads: 'Folders shared with 'view' permission are either not shown or shown disabled here for adding accounts. Contact administrator for details.' Below the folder dropdown, there are sections for 'Tags' and 'Notes', each with a text input field. At the bottom of the form is a green 'Save' button.

- **File:** You can browse and select a file from your mobile device to attach with the account. Click on the 'Browse' button to add files from your mobile. When additional information needs to be stored alongside the

creation of an account, attaching a file can be beneficial. When sharing the account to others, the attached file is also shared.



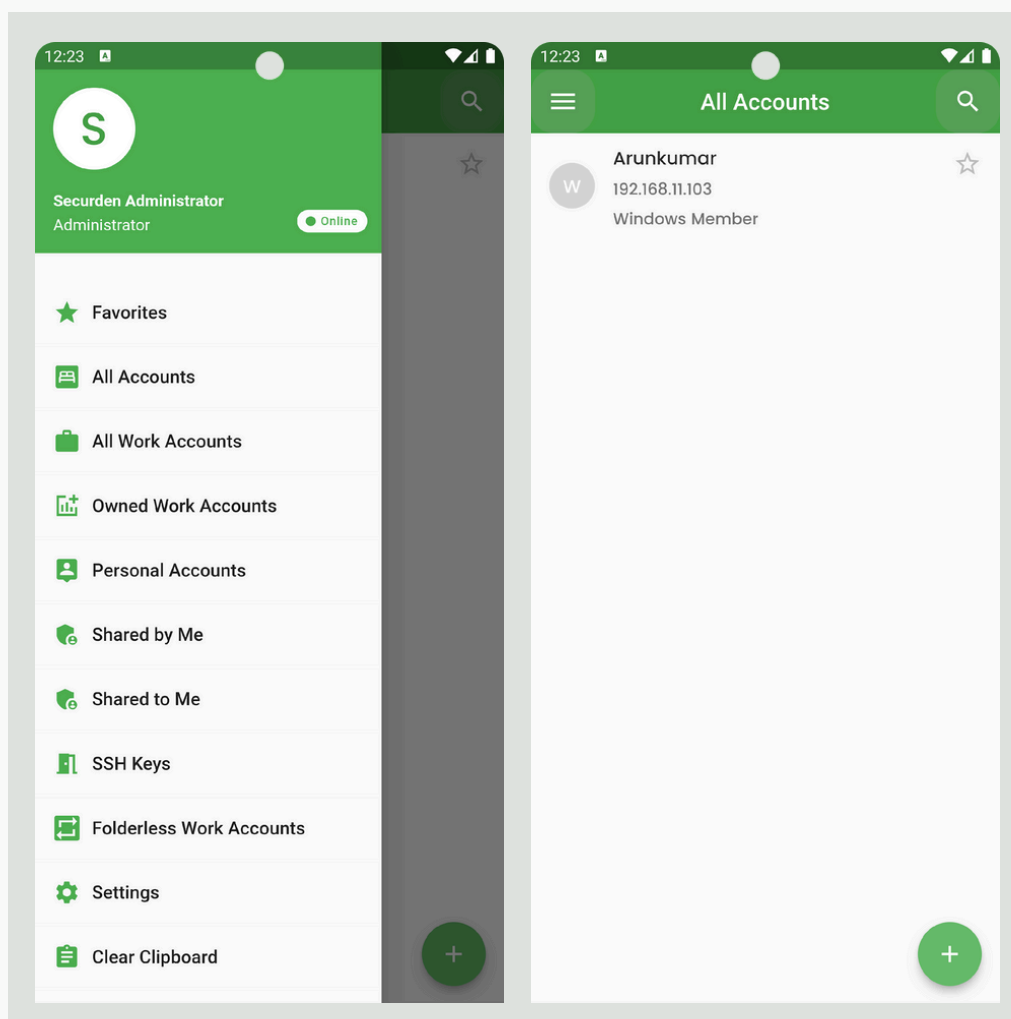
- **Notes and Tags:** You can add notes and tags to accounts for easy identification and management. When you want to search for accounts, content in notes / tags will come in handy.

Once you've added all the details, click Save. The account is added to Securden and you can now share or perform various password management operations on the account.

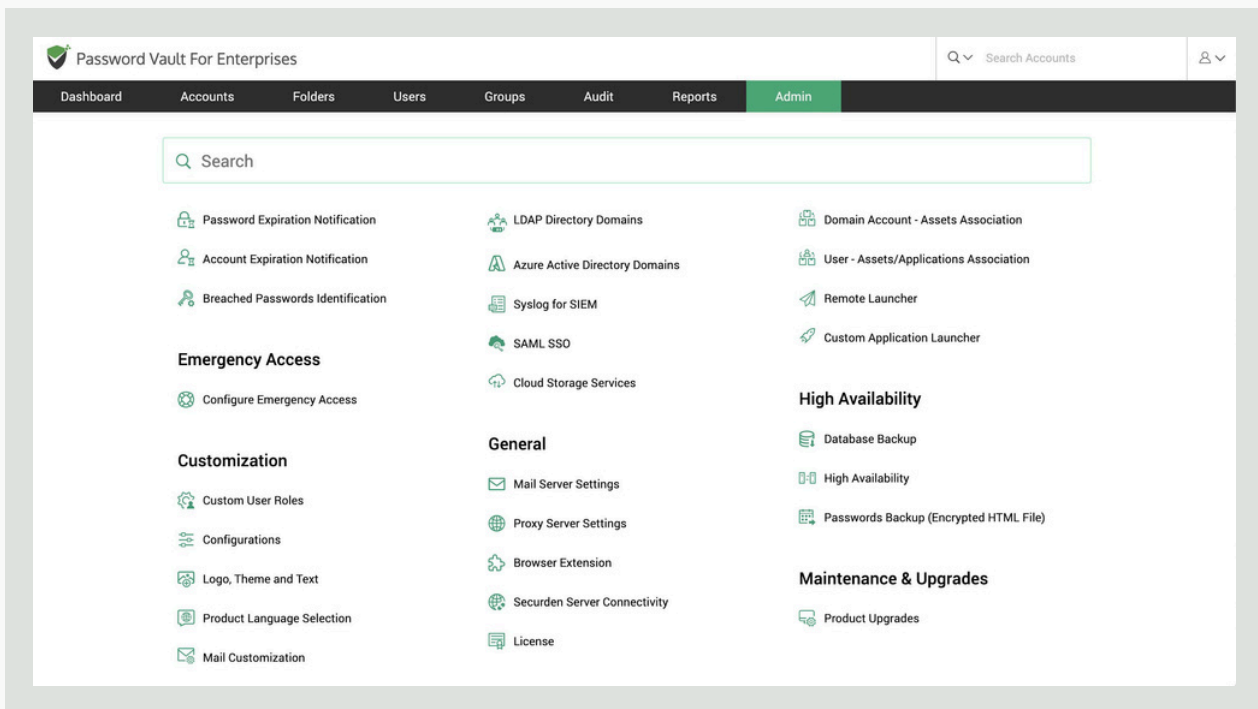
Accounts

To view the list of accounts present in the Password Vault application, click on the hamburger icon towards the top left corner of the Home Screen. It opens the navigation menu. You will find the following accounts listed -

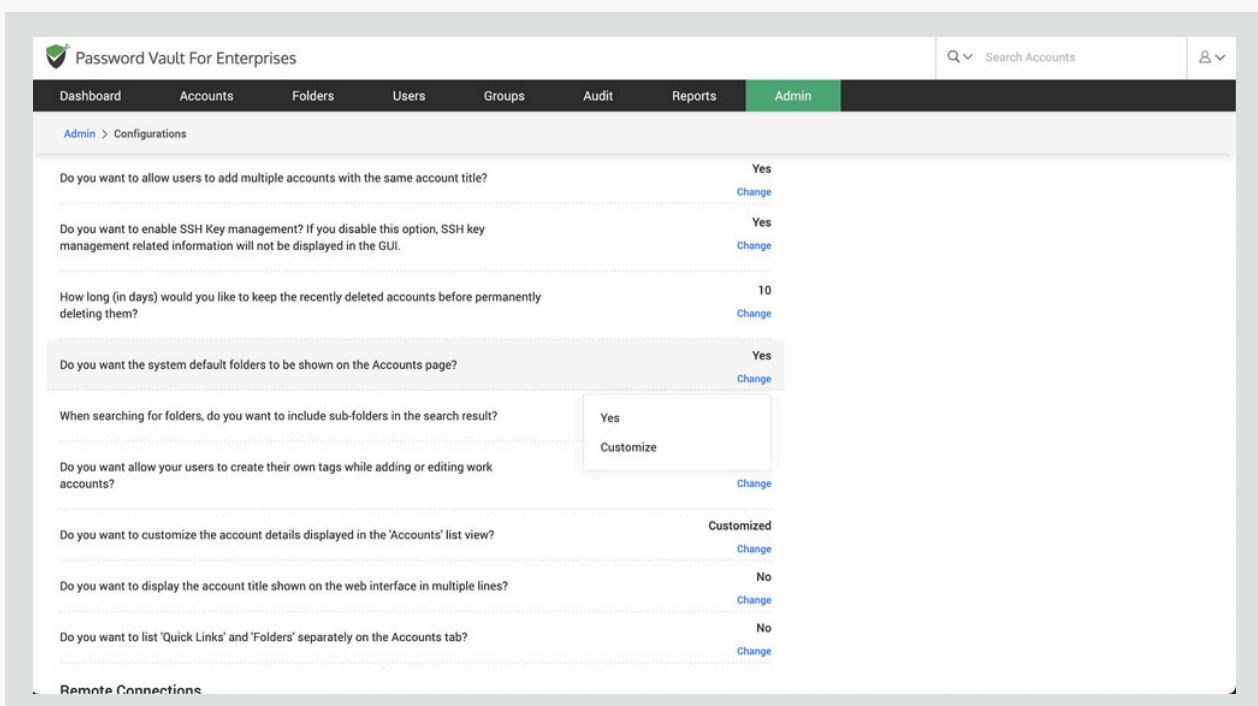
- Favorites
- All Accounts
- All Work Accounts
- Owned Work Accounts
- Personal Accounts
- Shared by Me
- Shared to Me
- Service Accounts
- SSH Keys
- Folderless Work Accounts
- Locked Accounts



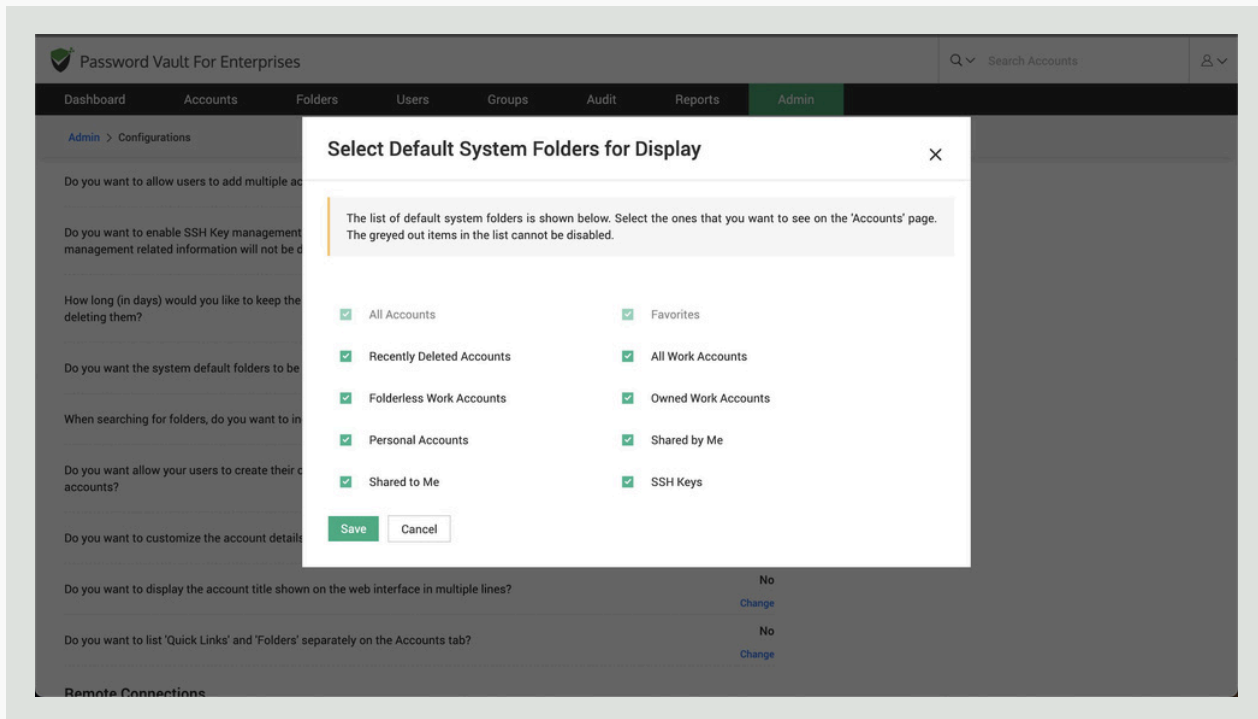
Note: You have the flexibility to customize the options displayed in the Navigation Menu in the Password Vault web UI. Navigate to Admin >> Configurations >> Account Management.



Locate the question 'Do you want the system default folders to be shown on the Accounts page?', click on 'Change' and choose 'Customize'.

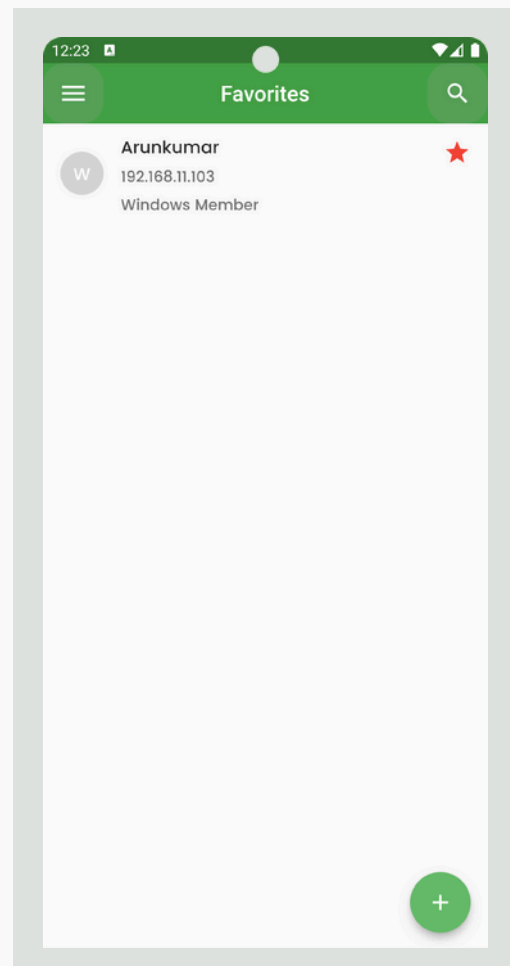


A pop-up box will appear displaying a list of options to be shown on the 'Accounts' page. Select your desired options and then click 'Save.' The chosen options will then be visible in the Navigation Menu of the mobile application.



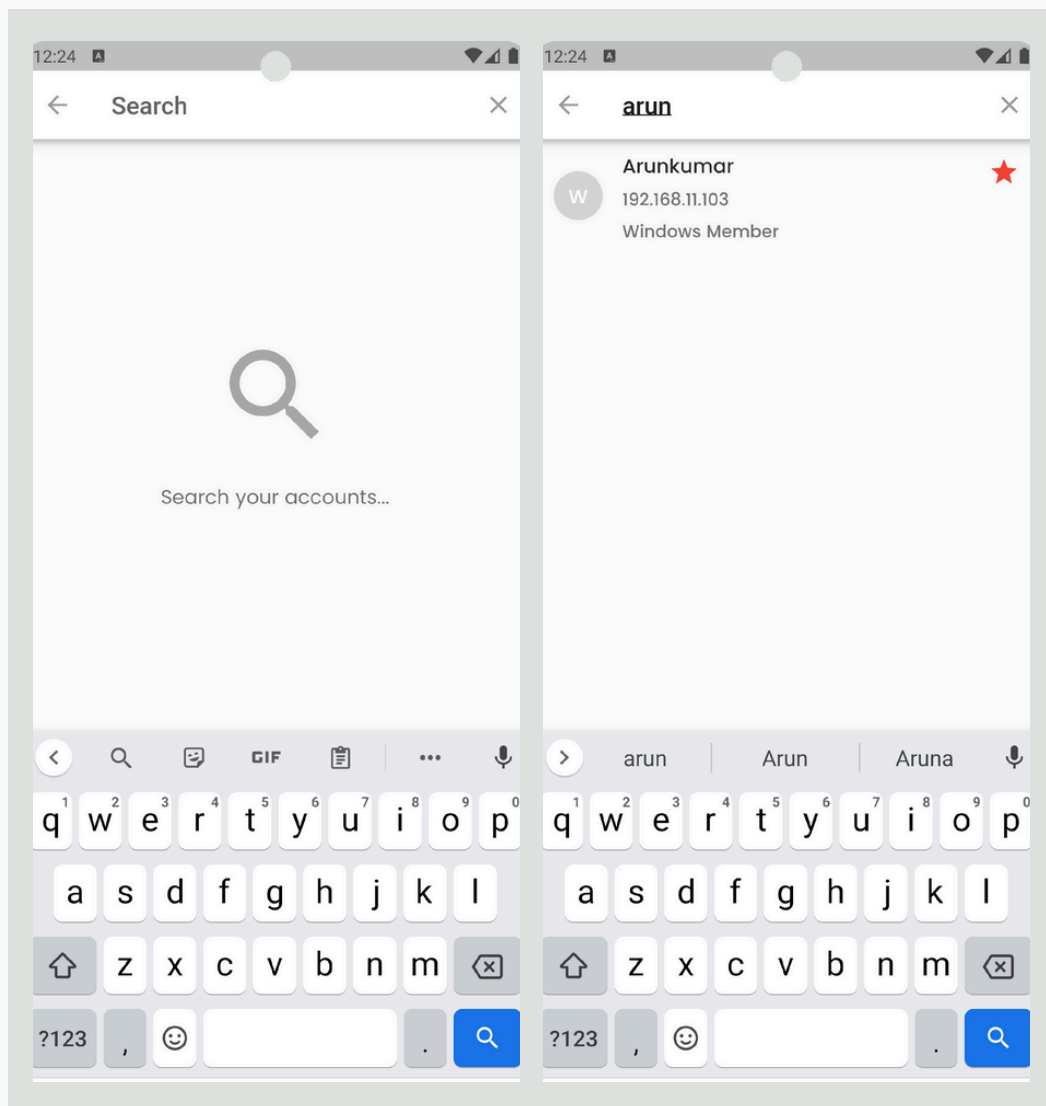
Favorites

Select the 'Favorites' tab located in the Navigation Menu to access the list of accounts categorized as favorites.

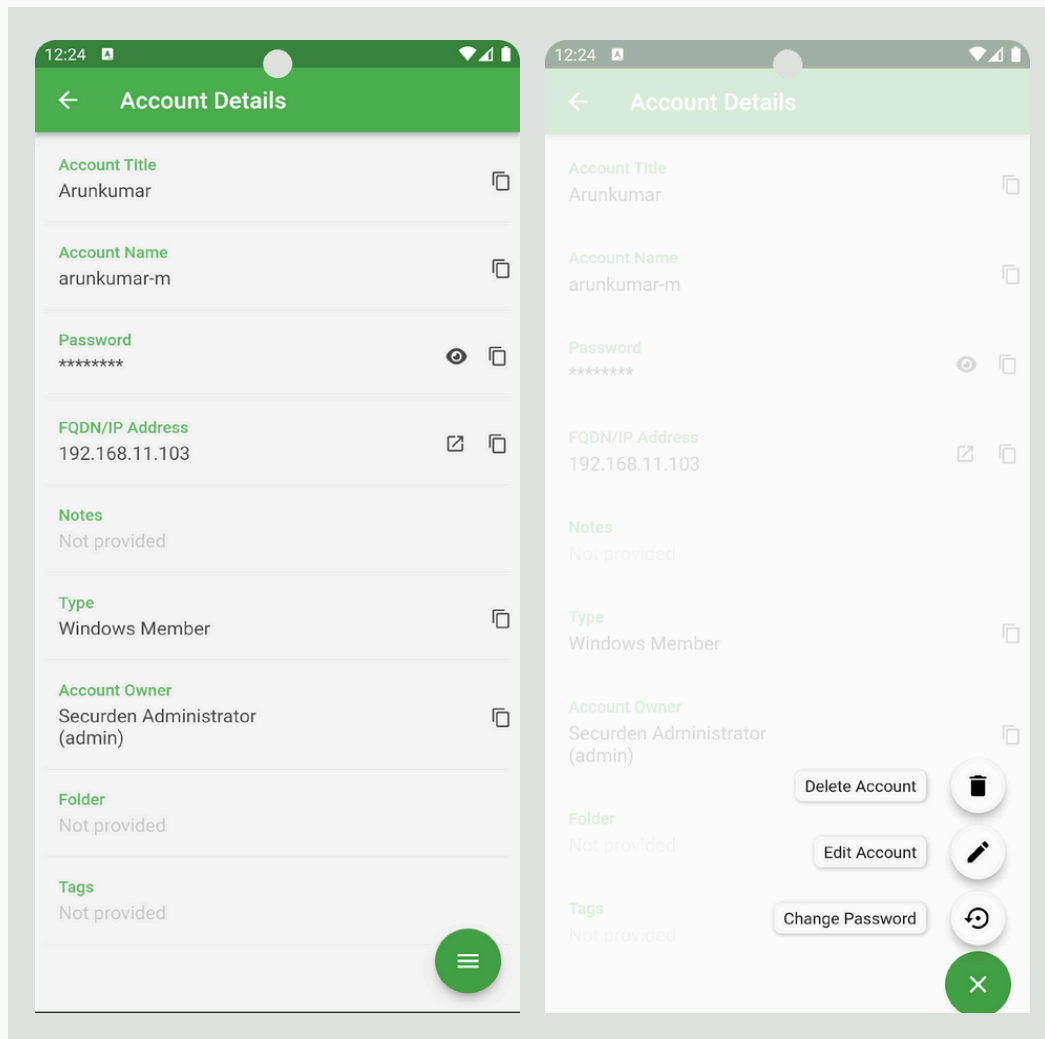


All Accounts

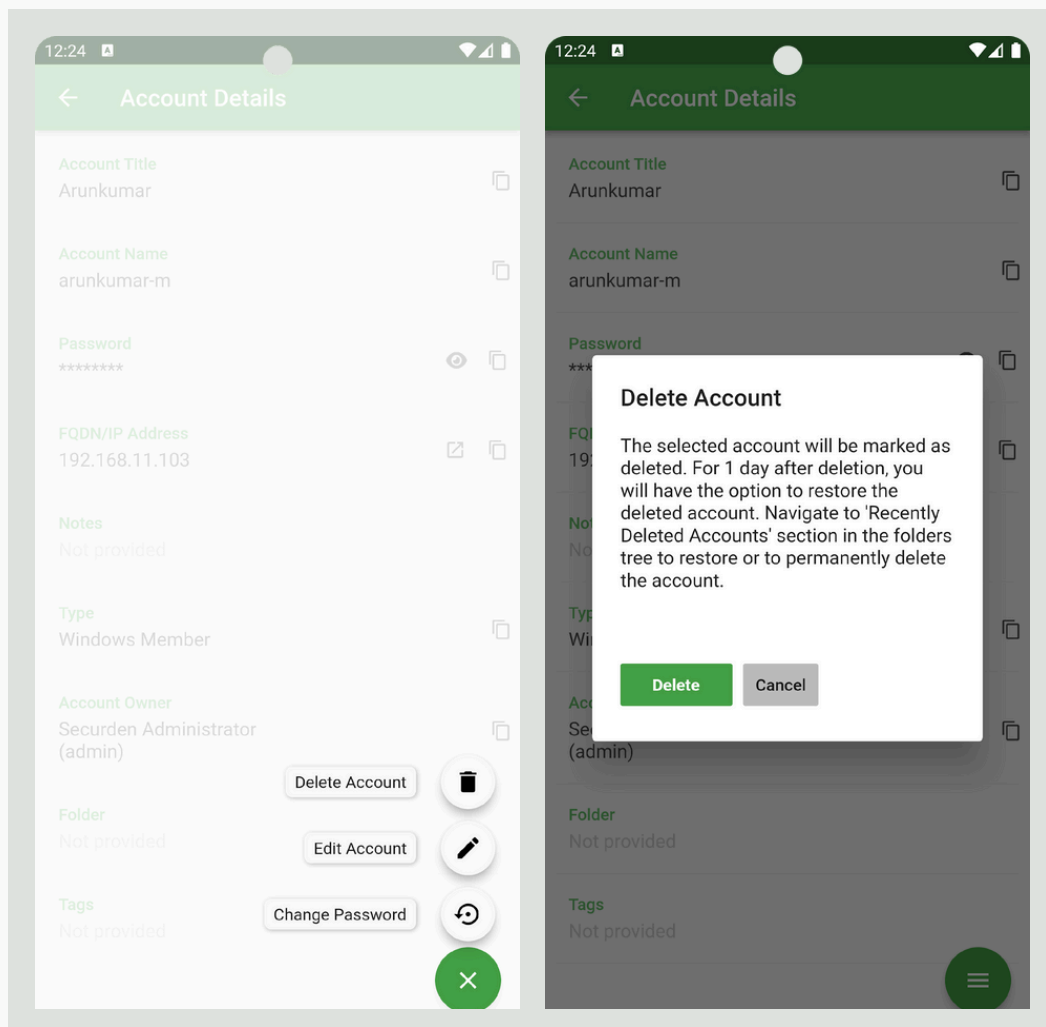
Click on the 'All Accounts' tab present on the Navigation Menu to see the list of all accounts present in the password vault. You can search for specific accounts with account names, and also view the account details by clicking on each individual account.



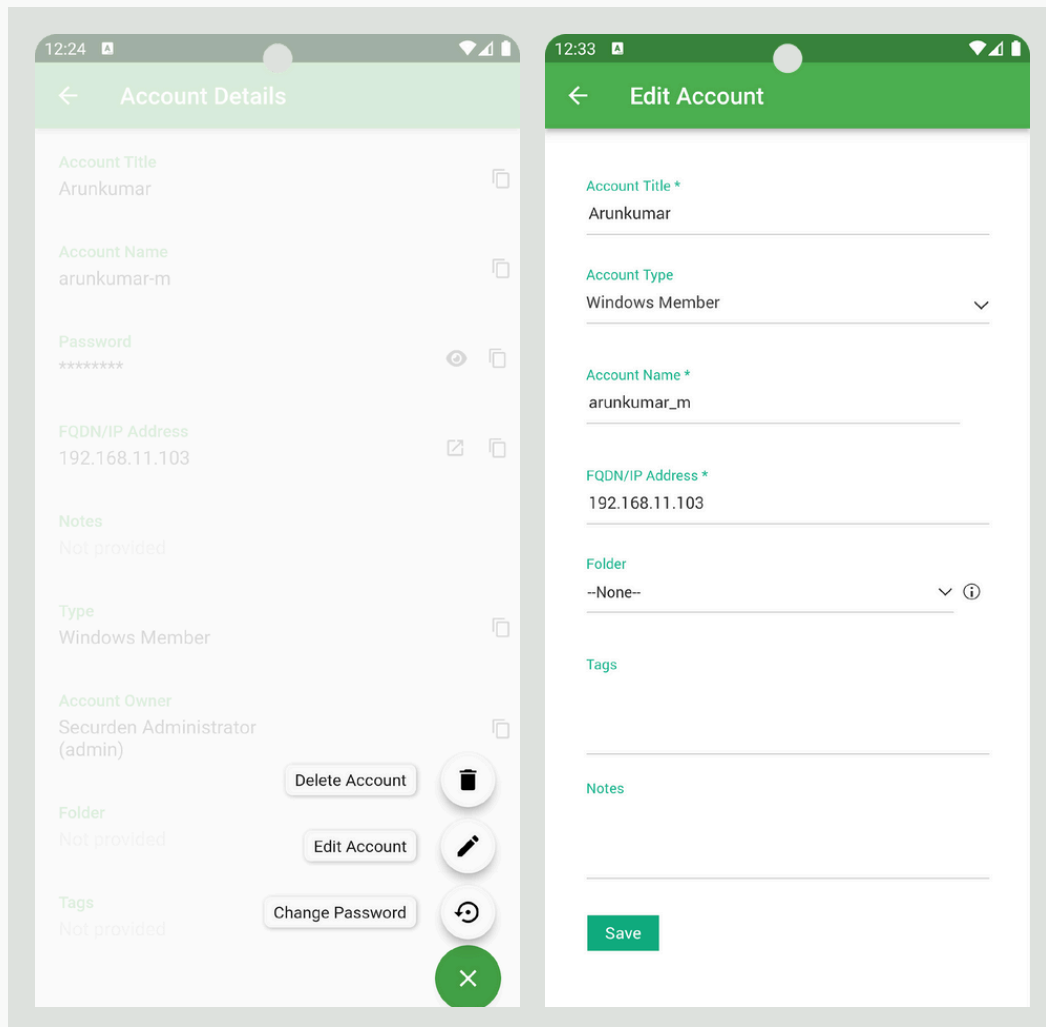
If the account is shared with view permissions, you can view the password of the accounts by clicking on the eye icon. You can also copy the account credentials to your clipboard by clicking on the copy icon present on each field. The hamburger icon situated in the lower right corner of the 'Account Details' page shows the options for deleting, editing, and changing the password of the account.



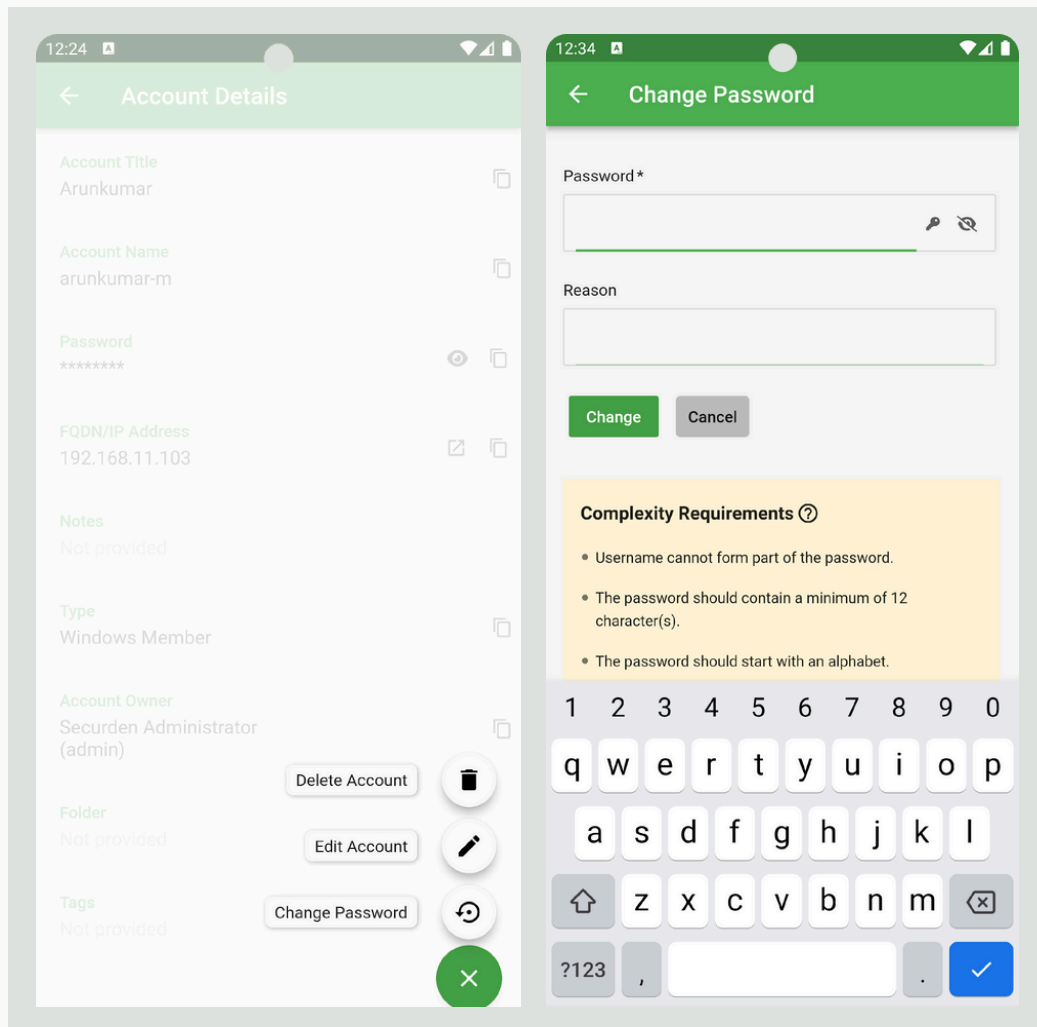
Click on the '**Delete Account**' option to delete the account from the application. You can choose to restore the account or permanently delete the account by navigating to 'Recently Deleted Accounts' section present in the folders tree.



Select the '**Edit Account**' option to modify account details such as the account title, type, name, and other relevant information. Then, click '**Save**' to confirm and save the edited details.

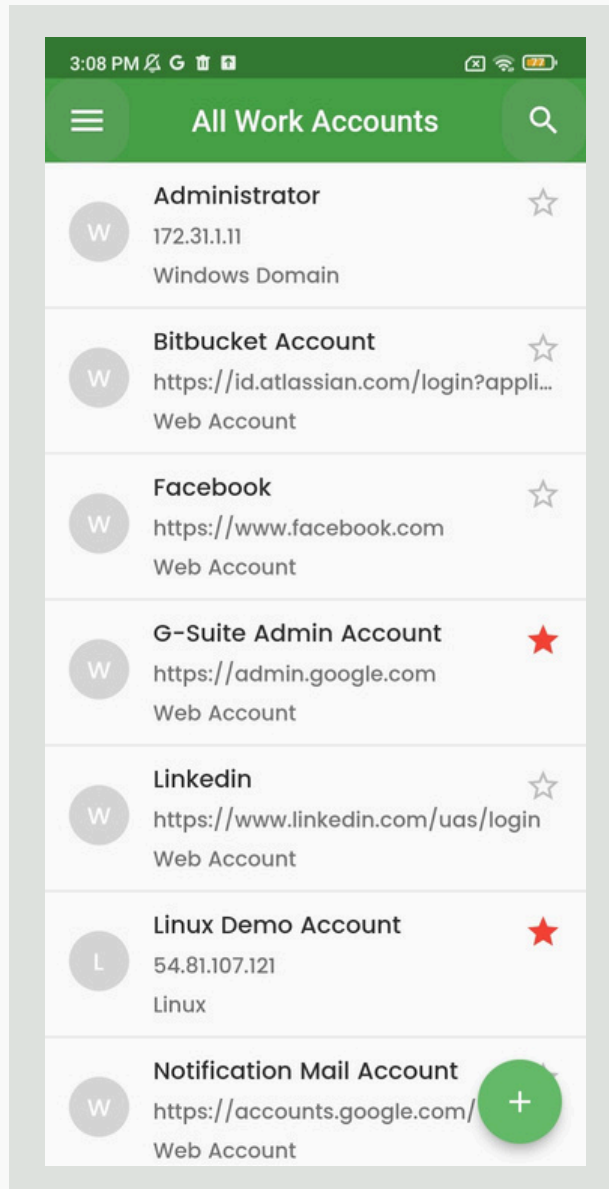


The 'Change Password' option lets you change the password of the selected account. While changing the existing password, it is mandatory that you justify the reason for changing. It is to be noted that the new password to be set matches the complexity requirements defined for that account.



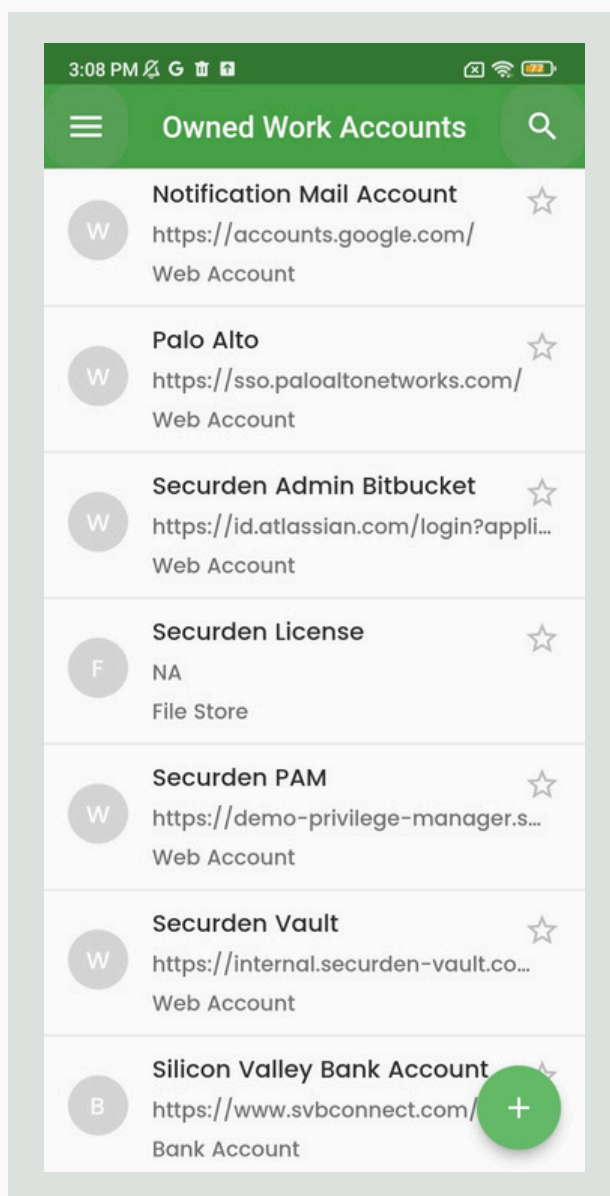
All Work Accounts

Under 'All Work Accounts' section, you get to see the list of all work accounts present in the application.



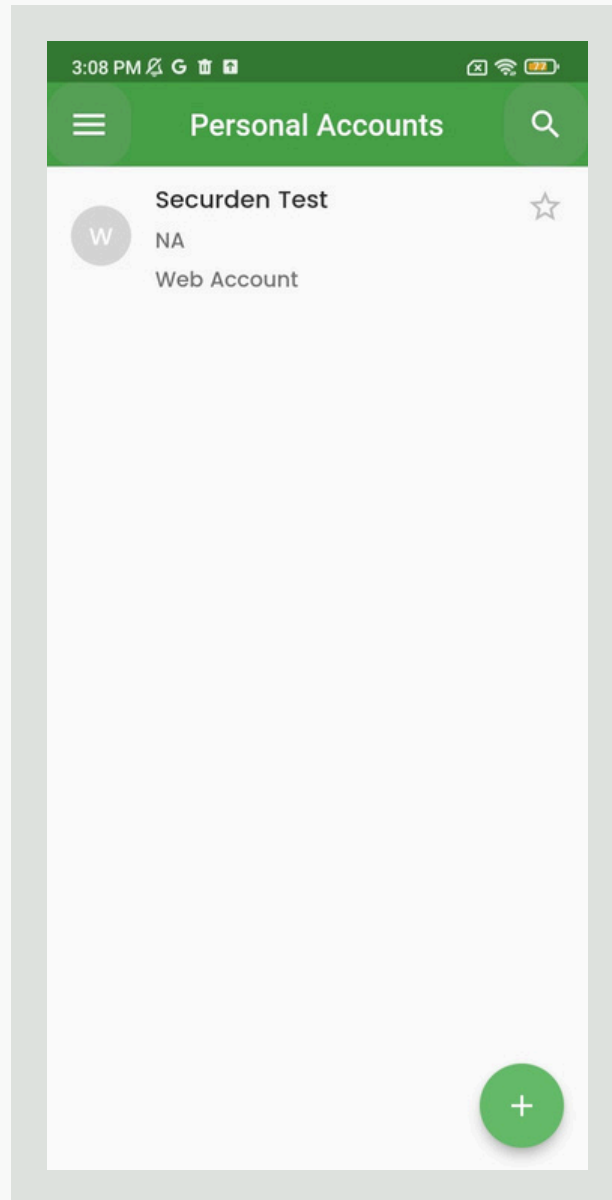
Owned Work Accounts

This section lists the total number of work accounts that are created by the logged in user.



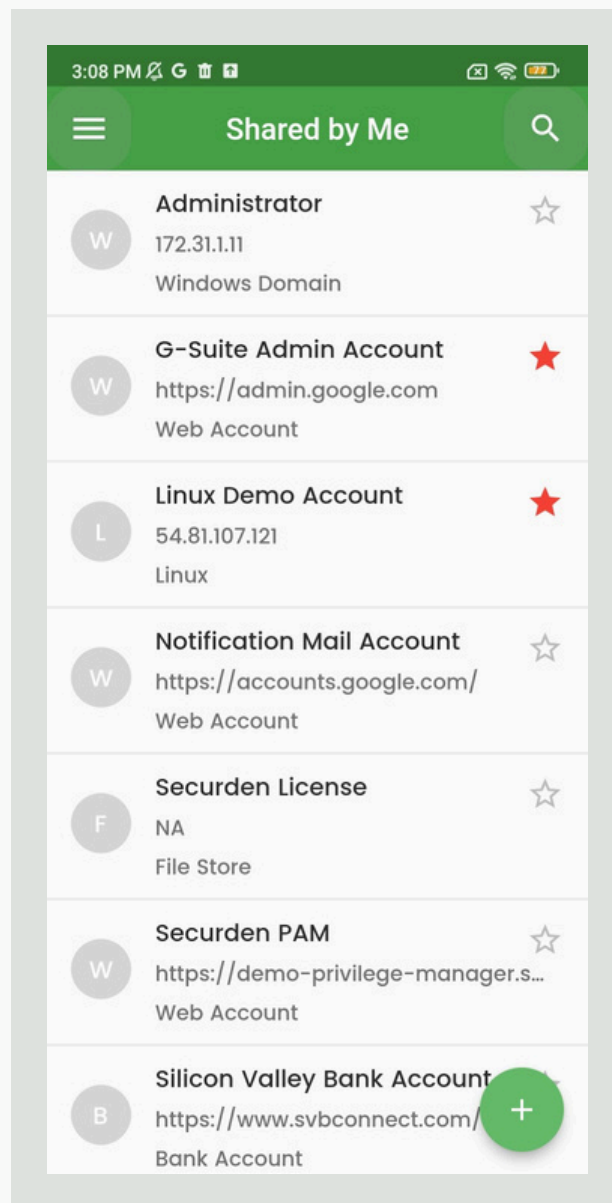
Personal Accounts

This section lists the total number of personal accounts present in the application.



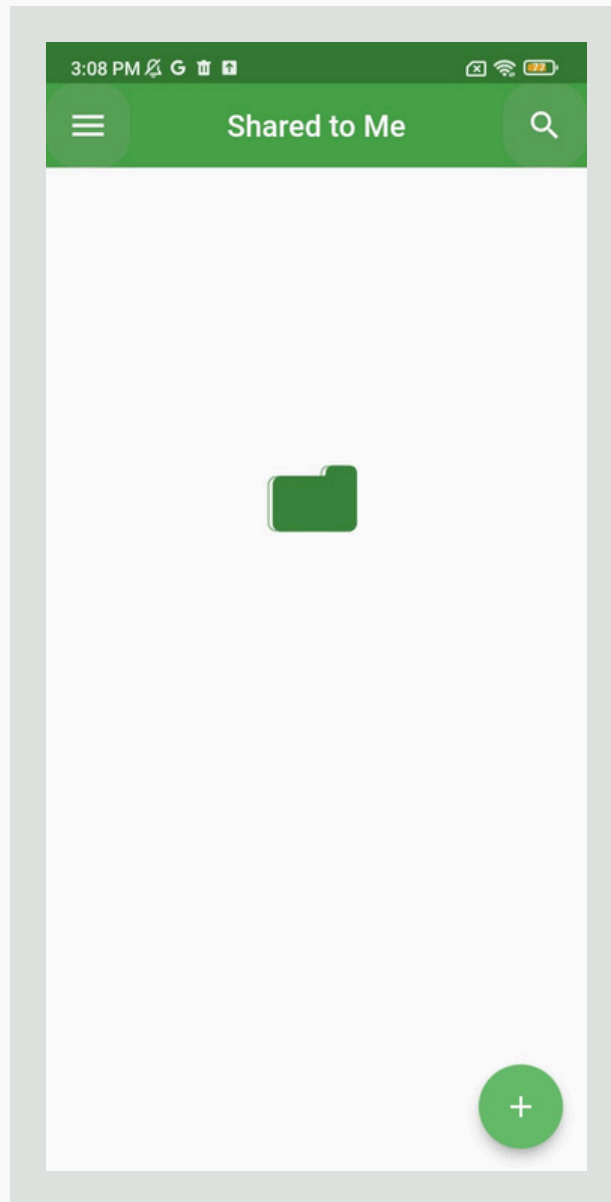
Shared by Me

This section lists the accounts that are shared to others by the logged in user.



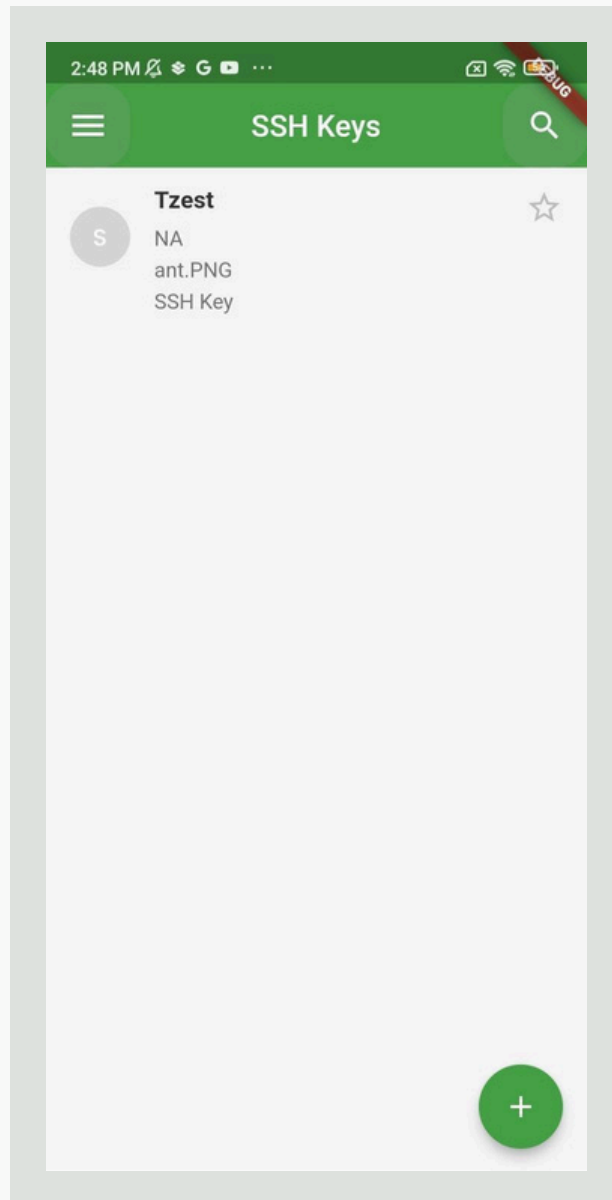
Shared to Me

This section lists the accounts that are shared by others to the logged in user.



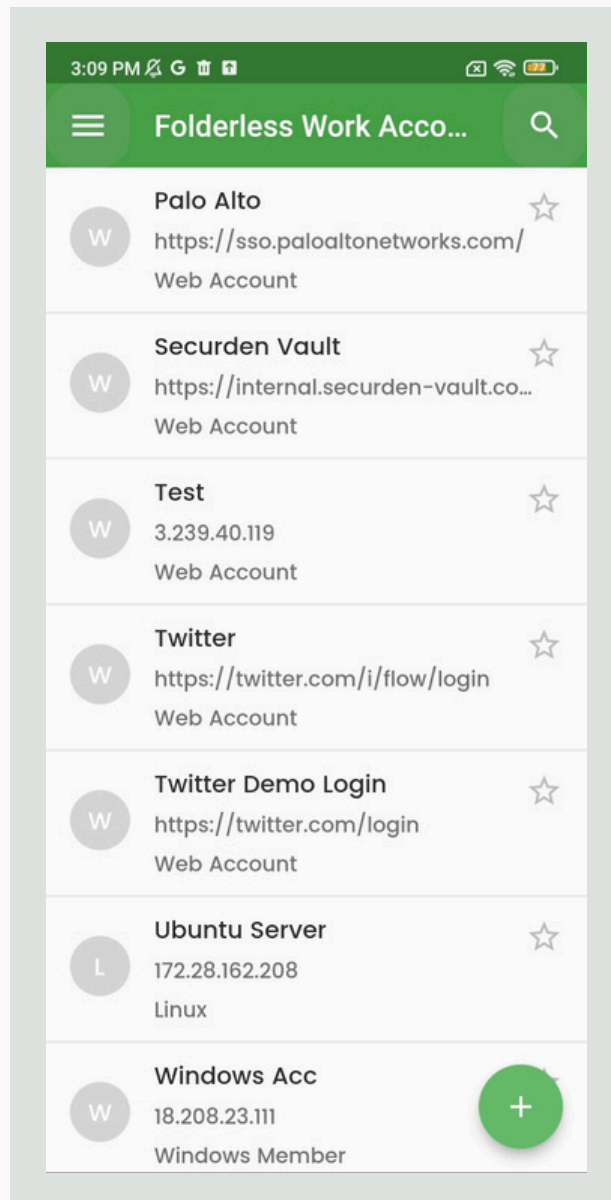
SSH Keys

Click on the 'SSH Keys' tab present on the navigation menu to view the list of SSH keys that you manage in the password vault application.



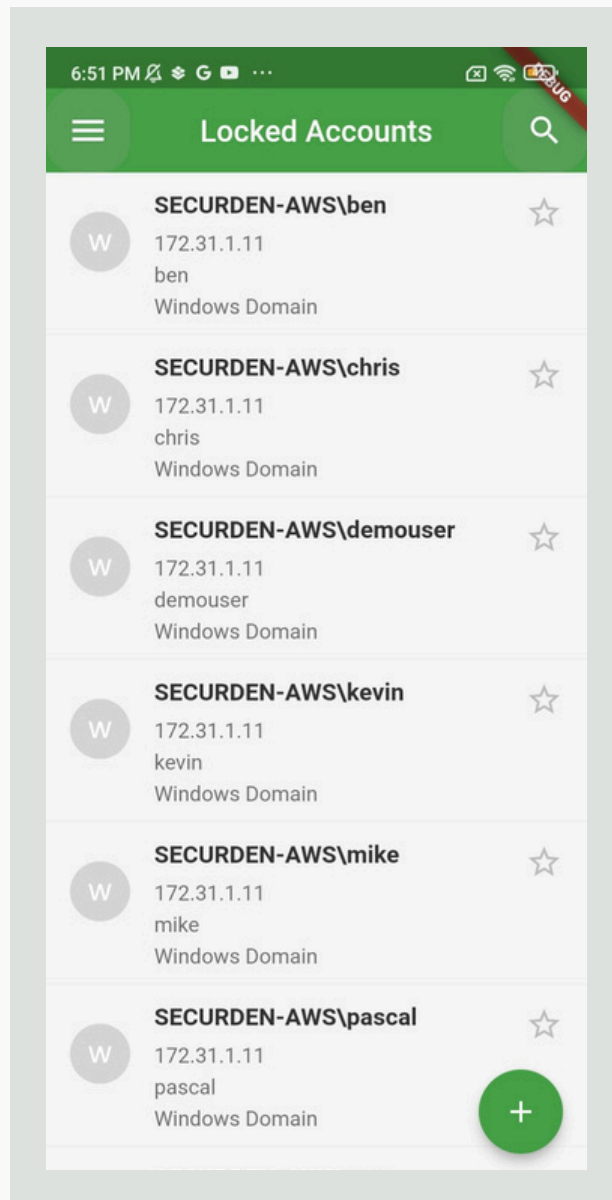
Folderless Work Accounts

In this section, you will see the list of accounts that are not associated with any folders.



Locked Accounts

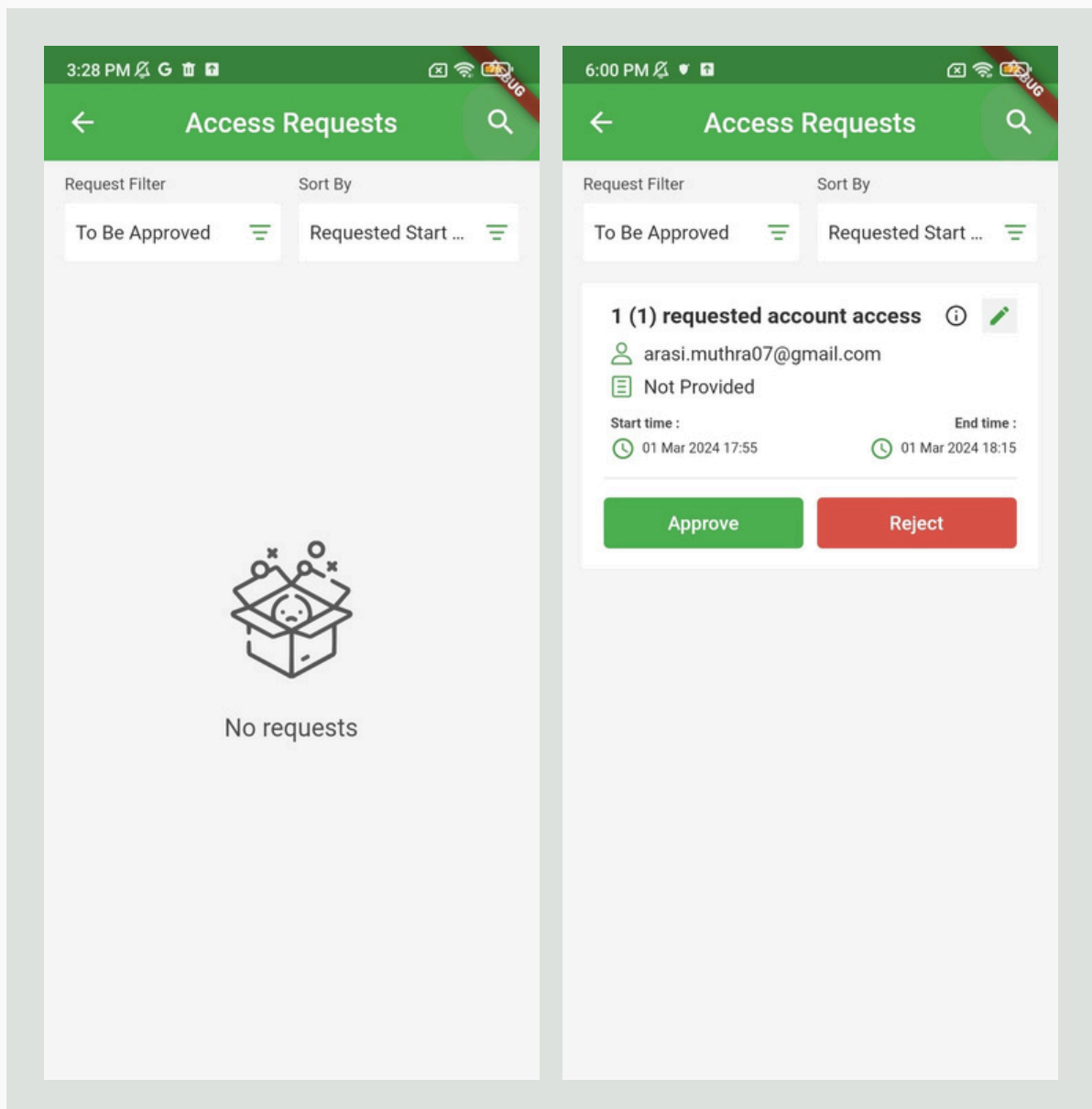
Here, you will get to see the list of all locked accounts.



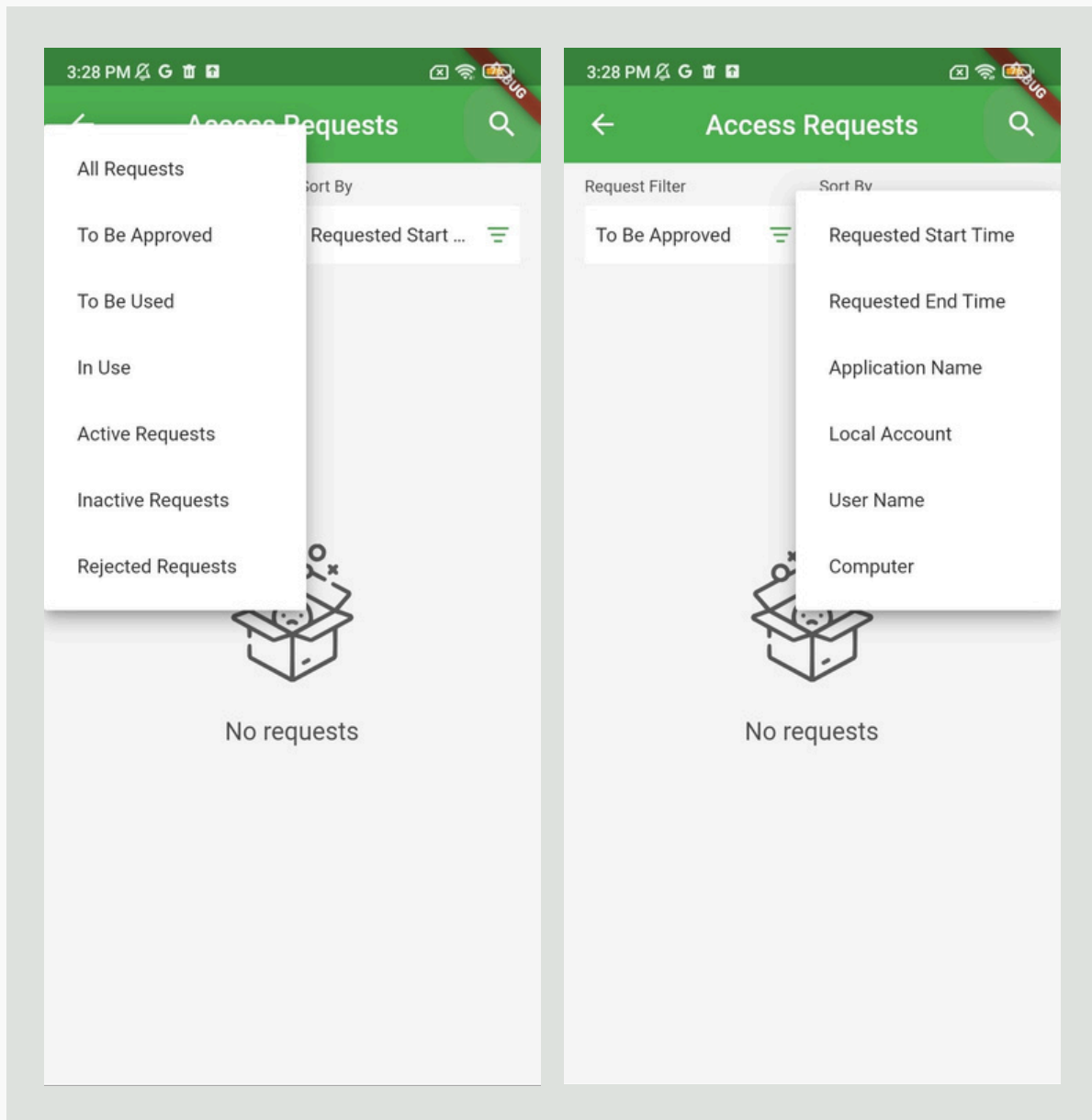
Access Request Approval Workflow

Securden Unified PAM allows IT administrators approve or reject password / privilege access requests from the mobile application.

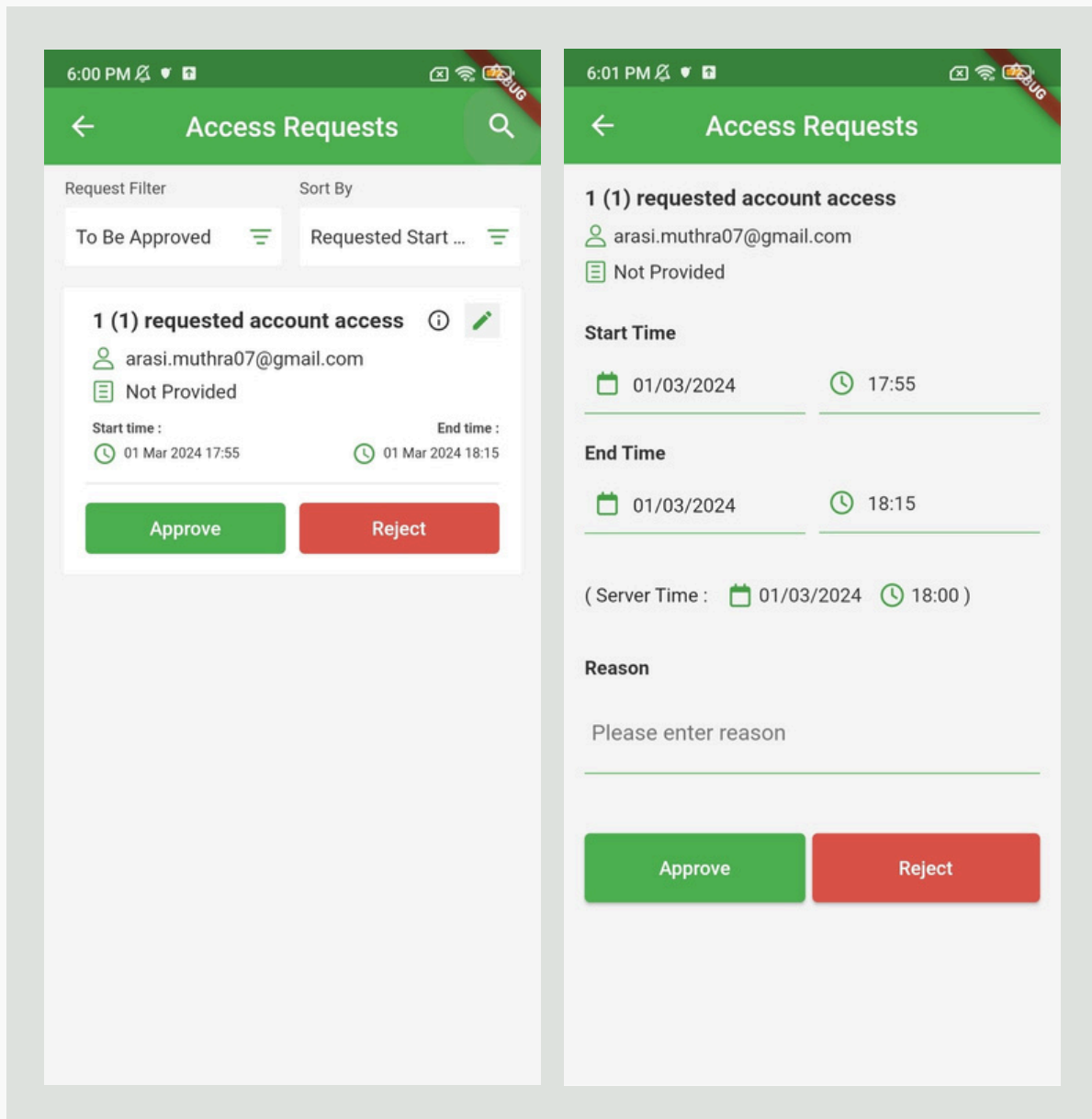
- Click Access Requests from the navigation menu
- You can see the list of access requests raised
- Offline Access Mode



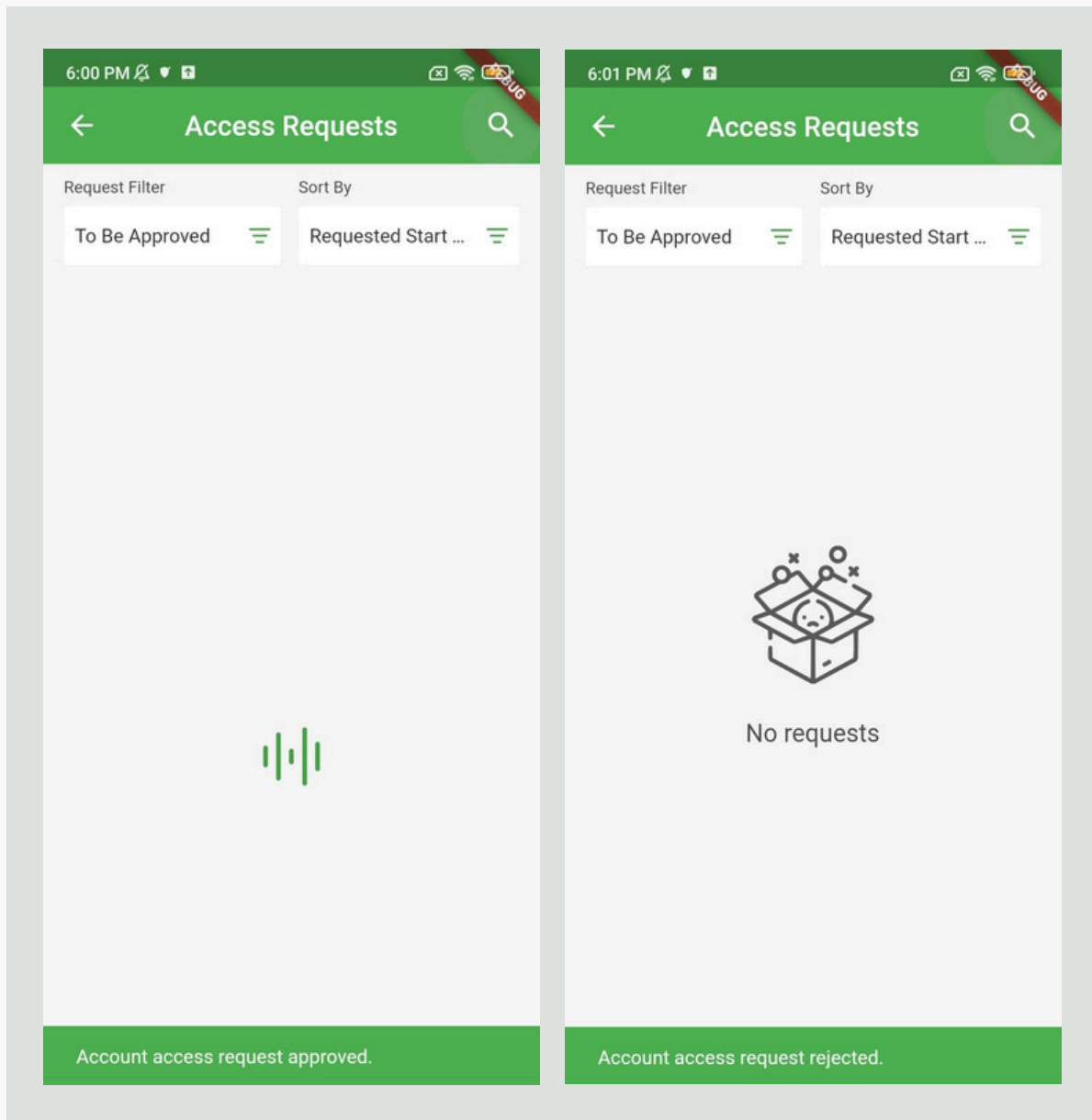
Use the 'Request Filter' option to classify access requests into categories such as 'to be approved,' 'to be used,' 'in use,' 'active requests,' 'inactive requests,' and 'rejected requests.' The 'Sort By' option lets you view the access requests based on start time, end time, application name, local account, username, and computer.



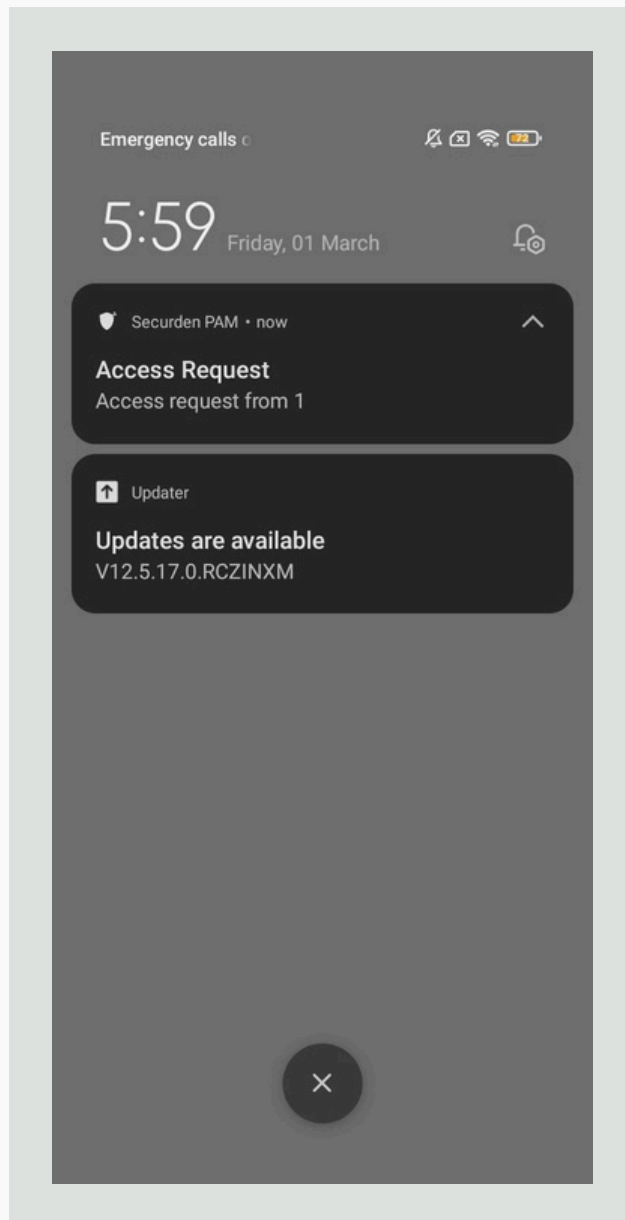
Select the pending requests listed on this page to access the request details, including the requester's identity, start and end times, as well as the reason for the request. Upon reviewing the reason and validating its legitimacy, the approver can then proceed to either approve or reject the request as appropriate.



Upon approval or rejection of the request, a confirmation message will be displayed through a green banner at the bottom of the 'Access Requests' page.



You also receive push notifications for access requests, allowing you to approve or reject them directly.

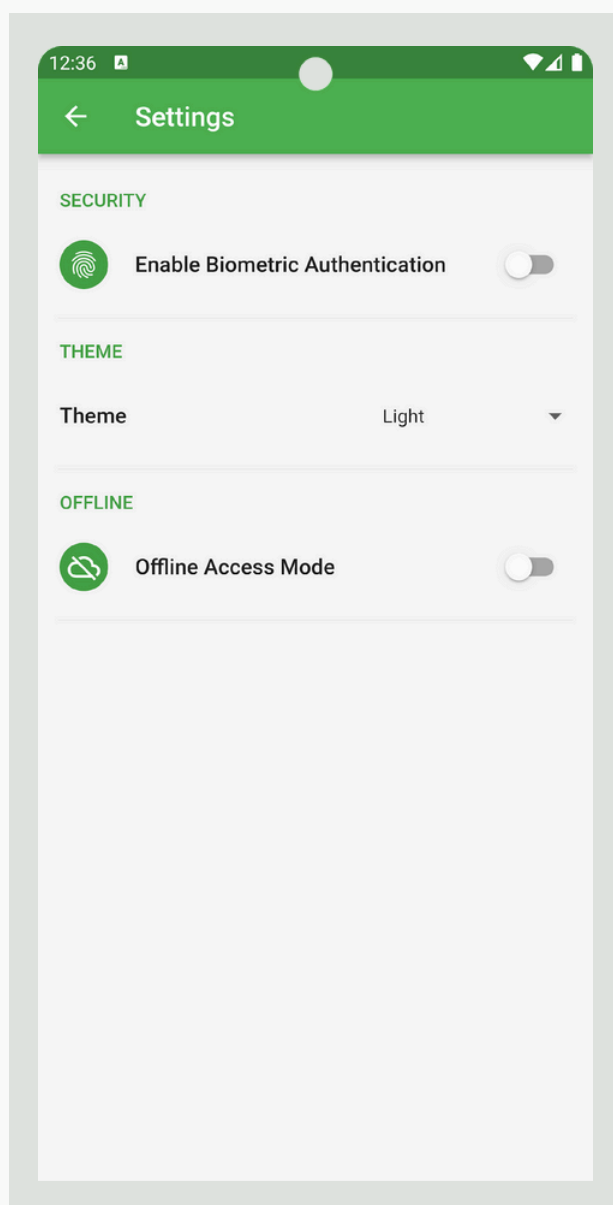


Settings



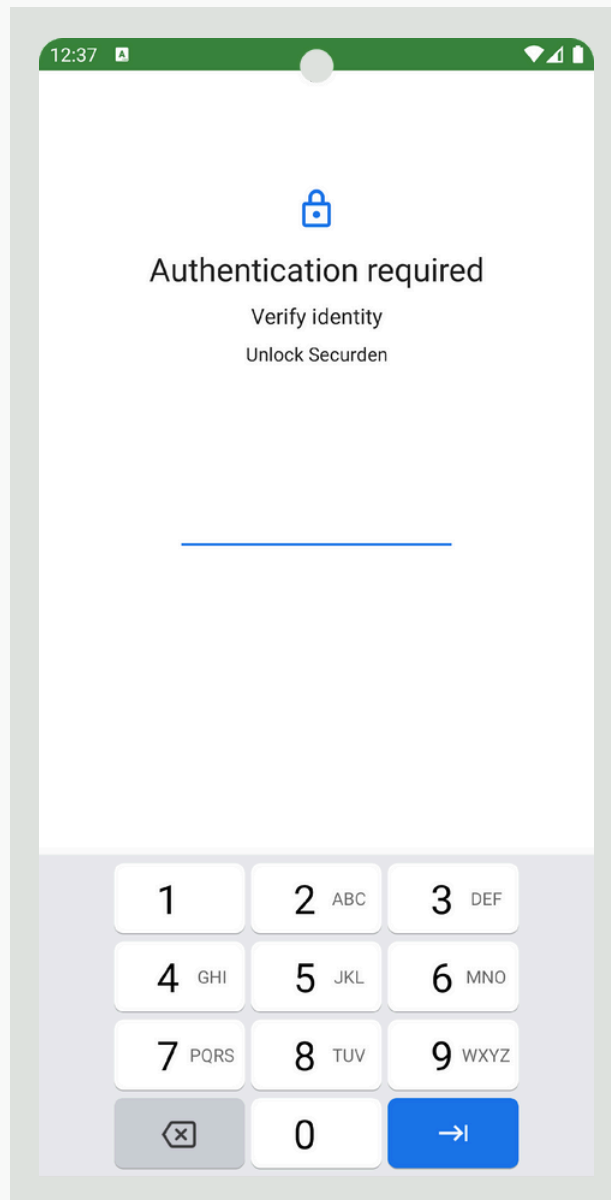
Under the 'Settings' section of the mobile application, you will see the following options:

- Enable Biometric Authentication
- Theme
- Offline Access Mode



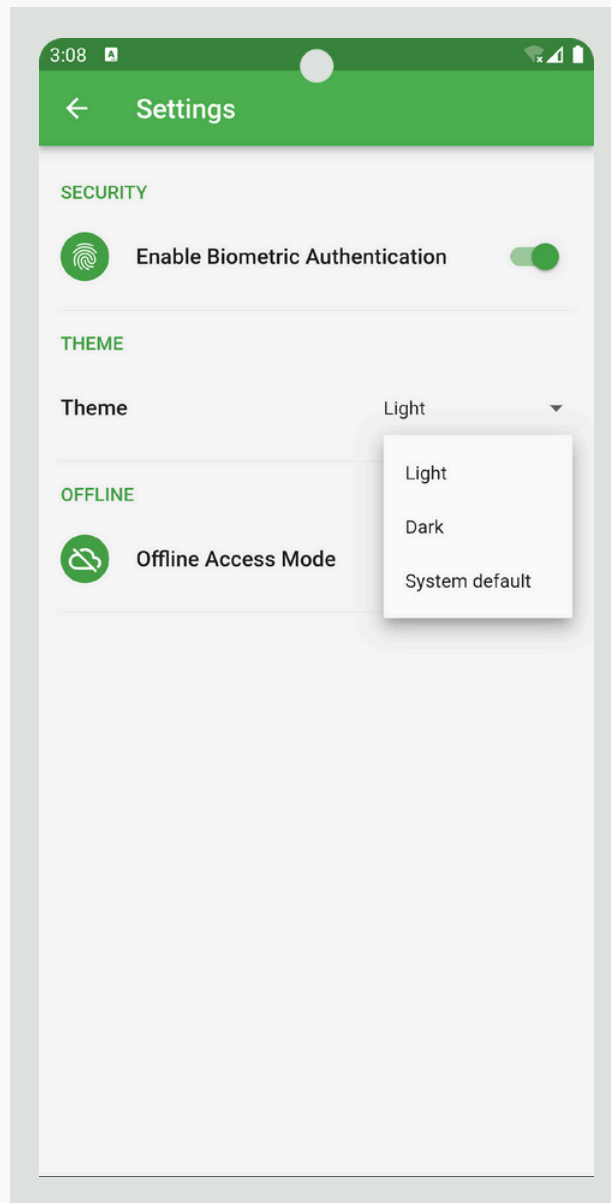
Enable Biometric Authentication

To activate biometric authentication, toggle the switch to the "on" position. This will direct you to the authentication page, where you'll need to verify using the same credentials you use to authenticate your mobile device.



Theme

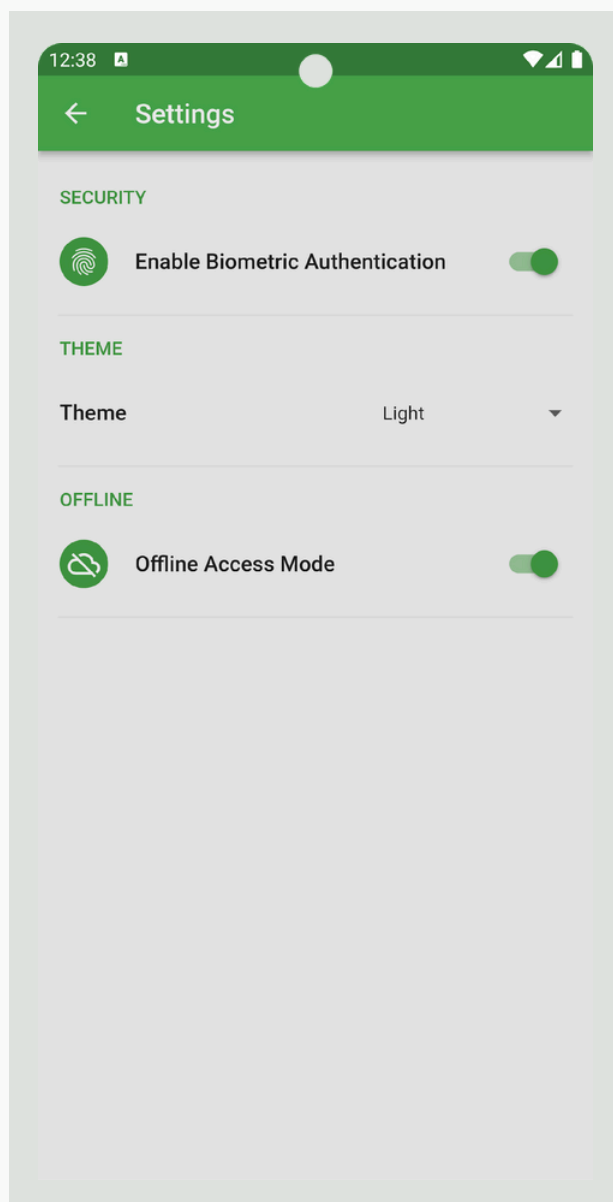
Click on the drop-down arrow present in the 'Theme' section on the '**Settings**' page. You may select your desirable theme for the mobile application from the available options – Light, Dark, and System Default.



Offline Access Mode

Securden Password Vault provides an offline access mode, allowing you to access accounts and passwords even without an internet connection.

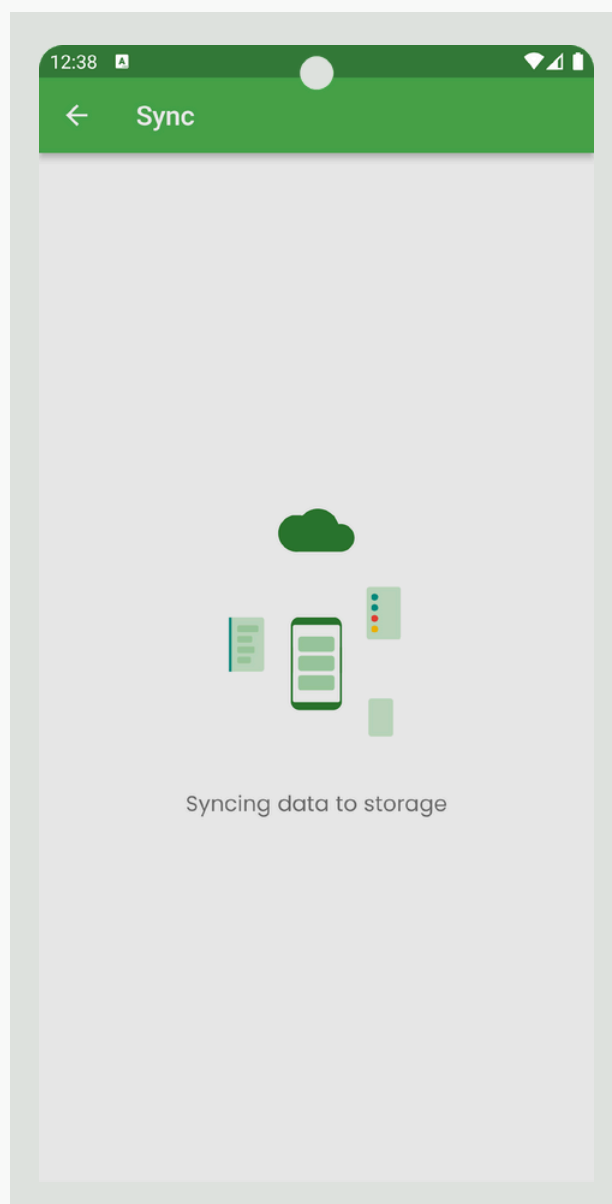
Toggle the switch for 'Offline Access Mode' to activate it.



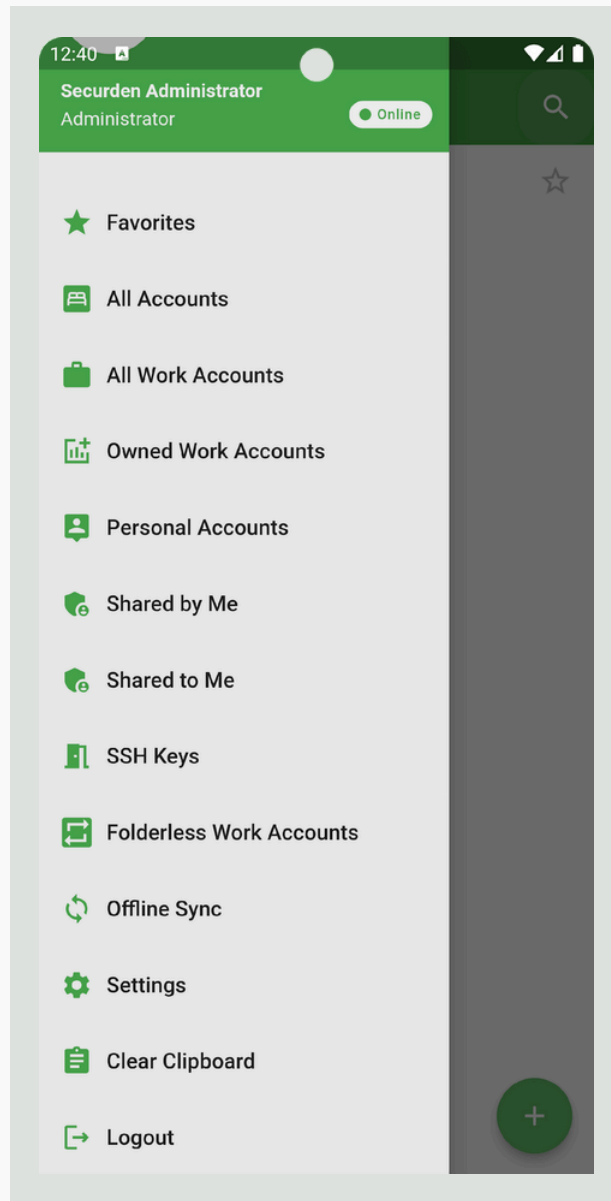
Once you do that, you need to set up a new password to login when you are accessing the offline mode.

The screenshot shows a mobile application interface for setting a password. At the top, the status bar displays the time 12:37 and various icons. The app's title bar is green with a white back arrow and the text 'Back to Index'. The main content area is light gray and titled 'Set password'. It contains two input fields: 'New password' and 'Verify password'. The 'New password' field has a green border and a green eye icon on the right. The 'Verify password' field has a gray border and a gray eye icon on the right. Below the fields are two buttons: a green 'Save' button and a gray 'Cancel' button. At the bottom of the screen, a virtual keyboard is visible, showing numbers, letters, and symbols. The keyboard has a blue checkmark button on the right.

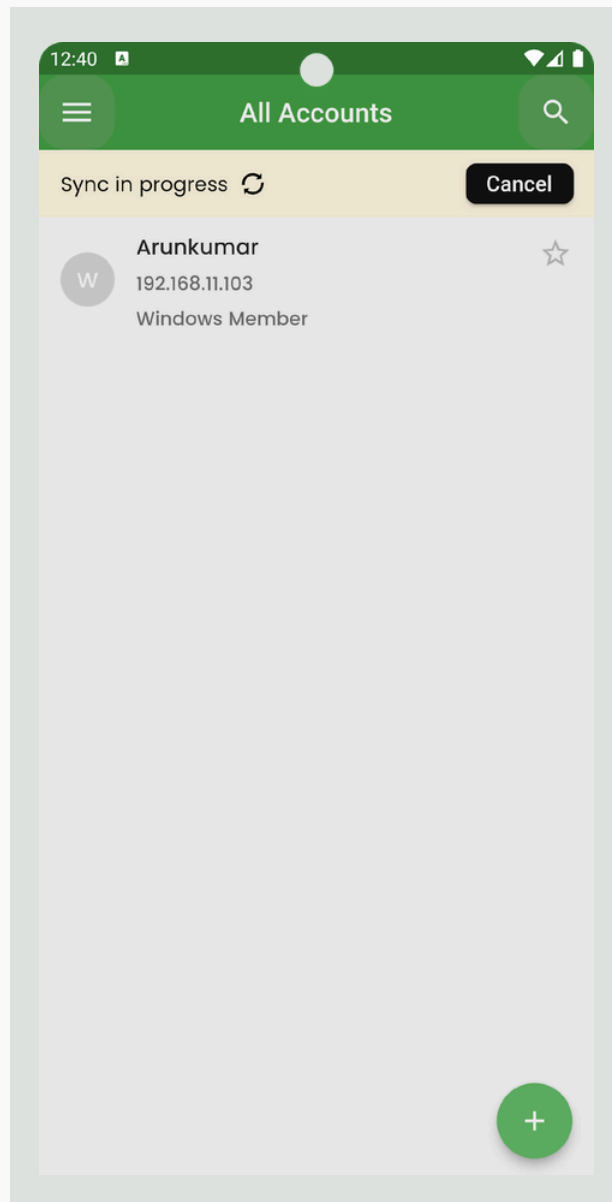
In order to access accounts in offline mode, you must synchronize the data present in the application to your mobile device.



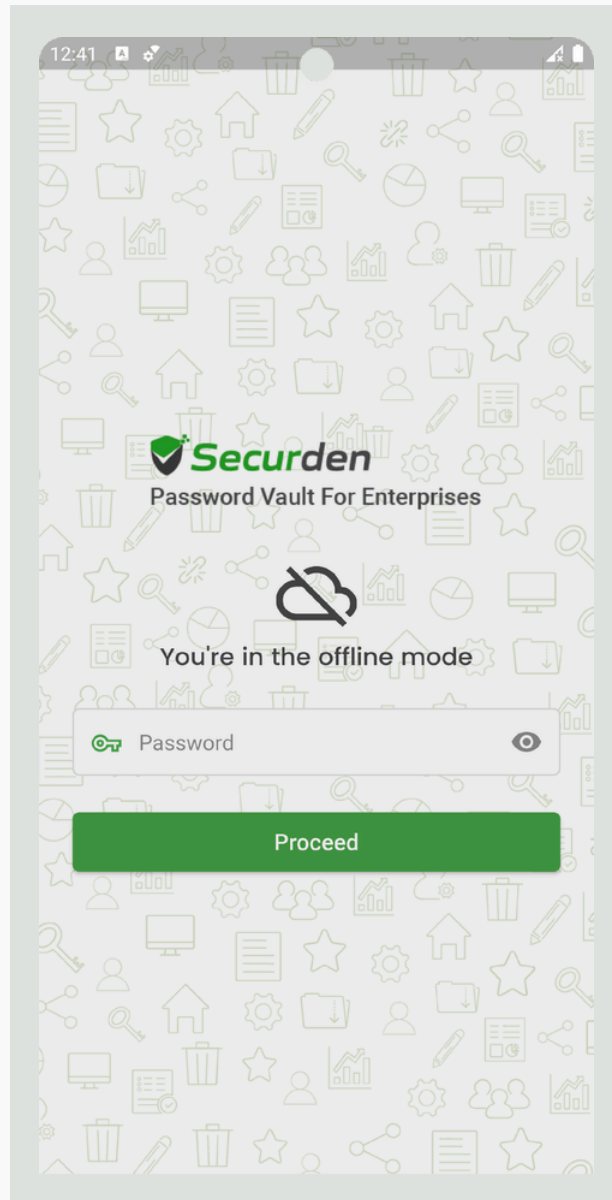
When you activate the 'Offline Access Mode,' you'll find the 'Offline Sync' option available in the Navigation Menu.



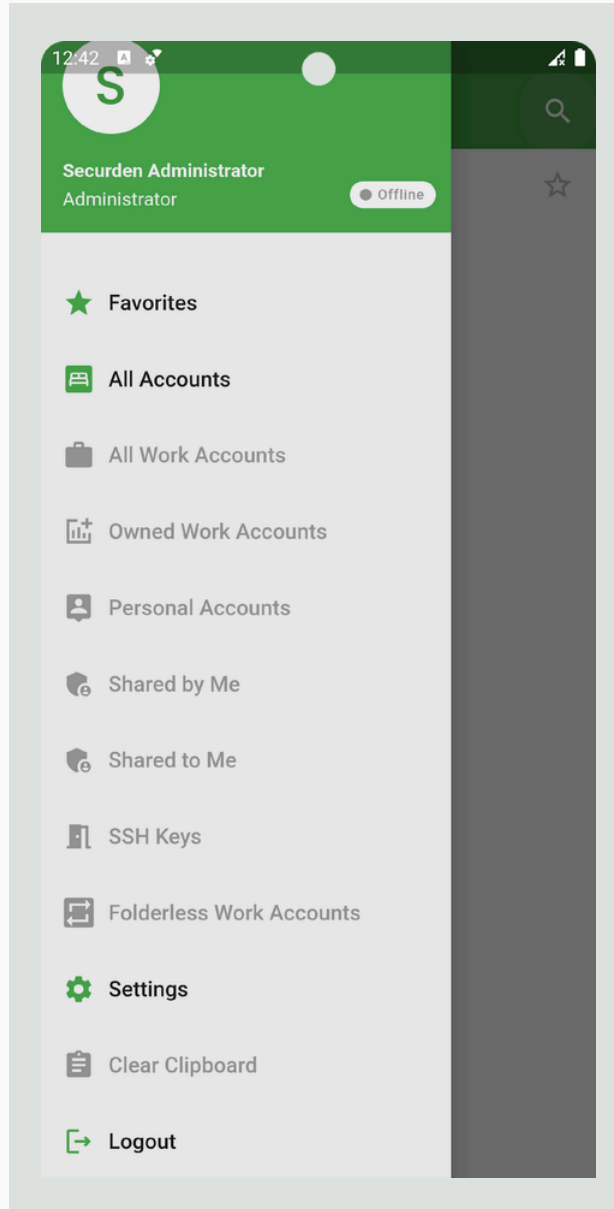
The data within the application automatically syncs with mobile storage, enabling access in offline mode whenever you need it. You will notice a yellow sticky bar at the top of the page, indicating that the data sync is currently in progress in the background.



When accessing the application offline, you will encounter this login screen, prompting you to enter the password set up when enabling 'Offline Access Mode.'

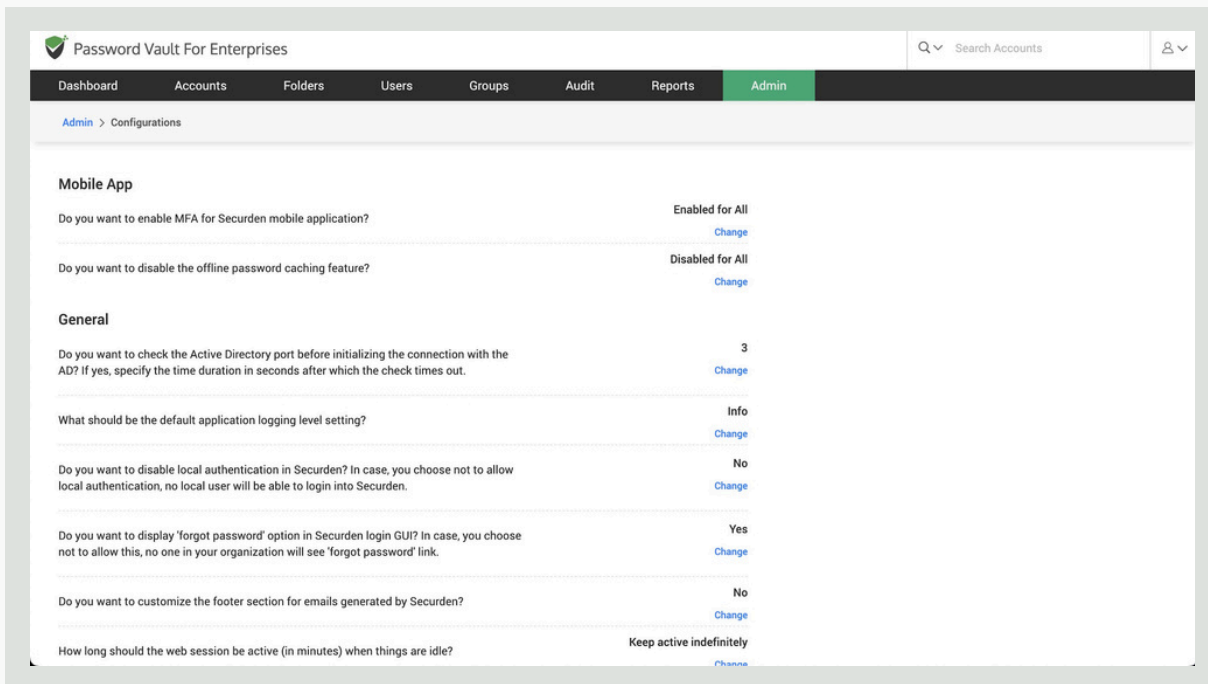


In offline mode, you'll have access to the following options: Favorites, All Accounts, and Settings.



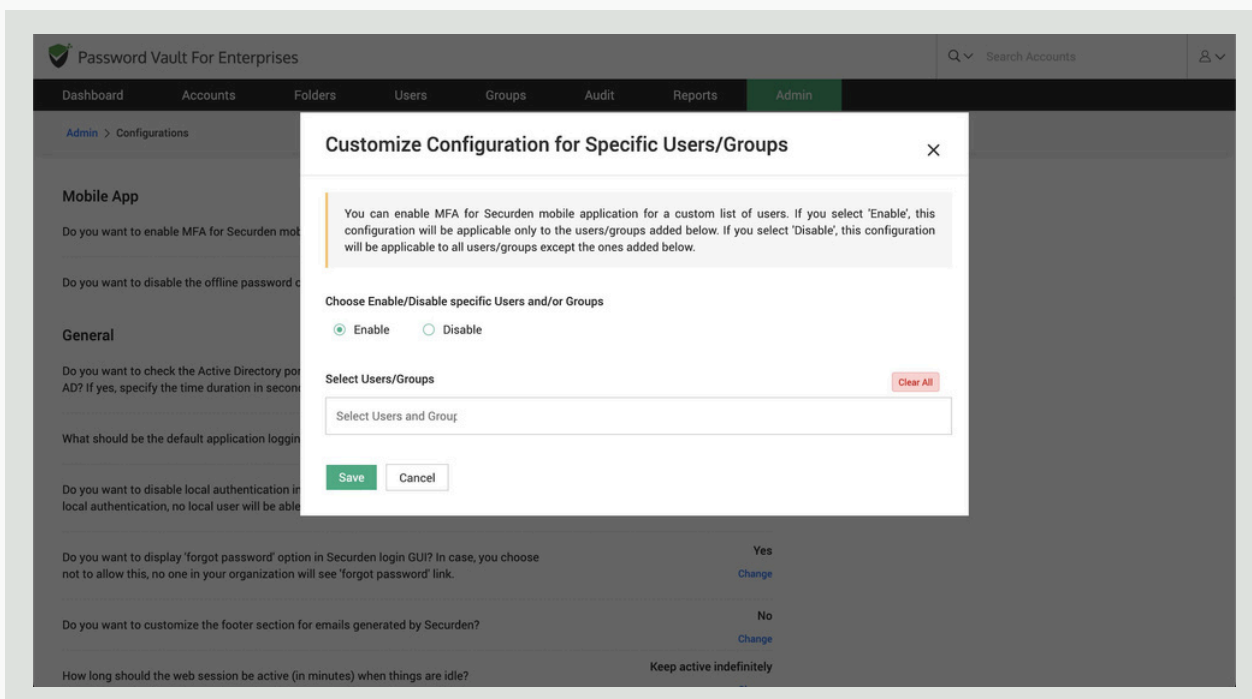
Note:

To enable MFA and Offline Access Mode functionality within the mobile application, you must activate it in the password vault solution. To do so, navigate to **Admin >> Configurations >> Mobile App**.



Under Mobile App section, you will see the questions 'Do you want to enable MFA for Securden mobile application?' and 'Do you want to disable the offline password caching feature?'

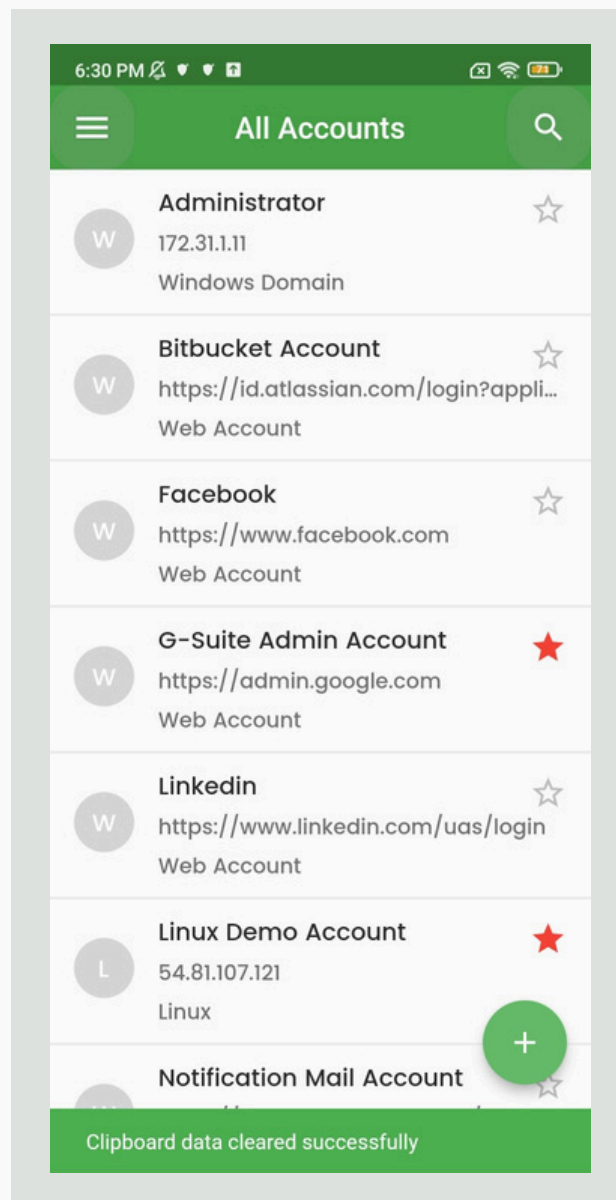
You have the flexibility to enable or disable these features for all users. Additionally, you can tailor these settings for specific users if needed.



Miscellaneous



You have the option to preserve copied data from within the app for a set period. Select the 'Clear Clipboard' option to clear the retained data.



Logout

By clicking on your logged-in username, a dialog box will appear, prompting you to confirm your logout from the application.

