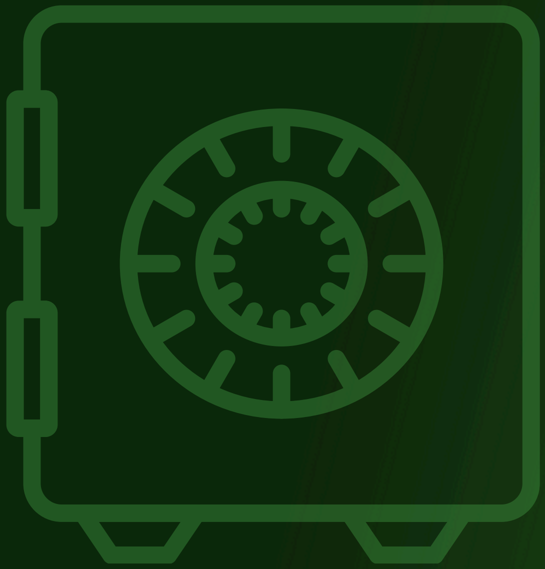
Securden

Password Vault for Enterprises

Quick Start Guide



Securden Password Vault for Enterprises

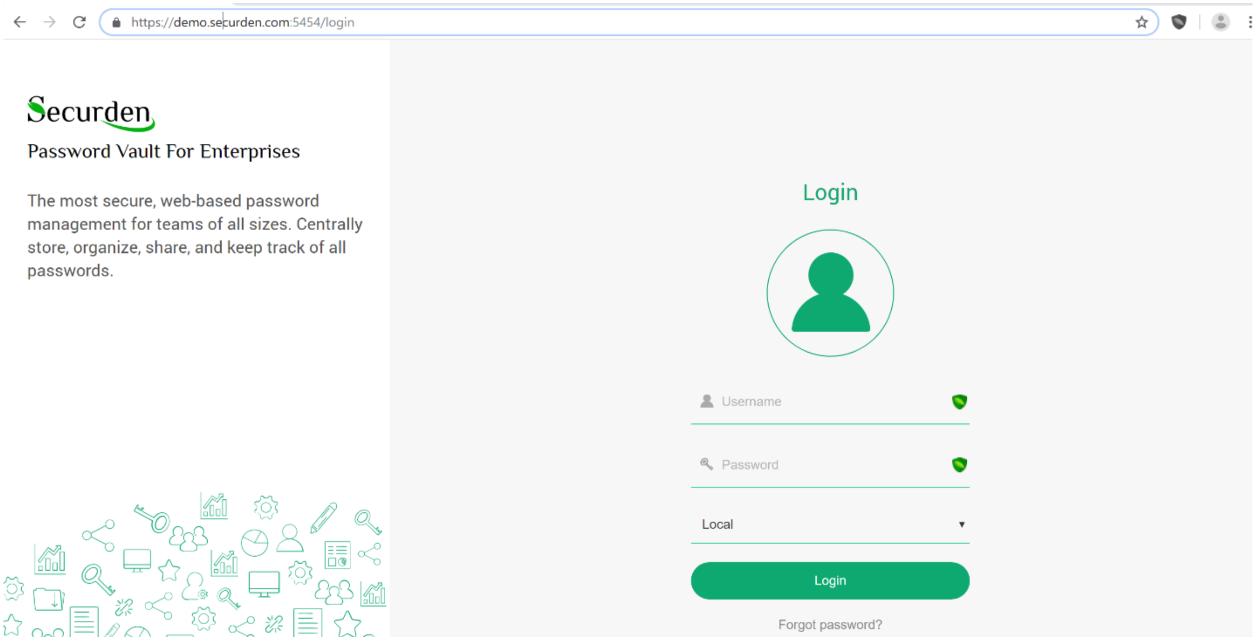
Section 1: Getting Started

This document provides a quick summary of the steps you need to do to get started with Securden Password Vault For Enterprises (Vault). Detailed instructions for each step are given in the product GUI itself.

Starting the Password Vault Server

- You can start and shutdown Vault from Windows Services Manager (services.msc).
- Locate **Securden Vault Service** and start, stop it as required. This takes care of starting and stopping the dependent services too. You may **<u>safely ignore</u>** the other service named **Securden Vault Web Service**, which is taken care of by Securden automatically.

Launching Web Interface



https://demo.securden.com:5454/login

Securden

Password Vault For Enterprises

The most secure, web-based password management for teams of all sizes. Centrally store, organize, share, and keep track of all passwords.

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

https://<Vault server hostname>:5454

To access an unconfigured setup, the default login details are as below:

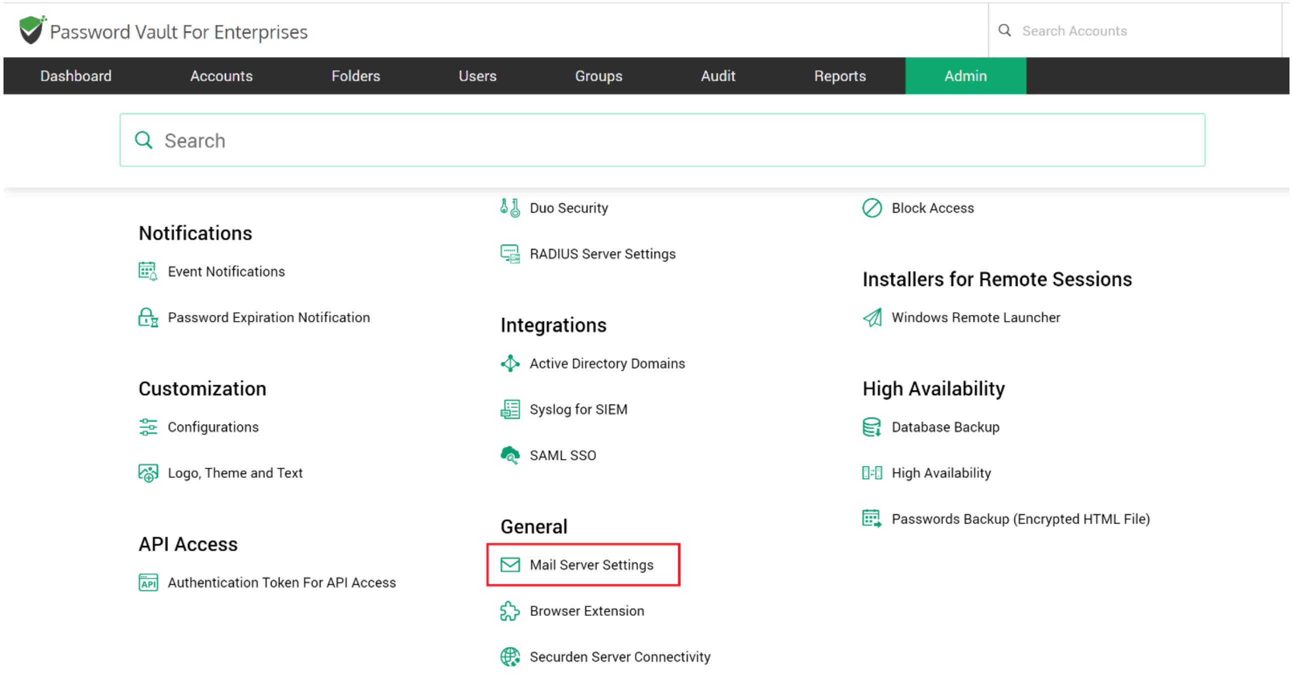
Username: admin

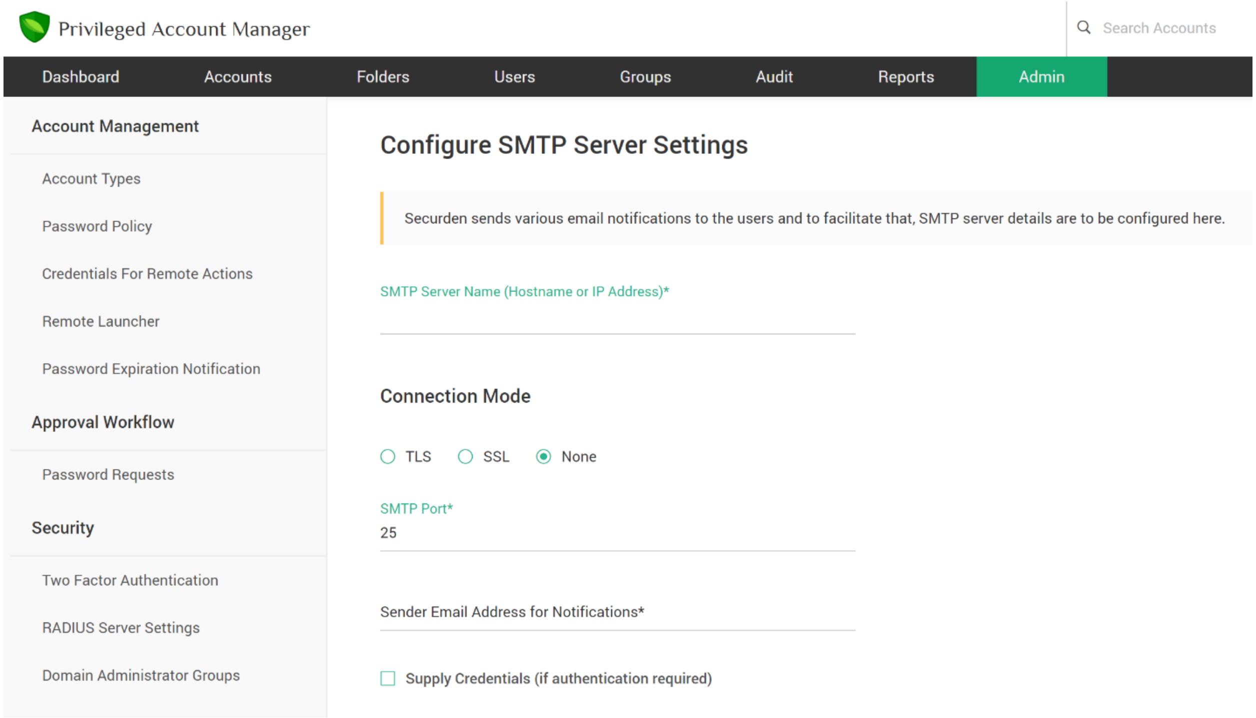
Password: admin

Section 2: User Management

Prerequisite: Configure Mail Server Settings

Securden sends various email notifications to the admins/users and to facilitate that SMTP server details are to be configured. Navigate to **Admin >> General >> Mail Server Settings** in the GUI to perform this step.





Configure SMTP Server Settings

Securden sends various email notifications to the users and to facilitate that, SMTP server details are to be configured here.

SMTP Server Name (Hostname or IP Address)*

Connection Mode

○ TLS ○ SSL ● None

SMTP Port*
25

Sender Email Address for Notifications*

□ Supply Credentials (if authentication required)

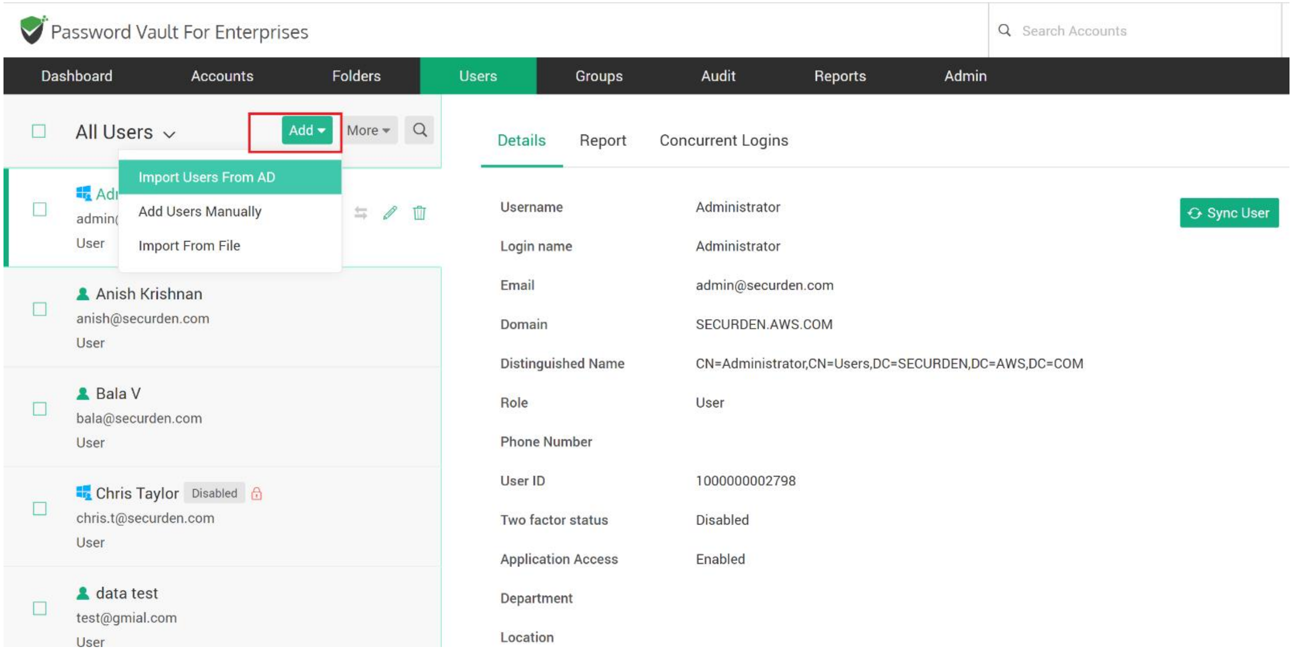
Step 1: Onboard Your Users

You need to create accounts for your team members to enable them to use Securden. There are two options to do this. You can import users from Active Directory or manually add users.

Import from Active Directory

In the case of importing from 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.

Note: When importing users from AD, you have the option to import them with specific roles. You can find more information about user roles in step 2 below. By default, the role 'user' will be assigned for all users imported from AD.



Anish Krishnan
anish@securden.com
User

Bala V
bala@securden.com
User

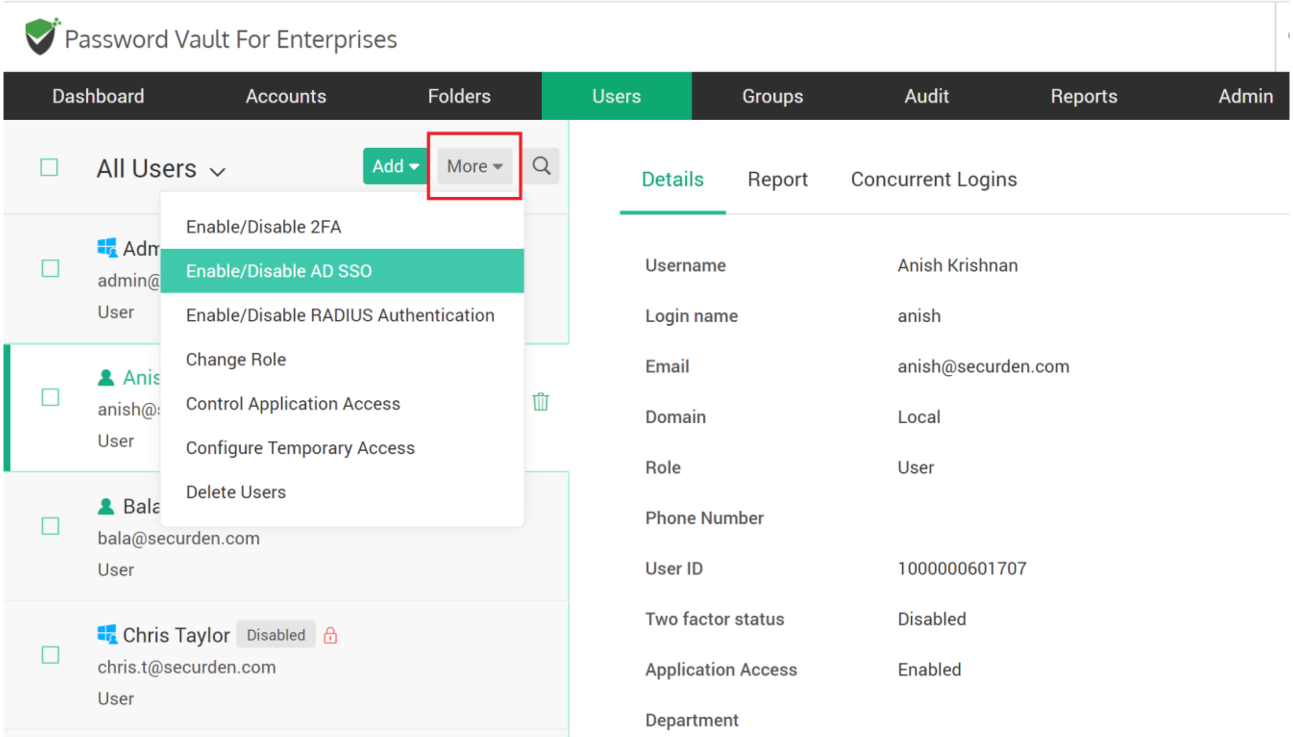
Chris Taylor Disabled
chris.t@securden.com
User

data test
test@gmial.com
User

Username Administrator
Login name Administrator
Email admin@securden.com
Domain SECURDEN.AWS.COM
Distinguished Name CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM
Role User
Phone Number
User ID 1000000002798
Two factor status Disabled
Application Access Enabled
Department
Location

If you want to import users with any other specific role, you can modify the setting in **Admin >> Customization >> Configurations >> Defaults Selection** section and then import.

AD SSO



bala@securden.com
User

Chris Taylor Disabled
chris.t@securden.com
User

Username Anish Krishnan
Login name anish
Email anish@securden.com
Domain Local
Role User
Phone Number
User ID 1000000601707
Two factor status Disabled
Application Access Enabled
Department

Once you integrate Active Directory, you can leverage the Active Directory authentication and single sign on. If your users are already logged into their AD account, they can automatically access Securden web-interface.

To enable ADSSO, navigate to '**Users**' tab, select the users for whom SSO needs to be enabled. From '**More**' drop-down, click '**Enable/Disable AD SSO**'.

Add Users Manually

You can also create accounts for users in Securden manually. In this case, users will get login credentials to access the PAM. Navigate to **Users >> Add >> Add Users Manually** in the GUI to perform this step.

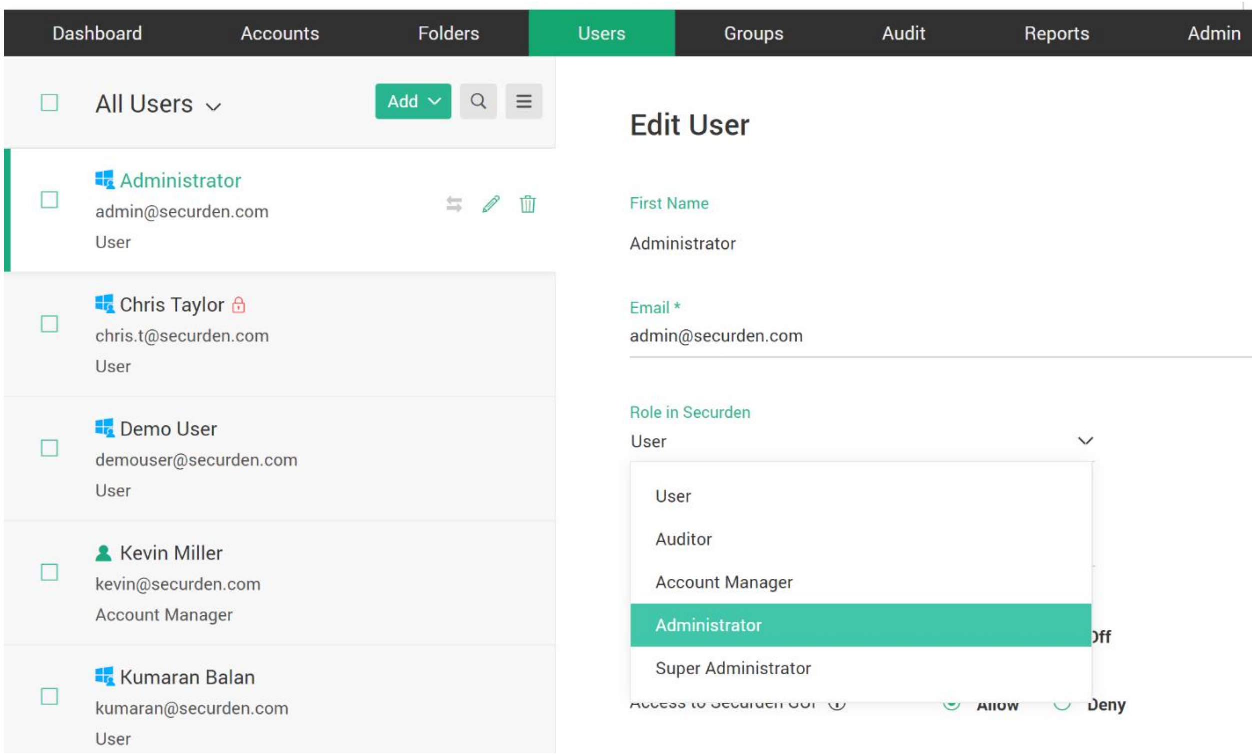
Another Option: Import from Files

Another option to add your users to Securden is to import the details from a CSV or XLSX file. This essentially adds all users locally in Securden at one go. Navigate to **Users >> Add >> Import from File** in the GUI to perform this step. In the import screen, you can specify the role with which the users are to be imported to Securden (see below for more information about user roles).

Step 2: Assign Roles for Users

By default, the users imported from Active Directory will have the role 'Users'. You can assign appropriate roles for many users in bulk or individually for each user.

To change the role of users in bulk, navigate to **Users** section in the GUI and select the required users. Then click '**Change Role**' option under '**More Actions**'. Alternatively, use the '**Edit**' option to change the role of users individually.



Administrator
admin@securden.com
User

Chris Taylor
chris.t@securden.com
User

Demo User
demouser@securden.com
User

Kevin Miller
kevin@securden.com
Account Manager

Kumaran Balan
kumaran@securden.com
User

Edit User

First Name
Administrator

Email *
admin@securden.com

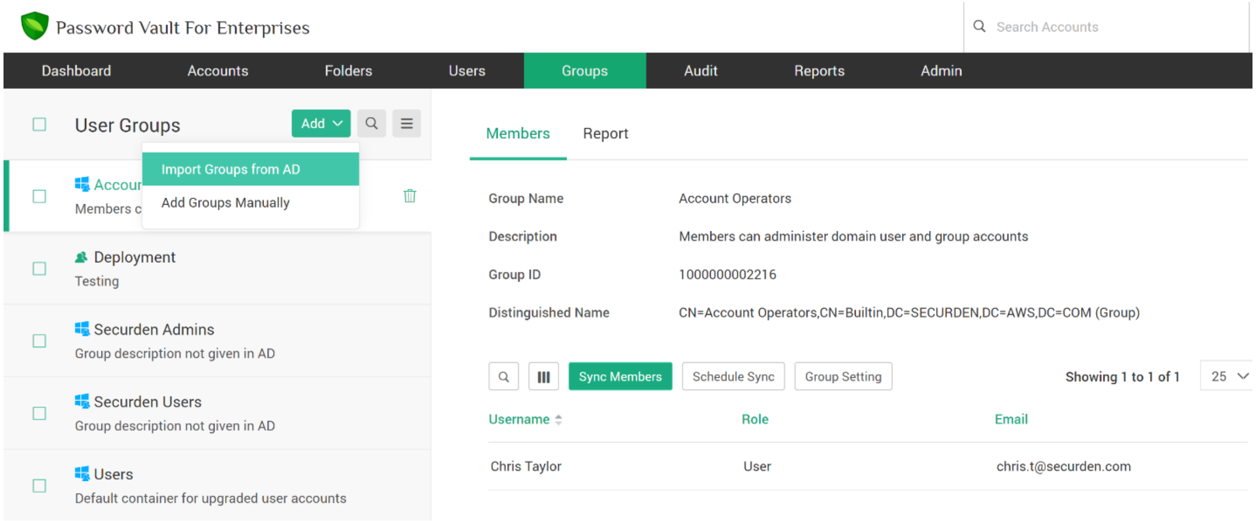
Role in Securden
User

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

- **Super Administrator** - Can view all work related passwords stored in the application. Overall administration of the application, including user management.
- **Administrator** - Can administer the application, including user management. Can see only the passwords that are owned and the ones that are shared with.
- **Account Manager** - Can add accounts to the application. Performs all administrative tasks related to the accounts.
- **User** - Can view the accounts shared by administrators. They can manually add accounts and share them with others. (They will not have the privilege to import accounts). If needed, you can disable account addition privilege for users.
- **Auditor** - Can view the reports and audit trails generated in the application. They can manually add accounts and share them with others.

Step 3: Create 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 organization.



Group Name	Account Operators
Description	Members can administer domain user and group accounts
Group ID	1000000002216
Distinguished Name	CN=Account Operators,CN=Builtin,DC=SECURDEN,DC=AWS,DC=COM (Group)

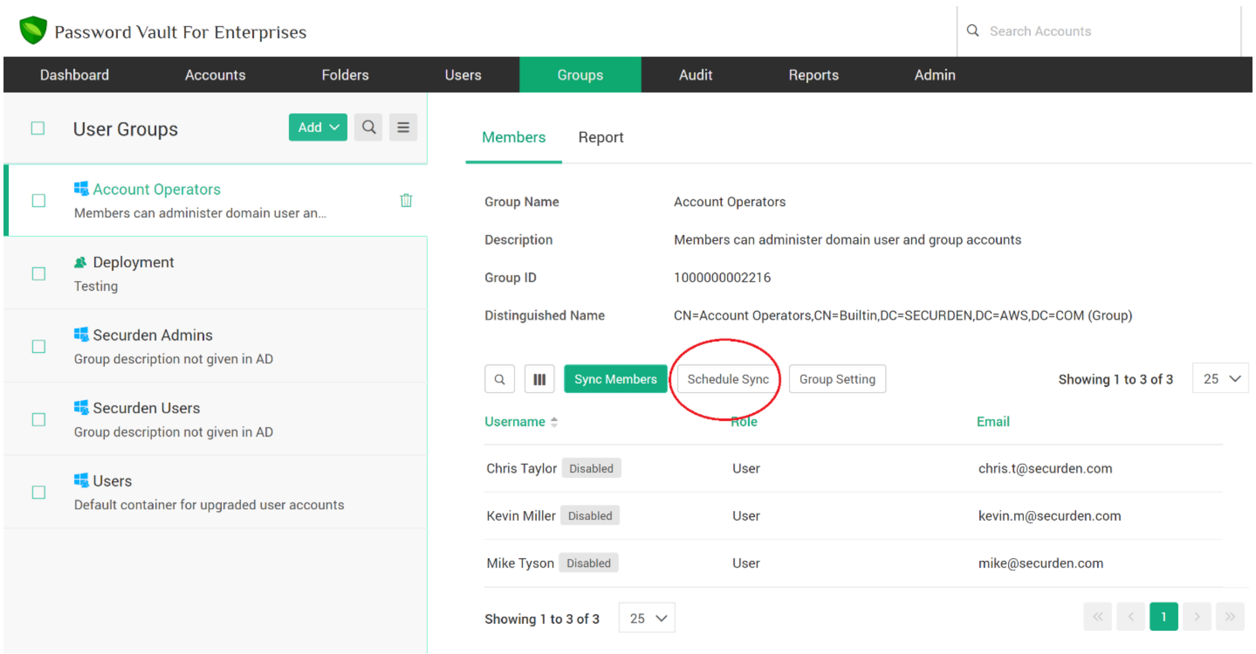
Username	Role	Email
Chris Taylor	User	chris.t@securden.com

You can define various access permissions at the group level so that when a new member joins the organization, by placing the member at the right group, the member can inherit the access permissions automatically. There are two ways to create user groups - you can import groups directly from AD or add groups manually. Navigate to **Groups >> Add** in the GUI to perform this step.

Configure Periodic Synchronization of Groups

You can create a scheduled task to 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.

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



□ Account Operators
Members can administer domain user an...

□ Deployment
Testing

□ Securden Admins
Group description not given in AD

□ Securden Users
Group description not given in AD

□ Users
Default container for upgraded user accounts

Group Name	Account Operators
Description	Members can administer domain user and group accounts
Group ID	1000000002216
Distinguished Name	CN=Account Operators,CN=Builtin,DC=SECURDEN,DC=AWS,DC=COM (Group)

Showing 1 to 3 of 3 25

Username	Role	Email
Chris Taylor Disabled	User	chris.t@securden.com
Kevin Miller Disabled	User	kevin.m@securden.com
Mike Tyson Disabled	User	mike@securden.com

Showing 1 to 3 of 3 25

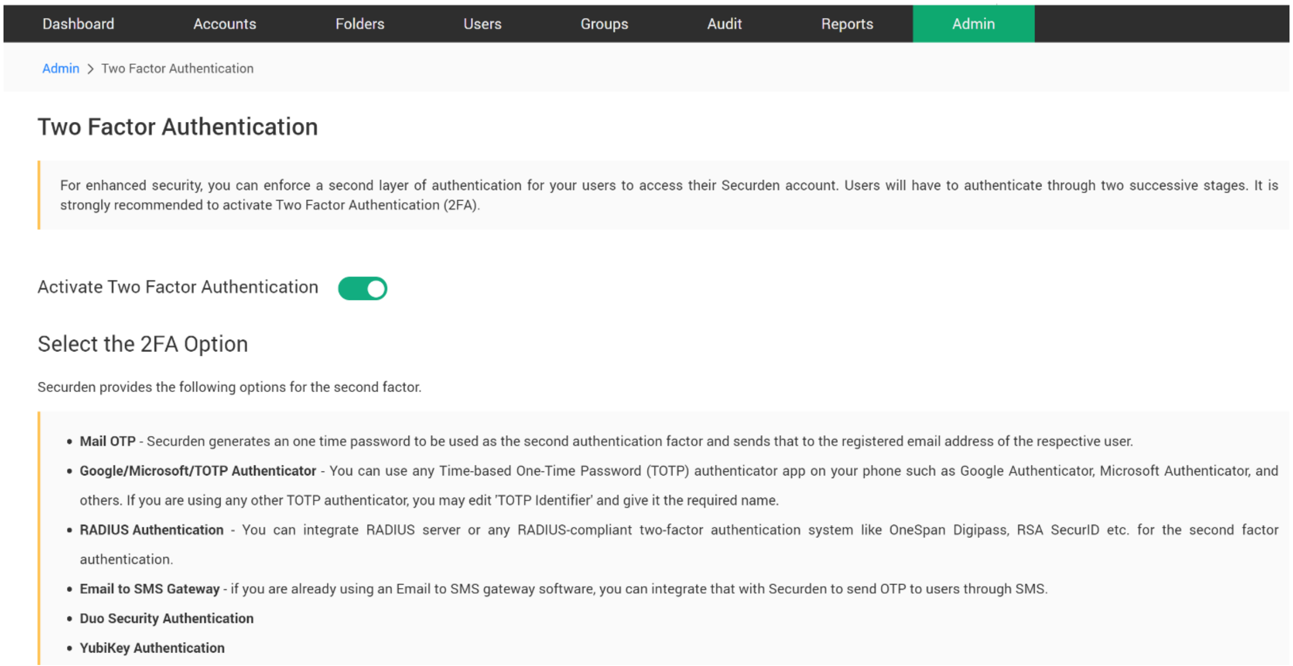
Step 4: Explore Single SignOn Options

Securden integrates with various SAML-compatible federated identity management solutions such as Okta, G Suite, Microsoft ADFS, OneLogin, PingIdenity, 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). If you are using any SSO solution already, you may integrate that with Securden.

To enable Single Sign On, navigate to **Admin >> Integration >> SAML SSO** section in the GUI.

Step 5: Configure Two Step Verification

For enhanced security, you can enforce a second layer of authentication for your users to access their Securden account. Users will have to authenticate through two successive stages. It is strongly recommended to activate Two Factor Authentication (2FA).



Two Factor Authentication

For enhanced security, you can enforce a second layer of authentication for your users to access their Securden account. Users will have to authenticate through two successive stages. It is strongly recommended to activate Two Factor Authentication (2FA).

Activate Two Factor Authentication ●

Select the 2FA Option

Securden provides the following options for the second factor.

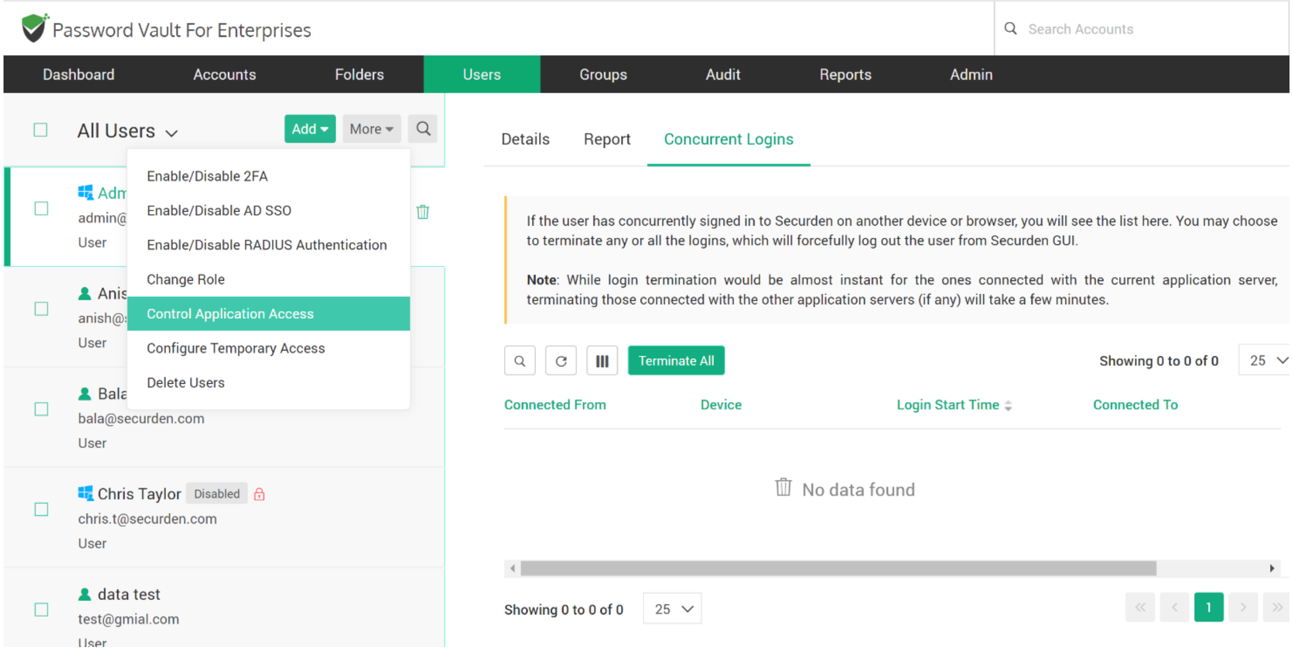
- **Mail OTP** - Securden generates an one time password to be used as the second authentication factor and sends that to the registered email address of the respective user.
- **Google/Microsoft/TOTP Authenticator** - You can use any Time-based One-Time Password (TOTP) authenticator app on your phone such as Google Authenticator, Microsoft Authenticator, and others. If you are using any other TOTP authenticator, you may edit 'TOTP Identifier' and give it the required name.
- **RADIUS Authentication** - You can integrate 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**
- **YubiKey Authentication**

At present, Securden supports TOTP authenticators (Google Authenticator, Microsoft Authenticator and others), any RADIUS-compliant 2FA mechanism (OneSpan Digipass, RSA SecurID, and others), Duo Security, Yubikey, a one-time password through email, and OTP via SMS (using Email to SMS tools) as the second factor. Navigate to **Admin >> General >> Two Factor Authentication** in the GUI to perform this step.

Step 6: Explore Granular Controls

You can exercise granular control over the users in Securden. From the '**Users**' tab, you will be able to monitor the concurrent logins of each user separately. For example, if a user has logged in to the Securden web-interface through web on multiple browsers, and also through mobile apps, the '**Concurrent Logins**' section lists out all the logins. You can review and even terminate any or all the logins.

In addition, from the '**More**' drop-down, you can exercise other controls such as selectively enabling/disabling 2FA, AD SSO, grant temporary access to Securden, temporarily disable access and even delete users.



If the user has concurrently signed in to Securden on another device or browser, you will see the list here. You may choose to terminate any or all the logins, which will forcefully log out the user from Securden GUI.

Note: While login termination would be almost instant for the ones connected with the current application server, terminating those connected with the other application servers (if any) will take a few minutes.

Showing 0 to 0 of 0

No data found

Showing 0 to 0 of 0

Section 3: Password Management

Account Ownership and Sharing: The Basic Design

Any login information - username and password - stored in Securden is referred to as an account. One who adds an account becomes the owner of that particular account. The owner alone can see that account when logging in to Securden. If the owner wants others to view, the account has to be shared. When you login to Securden web-interface, you will see only the accounts that are owned by you and the ones that are shared with you. Only the super administrator is exempted from this rule. Super admin can see all the work-related accounts stored.

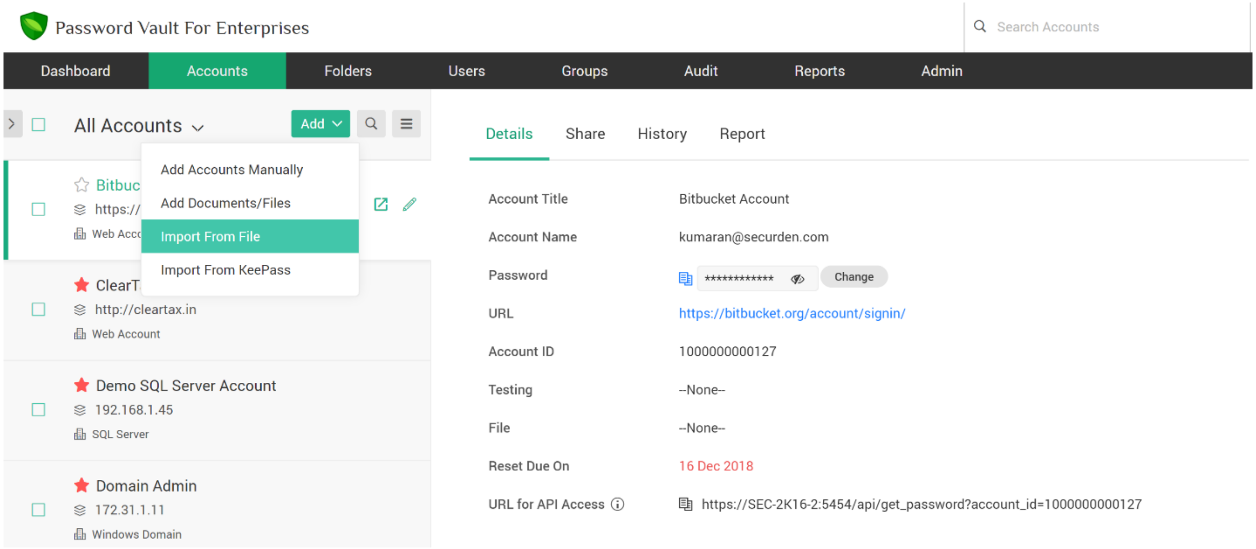
Step 1: Add Your Accounts

The first step to getting started with password management is to consolidate all your accounts to the central repository. You can add accounts in two ways – import from a CSV/XLSX file or manually add them.

1.1 Import Accounts

If you are already using another password manager or keeping your passwords on excel sheets, you can import accounts from a standard CSV file.

Navigate to **Accounts >> Add >> Import From File** to perform this.



Account Title	Bitbucket Account
Account Name	kumaran@securden.com
Password	************
URL	https://bitbucket.org/account/signin/
Account ID	1000000000127
Testing	--None--
File	--None--
Reset Due On	16 Dec 2018
URL for API Access	https://SEC-2K16-2:5454/api/get_password?account_id=1000000000127

If you are using KeePass, you can export your data from KeePass either as a KDBX file or as XML 1.0/2.0 file and import them to Securden in one click. Navigate to **Accounts >> Add >> Import From KeePass** to perform this.

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 that of Securden. So, the format of the import file doesn't have a major role.

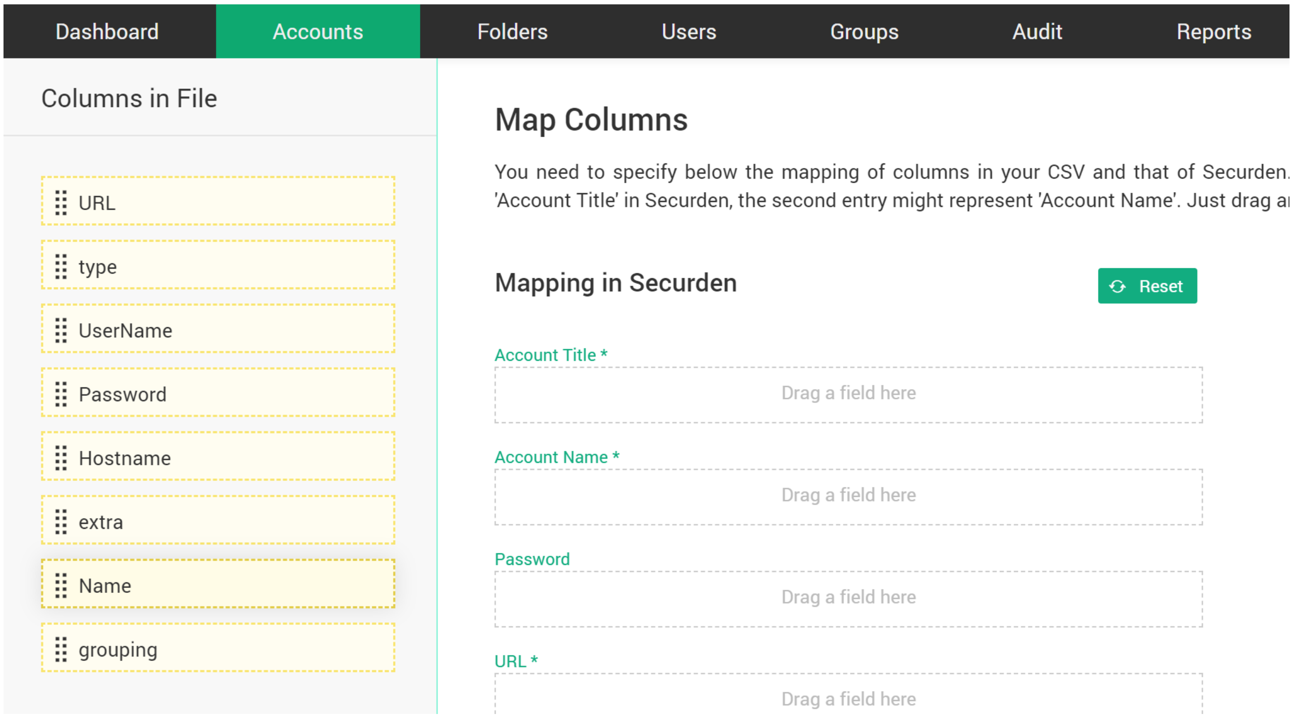
Steps to import

- Navigate to **Accounts >> Add** and select "**Import From File**" option.

- Browse and select the file
- Click '**Nex**t'. 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.



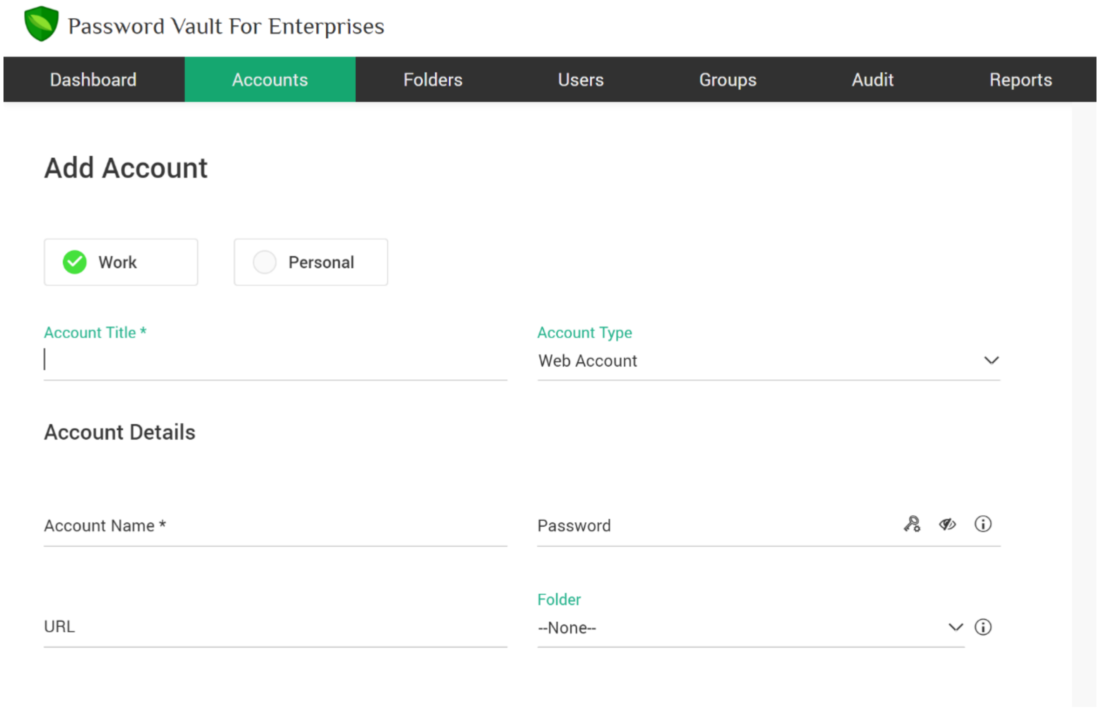
You need to specify below the mapping of columns in your CSV and that of Securden. 'Account Title' in Securden, the second entry might represent 'Account Name'. Just drag a

Taking Care of Additional Fields

To include the additional fields 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. To do this, navigate to **Admin >> Account Management >> Account Types** and click "**Add Account Type**". Fill in the details. For '**Password Policy**', select the option '**Don't link any policy**' and at the bottom of the page, you will see "**Add Fields**". Click that and add the required additional fields. Give the additional field the required name (in your case Hostname, extra) using '**Field Label**'. This takes care of the additional fields.

1.2 Add Accounts Manually

You can add accounts manually too. Navigate to **Accounts >> Add** in the GUI to perform this step.



Add Account

☑ Work ○ Personal

Account Title *

Account Type: Web Account

Account Details

Account Name *

Password

URL

Folder: --None--

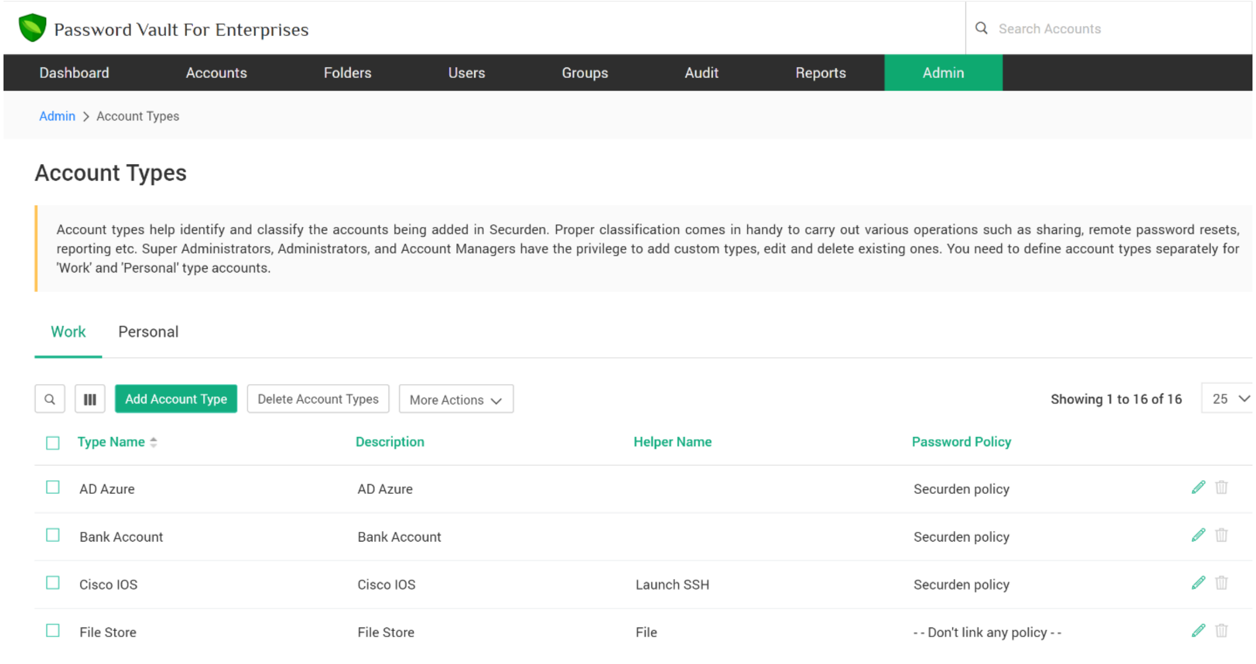
1.3 Accounts Classification – Work and Personal Accounts

When adding accounts, you can classify them as 'Work' or 'Personal'. Work accounts belong to your organization and hence can be shared with your colleagues on need basis. 'Personal' accounts belong to you and cannot be shared with others. Only you can see such accounts.

Note: Super admin cannot view the personal accounts of other users. If your organization prefers not to have 'Personal' classification, it can be disabled from **Admin >> Customization >> Configurations** >> **Personal** section.

1.4 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, whether certain fields should be marked as 'mandatory' and the default values for each field.



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. 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.

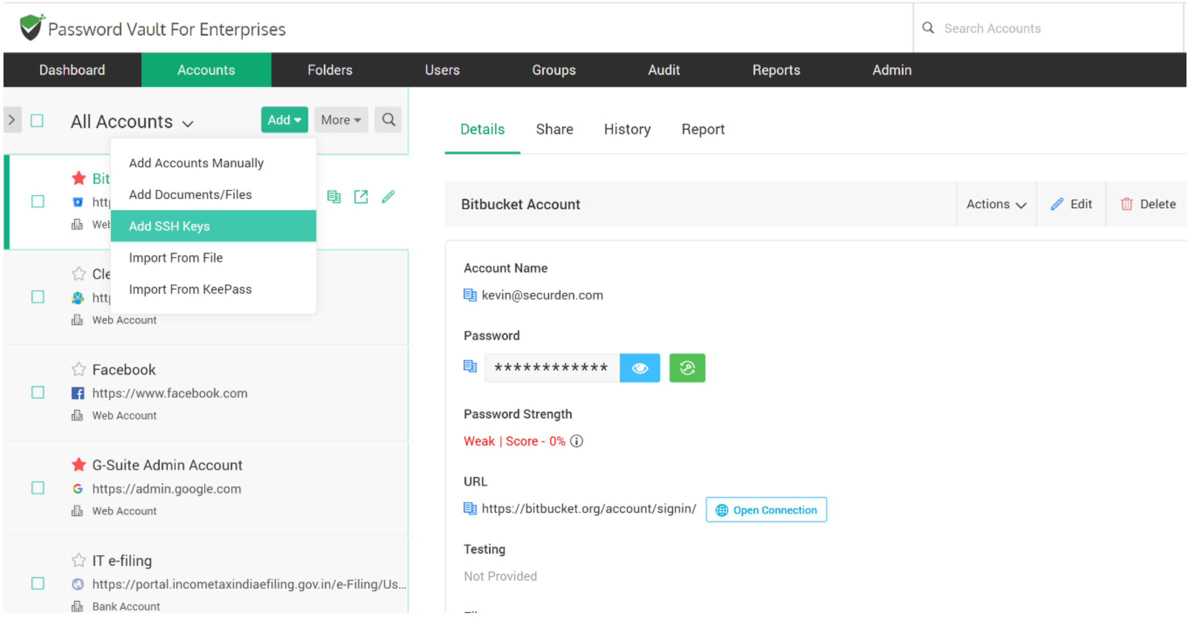
Showing 1 to 16 of 16

□	Type Name	Description	Helper Name	Password Policy
□	AD Azure	AD Azure		Securden policy
□	Bank Account	Bank Account		Securden policy
□	Cisco IOS	Cisco IOS	Launch SSH	Securden policy
□	File Store	File Store	File	- - Don't link any policy - -

Navigate to **Admin >> Account Management >> Account Types** to create new account types and to manage existing ones.

1.5 Add SSH Keys

In addition to storing passwords, you can also store and manage SSH keys. The provision to manage SSH keys help 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.



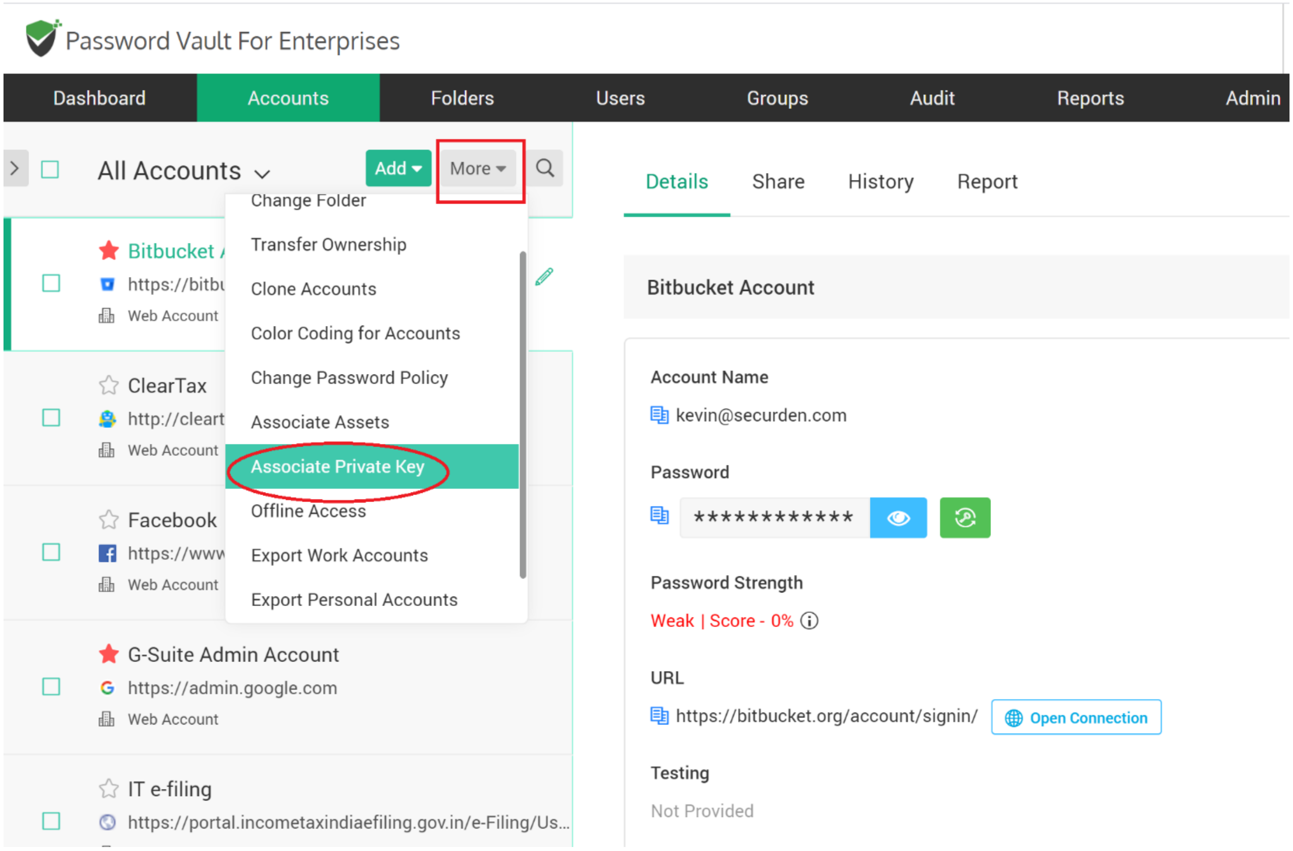
Account Name
kevin@securden.com

Password
****

Password Strength
Weak | Score - 0%

URL
https://bitbucket.org/account/signin/

Testing
Not Provided



Account Name
kevin@securden.com

Password
****

Password Strength
Weak | Score - 0%

URL
https://bitbucket.org/account/signin/

Testing
Not Provided

After adding the keys, you can associate the required key with the required account by clicking '**Associate Private Key**' option in 'More Actions' (the icon showing three horizontal lines 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.

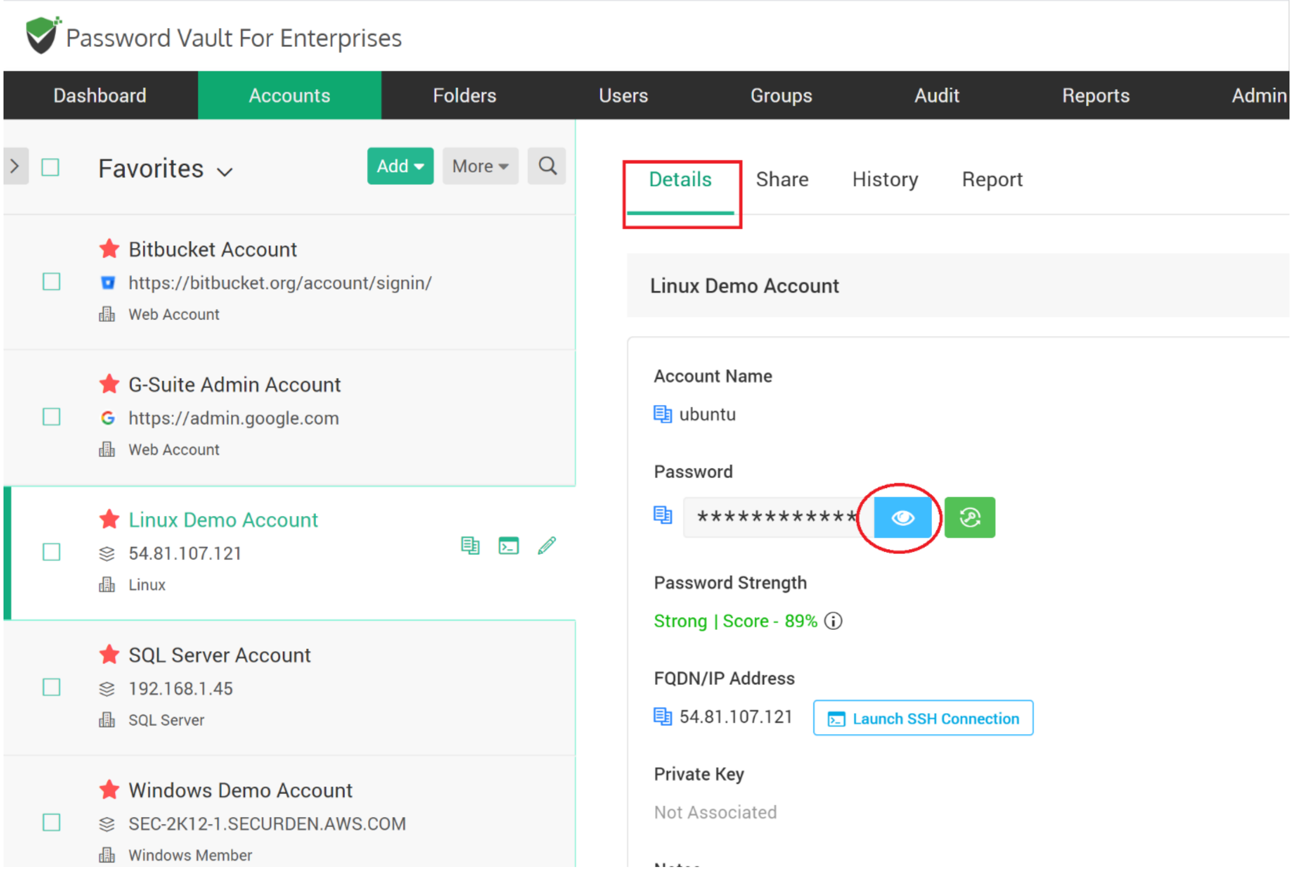
1.6 Add Documents, Files

In addition to storing passwords, you can also store and manage documents, files, images, license keys and others. 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.

Step 2: 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.



Bitbucket Account
https://bitbucket.org/account/signin/
Web Account

G-Suite Admin Account
https://admin.google.com
Web Account

Linux Demo Account
54.81.107.121
Linux

SQL Server Account
192.168.1.45
SQL Server

Windows Demo Account
SEC-2K12-1.SECURDEN.AWS.COM
Windows Member

Linux Demo Account

Account Name
ubuntu

Password
****

Password Strength
Strong | Score - 89%

FQDN/IP Address
54.81.107.121

Private Key
Not Associated

Click the 'Eye' icon to view the password. The bottom of the 'Details' section provides more information about the other attributes of the account. In addition, security-related information such account creation time, ownership details, last access and modification details.

Click '**Show More Details**' link to view these details.

Whenever you change the passwords of the accounts, you can update the same in Securden too from the **Accounts >> Details** section in the GUI. Click the '**Change**' icon located alongside the password field to change the password.

Step 3: RDP, SSH, SQL, Website Connections (Remote Connections for Employees, 3rd-party Contractors)

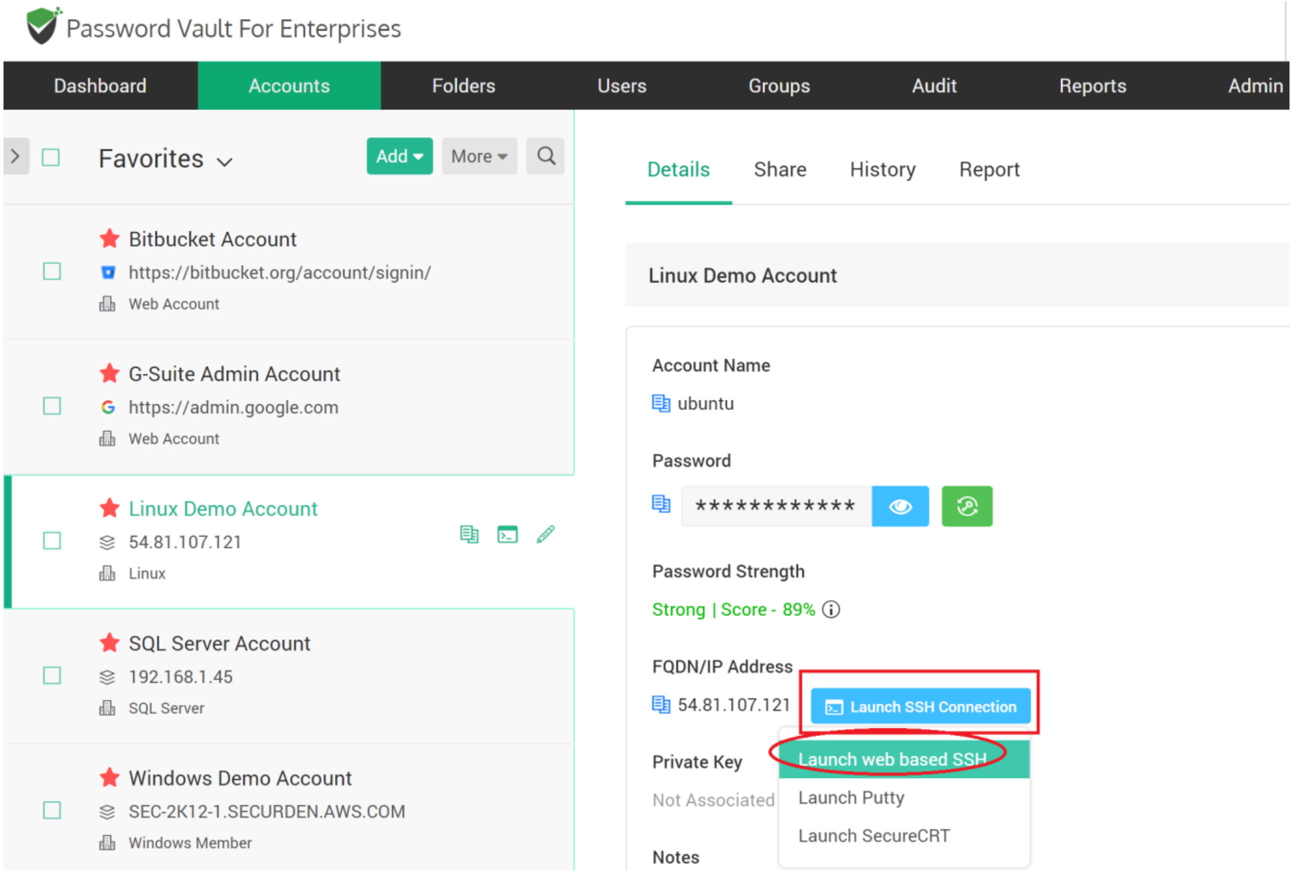
You can open direct remote connections with Windows, Linux and other devices from Securden GUI. This feature helps you can grant your remote workforce, including IT administrators, and third-party technicians secure administrative access to internal IT assets that are kept behind corporate firewalls.

You can eliminate the need for VPN and enable them to launch web-based connections or by using 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.

3.1 Web-based Connections

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

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



Bitbucket Account
https://bitbucket.org/account/signin/
Web Account

G-Suite Admin Account
https://admin.google.com
Web Account

Linux Demo Account
54.81.107.121
Linux

SQL Server Account
192.168.1.45
SQL Server

Windows Demo Account
SEC-2K12-1.SECURDEN.AWS.COM
Windows Member

Linux Demo Account

Account Name
ubuntu

Password
****

Password Strength
Strong | Score - 89%

FQDN/IP Address
54.81.107.121

Private Key
Not Associated

Notes

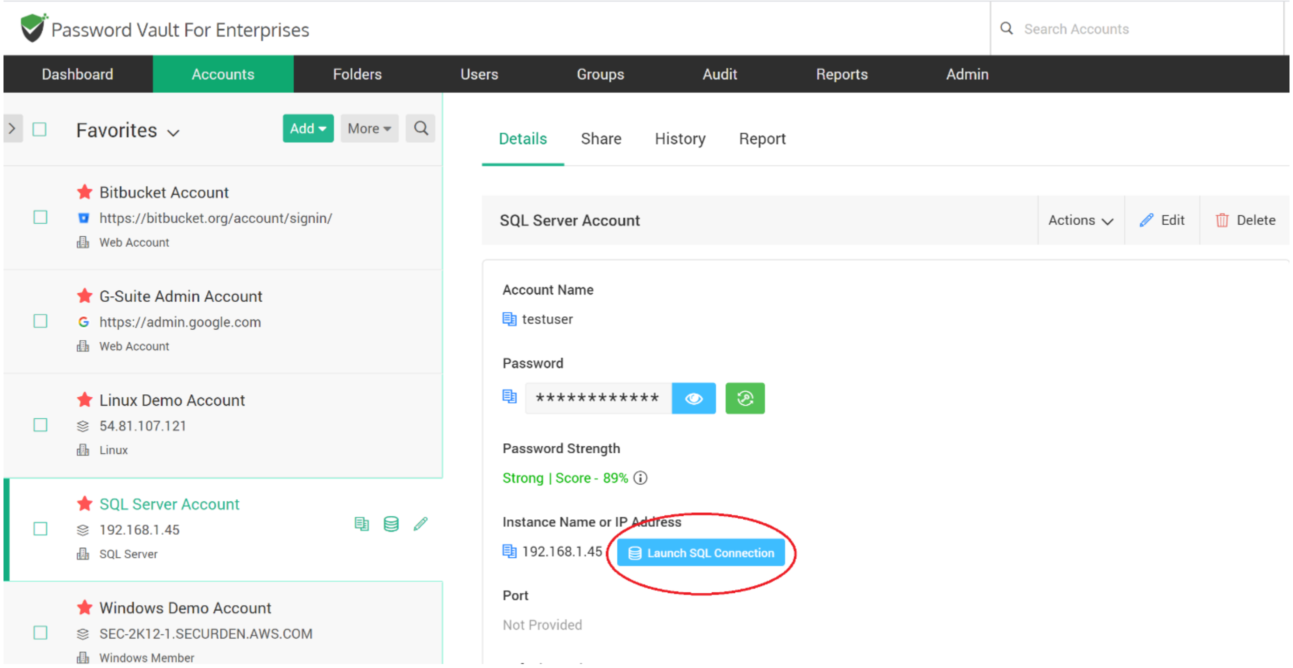
3.2 Using Native Client Applications

To use native client applications for SSH (PuTTY, SecureCRT etc.) and SQL, you need not install any pre-requisite software. For RDP connections, a light-weight 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 light-weight launcher called '**Securden Remote Launcher**' on all the machines from where you/your users would be connecting to Securden web-interface. The launcher can be downloaded and installed from **Admin >> Installers for 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**' icon 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, SSH connections don't require installation of remote launchers).



Bitbucket Account
https://bitbucket.org/account/signin/
Web Account

G-Suite Admin Account
https://admin.google.com
Web Account

Linux Demo Account
54.81.107.121
Linux

SQL Server Account
192.168.1.45
SQL Server

Windows Demo Account
SEC-2K12-1.SECURDEN.AWS.COM
Windows Member

SQL Server Account

Account Name
testuser

Password
****

Password Strength
Strong | Score - 89%

Instance Name or IP Address
192.168.1.45

Port
Not Provided

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

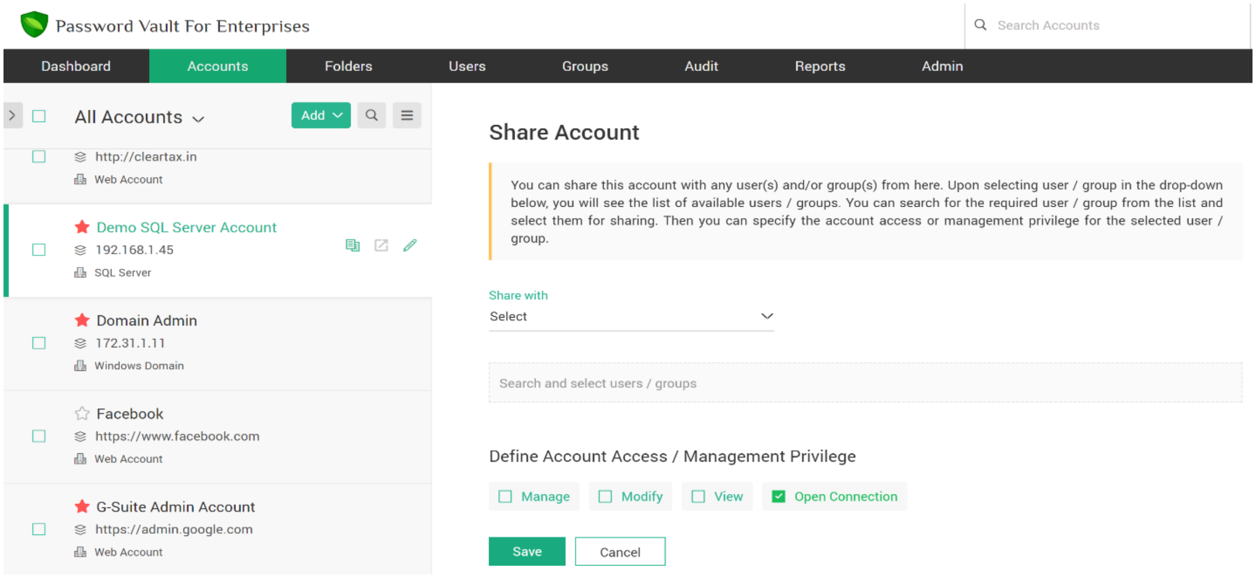
3.3 Auto-fill Credentials on Websites

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. The installation instructions and how to work with the extensions are available in this document. (Auto-fill will not work if 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.

Step 4: 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 in the right pane and then follow the instructions in the GUI.



Share Account

You can share this account with any user(s) and/or group(s) from here. Upon selecting user / group in the drop-down below, you will see the list of available users / groups. You can search for the required user / group from the list and select them for sharing. Then you can specify the account access or management privilege for the selected user / group.

Share with
Select

Search and select users / groups

Define Account Access / Management Privilege

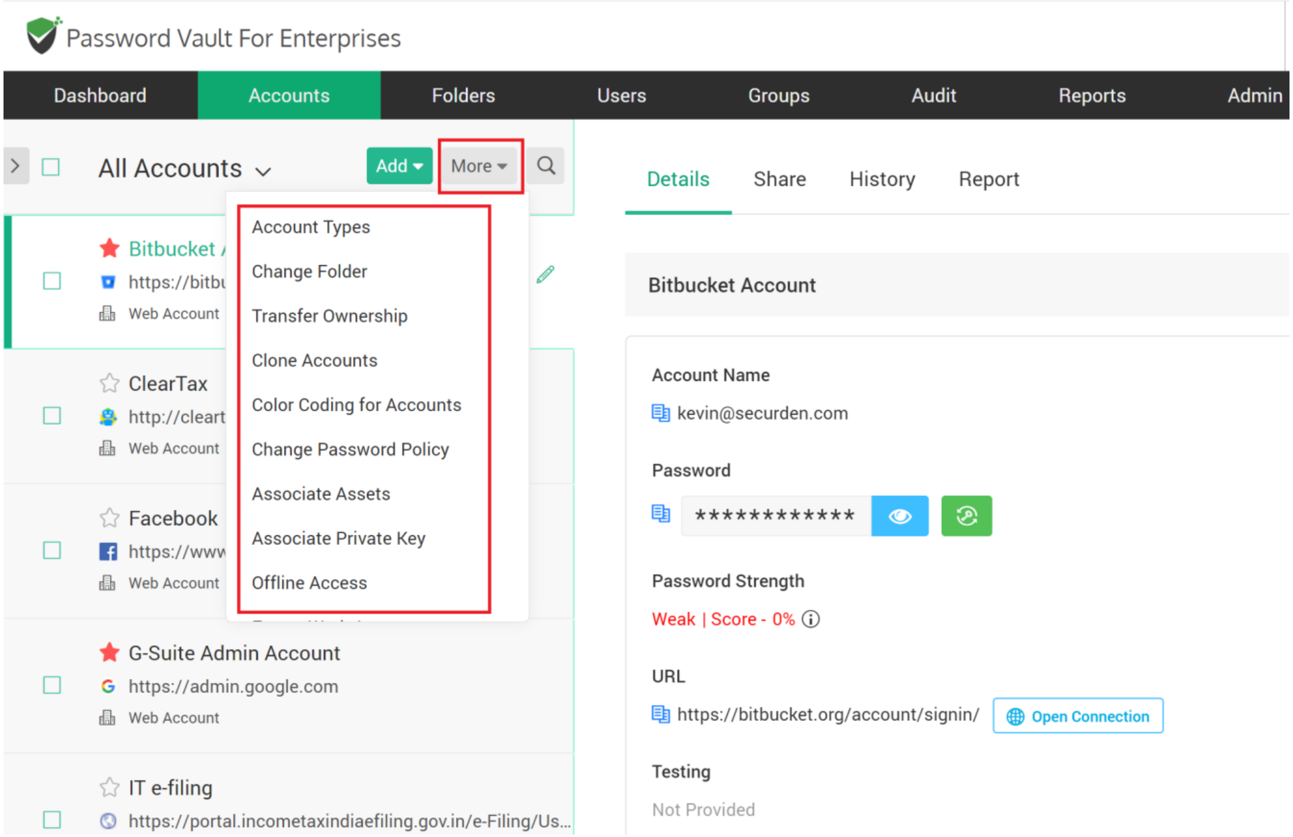
□ Manage □ Modify □ View ☑ Open Connection

Save Cancel

You can share an account with the following share 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 and is similar to concurrent ownership.

Step 5: Explore Features Under ‘More Actions’



Bitbucket A
https://bitbu
Web Account

ClearTax
http://cleart
Web Account

Facebook
https://www
Web Account

G-Suite Admin Account
https://admin.google.com
Web Account

IT e-filing
https://portal.incometaxindiaefiling.gov.in/e-Filing/Us...

Bitbucket Account

Account Name
kevin@securden.com

Password
****

Password Strength
Weak | Score - 0%

URL
https://bitbucket.org/account/signin/

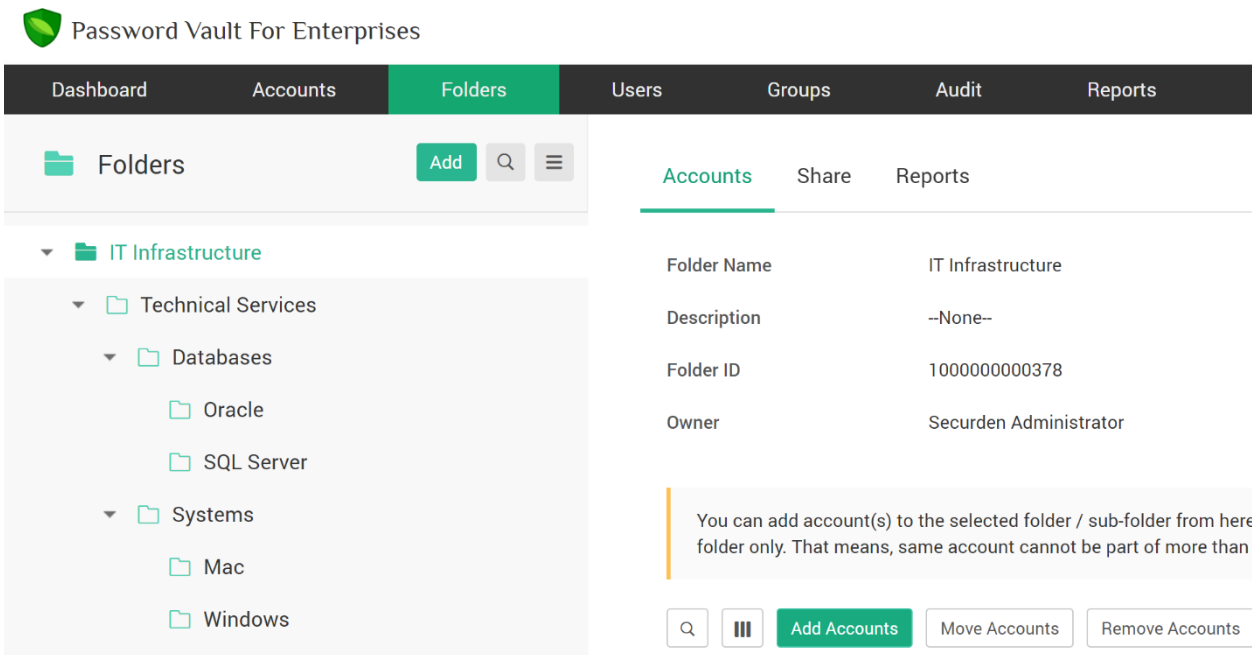
Testing
Not Provided

The **‘More’** drop-down in ‘**Accounts**’ tab contains a good number of features such as provision to transferring ownership of accounts, creating clones of existing accounts, establishing color coding for accounts for easy identification, associating SSH private keys with accounts, exporting data for offline access, provision to delete accounts and a lot more.

Navigate to **Accounts >> More Actions** in the GUI to explore these features.

Step 6: Organize Accounts by Creating Folders

You can organize the accounts in Securden by grouping them as folders for easy and efficient management. At any point of time, a specific account could remain a member of one folder only. That means, same account cannot become a member of multiple folders.



Folder Name IT Infrastructure

Description --None--

Folder ID 1000000000378

Owner Securden Administrator

You can add account(s) to the selected folder / sub-folder from here
folder only. That means, same account cannot be part of more than

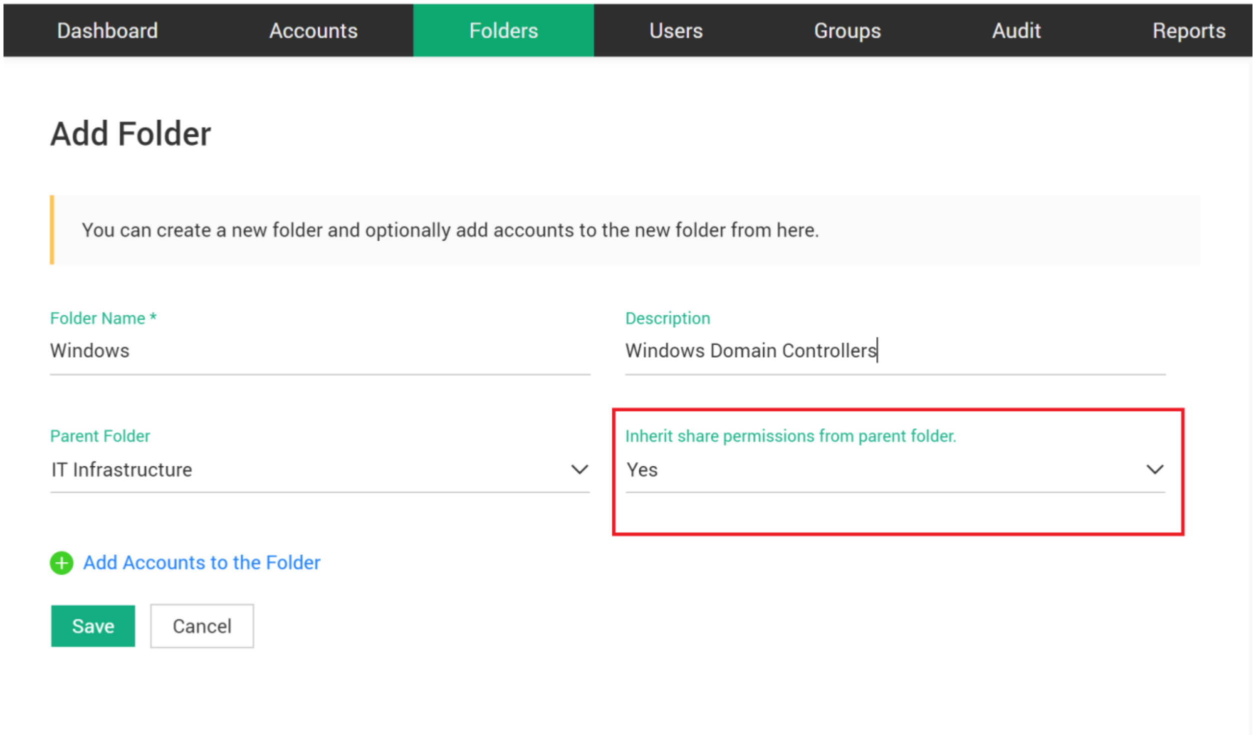
If you structure the folders in Securden to reflect your organizational hierarchy, you will be able to easily achieve permissions inheritance. Navigate to **Folders >> Add Folder** in the GUI to perform this step.

Step 7: Share Folders with Users/Groups

You can share an entire folder or a sub-folder with any user(s) and/or user group(s). When you share the folder, all the accounts that are part of the folder get shared. To share a folder, navigate to **Folders** section in the GUI, **click the required folder,** click the '**Share**' tab in the right pane and then follow the instructions in the GUI.

Sharing a folder along with its sub-folders – Permissions inheritance

If you want to share a folder along with any/all of its sub-folders, you need to take care of permissions inheritance from the parent folder. Sub-folder sharing in Securden is handled through permissions inheritance. Sub-folders can inherit share permissions from the parent folder. While creating the sub-folders, you need to select "yes" for the field "**inherit share permissions from parent folder**".



Add Folder

You can create a new folder and optionally add accounts to the new folder from here.

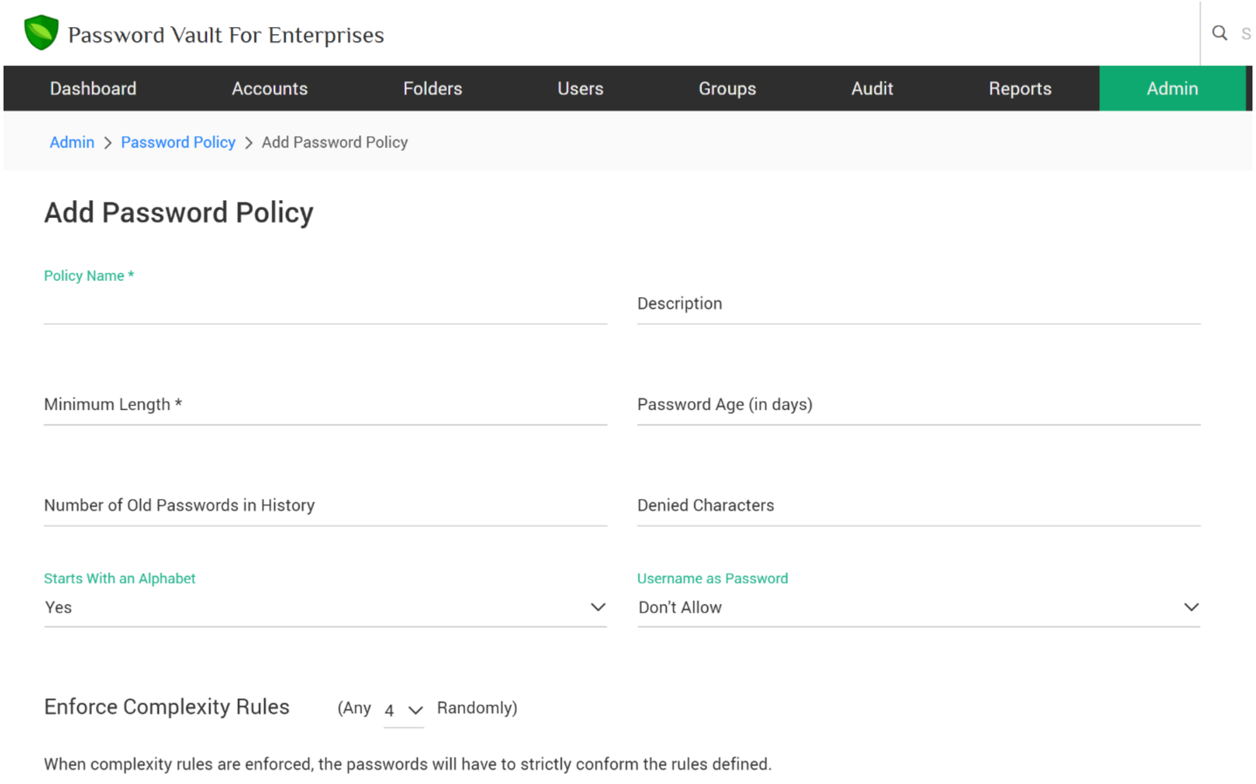
Folder Name * Windows

Description Windows Domain Controllers

Parent Folder IT Infrastructure

Inherit share permissions from parent folder. Yes

Step 8: Create and Enforce Password Policy


Password Vault For Enterprises
Dashboard
Accounts
Folders
Users
Groups
Audit
Reports
Admin
Admin > Password Policy > Add Password Policy

Add Password Policy

Policy Name *

Description

Minimum Length *

Password Age (in days)

Number of Old Passwords in History

Denied Characters

Starts With an Alphabet Yes

Username as Password Don't Allow

Enforce Complexity Rules (Any 4 Randomly)

When complexity rules are enforced, the passwords will have to strictly conform the rules defined.

Security best practices recommend usage of strong, unique passwords for every account. Password policy in Securden helps you define the strength, complexity requirements, periodicity for password resets and other conditions. Securden password generator will generate passwords as per the policy defined.

Navigate to **Admin >> Account Management >> Password Policy** in the GUI to create password policies.

After creating a policy that suits your requirements, you can set that policy as the default policy for your organization from **Admin >> Account Management >> Password Policy >> Set As Default Policy** section in the GUI.

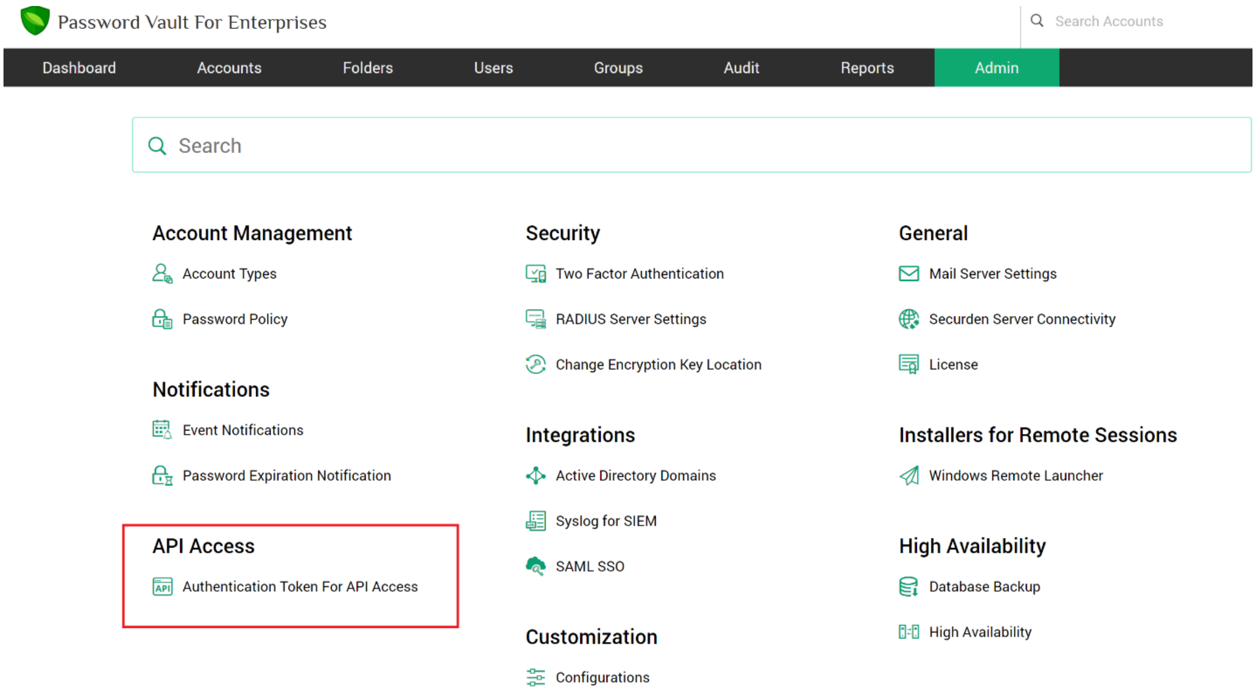
In addition, you can enforce password policies at '**Account Types**' level. Each account type can have a different password policy. You can also enforce password policy validation during account addition **Admin >> General >> Configurations >> Password Policy** section.

When you do so, Securden will allow only the accounts that conform to the policy defined. You can make use of the password generator to generate strong passwords, apply them to the respective websites first and then update the Securden Vault.

Step 9: Application Password Management using APIs

Securden provides APIs for application-to-application and application-to-database communication. APIs can be used to connect to Securden and fetch the required data automatically.

Navigate to **Admin >> API Access >> Authentication Token for API Access** to start using the APIs. Refer to the API reference guide for information on making use of the APIs.



Account Management
- Account Types
- Password Policy

Notifications
- Event Notifications
- Password Expiration Notification

API Access
- Authentication Token For API Access

Security
- Two Factor Authentication
- RADIUS Server Settings
- Change Encryption Key Location

Integrations
- Active Directory Domains
- Syslog for SIEM
- SAML SSO

Customization
- Configurations

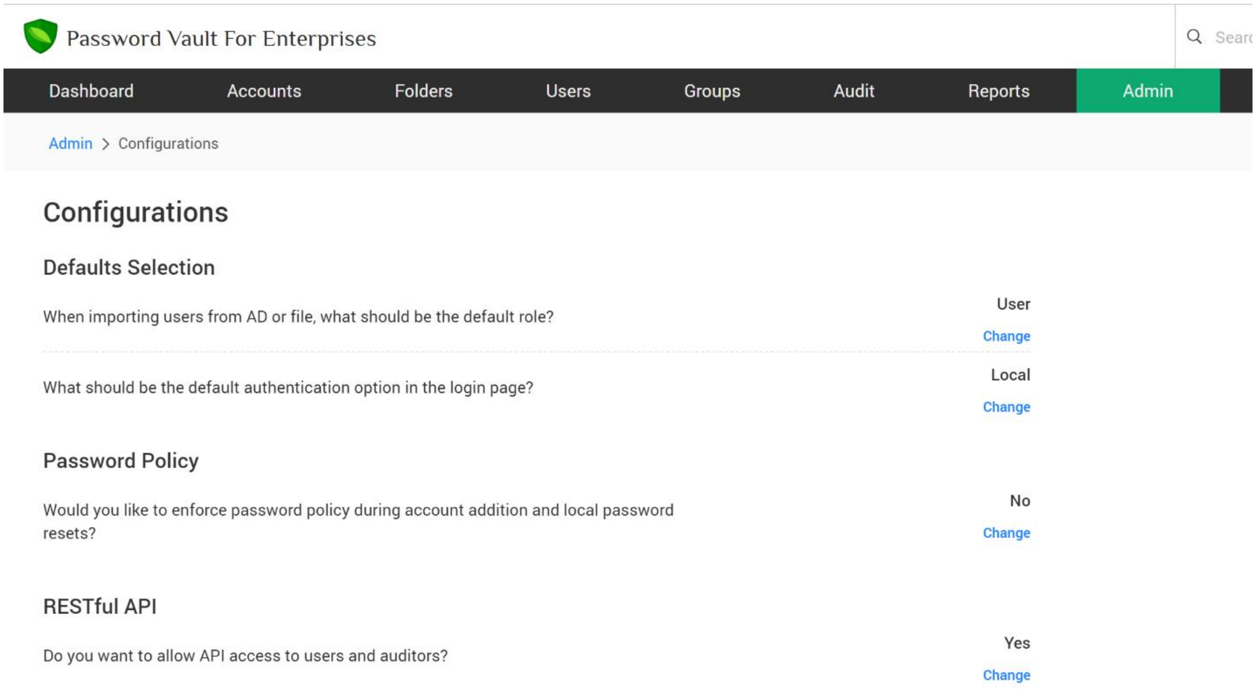
General
- Mail Server Settings
- Securden Server Connectivity
- License

Installers for Remote Sessions
- Windows Remote Launcher

High Availability
- Database Backup
- High Availability

Step 10: Customize the Features

You can customize the features of Securden in a granular manner. You can switch on and switch off certain features anytime as desired. Navigate to **Admin >> Customization >> Configurations** section to exercise the customization options.



Configurations

Defaults Selection

When importing users from AD or file, what should be the default role? User Change

What should be the default authentication option in the login page? Local Change

Password Policy

Would you like to enforce password policy during account addition and local password resets? No Change

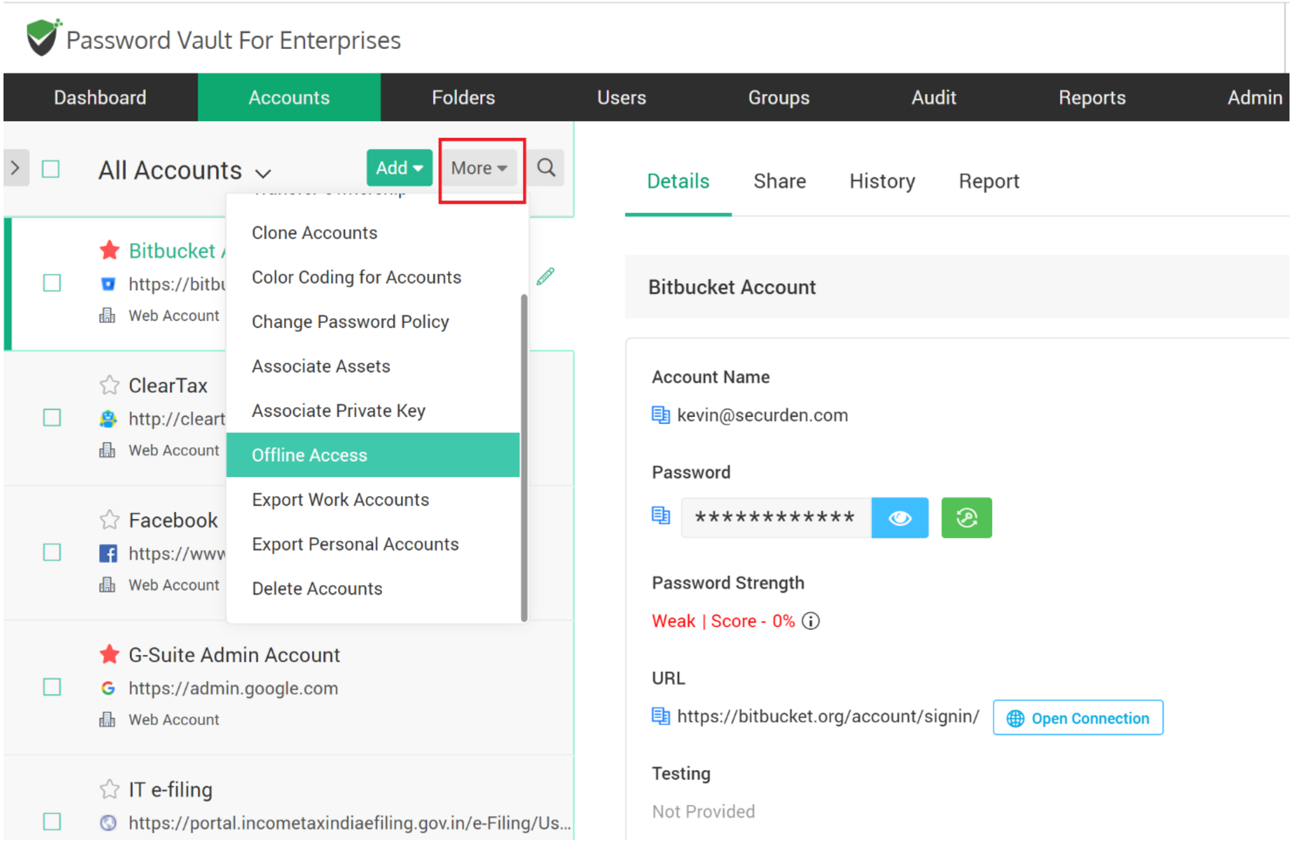
RESTful API

Do you want to allow API access to users and auditors? Yes Change

Step 11: Configure Offline Access

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.



Bitbucket Account

Account Name
kevin@securden.com

Password
****

Password Strength
Weak | Score - 0%

URL
https://bitbucket.org/account/signin/

Testing
Not Provided

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.

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. Navigate to **Accounts** section in the GUI, from "**More Actions**" (three vertical lines icon in the LHS), click the '**Offline Access**' option and then follow the instructions in the GUI.

Step 12: Secure Access over the Internet

(Restricted Access to Securden interface for Remote Employees over Internet)

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. Basically, this requires adding to the browser either a valid CA-signed certificate (.p12 or .pfx or .keystore) or a private keypair generated by Securden in .pfx format. Only those users who possess the certificate will be able to access Securden.

Navigate to **Admin >> Restricted Access Over the Internet >> Certificate-based Authentication** section for details.

Step 13: Configure Notifications

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.

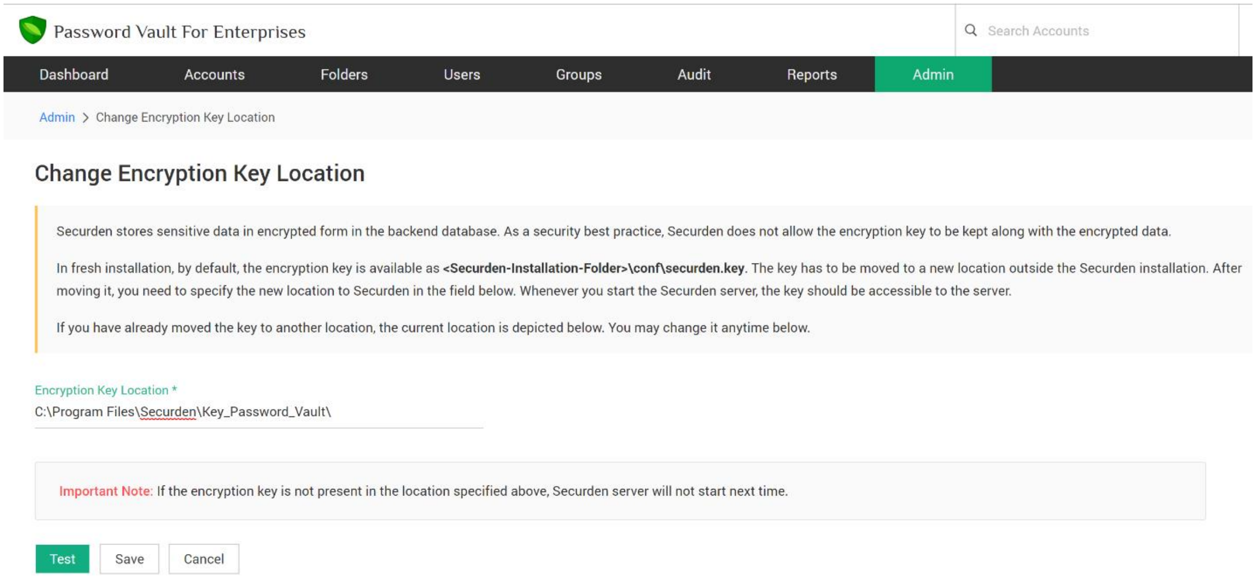
Navigate to **Admin >> Notifications >> Event Notifications** section to configure notifications. Similarly, you can configure password expiration notifications. Based on the password age set as part of password policy, Securden sends timely notifications reminding about password expiration.

Step 14: Change the Encryption Key Location

Every installation of Securden is guarded by a unique encryption key. In a fresh installation for evaluation purposes, by default, the encryption key is available as <Securden-Installation-Folder>\conf\securden.key.

The key has to be moved to a new location outside the Securden installation folder as Securden doesn't allow the encryption key and the encrypted data to be kept together. Securden enforces this once you apply the registered license key and move to production. It is recommended to move the key even during the evaluation process.

After moving the key to a new location, you need to specify the new location in the GUI. Whenever you start the Securden server, the key should be accessible to the server. Otherwise, the server won't start and you won't be able to access the passwords. You can manage the key location from **Admin >> Security >> Change Encryption Key Location**.


Password Vault For Enterprises
Search Accounts
Dashboard
Accounts
Folders
Users
Groups
Audit
Reports
Admin
Admin > Change Encryption Key Location

Change Encryption Key Location

Securden stores sensitive data in encrypted form in the backend database. As a security best practice, Securden does not allow the encryption key to be kept along with the encrypted data.

In fresh installation, by default, the encryption key is available as **<Securden-Installation-Folder>\conf\securden.key**. The key has to be moved to a new location outside the Securden installation. After moving it, you need to specify the new location to Securden in the field below. Whenever you start the Securden server, the key should be accessible to the server.

If you have already moved the key to another location, the current location is depicted below. You may change it anytime below.

Encryption Key Location *
C:\Program Files\Securden\Key_Password_Vault\

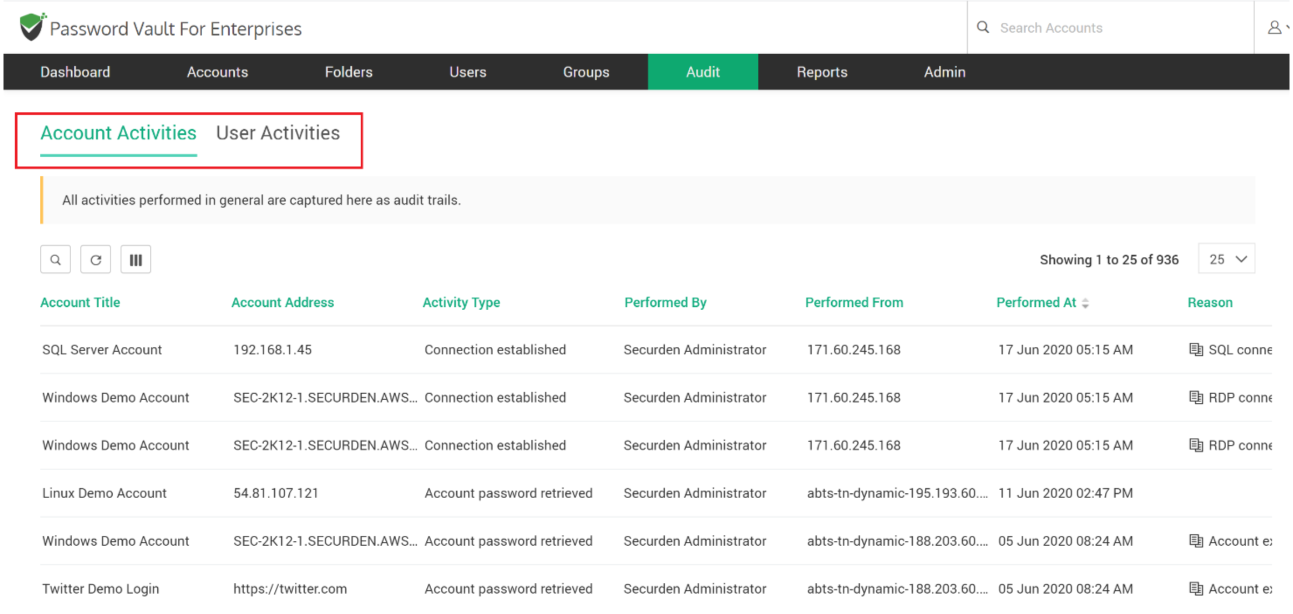
Important Note: If the encryption key is not present in the location specified above, Securden server will not start next time.

Section 4: Audit Trails, Reports

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.

4.1 Audit Trails

To view the audit trails, navigate to the ‘**Audit**’ tab in the GUI. The trails are classified into two categories – account activities and user activities. Account activities capture the activities on the accounts. User activities capture the activities of the users.



All activities performed in general are captured here as audit trails.

Account Title	Account Address	Activity Type	Performed By	Performed From	Performed At	Reason
SQL Server Account	192.168.1.45	Connection established	Securden Administrator	171.60.245.168	17 Jun 2020 05:15 AM	SQL conne
Windows Demo Account	SEC-2K12-1.SECURDEN.AWS...	Connection established	Securden Administrator	171.60.245.168	17 Jun 2020 05:15 AM	RDP conne
Windows Demo Account	SEC-2K12-1.SECURDEN.AWS...	Connection established	Securden Administrator	171.60.245.168	17 Jun 2020 05:15 AM	RDP conne
Linux Demo Account	54.81.107.121	Account password retrieved	Securden Administrator	abts-tn-dynamic-195.193.60....	11 Jun 2020 02:47 PM	
Windows Demo Account	SEC-2K12-1.SECURDEN.AWS...	Account password retrieved	Securden Administrator	abts-tn-dynamic-188.203.60....	05 Jun 2020 08:24 AM	Account e:
Twitter Demo Login	https://twitter.com	Account password retrieved	Securden Administrator	abts-tn-dynamic-188.203.60....	05 Jun 2020 08:24 AM	Account e:

4.2 Explore Reports

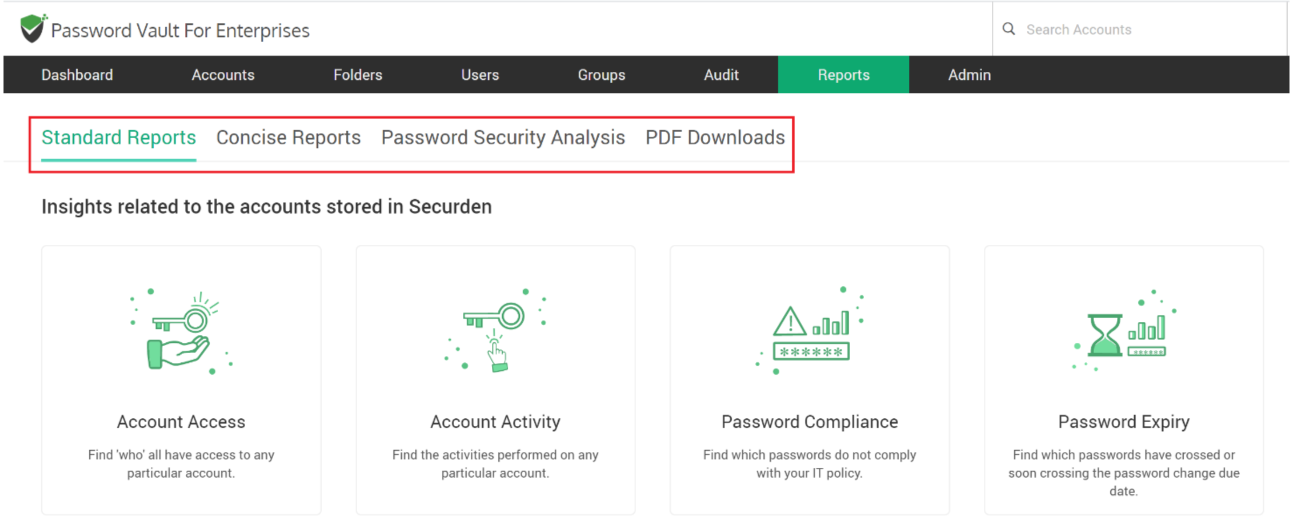
Reports are classified into three categories – standard reports, concise reports, and security analysis report. All the reports can be downloaded in the form of PDF.

Standard Reports

Standard reports provide a detailed reporting on a specific topic. For example, 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.

Other reports in this section include:

Account Access Report (list of users who have access to a particular account), **Account Activity** (list of activities on a specific account), **User Activity** (list of activities of a specific user), **Password Compliance** (whether stored passwords comply to the organization's IT policy), **Password Expiration Report** (information on the passwords that are due for changing, the ones already expired etc.).



Insights related to the accounts stored in Securden

Account Access
Find 'who' all have access to any particular account.

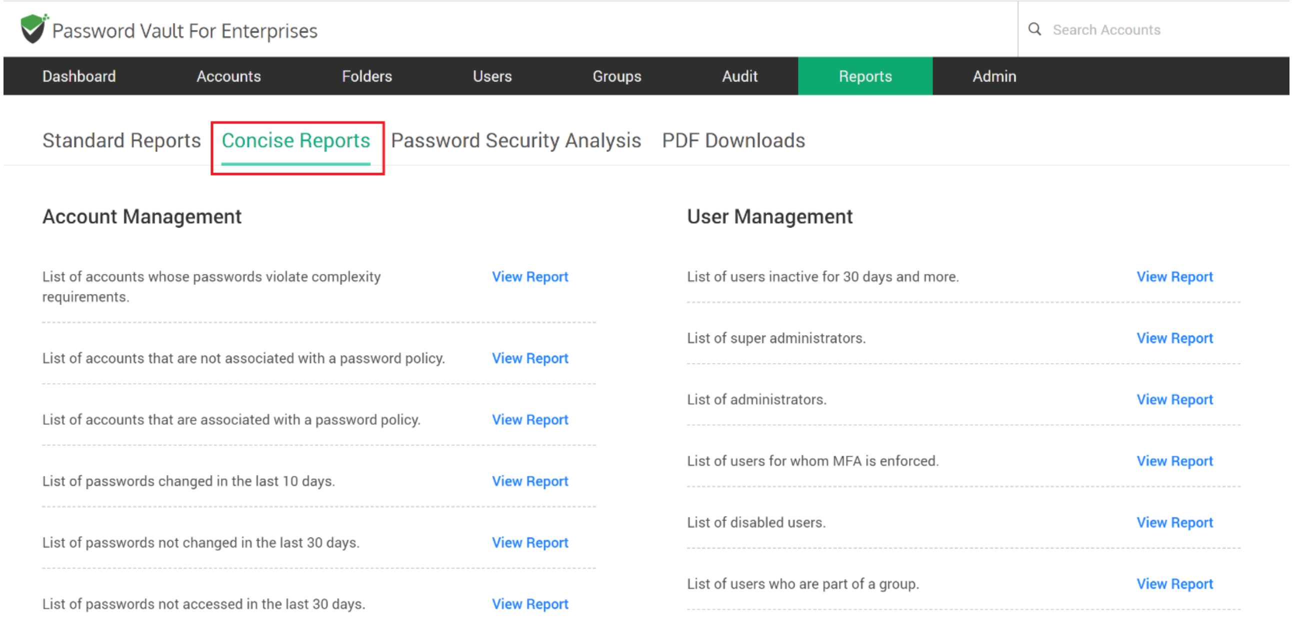
Account Activity
Find the activities performed on any particular account.

Password Compliance
Find which passwords do not comply with your IT policy.

Password Expiry
Find which passwords have crossed or soon crossing the password change due date.

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.



Account Management

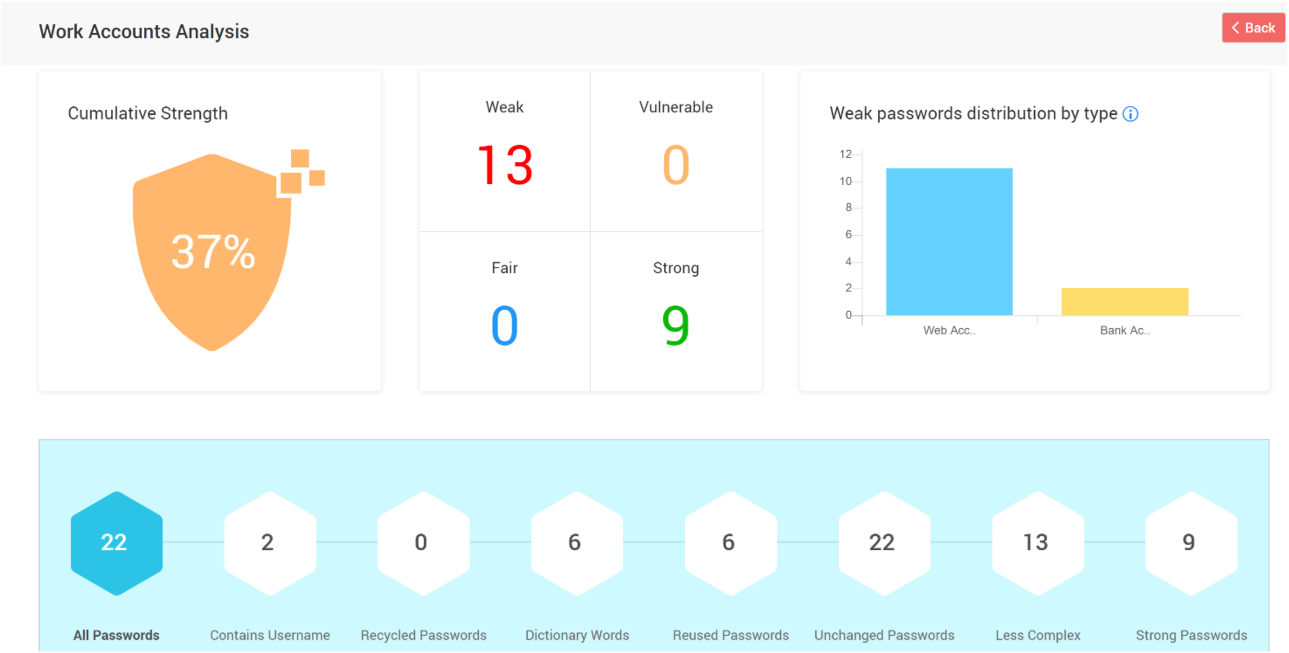
List of accounts whose passwords violate complexity requirements.	View Report
List of accounts that are not associated with a password policy.	View Report
List of accounts that are associated with a password policy.	View Report
List of passwords changed in the last 10 days.	View Report
List of passwords not changed in the last 30 days.	View Report
List of passwords not accessed in the last 30 days.	View Report

User Management

List of users inactive for 30 days and more.	View Report
List of super administrators.	View Report
List of administrators.	View Report
List of users for whom MFA is enforced.	View Report
List of disabled users.	View Report
List of users who are part of a group.	View Report

Password Security Analysis Report

Securden carries out a comprehensive analysis of various passwords used 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 security analysis report is provided separately for work and personal accounts.

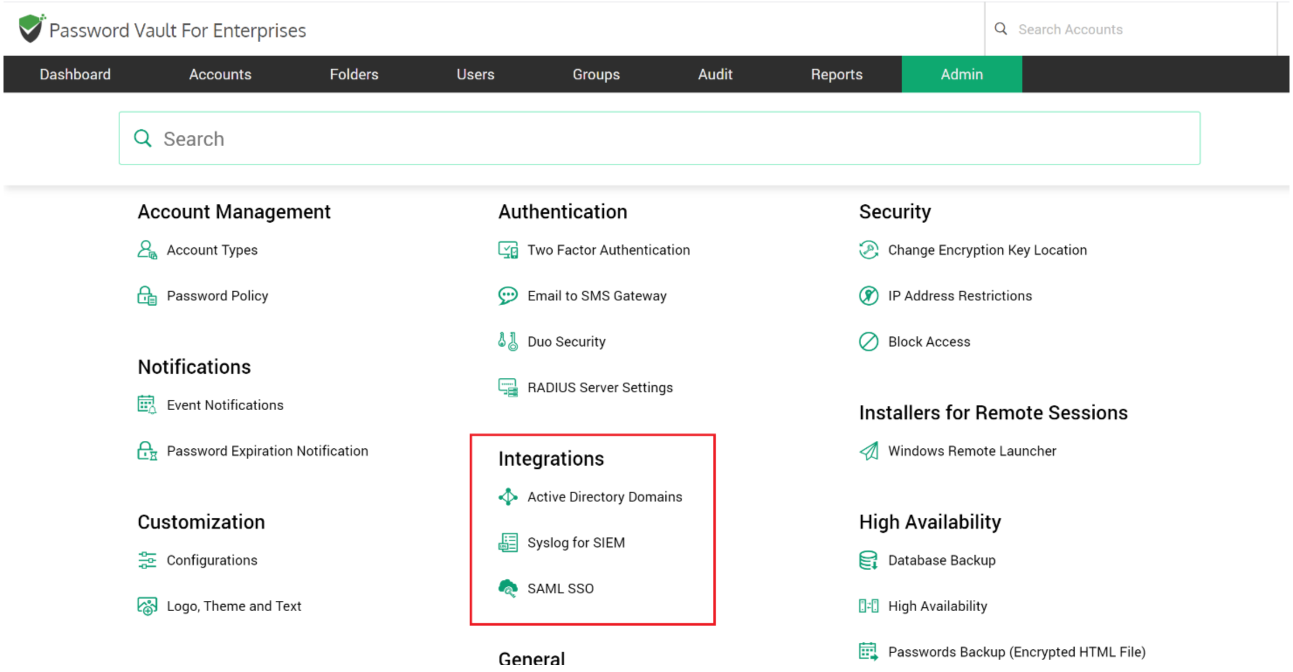


Section 5: Integrations & Security Aspects

Securden readily integrates with various enterprise infrastructure and also offers a good number of options to add additional layers of security.

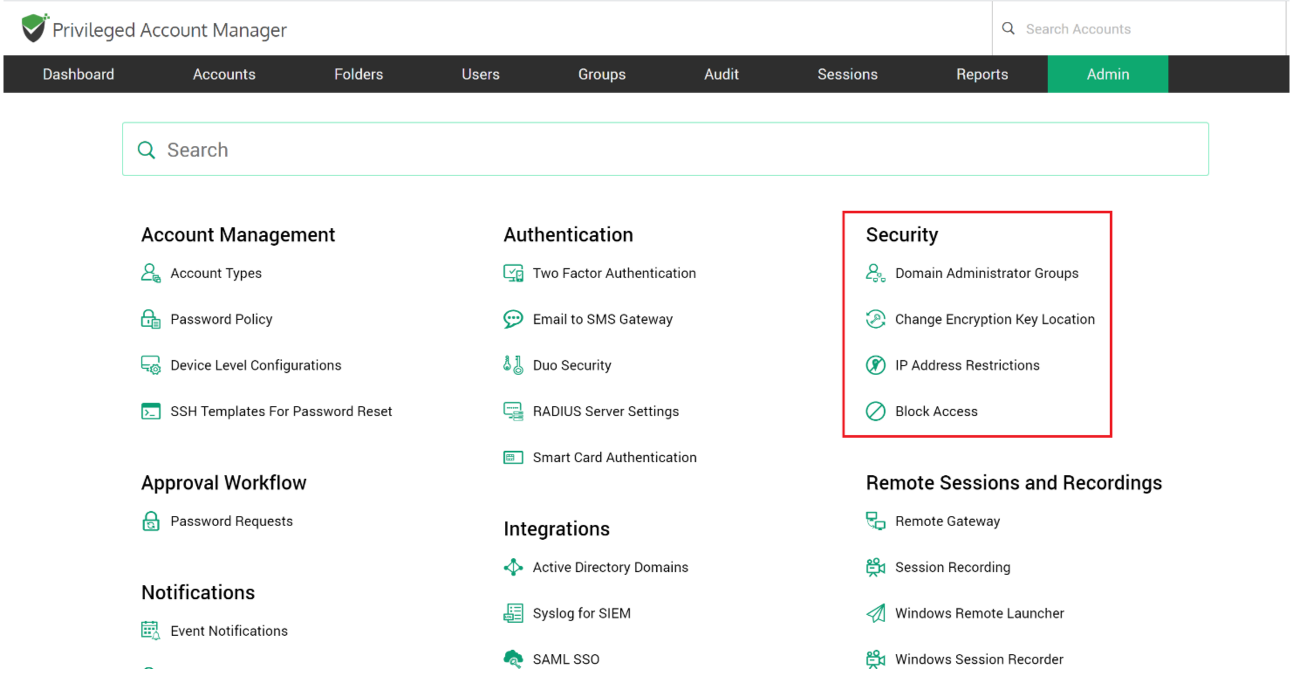
5.1 Integrations

To explore integrations, navigate to **Admin >> Integrations**. You will find the steps to integrate with SIEM solutions, and SAML-based Single Sign On solutions.



5.2 Additional Security Aspects

To explore the additional security aspects, navigate to **Admin >> Security** section. You can monitor the changes happening to Windows domain administrator groups, establish IP-based restrictions for accessing Securden web-interface, and control/block access to Securden through browser extensions and APIs.



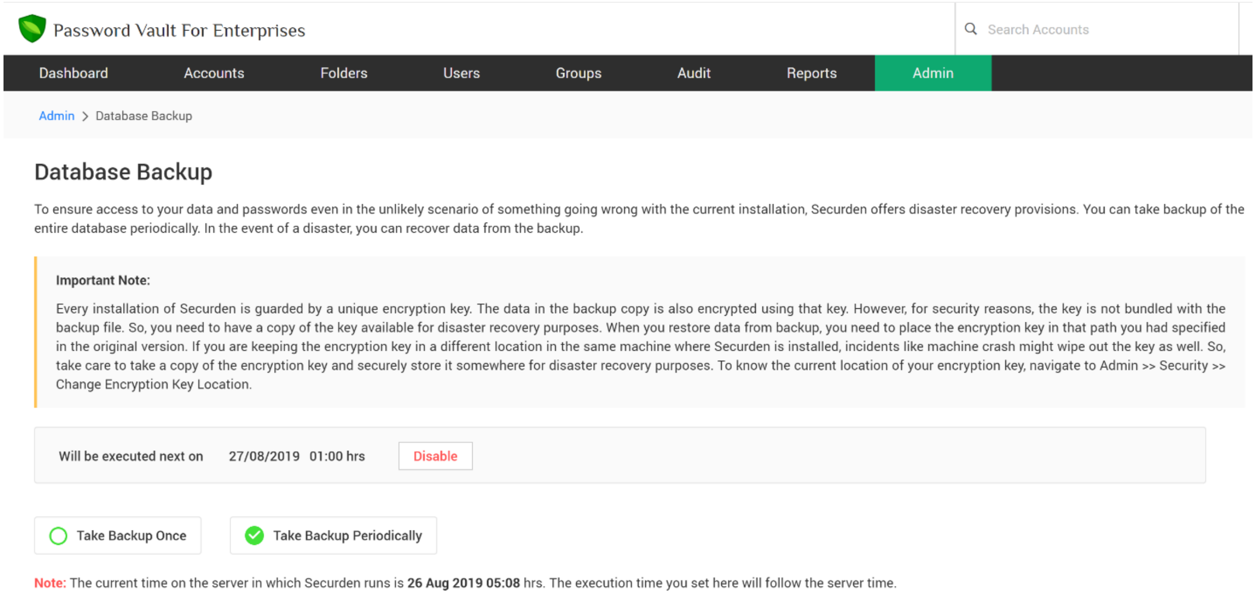
Section 6: Database Backup, Disaster Recovery and High Availability

6.1 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. In the event of a disaster, you can recover data from the backup.

Securden allows you to specify the "Backup Destination". You may give the network path of a remote machine, where the backup copy will be stored. The periodicity could be as low as one hour and you may decide to maintain x number of past backup copies.

Navigate to **Admin >> High Availability >> Database Backup** in the GUI to perform this.



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. In the event of a disaster, you can recover data from the backup.

Important Note:

Every installation of Securden is guarded by a unique encryption key. The data in the backup copy is also encrypted using that key. However, for security reasons, the key is not bundled with the backup file. So, you need to have a copy of the key available for disaster recovery purposes. When you restore data from backup, you need to place the encryption key in that path you had specified in the original version. If you are keeping the encryption key in a different location in the same machine where Securden is installed, incidents like machine crash might wipe out the key as well. So, take care to take a copy of the encryption key and securely store it somewhere for disaster recovery purposes. To know the current location of your encryption key, navigate to Admin >> Security >> Change Encryption Key Location.

Will be executed next on 27/08/2019 01:00 hrs

Note: The current time on the server in which Securden runs is **26 Aug 2019 05:08** hrs. The execution time you set here will follow the server time.

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 placed under **<Securden-Installation-Folder>/conf/securden.key**.

In production instances, Securden doesn't allow the encryption key and encrypted data to reside together. It has to be moved to some other location. Every time when you start Securden server, the key should be available in the path specified. 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.

6.2 Disaster Recovery

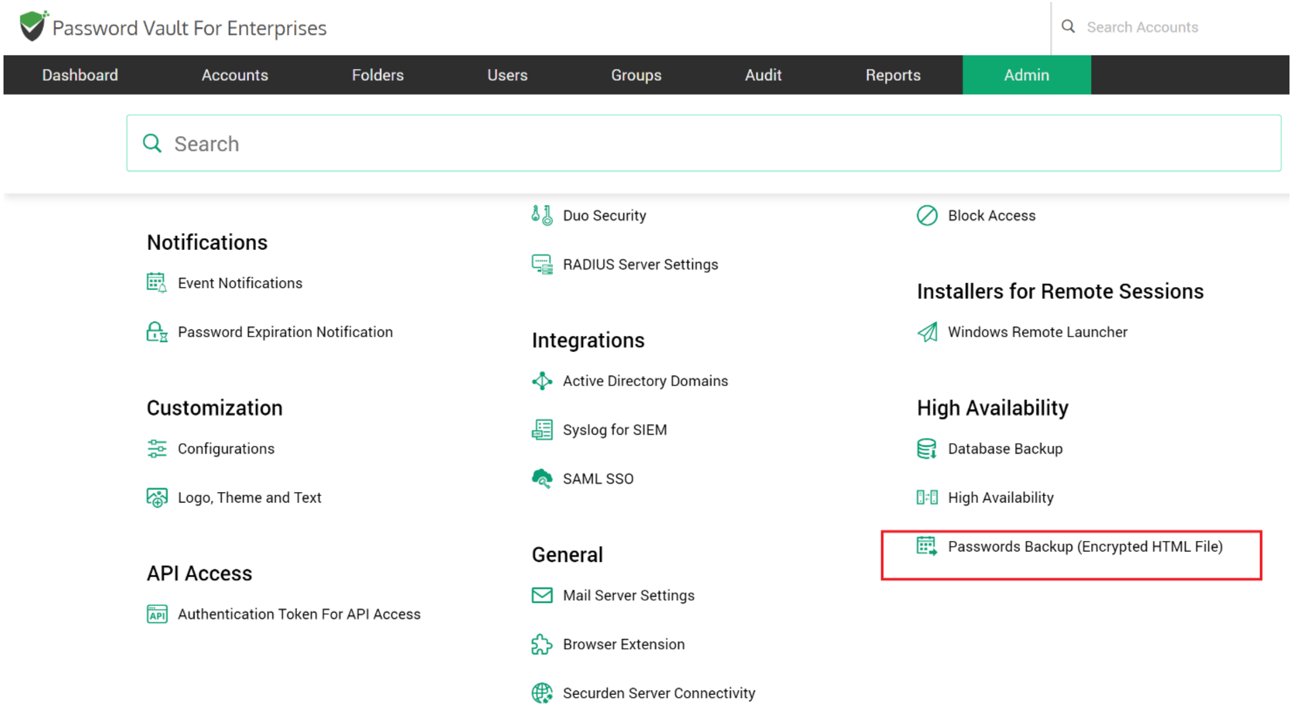
Steps to restore data from backup copy

If you want to test how data restoration works, take a copy of the entire Securden installation folder and keep it in a secure location.

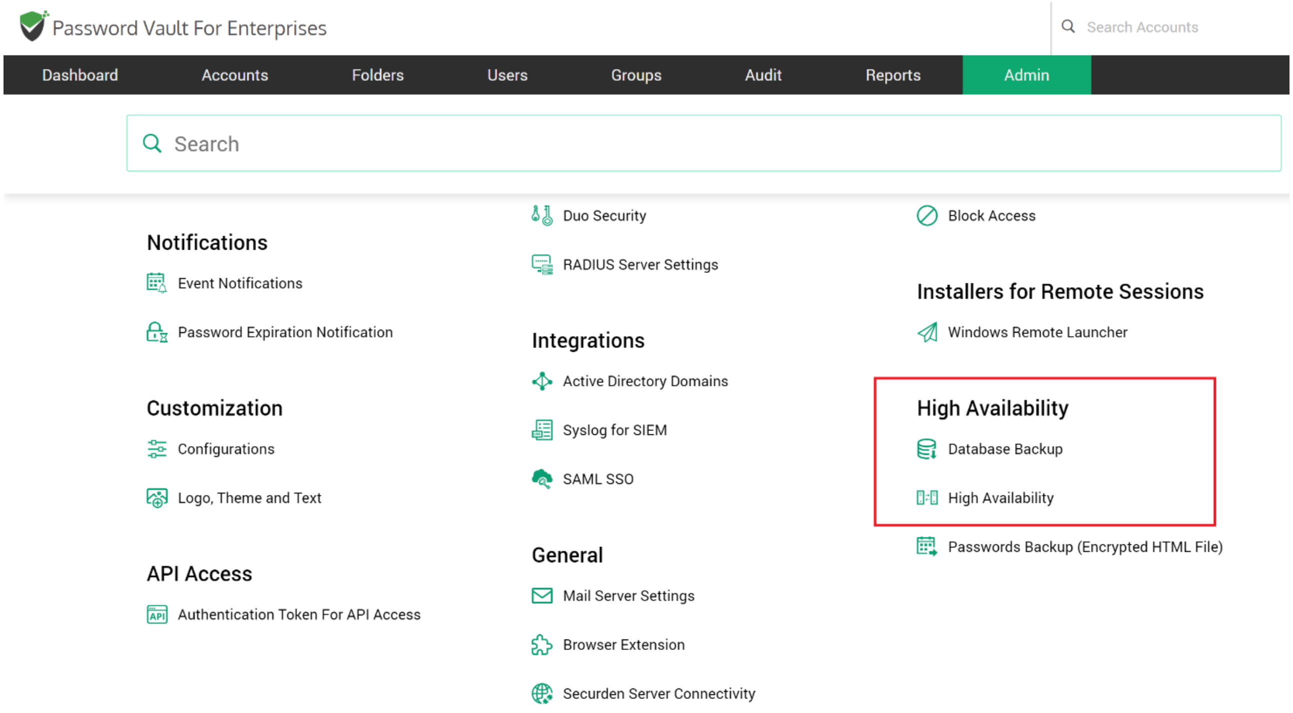
- Install the product in another machine **without disturbing the existing version** (if you are using Securden versions prior to 6.2.2, the product version of the restoration copy should be the same as the backup product version. From v 6.2.2 onwards, this restriction has been removed. If you are using previous versions, write to Securden support to get the required product version).
- Stop the Securden server
- Open a command prompt with admin privilege and navigate to **<Securden-Installation-Folder>/bin** folder
- Execute **RestoreDatabase.exe** <enter the full path of the backup file> Example: **RestoreDatabase.exe** C:\Program Files\Securden\Password_Vault\exports\PostgreSQL_Backups\Securden_postgresql_db_backup_2019-05-22-11-48-22.zip
- The backup copy also shares the same encryption key as that of the original copy. Ensure that the encryption key is available in the location as specified in the current version (you may identify the current location of the encryption key from **Admin >> Change Encryption Key** file)
- Start Securden Vault Service (You may safely ignore the other service named Securden Web Service, which is automatically taken care of).

6.3 Periodic Backup of Passwords as Encrypted HTML

As an additional backup option, Securden allows **Super Administrators** to create a scheduled task for taking a backup of all work accounts in the form of an encrypted HTML file. When configuring the schedule, a passphrase has to be provided, which will be used as the encryption key. Whenever the backup copy is to be viewed, passphrase has to be supplied. Without the passphrase, the backup copy cannot be opened. The encrypted HTML file can be stored in a secure, remote location.



6.4 Configure High Availability



To ensure uninterrupted access to accounts and passwords, Securden comes with high availability architecture. This is achieved by deploying another application server, which would serve as the secondary server. In the event of the primary server going down, users can connect to the secondary server.

Navigate to **Admin >> High Availability** in the GUI to configure High Availability.

Note: You can configure any number of additional application servers and deploy them in different locations. If you are using MS SQL server as the backend database, you can make use of SQL clusters.

Section 7: Miscellaneous

7.1: Explore Mobile Apps

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

7.2 Replacing Self-Signed Certificate

By default, Securden comes bundled with a self-signed certificate. You can add your own CA signed certificate by following the steps below. Basically, Securden requires the certificate and the private key.

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

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

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

Step 2: Copy your certificate (e.g. certificate.pfx) and paste it in the

system from where you can execute OpenSSL exe.
The *.pfx file is in PKCS#12 format and includes both the certificate and the private key.

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

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

Step 4: Run the following command to export the certificate

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

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

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

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

This replaces the self-signed certificate with your certificate.

7.3 (Optional): Change 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 Service**" from services.msc (in the machine in which Securden is installed)
- Navigate to **<Securden Installation Folder>/bin** folder and execute "**ChangeDatabase.exe**" and in the GUI, supply SQL instance name, database name, username, and password to connect to the database.
- Now, start the "**Securden 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>:5454 (or) https://<host-name>:5454
- Clear browser cache

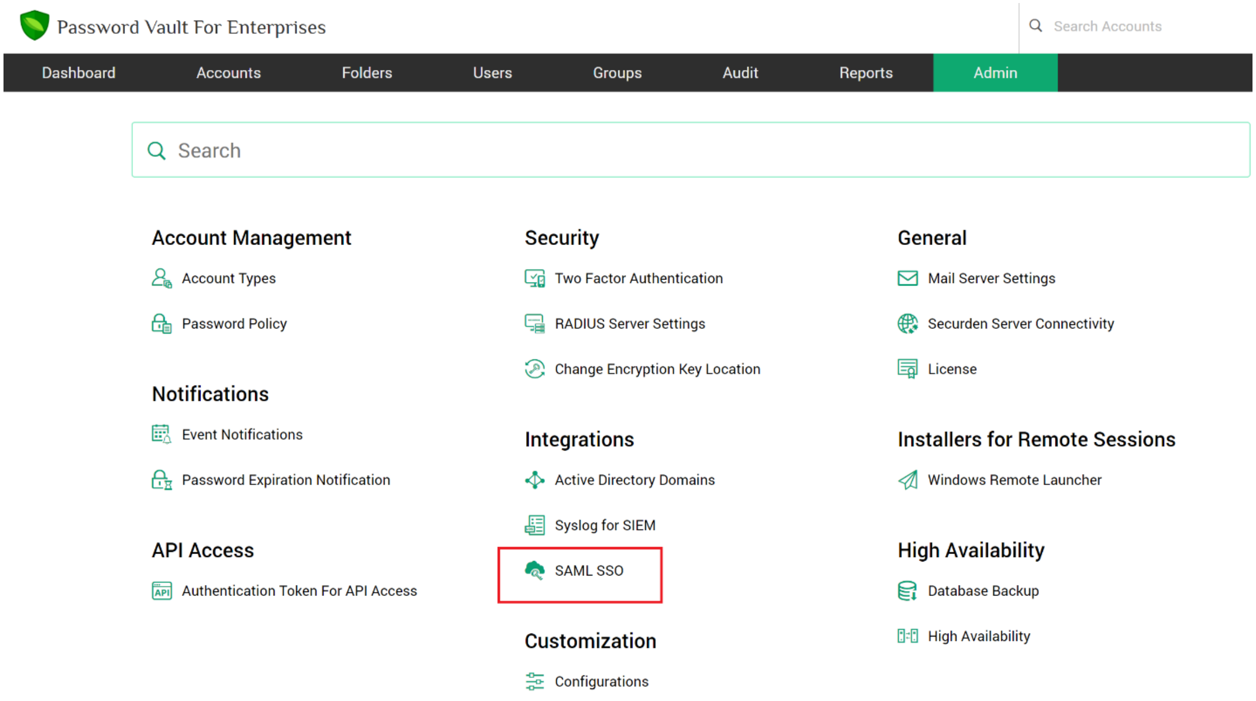
7.4 Single Sign On: Federation with Identity Providers

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

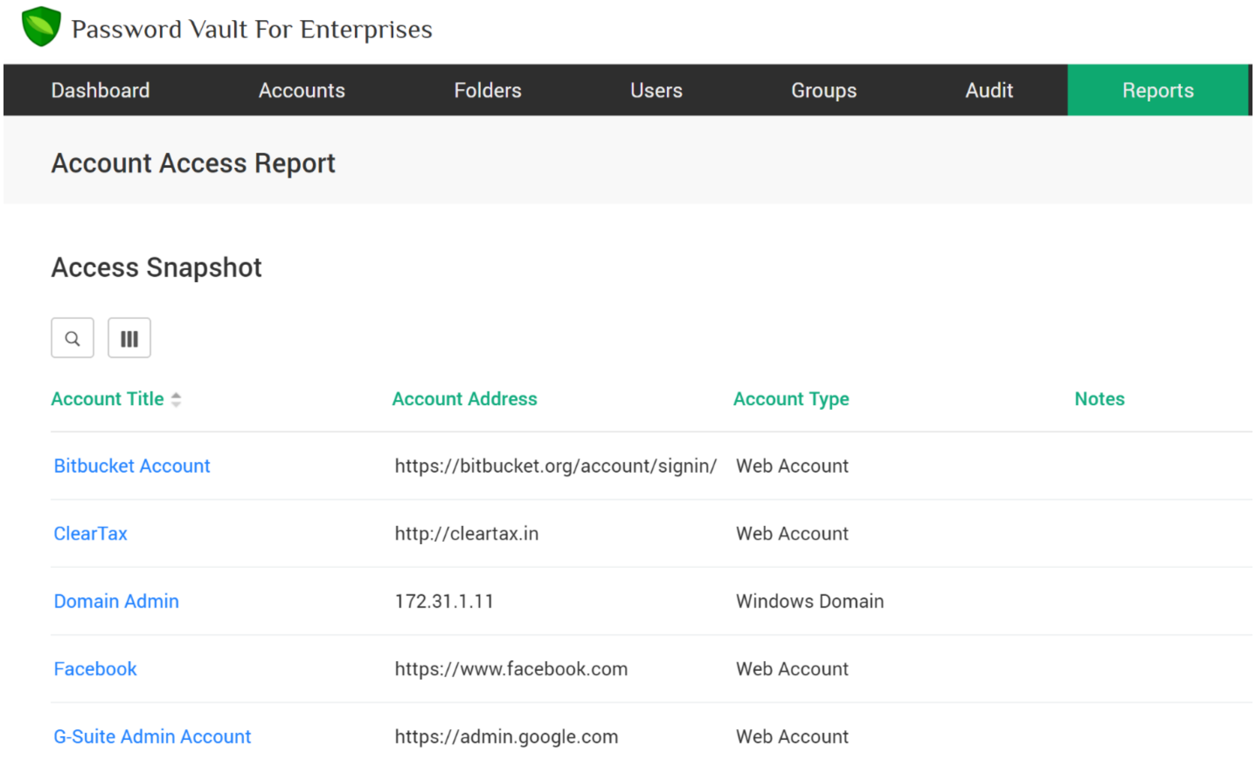
Securden serves as the SAML Service Provider (SP) and it integrates with SAML Identity Providers (IdP). Once this is done, users who login to solutions like Okta (IdP), will be automatically logged in to Securden. The IdP and Securden exchange validation details in the background. Steps below involve providing details about the SP to the respective IdP:

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

Navigate to **Admin >> Integrations >> SAML SSO** to integrate Securden with any of your SAML 2.0 identity provider.



7.5 Track 'Who' has access to 'What'



Account Access Report

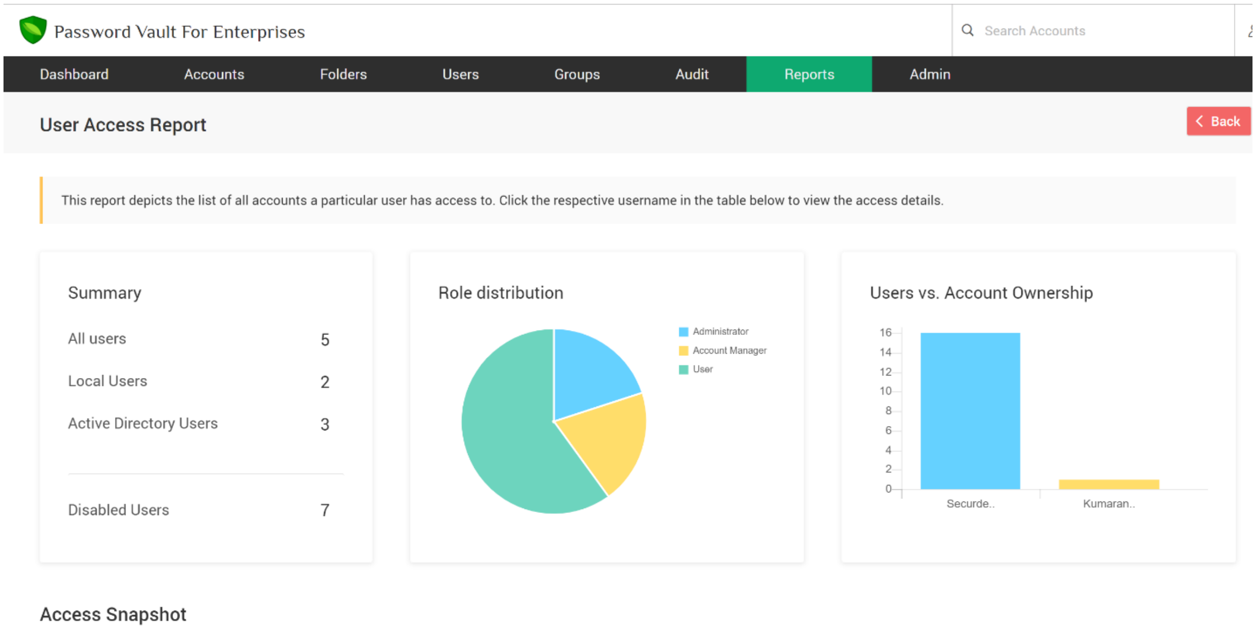
Access Snapshot

Account Title	Account Address	Account Type	Notes
Bitbucket Account	https://bitbucket.org/account/signin/	Web Account	
ClearTax	http://cleartax.in	Web Account	
Domain Admin	172.31.1.11	Windows Domain	
Facebook	https://www.facebook.com	Web Account	
G-Suite Admin Account	https://admin.google.com	Web Account	

Securden provides two types of reports for this purpose – Account Access Report and User Access Report.

Account Access Report depicts the list of all users who have access to a particular account.

User Access Report depicts the list of all accounts a particular user has access to.



User Access Report

This report depicts the list of all accounts a particular user has access to. Click the respective username in the table below to view the access details.

Summary

All users	5
Local Users	2
Active Directory Users	3
Disabled Users	7

Access Snapshot

Navigate to '**Reports**' tab to access these reports. '**Audit**' tab provides finer details of user and account activities.