Securden

Unified PAM

Quick Start Guide

Securden Privileged Account Manager

Quick Start Guide

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

Starting the PAM Server

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

Launching Web Interface

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

https://<PAM server hostname>:5959

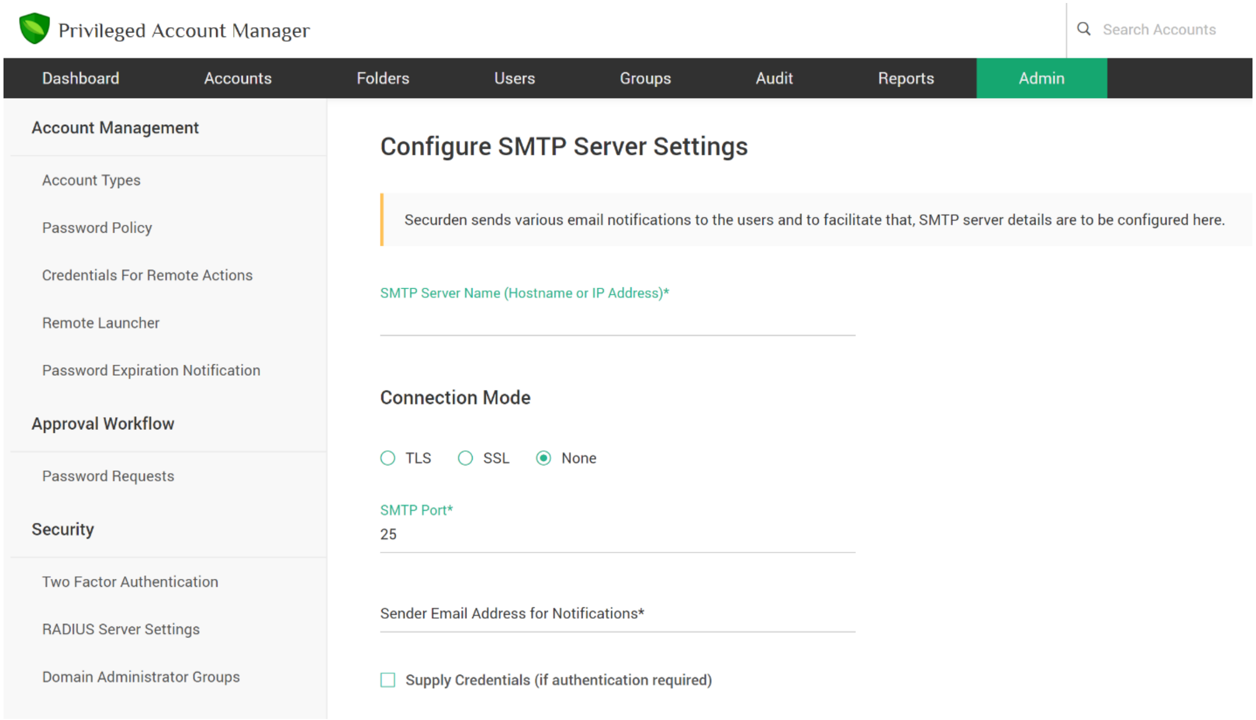
To access an unconfigured setup, the default login details are as below:

Username: admin
Password: admin

Section 1: 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*

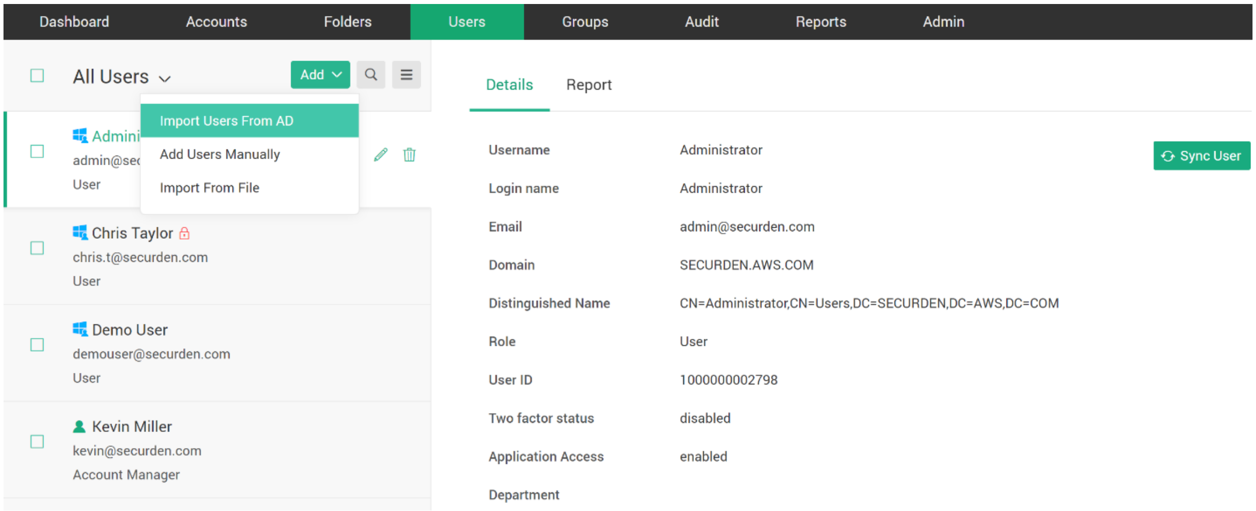
□ Supply Credentials (if authentication required)

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.



Admini
admin@sec
User

Chris Taylor
chris.t@securden.com
User

Demo User
demouser@securden.com
User

Kevin Miller
kevin@securden.com
Account Manager

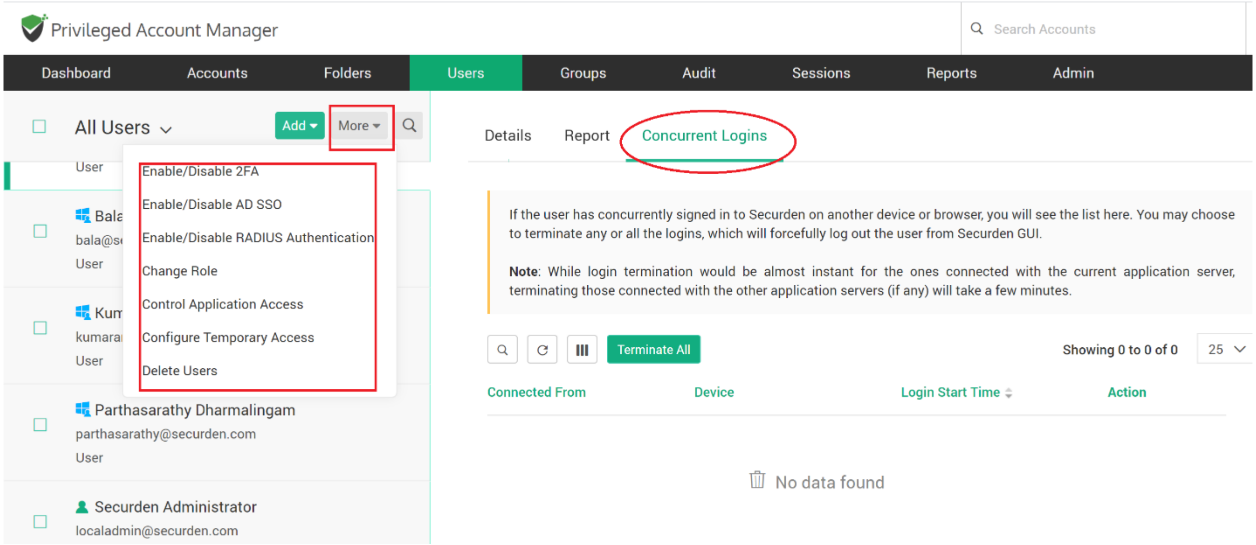
Username	Administrator
Login name	Administrator
Email	admin@securden.com
Domain	SECURDEN.AWS.COM
Distinguished Name	CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM
Role	User
User ID	1000000002798
Two factor status	disabled
Application Access	enabled
Department	

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.

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

Once you integrate Active Directory, you can leverage the Active Directory authentication and single signon. 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**’.



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

Connected From	Device	Login Start Time	Action

No data found

Add Users Manually

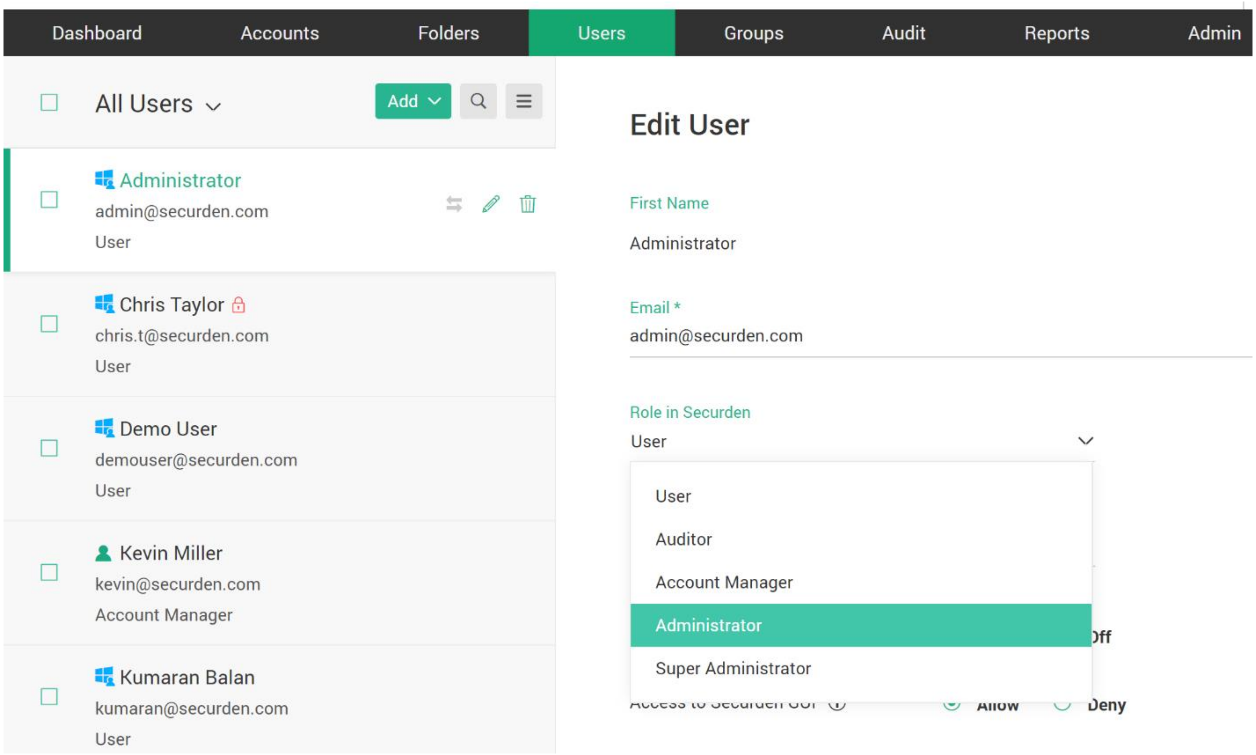
You can also create accounts for users in Securden manually. In this case, users will get login credentials to access the PAM. Navigate to **Users >> Add >> Add Users Manually** in the GUI to perform this step.

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

- User
- Auditor
- Account Manager
- Administrator
- Super Administrator

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.

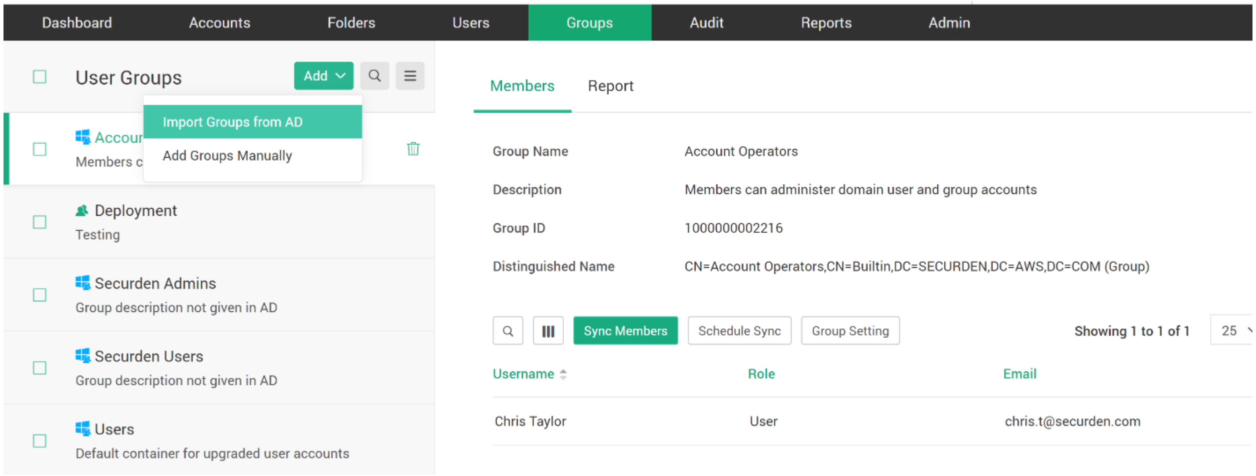
- **Account Manager** - Can add accounts to the application. Performs all administrative tasks related to the accounts.

- **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.



Accour
Members c

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)

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.

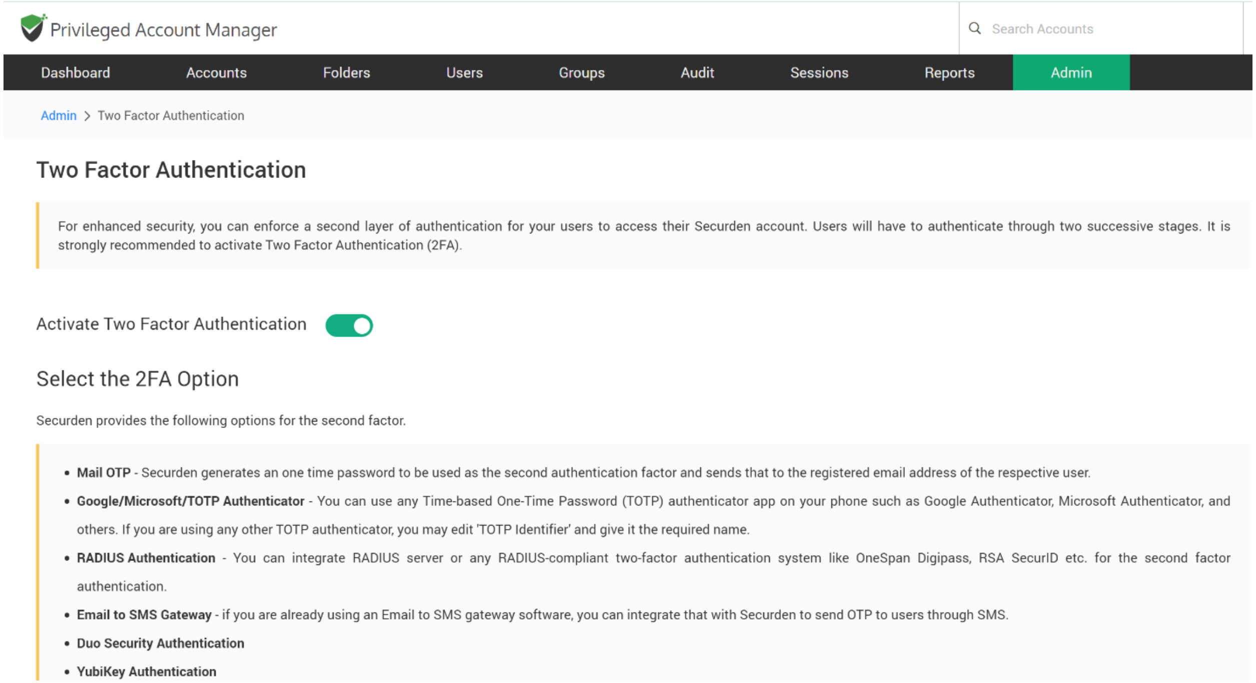
Navigate to **Groups >> Select the required group >> Members >> Schedule Sync** section in the GUI to perform this step.

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.

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.

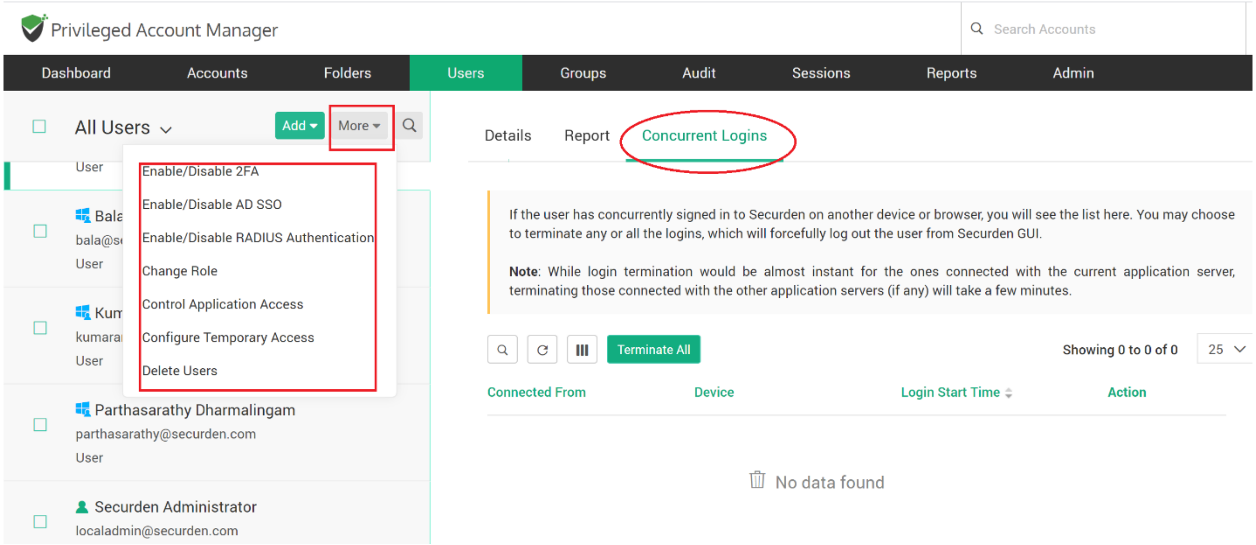
- **Mail OTP** - Securden generates an one time password to be used as the second authentication factor and sends that to the registered email address of the respective user.
- **Google/Microsoft/TOTP Authenticator** - You can use any Time-based One-Time Password (TOTP) authenticator app on your phone 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.

Section 2: Privileged Account Management

Account Ownership and Sharing: The Basic Design

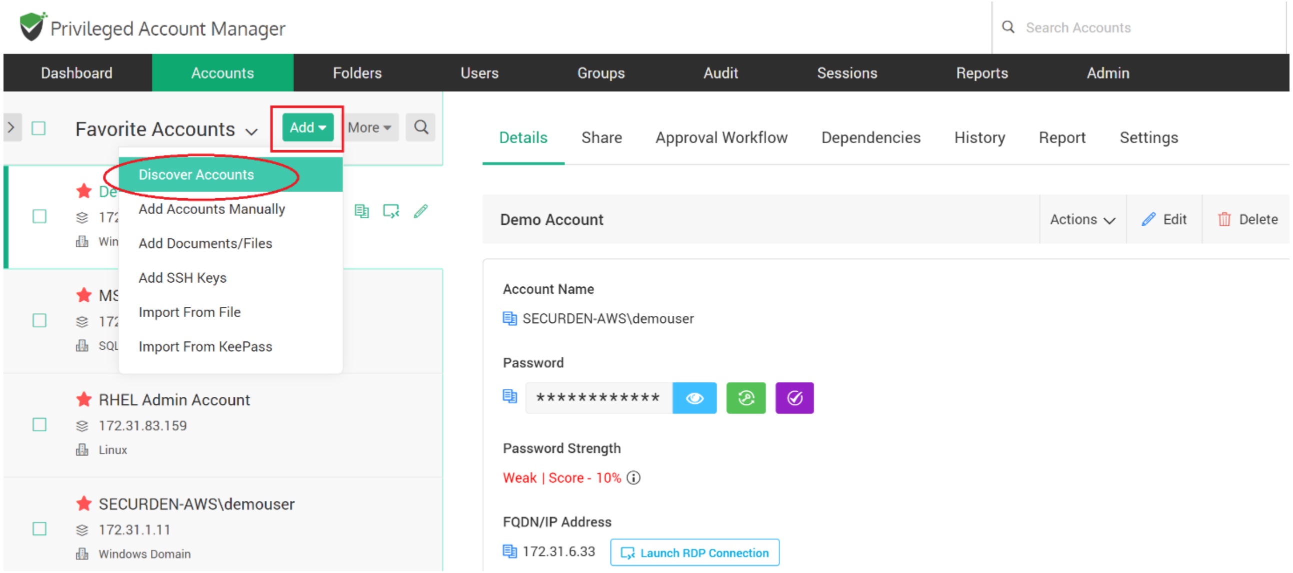
Any login information - username and password - stored in Securden is referred to as an account. One who adds an account becomes the owner of that particular account. The owner alone can see that account when logging in to Securden. If the owner wants others to view, the account has to be shared. When 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: Discover Accounts

The first step to get started with Securden is to discover the computers (Windows, Mac and Linux), databases and SSH devices in your network and the accounts that are part of those computers/devices.

1.1 Windows Accounts

In the case of Windows, Securden scans your Active Directory domain and obtains the OUs and computers in the domain. It also fetches the local admin accounts, domain accounts and service accounts on member servers. Typically, each discovered computer is scanned for identifying the dependencies - domain accounts which are used as service accounts to run services, scheduled tasks and IIS App pools. Navigate to **Accounts >> Add >> Discover** in the GUI to perform this step.



RHEL Admin Account
172.31.83.159
Linux

SECURDEN-AWS\demouser
172.31.1.11
Windows Domain

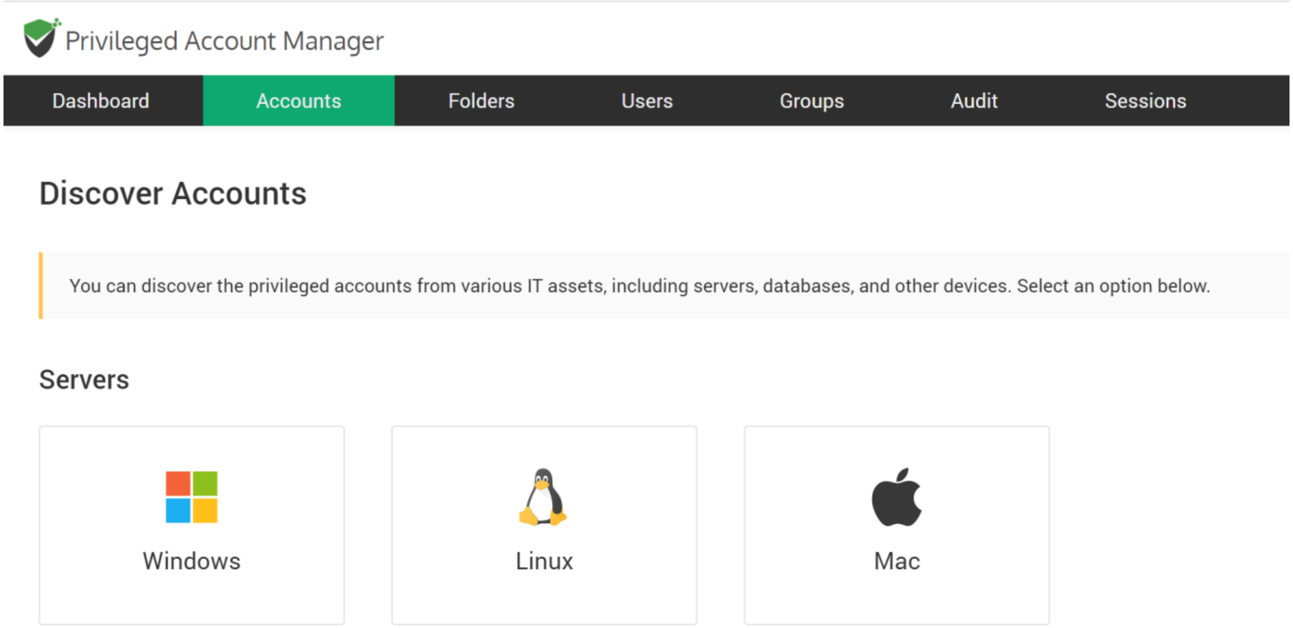
Demo Account

Account Name
SECURDEN-AWS\demouser

Password
****

Password Strength
Weak | Score - 10%

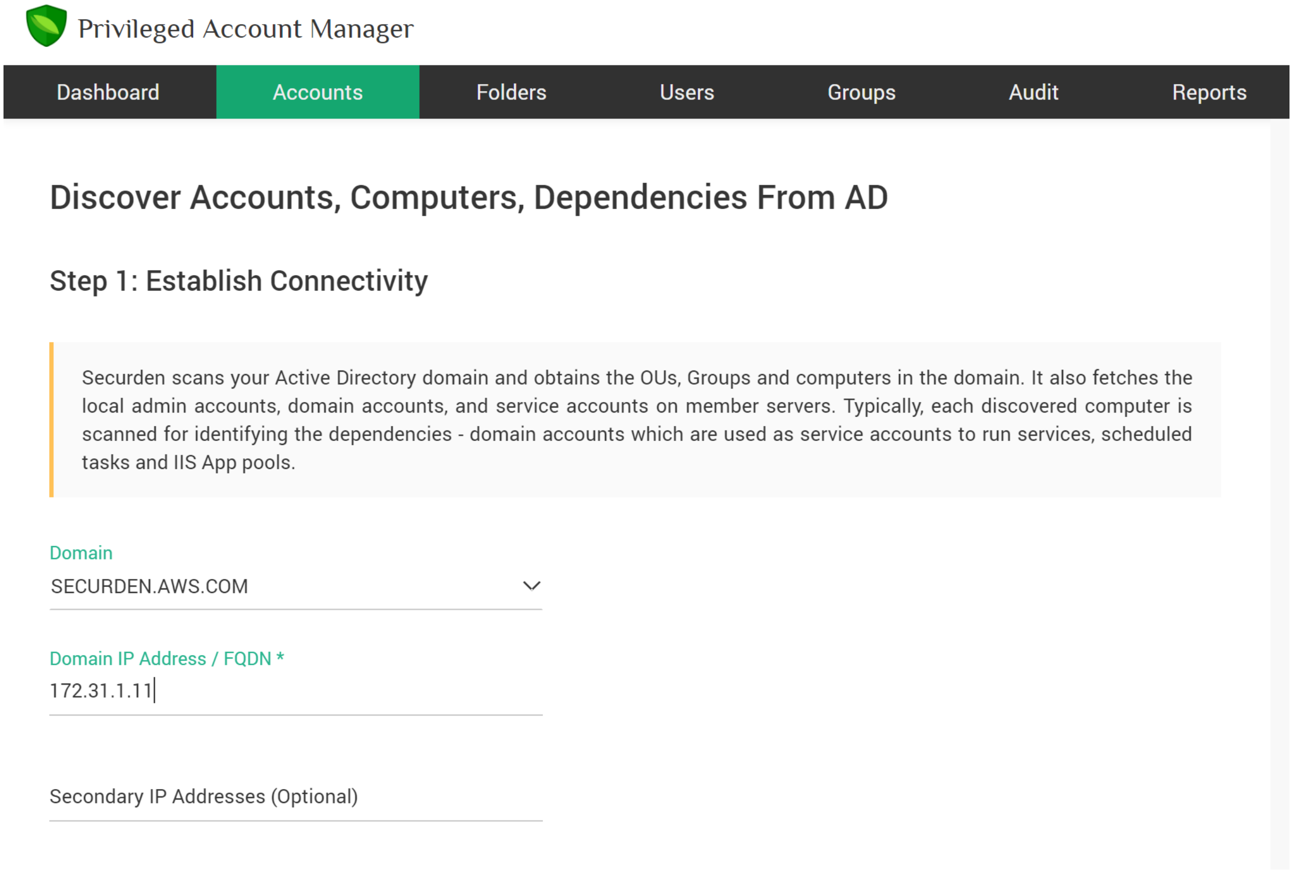
FQDN/IP Address
172.31.6.33



Discover Accounts

You can discover the privileged accounts from various IT assets, including servers, databases, and other devices. Select an option below.

Servers



Discover Accounts, Computers, Dependencies From AD

Step 1: Establish Connectivity

Securden scans your Active Directory domain and obtains the OUs, Groups and computers in the domain. It also fetches the local admin accounts, domain accounts, and service accounts on member servers. Typically, each discovered computer is scanned for identifying the dependencies - domain accounts which are used as service accounts to run services, scheduled tasks and IIS App pools.

Domain: SECURDEN.AWS.COM

Domain IP Address / FQDN *: 172.31.1.11

Secondary IP Addresses (Optional)

1.2 Configure Periodic Synchronization of Accounts, Endpoints and Servers

You can create a scheduled task to keep the accounts in Securden in synchronization with those in the AD. Accounts imported from specific OUs and Groups can be periodically synchronized. When accounts get added to or removed from the OUs/Groups in AD, the changes get reflected here.

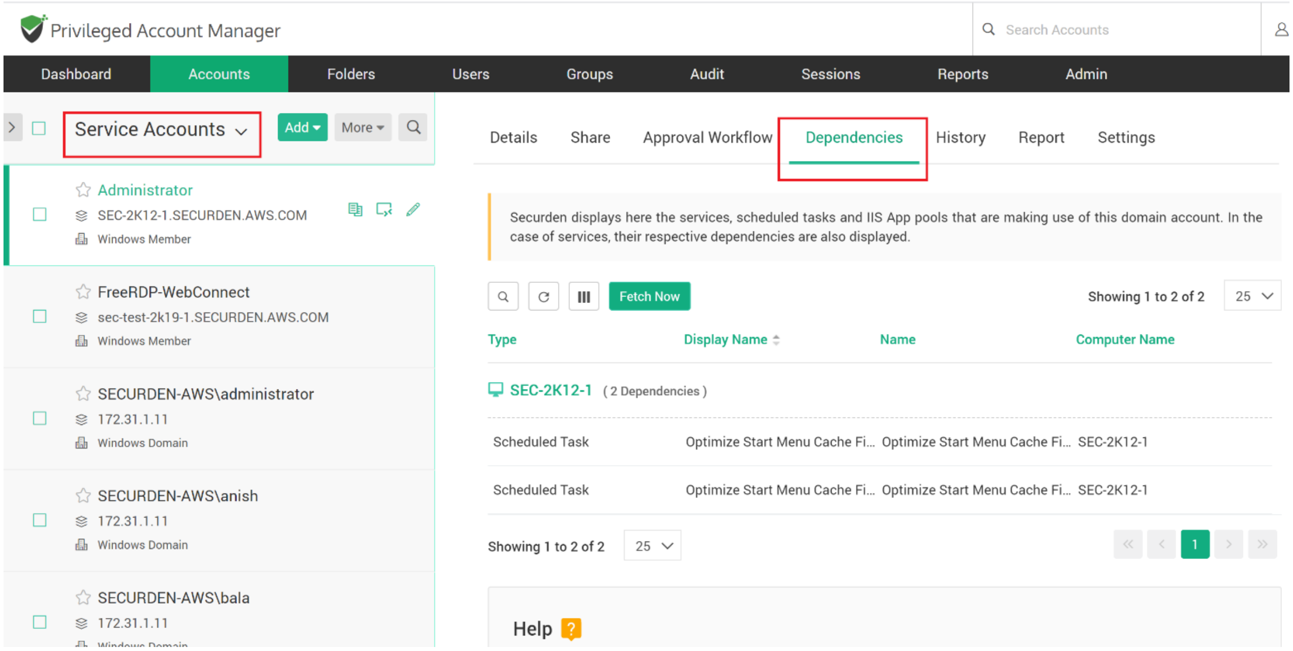
Navigate to **Accounts >> More Actions >> Configure AD Sync** section to perform this step. (The icon that displays three horizontal lines next to the 'Add' button in the 'Accounts' GUI represents 'More Actions'.

1.3 Manage Windows Service Accounts

During the Windows discovery process, Securden fetches and displays the services, scheduled tasks and IIS App pools that are making use of any particular domain account. In the case of services, their respective dependencies are also displayed.

You can manage service accounts in two ways:

1. Navigate to **Accounts >> Click 'Service Accounts'** in the "**All Accounts**" drop-down. It will list down all the accounts that have dependencies. When you click a particular account, and then click '**Dependencies**' tab in the right pane, you will see the list of all dependencies.
2. Alternatively, you can click any account on '**Accounts**' tab and then click '**Dependencies**' tab in the right pane, you will see the list of all dependencies.



Administrator
SEC-2K12-1.SECURDEN.AWS.COM
Windows Member

FreeRDP-WebConnect
sec-test-2k19-1.SECURDEN.AWS.COM
Windows Member

SECURDEN-AWS\administrator
172.31.1.11
Windows Domain

SECURDEN-AWS\anish
172.31.1.11
Windows Domain

SECURDEN-AWS\bala
172.31.1.11
Windows Domain

Securden displays here the services, scheduled tasks and IIS App pools that are making use of this domain account. In the case of services, their respective dependencies are also displayed.

Showing 1 to 2 of 2 25

Type	Display Name	Name	Computer Name
SEC-2K12-1 (2 Dependencies)			
Scheduled Task	Optimize Start Menu Cache Fi...	Optimize Start Menu Cache Fi...	SEC-2K12-1
Scheduled Task	Optimize Start Menu Cache Fi...	Optimize Start Menu Cache Fi...	SEC-2K12-1

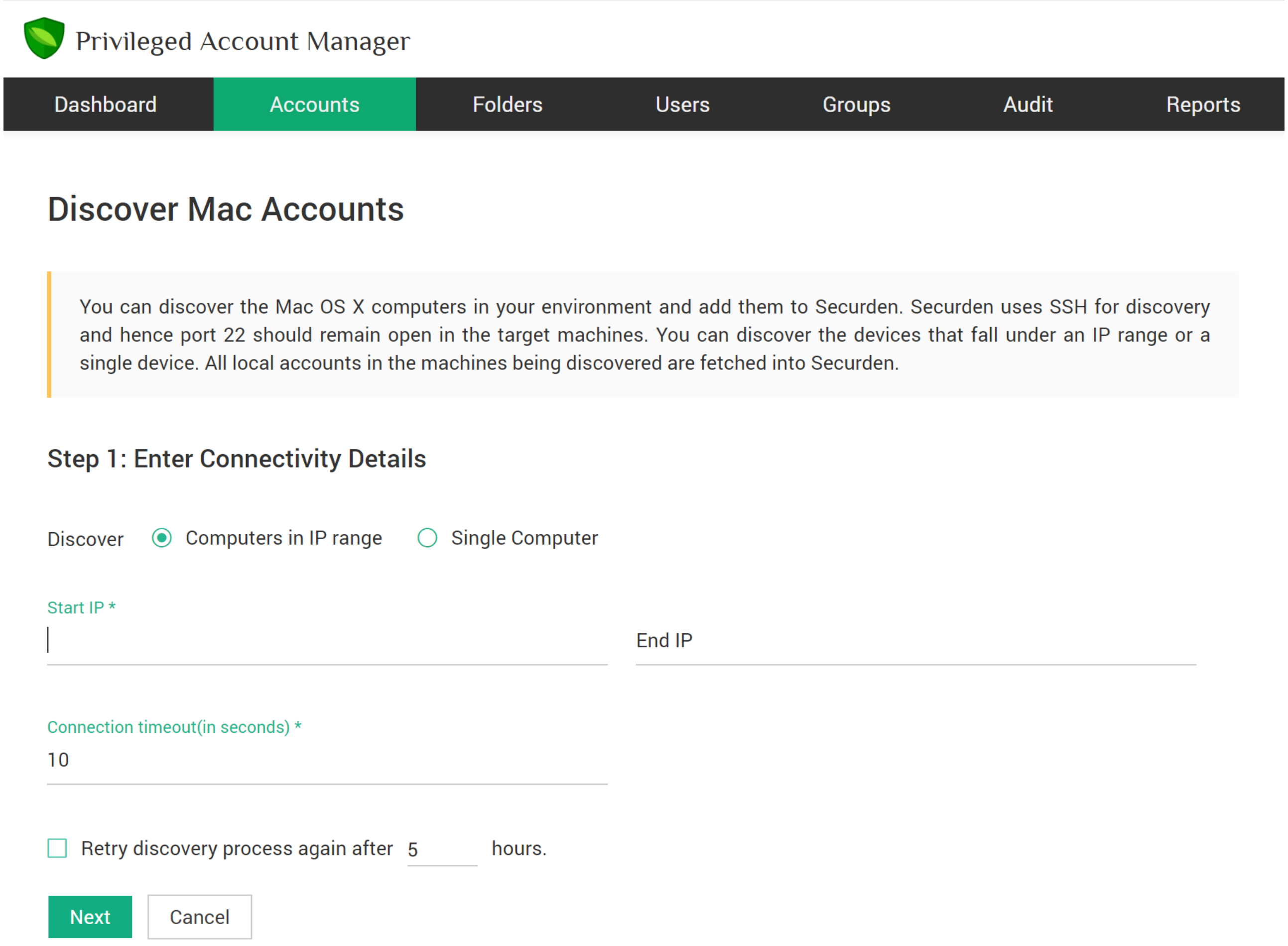
Showing 1 to 2 of 2 25

Whenever the password of a domain account is changed, Securden takes care of propagating the change across all dependencies. This way, you can always have complete visibility and control over service accounts and dependencies.

1.4 Discover Mac OS X Computers and Accounts

To discover the Mac OS X computers in your network and the accounts that are part of those computers, all you need to do is to specify the IP address range and supply either root account credentials or the common '**sudo**' account credential. Securden will use this to discover all local accounts in the specified range and also perform remote actions.

Navigate to **Accounts >> Add >> Discover** and then click **'Mac'** under **'Servers'** in the GUI to perform this step.



Discover Mac Accounts

You can discover the Mac OS X computers in your environment and add them to Securden. Securden uses SSH for discovery and hence port 22 should remain open in the target machines. You can discover the devices that fall under an IP range or a single device. All local accounts in the machines being discovered are fetched into Securden.

Step 1: Enter Connectivity Details

Discover ● Computers in IP range ○ Single Computer

Start IP *

End IP

Connection timeout(in seconds) * 10

□ Retry discovery process again after 5 hours.

1.5 Discover Linux Computers and Accounts

To discover the Linux computers in your network and the accounts that are part of those computers, all you need to do is to specify the IP address range and supply either root account credentials or the common '**sudo**' account credential. Securden will use this to discover all local accounts in the specified range and also perform remote actions.

Navigate to **Accounts >> Add >> Discover** and then click **'Linux'** under **'Servers'** in the GUI to perform this step.

1.6 Discover Databases

To discover PostgreSQL, MySQL, MS SQL and Oracle databases and the privileged accounts thereof, navigate to **Accounts >> Add >> Discover** and then click the required database under **'Databases'** in the GUI. You need to provide basic details such as database port, connector details and the administrator credentials.

1.7 Discover Devices

You can discover SSH devices such as switches, routers and firewalls along with the privileged accounts thereof. Navigate to **Accounts >> Add >> Discover** and then click the required device type under **'Devices'** in the GUI.

1.8 Import Accounts

Alternatively, you can import accounts from a standard CSV or XLSX file. Navigate to **Accounts >> Add >> Import from File** to perform this.

Format

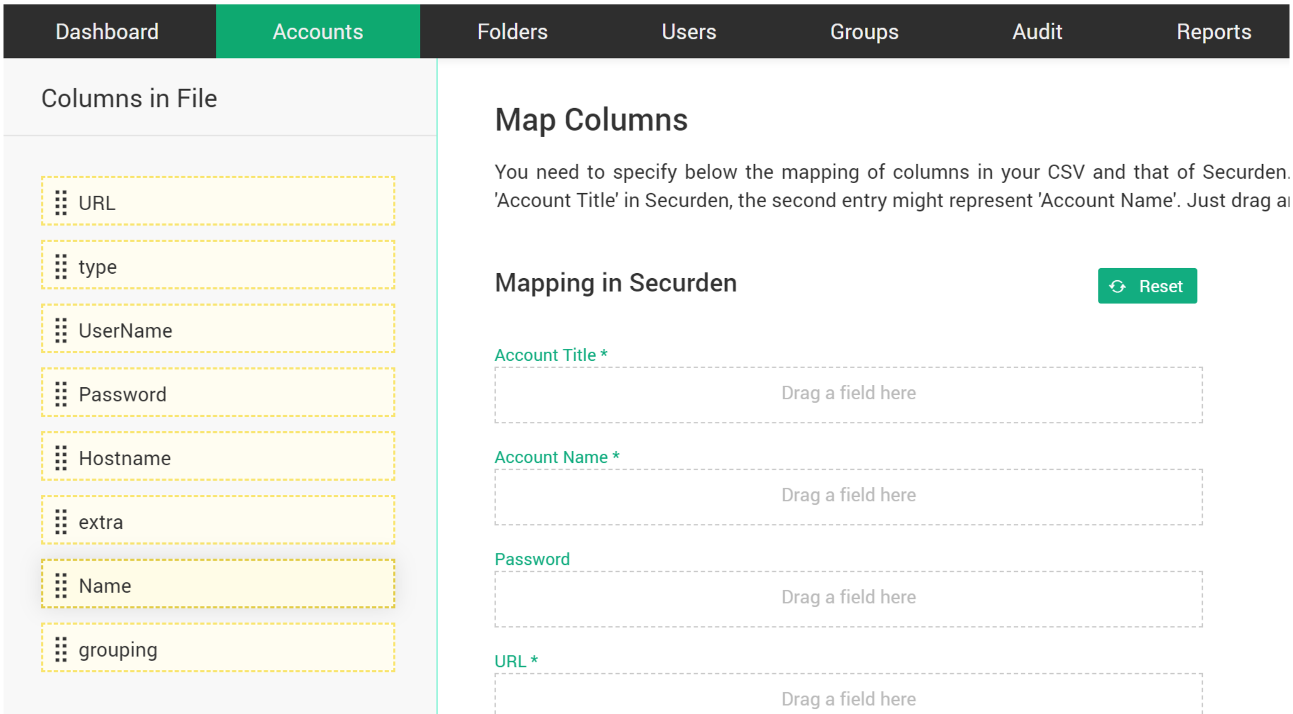
Accounts import is very flexible in Securden. You can simply import the file you have exported from your current repository into Securden. Typically, each line in the file is added as an account. In the second step of accounts import, you can **map the columns** in the input file and that of Securden. 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.



Map Columns

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

Mapping in Securden

Account Title *

Account Name *

Password

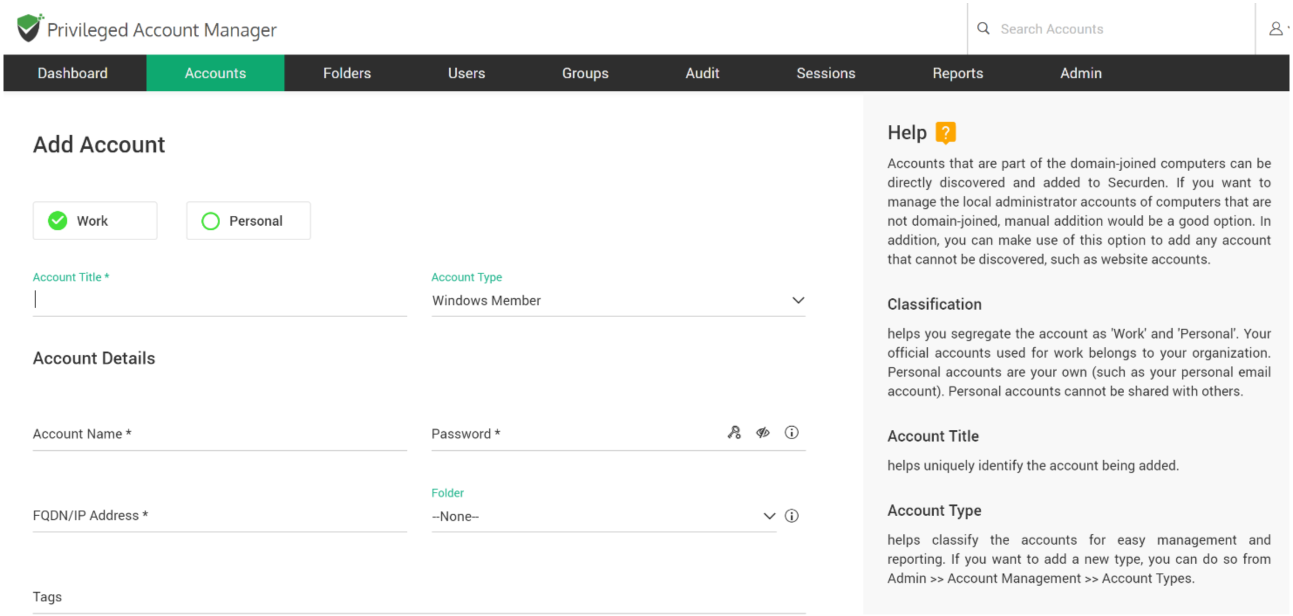
URL *

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.

1.9 Add Accounts Manually

You can add accounts manually too. You can make use of this provision to add website accounts and others that are not discoverable. Navigate to **Accounts >> Add >> Add Accounts Manually** in the GUI to perform this step.



Add Account

● Work ○ Personal

Account Title *

Account Type: Windows Member

Account Details

Account Name *

Password *

FQDN/IP Address *

Folder: --None--

Tags

Help ?

Accounts that are part of the domain-joined computers can be directly discovered and added to Securden. If you want to manage the local administrator accounts of computers that are not domain-joined, manual addition would be a good option. In addition, you can make use of this option to add any account that cannot be discovered, such as website accounts.

Classification

helps you segregate the account as 'Work' and 'Personal'. Your official accounts used for work belongs to your organization. Personal accounts are your own (such as your personal email account). Personal accounts cannot be shared with others.

Account Title

helps uniquely identify the account being added.

Account Type

helps classify the accounts for easy management and reporting. If you want to add a new type, you can do so from Admin >> Account Management >> Account Types.

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

1.10 Explore 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.

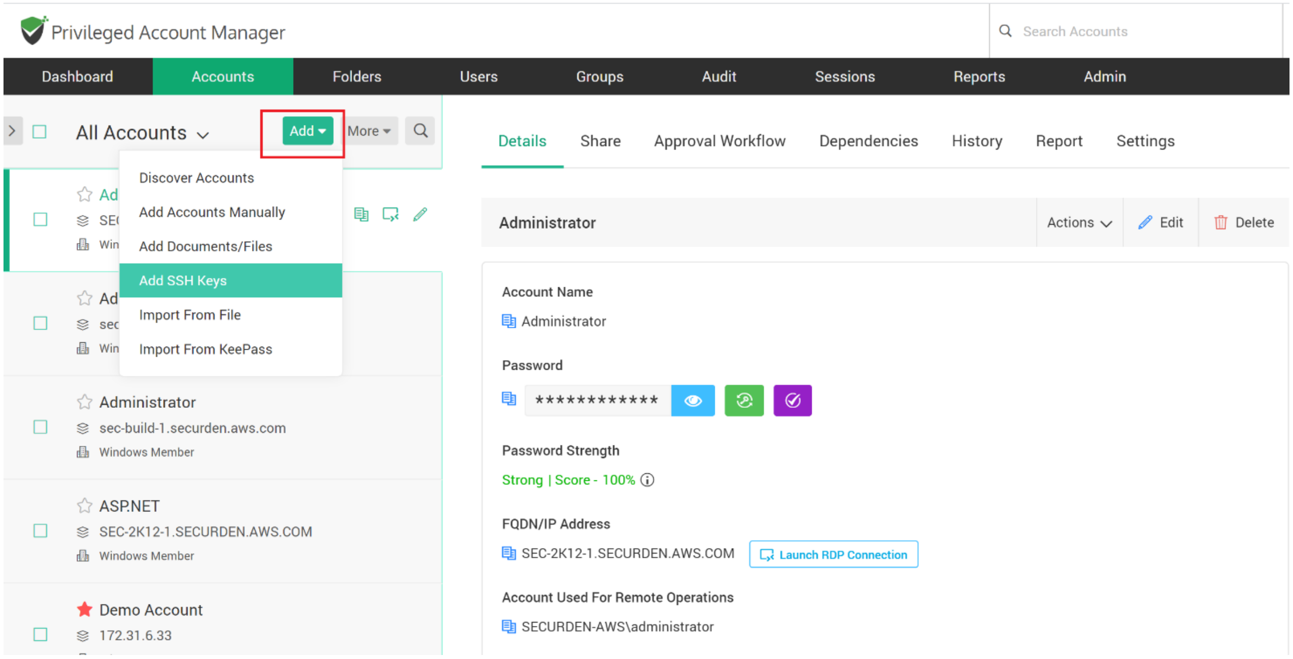
When creating your own account types, you can define the fields needed for that type, decide if certain fields should be marked as 'mandatory', if any field to hold default values and so on.

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

1.11 Add and Manage 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
Administrator

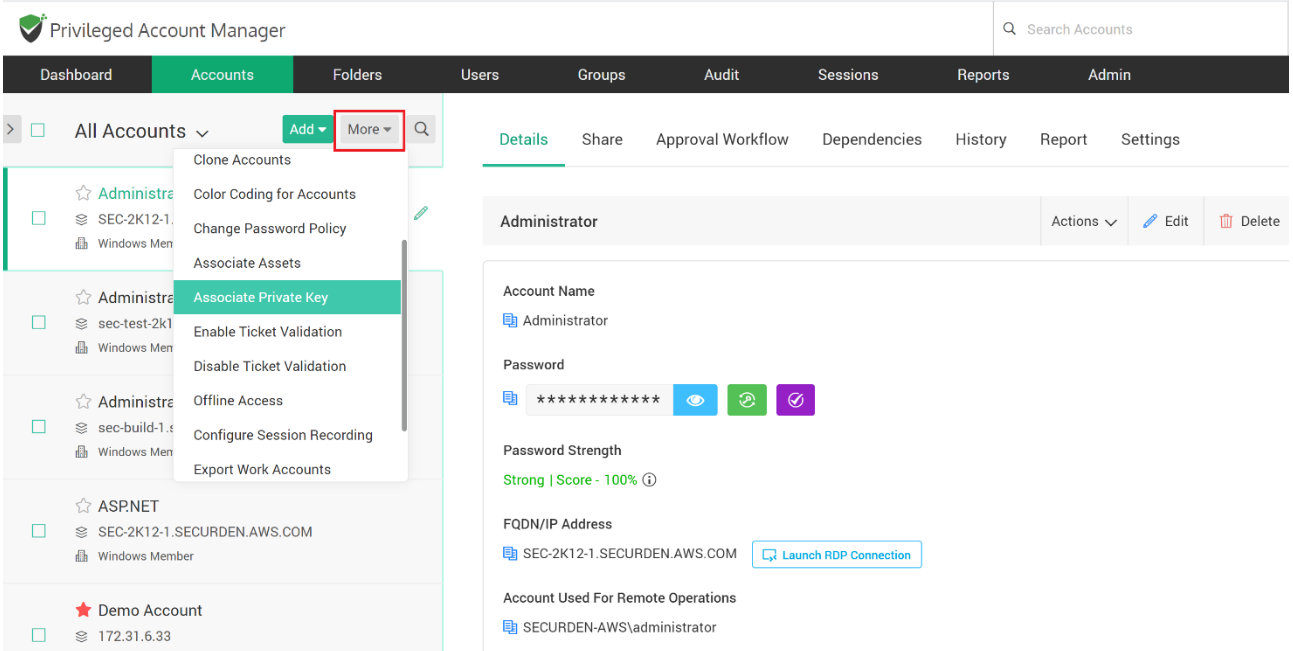
Password
****

Password Strength
Strong | Score - 100%

FQDN/IP Address
SEC-2K12-1.SECURDEN.AWS.COM

Account Used For Remote Operations
SECURDEN-AWS\administrator

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.



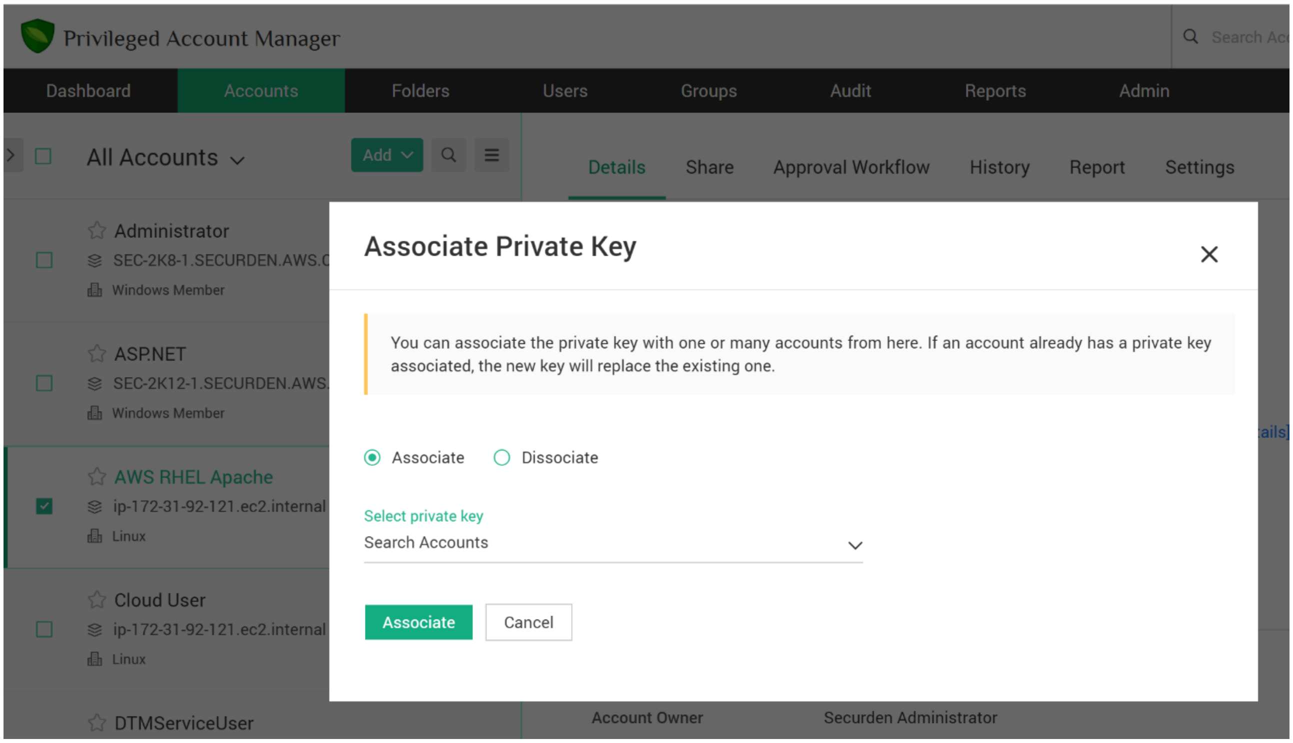
Account Name
Administrator

Password
****

Password Strength
Strong | Score - 100%

FQDN/IP Address
SEC-2K12-1.SECURDEN.AWS.COM

Account Used For Remote Operations
SECURDEN-AWS\administrator



Associate Private Key

You can associate the private key with one or many accounts from here. If an account already has a private key associated, the new key will replace the existing one.

● Associate ○ Dissociate

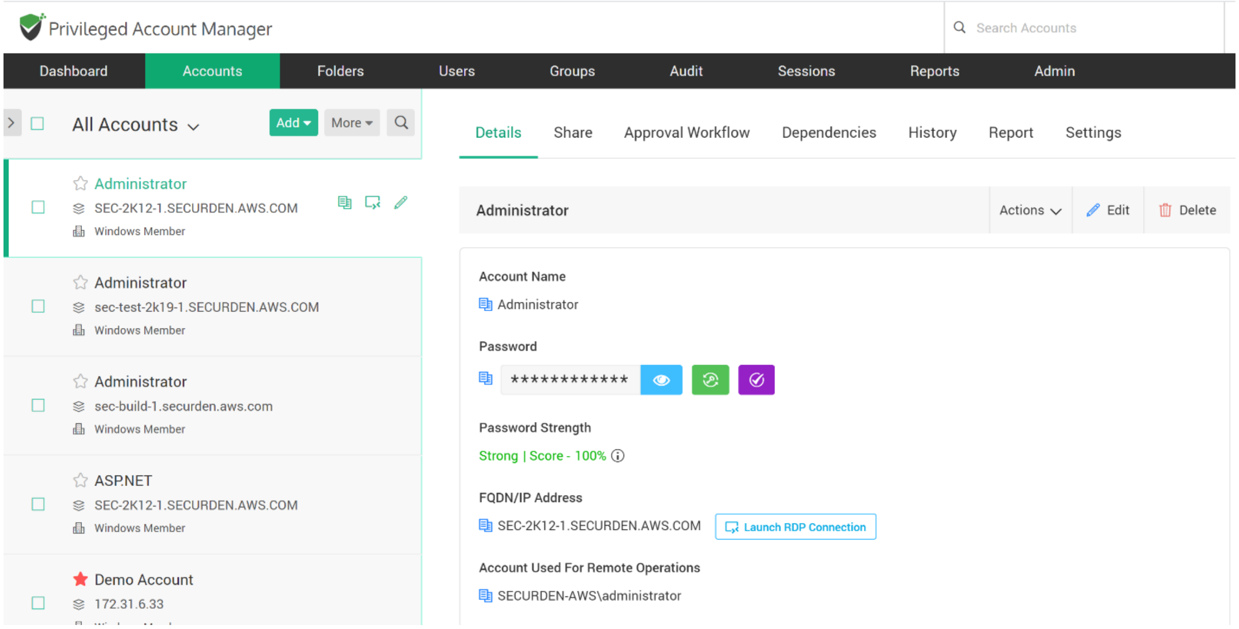
Select private key
Search Accounts

1.11 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.



Administrator
SEC-2K12-1.SECURDEN.AWS.COM
Windows Member

Administrator
sec-test-2k19-1.SECURDEN.AWS.COM
Windows Member

Administrator
sec-build-1.securden.aws.com
Windows Member

ASP.NET
SEC-2K12-1.SECURDEN.AWS.COM
Windows Member

Demo Account
172.31.6.33

Administrator

Account Name
Administrator

Password
****

Password Strength
Strong | Score - 100%

FQDN/IP Address
SEC-2K12-1.SECURDEN.AWS.COM

Account Used For Remote Operations
SECURDEN-AWS\administrator

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.

Step 3: RDP, SSH, SQL, Website Connections

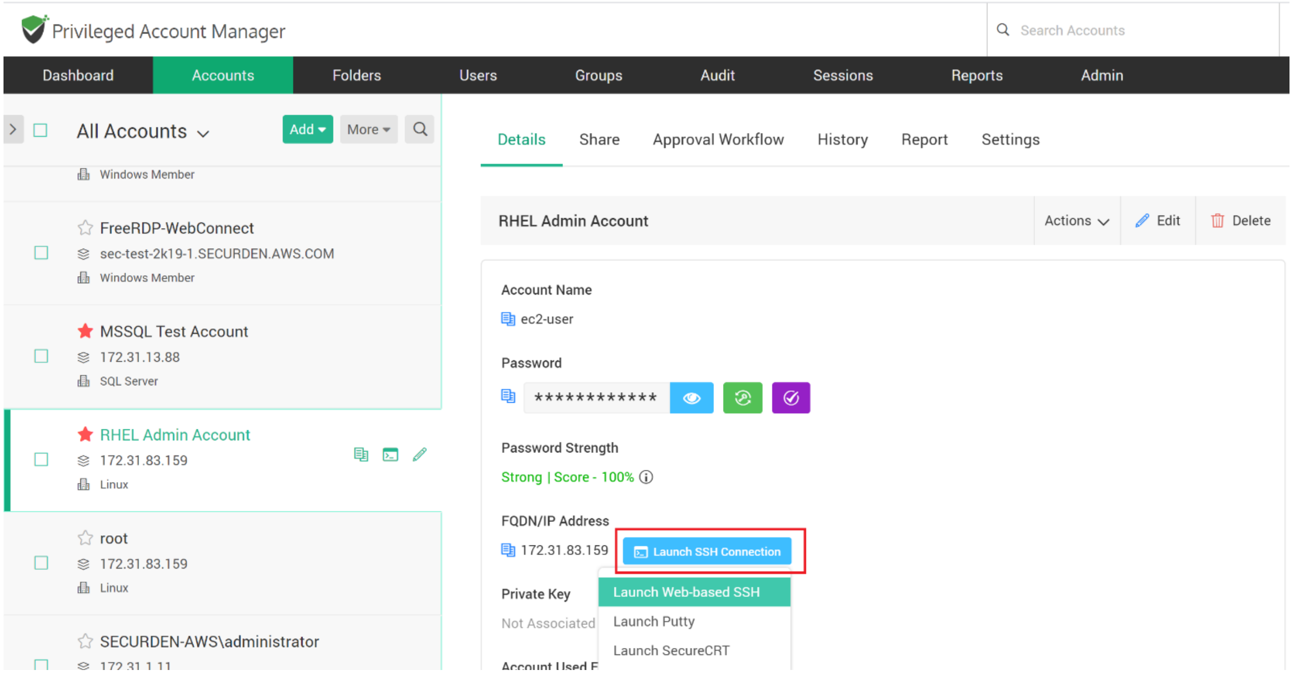
(Remote Connections for Employees, 3rd-party Contractors)

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.



Windows Member

FreeRDP-WebConnect
sec-test-2k19-1.SECURDEN.AWS.COM
Windows Member

MSSQL Test Account
172.31.13.88
SQL Server

RHEL Admin Account
172.31.83.159
Linux

root
172.31.83.159
Linux

SECURDEN-AWS\administrator
172.31.1.11

RHEL Admin Account

Account Name
ec2-user

Password
****

Password Strength
Strong | Score - 100%

FQDN/IP Address
172.31.83.159

Private Key
Not Associated

Account Used F

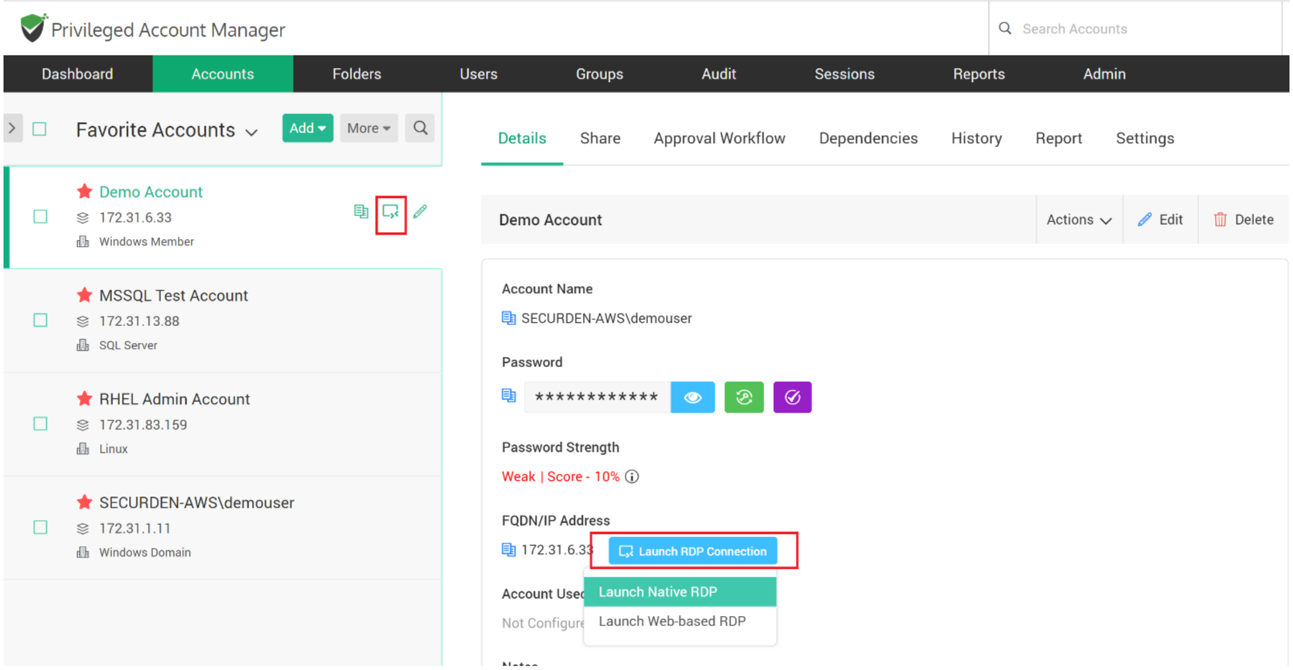
To launch web-based RDP, SSH connections, select the required account and click “**Launch RDP Connection**” or “**Launch SSH Connection**” and then choose the web-based option.

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.



Demo Account
172.31.6.33
Windows Member

MSSQL Test Account
172.31.13.88
SQL Server

RHEL Admin Account
172.31.83.159
Linux

SECURDEN-AWS\demouser
172.31.1.11
Windows Domain

Demo Account

Account Name
SECURDEN-AWS\demouser

Password
****

Password Strength
Weak | Score - 10%

FQDN/IP Address
172.31.6.33

Account Used
Not Configure

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).

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.

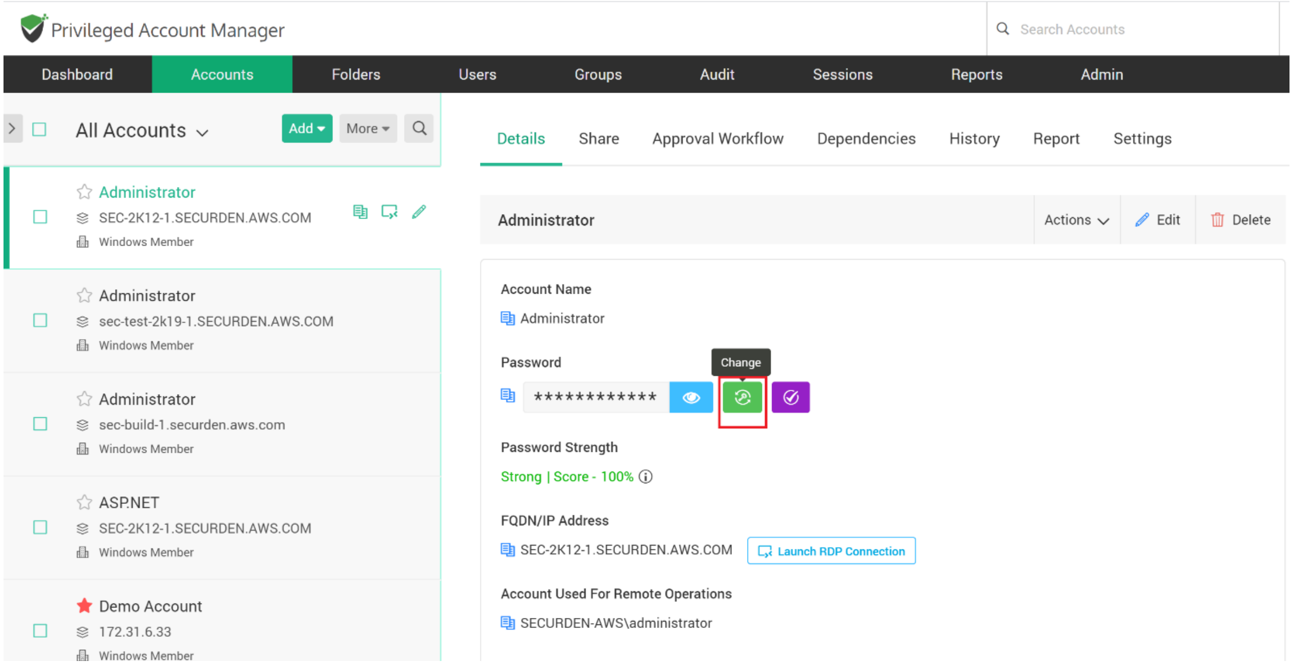
3.3 Auto-fill Credentials on Websites

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: Reset Passwords, Verify Synchronization

You can reset passwords of accounts on remote devices from the **Accounts >> Details** section in the GUI. While resetting the passwords, you can take the help of Securden's password generator, which helps generate strong passwords. Whenever you want to verify if the password stored in Securden is in synchronization with the remote machine, you can do that too.



Administrator
SEC-2K12-1.SECURDEN.AWS.COM
Windows Member

Administrator
sec-test-2k19-1.SECURDEN.AWS.COM
Windows Member

Administrator
sec-build-1.securden.aws.com
Windows Member

ASP.NET
SEC-2K12-1.SECURDEN.AWS.COM
Windows Member

Demo Account
172.31.6.33
Windows Member

Administrator

Account Name
Administrator

Password
****

Password Strength
Strong | Score - 100%

FQDN/IP Address
SEC-2K12-1.SECURDEN.AWS.COM

Account Used For Remote Operations
SECURDEN-AWS\administrator

To reset the password,

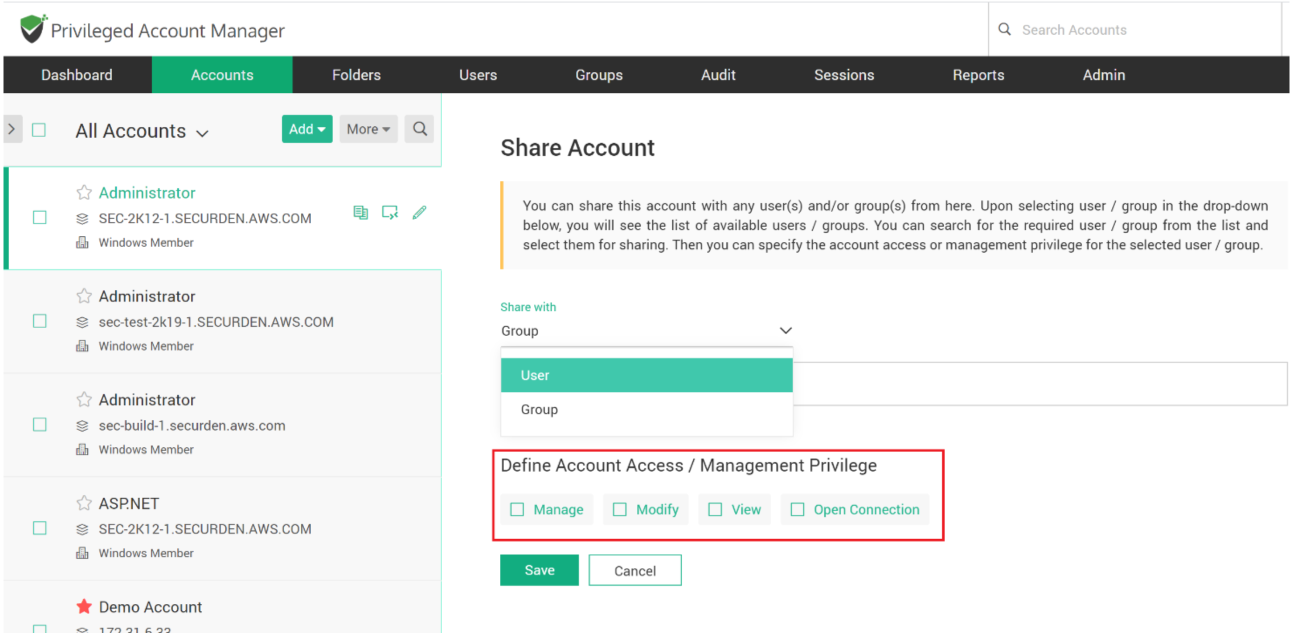
- Navigate to **Accounts** section in the GUI, **click the required account,** click the '**Change**' button in the right pane next to the account password and then follow the instructions in the GUI.

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.

Step 5: 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: Group

Define Account Access / Management Privilege

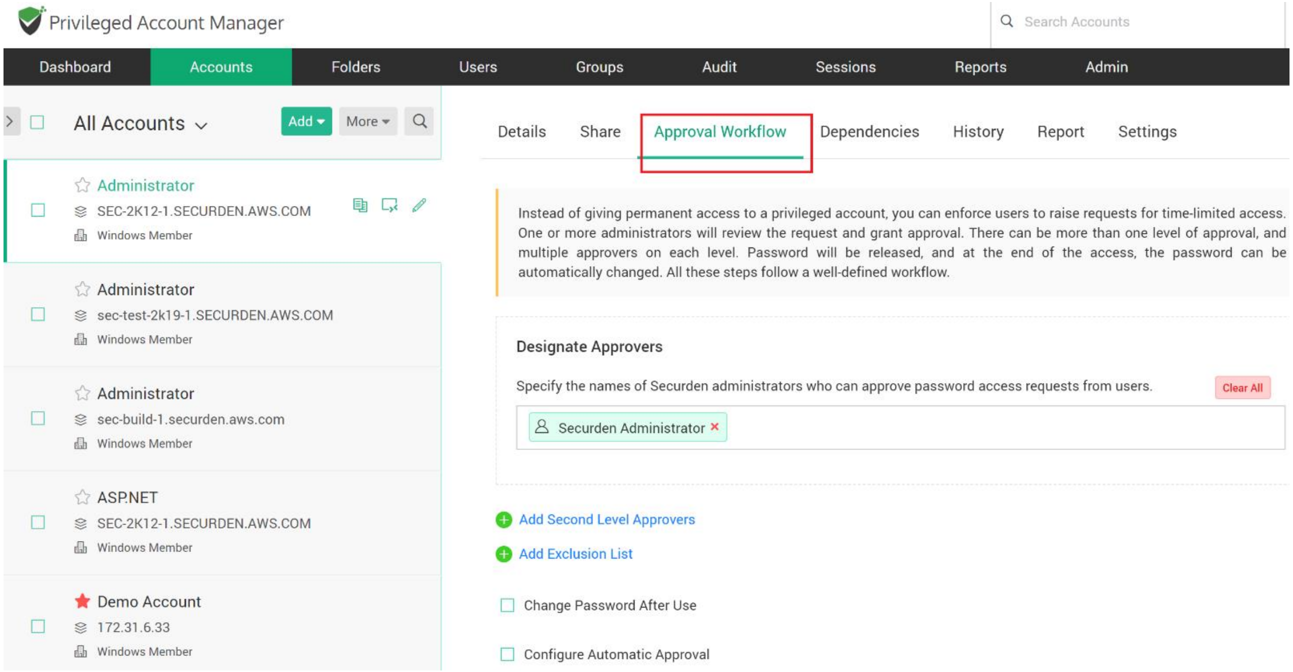
□ Manage □ Modify □ View □ Open Connection

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 changing the password alone
- '**Manage**' grants all privileges and is similar to concurrent ownership.

Step 6: Just-in-time Access through Approval Workflows

You can establish an additional layer of security for sensitive accounts by enforcing your users to go through approval workflows. This also serves as just-in-time access provisioning mechanism. Whenever the passwords of such accounts are to be accessed, users will have to raise a request and select administrators or account managers, who are designated as 'Approvers' will grant time-limited access. At the end of the usage period, the password will be automatically reset. This feature comes with adequate provisions to handle various scenarios such as obtaining permission in advance, granting automated approvals.



Instead of giving permanent access to a privileged account, you can enforce users to raise requests for time-limited access. One or more administrators will review the request and grant approval. There can be more than one level of approval, and multiple approvers on each level. Password will be released, and at the end of the access, the password can be automatically changed. All these steps follow a well-defined workflow.

Designate Approvers

Specify the names of Securden administrators who can approve password access requests from users.

□ Change Password After Use

□ Configure Automatic Approval

To configure approval workflow,

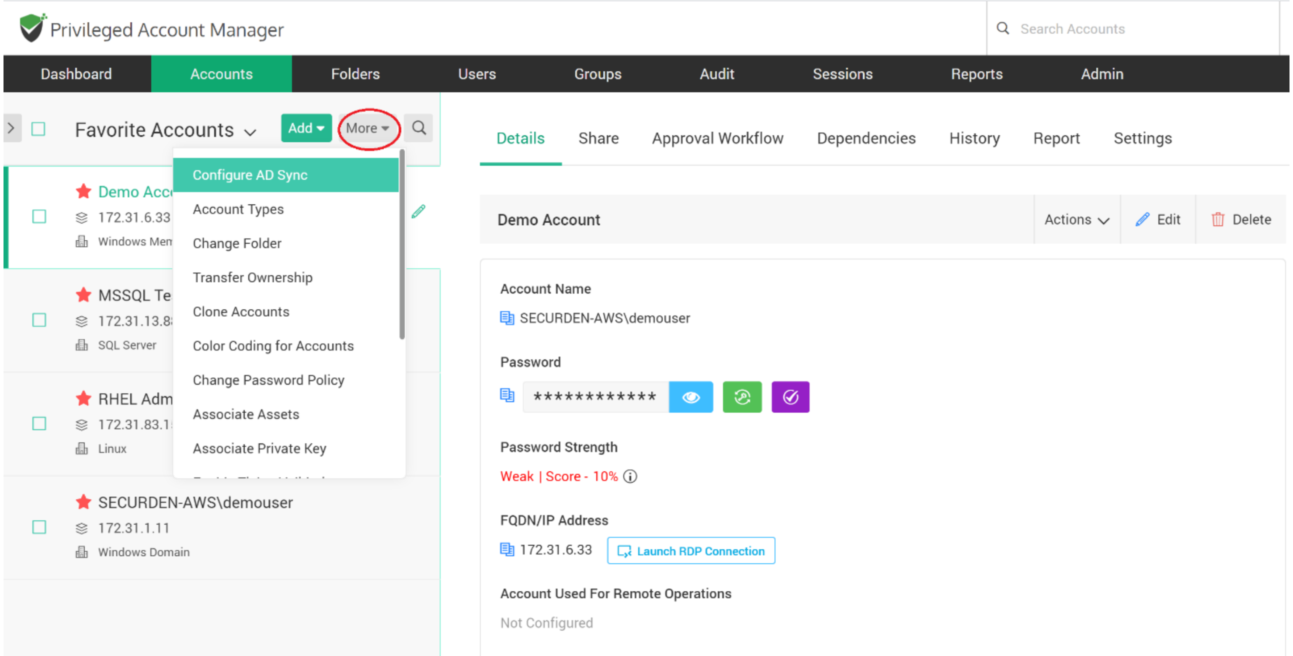
- Navigate to **Accounts** section in the GUI, **click the required account,** click the '**Approval Workflow**' tab in the right pane and then follow the instructions in the GUI.

To approve/reject the requests raised by users,

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

Step 7: Explore Features Under 'More Actions'

The '**More Actions**' section 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.



Demo Acc
172.31.6.33
Windows Mem

MSSQL Te
172.31.13.8
SQL Server

RHEL Adm
172.31.83.1
Linux

SECURDEN-AWS\demouser
172.31.1.11
Windows Domain

Demo Account

Account Name
SECURDEN-AWS\demouser

Password
****

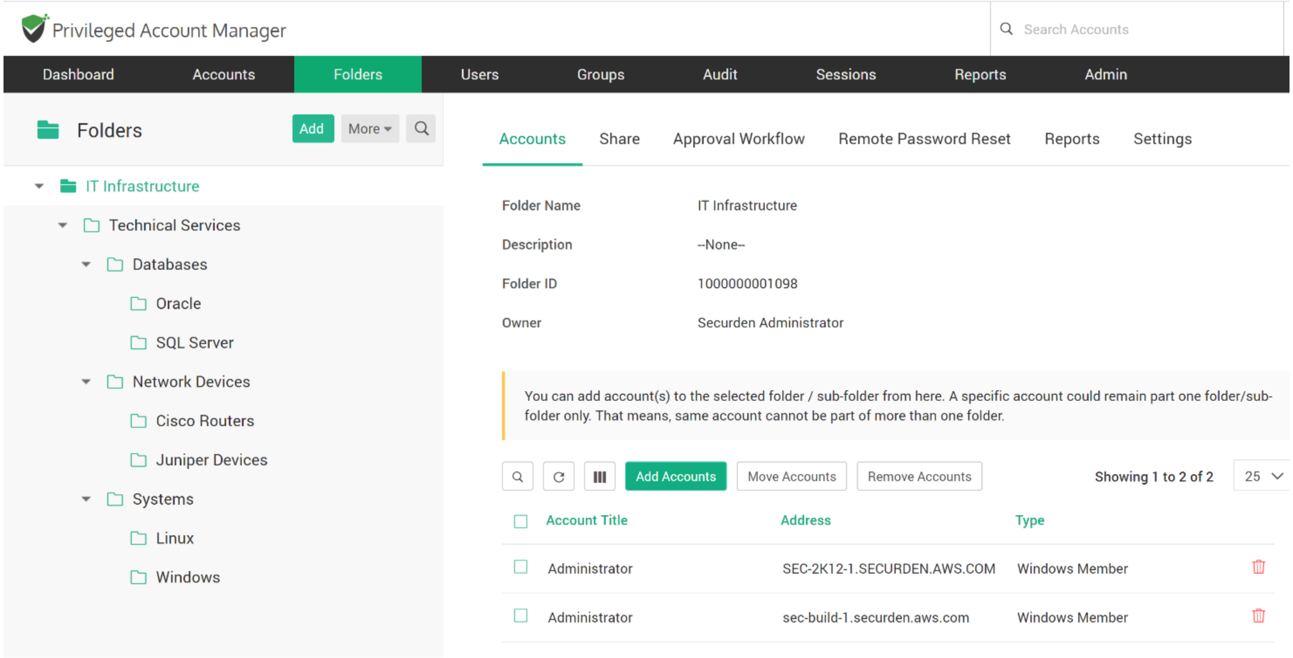
Password Strength
Weak | Score - 10%

FQDN/IP Address
172.31.6.33

Account Used For Remote Operations
Not Configured

Step 8: 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 1000000001098

Owner Securden Administrator

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

Showing 1 to 2 of 2

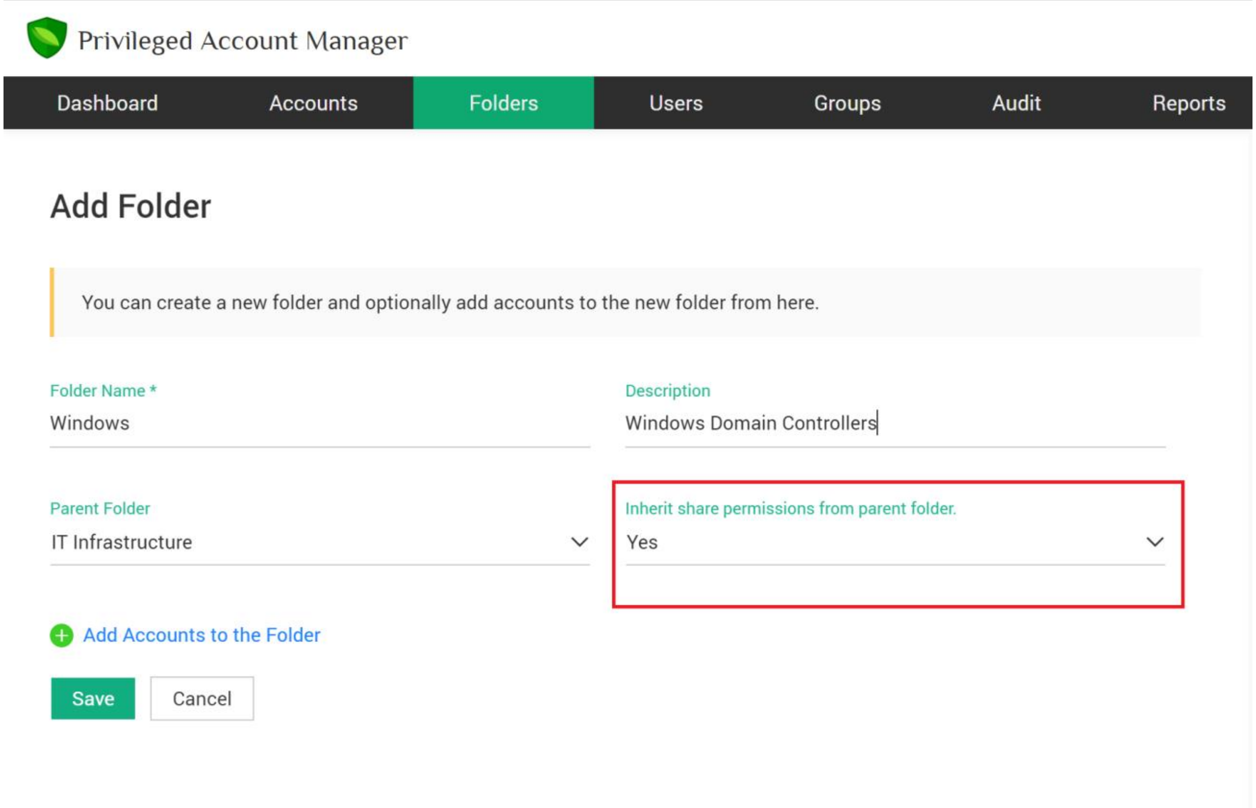
Account Title	Address	Type
Administrator	SEC-2K12-1.SECURDEN.AWS.COM	Windows Member
Administrator	sec-build-1.securden.aws.com	Windows Member

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 9: 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



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

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

In the screenshot above, the new folder ‘Windows’, which is created as a sub-folder of IT Infrastructure will inherit permissions from its parent. As a result, when you share the folder IT Infrastructure, the sub-folder also gets shared. For the already created sub-folders, you can edit the folders and change the inheritance option as "Yes".

Step 10: Configure Approval Workflow for Folders

In step 6 above, we dealt with configuring request-release approval workflow for individual accounts. The same can be done for all the account belonging to a folder too.

To enforce workflow for an entire folder,

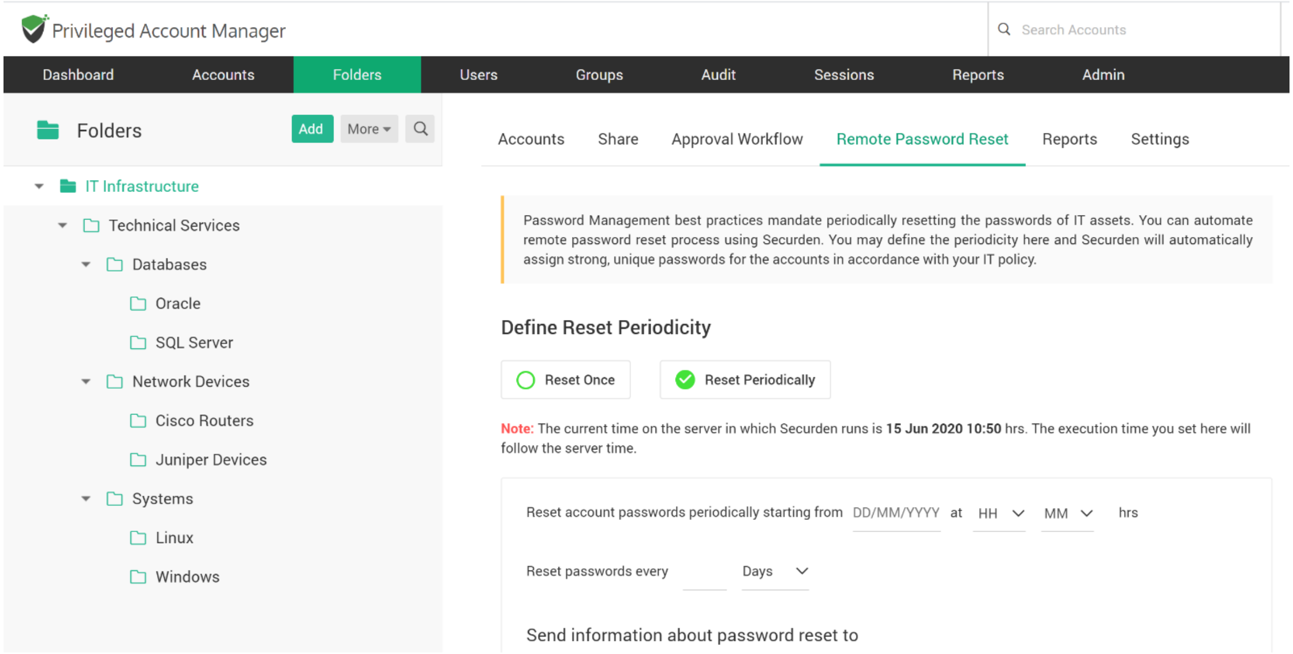
- navigate to **Folders** section in the GUI, **click the required folder,** click the ‘**Approval Workflow**’ tab in the right pane and then follow the instructions in the GUI.

Step 11: Configure Automated, Periodic Remote Password Reset

You can periodically reset the passwords of accounts in a fully automated manner. You can create scheduled tasks for periodic password reset for all accounts belonging to a folder. Securden then takes care of assigning strong, unique passwords to each account at periodic intervals. The remote password reset could be configured only at the folder level.

To configure periodic password reset to the accounts belonging to a folder,

- Navigate to **Folders** section in the GUI, **click the required folder,** click the ‘**Remote Password Reset**’ tab in the right pane and then follow the instructions in the GUI.



Password Management best practices mandate periodically resetting the passwords of IT assets. You can automate remote password reset process using Securden. You may define the periodicity here and Securden will automatically assign strong, unique passwords for the accounts in accordance with your IT policy.

Define Reset Periodicity

○ Reset Once ● Reset Periodically

Note: The current time on the server in which Securden runs is **15 Jun 2020 10:50** hrs. The execution time you set here will follow the server time.

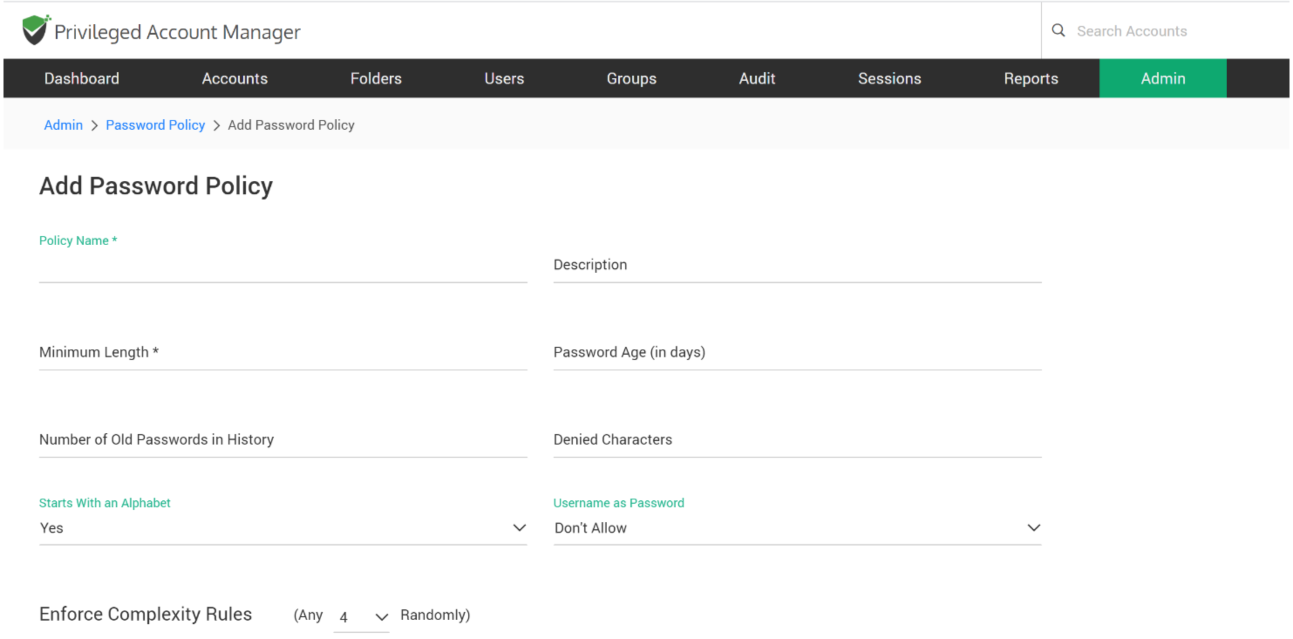
Reset account passwords periodically starting from DD/MM/YYYY at HH MM hrs

Reset passwords every Days

Send information about password reset to

Step 12: Create and Enforce Password Policy

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.



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)

Wherever automation is possible, Securden password generator will automatically assign unique 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.

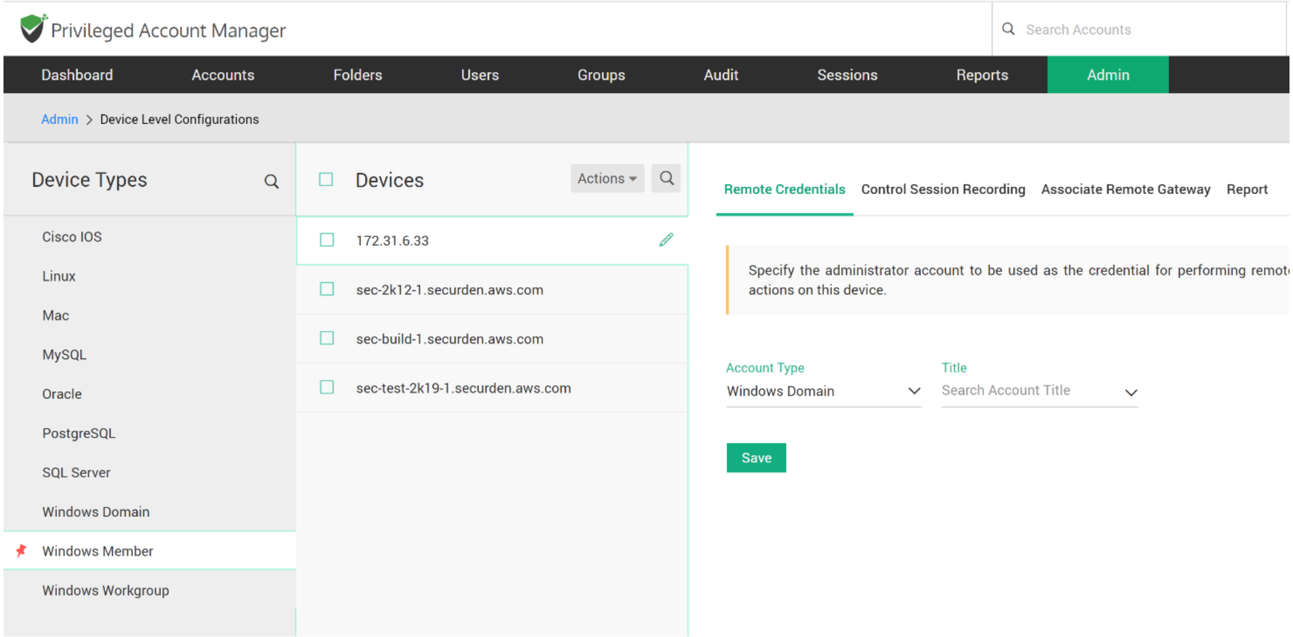
When you do so, Securden will allow only the accounts that conform to the policy defined. You can make use of the password generator to generate strong passwords, apply them to the respective websites first and then update the Securden Vault.

Step 13: Specify Credentials for Performing Remote Actions

(If you have supplied domain administrator credentials for accounts discovery (Step 1), you may ignore this step).

You need to supply the credentials that are to be used by Securden for performing various remote actions such as fetching accounts, dependencies, and carrying out password resets. You have the option to specify the domain administrator credentials that will take effect globally for all accounts. You can also overwrite the global configuration for specific computers through the 'Specific Computer' option. Navigate to **Admin >> Account Management >> Device Level**

Configurations. Select the required device type, then the specific device and then click **'Remote Credentials'** tab in the GUI to perform this step.



Specify the administrator account to be used as the credential for performing remot actions on this device.

Account Type: Windows Domain

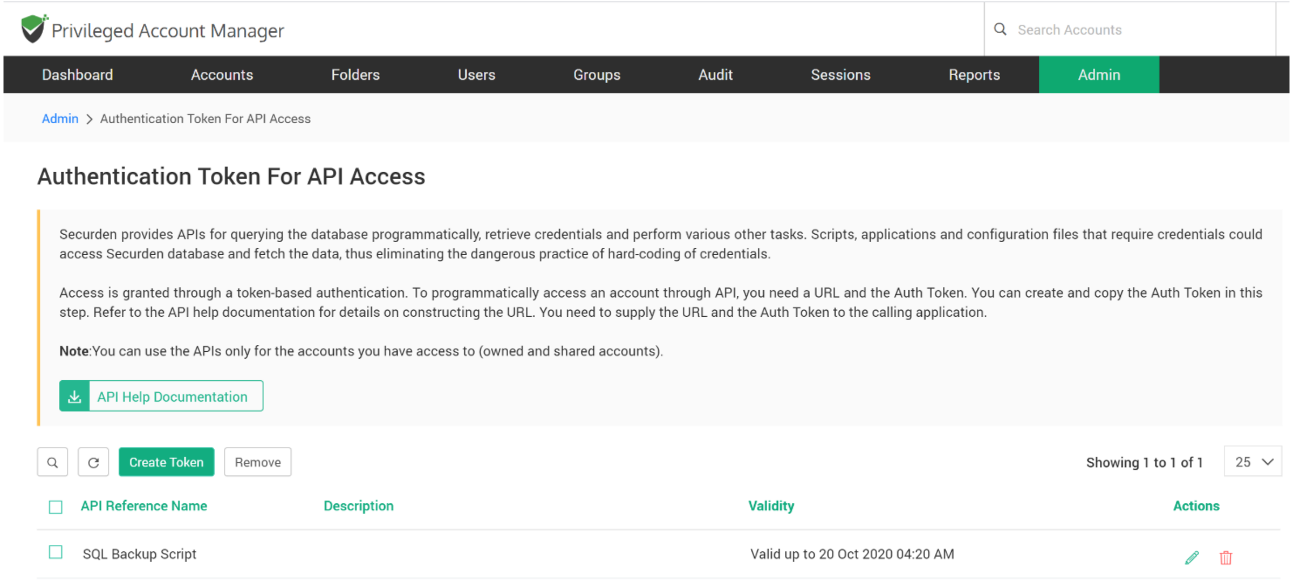
Title: Search Account Title

Note: To carry out remote actions for non-domain joined computers, you need to enter the credentials under '**Specific Computer**' section in the above GUI.

Step 14: 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 >> General >> Authentication Token for API Access** to start using the APIs. Refer to the API reference guide for information on making use of the APIs.



Authentication Token For API Access

Securden provides APIs for querying the database programmatically, retrieve credentials and perform various other tasks. Scripts, applications and configuration files that require credentials could access Securden database and fetch the data, thus eliminating the dangerous practice of hard-coding of credentials.

Access is granted through a token-based authentication. To programmatically access an account through API, you need a URL and the Auth Token. You can create and copy the Auth Token in this step. Refer to the API help documentation for details on constructing the URL. You need to supply the URL and the Auth Token to the calling application.

Note:You can use the APIs only for the accounts you have access to (owned and shared accounts).

□	API Reference Name	Description	Validity	Actions
□	SQL Backup Script		Valid up to 20 Oct 2020 04:20 AM	

Step 15: 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 16: 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.

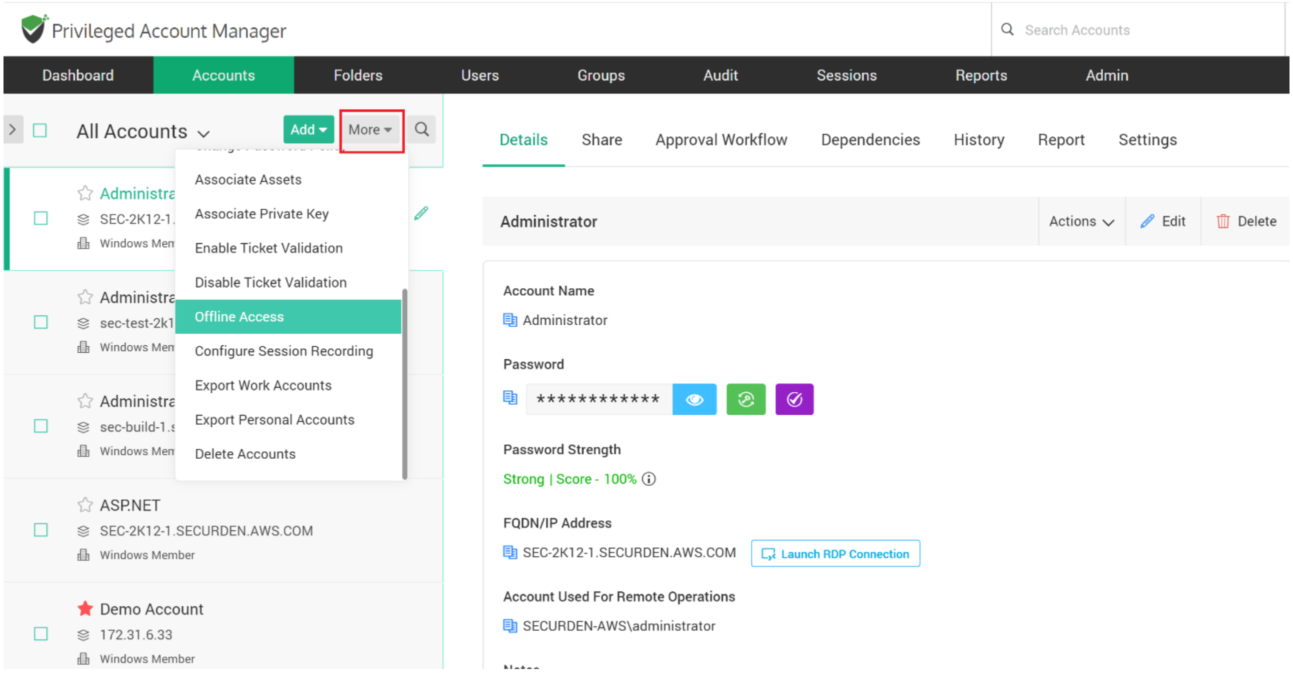
In addition, you can replace Securden’s logo with your company logo and also choose different GUI color themes. Navigate to **Admin >> Notifications >> Password Expiration Notification** to configure this.

Step 17: 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.

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.



Administra… SEC-2K12-1… Windows Mem…

Administra… sec-test-2k1… Windows Mem…

Administra… sec-build-1.s… Windows Mem…

ASP.NET
SEC-2K12-1.SECURDEN.AWS.COM
Windows Member

Demo Account
172.31.6.33
Windows Member

Administrator

Account Name
Administrator

Password
****

Password Strength
Strong | Score - 100%

FQDN/IP Address
SEC-2K12-1.SECURDEN.AWS.COM

Account Used For Remote Operations
SECURDEN-AWS\administrator

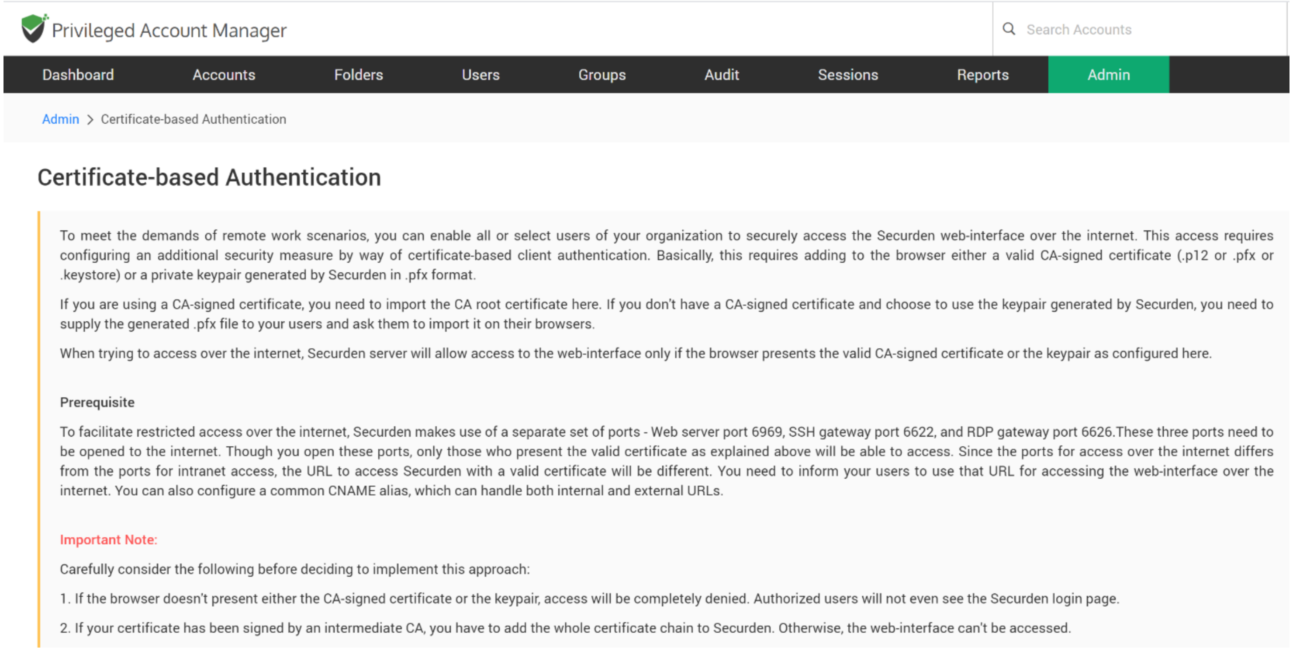
Navigate to **Accounts** section in the GUI, from "**More Actions**" (three horizontal lines icon on the LHS), click the '**Offline Access**' option and then follow the instructions in the GUI.

Step 18: Explore Restricted Access over the 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.



Certificate-based Authentication

To meet the demands of remote work scenarios, you can enable all or select users of your organization to securely access the Securden web-interface over the internet. This access requires configuring an additional security measure by way of certificate-based client authentication. 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.

If you are using a CA-signed certificate, you need to import the CA root certificate here. If you don't have a CA-signed certificate and choose to use the keypair generated by Securden, you need to supply the generated .pfx file to your users and ask them to import it on their browsers.

When trying to access over the internet, Securden server will allow access to the web-interface only if the browser presents the valid CA-signed certificate or the keypair as configured here.

Prerequisite

To facilitate restricted access over the internet, Securden makes use of a separate set of ports - Web server port 6969, SSH gateway port 6622, and RDP gateway port 6626.These three ports need to be opened to the internet. Though you open these ports, only those who present the valid certificate as explained above will be able to access. Since the ports for access over the internet differs from the ports for intranet access, the URL to access Securden with a valid certificate will be different. You need to inform your users to use that URL for accessing the web-interface over the internet. You can also configure a common CNAME alias, which can handle both internal and external URLs.

Important Note:

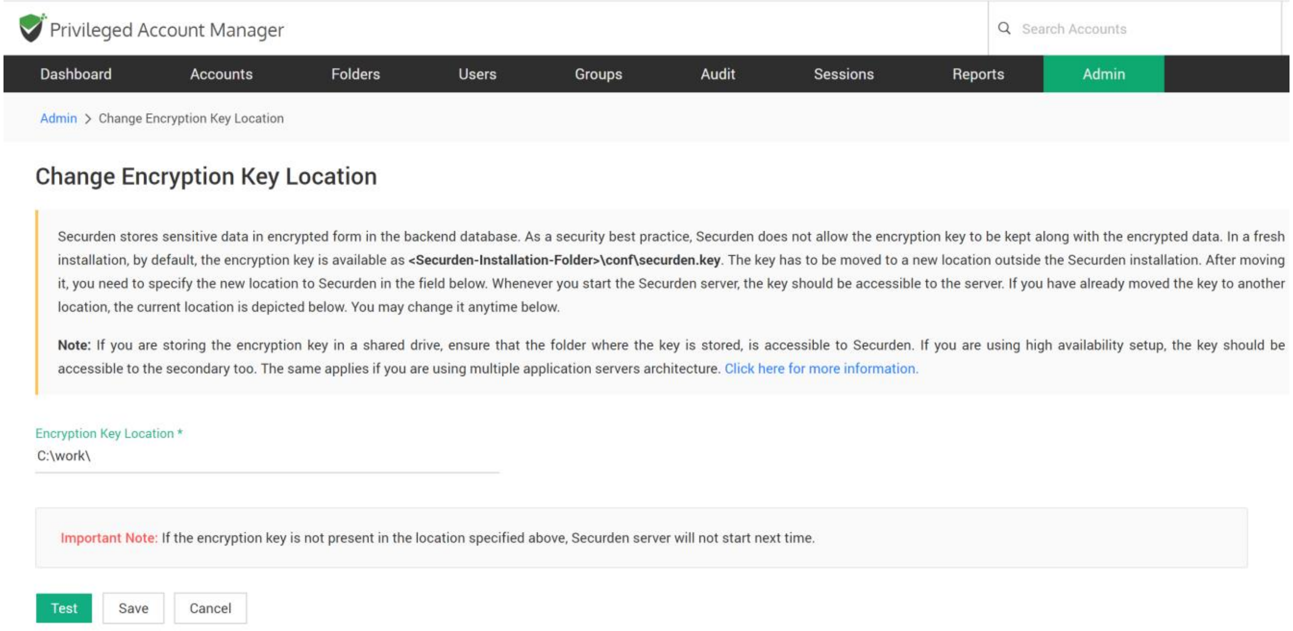
Carefully consider the following before deciding to implement this approach:

1. If the browser doesn't present either the CA-signed certificate or the keypair, access will be completely denied. Authorized users will not even see the Securden login page.

2. If your certificate has been signed by an intermediate CA, you have to add the whole certificate chain to Securden. Otherwise, the web-interface can't be accessed.

Step 19: 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.



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 a 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.

Note: If you are storing the encryption key in a shared drive, ensure that the folder where the key is stored, is accessible to Securden. If you are using high availability setup, the key should be accessible to the secondary too. The same applies if you are using multiple application servers architecture. Click here for more information.

Encryption Key Location *
C:\work\

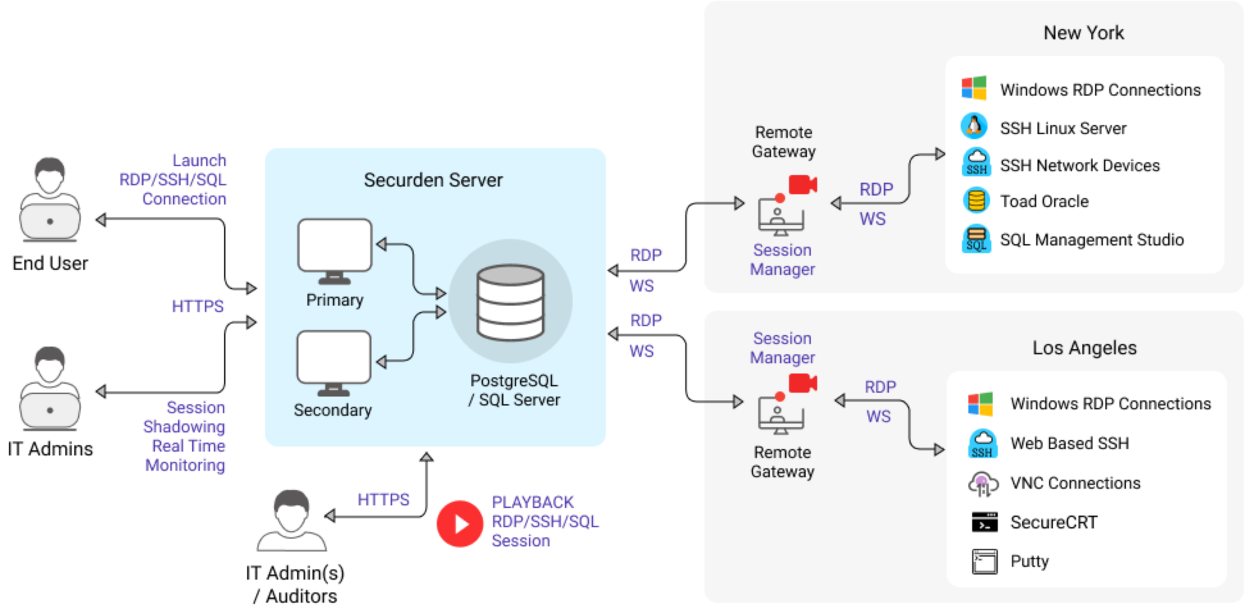
Important Note: If the encryption key is not present in the location specified above, Securden server will not start next time.

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 >> General >> Change Encryption Key Location**.

Section 3: Privileged Session Management (PSM)

Securden PAM serves as a robust session management solution too. In addition to enabling users to launch secure remote connections with the IT assets, Securden allows administrators to monitor sensitive sessions in parallel, record and playback the sessions.

Securden adopts the secure gateway concept for remote sessions management. That means, you can route all remote operations originating from Securden through a single gateway. All operations, including remote connections, session recording, and password resets are handled through the gateway. The remote gateway is designed to hold two components known as Securden Session Manager and Securden Application Server.



For session recording to take effect, you should first deploy the Securden Remote Gateway. In addition to session recording, there are other scenarios that would require deployment of the remote gateway.

When should you deploy a remote gateway?

1. To record remote sessions to IT assets launched by the users
2. To manage the IT assets/accounts distributed across multiple networks with interconnectivity
3. To route all remote operations (including password resets and connections) through a common gateway instead of direct connections to target devices from endpoints

The remote gateway comprises two components:

1. **Securden Session Manager** (Handles remote connections and session recording)
2. **Securden Application Server** (Handles remote password reset operations and serves as a remote broker)

How to decide which components to deploy on the remote gateway?

Based on your network structure and requirements, you should decide on having one or both the components.

- If your IT assets/accounts are distributed across multiple networks with interconnectivity, you should **deploy both** the above components on the remote gateway.
- On the other hand, if all your devices are present in the same network and if you want to handle only remote connections and session recording through a common gateway, **install Securden Session Manager alone**.
- If you want to handle remote connections as well as remote password resets through a common gateway, **deploy both**.

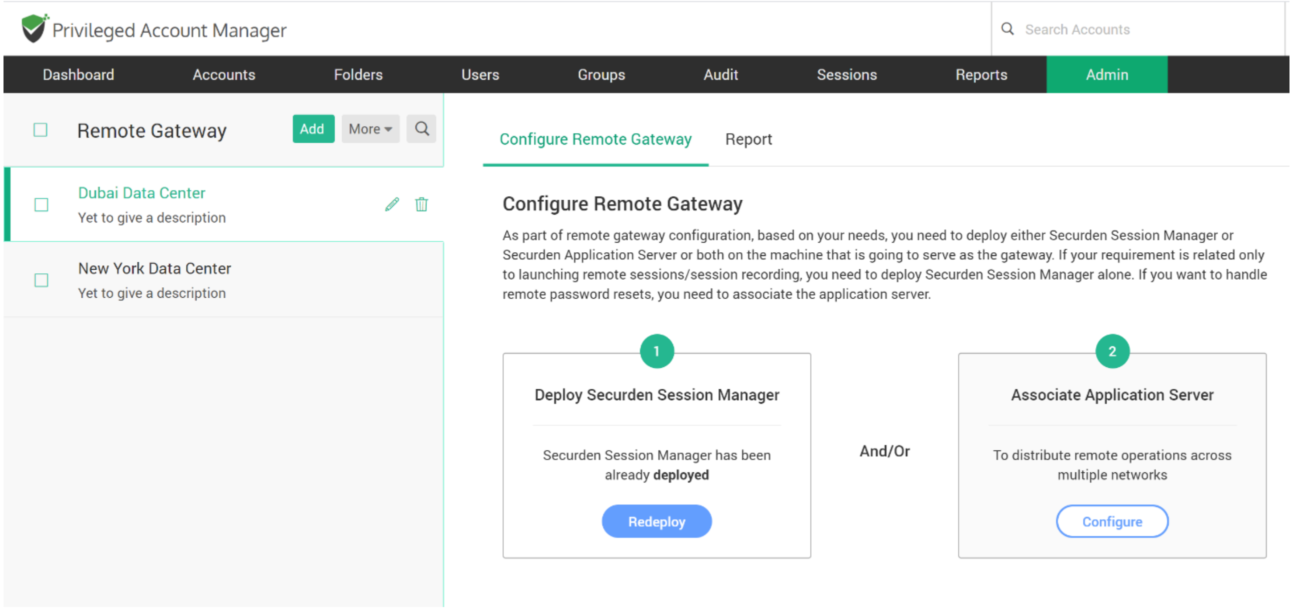
After establishing the remote gateway and the components, you need to finally associate the gateway with the required devices or the domain. Following is the summary of steps related to remote gateway configuration:

Remote Gateway Configuration: Summary of Steps

1. Create a remote gateway
2. Deploy Securden Session Manager and/or Securden Application Server
3. Associate devices with the gateway
4. Associate domains with the gateway (if required)

3.1 How to Configure Remote Gateway?

Navigate to **Admin >> Remote Sessions and Recordings >> Remote Gateway**. The configuration wizard will guide you through the steps.



Configure Remote Gateway

As part of remote gateway configuration, based on your needs, you need to deploy either Securden Session Manager or Securden Application Server or both on the machine that is going to serve as the gateway. If your requirement is related only to launching remote sessions/session recording, you need to deploy Securden Session Manager alone. If you want to handle remote password resets, you need to associate the application server.

Securden Session Manager has been already **deployed**

To distribute remote operations across multiple networks

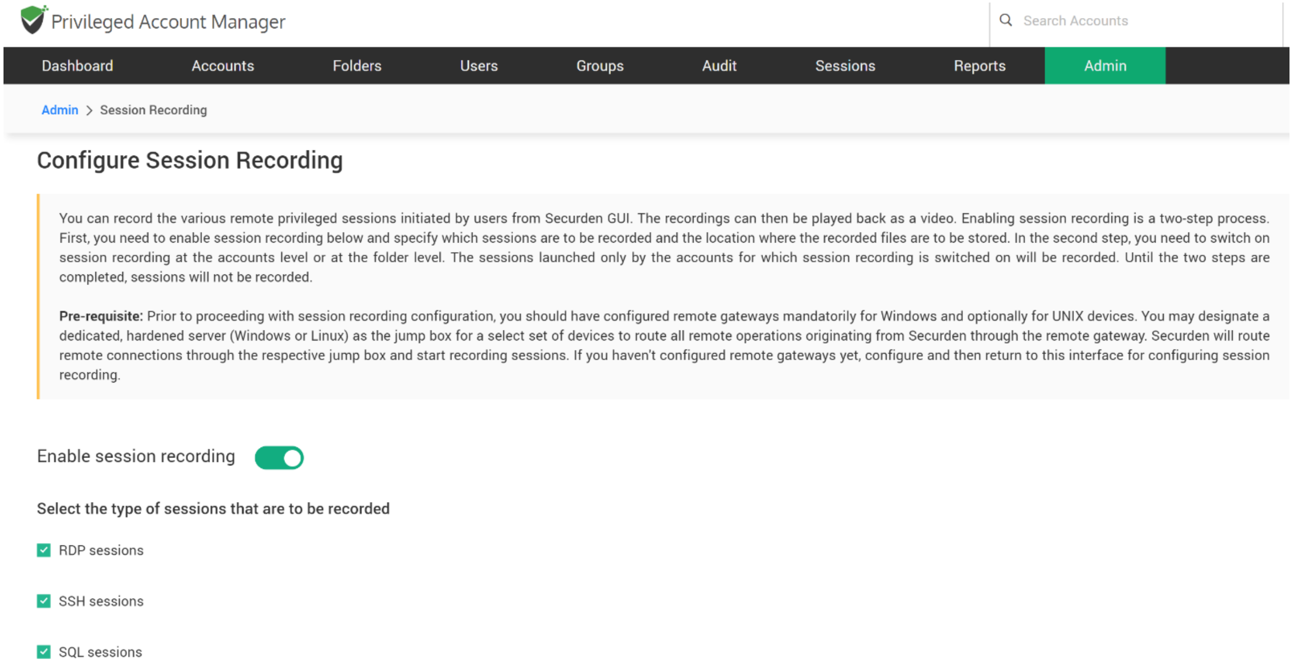
3.2 Configure Session Recording

After configuring the remote gateway as explained above, you need to configure session recording. The configuration is a two-step process:

1. First, you need to enable session recording and specify which sessions are to be recorded - RDP, SSH, and SQL. You also need to specify the location where the recorded files are to be stored.

2. In the second step, you need to switch on session recording at the accounts level or at the folder level. The sessions launched only by the accounts for which session recording is switched on will be recorded.

Until the two steps are completed, sessions will not be recorded.



Configure Session Recording

You can record the various remote privileged sessions initiated by users from Securden GUI. The recordings can then be played back as a video. Enabling session recording is a two-step process. First, you need to enable session recording below and specify which sessions are to be recorded and the location where the recorded files are to be stored. In the second step, you need to switch on session recording at the accounts level or at the folder level. The sessions launched only by the accounts for which session recording is switched on will be recorded. Until the two steps are completed, sessions will not be recorded.

Pre-requisite: Prior to proceeding with session recording configuration, you should have configured remote gateways mandatorily for Windows and optionally for UNIX devices. You may designate a dedicated, hardened server (Windows or Linux) as the jump box for a select set of devices to route all remote operations originating from Securden through the remote gateway. Securden will route remote connections through the respective jump box and start recording sessions. If you haven't configured remote gateways yet, configure and then return to this interface for configuring session recording.

Enable session recording ●

Select the type of sessions that are to be recorded

☑ RDP sessions

☑ SSH sessions

☑ SQL sessions

3.3 Monitor Live Sessions, Playback Recordings

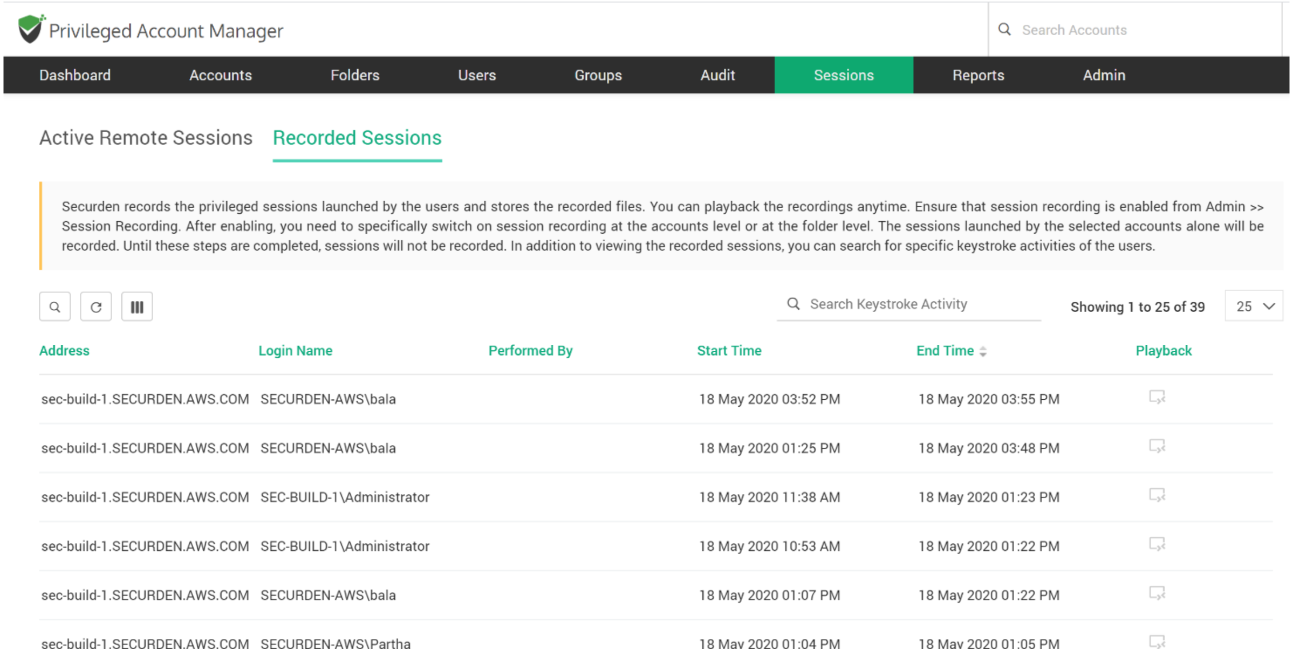
After configuring session recording, as an administrator, you can do two things:

- **Monitor live sessions in parallel** (you can monitor sensitive access by 3rd-parties. You may also use this to collaborate with your colleagues like offering technical instructions while watching what they are doing). You will have full controls over the live monitoring. That means, you can terminate sessions anytime.

- **Playback recorded sessions** (you can playback the recordings to understand what exactly was done. This may even be used in forensic audits).

To monitor live sessions, navigate to **Sessions >> Active Remote Sessions** in the GUI. You can monitor sessions in parallel and terminate sessions if you find any suspicious activities.

To playback recorded sessions, navigate to **Sessions >> Recorded Sessions** and click the required session. You can also do a search for specific keystroke activities to identify specific actions.



Securden records the privileged sessions launched by the users and stores the recorded files. You can playback the recordings anytime. Ensure that session recording is enabled from Admin >> Session Recording. After enabling, you need to specifically switch on session recording at the accounts level or at the folder level. The sessions launched by the selected accounts alone will be recorded. Until these steps are completed, sessions will not be recorded. In addition to viewing the recorded sessions, you can search for specific keystroke activities of the users.

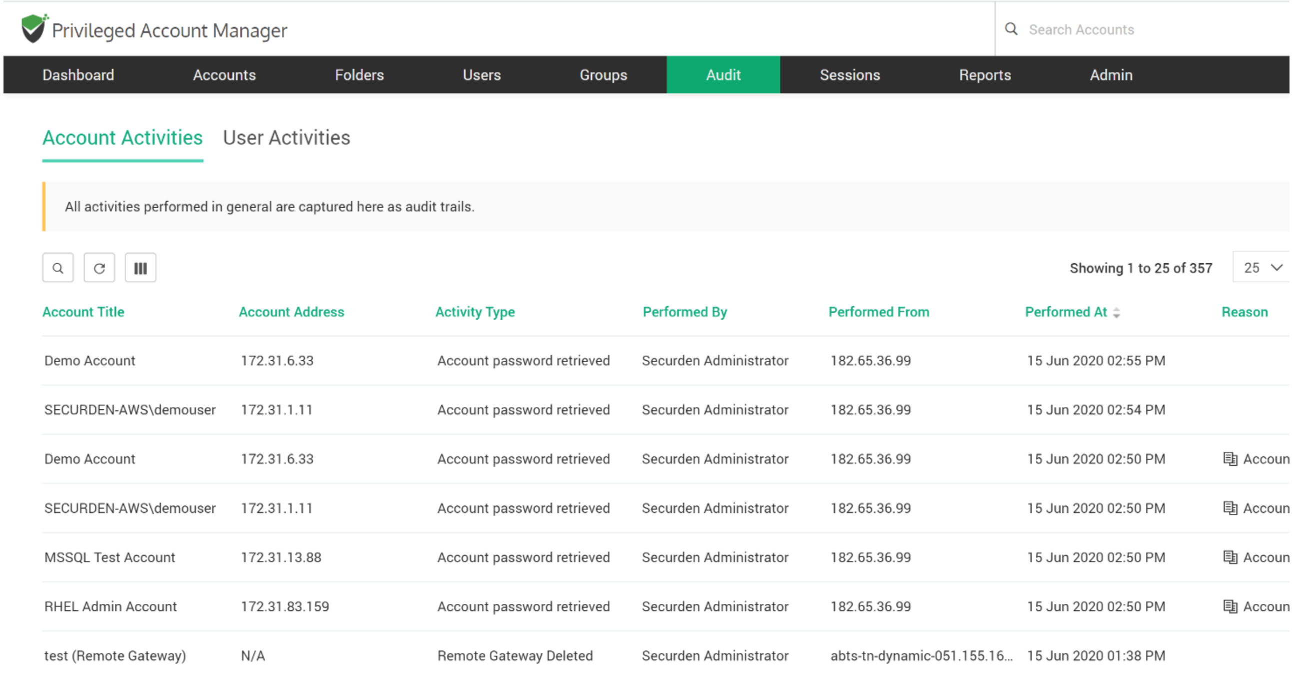
Address	Login Name	Performed By	Start Time	End Time	Playback
sec-build-1.SECURDEN.AWS.COM	SECURDEN-AWS\bala		18 May 2020 03:52 PM	18 May 2020 03:55 PM	🖵
sec-build-1.SECURDEN.AWS.COM	SECURDEN-AWS\bala		18 May 2020 01:25 PM	18 May 2020 03:48 PM	🖵
sec-build-1.SECURDEN.AWS.COM	SEC-BUILD-1\Administrator		18 May 2020 11:38 AM	18 May 2020 01:23 PM	🖵
sec-build-1.SECURDEN.AWS.COM	SEC-BUILD-1\Administrator		18 May 2020 10:53 AM	18 May 2020 01:22 PM	🖵
sec-build-1.SECURDEN.AWS.COM	SECURDEN-AWS\bala		18 May 2020 01:07 PM	18 May 2020 01:22 PM	🖵
sec-build-1.SECURDEN.AWS.COM	SECURDEN-AWS\Partha		18 May 2020 01:04 PM	18 May 2020 01:05 PM	🖵

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.

Showing 1 to 25 of 357 | 25

Account Title	Account Address	Activity Type	Performed By	Performed From	Performed At	Reason
Demo Account	172.31.6.33	Account password retrieved	Securden Administrator	182.65.36.99	15 Jun 2020 02:55 PM	
SECURDEN-AWS\demouser	172.31.1.11	Account password retrieved	Securden Administrator	182.65.36.99	15 Jun 2020 02:54 PM	
Demo Account	172.31.6.33	Account password retrieved	Securden Administrator	182.65.36.99	15 Jun 2020 02:50 PM	Accoun
SECURDEN-AWS\demouser	172.31.1.11	Account password retrieved	Securden Administrator	182.65.36.99	15 Jun 2020 02:50 PM	Accoun
MSSQL Test Account	172.31.13.88	Account password retrieved	Securden Administrator	182.65.36.99	15 Jun 2020 02:50 PM	Accoun
RHEL Admin Account	172.31.83.159	Account password retrieved	Securden Administrator	182.65.36.99	15 Jun 2020 02:50 PM	Accoun
test (Remote Gateway)	N/A	Remote Gateway Deleted	Securden Administrator	abts-tn-dynamic-051.155.16...	15 Jun 2020 01:38 PM	

4.2 Explore Reports

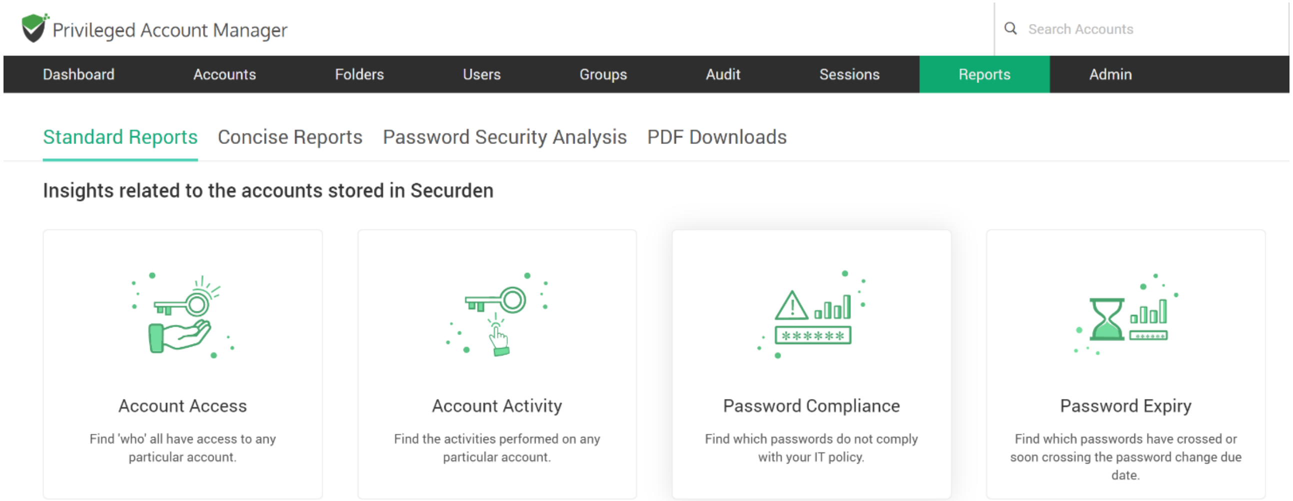
Reports are classified into three categories – standard reports, concise reports, and security analysis report. All the reports can be downloaded in the form of PDF.

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.). **Dependencies** report provides complete visibility on the dependencies of domain/local accounts on each computer.



Insights related to the accounts stored in Securden

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

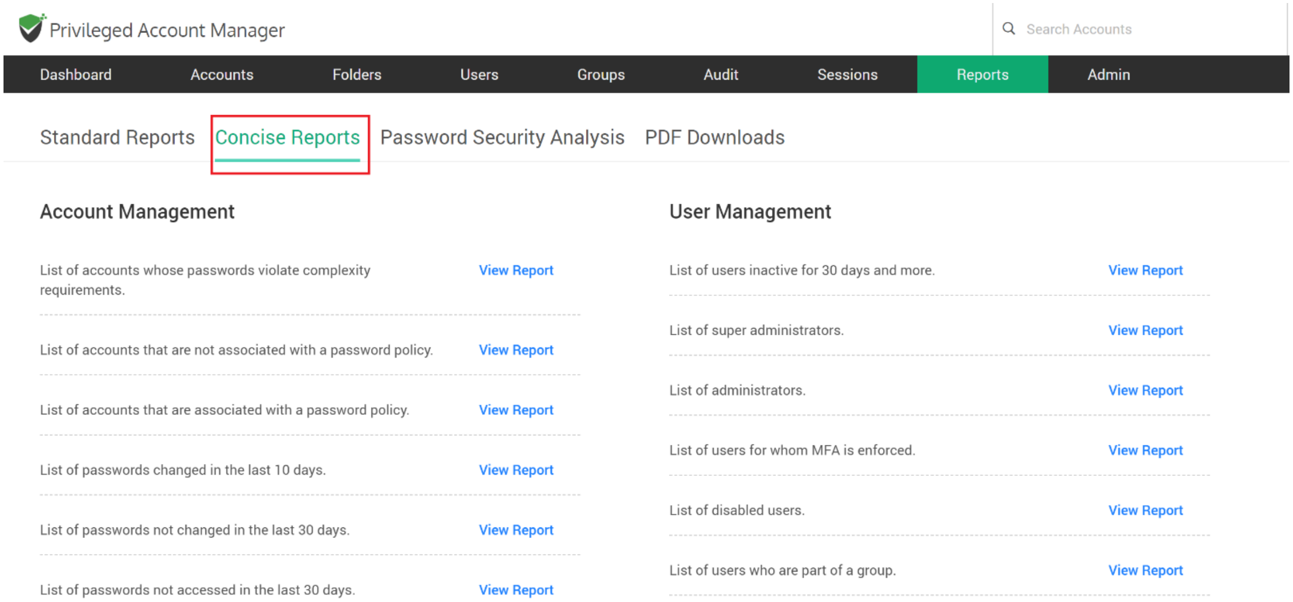
Account Activity
Find the activities performed on any particular account.

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

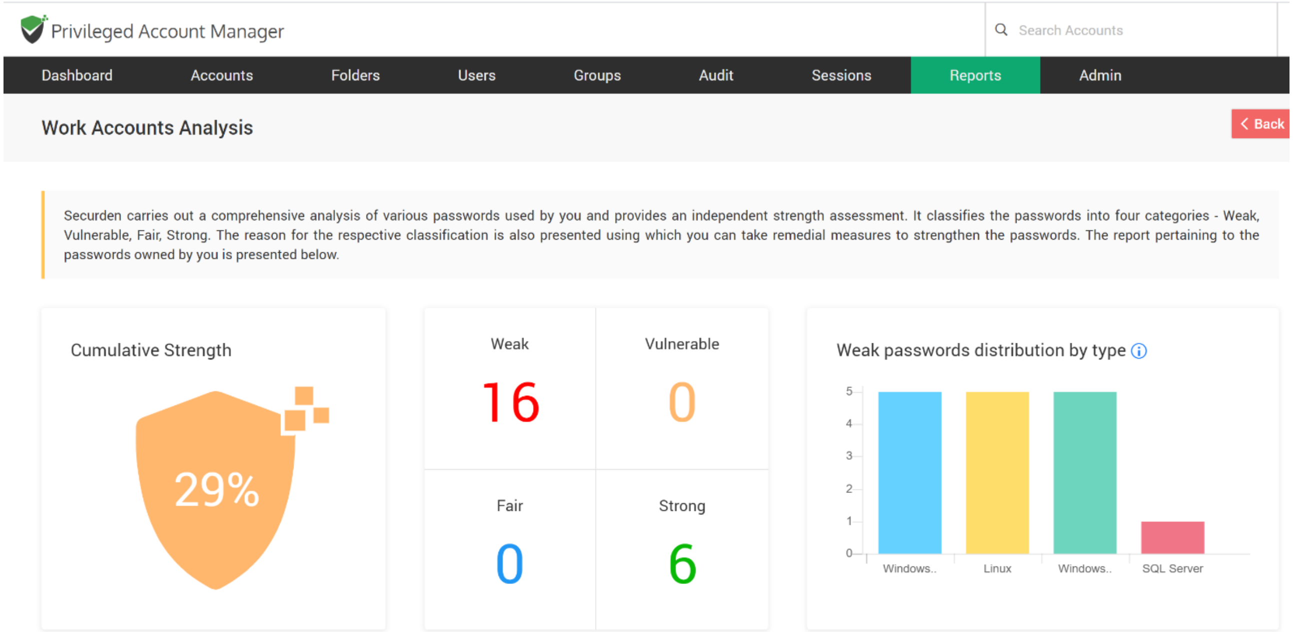
List of users for whom MFA is enforced. View Report

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.



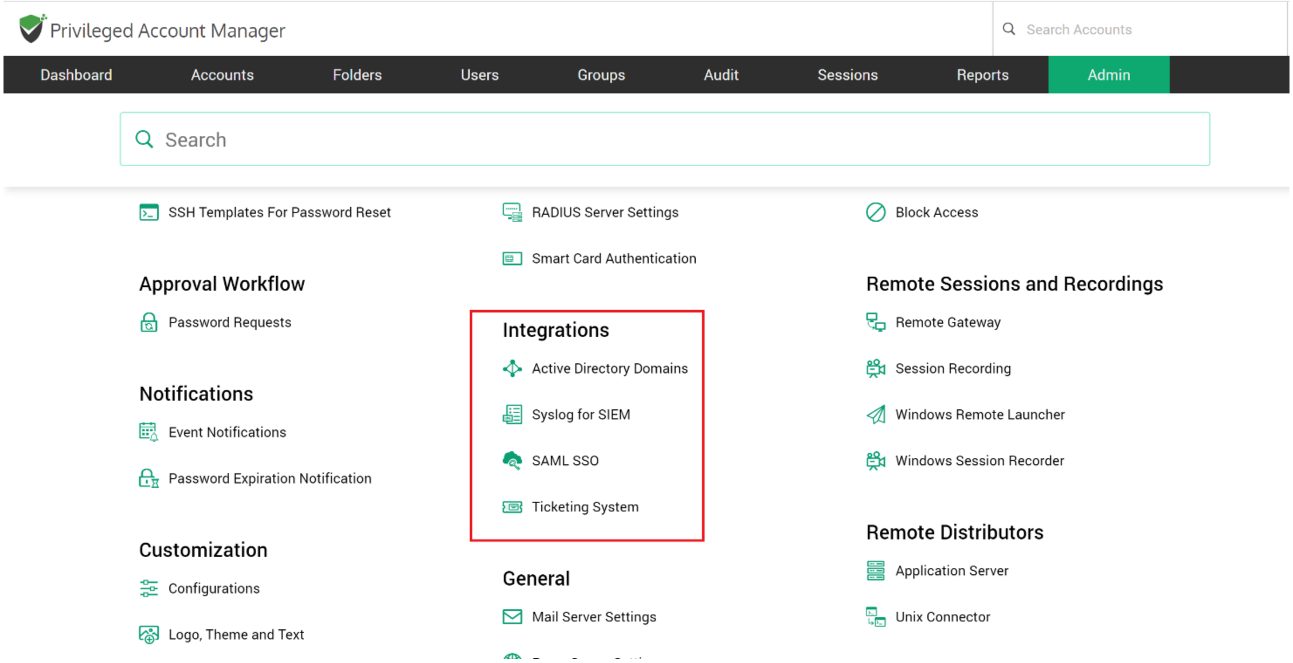
Work Accounts Analysis

Securden carries out a comprehensive analysis of various passwords used by you and provides an independent strength assessment. It classifies the passwords into four categories - Weak, Vulnerable, Fair, Strong. The reason for the respective classification is also presented using which you can take remedial measures to strengthen the passwords. The report pertaining to the passwords owned by you is presented below.

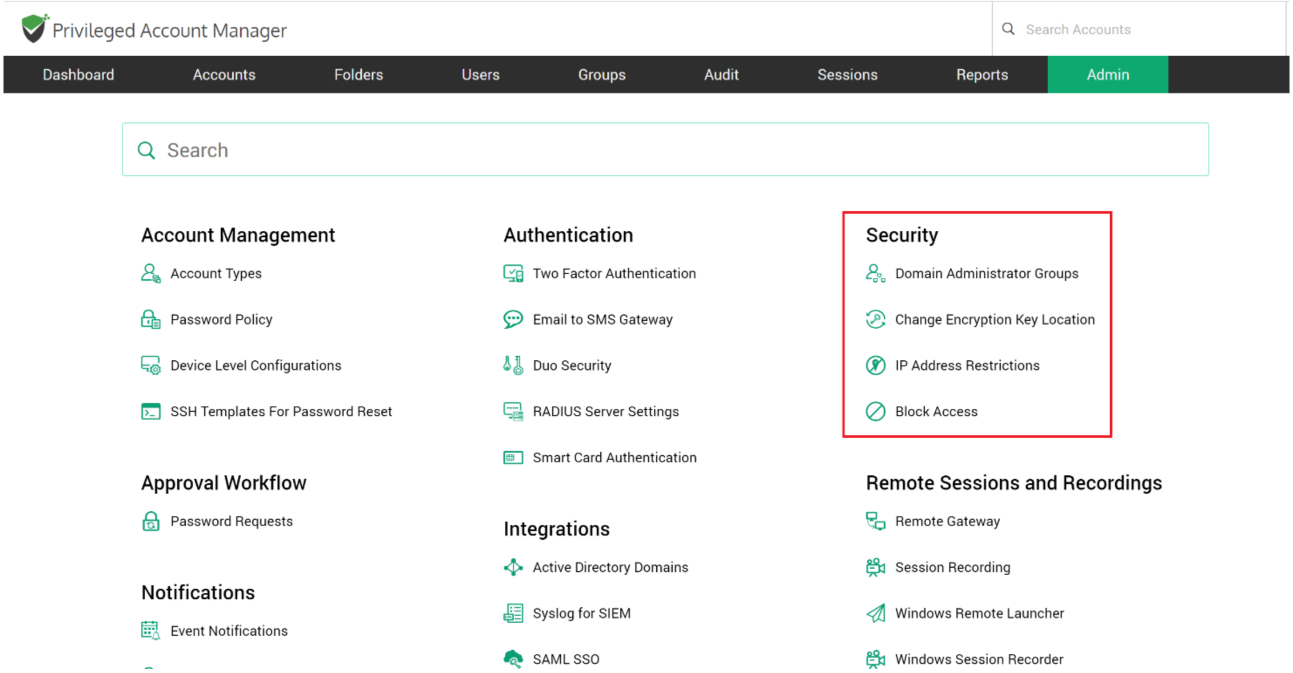
Section 5: Integrations & Security Aspects

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

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

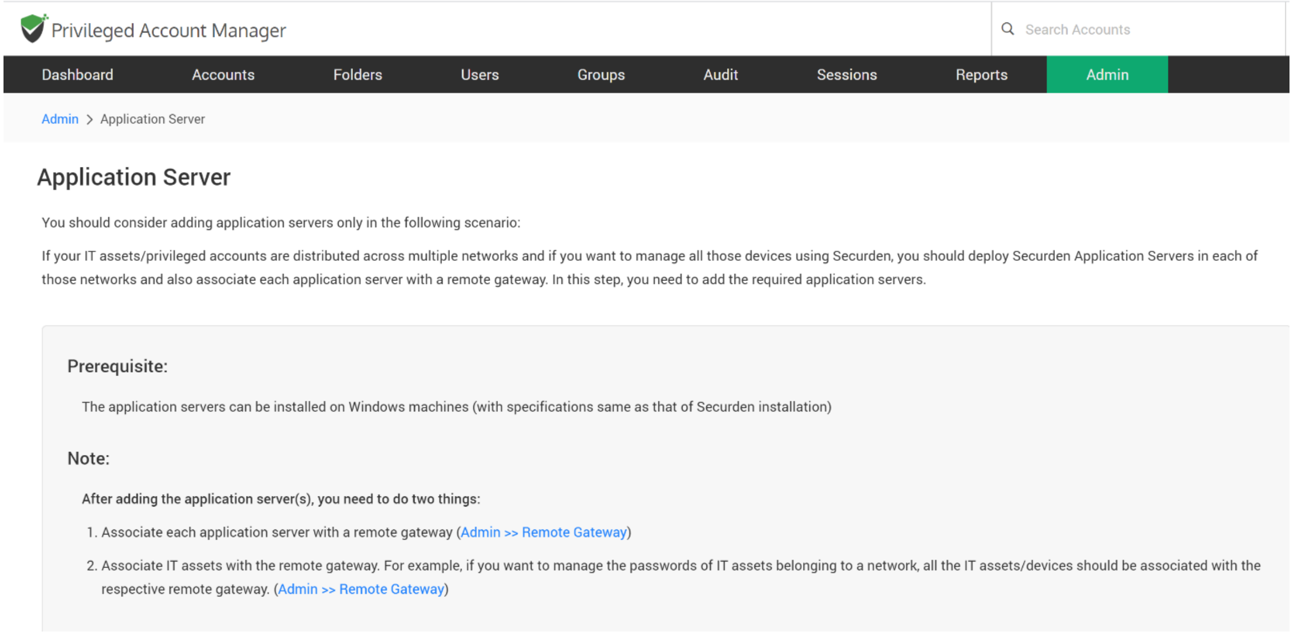


To explore the additional security aspects, navigate to **Admin >> Security** section. You can monitor the changes happening to Windows domain administrator groups, establish IP-based restrictions for accessing Securden web-interface, and control/block access to Securden through browser extensions and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



Section 6: Explore Distributed Deployment

If your IT assets or privileged accounts are distributed across multiple networks and if you want to manage all those devices using Securden, you can deploy Securden Application Servers in each of those networks and also associate each application server with a remote gateway.



Application Server

You should consider adding application servers only in the following scenario:

If your IT assets/privileged accounts are distributed across multiple networks and if you want to manage all those devices using Securden, you should deploy Securden Application Servers in each of those networks and also associate each application server with a remote gateway. In this step, you need to add the required application servers.

Prerequisite:

The application servers can be installed on Windows machines (with specifications same as that of Securden installation)

Note:

After adding the application server(s), you need to do two things:

1. Associate each application server with a remote gateway (Admin >> Remote Gateway)
2. Associate IT assets with the remote gateway. For example, if you want to manage the passwords of IT assets belonging to a network, all the IT assets/devices should be associated with the respective remote gateway. (Admin >> Remote Gateway)

The process of deploying additional application servers is quite simple and can be done as and when the need the arises. It is a simple three-step process and you can do these steps from **Admin >> Remote Distributors >> Application Serve**r.

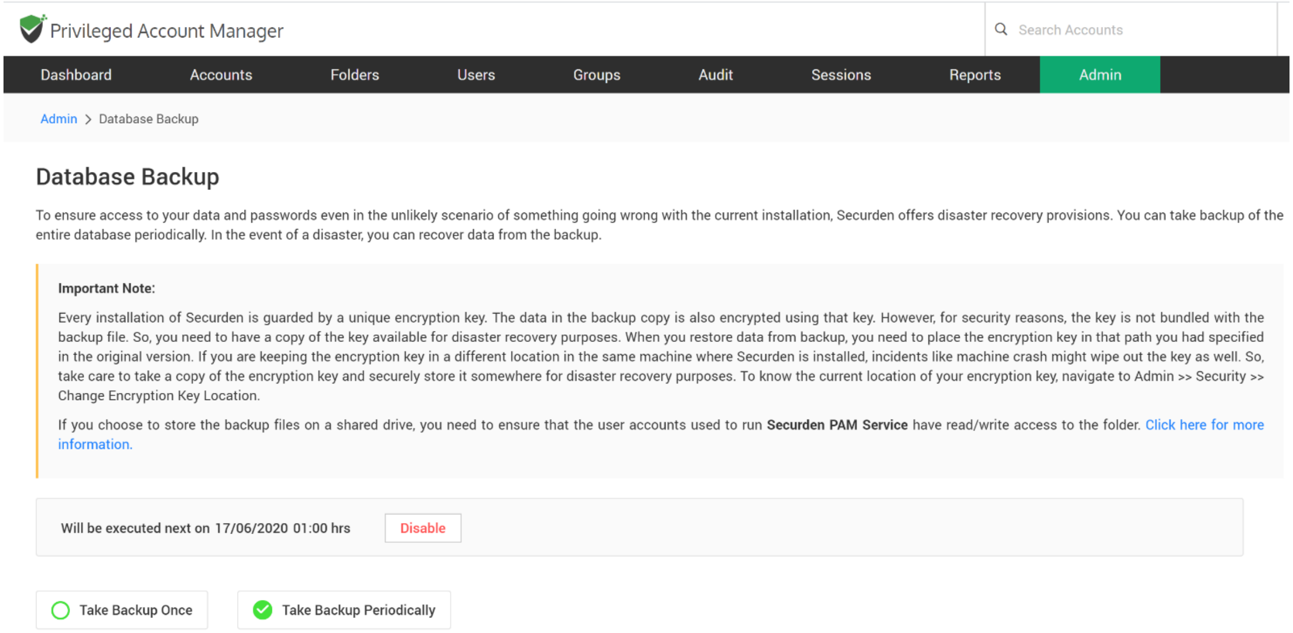
1. Identify the machine where the additional application server is to be installed. Typically, you will install a full version of Securden in the machine.
2. Create an 'Application Server Package' from Securden GUI by entering the details about the Application Server machine. You will get Application Server package as a .zip file.
3. Deploy this package on the machine identified for the Application Server. Repeat the above steps to add multiple application servers.

Section 7: Database Backup, Disaster Recovery and High Availability

7.1 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.

If you choose to store the backup files on a shared drive, you need to ensure that the user accounts used to run **Securden PAM Service** have read/write access to the folder. Click here for more information.

Will be executed next on 17/06/2020 01:00 hrs

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.

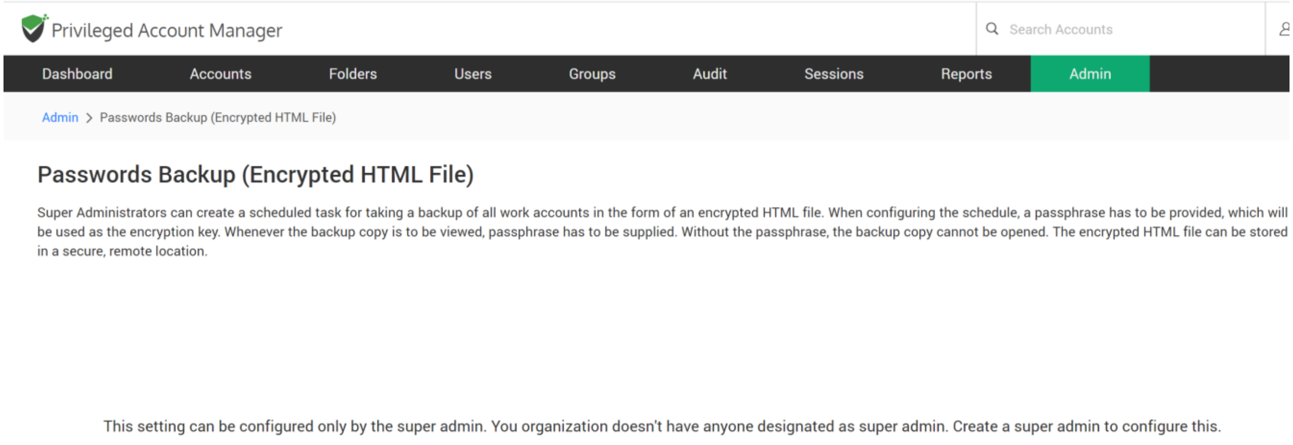
7.2 Disaster Recovery

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**.
- 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\PAM\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 PAM Service (You may safely ignore the other service named Securden Web Service, which is automatically taken care of).

7.3 Periodic Backup of Passwords as Encrypted HTML



Admin > Passwords Backup (Encrypted HTML File)

Passwords Backup (Encrypted HTML File)

Super Administrators can 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.

This setting can be configured only by the super admin. You organization doesn't have anyone designated as super admin. Create a super admin to configure this.

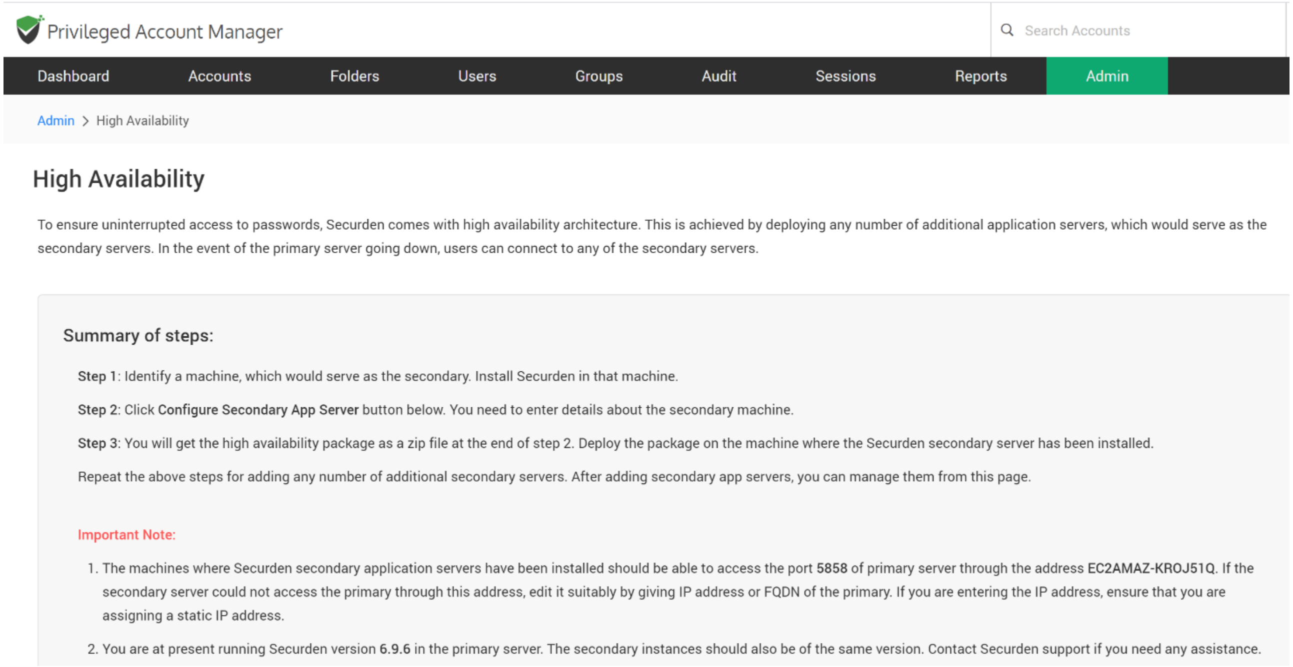
As an additional backup option, Securden allows Super Administrators to create a scheduled task for taking a backup of all work accounts in the form of an encrypted HTML file. When configuring the schedule, a passphrase has to be provided, which will be used as the encryption key. Whenever the backup 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.

7.4 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.



High Availability

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

Summary of steps:

Step 1: Identify a machine, which would serve as the secondary. Install Securden in that machine.

Step 2: Click **Configure Secondary App Server** button below. You need to enter details about the secondary machine.

Step 3: You will get the high availability package as a zip file at the end of step 2. Deploy the package on the machine where the Securden secondary server has been installed.

Repeat the above steps for adding any number of additional secondary servers. After adding secondary app servers, you can manage them from this page.

Important Note:

1. The machines where Securden secondary application servers have been installed should be able to access the port **5858** of primary server through the address **EC2AMAZ-KROJ51Q**. If the secondary server could not access the primary through this address, edit it suitably by giving IP address or FQDN of the primary. If you are entering the IP address, ensure that you are assigning a static IP address.
2. You are at present running Securden version **6.9.6** in the primary server. The secondary instances should also be of the same version. Contact Securden support if you need any assistance.

Section 8: Miscellaneous

8.1 Replace 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.

8.2 (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 PAM 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 PAM Service**" from services.msc (you may ignore the other service named Securden Web Service, which is automatically taken care of)
- Connect to the web interface https://<local-host>:5959 (or) https://<host-name>:5959
- Clear browser cache