



Unified PAM

Administrator Guide

This document covers the steps involved in configuring Securden Unified PAM along with troubleshooting tips.



Table of Contents

Section 1: Getting Started	7
Starting the PAM Service.....	7
Launching the Web Interface	8
 Section 2: General Configuration Settings.....	 10
Configure Mail Server Settings	10
Proxy Server Settings.....	14
Securden Server Connectivity	16
Replace Self-signed Certificate	20
 Section 3: User Management	 23
User Management.....	23
Import Users from Active Directory.....	24
Import Users from LDAP	33
Import from Azure AD	38
Import Users from File	43
Add Users Manually	47
Assigning Roles to Users	52
Custom User Roles.....	57
User Groups.....	91
Import User Groups from AD	92
Import groups from LDAP	96
Import from Azure AD	101
Add User Groups Manually	103
Configure Periodic Synchronization of Groups	105

Explore Single Sign-On Options	108
Configure Single Sign-On for Okta	113
Configure Single Sign-On for Azure AD	118
Configure Single Sign-On for Ping Identity.....	120
Configure Single Sign-On for One Login	123
Configure Single Sign-On for G-Suite	125
Configure Single Sign-On for Microsoft ADFS	127
Section 4: Configuring Two Step Verification	132
Mail OTP	134
Google Authenticator/Microsoft Authenticator/TOTP Authenticator.....	135
Yubikey	136
Radius Authentication	141
Email to SMS Gateway	142
DUO Authentication	143
Smart Card Authentication	149
Section 5: Account Management.....	152
Discovering Privileged Accounts.....	152
Running Discovery on Windows Servers.....	154
Discovering Privileged Accounts on Mac Devices	182
Discovering through Remote Gateway.....	185
Discovering through a Unix Connector.....	185
Discovering Privileged Accounts on Linux Devices.....	195
Discovering through Remote Gateway.....	198
Discovering through a Unix Connector.....	199
Discover and Import Accounts from Databases.....	208
Discover Privileged Accounts from PostgreSQL Databases.....	208
Discover Privileged Accounts from SQL Servers	218
Discover Privileged Accounts from Oracle Databases.....	229
Discovering Privileged Accounts from MySQL Databases	240

Discovering and Importing accounts from Cisco IOS Devices	250
Importing Accounts from CSV/XLSX Files	265
Adding Accounts Manually	268
Importing accounts from KeePass	275
Add and Manage SSH Keys	277
Add Documents/Files	280
Password Management Operations	285
Manage Windows Dependencies and Service Accounts	294
Launching Remote Connections	296
Launching Native RDP connections	300
Launching Native SSH connection	308
Launching Native SQL connections	309
Launching connections to thick application clients	310
Share Accounts with Users/Groups	319
Configuring Shared MFA Tokens	327
Share Accounts/Passwords with Third Parties	329
Just-in-time Access through Approval Workflows	335
Performing Operations on Multiple Accounts	351
Add and Manage Account Types	354
Section 6: Notifications	376
Event Notification	376
Account Expiration Notification	378
Password Expiration Notification	380
Breached Password Identification	382
Expired Password Rotation	384
Event Listener	386
Section 7: API Access	398
APIs for Programmatic Access	398

Section 8: Folder Management	406
Manually Adding Folders	406
Import Folders from Files.....	409
Configure Automated, Periodic Remote Password Resets	428
 Section 9: Audits.....	 442
Account activities:	442
User activities.....	449
Session Trails:	451
 Section 10: Configure Session Recording	 454
Steps to configure session recording	455
Playback recorded sessions	461
Search by keystroke activity	462
 Section 11: Configuring the Remote Gateway	 466
Create a remote gateway	467
Add Assets for Remote Connections.....	488
Domain Accounts - Asset Associations.....	494
User – Assets/Application Association.....	500
Custom Application Launcher.....	504
 Section 12: Privilege Elevation and Delegation (PEDM)	 517
Deploy Securden Agent on Computers	517
Discover / Add Applications, Processes, Commands	522
Create Control Policies	527
Technician Access Policies.....	532
Approval for policies	534
Eliminate Local Admin Rights	536

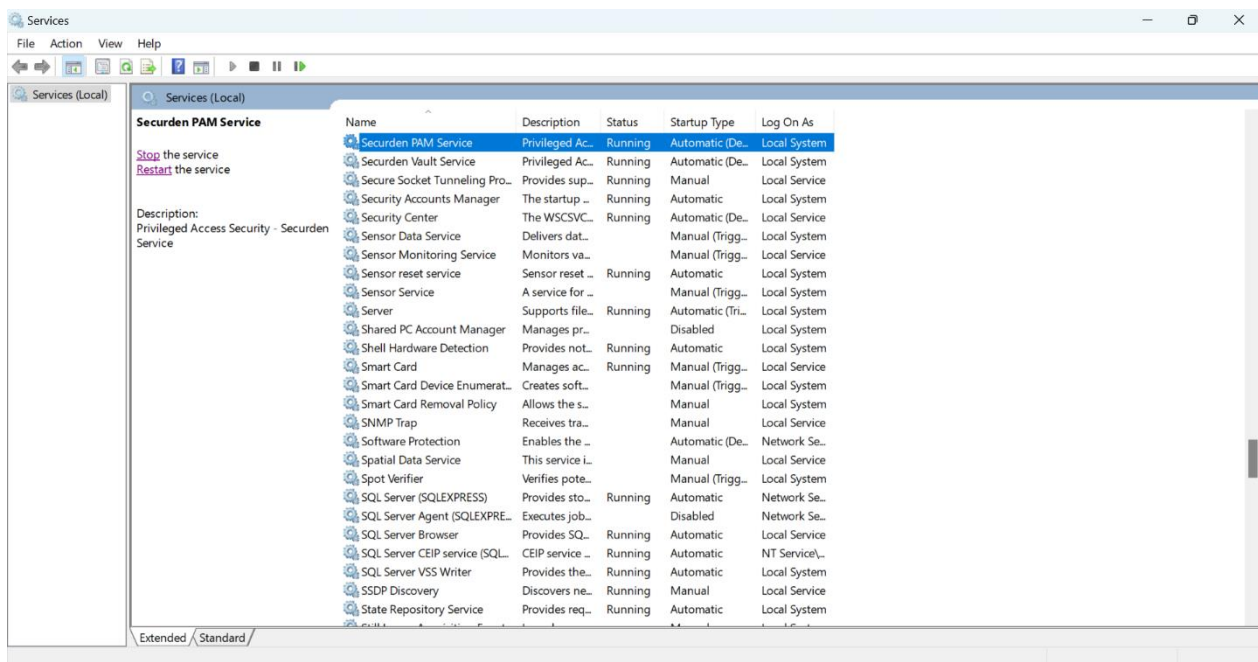
Section 13: Customization	542
Customize Securden PAM	542
Securden Agent Text Customization.....	542
Configurations.....	545
Changing Logo, Theme, and Text.....	595
 Section 14: Security Settings.....	 601
Change the Encryption Key Location	604
Block Access through API, Extensions, Mobile Apps.....	608
 Section 15: Emergency Access Settings	 609
Configure Emergency Access	609
Database Backup	613
Backup of Passwords as an Encrypted HTML File.....	617
 Section 16: High Availability.....	 619
Configure High Availability.....	619
 Section 17: Distributed Architecture	 631
Remote Distributors	631
Unix Connector.....	635
 Section 18: Reports	 638
Standard Reports.....	638
Concise Reports	656
Account Management	656
User Management.....	657
Password Security Analysis.....	658
Work Account Analysis	658

Personal Account Analysis	660
Exported Reports	661
Section 19: Miscellaneous.....	662
Change Database.....	662
Browser Extensions	665
Moving Securden Installation from One Machine to Another.....	670
Section 20: Product License Key	672

Section 1: Getting Started

Starting the PAM Service

- You can start and shut down the PAM service from the Windows Services Manager.
- Locate **Securden PAM Service** and start or stop it as required. This takes care of starting and stopping the dependent services too.



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

Troubleshooting tips:

1. The PAM Service/Web Service does not start automatically

Ensure the following:

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

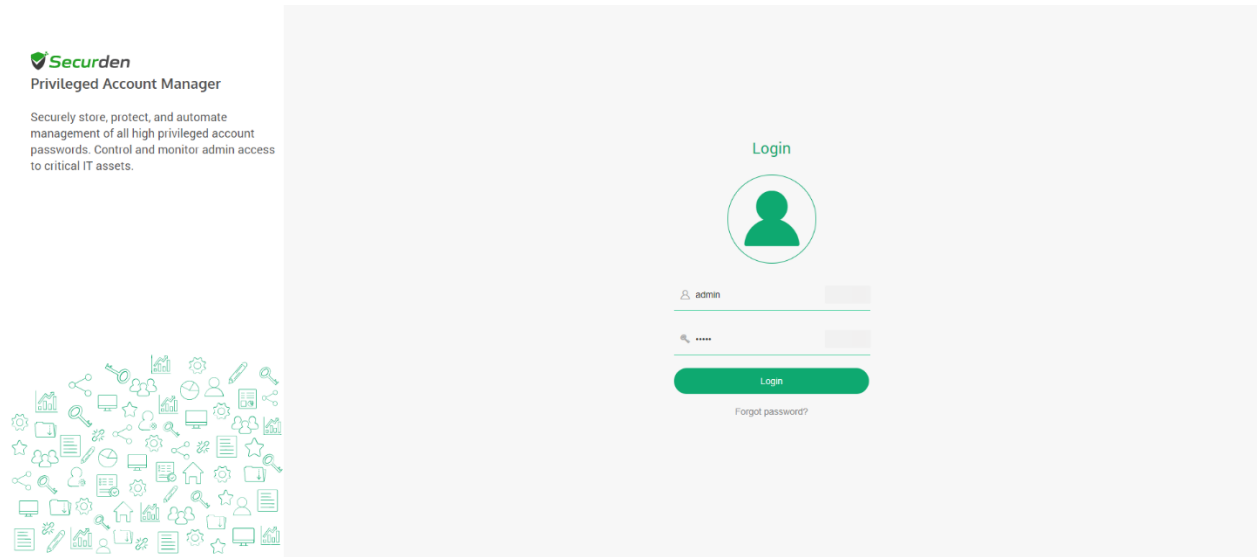
Launching the Web Interface

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

https://<PAM server hostname>:5959

If you have configured a port to be something other than the default port **5959**, you need to enter that port in the URL instead.

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



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

Username: admin

Password: admin

Troubleshooting Tips:

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

- In Chrome, click **Advanced** and then click **Proceed to <hostname> (unsafe)**.
- In the case of Internet Explorer, click **Details** and then **Go on to the webpage**

Section 2: General Configuration Settings

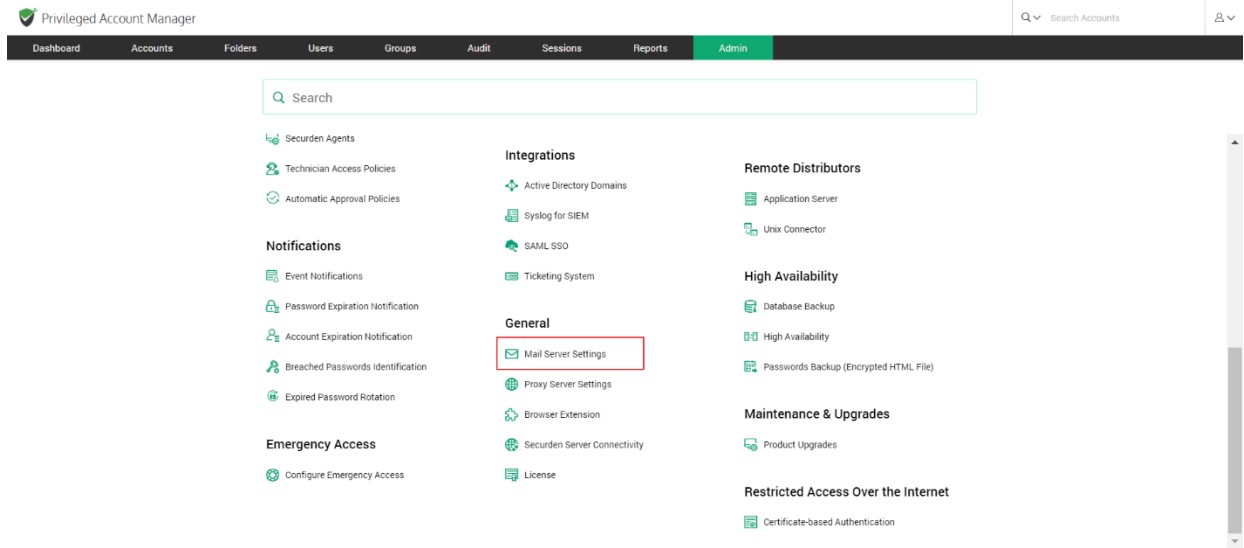
Upon deploying Securden, you need to carry out certain settings before proceeding with configuring the features. These settings are classified under the **Admin >> General** section.

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

Configure Mail Server Settings

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

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



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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Search Accounts

Admin > Configure SMTP Server Settings

SMTP Server Name (Hostname or IP Address)*
smtp.securden.com

Connection Mode
☐ TLS ☐ SSL ☒ None

SMTP Port*
25

Sender Email Address for Notifications*

☒ Supply Credentials (if authentication required)

Username

Password

Save Send Test Email Cancel

Enter the following SMTP details:

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

Connection Mode: Select the mode in which the SMTP accepts connections. Select TLS or SSL for encrypted connections. The option **None** indicates the default SMTP connection mode (not recommended).

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

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

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

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

The screenshot shows the 'Admin' section of the Securden Privileged Account Manager. The breadcrumb trail is 'Admin > Configure SMTP Server Settings'. A message states: 'Securden sends various email notifications to the users and to facilitate that, SMTP server details are to be configured here.'

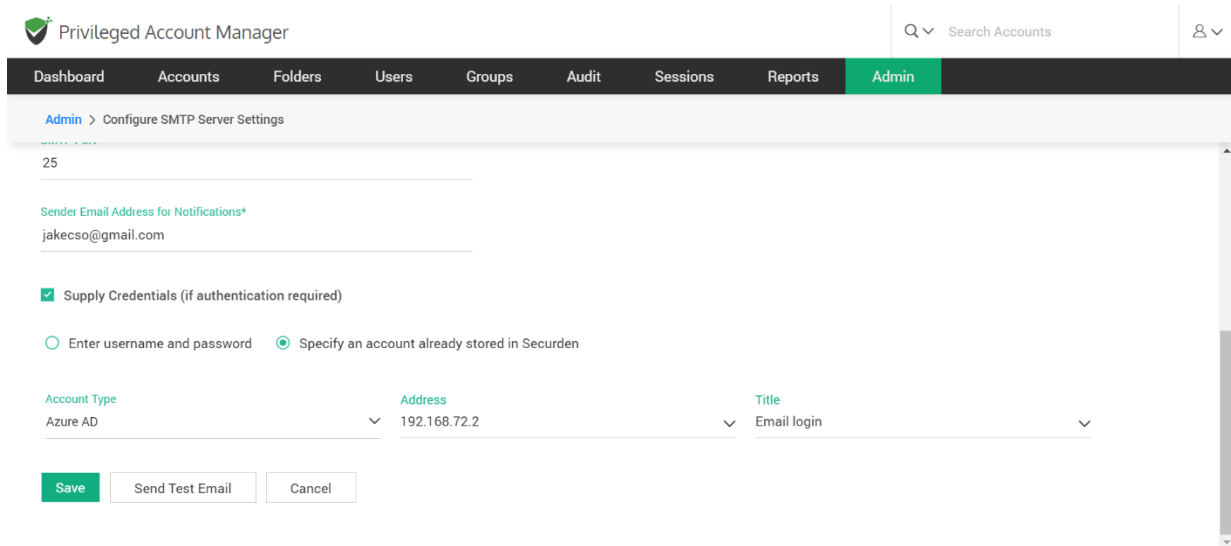
The configuration form includes the following fields and options:

- SMTP Server Name (Hostname or IP Address)*:** smtp.gmail.com
- Connection Mode:** Radio buttons for TLS, SSL, and None. 'None' is selected.
- SMTP Port*:** 25
- Sender Email Address for Notifications*:** (Empty field)
- Supply Credentials (if authentication required):**
 - ☒ Supply Credentials (if authentication required)
 - ☐ Enter username and password
 - ☒ Specify an account already stored in Securden (This option is highlighted with a red box in the image)
- Account Selection:** A table with columns 'Account Type', 'Address', and 'Title'.

Account Type	Address	Title
Windows Member	test	Test

At the bottom, there are three buttons: 'Save' (in green), 'Send Test Email', and 'Cancel'.

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



The screenshot shows the 'Admin' section of the Securden Privileged Account Manager. The breadcrumb trail is 'Admin > Configure SMTP Server Settings'. The page contains several configuration fields: a port field set to '25', a 'Sender Email Address for Notifications*' field with the value 'jakecso@gmail.com', a checked checkbox for 'Supply Credentials (if authentication required)', and two radio buttons for authentication: 'Enter username and password' (unselected) and 'Specify an account already stored in Securden' (selected). Below these are three dropdown menus: 'Account Type' (set to 'Azure AD'), 'Address' (set to '192.168.72.2'), and 'Title' (set to 'Email login'). At the bottom are three buttons: 'Save' (highlighted in green), 'Send Test Email', and 'Cancel'.

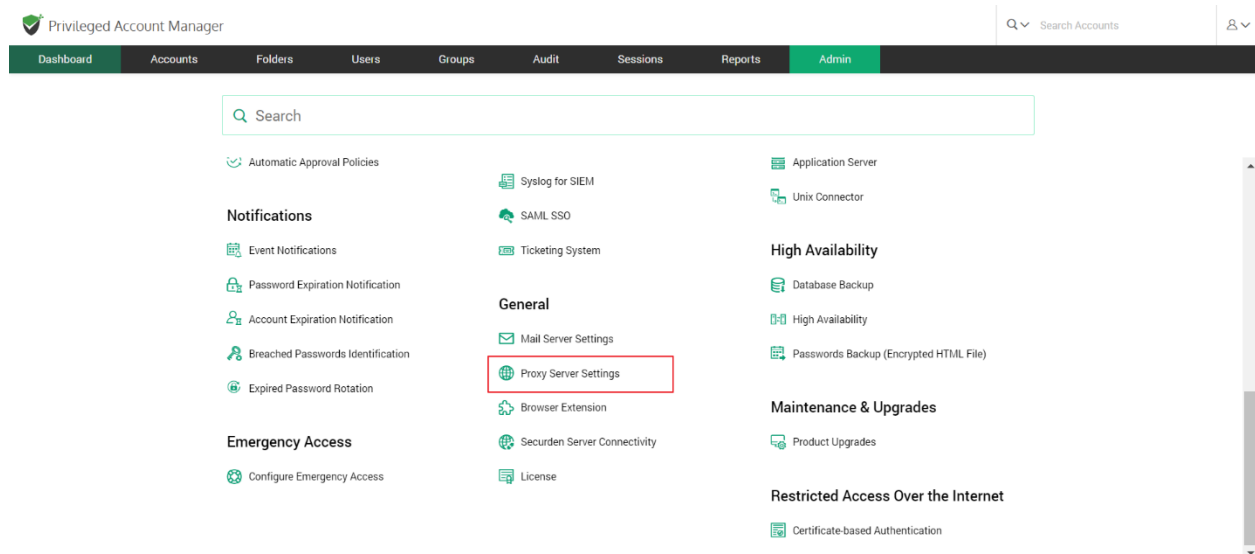
After providing the required details and authentication credentials, click **Save**.

You can also test and validate the configuration setting by sending a test email.

Proxy Server Settings

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

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



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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Proxy Server Settings

Configure Proxy Server

If your organization makes use of a proxy server to regulate internet traffic, configure the proxy server details here to facilitate Securden to connect to the internet. If you have application servers in multiple regions, you can add the proxy servers of each region here and associate them with their respective application servers under Admin >> Remote Distributors >> Application Server.

Enable Proxy ☒

Search Add Proxy Server Set as Default

Showing 0 to 0 of 0 25

Proxy Server Name	Hostname / IP Address	Port	Actions
No data found			

Showing 0 to 0 of 0 25

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Proxy Server Settings > Add Proxy Server

Add Proxy Server

Proxy Server Name*
InternetProxy1

Hostname or IP Address*
192

Port*
2

Proxy Protocol*
HTTP

☒ Supply Credentials (if authentication required)

☐ Enter username and password ☒ Specify an account already stored in Securden

Account Type Address Title
Azure AD Search Account Address Search Account Title

Save Test Internet Connection Cancel

Note: If the proxy server requires authentication, you need to enter the credentials to enable Securden to connect to the proxy server. Click the

checkbox **Supply Credentials**. You can either select an account added in Securden or enter username and password to authenticate.

If you want to choose an account stored in Securden, you can do so by searching for the **Account type**, **Address**, and **Title** in Securden.

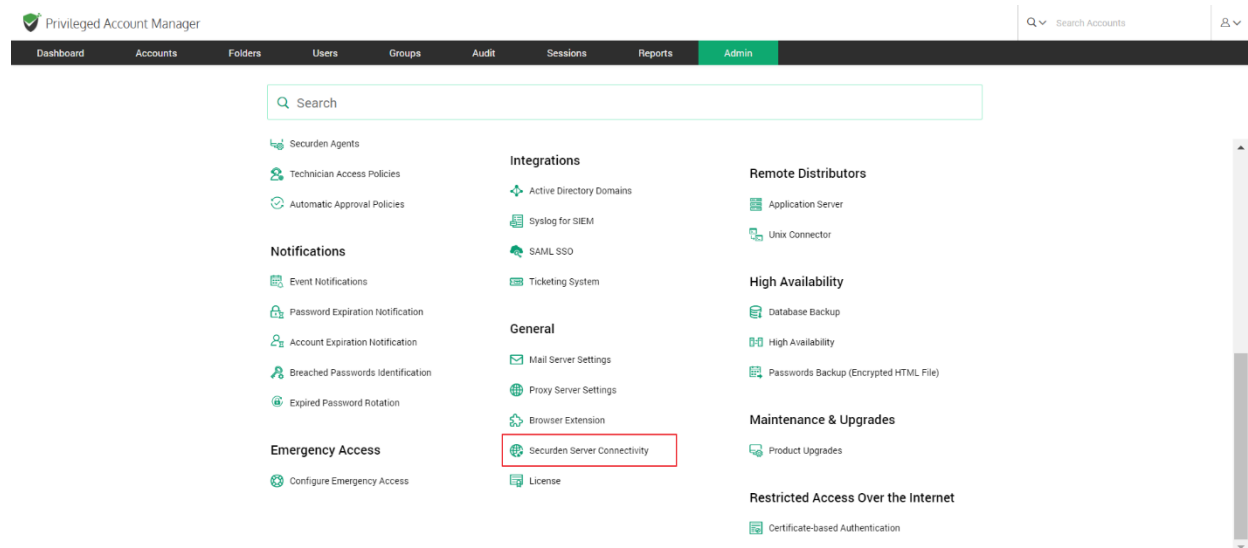
Save the settings and then run a test to verify the internet connection.

Securden Server Connectivity

This setting is to specify how to connect to the Securden web interface from client machines and the name with which the client machines identify the Securden server host.

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

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



In the GUI that opens, enter the following details.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Securden Server Connectivity

Securden Server Connectivity

This setting is to specify how to connect to Securden web interface from client machines and the name with which the client machines identify the Securden server host while deploying agents.

URL to access Securden server: You can specify below the exact details of the host in which Securden server is running to enable client machines to establish a connection with the server. In case, you have configured an alias, you may specify the same.

Web-based RDP Connections: This is to launch Web-based remote RDP connections from Securden. Specify the RDP server's gateway URL.

Web-based SSH Connections: This is to launch Web-based remote SSH connections from Securden. Specify the SSH server's gateway URL.

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

URL to access Securden server*
https://W10PFZYASOP5959

Web-based RDP Connections*
https://W10PFZYASOP5626

Web-based SSH Connections*
https://W10PFZYASOP5622

Server Machine Address*
W10PFZYASOP

Save Cancel

URL to access Securden server

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

Securden server uses port **5959** by default. If you wish to change the Server port, follow the steps below.

To change server port:

1. Navigate to the Securden installation folder/conf directory and open the 'server.properties' file with Wordpad or notepad++.
2. Look for the entry "SERVER_PORT" and enter the required port number.

3. Restart Securden PAM Service alone (DO NOT restart 'Web Service – Securden PAM').

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

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

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

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

Troubleshooting tip

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

Web-based RDP Connections

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

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

To change RDP Server Gateway Port:

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

Web-based SSH Connections

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

To change SSH Server Gateway Port Number,

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

Server Machine Address

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

Replace Self-signed Certificate

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

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

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

You can download OpenSSL from

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

2. Copy your certificate (e.g., certificate.pfx) and paste it in the system from where you can execute OpenSSL exe.

The *.pfx file is in PKCS#12 format and includes both the certificate and the private key.

3. Run the following commands to export the private key.

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

4. Run the following command to export the certificate.

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

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

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

6. In services.msc, restart Securden PAM Service.

Troubleshooting tips:

- In some cases, the PEM file does not contain the private key, and this brings up the error - **Expecting: ANY PRIVATE KEY**. Ensure that you have the key along with the certificate.
- Ensure that the .pfx file is in PKCS#12, as this format holds both the certificate and key in it. Hence, we recommend the certificate be exported in PKCS#12 format to extract the certificate and key separately.

Section 3: User Management

User Management

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

Onboard Your Users

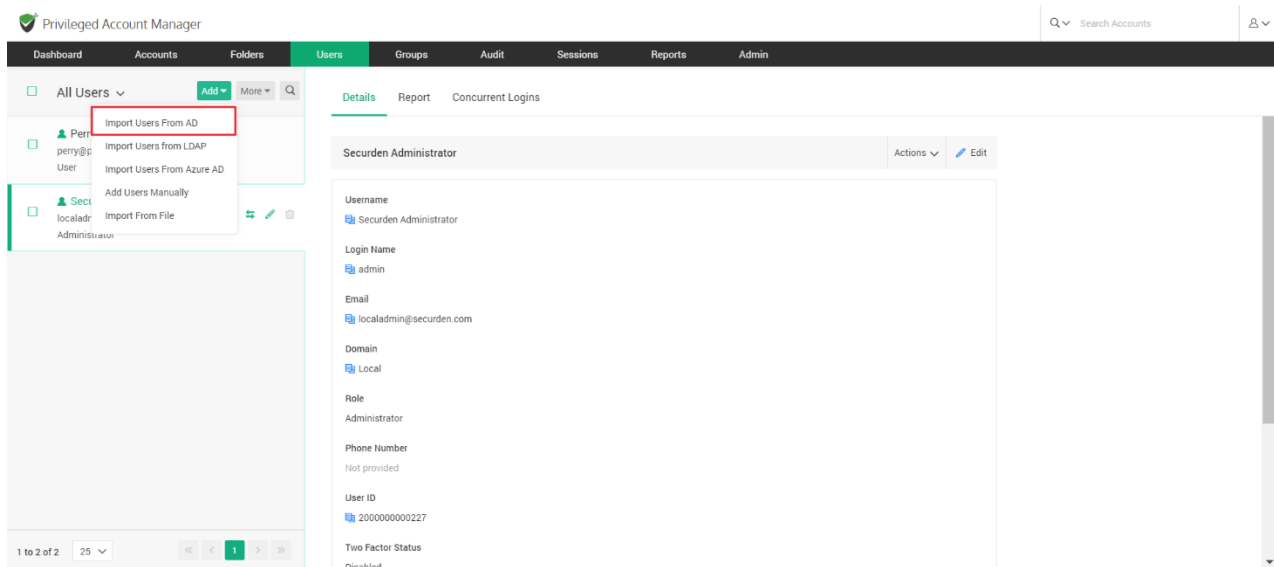
You need to create accounts for your team members to enable them to use Securden. There are multiple options to do this. The options are:

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

Import Users from Active Directory

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

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



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

Step 1: Establish Connectivity

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

Privileged Account Manager

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

Import Users from AD

Step 1: Establish Connectivity

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

Domain IP Address / FQDN *
192.168.72.2

Secondary IP Addresses (Optional)

Select Remote Gateway
--None--

Connection Mode
☐ SSL

Help

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

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

Connection Mode
Specify the mode (SSL/non-SSL) through which Securden has to establish connection with the AD domain. If SSL mode is selected, the domain controller should be serving over SSL in port 636 and the certificate of the domain controller should have been signed by a CA. If the certificate of the domain controller is not signed by a certified CA, you need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the domain controller and all the intermediate certificates if any. For details, [click here](#).

Supply Administrator Credentials
You need to supply administrator credentials so as to enable Securden to scan the members in the domain. You may enter the username and password manually once and this will be

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

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

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

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

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

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

Supply Administrator Credentials: You need to supply administrator credentials to enable Securden to scan the members in the domain. You may

enter the username and password manually once and this will be stored in Securden for use during subsequent import attempts.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

Secondary IP Addresses (Optional)

Select Remote Gateway
-None-

Connection Mode

☐ SSL

Supply Administrator Credentials

Username
|

Password

Next Cancel

Specify the mode (SSL/non-SSL) through which Securden has to establish connection with the AD domain. If SSL mode is selected, the domain controller should be serving over SSL in port 636 and the certificate of the domain controller should have been signed by a CA. If the certificate of the domain controller is not signed by a certified CA, you need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the domain controller and all the intermediate certificates if any. For details, [click here](#)

Supply Administrator Credentials

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

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

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

Import Users from AD

Step 2: Discover and Import

Securden fetches users and user groups from the AD domain specified. When you import user groups, Securden will maintain the same group structure here too. You have three options here and you can exercise any or a combination of the three options below as required in a single step.

Domain Name : **SECURDEN.AWS.COM** Domain IP : **172.31.1.11**

OUs Groups Users

Fetch all users who are part of the selected OU/OUs. Enter your search text. Then click the 'Discover' button.

Search OUs **Discover** **Browse OU Tree and Select**

Verify the Objects Selected for Discovery

Verify your search results before proceeding to importing them to Securden.

Help

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

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

For example, if you want to fetch users from an OU and a Group, first enter/browse and select the name of the OU, click 'Discover'. Then go to the 'Groups' tab, select/browse the name of the Group, click 'Discover'. Verify your discovery details and finally click 'Import'. Securden will fetch all users that are part of the OU and Group specified.

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

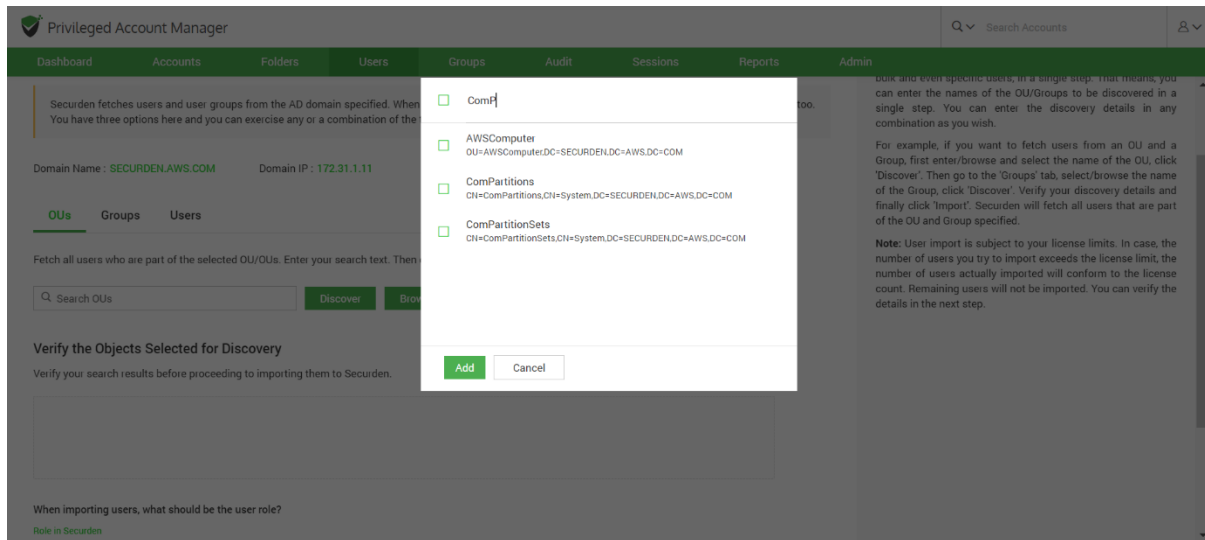
Step 2: Select Users to Import

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

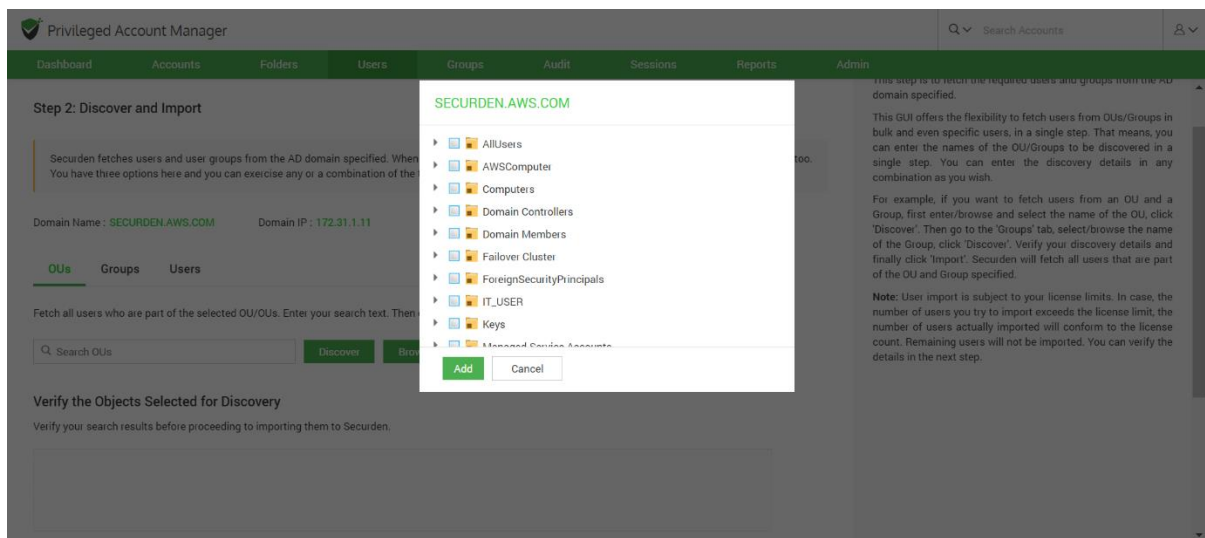
This GUI offers the flexibility to fetch users from OUs/Groups in bulk and even specific users, in a single step. That means you can enter the names of the OU/Groups to be discovered in a single step. You can enter the discovery details in any combinations (OUs, Groups, Users) as you wish.

To import OUs, select the OU tab.

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



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



- You can then verify your selection in the **Verify the Objects Selected for Discovery**.

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

To import Groups, select the Groups tab.

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

To import Users, select the Users tab.

1. Enter the user name and select **Discover**.
2. You can then verify your selection in the **Verify the Objects Selected for Discovery**.

3. You can then select the role for the individual users imported using the **Role in Securden** drop down. This is set to the **User** role by default.
4. Before selecting the import button, you can look into the additional settings which are explained below.
5. Select **Import**.

Advanced Settings:

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

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

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

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

Troubleshooting tips:

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

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

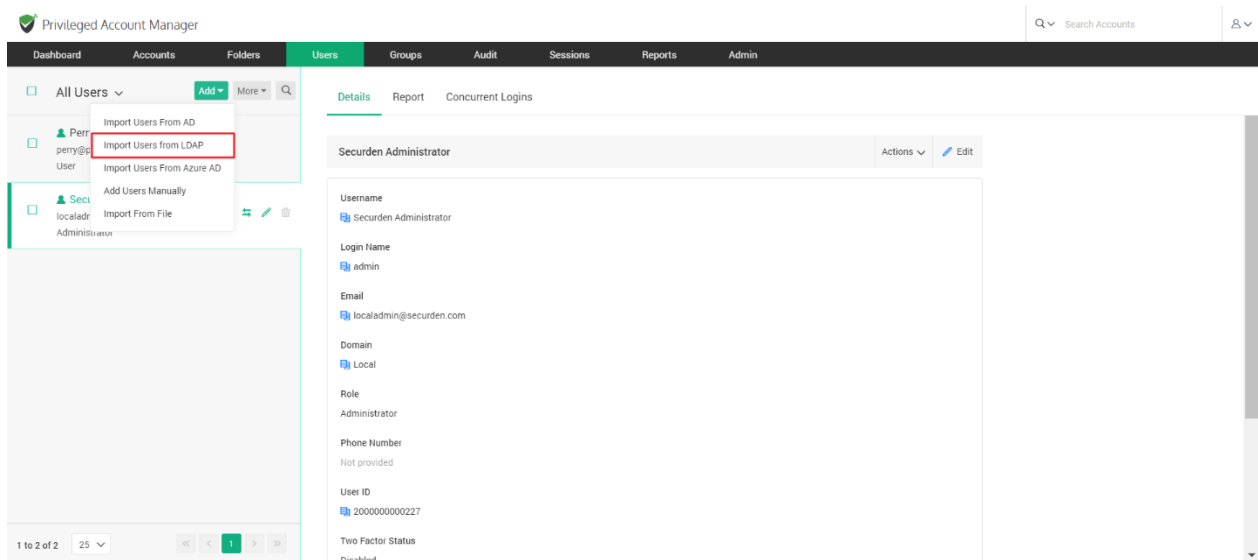
Navigate to **Accounts >> Discover Accounts >> Windows**. Click **Modify >>** Enter username and password.

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

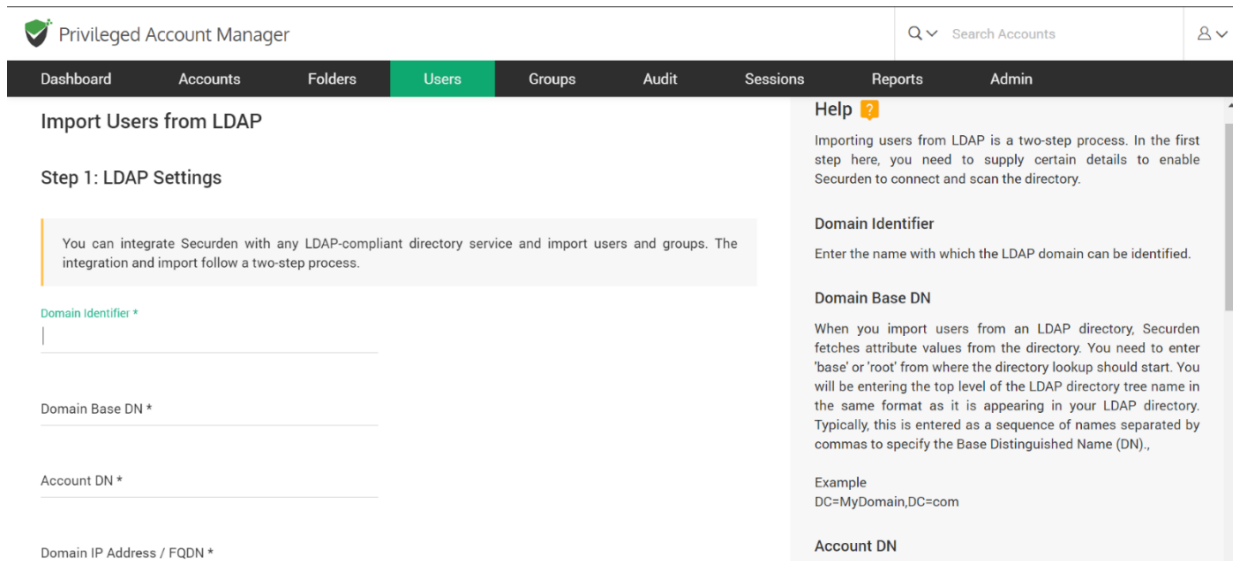
Import Users from LDAP

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

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



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



Privileged Account Manager

Search Accounts

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

Import Users from LDAP

Step 1: LDAP Settings

You can integrate Securden with any LDAP-compliant directory service and import users and groups. The integration and import follow a two-step process.

Domain Identifier *

Domain Base DN *

Account DN *

Domain IP Address / FQDN *

Help

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

Domain Identifier

Enter the name with which the LDAP domain can be identified.

Domain Base DN

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

Example

DC=MyDomain,DC=com

Account DN

Step 1: LDAP Settings

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

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

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

Example

DC=MyDomain,DC=com

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

Example

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

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

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

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

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

Step 2: Discover and Import from LDAP

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

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

Import Users from LDAP

Step 2: Discover and Import from LDAP

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

Domain Name : ldap Domain IP : 172.31.1.11

Base DN *

DC=SECURDEN,DC=AWS,DC=COM

Search Filter *

LDAP Scope

Base

Help

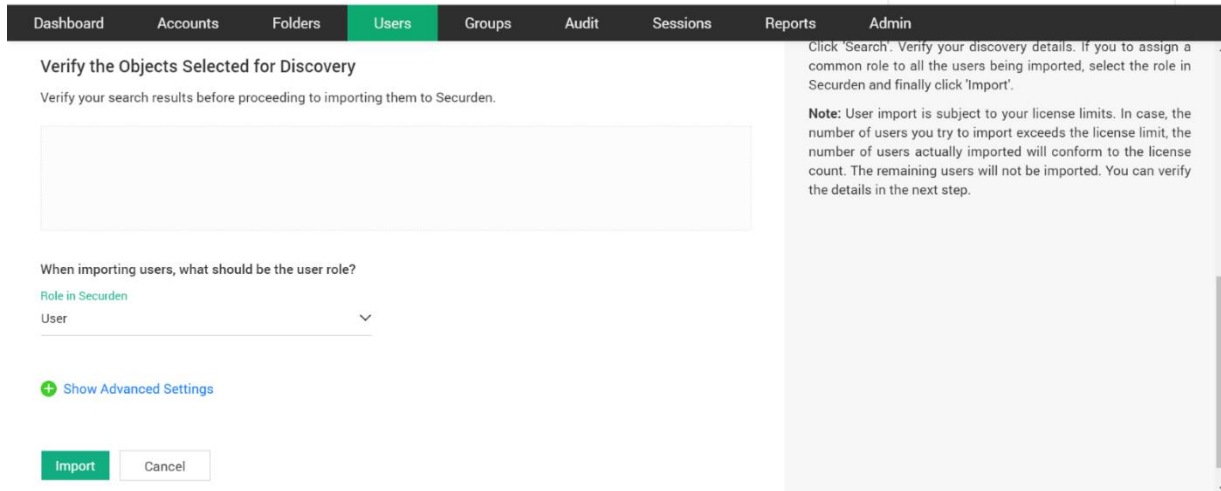
This step is to fetch the required users and groups from the LDAP domain specified.

This GUI offers the flexibility to fetch only the required users from the LDAP domain. Typically, the search happens by combining the Base DN, which is the base of the search tree for all users, the specific level under the Base DN (the LDAP Scope), and the Search filter that gets granular to fetch only the required users. In the search filter, you can specify a Object Class, which defines the types of results that Securden will fetch. If the Base DN contains a mix of object types like people, groups, assets, and so on, you may specify only the required set of objects here. You may use (objectClass=*) to include all objects.

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

If you want to restrict your search within a specific level under

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



- **Base DN** - Typically, the search happens by combining the **Base DN**, which is the base of the search tree for all users, the specific level under the Base DN (the **LDAP Scope**), and the **Search Filter** that gets granular to fetch only the required users.
- **Search filter** - In the search filter, you can specify an Object Class, which defines the types of results that Securden will fetch. If the Base DN contains a mix of object types like people, groups, assets, and so on, you may specify only the required set of objects here. You may use (objectClass=*) to include all objects.
- If you want to add only specific users from your LDAP directory, just perform a search using the appropriate search filter. For example, if you want to import only the users from the OU Sysadmin and O Securden, the Base DN has to be ou=Sysadmin,o=securden,c=com, and the search filter has to be written within brackets as: (objectClass=user)

- If you want to restrict your search to a specific level under the BaseDN, you may select the required scope from the drop-down.
- Click **Search**. Verify your discovery details under **Verify the Objects Selected for Discovery**. If you want to assign a common role to all the users being imported, select the role in Securden and finally click **Import**.

Advanced Settings:

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

Import from Azure AD

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

The screenshot displays the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. The 'Users' section is active, showing a list of users on the left and a detailed view of the 'Administrator' user on the right. A dropdown menu is open under the 'Add' button in the 'All Users' section, with 'Import Users From Azure AD' highlighted. The detailed view for the 'Administrator' user shows fields for Username, Login Name, Email, Domain, Distinguished Name, Role, and Phone Number. A 'Sync User' button is visible in the top right of the detailed view.

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

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

Step 1: Establish Connectivity

Privileged Account Manager

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

Import Users from Azure AD

Step 1: Establish Connectivity

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

Tenant ID*

Client ID*

Client secret*

Next **Cancel**

Help

Importing users from Azure AD is a two step process. In the first step, you need to supply certain connectivity details to enable Securden to scan the members in the domain. This step requires integration with Azure AD and some configuration steps. For details, [refer to this document](#).

Tenant ID
Directory ID (Your organization's ID with Azure AD)

Client ID
Application ID (Client ID of the application)

Client secret
Secret Key Created for Securden

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

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

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

Client ID: Enter the Client ID of the application.

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

Step 2: Import Users

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

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

To import OUs, select the OU tab.

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

To import Groups, select the Groups tab.

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

To import Users, select the Users tab.

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

Advanced Settings:

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

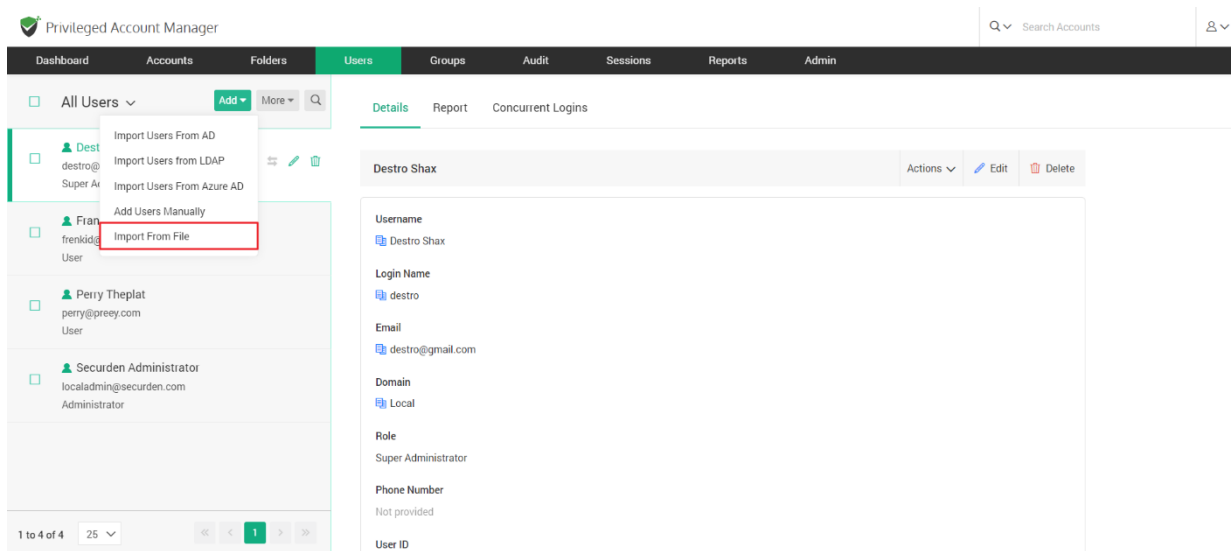
Note: User import is subject to your license limits. In case, the number of users you try to import exceeds the license limit, the number of users actually imported will conform to the license count. The remaining users will not be imported. You can verify the details in the next step.

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

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

Import Users from File

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



File Format

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

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

Steps to import CSV file:

Privileged Account Manager

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

Your license allows a maximum of 250 users. You can add 188 more.

Import Users From File

☒ CSV
 ☐ XLSX

Specify how each entry in your CSV has been separated

Delimiter
 Comma Separated values

Role in Securden
 User

Password
 Use username as password

Choose a file

1. In the GUI that opens, click the **CSV** option.
2. Select the **Delimiter**. This can either be Comma/Tab/Colon/Semi-Colon separated.
3. You can then select the role of the user in **Role in Securden**.
4. You then have the option to choose between **Email Password Creation** and **Use username as password** under **Password**.
5. Browse and select the file.
6. Click **Next**. In the second step of the import, we provide the option to map the columns in the input file and that of attributes in Securden.

Steps to import XLSX file:

Privileged Account Manager

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

Your license allows a maximum of 250 users. You can add 188 more.

Import Users From File

CSV XLSX

Role in Securden
User

Password
Use username as password

sample.xlsx Browse

Next Cancel

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

Mapping

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

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

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

Privileged Account Manager Q Search Accounts Person Icon

Dashboard **Accounts** **Folders** **Users** **Groups** **Audit** **Sessions** **Reports** **Admin**

Columns in File

- First Name
- Last Name
- Username
- Password
- URL
- Type
- Hostname
- Grouping
- Extra

Map Columns

You need to specify below the mapping of columns in your CSV and that of Securden. For example, the first entry in your CSV/XLS could represent 'First Name' in Securden, the second entry might represent 'Last Name'. Just drag and drop the respective columns from left to right.

Mapping in Securden Reset

First Name *
Drag a field here

Last Name
Drag a field here

Username *
Drag a field here

Email *
Drag a field here

Phone Number

Include first row

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

Add Additional Fields

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

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

User import configurations

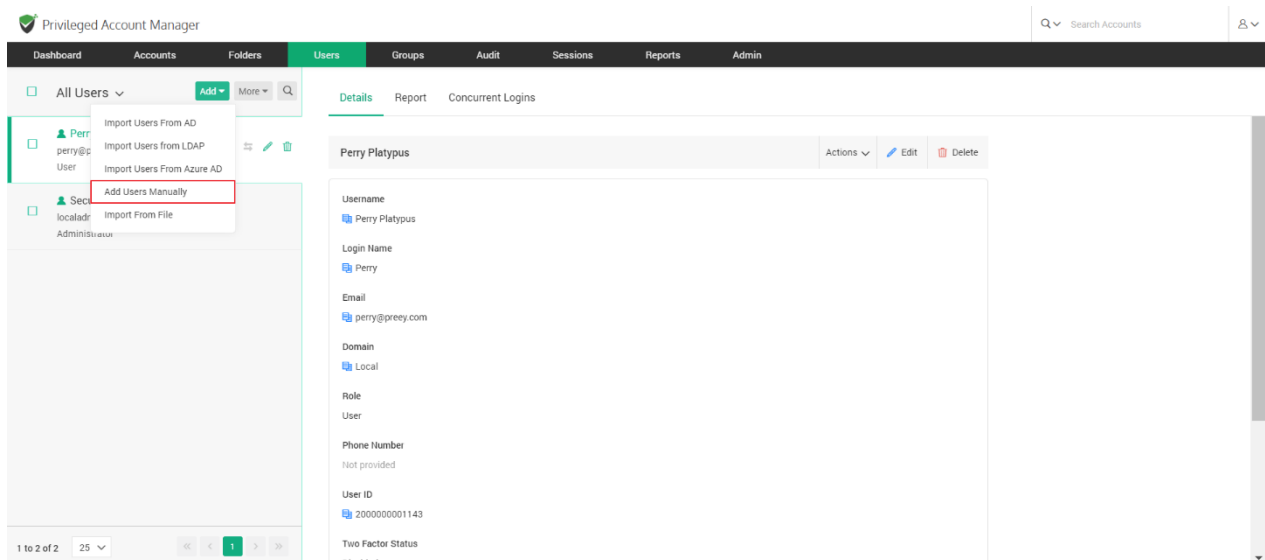
You have the option to modify the default role that is set while importing users from AD or from a file.

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

Add Users Manually

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

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



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

Privileged Account Manager

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

Search Accounts

Add User

First Name *
Peter

Last Name
Drury

Username *
Peter

Password
Use username as password

Email *
petedr@del.com

Role in Securden
User

Phone Number
732459103949

Location
|

Department

☐ User Specific 2FA Options

Save **Cancel**

Help

User Roles

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

Super Administrator - Can view all passwords stored in the application. Overall administration of the application, including user management.

Administrator - Can administer the application, including user management.

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.

Auditor - Can view the reports and audit trails generated in the application.

User Specific 2FA

On clicking 'User Specific 2FA Options', you will be able to configure 2FA for users individually. You have the option to keep 2FA 'On' or 'Off'. When kept 'On', you can select one or more 2FA methods to be enforced for an individual user. When

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

- **First Name** - Enter the user's first name in the respective field.
- **Last Name** - Enter the user's last name. This field is not mandatory.
- **Username** - Enter a unique username with which the user can log in to Securden.
- For the **password**, you may choose from two options:
- **Email Password Creation Link** – If you have selected this option and provided the email address of the user, they will receive an email allowing them to login to Securden PAM.
- **Use Username as Password** - The password will be the same as the username provided.

- **Email** - Enter the user's email address. Login credentials for Securden will be emailed to this address once the user account is created.
- **Role in Securden** – You can set the access level of each user by assigning them a specified user role. You can select from the five predefined user roles, Super Administrator, Administrator, Auditor, Account Manager, and User. You also have provision to create any number of custom user roles. The access level of default user roles are explained under the section **Default User Roles**. The **Custom User Roles section** explains in detail how user roles can be customized.
- **Phone number, Department, and Location** - These three fields are not mandatory, but you can add them to ensure precise user information for efficient management.
- **Enforce Two Factor Authentication** – You can choose to enable or disable two factor authentication for the added user.

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

Note: Once users login into PAM for the first time, they need to set a new password. This must be in compliance with the password policy enforced by the administrator and can be configured under **Admin >> Account Management >> Password Policy**.

Editing Users added in Securden

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

All Users ▾ Add ▾ More ▾

Frankel Lampard
frenkid@gmail.com
User

Perry Theplat
perry@prey.com
User

Securden Administrator
localadmin@securden.com
Administrator

1 to 3 of 3 25 ▾

Details Report Concurrent Logins

Frankel Lampard Actions ▾ Edit Delete

Username
Frankel Lampard

Login Name
Frank

Email
frenkid@gmail.com

Domain
Local

Role
User

Phone Number
Not provided

User ID

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

All Users ▾ Add ▾ More ▾

Administrator
admin_1@securden.com
User

Anish Krishnan Sridhar
anish@securden.com
Administrator

Bala Bala
bala@securden.com
User

Bala Govindarajan Kasthuri Rajan
balagovindarajan@securden.com
User

Balasubramanian Venkatramani

1 to 57 of 57 100 ▾

Edit User

First Name
Administrator

Email *
admin_1@securden.com

Role in Securden
User ▾ Phone Number

Department Location

Enforce Two Factor Authentication ☐ On ☒ Off

Access to Securden GUI ⓘ ☒ Allow ☐ Deny

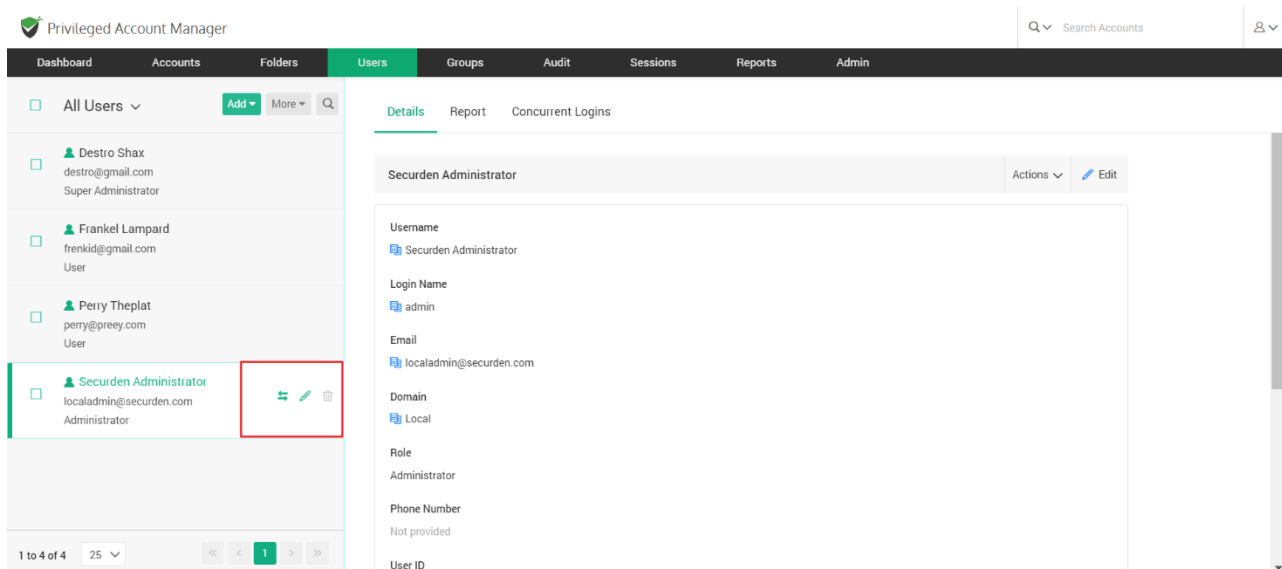
You also have these options:

- **Enforce Two Factor Authentication:** You can turn off 2FA for specific users by turning 2FA off.

- **Access to Securden GUI:** You can allow/deny users from accessing the Securden GUI from here.

Quick Access Options – Users

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

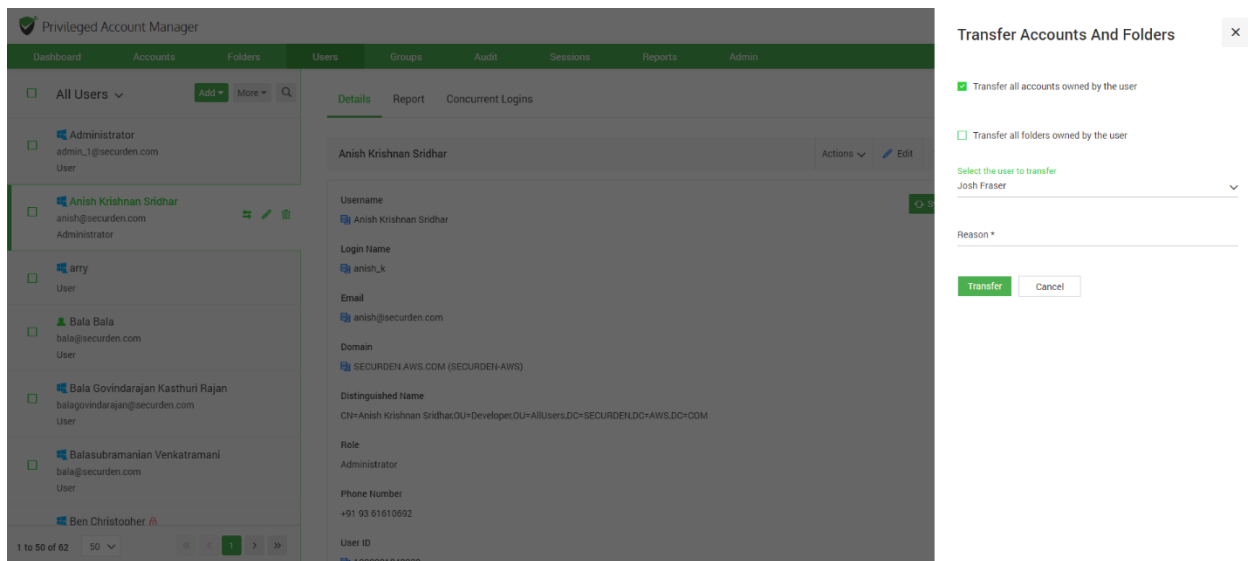


Transfer Ownership

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

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

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



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

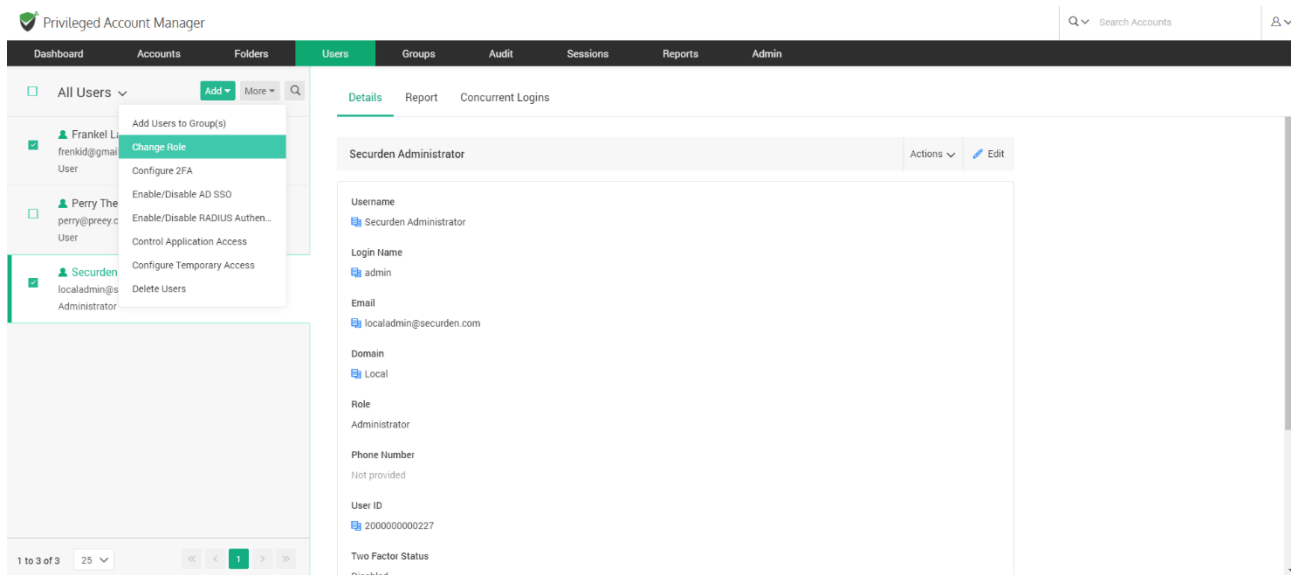
Assigning Roles to Users

By default, users added or imported will have the role **User** in Securden. This can be changed while importing/adding them, or after you have added them. Each Role has certain privileges associated with them, that let the user carry out certain operations within the PAM solution. You have the option to create

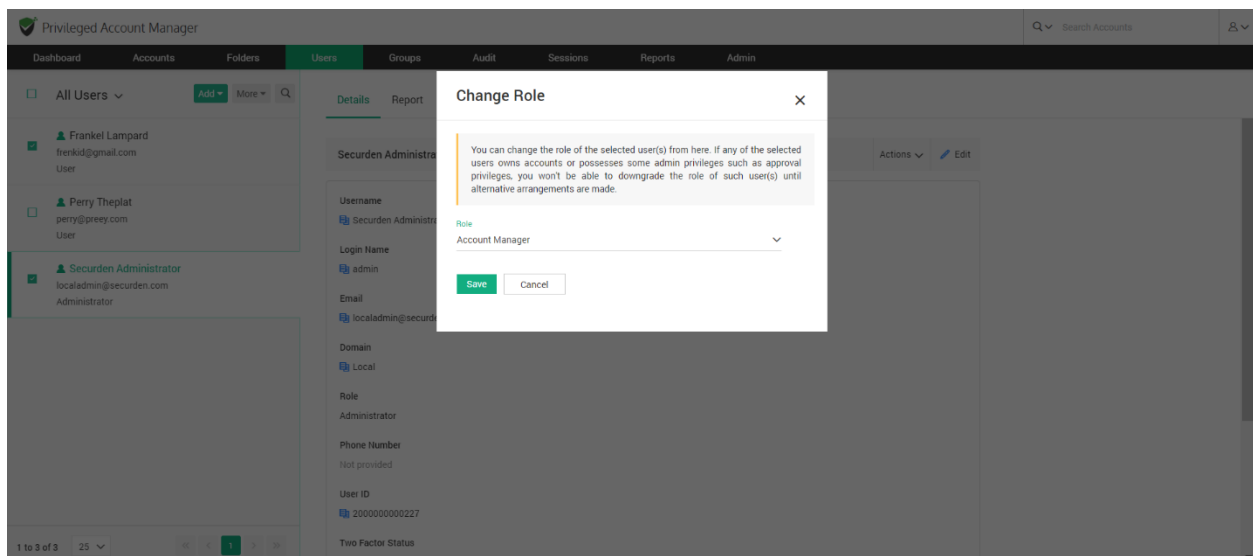
custom user roles outside the default roles available. These settings are further explained under **Default User Roles** and **Custom User Roles**.

To change the role assigned to multiple users,

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



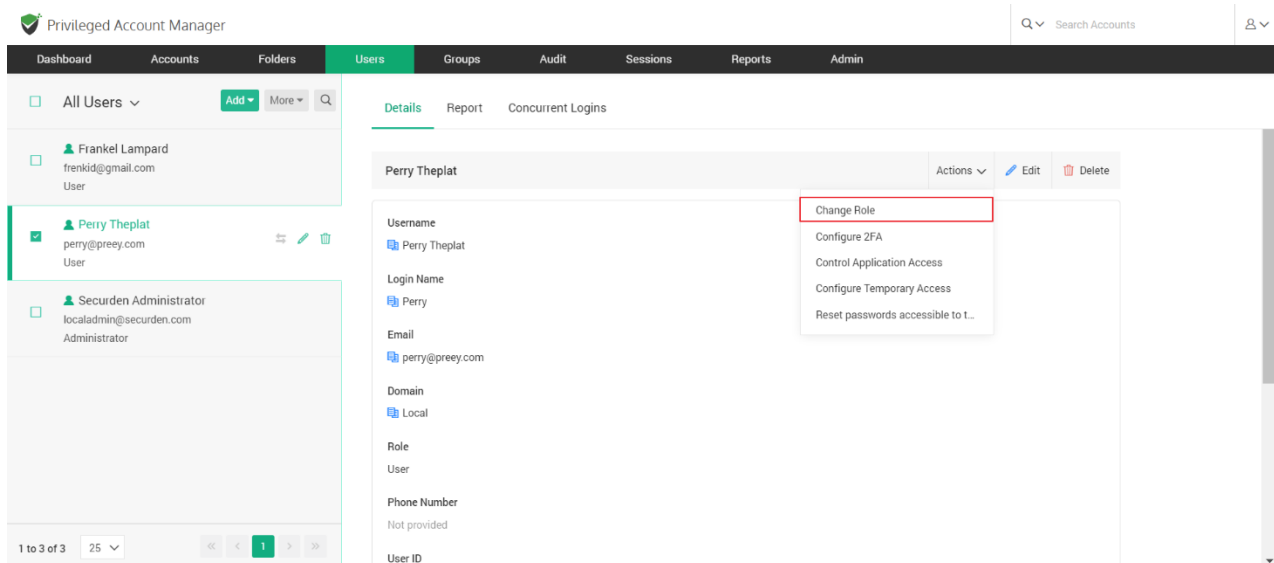
Once you've selected the users, click **More >> Change Role**.



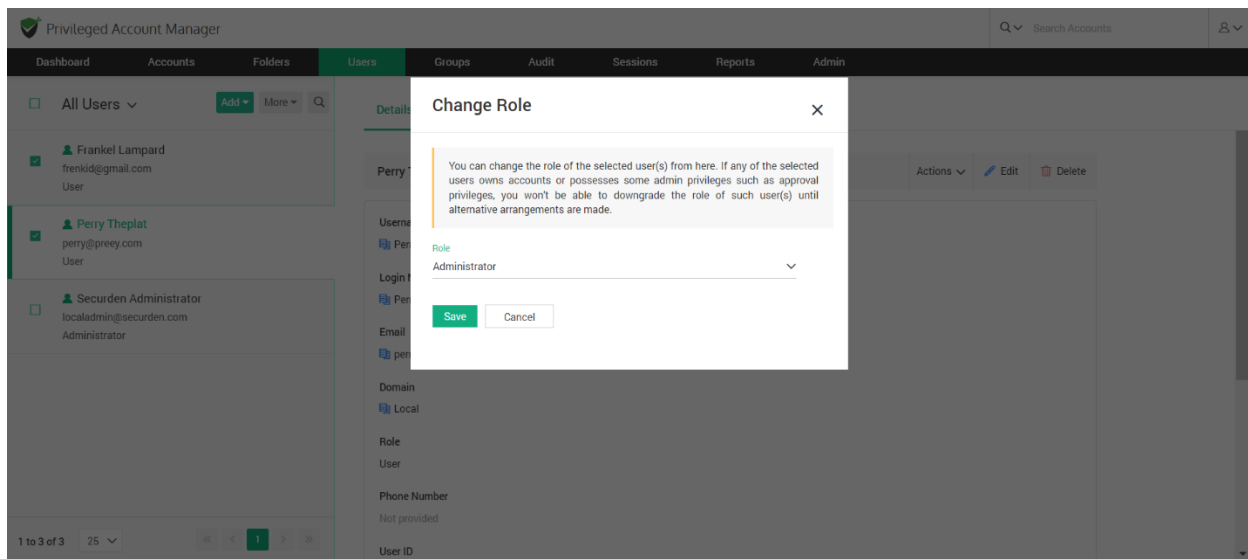
You can select the required role from the dropdown and **Save** changes.

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

To change the role assigned to an individual user, navigate to the **Users** section in the GUI and select the required user. Select **Change Role** under the **Actions** drop-down.



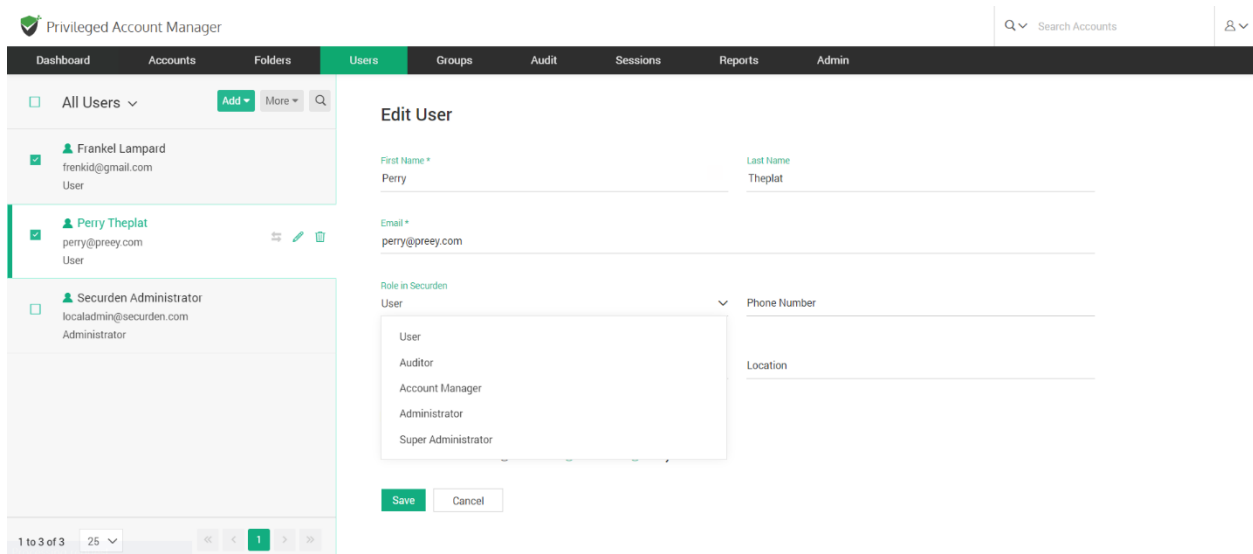
In the popup that opens, you can select the **Role** from the list of available ones in the drop-down.



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

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

To change the role of a user, you can also **Edit** the user attributes, and pick the required role.



Default User Roles

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

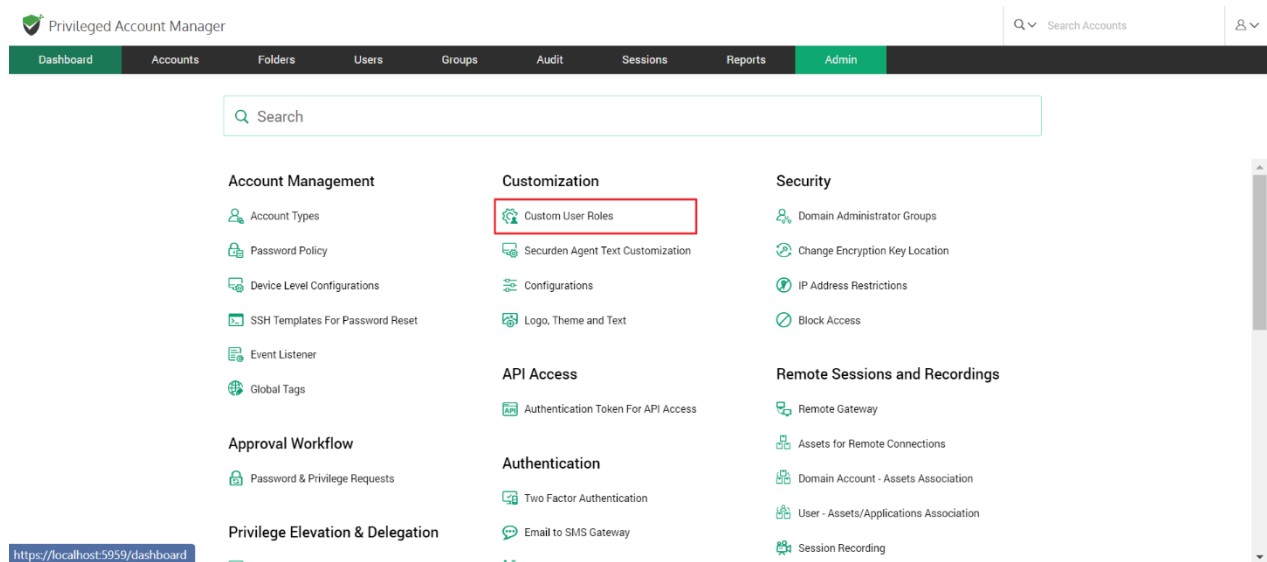
- **Super Administrator** - This is like an emergency/break-glass account which allows viewing all the work-related passwords stored in the application. They can also view the overall administration of the application, including user management.
- **Administrator** - They can administer the application, including user management. Unlike super administrators, administrators can see only the passwords that are owned by them and the ones that are shared with them.
- **Account Manager** - They can add accounts to the application. They can also perform all administrative tasks related to the accounts.
- **User** - They can view the accounts shared by administrators. They can manually add accounts and share them with others. (They do not have the privilege to import accounts). If needed, you can disable account addition privilege for users.

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

Custom User Roles

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

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



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

The screenshot shows the 'Privileged Account Manager' interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin' (which is highlighted). Below the navigation bar, there is a breadcrumb trail: 'Admin > Custom User Roles'. The main heading is 'Custom User Roles'. A descriptive text block states: 'You can create custom user roles assigning specific access permissions to users based on the specific needs of your organization. You can assign features at granular level selecting specific features. After creating a role, if the permissions are to be modified, the changes will have to be approved by another administrator.' Below this text, there are three buttons: 'Create Custom Role' (highlighted with a red box), 'Delete Roles', and a search icon. To the right, it says 'Showing 1 to 5 of 5' and '25'. A table lists five roles: 'Account Manager', 'Administrator', 'Auditor', 'Super Administrator', and 'User'. Each row includes a checkbox, the role name, a description, a status (all are 'Active'), and action icons (edit and delete). At the bottom, it says 'Showing 1 to 5 of 5' and '25' again, with pagination controls.

Role Name	Description	Status	Actions
<input type="checkbox"/> Account Manager	All account management features	✓ Active	
<input type="checkbox"/> Administrator	All features accessible	✓ Active	
<input type="checkbox"/> Auditor	General access and auditing features	✓ Active	
<input type="checkbox"/> Super Administrator	All features enabled	✓ Active	
<input type="checkbox"/> User	General access	✓ Active	

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

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Custom User Roles > Create a Custom Role

Create a Custom Role

You can create custom user roles from here. You need to select the privileges required for the role from the list below.

Role Name*
Report Generator

Role Description
To generate report

Features

☐ Select All Features

☐ Account Management

<input checked="" type="checkbox"/> View Account Details	<input type="checkbox"/> Add Account	<input type="checkbox"/> Edit Account	<input type="checkbox"/> Import Work Accounts	<input type="checkbox"/> Discover Accounts	<input type="checkbox"/> Delete Accounts
<input type="checkbox"/> Share Accounts	<input type="checkbox"/> Clone Account	<input type="checkbox"/> Transfer Accounts	<input type="checkbox"/> Accounts Color Coding	<input type="checkbox"/> View Password History	<input type="checkbox"/> Accounts Reports
<input type="checkbox"/> Offline Access	<input type="checkbox"/> Export Accounts	<input type="checkbox"/> Associate Private Keys	<input type="checkbox"/> Bulk Password Policy Change	<input type="checkbox"/> Bulk Folder Change	<input type="checkbox"/> Configure Approval Workflow
<input type="checkbox"/> Account Dependencies	<input type="checkbox"/> Add Folder from Folder Tree	<input type="checkbox"/> Account Settings	<input type="checkbox"/> Manage Personal Passwords	<input type="checkbox"/> Import Personal Accounts	<input type="checkbox"/> Configure Autofill URLs
<input type="checkbox"/> Configure TOTP	<input type="checkbox"/> Share with Third Parties	<input type="checkbox"/> Add Tags in Bulk	<input type="checkbox"/> Import Accounts from KeePass	<input type="checkbox"/> Import Accounts from LastPass	<input type="checkbox"/> Copy Account Details

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

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

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

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Custom User Roles

Custom User Roles

You can create custom user roles assigning specific access permissions to users based on the specific needs of your organization. You can assign features at granular level selecting specific features. After creating a role, if the permissions are to be modified, the changes will have to be approved by another administrator.

Q **Create Custom Role** Delete Roles Showing 1 to 6 of 6 25

Role Name	Description	Status	Actions
Account Manager	All account management features	Active	
Administrator	All features accessible	Active	
Auditor	General access and auditing features	Active	
Reporter		Approve/Reject	
Super Administrator	All features enabled	Active	
User	General access	Active	

Showing 1 to 6 of 6 25

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Custom User Roles > Approve/Reject User Roles

Role Name
Reporter

Role Description

Features

You can specify the operations for which the token generated here would be applicable. In other words, the API, with this token, cannot be used for operations other than the ones selected below.

Account Management

View Account Details

Reports

Standard Reports Concise Reports Password Analysis Report Export Reports Dashboard Reports

Approve Reject & Delete Cancel

List of privilege operations for custom user roles

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

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

	assets, including servers, databases, and other devices.
Delete Accounts	Users with this privilege can delete accounts owned by them/shared with them.
Share Accounts	Users with this privilege will be able to share the accounts they own with other users with granular access permissions.
Clone Account	Users with this privilege will be able to make a copy of the selected accounts with all the account details duplicated. Cloned accounts will carry the suffix 'copy'.
Transfer Accounts	Users with this privilege will be able to transfer ownership of the accounts they own to other users added in Securden.
Accounts Color Coding	Users with this privilege will be able to change the background display color for all accounts to which they have modify access permission.
View Password History	Users with this privilege will be able to view all the previous passwords assigned to accounts to which they have 'View' permissions.
Accounts Reports	Users with this privilege can view individual account reports for accounts present in Securden.
Offline Access	Users with this privilege will be able to make offline copies of the accounts they have access to. The offline copy will be protected with a passphrase chosen by the user.

Export Accounts	Users with this privilege will be able to export all the accounts they have access to in a CSV or XLSX file.
Associate Private Keys	Users with this privilege will be able to associate private keys (SSH) with the accounts to which they have 'Modify' access permissions.
Bulk Password Policy Change	Users with this privilege will be able to carry out password policy changes for multiple accounts at the same time. The user should have "Modify" access permissions to all the selected accounts in addition to this ability to be able to carry out bulk password policy change.
Bulk Folder Change	Users with this privilege will be able to carry out a folder change for multiple accounts at the same time. The User should have "Modify" access permissions to all the selected accounts and the destination folder in addition to this ability to be able to carry out folder change.
Configure Approval Workflow	Users with this privilege will be able to configure approvers for request release workflows. The user will need to have 'Manage' access permissions for the account involved to be able to configure approvers.
Account Dependencies	Users with this privilege will be able to fetch the dependencies of accounts they have access to.

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

Folder Management	
Add Folder	Users with this privilege will be able to add folders to Securden.
Edit Folder	Users with this privilege will be able to edit different attributes of folders to which they have access.
Import Folders	Users with this privilege will be able to import folders and their structure from files.
Delete Folder	Users with this privilege will be able to delete folders to which they have access to.
Transfer Folders	Users with this privilege will be able to transfer ownership of folders that they own (Along with the accounts it contains).
Share Folders	Users with this privilege will be able to share folders with other users with a granularity they choose.
Configure Remote Password Reset	Users with this privilege will be able to schedule remote password resets for all accounts in the folders they have access to.
Folder Reports	Users with this privilege will be able to view the reports section of folders they have access to.
Folder Settings	Users with this privilege will be able to view and change the preferences in the

	'Settings' section of the folders they can access.
Configure Approval Workflow	Users with this privilege will be able to designate approvers for accounts in a folder for request-release workflows.
Change Folder Inheritance in Bulk	Users with this privilege will be able to modify inheritance permissions preferences for multiple folders at the same time.
User Management	
Add User	Users with this privilege will be able to add other users to Securden.
Edit User	Users with this privilege will be able to edit attributes of existing users such as roles, permissions, etc.
Import Users from File	Users with this privilege will be able to import users into Securden from a CSV or an XLSX file.
Delete Users	Users with this privilege will be able to permanently delete existing users in Securden.
Import Users from AD	Users with this privilege will be able to import users from AD using existing Active Directory domain credentials.
Import Users from Azure AD	Users with this privilege will be able to import users from Azure AD using existing domain credentials.

Import Users from LDAP	Users with this privilege will be able to import users from LDAP using existing domain credentials.
Transfer Ownership	Users with this privilege will be able to transfer the ownership of all the accounts owned by them.
Concurrent Logins	Users with this privilege will be able see if any users have concurrently signed in to Securden on another device or browser, and will also be able to terminate any or all the logins, which will forcefully log out the user from Securden GUI.
User Reports	Users with this privilege can view and access all the user-related details under 'Report' section in the 'Users' tab.
Configure temporary Access	Users with this privilege will be able to grant temporary access to Securden web interface to selected user(s) by specifying access expiration time.
Change User role	Users with this privilege will be able to change the roles of other users.
Control Application Access	Users with this privilege can allow or deny access to other user(s) to access the Securden interface.
Change 2FA	Users with this privilege can alter the two-factor authentication login method used by the selected users(s) to access the Securden interface.
Change Radius Authentication in Bulk	Users with this privilege can alter RADIUS authentication for many users at once.

Reset passwords of accounts accessible to a user	Users with this privilege can reset the passwords of accounts that are owned/shared with them.
Add Users to Groups	Users with this privilege will be able to add other users to groups.
User Group Management	
Add User Group	Users with this privilege will be able to create new user group(s) in Securden.
Edit User Group	Users with this privilege will be able to edit user groups.
Delete User Group	Users with this privilege will be able to delete user groups. Deleting user groups does not delete the users in them.
User Group Reports	Users with this privilege will be able to view reports specific to user groups.
Import User Groups from AD	Users with this privilege will be able to import user groups from AD using existing domain credentials.
Import User Groups from Azure AD	Users with this privilege will be able to import user groups from Azure AD using existing domain credentials.
Import User Groups from LDAP	Users with this privilege will be able to import user groups from LDAP using existing domain credentials.
Change 2FA in Bulk	Users with this privilege will be able to change the 2FA method used by users in a user group to login to the Securden interface.

View Account Activity Trails	Users with this privilege will be able to view and access all the records of account-related activities.
View User Activity Trails	Users with this privilege will be able to view and access all the records of user-related activities.
Reports	
Standard Reports	Users with this privilege will be able to access all the standard reports, which include the following reports: Account access, Account Activity, Password Compliance, Password Expiry, User Access, User Activity, Dependencies, Processes and Software Inventory, Processes Inventory, Software Inventory, and Securden Agents on Computers.
Concise Reports	Users with this privilege will be able to view and access concise/micro reports pertaining to accounts and users. (Reports >> Concise Reports)
Password Analysis Report	Users with this privilege will be able to view the password security analysis report. This includes the Work Account Analysis report and Personal Accounts Analysis report.
Exported Report	Users with this privilege can view all the reports that were exported and downloaded by other users.

Dashboard Reports	Users with this privilege can view the detailed summary of all the users and accounts present on the dashboard.
Sessions	
Playback Recorded Sessions	Users with this privilege will be able to view and play back all the recorded sessions of other users.
Monitor Live Sessions	Users with this privilege can shadow and monitor ongoing sessions of other users. They can also terminate these sessions.
Admin Operations	
Manage Account Types	Account Types define the type of accounts being added under 'Work' and 'Personal' accounts in Securden. Users with this privilege will be able to add custom account types or edit and delete existing account types.
Manage Password Policies	Password policy in Securden helps you define the strength, complexity requirements, periodicity for password resets and other conditions. Users with this privilege will be able to add/delete a password policy and perform all actions related to it. (Under Admin >> Account Management > Password Policy)
Manage Event Listeners	You can trigger an action after the occurrence of any specific event or a

	sequence of events in Securden. For example, when the password of an account is changed, you can trigger a follow-up action automatically. This privilege lets the user add/delete and manage the listeners.
Device Level Configurations	A user with this privilege will be able to manage all device level configurations that includes managing remote credentials, session recording, remote gateway, and reports.
Manage SSH Templates	You can define customized templates to carry out remote password resets on devices that can be connected through SSH. Users given this privilege will be able to add, define, delete, and manage all actions related to SSH templates.
Approve Password Access Requests	Users with this privilege will be able to approve all the requests from other users to access certain passwords.
Technician Access Policies for Specific Users and Specific Computers	Users with this privilege can create policies authorizing specific technicians to perform administrative tasks on specific endpoints.
Technician Access Policies for all Users and all Computers	Users with this privilege can create policies authorizing all the users (technicians) to perform administrative tasks on all endpoints.
Delete Technician Access Policies	You can create policies authorizing specific technicians to perform administrative tasks on specific endpoints. Users with this privilege will

	be able to delete all the existing technician access policies.
Add Applications, Commands for Privilege Elevation	Users with this privilege will be able to add applications/commands for performing privilege elevation. (Elevating the privileges for applications (in Windows) and allowing users to run with specific commands with SUDO privileges in Linux.)
Configure Privilege Elevation Policies	Users with this privilege can define and manage control policies for seamless, on-demand elevation of applications for standard users (in Windows) and elevation of specific commands with SUDO privileges on Linux.
Remove Admin Rights	Users with this privilege will be able to remove admin rights of any number of users on any number of computers.
Manage Securden Agents	'Privilege Elevation and Delegation' operates when a Securden agent is installed at all endpoints. Users with this permission will be able to manage the agent across all the endpoints.
Manage Event Notifications	Securden can send email notifications upon the occurrence of certain events such as password retrieval, deletion, change in share permissions, and others. Users given this privilege will be able to configure the event notifications.
Manage Expiration Notifications	You can send email notifications a certain number of days prior to the expiration date of the passwords to serve as a

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

Manage Configuration Settings	You can customize the features of Securden in a granular manner. You can switch on and switch off certain features anytime as desired under the 'Configurations' section in the 'Admin' tab. Users with this privilege will be able to access it.
Customize Logo, Text	You can replace the Securden logo that appears in the login page and also the text that appears throughout the GUI as you wish. Users with this privilege will be able to customize it.
Change Product Language	Securden supports multiple languages, and you can carry out the desired language selection. Users with this privilege will be able to change the product language.
Access and Manage APIs	Securden provides APIs for querying the database programmatically, retrieving credentials, and performing various other tasks. Users with this privilege will be able to create authentication tokens for carrying out various operations using APIs.
Configure 2FA	You can enforce a second layer of authentication for your users to access their Securden account. Users with this privilege will be able to activate two-factor authentication.
Manage Email to SMS Gateway	As part of two-factor authentication, Securden integrates with Email to SMS gateway providers to send one-time

	passwords as SMS to the phone numbers of the users. This privilege lets users configure this feature.
Manage Duo Configuration	Securden integrates with Duo Security for two factor authentication. Once configured, users will be enforced to authenticate through Duo for accessing the web interface. Users given this privilege will be able to configure this feature.
Configure RADIUS Server Settings	You can integrate RADIUS server or any RADIUS-compliant two-factor authentication system like OneSpan Digipass, RSA SecurID, Swivel Secure etc. for the second factor authentication. Users given this privilege will be able to configure these settings.
Smart Card Authentication	If your organization uses smart cards for authenticating user logons, you can leverage the same for Securden authentication. Users given this privilege will be able to enable smart card authentication.
Manage SIEM Integration	You can periodically share privileged access data logs with SIEM solutions. Users given this privilege will be able to manage the Syslog configuration in Securden.
Manage SAML SSO Integration	Securden leverages SAML 2.0 to integrate with SAML-compatible federated identity management solutions like Okta, G Suite, Microsoft ADFS,

	OneLogin, PingIdentity, Azure AD SSO, and others for Single Sign On. Users given this privilege will be able to enable SAML SSO and configure it.
Manage Ticketing System Integration	Securden integrates with web-based ticketing systems. The integration helps trace specific activities like password retrieval in Securden to corresponding entries in the ticketing system. This privilege lets users activate and configure ticketing system integration in Securden.
Manage Mail Server Settings	Securden sends various email notifications to the users and to facilitate that, SMTP server details are to be configured. Users with this privilege will be able to configure the server settings.
Manage Proxy Server Settings	If your organization makes use of a proxy server to regulate internet traffic, you should configure the proxy server details in Securden to connect to the internet. Users who are given this ability will be able to configure the proxy server settings.
Manage Securden Server Connectivity Settings	Securden server connectivity specifies how client machines connect to the Securden web interface and the name with which client machines identify the Securden server host when deploying agents. Users who are given this privilege will be able to configure these settings.
Manage Securden License	Users with this privilege can apply for the Securden license key and get information

	about the existing license from the 'Admin' section. Users who are given this privilege will be able to view the available information about the existing license, and also can apply for a new license.
Manage Domain Administrator Groups	You can create a scheduled task to get notified if there is any modification in the domain administrator groups. Users with this privilege will get access to the Domain Administrator Groups and can also schedule the notifications.
Change Encryption Key Location	Every installation of Securden is protected with a unique encryption key. Securden doesn't allow the encryption key and the encrypted data to reside in the same location to ensure security. Hence, the key has to be moved outside the Securden installation folder. Users who are given this privilege will be able to change the location of the encryption key.
Manage Certificate-based Authentication	To meet the demands of remote work scenarios, you can enable all or select users of your organization to securely access the Securden web interface over the internet. This access requires configuring an additional security measure by way of certificate-based client authentication. This privilege lets users enable certificate-based authentication and configure it.

Manage IP-based Restrictions	You can control access to Securden server based on the IP addresses of users. Users with this privilege will be able to enable IP restrictions for other users.
Manage User Access to Securden	If required, you can block access to Securden server from the browser extensions, APIs, and mobile apps. Users who are given this privilege will be able to block access, which will take effect for all users, including the super admin globally.
Configure Remote Gateway	By default, all remote sessions launched from end user machines are tunneled through the Securden server, which acts as the gateway. There will not be any direct connectivity between the end user machines and the target device. For enhanced security, you may route all remote operations originating from Securden through a single, dedicated gateway (instead of Securden server acting as the gateway). Once configured, Securden will route all operations, including remote connections, session recording, and password resets through the gateway. Users who are given this privilege will be able to configure the remote gateway.
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. Users who are given this privilege will be able to enable session recording.
Use Advanced Session Recorder for Windows	To record the sessions on remote computers, you need to install Securden session recorder on the machines whose sessions are to be recorded. Users with this privilege will be able to deploy this advanced session recorder.
Deploy Application Servers	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. Users who are given this privilege will be able to deploy it.
Configure Unix Connectors	You can associate the UNIX connector with the required devices. Once you associate, all remote connections and remote operations (including session initiation, session recording, remote password resets, and password verification) to the devices associated will be initiated through the connector. Users with this privilege will be able to configure it.
Configure Database Backup	To ensure access to your data and passwords even in the unlikely scenario of something going wrong with the current installation, Securden offers

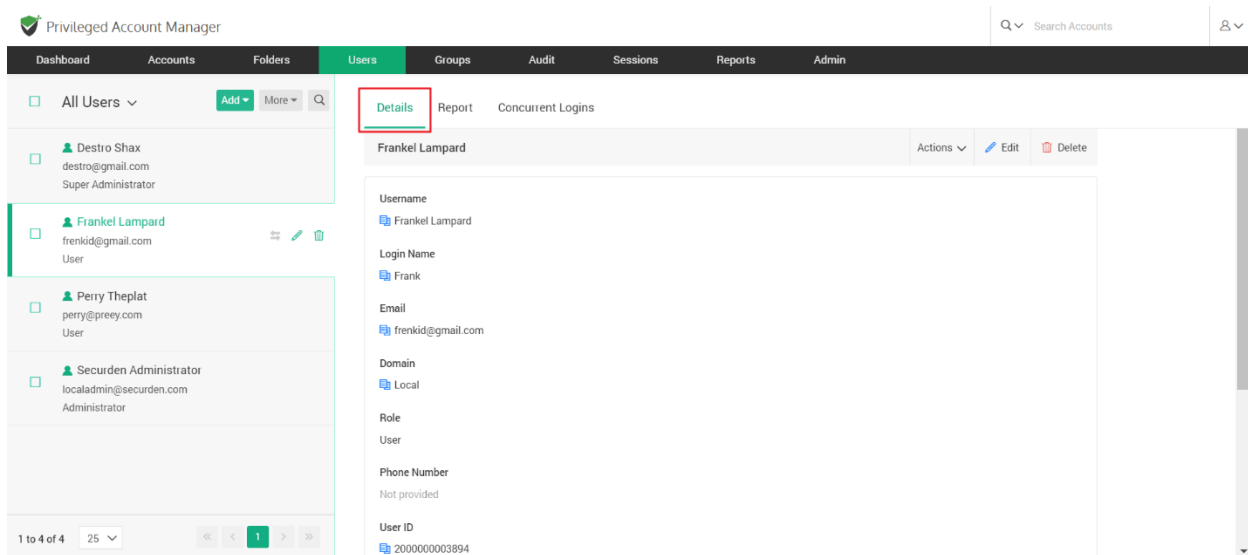
	disaster recovery provisions. You can take backup of the entire database periodically. Users who are given this privilege will be able to schedule the backup.
Configure High Availability	To ensure uninterrupted access to the web application, Securden comes with high availability architecture. You can deploy any number of additional application servers, which would serve as the secondary servers. In the event of the primary server going down, users can connect to any of the secondary servers. Securden agents will also connect to the secondary server, when the primary goes down. Users who are given this privilege will be able to set this feature on and configure the secondary application server(s).
Maintenance and Upgrades	Users who are given this privilege will be able to access 'Product Upgrades' section where the latest product updates, release notes, and the steps to upgrade the latest version are present.
Configure Emergency Access	You can enable a designated list of users to access all passwords (work accounts) stored in Securden, breaking the usual access controls. This is to meet password access needs during certain emergencies. Users who are given this privilege will be able to configure the emergency access.

Configure Assets and Assets Association for Remote Connections	Users who have this privilege can add their IT assets to Securden and configure the association between domain accounts and assets for launching remote connections.
User Assets Association for Remote Connections	You can allow your users to launch remote connections to specific resources using the AD account with which they have logged in to Securden. You can associate the IT assets with the users, which will permit them to launch the connection with the assets allotted. This privilege lets the user configure the association between users and assets for launching remote connections.
Configure Expired Password Rotation	Securden can automatically rotate passwords for accounts that support remote password reset when they expire or are about to expire. Users who have this privilege will be able to configure the password rotation upon expiration.
Configure Custom Application Launcher	In addition to the default modes of launching web-based connections and through native clients, you can define custom application launchers to supply credentials and automatically launch any application, including thick application clients. Users who have this privilege will be able to create a profile for any such application and manage them in Securden to launch remote connections.

Manage Global Tags	When user tag creation is disabled, they have the option to select from tags created globally. So, the user with this privilege will be able to create, edit, and delete global tags.
Miscellaneous	
Access Browser Extensions	Users with this privilege can access browser extensions to facilitate auto-fill of credentials on websites and web applications.
Manage Browser Extensions	Users with this privilege will be able to manage and configure the browser extension settings.
Use Windows Remote Launcher	Users with this privilege will be able to launch RDP and other remote connections from Securden web interface.

User Details

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



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

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

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

All Users ▾ Add ▾ More ▾

Destro Shax
destro@gmail.com
Super Administrator

Frankel Lampard
frenkid@gmail.com
User

Perry Theplat
perry@preey.com
User

Securden Administrator
localadmin@securden.com
Administrator

Details Report Concurrent Logins

Role
User

Phone Number
Not provided

User ID
2000000003894

Two Factor Status
Disabled

Application Access
Enabled

Department
Not provided

Location
Not provided

https://localhost:3959/dashboard

Keeping users in Synchronization with your Active Directory

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

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

All Users ▾ Add ▾ More ▾

Sanjay M.
sanjay@testkarthikrajasoutlook.onmicros...
Auditor

Details Report Concurrent Logins

Sanjay M. Actions ▾ Edit Delete

Username
Sanjay

Login Name
sanjay_m

Email

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

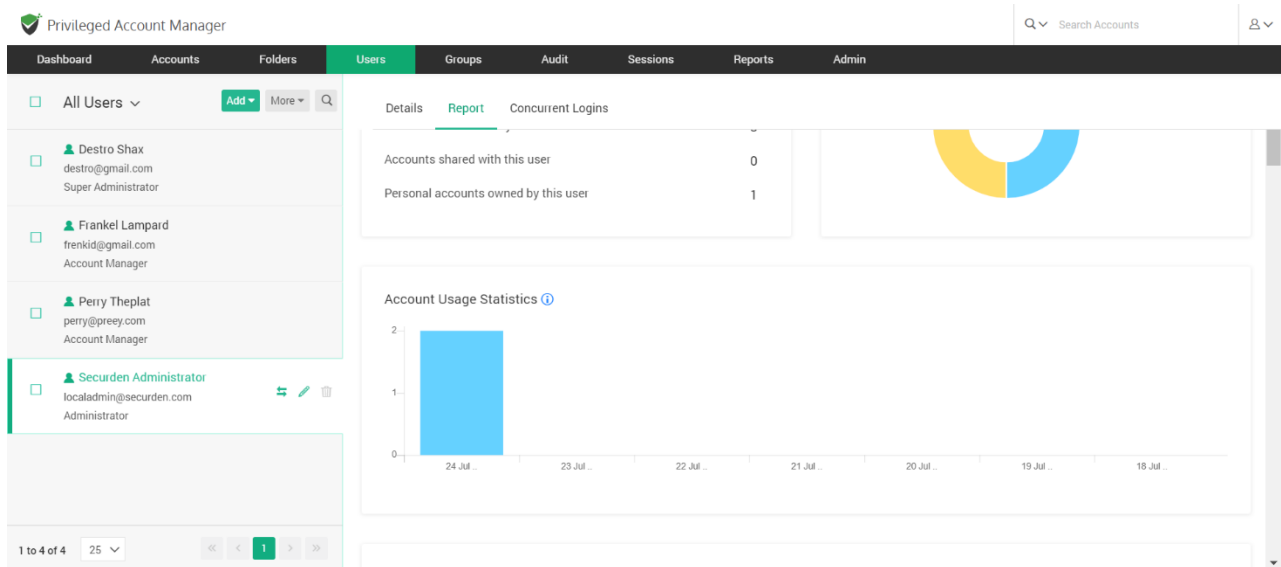
Distinguished Name
CN=Sanjay M.,OU=QA,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM

Role
Auditor

Sync User

1 to 50 of 62

https://demo-unified-pam.securden.com/dashboard



Access Details

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

The screenshot displays the 'Privileged Account Manager' interface. The 'Users' tab is active, showing a list of users on the left. The main panel shows the 'Access Details' table for a selected user, displaying a list of accounts with their addresses and access permissions for Manage, Modify, View, and Open Connection.

Account Title	Account Address	Manage	Modify	View	Open Connection	Tags
Domain Admin	192.164.23.1	✗	✗	✗	✓	
Email login	192.168.72.2	✓	✓	✓	✓	
File		✓	✓	✓	✓	Mark
Hitchhiker		✓	✓	✓	✓	
Server3	173.134.23.4	✓	✓	✓	✓	
Test	test	✓	✓	✓	✓	

User Activity

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

The screenshot displays the Privileged Account Manager (PAM) interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users' (selected), 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' is on the right. The left sidebar shows a list of users: Destro Shax (Super Administrator), Frankel Lampard (Account Manager), Jonathan Ridge (Administrator), Perry Theplat (Account Manager), and Securden Administrator (Administrator). The main content area is titled 'Details Report Concurrent Logins'. It features a table with columns: 'Performed From', 'Performed At', 'Activity Type', 'Username', and 'Reason'. The table shows a list of activities, including user logins, logouts, role changes, and emergency access enabled. The table is paginated, showing 1 to 25 of 142 results.

Performed From	Performed At	Activity Type	Username	Reason
W10PF2YASOP	24 Jul 2023 23:00	User logged in	N/A	Securden Authentication
W10PF2YASOP	24 Jul 2023 22:57	User logged out	N/A	
W10PF2YASOP	24 Jul 2023 22:57	User added	Jonathan Ridge	
W10PF2YASOP	24 Jul 2023 22:49	User role changed	Frankel Lampard	Role changed from User to Ac...
W10PF2YASOP	24 Jul 2023 22:49	User role changed	Perry Theplat	Role changed from User to Ac...
W10PF2YASOP	14 Jul 2023 15:09	Emergency access enabled	N/A	
W10PF2YASOP	12 Jul 2023 14:35	Inactivity period for logout modifi...	N/A	Inactivity Timeout Changed
W10PF2YASOP	12 Jul 2023 14:24	User logged in	N/A	Securden Authentication
W10PF2YASOP	06 Jul 2023 16:14	User logged out	N/A	User logged out due to inactiv...
W10PF2YASOP	06 Jul 2023 16:14	User logged in	N/A	Securden Authentication

Account Activity

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

Privileged Account Manager

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

All Users ▾ Add ▾ More ▾

Destro Shax
destro@gmail.com
Super Administrator

Frankel Lampard
frenkid@gmail.com
Account Manager

Jonathan Ridge
john@gmail.com
Administrator

Perry Theplat
pery@prey.com
Account Manager

Securden Administrator
localadmin@securden.com
Administrator

1 to 5 of 5 25 ▾

Details **Report** Concurrent Logins

Account Activity

Showing 1 to 25 of 37 25 ▾

Account Title	Account Address	Activity Type	Performed From	Performed At	Reason
Server3	173.134.23.4	Account shared with user	W10PF2YASOP	24 Jul 2023 22:55	Shared to Perry Th
Server3	173.134.23.4	Account connectivity check f...	W10PF2YASOP	24 Jul 2023 22:55	Domain unreachat
Server3	173.134.23.4	Account added	W10PF2YASOP	24 Jul 2023 22:55	
Server3	173.134.23.4	Account added to folder	W10PF2YASOP	24 Jul 2023 22:55	Account 'Server3' e
Test	test	Password verification failed	W10PF2YASOP	24 Jul 2023 22:53	Credentials for per
Test	test	Account connectivity check f...	W10PF2YASOP	24 Jul 2023 22:53	Computer unreach
Test	test	Account password changed L...	W10PF2YASOP	24 Jul 2023 22:53	
Test	test	Account password retrieved	W10PF2YASOP	24 Jul 2023 22:52	
Hitchhiker	N/A	Account password retrieved	W10PF2YASOP	24 Jul 2023 22:51	

Groups this user is a part of – User groups that the selected user is part of.

Privileged Account Manager

Dashboard Accounts Folders **Users** Groups Audit Sessions Reports Admin

All Users ▾ Add ▾ More ▾

Chris
chris@gmail.com
User

Destro Shax
destro@gmail.com
Super Administrator

Frankel Lampard
frenkid@gmail.com
Account Manager

Jonathan Ridge
john@gmail.com
Administrator

Matthew Hart
mhart@gmail.com
User

1 to 8 of 8 25 ▾

Details **Report** Concurrent Logins

Showing 1 to 3 of 3 25 ▾

Groups this user is a part of

Showing 1 to 3 of 3 25 ▾

Group Name	Group Description	Domain
Application Development		Local
IT Team		Local
Sysadmins		Local

Showing 1 to 3 of 3 25 ▾

Directly shared folder(s) details

Directly shared folder(s) details – Folders that have been shared to this user directly and not shared through a user group.

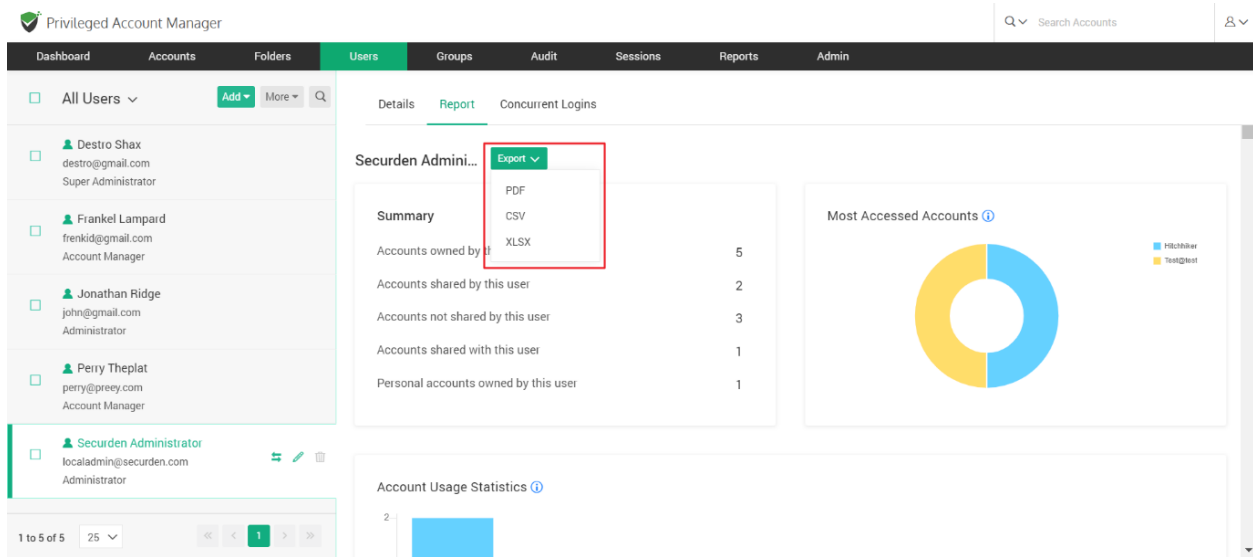
The screenshot shows the 'Privileged Account Manager' interface. The 'Users' tab is selected in the top navigation bar. On the left, a list of users is displayed, with 'Administrator' (admin_1@securden.com) selected. The main panel shows the 'Directly shared folder(s) details' for this user. The table lists folders shared directly to the user.

Folder Name	Folder Description	Manage Folder	Add Accounts to Folder	View Folder
API Test		✓	✓	✓
Cisco Routers		✓	✓	✓
Client Services		✓	✓	✓
Databases		✓	✓	✓
File Server		✓	✓	✓
Internal		✓	✓	✓
IT Infrastructure		✓	✓	✓

The screenshot shows the 'Privileged Account Manager' interface. The 'Users' tab is selected in the top navigation bar. On the left, a list of users is displayed, with 'Administrator' (admin_1@securden.com) selected. The main panel shows the 'Group shared folder(s) details' for this user. The table lists folders shared to the user through a group.

Folder Name	Folder Description	Group Name	Manage Folder	Add Accounts to Folder	View Folder
API Test		Securden Admins	✓	✓	✓
Cisco Routers		Administrators	✓	✓	✓
Cisco Routers		Securden Admins	✓	✓	✓
Client Services			✓	✓	✓
Databases		Administrators	✓	✓	✓
Databases		Securden Admins	✓	✓	✓
Databases		Storage Replica Adm...	✓	✓	✓

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



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

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

Monitor Concurrent Logins

You can monitor the concurrent logins of each user.

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

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

The screenshot displays the Securden Privileged Account Manager interface. The top navigation bar includes tabs for Dashboard, Accounts, Folders, **Users**, Groups, Audit, Sessions, Reports, and Admin. The left sidebar shows a list of users under 'All Users', including Destro Shax, Frankel Lampard, Jonathan Ridge, Perry Theplat, and Securden Administrator. The main content area is titled 'Concurrent Logins' and contains a note about concurrent logins and a 'Terminate All' button. Below this is a table with columns: Connected From, Device, Login Start Time, and Action. The table shows one entry for W10PF2YASOP on a PC / Windows 10 / Chrome 114.0.0, logged in on 24 Jul 2023 23:00. The bottom of the interface shows pagination controls indicating 'Showing 1 to 1 of 1' and '25' items per page.

User Groups

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

Adding groups can be done in the following ways:

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

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

The screenshot displays the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups' (active), 'Audit', 'Sessions', 'Reports', and 'Admin'. The left sidebar shows a list of groups, with 'Administrators' selected. A dropdown menu is open, showing options: 'Import Groups from AD', 'Import Groups From LDAP', 'Import Groups from Azure AD', and 'Add Groups Manually'. The main panel shows details for the 'Administrators' group, including its name, description, and ID. Below this, there are buttons for 'Sync Members', 'Schedule Sync', and 'Group Setting'. A table lists the group's members, including 'Administrator', 'Parthasarathy Dharmalingam', 'Securden Service Account', and 'Securden Service Account 2'.

Import User Groups from AD

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

Step 1: Establish Connectivity

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users **Groups** Audit Sessions Reports Admin

Import Groups from AD

Step 1: Establish Connectivity

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

Domain
SECURDEN.AWS.COM

Domain IP Address / FQDN *
172.31.1.11

Secondary IP Addresses (Optional)

[Select Remote Gateway](#)

Help

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

Domain IP Address

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

Connection Mode

Specify the mode (SSL/non-SSL) through which Securden has to establish connection with the AD domain. If SSL mode is selected, the domain controller should be serving over SSL in port 636 and the certificate of the domain controller should have been signed by a CA. If the certificate of the domain controller is not signed by a certified CA, you need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the domain controller and all the intermediate certificates if any. For details, [click here](#)

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

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

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

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

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

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

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

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

You can discover any group of users and add them to Securden.

Step 2: Go to Import

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

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

To import OUs, select the OU tab.

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

To import Groups, select the Groups tab.

1. Enter the Group name and select **Discover**.
2. You can also browse by clicking on the **Browse Groups and Select** option. You can select one or multiple groups and select **Add**.
3. You can then verify your selection in the **Verify the Objects Selected for Discovery**.
4. You can then select the role for the OUs imported using the **Role in Securden** drop down.

5. Before selecting the import button, you can look into the additional settings which are explained below.
6. Select **Import**.

Advanced settings:

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

Import groups from LDAP

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

The screenshot shows the Securden Privileged Account Manager web interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups' (highlighted), 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar and a user profile icon are on the right. The main content area is titled 'Import Groups from LDAP' and 'Step 1: LDAP Settings'. It contains a descriptive text box and four input fields: 'Domain Identifier *', 'Domain Base DN *', 'Account DN *', and 'Domain IP Address / FQDN *'. The 'Domain IP Address / FQDN *' field has a red error message 'Invalid DNS format' below it. A 'Help' sidebar on the right provides detailed instructions for each field, including an example for 'Domain Base DN': 'DC=MyDomain,DC=com'.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users **Groups** Audit Sessions Reports Admin

Import Groups from LDAP

Step 1: LDAP Settings

You can integrate Securden with any LDAP-compliant directory service and import users and groups. The integration and import follow a two-step process.

Domain Identifier *

Domain Base DN *

Account DN *

Domain IP Address / FQDN *

Invalid DNS format

Help

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

Domain Identifier

Enter the name with which the LDAP domain can be identified.

Domain Base DN

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

Example
DC=MyDomain,DC=com

Account DN

For connection authentication, Securden needs access to an

Step 1: LDAP Settings

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

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

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

Example

DC=MyDomain,DC=com

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

Example

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

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

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

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

Supply Administrator Credentials: You need to supply administrator credentials so as to enable Securden to scan the members in the domain. You may enter the username and password manually once and this will be stored in Securden for use during subsequent import attempts. If the users belong

to a different network than the Securden server, you can route the connection through a remote gateway. You can select the appropriate remote gateway from the drop-down and the discovery will happen through the selected gateway.

Step 2: Discover and Import from LDAP

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

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

Import Groups from LDAP

Step 2: Discover and Import from LDAP

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

Domain Name : ldap Domain IP : 172.31.1.11

Base DN *
DC=SECURDEN,DC=AWS,DC=COM

Search Filter *

LDAP Scope
Base

Help

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

This GUI offers the flexibility to fetch only the required users from the LDAP domain. Typically, the search happens by combining the Base DN, which is the base of the search tree for all users, the specific level under the Base DN (the LDAP Scope), and the Search filter that gets granular to fetch only the required users. In the search filter, you can specify a Object Class, which defines the types of results that Securden will fetch. If the Base DN contains a mix of object types like people, groups, assets, and so on, you may specify only the required set of objects here. You may use (objectClass=*) to include all objects.

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

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

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

- In the search filter, you can specify an Object Class, which defines the types of results that Securden will fetch. If the Base DN contains a mix of object types like people, groups, assets, and so on, you may specify only the required set of objects here. You may use (objectClass=*) to include all objects.
- If you want to add only specific user groups from your LDAP directory, just perform a search using the appropriate search filter. For example, if you want to import only the groups from the OU Sysadmin and O Securden, the Base DN has to be ou=Sysadmin,o=securden,c=com and the search filter has to be written within brackets as: (objectClass=user).
- If you want to restrict your search to a specific level under the BaseDN, you may select the required scope from the drop-down.
- Click **Search**. Verify your discovery details under **Verify the Objects Selected for Discovery**. If you to assign a common role to all the users being imported, select the role in Securden and finally click **Import**.

Dashboard Accounts Folders Users **Groups** Audit Sessions Reports Admin

Verify the Objects Selected for Discovery

Verify your search results before proceeding to importing them to Securden.

When importing users, what should be the user role?

Role in Securden

User ▼

[+ Show Advanced Settings](#)

Import Cancel

common role to all the users being imported, select the role in Securden and finally click 'Import'.

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

Advanced Settings:

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

Import from Azure AD

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

Step 1: Establish Connectivity

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

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

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

Client ID: Enter the Client ID of the application.

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

Step 2: Import Users

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

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

To import OUs, select the OU tab

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

To import Groups, select the Groups tab

1. Enter the Group name and select **Discover**.
2. You can also browse from the OU tree by clicking on the **Browse Groups and Select** option. You can select one or multiple OUs and select **Add**.

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

Advanced Settings:

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

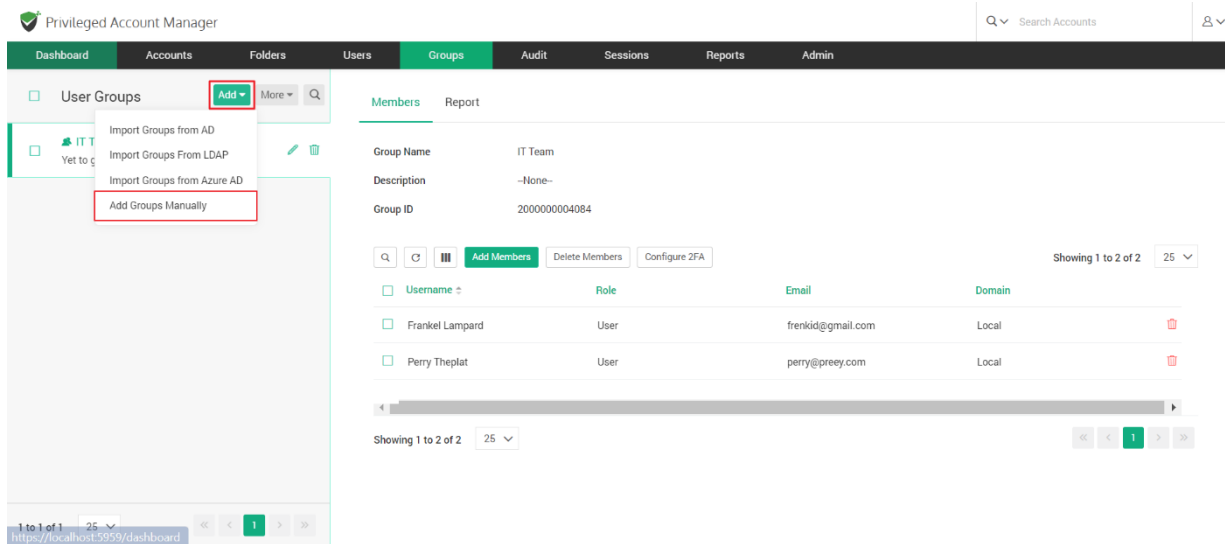
User Groups to Import: You can import all or specific user groups to import, depending on your requirements. You can type in the names in the respective text fields in comma separated form.

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

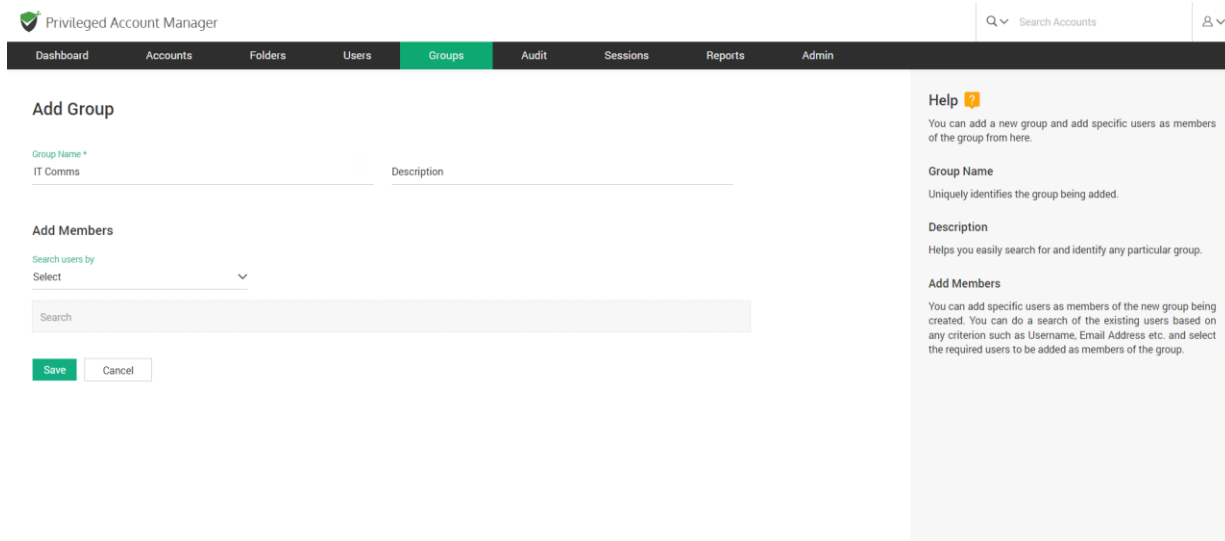
Add User Groups Manually

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

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



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



Group Name: Uniquely identifies the group being added.

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

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

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

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users **Groups** Audit Sessions Reports Admin

Add Group

Group Name *
IT Comms

Description

Add Members

Search users by
Email

Perry Theplat (Perry) x

Clear all

Save Cancel

Help ?

You can add a new group and add specific users as members of the group from here.

Group Name
Uniquely identifies the group being added.

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

Add Members
You can add specific users as members of the new group being created. You can do a search of the existing users based on any criterion such as Username, Email Address etc. and select the required users to be added as members of the group.

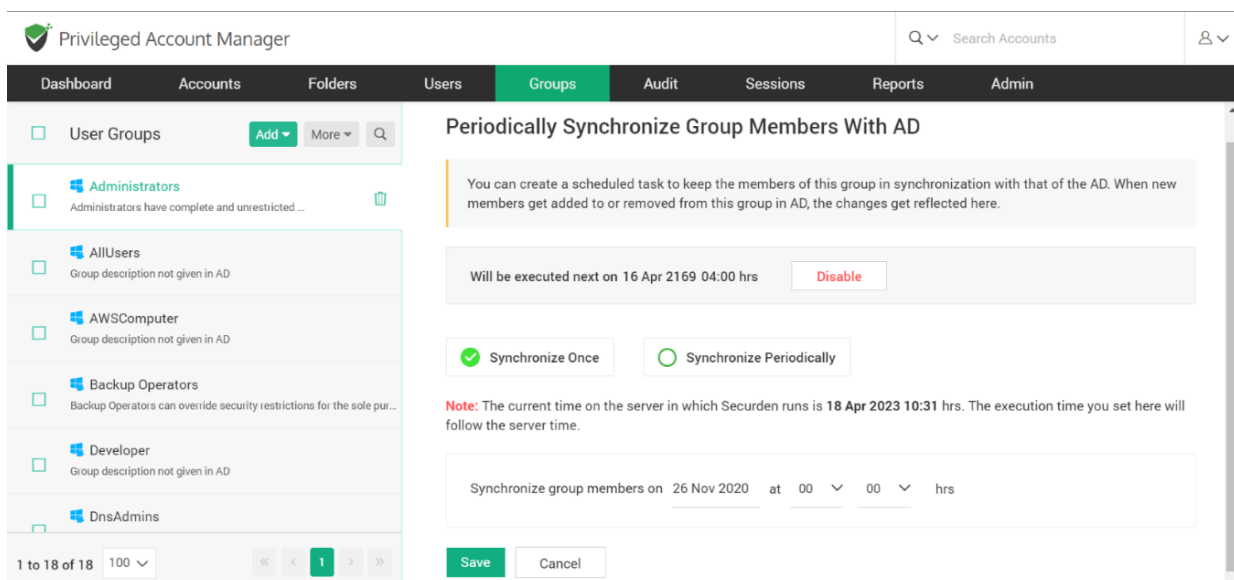
After providing these details, click on **Save** to create the user group.

Configure Periodic Synchronization of Groups

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

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

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



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

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users **Groups** Audit Sessions Reports Admin

User Groups Add More

☐ Administrators
Administrators have complete and unrestricted ...

☐ AllUsers
Group description not given in AD

☐ AWSComputer
Group description not given in AD

☐ Backup Operators
Backup Operators can override security restrictions for the sole pur...

☐ Developer
Group description not given in AD

☐ DnsAdmins

1 to 18 of 18 100

Periodically Synchronize Group Members With AD

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.

Will be executed next on 16 Apr 2169 04:00 hrs Disable

☐ Synchronize Once ☒ Synchronize Periodically

Note: The current time on the server in which Securden runs is **18 Apr 2023 10:31 hrs**. The execution time you set here will follow the server time.

Synchronize group members periodically starting from 26 Nov 2020 at 00 00 hrs

Synchronize members every 1 Hours

Group Settings

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

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users **Groups** Audit Sessions Reports Admin

User Groups Add More

☒ Administrators
Administrators have complete and unrestricted ...

☐ AllUsers
Group description not given in AD

☐ AWSComputer
Group description not given in AD

☐ Backup Operators
Backup Operators can override security restrictions for the sole pur...

☐ Developer
Group description not given in AD

☐ DnsAdmins

1 to 18 of 18 100

Modify Group Settings

When importing users, what should be the user role?

Role in Securden
User

What would you like to do with subgroups when importing a group?

☒ Include domain users of all subgroups to the group being imported (Users of subgroups will be imported; but subgroup structure will not be retained in Securden)

☐ Ignore subgroups. Import only the users of the first level group

Save Cancel

Explore Single Sign-On Options

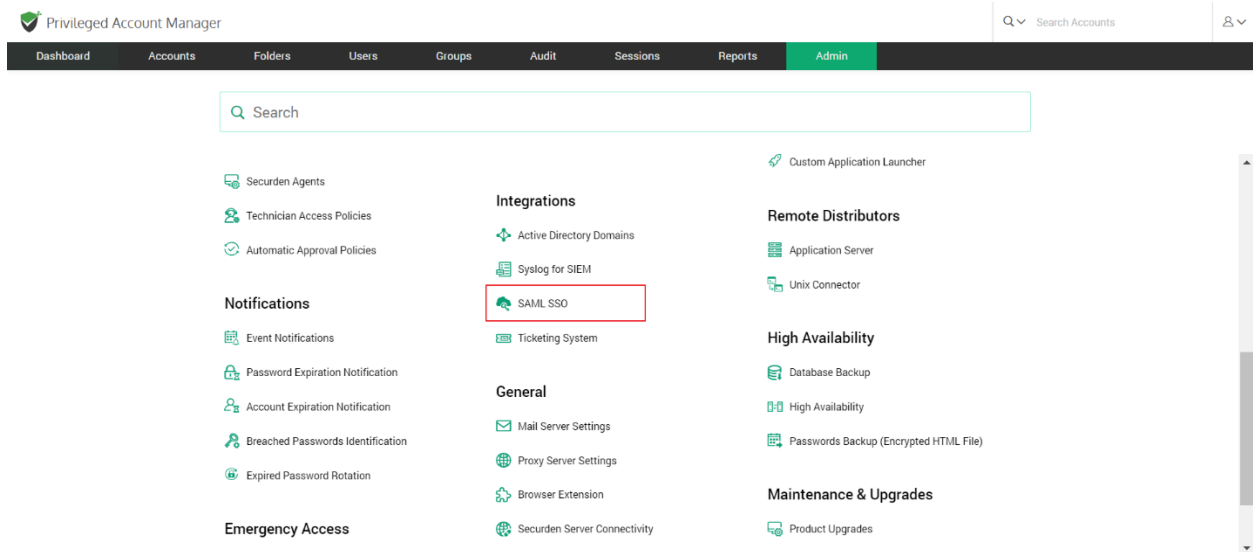
Securden leverages SAML 2.0 to seamlessly integrate with SAML-compatible federated identity management solutions like Okta, G Suite, Microsoft ADFS, OneLogin, PingIdentity, Azure AD SSO, and others for Single Sign On. Securden serves as the SAML Service Provider (SP), and it integrates with SAML Identity Providers (IdP). Once this is done, users who log in to solutions like Okta (IdP) will be automatically logged in to Securden. The IdP and Securden exchange validation details are in the background.

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

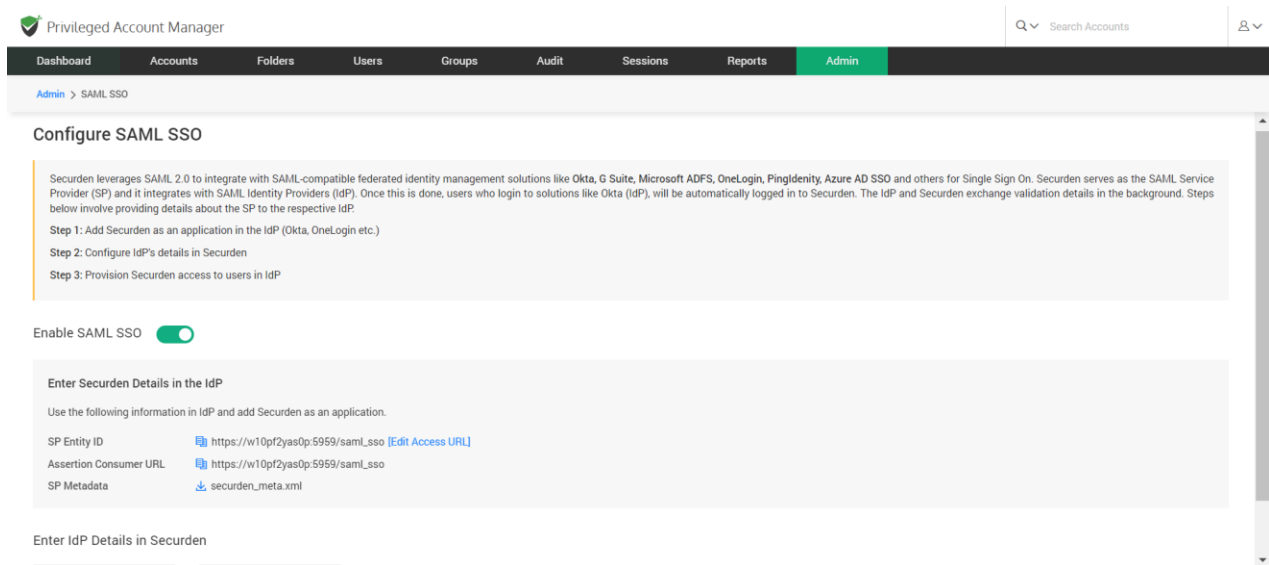
- Step 1: Add Securden as an application in the IdP (Okta, OneLogin, etc).
- Step 2: Configure IdP's details in Securden.
- Step 3: Provision access to Securden for your users in the IdP.

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

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



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



Step 1: Add Securden as an application in your SSO solution (known as the IdP). You need to perform this step on your SSO solution.

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

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

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > SAML SSO

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

Enable SAML SSO ☒

Enter Securden Details in the IdP

Use the following information in IdP and add Securden as an application.

SP Entity ID	https://w10pf2yas0p.5959/saml_sso [Edit Access URL]
Assertion Consumer URL	https://w10pf2yas0p.5959/saml_sso
SP Metadata	securden_meta.xml

Enter IdP Details in Securden

Step 2: Configure IdP's details in Securden

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > SAML SSO

Configure SAML SSO

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

Enable SAML SSO ☒

Enter Securden Details in the IdP

Use the following information in IdP and add Securden as an application.

SP Entity ID	https://vr10pf2yasdp:5959/saml_sso [Edit Access URL]
Assertion Consumer URL	https://vr10pf2yasdp:5959/saml_sso
SP Metadata	securden_meta.xml

Enter IdP Details in Securden

☒ Configure IdP Details ☐ Upload IdP Metadata

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

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

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > SAML SSO

Enter IdP Details in Securden

☒ Configure IdP Details ☐ Upload IdP Metadata

Identifier*

IdP Entity ID*

IdP Login URL*

Protocol Type
HTTP-POST

Upload Certificate File *

Choose a file

Custom Rule for Securden Login Name (optional)

You need to enter the following information:

Identifier – Enter an Identifier text that will appear on the Securden login screen to display the SSO option.

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

IdP Login URL - Enter the URL used to login into your IdP portal.

PROTOCOL TYPE – Select the type of protocol to use from the two available options.

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

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

Custom rule for Securden login -

As part of the integration, one of the important aspects is the 'login name' format. The Identity Provider returns a login name, which Securden uses as the username for logging in to the application. If you want to map the name returned by the identity provider with a different name, you can create custom rules.

Basically, you can make use of the following string functions to create custom rules to manipulate the login name returned by the identity provider. In the string function, login name denotes the name returned by the identity provider.

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

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

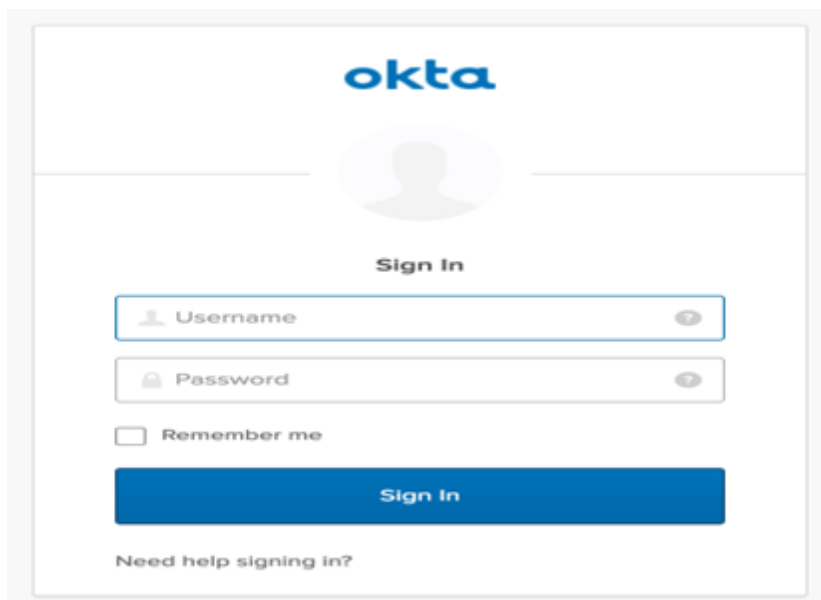
Configure Single Sign-On

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

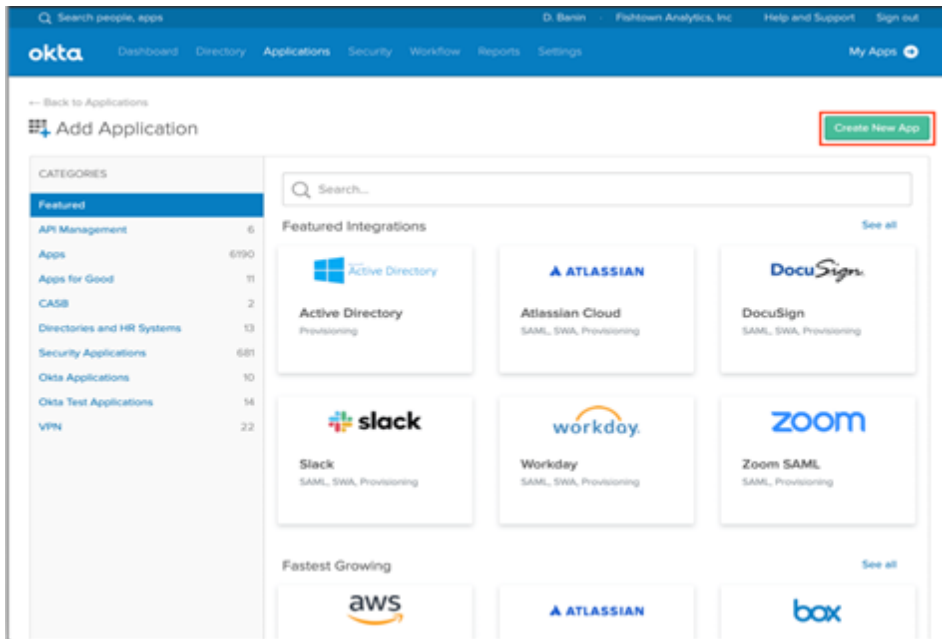
Configure Single Sign-On for Okta

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

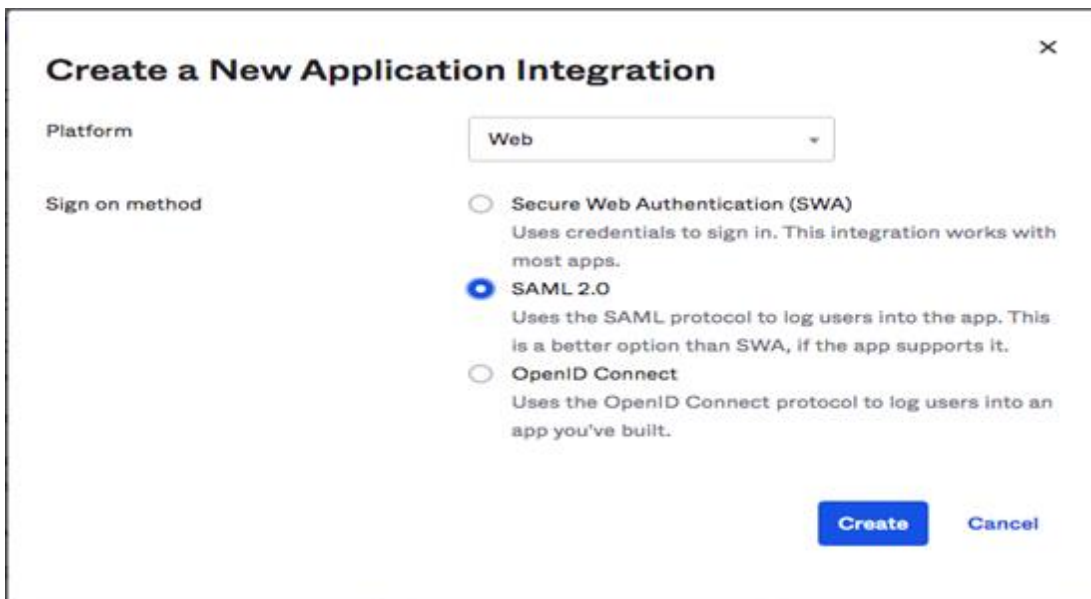
1. Log in to your Okta account using your admin credentials.



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




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




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

1 General Settings

App name: SAML_app

App logo (optional) 

 Browse...

Upload Logo

App visibility

☐ Do not display application icon to users




☐ Do not display application icon in the Okta Mobile app

Cancel Next

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

Enter Securden Details in the IdP

Use the following information in IdP and add Securden as an application.

SP Entity ID	 https://pam-demo.securden.com/saml_sso [Edit Access URL]
Assertion Consumer URL	 https://pam-demo.securden.com/saml_sso
SP Metadata	 securden_meta.xml

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

Create SAML Integration

1 General Settings 2 **Configure SAML** 3 Feedback

A SAML Settings

General

Single sign on URL
☒ Use this for Recipient URL and Destination URL
☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState
If no value is set, a blank RelayState is sent

Name ID format

Application username

Update application username on

[Show Advanced Settings](#)

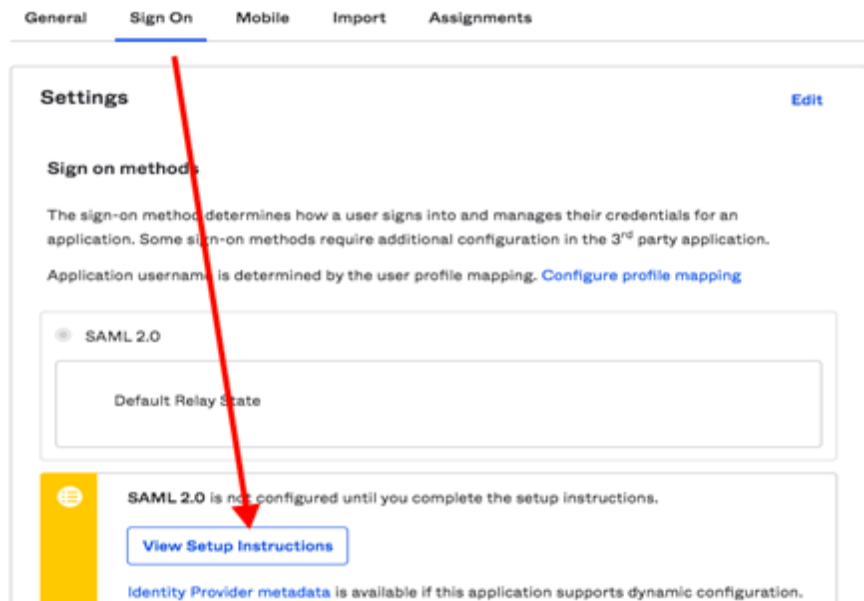
What does this form do?
 This form generates the XML needed for the app's SAML request.

Where do I find the info this form needs?
 The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate
 Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

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



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

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

Enter IdP Details in Securden

☒ **Configure IdP Details** ☐ Upload IdP Metadata

Identifier*

IdP Entity Id*

IdP Login URL*

Protocol Type
HTTP-POST

Upload Certificate File *
Choose a file [Browse](#)

Custom Rule for Securden Login Name (optional)

[Save](#)

Configure Single Sign-On for Azure AD

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

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

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

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

5. Click on the **Register** button to complete the addition of Securden PAM.
6. The newly registered Securden PAM's application will open up. Click on **Authentication** under **Manage** in the left pane. In the **Authentication** page, under **Advanced Settings**, enable **Allow Public Client Flows** by clicking on the **Yes** button.
7. Click on **API Permissions** under **Manage** in the left pane. In the **API Permissions** page, click on the **+Add a Permission** button.
8. A **Request API Permissions** window will pop up. Here, choose **Azure AD Directory Graph** under **Supported Legacy APIs**.
9. Click on **Delegated Permissions** and search for "read" in the **Select Permissions** search bar to populate relevant permissions. Select the

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

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

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

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

Troubleshooting Tips

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

Solution:

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

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

```
stringAppend('DOMAINNAME\', loginname)
```

Example: `stringAppend('SECURDENEDEV\', loginname)`

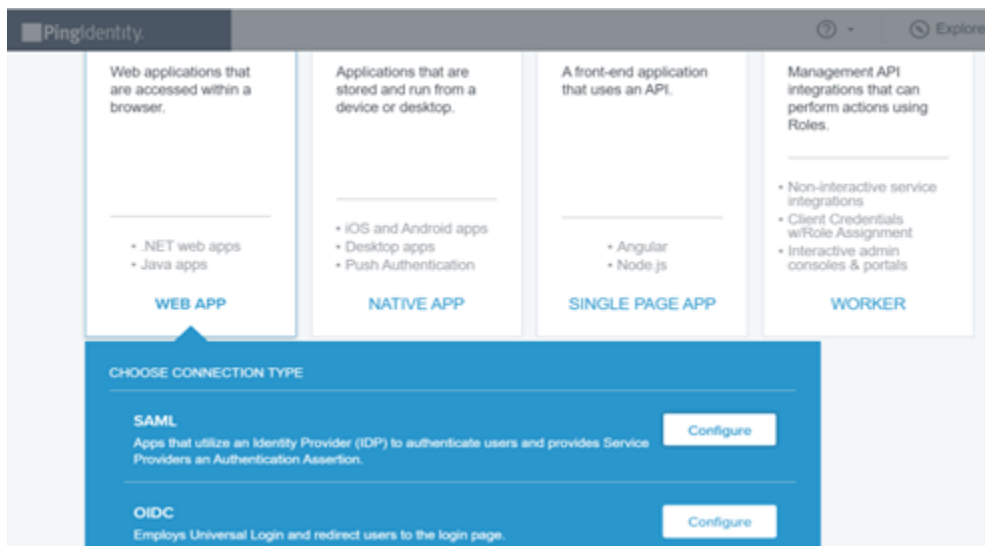
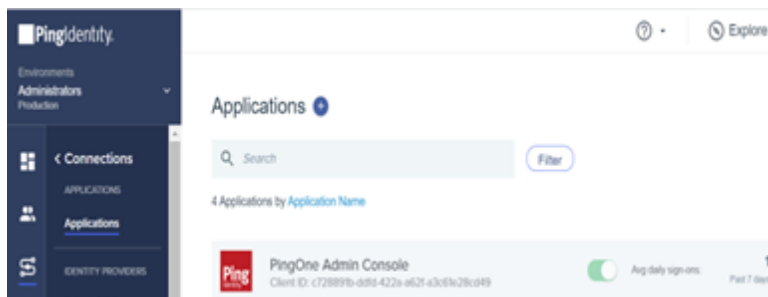
If an email is received from Identity Provider, the login name has to be stripped from the value:

```
stringAppend('DOMAINNAME\', substringBefore(loginname, '@'))
```

For extracting username from email: `substringBefore(loginname, '@')`

Configure Single Sign-On for Ping Identity

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



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

Create App Profile

Personalize your application by creating a unique profile. The description will help your customers identify the purpose of the application and provide important information to misguided connections.

APPLICATION NAME

DESCRIPTION

ICON

Max Size: 10 MB
JPEG, JPG, GIF, PNG

Cancel Next

PROGRESS

- 1 Create App Profile
Personalize your application
- 2 Configure SAML
Configure connection between your app and PingOne.
- 3 Map Attributes
Provide access to your application for customers to authenticate.

PingIdentity

APPLICATION NAME: securden1

TYPE: Web App

PROTOCOL: SAML

PROVIDE APP METADATA

☒ Import Metadata ☐ Import From URL ☐ Manually Enter

securden_meta.xml

ACS URLS

https://pam-demo.securden.com/saml_sso

Cancel Save and Continue

PROGRESS

- 1 Create App Profile
Personalize your application
- 2 Configure SAML
Configure connection between your app and PingOne.
- 3 Map Attributes
Provide access to your application for customers to authenticate.

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

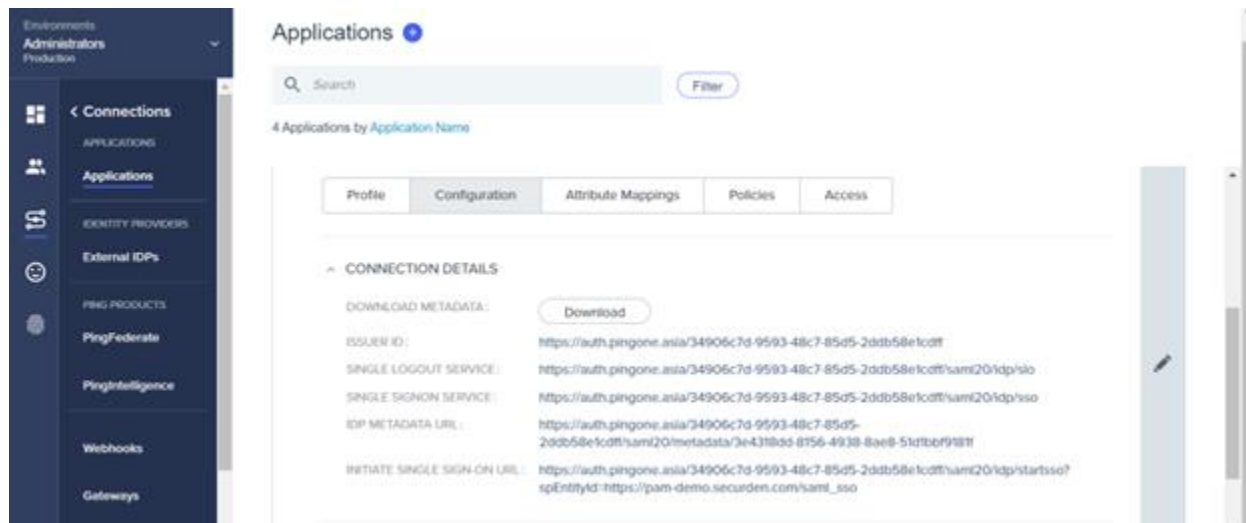
Enter Securden Details in the IdP

Use the following information in IdP and add Securden as an application.

SP Entity ID	https://pam-demo.securden.com/saml_sso [Edit Access URL]
Assertion Consumer URL	https://pam-demo.securden.com/saml_sso
SP Metadata	↓ securden_meta.xml

Use the provided details to integrate Securden with Ping Identity.

5. Map attributes to provide access to your application for customers to authenticate.
6. Click on the **Finish** button to complete the SAML creation process.
7. Navigate to **Applications >> Securden >> Configuration** and download metadata or copy the respective Issuer ID (Entity Id) and IDP metadata URL (Login URL).



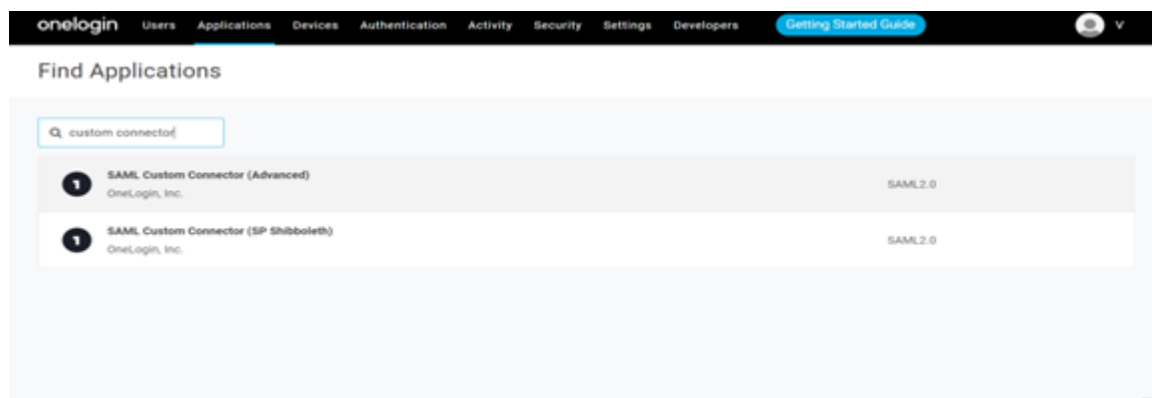
8. Navigate to **Securden >> Admin >> Integrations >> SAML SSO**. Click on the **Configure IdP Details** option to display the IdP options.

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

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

Configure Single Sign-On for One Login

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



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

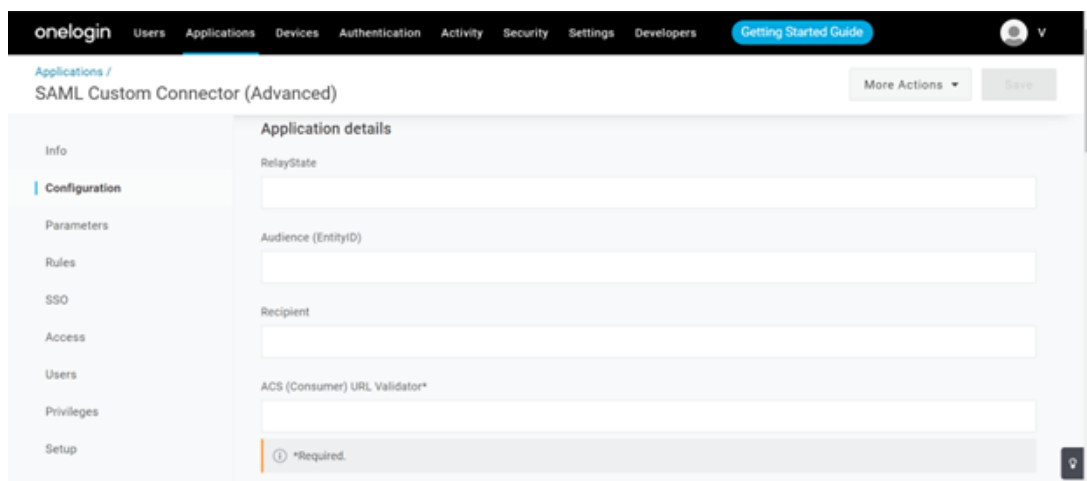
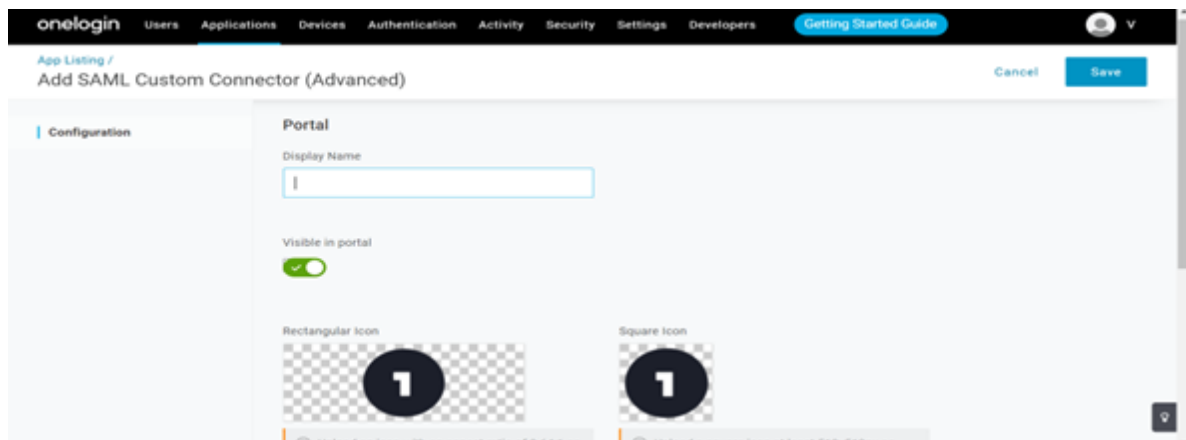
Enter Securden Details in the IdP

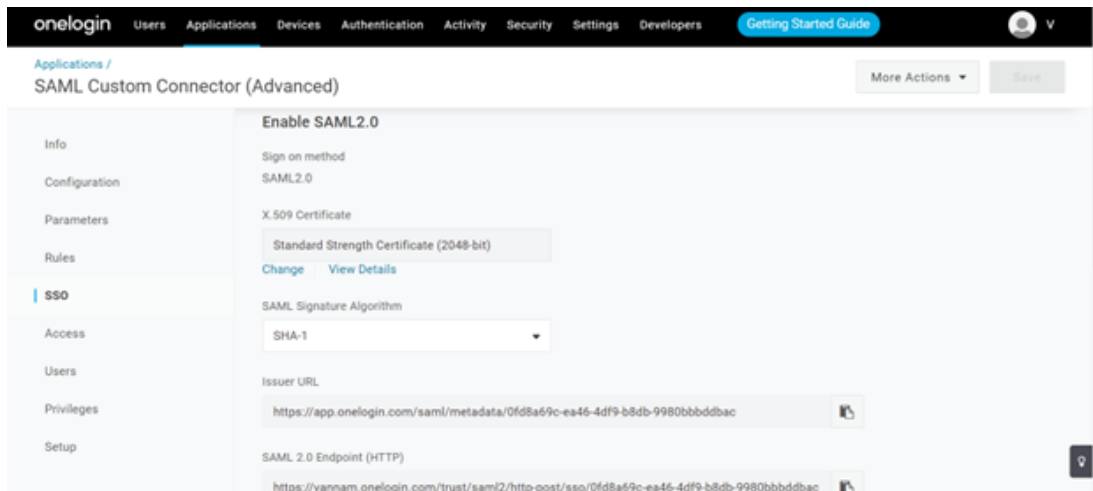
Use the following information in IdP and add Securden as an application.

SP Entity ID	 https://pam-demo.securden.com/saml_sso [Edit Access URL]
Assertion Consumer URL	 https://pam-demo.securden.com/saml_sso
SP Metadata	 securden_meta.xml

Use the provided details to integrate Securden with One Login.

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





5. Click on the **Save** button to complete the SAML creation process and navigate to **Securden >> Admin >> Integrations >> SAML SSO**.
6. Toggle the **Enable SAML SSO** switch on.
7. Click on the **Configure IdP Details** option to display the IdP options. Here, you need to enter details of your SAML IdP. You can add the details manually or choose to import them from the IdP Metadata file.
8. Click the **Save** button to complete the setup.
9. You can now assign Securden to your users. Navigate to **Applications >> SAML Custom Connector (Advanced) >> Users**. Select the required users and assign them the application.

Configure Single Sign-On for G-Suite

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

1. You need to possess a super administrator account to proceed further and open the Google Admin console.
2. From the Admin console Home page, go to **Apps >> Web and Mobile Apps**.

3. Click **Add App >> Add Custom SAML** app.
4. On the **App Details** page:
 - a. Enter the name of the custom app (here Securden).
 - b. (Optional) Upload an **app icon**. The app icon appears on the web and mobile apps list, the app settings page, and the app launcher. If you don't upload an icon, an icon is created using the first two letters of the app name.
5. Click **Continue**.
6. On the **Google Identity Provider** details page, get the setup information needed by the service provider using one of these options:
 - a. Download the **IDP metadata**.
 - b. Copy the **SSO URL** and **Entity ID** and download the **Certificate** (or SHA-256 fingerprint, if needed).
7. (Optional) In a separate browser tab or window, sign in to your service provider and enter the information you copied in Step 4 into the appropriate SSO configuration page, then return to the Admin console.
8. Click **Continue**.
9. In the **Service Provider Details** window, enter an **ACS URL, Entity ID, and Start URL** (if needed) for your custom app. These values are all provided by the service provider. **Note:** The ACS URL has to start with https://
10. The default **Name ID** is the primary email. Multi-value input is not supported.
11. Click **Continue**.
12. Under **Google Directory Attributes**, click the **Select Field** menu to choose a field name. Then, enter the corresponding attribute for your custom SAML app under **App Attributes**.
13. Click **Finish**.

Turn on your SAML App

1. Click **User Access**.
2. To turn on or off a service for everyone in your organization, click **On** for everyone or **Off** for everyone, and then click **Save**.
3. (Optional) To turn a service on or off for an organizational unit:
 - At the left, select the organizational unit.
 - Select On or Off.
 - Click **Override** to keep your setting if the service for the parent organizational unit is changed.
 - If Overridden is already set for the organizational unit, choose an option:
 - Inherit—Reverts to the same setting as its parent.
 - Save—Saves your new setting (even if the parent setting changes).
4. To turn on a service for a set of users across or within organizational units, select an access group.
5. Ensure that the email addresses your users use to sign in to the SAML app match the email addresses they use to sign in to your Google domain.

Configure Single Sign-On for Microsoft ADFS

Before configuring ADFS

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

Step 1: Install the ADFS role

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

Step 2: Configure the Federation Server

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

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

Step 3: Configure ADFS to integrate with Securden

1. Open Server **Manager >> Tools >> ADFS Management**. The ADFS wizard is launched.
2. Expand to **Relying Party Trusts** and click **Add Relying Party Trust**.
3. On the "**Add Relying Party Trusts**" wizard, click **Start**.
4. Launch Securden web interface (<https://<Securden-Server-Hostname>:5454/>), navigate to **Admin >> Integrations >> SAML SSO** and download the metadata file - **securden_metadata.xml**.
5. Go back to **Add Relying Party Trusts** Wizard. Under **Select Data Source**, select **Import data about the relying party from a file**. Browse and select the **securden_metadata.xml**, which you downloaded from Securden and click **Next**.
6. In the **Specify Display Name** field, enter **Securden** and then click **Next**.

7. Choose **I don't want to configure multifactor authentication settings for this relying party trust at this time** and then click **Next**.
8. Choose **Permit all users to access this relying party**.
9. Keep clicking **Next** until you reach the **Finish** screen.
10. Choose to open the **Edit Claim Rules dialog** before clicking Finish. This will launch the **Edit Claim Rules** window.
11. On the **Issuance Transform Rules** tab, click **Add Rule**.
12. Under **Select Rule Template**, set **Transform an incoming claim** as the rule template and click **Next**.
13. Choose **Windows account name** in **Incoming Claim Type** and **Name ID** in **Outgoing Claim Type** and then click Finish. Apply the claim rules in **Issuance Transform Rules** tab.
14. Navigate to **Endpoints**, and then to **MetaData Group**. Select the entry with type **Federation MetaData**.
15. Open a web browser and access the following URL path as in the entry "https://<ADFS-Server-Name>/<URL-Path>"

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

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

Troubleshooting Tips:

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

Steps to follow:

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

```
stringAppend('DOMAINNAME\', loginname)
```

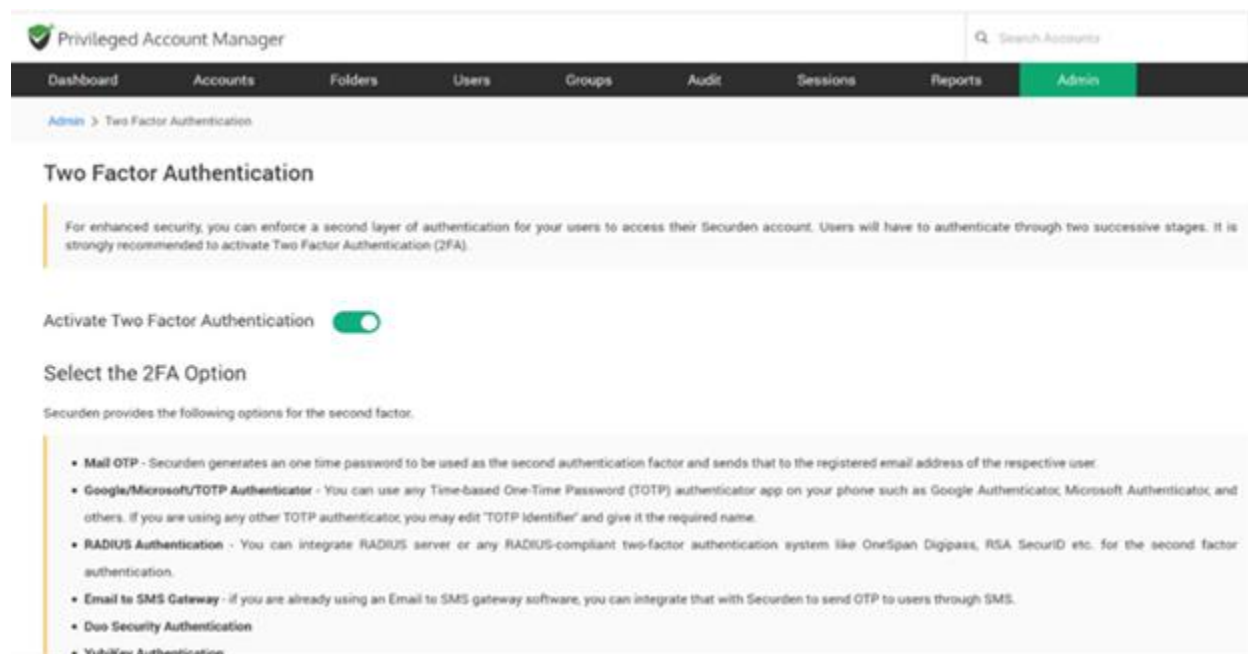
4. **Example:** `stringAppend('SECURDENEDEV\', loginname)`
5. In addition, there might be an email mismatch with username.
 - a. If an email is received from SSO, the domain name has to be trimmed from the value: `stringAppend('DOMAINNAME\', substringBefore(loginname, '@'))`
 - b. For extracting username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

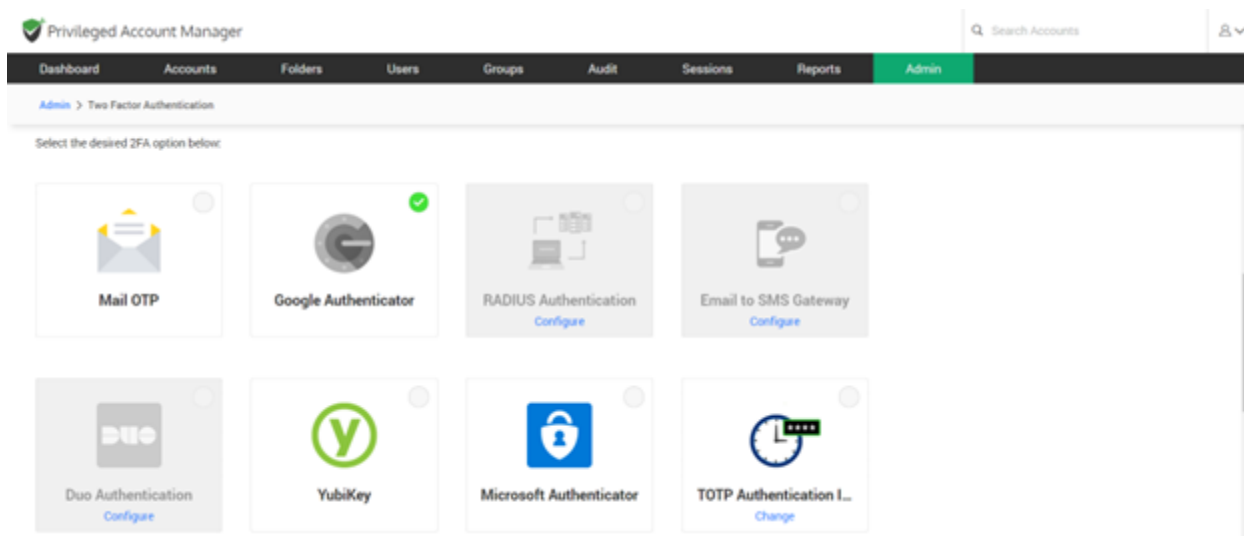
Section 4: Configuring Two Step Verification

Enforcing Two Factor Authentication (MFA)

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

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





At present, Securden supports:

- **Mail OTP** - Securden generates a one-time password to be used as the second authentication factor and sends that to the registered email address of the respective user.
- **Google/Microsoft/TOTP Authenticator** - You can use any Time-based One-Time Password (TOTP) authenticator app on your phones such as Google Authenticator, Microsoft Authenticator, and others. If you are using any other TOTP authenticator, you may edit the '**TOTP Identifier**' and give it the required name.
- **RADIUS Authentication** - You can integrate the RADIUS server or any RADIUS-compliant two-factor authentication system like OneSpan Digipass, RSA SecurID, etc. for the second-factor authentication.

- **Email to SMS Gateway** - If you are already using an Email to SMS gateway software, you can integrate that with Securden to send OTP to users through SMS.
- **Duo Security Authentication** – If you have enrolled in Duo Security, you can easily integrate that with Securden and make use of the various authentication methods (security key, biometric authenticator, touch ID, web authentication, and more).
- **YubiKey Authentication** – You can also make use of a YubiKey as a second-factor authentication, which generates one-time passwords upon integration.

Mail OTP

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

To configure Mail OTP for 2FA:

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

Google Authenticator/Microsoft Authenticator/TOTP Authenticator

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

Prerequisites:

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

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

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

1. Navigate to **Admin >> Authentication >> Two-Factor Authentication**.

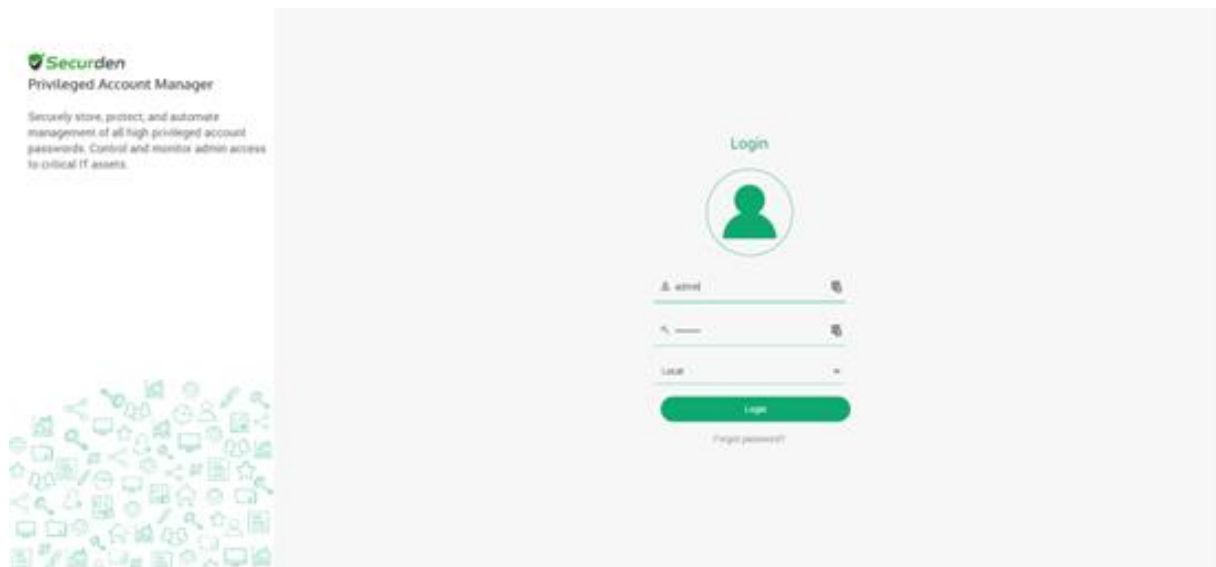
2. Choose the option **Google Authenticator/Microsoft Authenticator/TOTP Authenticator**.
3. Click **Confirm**.

Yubikey

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

To integrate Yubikey with Securden,

1. Navigate to **Admin >> Authentication >> Two-Factor Authentication**.
2. Click on **Yubikey**.
3. Click **Save**.
4. To connect to Securden PAM after integrating it with Yubikey, you need to launch the Securden PAM's web interface first.



5. Enter your Securden credentials and complete the first level of authentication. Once it succeeds, you will be asked to enter the Yubikey OTP.
6. In the USB port of your computer, insert the Yubikey.
7. Before generating a one-time password, you need to decide which of the two slots, slot 1 or slot 2, of the YubiKey you're going to use for authentication throughout.

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

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

will remain the same and the rest of the 32 characters will be randomized.

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

- cccjgdwdjkwjkdjkwjkdkhfhgrtnnlgedjlftrbdeut
- cccjgjubuebduhubnjkedjkehijeiocjbnublfrev
- cccjggkcbvejnvchfkfhiiuunbtvngihdfiktncvlhck

Note:

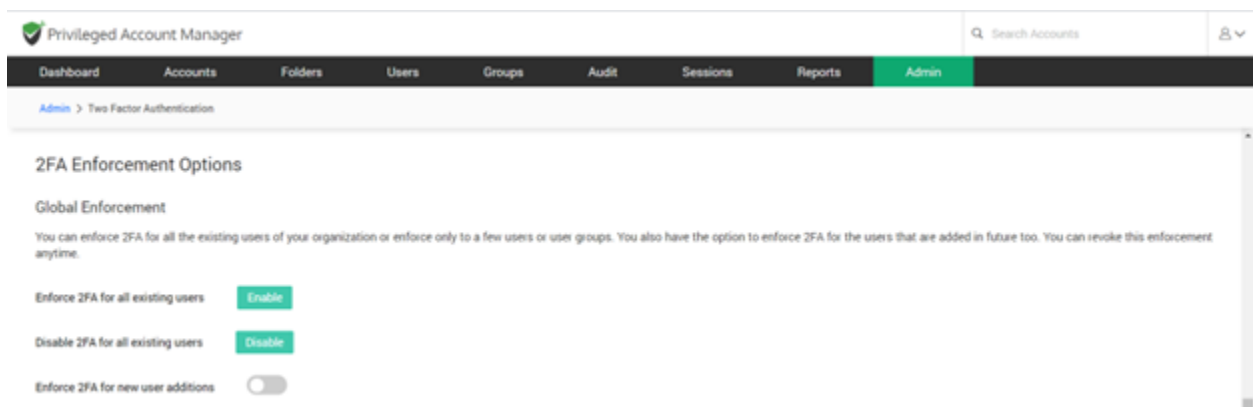
By default, YubiKey generates slot 1 passcode for NFC configured mobile devices. You can set slot 2 passcodes as default by changing the setting from slot 1 to slot 2 using the Yubikey Personalization Tool.

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

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

Global 2FA Enforcement

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

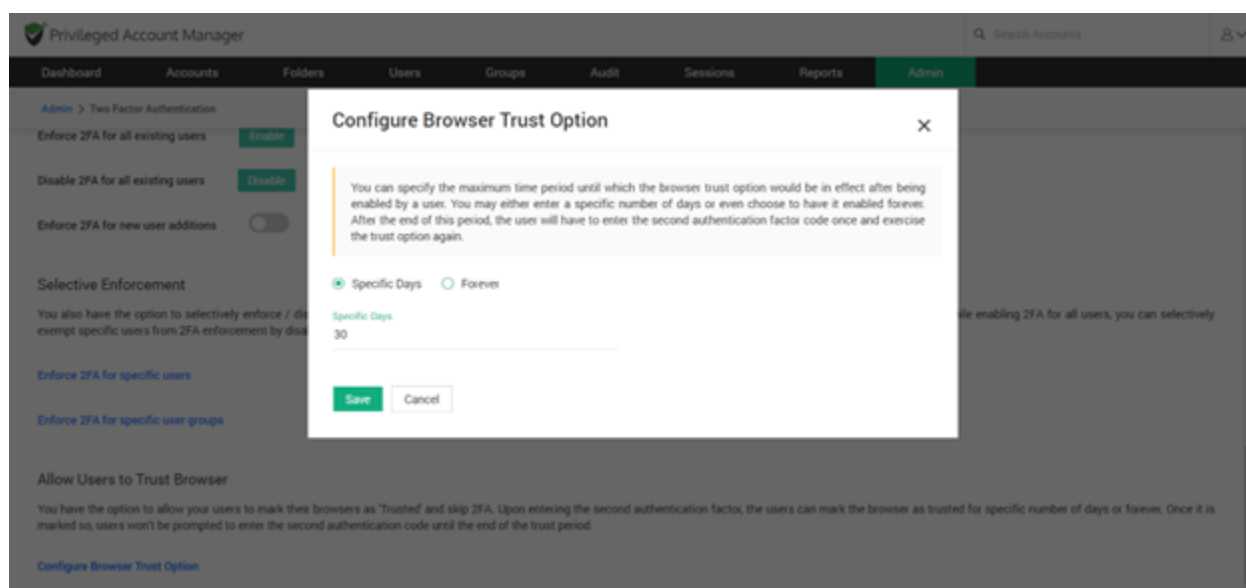


Selective 2FA Enforcement

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

Allow Users to Trust Browser

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



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

Radius Authentication

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

To configure RADIUS authentication,

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

Admin > RADIUS Server Settings

Configure RADIUS Server Settings

You can integrate RADIUS server or any RADIUS-compliant two-factor authentication system like OneSpan Digipass, RSA SecurID, Swivel Secure etc. for the second factor authentication. You need to configure RADIUS server details below for the integration to take effect.

Identifier (name of the RADIUS-compliant authentication system) *	Authentication Protocol *
	PAP
Server Name (hostname or IP Address) *	Authentication Port *
	1812
Server Secret *	User Login Name Format (to be sent to RADIUS server) *
	LOGIN_NAME
Authentication Retries *	Authentication Timeout (in seconds) *
2	3

Email to SMS Gateway

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Email to SMS Gateway

Email to SMS Gateway Configuration

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

Display Name *

SMS Service Provider (Domain Name) *

☐ Prefix country code with the phone numbers of all users

To configure Email to SMS Gateway as an option,

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

DUO Authentication

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

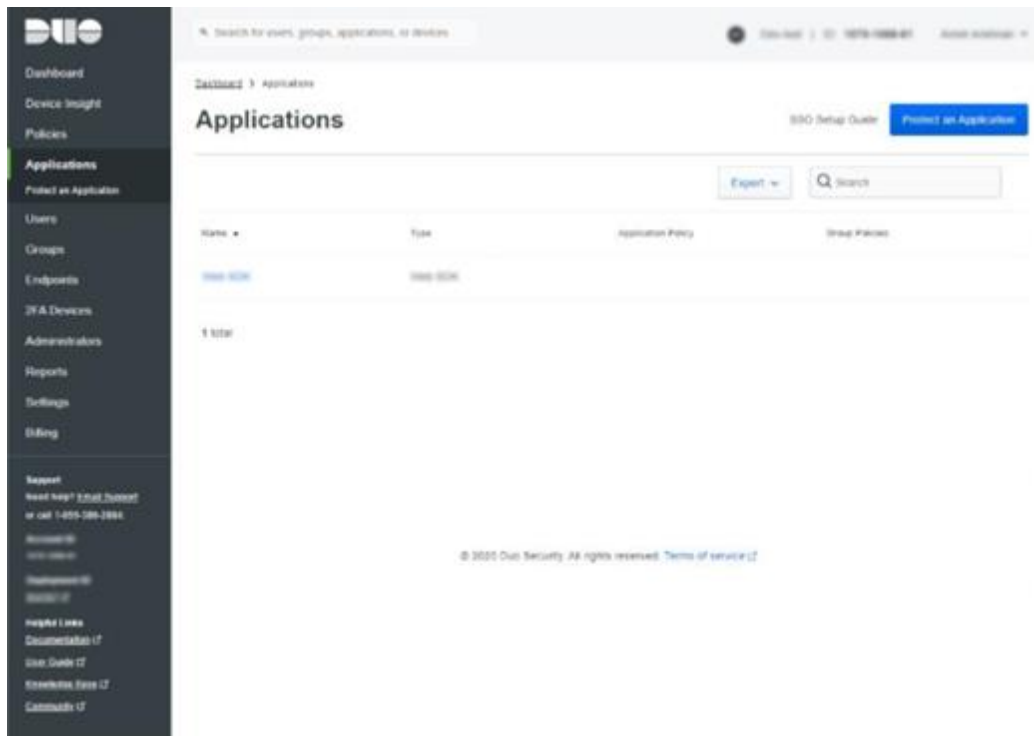
Prerequisite:

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

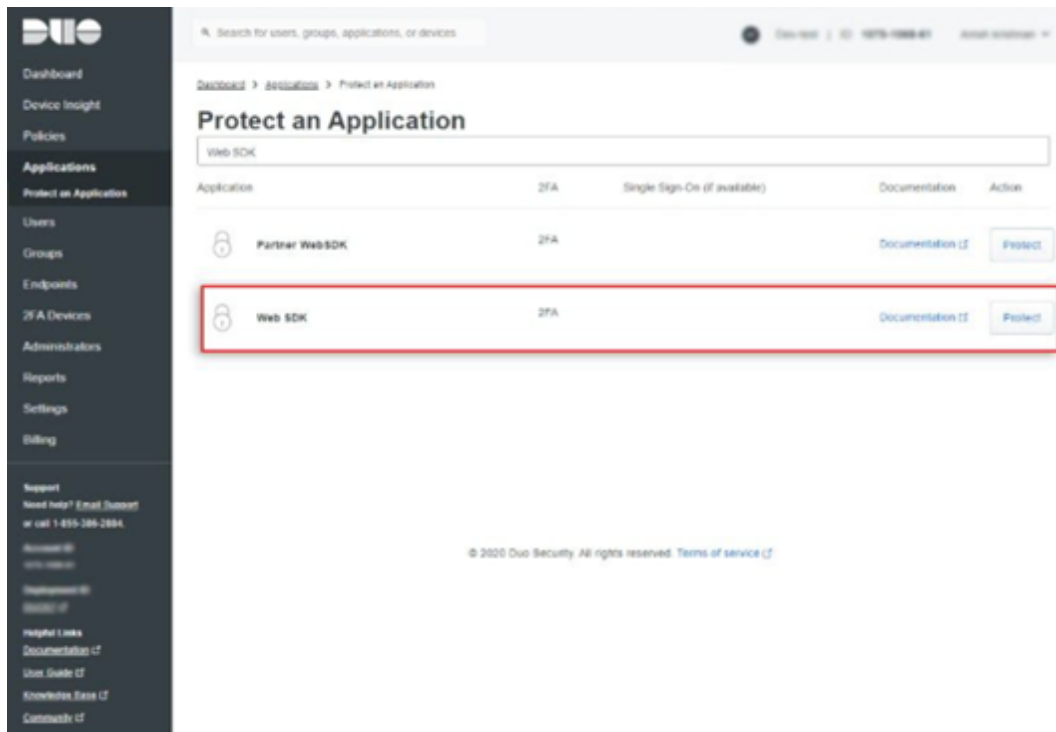
To enable Duo authentication in Securden, you need to carry out certain configuration steps in both Duo and Securden.

Step 1: Configurations in Duo

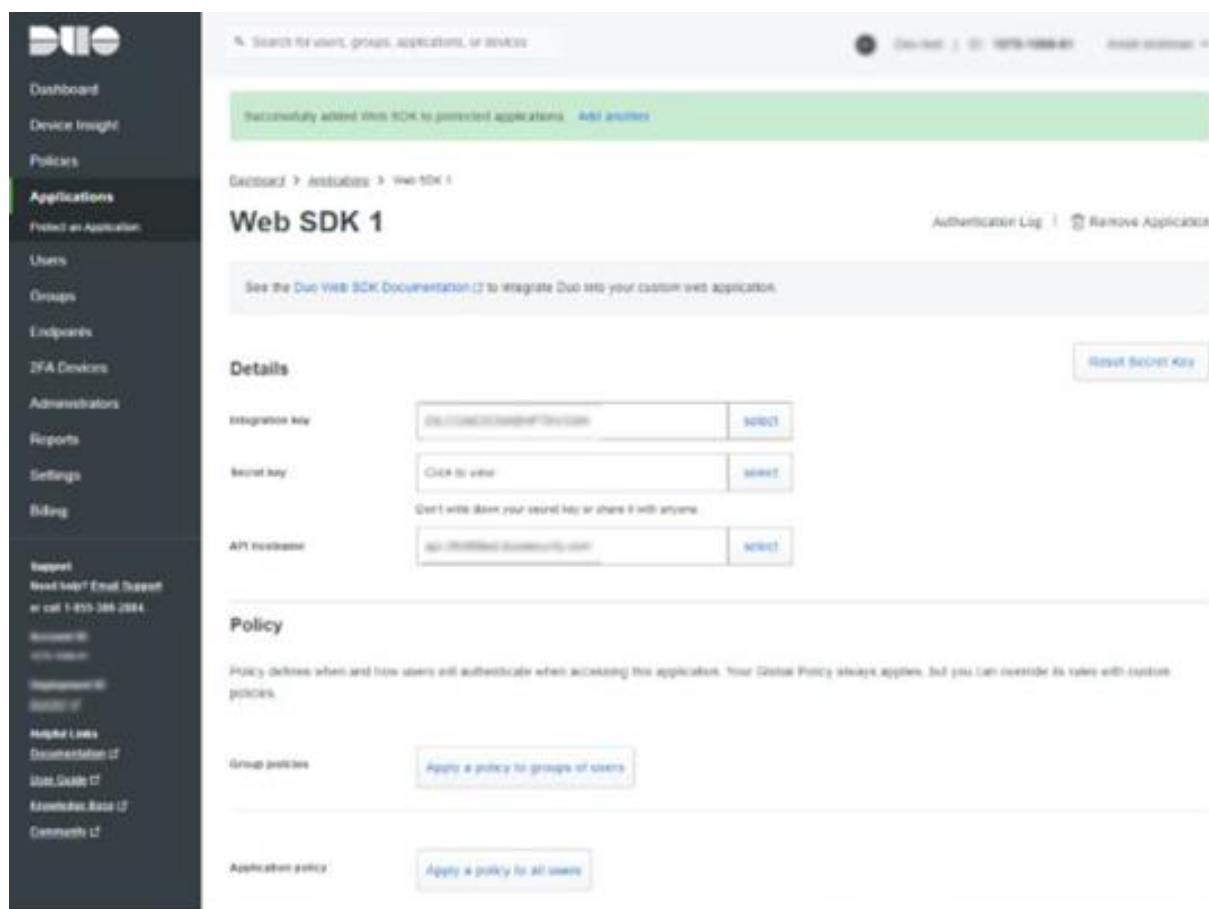
1. You should have an account with Duo and log into the Duo Admin Panel. Securden has to be added as a new application.
2. Click Applications in the left sidebar, and in the GUI that opens, click the **Protect an Application** button. Alternatively, you can click the **Protect an Application** submenu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



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



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



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

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

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

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

- **Deny access** - You can deny access to those who haven't enrolled with the duo. Users must be enrolled before attempting authentication.

The above steps complete the setup process in Duo.

Step 2: Configuration in Securden

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

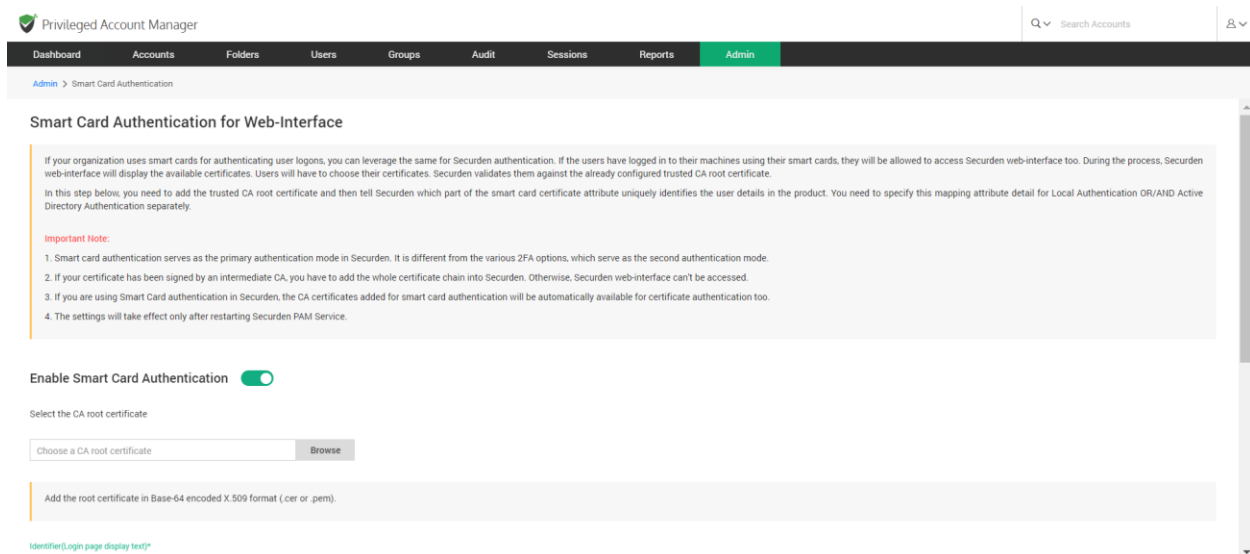
The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes links for Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin (which is highlighted). Below the navigation bar, the breadcrumb trail reads 'Admin > Duo Security'. The main heading is 'Configure Duo Security Authentication'. A note states: 'Securden integrates with Duo Security for two factor authentication. Once configured, users will be enforced to authenticate through Duo for accessing the web-interface. Pre-requisite: Before proceeding with the configuration steps below, you need to first carry out a few steps at Duo security for enabling the integration with Securden. Once you complete the steps in Duo, you will get an integration key, secret key, and API hostname, which you need to supply below. After configuring this, remember to enable Duo security authentication in 2FA settings page.' The form contains four input fields: 'Integration Key *', 'Secret Key *', 'API hostname *', and 'Custom Rule for Securden Login Name (optional)'. Each field has a copy icon to its right. At the bottom of the form are 'Save' and 'Cancel' buttons.

2. After entering the details, navigate to **Admin >> Authentication >> Two-factor Configuration** and select **Duo Security**.
3. Then Duo Security will now be used as the second-factor authentication for the users in Securden. The users may select two options for entering the second factor - to send push notifications to their mobile phones or to enter the code from the Duo mobile app.



Smart Card Authentication

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



To Enable Smart Card Authentication:

1. Navigate to **Admin >> Authentication >> Smart Card Authentication.**
2. Toggle the **Enable Smart Card Authentication** to on.

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

In the above step, you need to add the trusted CA root certificate and then tell Securden which part of the smart card certificate attribute uniquely identifies the user details in the product. You need to specify this mapping attribute detail separately for Local Authentication OR/AND Active Directory Authentication.

The screenshot shows the 'Admin > Smart Card Authentication' page in the Securden Privileged Account Manager. The interface includes a top navigation bar with tabs for Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin (which is active). A search bar for accounts is located in the top right. The main content area has a 'Choose a CA root certificate' section with a 'Browse' button. Below this is a text box for adding the root certificate in Base-64 encoded X.509 format. The 'Identifier(Login page display text)*' is set to 'Login through smart card'. Under 'Certificate Attribute and Securden User Identification', there are three sections: 'Attribute to retrieve from the CA-signed certificate*' with a dropdown menu, 'Local Authentication Users (Manually Added Users)' with a checkbox and an attribute dropdown, and 'Active Directory Users' with a checkbox and an attribute dropdown. At the bottom, there are 'Save' and 'Cancel' buttons.

Note:

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

Troubleshooting Tips

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

Solution:

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

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

Section 5: Account Management

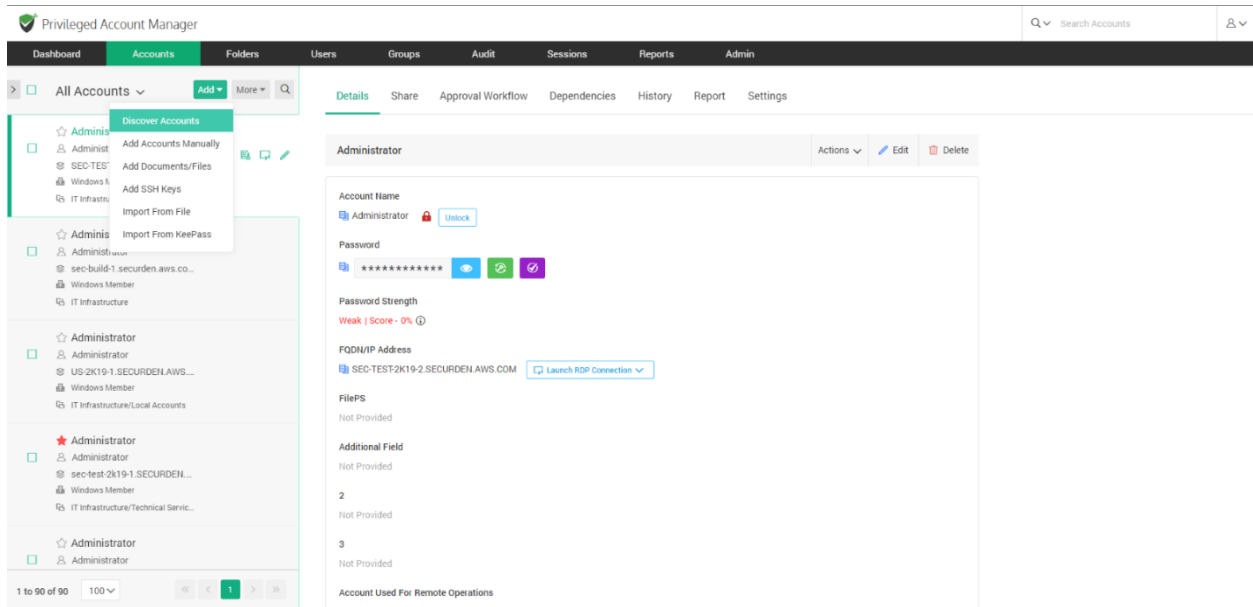
Securden provides a centralized credential vaulting facility in which you can add, remove, share, and monitor various privileged credentials that can be used to manage multiple privileged accounts in your organization. To manage the privileged credentials, you need to add them to the vault. You can discover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

Discovering Privileged Accounts

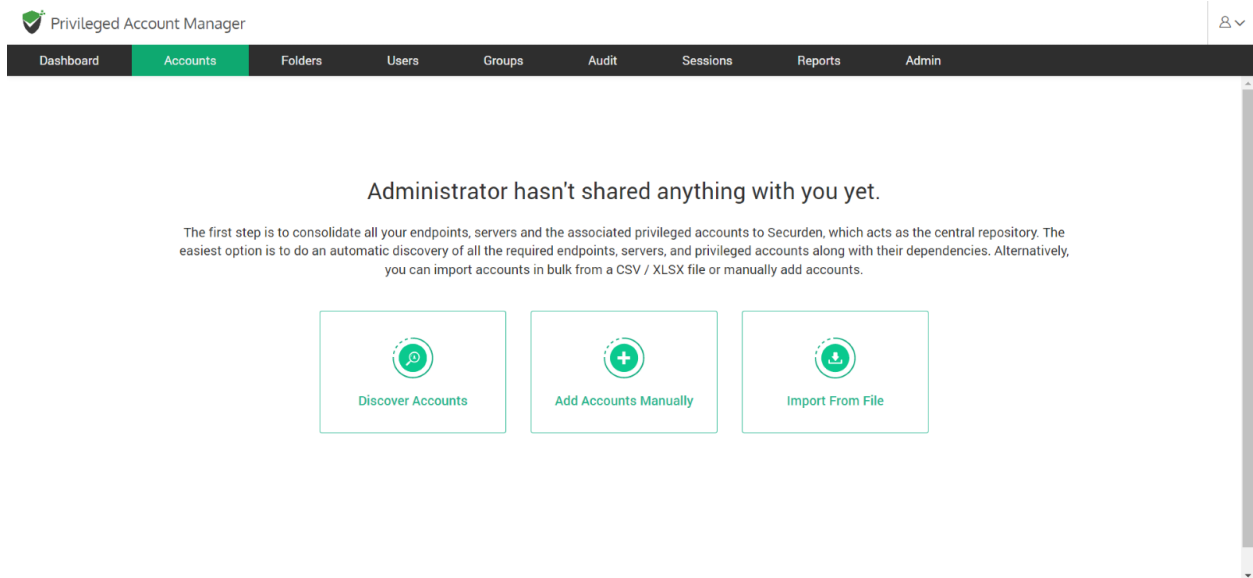
Once the users who are going to use Securden PAM are onboarded, the very first thing to do is add all the privileged accounts to PAM for centralized management.

One of the effective ways to accomplish this is to discover servers, databases, SSH devices, and network devices and the privileged accounts that are a part of those devices.

To run discovery, navigate to **Accounts >> Add >> Discover Accounts**.

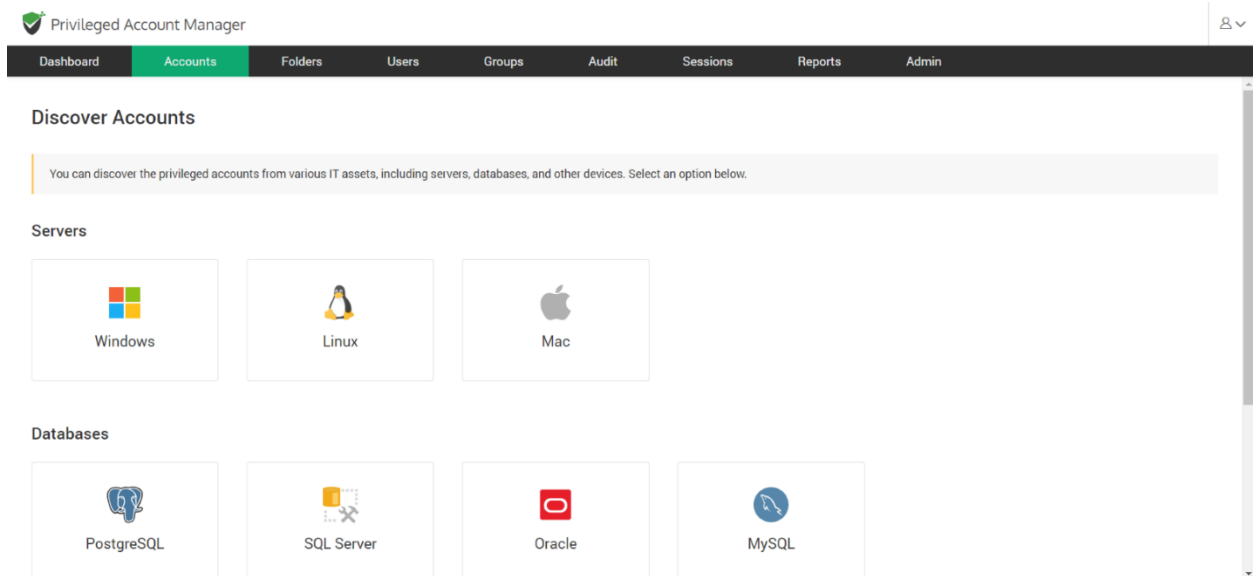


If your Securden instance doesn't have any account onboard, you can navigate to **Accounts >> Discover Accounts**.



You can run this discovery process on:

1. Servers running on Windows, Linux, and Mac platforms.
2. Databases such as PostgreSQL, MS SQL, Oracle, and MySQL.
3. Network devices such as Cisco IOS.



The process differs slightly for each type of device and the steps are explained below.

Running Discovery on Windows Servers

Prerequisites: To perform remote operations on Windows devices, you need to import your AD domain into Securden. This can be done separately or at the time of discovery. To connect to your domain, you must satisfy the following requirements.

1. Ports 389 (For Non-SSL) and port 636 (For SSL) must be open to Securden PAM.
2. AD Reachability – The active directory must remain connected to Securden PAM.
3. If the users are restricted from logging in from multiple computers, login permission should be allowed from the securden server also.

Securden scans the active directory in Windows servers to obtain the AD domain's OUs, Groups, and Computers. Along with them, the local admin accounts, domain accounts, and service accounts present on the servers are also obtained.

Once computers are discovered, Securden scans each device for the domain accounts used as service accounts to run services, scheduled tasks, and IIS App pools.

Accounts discovery is a two-step process. The very first step is to establish connectivity between Securden and the Active Directory. Then, the required OUs, groups, computers, and accounts can be selected and imported into Securden. The steps are explained in detail below.

Step 1: Connecting to the Active Directory Domain

To establish connectivity, you need to furnish details of the Active Directory domain. Navigate to **Admin >> Integrations >> Active Directory Domains**.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

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 IP Address / FQDN *

192.168.72.2

Secondary IP Addresses (Optional)

Select Remote Gateway

~None~

Connection Mode

☐ SSL

Supply Administrator Credentials

☐ Enter username and password ☒ Specify an account already stored in Securden

Account Type Address Title

Windows Domain Search Account Address Search Account Title

Next Cancel

FQDN/IP Address

To establish connectivity with the AD domain, you need to specify the FQDN/IP address of the domain. The FQDN/IP can be supplemented with secondary IP addresses to establish connectivity in cases where the primary addresses are not working.

Connection Mode

You can specify the mode of connection (SSL/Non-SSL) between Securden and the AD domain. If you select SSL mode, you need to ensure that the domain controller is serving over SSL in port 636. Additionally, the certificate of the domain controller should be signed by a certified CA. If the certificate is not signed by the CA, you can import all the certificates that are present in the root certificate chain (the certificate of domain controller and all the intermediate certificates if any).

Supply Administrator Credentials

You need to supply administrator credentials to enable Securden to scan the members in the domain. You may enter the username and password manually for the first time. The username and password specified will be stored in Securden for subsequent import attempts.

Note: AD domains can be added before running the accounts discovery process by using the AD integration option. To add the active directory domain, navigate to **Admin >> Integrations >> Active Directory Domains**.

Connecting to AD Domains on Secondary Networks

If you have configured a distributed deployment setup in Securden using an API-based application server, you can explicitly run the discovery on the secondary network to scan for devices and databases and obtain the accounts from them.

To establish connectivity between Securden and the AD domain, you can follow the same steps as above. Additionally, while establishing connectivity, you need to route the connection through the remote gateway associated with the API-based application server.

You may select the required gateway from the drop-down menu as shown below.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

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 *
172.31.1.11a

Secondary IP Addresses (Optional)

Select Remote Gateway

-None-

Searching...

-None-

New York Data Center

London DC

Belgium DC

SECURDEN-AWS/administrator [\[Modify\]](#)

connect to the active directory domain.

Next Cancel

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

Domain IP Address

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

Connection Mode

Specify the mode (SSL/non-SSL) through which Securden has to establish connection with the AD domain. If SSL mode is selected, the domain controller should be serving over SSL in port 636 and the certificate of the domain controller should have been signed by a CA. If the certificate of the domain controller is not signed by a certified CA, you need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the domain controller and all the intermediate certificates if any. For details, [click here](#).

Supply Administrator Credentials

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

Step 2: Discovering and Importing Accounts

Once the connection has been established between Securden and the AD Domain, you can select the required OUs, Groups, Computers, and Accounts available in the AD domain and import them into Securden.

You have the flexibility to choose any combination of the four options below and import them in a single easy step.

For example, if you want to discover accounts from an OU and a Group, first enter/browse and select the name of the OU, click **Discover**. Then go to the **Groups** tab, select/browse the name of the Group and click **Discover**. Verify your discovery details and finally click **Import**. Securden will fetch all accounts that are part of the OU and Group specified.

Importing Ous

Using this method, you can import all domain accounts and computers that are a part of the selected OUs.

You can use the search function to add specific OUs. Specify the search term and click **Discover**.

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

OU Groups Computers Accounts

Fetch all domain accounts and computers that are part of a specific OU/OUs. Securden also fetches dependencies and local accounts from all computers of the selected OU/OUs. Enter your search text. Then click the 'Discover' button.

Q Search OUs Discover Browse OU Tree and Select

Verify the Objects Selected for Discovery

Verify your search results before proceeding to importing them to Securden.

When importing accounts, should they be moved under a specific folder?

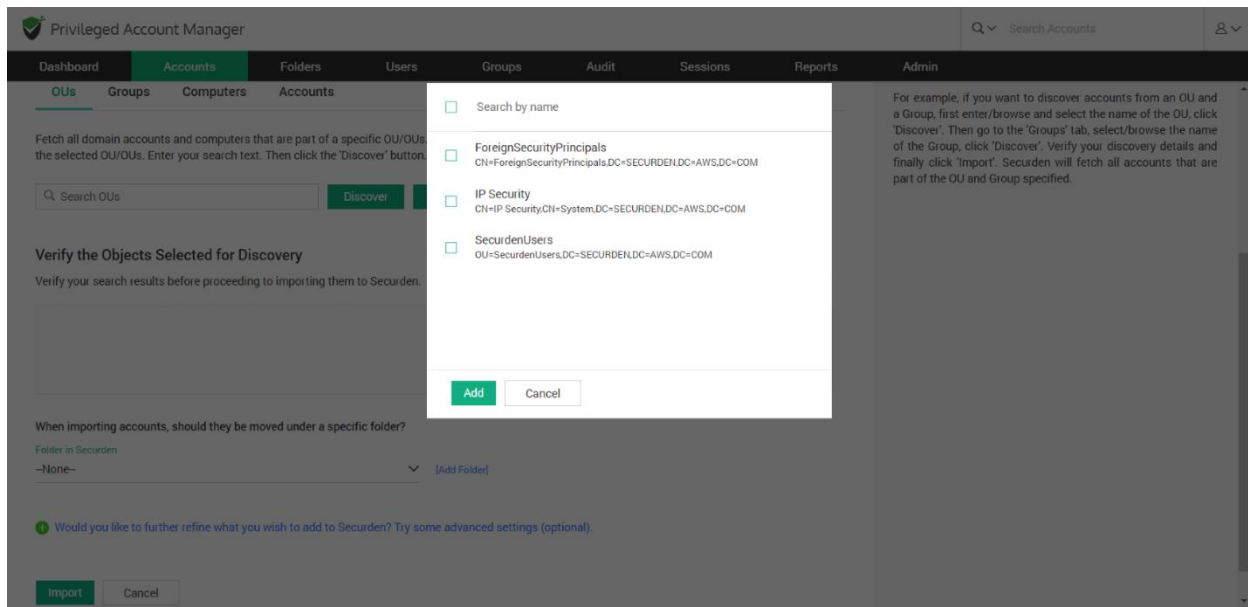
Folder in Securden
-None- [Add Folder]

Would you like to further refine what you wish to add to Securden? Try some advanced settings (optional).

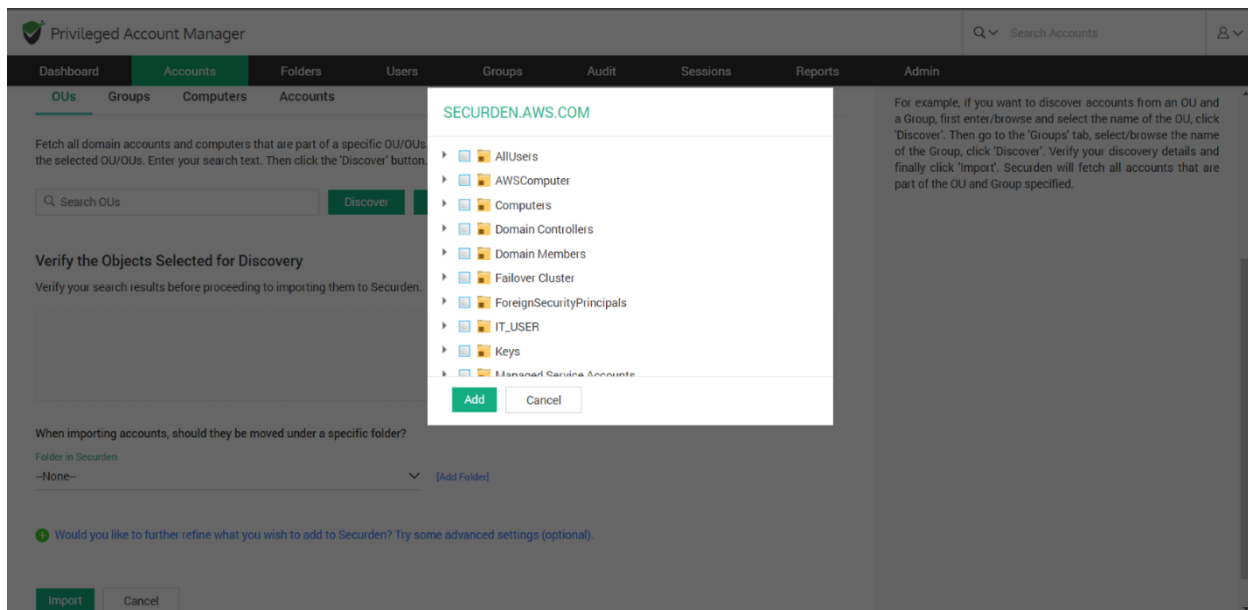
Import Cancel

For example, if you want to discover accounts from an OU and a Group, first enter/browse and select the name of the OU, click 'Discover'. Then go to the 'Groups' tab, select/browse the name of the Group, click 'Discover'. Verify your discovery details and finally click 'Import'. Securden will fetch all accounts that are part of the OU and Group specified.

Select the required OUs from the search result and click **Add**.



Alternatively, you can browse the OU tree and select the required OUs.



Once you have selected the required OUs, click **Add**.

Importing Groups

Using this method, you can import all domain accounts and computers that are a part of the selected groups.

You can use the search function to add specific groups. Specify the search term and click **Discover**.

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

OUs Groups Computers Accounts

Fetch all domain accounts and computers that are part of a specific group(s). Securden also fetches dependencies and local accounts from all computers of the selected group(s). Enter your search text. Then click the 'Discover' button.

Q Search Groups Discover Browse Groups and Select

Verify the Objects Selected for Discovery
Verify your search results before proceeding to importing them to Securden.

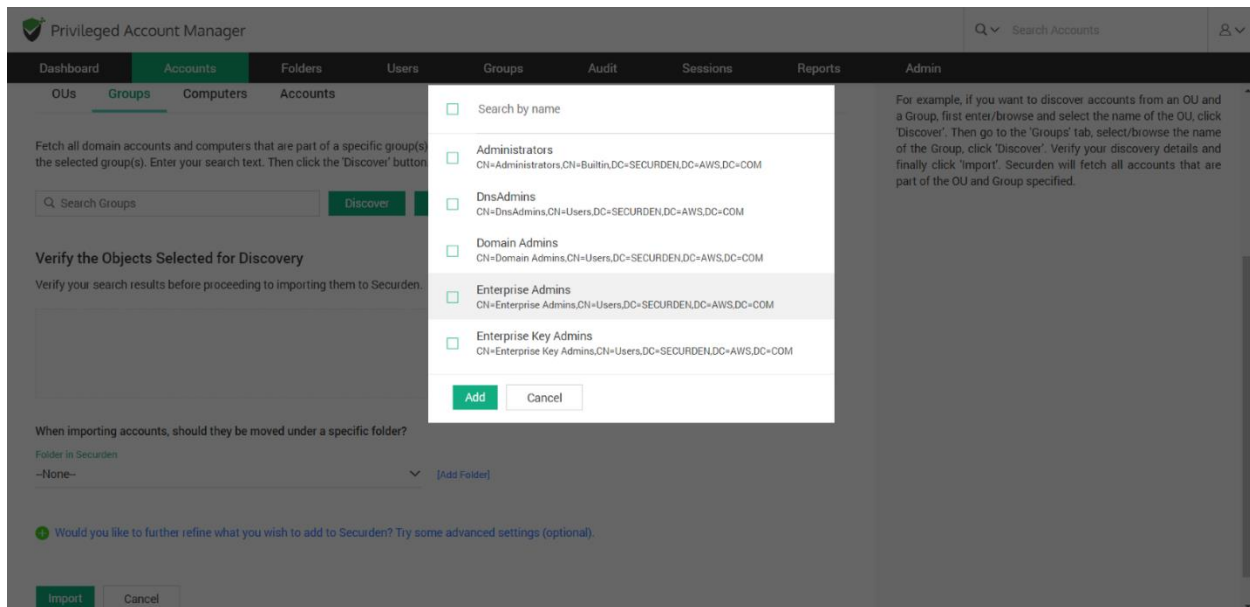
When importing accounts, should they be moved under a specific folder?
Folder in Securden
--None-- [Add Folder]

+ Would you like to further refine what you wish to add to Securden? Try some advanced settings (optional).

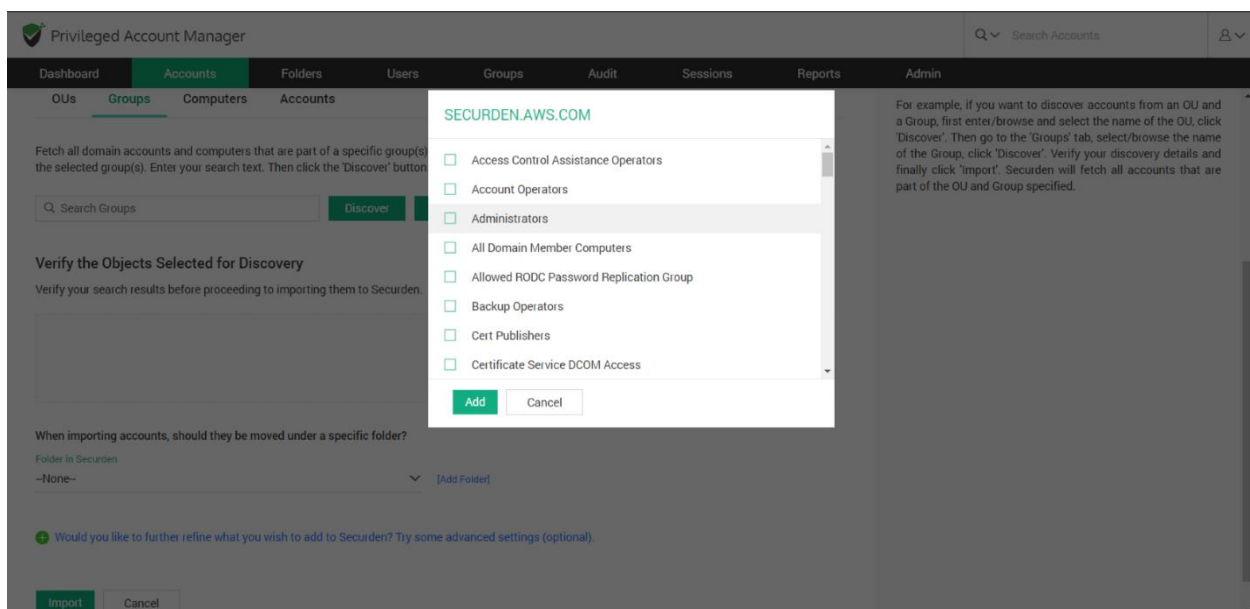
Import Cancel

For example, if you want to discover accounts from an OU and a Group, first enter/browse and select the name of the OU, click 'Discover'. Then go to the 'Groups' tab, select/browse the name of the Group, click 'Discover'. Verify your discovery details and finally click 'Import'. Securden will fetch all accounts that are part of the OU and Group specified.

Select the required groups from the search result and click **Add**.



Alternatively, you can browse different groups in the AD domain and select the required groups.



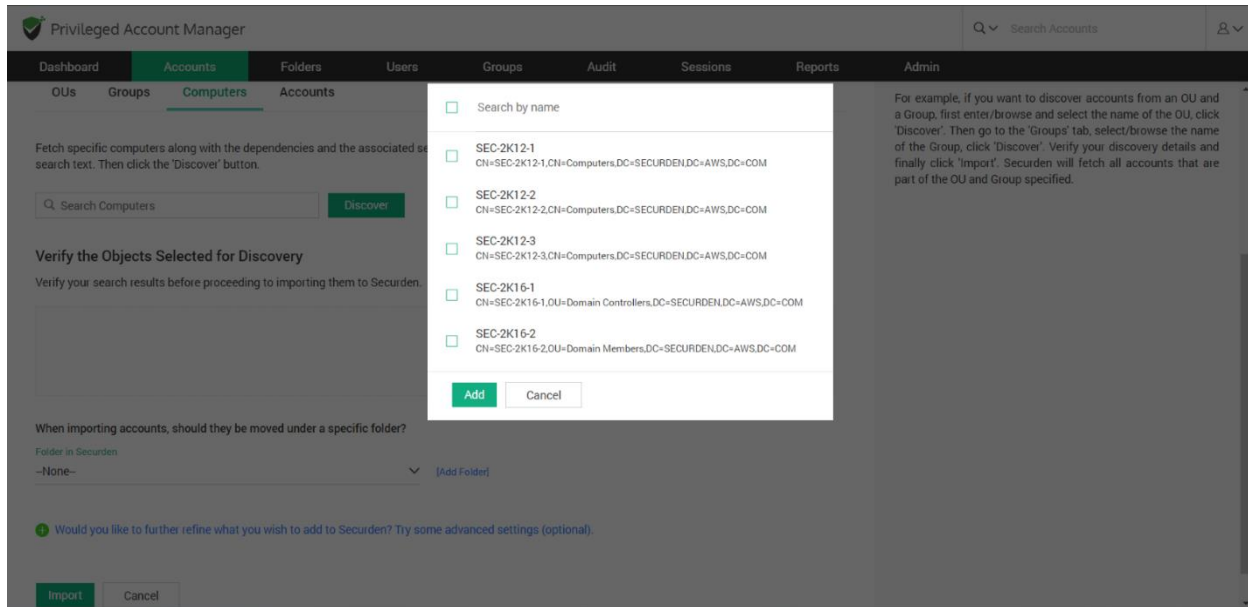
Once you have selected the required groups, click **Add**.

Importing Computers

You can search and select specific computers from your AD domain. The selected devices, local accounts, service accounts and their dependencies contained in each device will be imported into Securden.

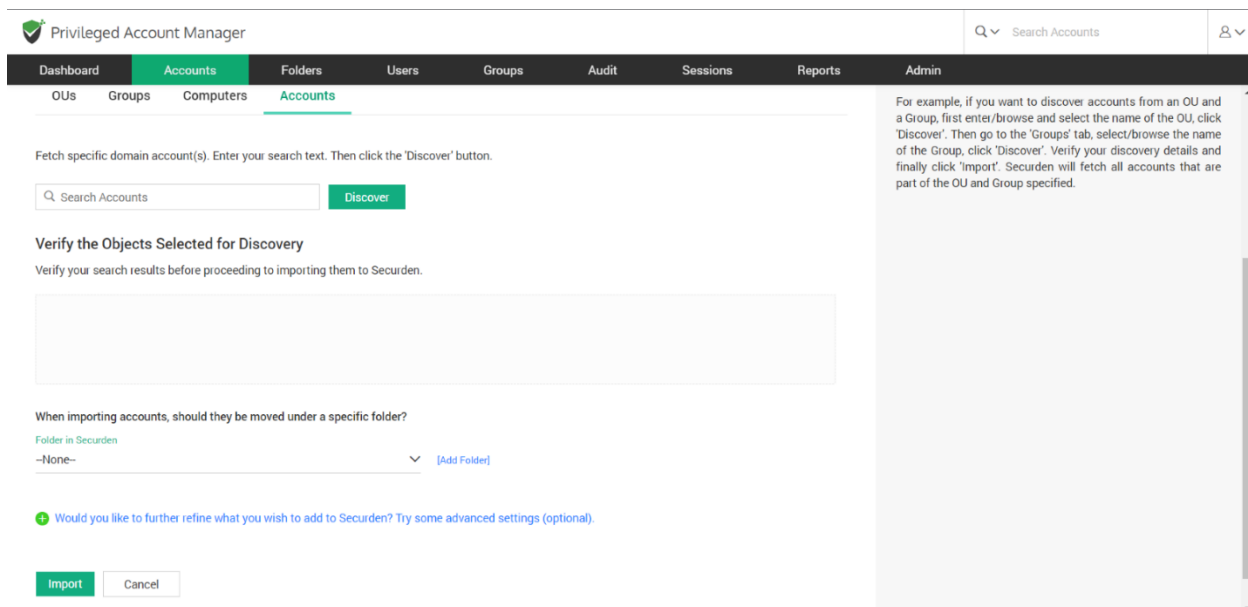
The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (selected), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. Below this, the 'Accounts' section has sub-tabs: 'OUs', 'Groups', 'Computers' (selected), and 'Accounts'. The main content area is titled 'Fetch specific computers along with the dependencies and the associated service accounts. Optionally, you can discover the local accounts too. Enter your search text. Then click the 'Discover' button.' It features a search input field labeled 'Search Computers' and a green 'Discover' button. Below this is a section 'Verify the Objects Selected for Discovery' with a note 'Verify your search results before proceeding to importing them to Securden.' and a large empty box for results. Further down, a question asks 'When importing accounts, should they be moved under a specific folder?' with a dropdown menu currently showing '-None-' and an '[Add Folder]' link. A green plus icon and text suggest further refinement: 'Would you like to further refine what you wish to add to Securden? Try some advanced settings (optional).' At the bottom are 'Import' and 'Cancel' buttons. A right-hand sidebar contains a search bar 'Search Accounts' and a user profile icon. A detailed help text on the right explains the discovery process: 'For example, if you want to discover accounts from an OU and a Group, first enter/browse and select the name of the OU, click 'Discover'. Then go to the 'Groups' tab, select/browse the name of the Group, click 'Discover'. Verify your discovery details and finally click 'Import'. Securden will fetch all accounts that are part of the OU and Group specified.'

You need to specify the search term and click **Discover**.

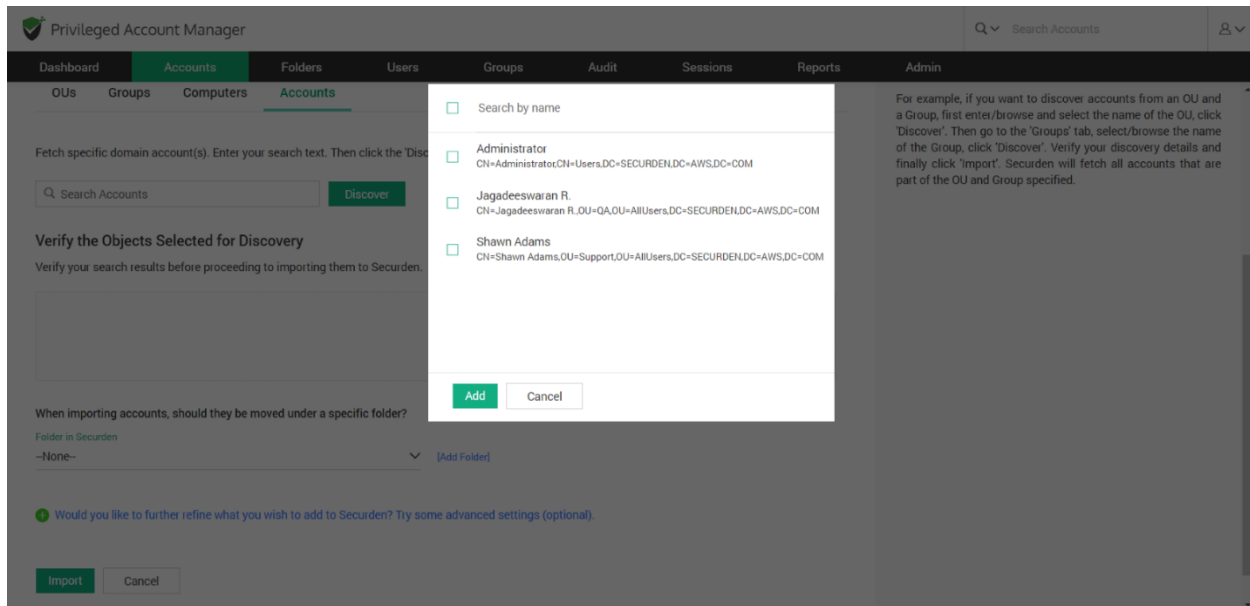


Importing Specific Accounts

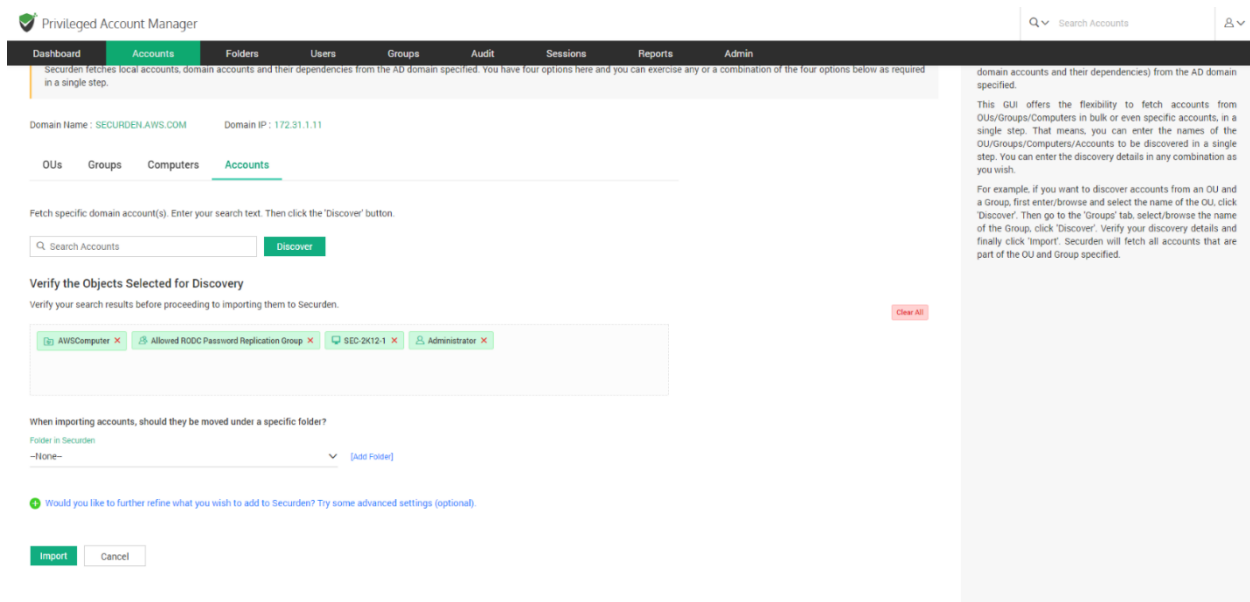
You can search and select specific domain accounts from your AD domain. You need to specify the search term and click **Discover**.



You can select the required domain accounts from the search result and click **Add**.



Selected OUs, Groups, Computers, and Accounts will be displayed in the field named **Verify the Objects Selected for Discovery**.



You can check whether all the required objects have been added here.

Add Imported Accounts to a Folder

While importing accounts, you can specify a Folder to which all the imported accounts will be added. You can click the drop-down menu and select the required folder.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Securden fetches local accounts, domain accounts and their dependencies from the AD domain specified. You have four options here and you can exercise any or a combination of the four options below as required in a single step.

Domain Name : SECURDEN.AWS.COM Domain IP : 172.31.1.11

OU's Groups Computers Accounts

Fetch specific domain account(s). Enter your search text. Then click the 'Discover' button.

Search Accounts Discover

Search

- None-
- IT Infrastructure
 - API Test
 - Local Accounts
 - Open Connection
 - Inforce

-None- [Add Folder]

Would you like to further refine what you wish to add to Securden? Try some advanced settings (optional).

Import Cancel

domain accounts and their dependencies) from the AD domain specified.

This GUI offers the flexibility to fetch accounts from OUs/Groups/Computers in bulk or even specific accounts, in a single step. That means, you can enter the names of the OUs/Groups/Computers/Accounts to be discovered in a single step. You can enter the discovery details in any combination as you wish.

For example, if you want to discover accounts from an OU and a Group, first enter/browse and select the name of the OU, click 'Discover'. Then go to the 'Groups' tab, select/browse the name of the Group, click 'Discover'. Verify your discovery details and finally click 'Import'. Securden will fetch all accounts that are part of the OU and Group specified.

If you want to add all the imported accounts to a new folder, you can create one by clicking **[Add Folder]**. You need to specify the folder attributes before saving.

Advanced Settings

These settings provide granular options to refine the objects imported to Securden.

The screenshot shows the 'Accounts' page in the Securden Privileged Account Manager. The interface includes a top navigation bar with tabs for Dashboard, Accounts (selected), Folders, Users, Groups, Audit, Sessions, Reports, and Admin. Below the navigation bar, there's a search bar and a 'Search Accounts' button. The main content area is titled 'Accounts' and contains a section for 'Fetch specific domain account(s)'. It includes a text input for 'Search Accounts' and a 'Discover' button. Below this, there's a 'Verify the Objects Selected for Discovery' section with a list of selected objects: AWSComputer, Allowed RODC Password Replication Group, SEC-2K12-1, and Administrator. A 'Clear All' button is next to the list. At the bottom, there's a dropdown menu for 'Folder in Securden' set to 'None', with an 'Add Folder' link. A note at the bottom asks if the user wants to further refine what they wish to add to Securden, with a link to 'Try some advanced settings (optional)'. An 'Import' button is at the bottom left.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Securden fetches local accounts, domain accounts and their dependencies from the AD domain specified. You have four options here and you can exercise any or a combination of the four options below as required in a single step.

Domain Name : SECURDEN.AWS.COM Domain IP : 172.31.1.11

OUs Groups Computers Accounts

Fetch specific domain account(s). Enter your search text. Then click the 'Discover' button.

Search Accounts Discover

Verify the Objects Selected for Discovery

Verify your search results before proceeding to importing them to Securden.

AWSComputer X Allowed RODC Password Replication Group X SEC-2K12-1 X Administrator X Clear All

When importing accounts, should they be moved under a specific folder?

Folder in Securden

None Add Folder

Would you like to further refine what you wish to add to Securden? Try some advanced settings (optional)

Import Cancel

domain accounts and their dependencies) from the AD domain specified.

This GUI offers the flexibility to fetch accounts from OUs/Groups/Computers in bulk or even specific accounts, in a single step. That means, you can enter the names of the OU/Groups/Computers/Accounts to be discovered in a single step. You can enter the discovery details in any combination as you wish.

For example, if you want to discover accounts from an OU and a Group, first enter/browse and select the name of the OU, click 'Discover'. Then go to the 'Groups' tab, select/browse the name of the Group, click 'Discover'. Verify your discovery details and finally click 'Import'. Securden will fetch all accounts that are part of the OU and Group specified.

Each setting is explained below.

What would you like to do when importing accounts?

When importing accounts, you have the option to generate and assign passwords to accounts after they are added to Securden.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Advanced Settings (optional)

What would you like to do when importing accounts?

- ☐ Randomize passwords of all accounts
- ☐ Randomize all passwords except that of service accounts
- ☒ Use username itself as password

What would you like to do with subgroups when importing a group?

- ☒ Include domain members of all subgroups to the group being imported (Members of subgroups will be imported; but subgroup structure will not be retained in Securden)
- ☐ Ignore subgroups. Import only the members of the first level group

What would you like to happen for domain accounts/computers when importing specific OUs / groups?

- ☐ Import only the domain accounts of the selected OUs / groups
- ☐ Import only the computers of the selected OUs / groups
- ☒ Import both
- ☐ Import none

What would you like to do when importing local accounts from computers?

- ☐ Import only 'Administrator' accounts
- ☒ Import 'All' accounts
- ☐ Import none

You can choose to

1. Randomize passwords of all accounts.

If you choose this option, passwords of all accounts will be randomized upon importing. The passwords assigned will be compliant with the default password policy in place at that time.

2. Randomize passwords for all accounts except service accounts.

If you choose this option, passwords of all accounts except service accounts will be randomized upon importing. The passwords assigned will be compliant with the default password policy in place at that time.

3. Use username as password.

If you choose this option, the username of the imported domain accounts will be used as the password for the account in Securden.

What would you like to do with subgroups when importing a group?

By default, when importing groups and OUs, Securden automatically discovers and imports all subgroups and their member accounts.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Advanced Settings (optional)

What would you like to do when importing accounts?

- ☐ Randomize passwords of all accounts
- ☐ Randomize all passwords except that of service accounts
- ☒ Use username itself as password

What would you like to do with subgroups when importing a group?

- ☒ Include domain members of all subgroups to the group being imported (Members of subgroups will be imported; but subgroup structure will not be retained in Securden)
- ☐ Ignore subgroups. Import only the members of the first level group

What would you like to happen for domain accounts/computers when importing specific OUs / groups?

- ☐ Import only the domain accounts of the selected OUs / groups
- ☐ Import only the computers of the selected OUs / groups
- ☒ Import both
- ☐ Import none

What would you like to do when importing local accounts from computers?

- ☐ Import only "Administrator" accounts
- ☒ Import "All" accounts
- ☐ Import none

You can choose to

1. Include domain members of all subgroups to the group being imported.

If you choose this option, the domain accounts of all subgroups of the selected group will be imported but the domain accounts will become the member of the parent group.

2. Ignore subgroups. Import only the members of the first group.

If you choose this option, only the members of the first level group will be imported. All the member accounts of the subgroups will be ignored.

What would you like to happen to domain accounts/computers when importing specific OUs/groups?

By default, Securden discovers and imports all domain accounts and computers when importing an OU or a Group.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (selected), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar labeled 'Search Accounts' is on the right. A modal dialog is open with the title 'What would you like to happen for domain accounts/computers when importing specific OUs / groups?'. It contains three radio button options: 'Import only the domain accounts of the selected OUs / groups', 'Import only the computers of the selected OUs / groups', and 'Import both' (which is selected). Below this, there are two sections for local accounts: 'What would you like to do when importing local accounts from computers?' with options 'Import only 'Administrator' accounts', 'Import 'All' accounts' (selected), and 'Import none'; and 'When importing domain accounts, what should be the account type?' with a dropdown menu showing 'Windows Domain Account Type' and 'Windows Domain'. A similar section for 'When importing Windows member accounts, what should be the account type?' shows 'Windows Member Account Type' and 'Windows Member'. At the bottom of the dialog are 'Import' and 'Cancel' buttons.

You can choose to

1. Import only the domain accounts of the selected OUs/Groups

If you choose this option, only domain accounts present in the selected OUs and Groups will be imported. The computers present in the OUs/Groups will not be imported.

2. Import only the computers of the selected OUs/Groups

If you choose this option, only the computers present in the selected OUs/Groups will be imported. The domain accounts present in the OUs/Groups will not be imported.

3. *Import both*

If you choose this option, both the computers and the domain accounts present in the selected OUs/Groups will be imported.

4. *Import None*

If you choose this option, neither the computers nor the domain accounts present in the selected OUs/Groups will be imported.

What would you like to do when importing local accounts from computers?

By default, when importing computers, Securden automatically discovers all local accounts on each computer and imports them for management.

The screenshot shows the Securden Privileged Account Manager web interface. The top navigation bar includes a search bar and a user profile icon. The main menu has tabs for Dashboard, Accounts (selected), Folders, Users, Groups, Audit, Sessions, Reports, and Admin. The 'Accounts' tab is active, displaying a form with the following sections:

- What would you like to happen for domain accounts/computers when importing specific OUs / groups?**
 - ☐ Import only the domain accounts of the selected OUs / groups
 - ☐ Import only the computers of the selected OUs / groups
 - ☒ Import both
 - ☐ Import none
- What would you like to do when importing local accounts from computers?**
 - ☐ Import only 'Administrator' accounts
 - ☒ Import 'All' accounts
 - ☐ Import none
- When importing domain accounts, what should be the account type?**
 - Windows Domain Account Type
 - Windows Domain
- When importing Windows member accounts, what should be the account type?**
 - Windows Member Account Type
 - Windows Member

At the bottom of the form are two buttons: 'Import' (highlighted in green) and 'Cancel'.

You can choose to

1. Import only Administrator Accounts

If you choose this option, only the local administrator accounts present on computers will be imported. The standard user accounts will be ignored.

2. Import All Accounts

If you choose this option, all local administrator accounts and standard accounts will be imported.

3. Import None

If you choose this option, only the computers will be imported. The local accounts will be ignored.

When importing domain accounts, what should be the account type?

You can select the Account type for the domain accounts imported from the AD domain. By default, it is set to **Windows Domain**.

The screenshot shows the 'Privileged Account Manager' interface. The 'Accounts' tab is selected in the top navigation bar. Below the navigation bar, there are three sections of configuration options:

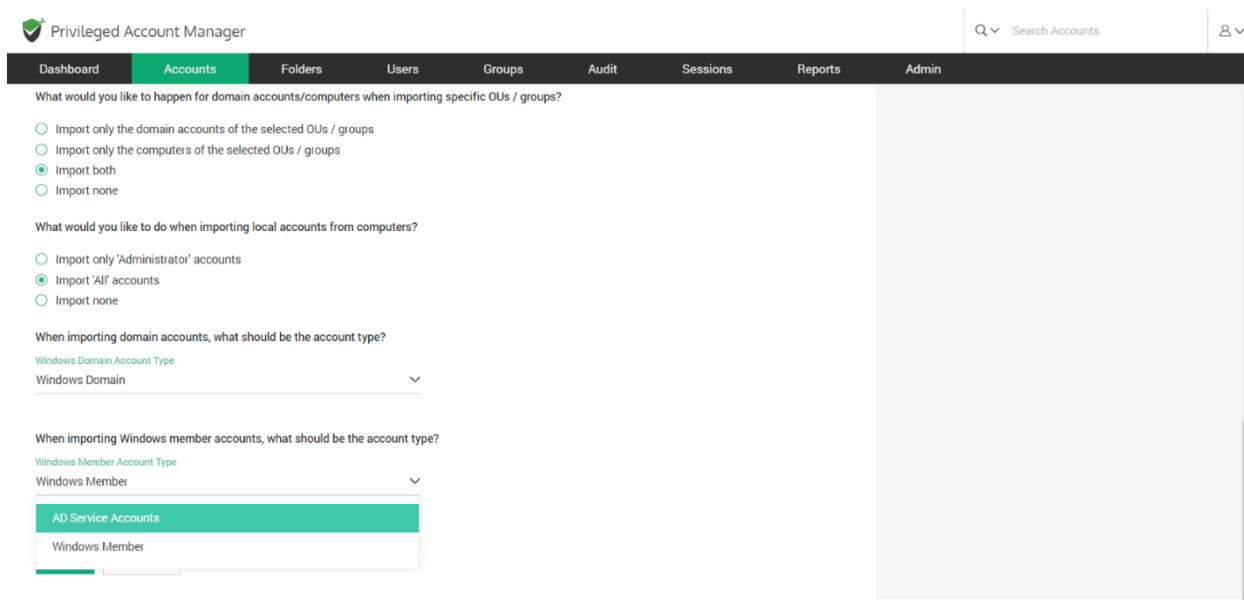
- What would you like to happen for domain accounts/computers when importing specific OUs / groups?**
 - ☐ Import only the domain accounts of the selected OUs / groups
 - ☐ Import only the computers of the selected OUs / groups
 - ☒ Import both
 - ☐ Import none
- What would you like to do when importing local accounts from computers?**
 - ☐ Import only 'Administrator' accounts
 - ☒ Import 'All' accounts
 - ☐ Import none
- When importing domain accounts, what should be the account type?**
 - Windows Domain Account Type
 - Windows Domain
 - Cisco Switch
 - Non-Domain Asset
 - SSH Connections
 - Windows Domain
 - windows domain account type - test

At the bottom of the form, there are 'Import' and 'Cancel' buttons.

If you want to assign a different account type, select one from the drop-down menu.

When importing Windows member accounts, what should be the account type?

You can select the Account type for the member accounts imported from the AD domain. By default, it is set to **Windows Member**.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

What would you like to happen for domain accounts/computers when importing specific OUs / groups?

- ☐ Import only the domain accounts of the selected OUs / groups
- ☐ Import only the computers of the selected OUs / groups
- ☒ Import both
- ☐ Import none

What would you like to do when importing local accounts from computers?

- ☐ Import only 'Administrator' accounts
- ☒ Import 'All' accounts
- ☐ Import none

When importing domain accounts, what should be the account type?

Windows Domain Account Type

Windows Domain

When importing Windows member accounts, what should be the account type?

Windows Member Account Type

Windows Member

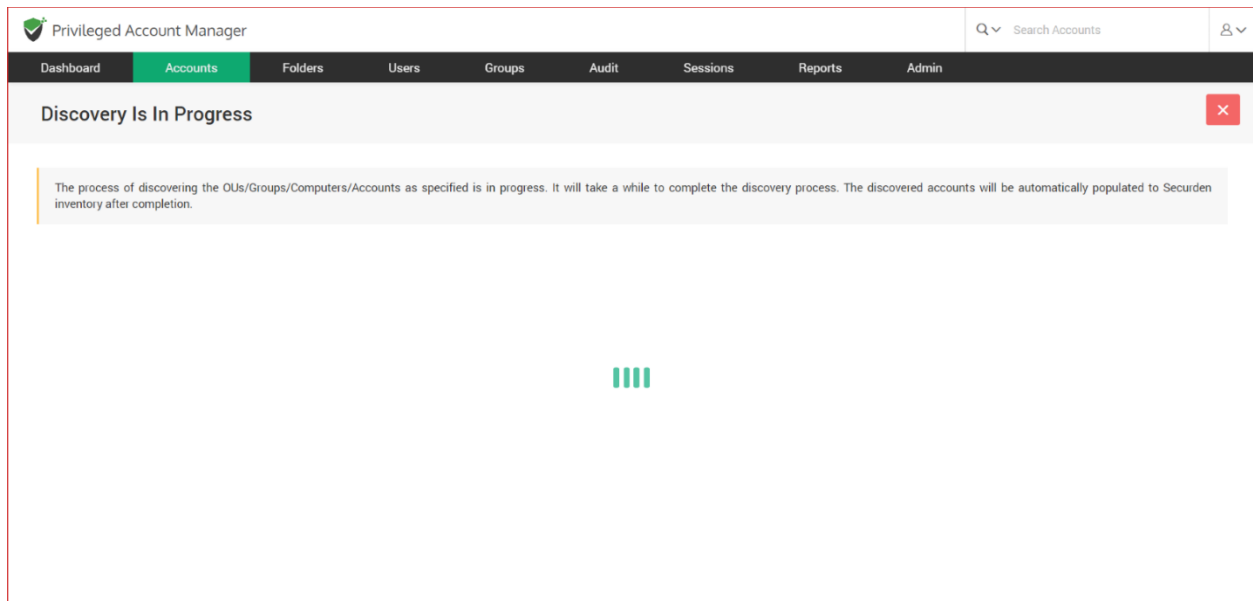
AD Service Accounts

Windows Member

If you want to assign a different account type, select one from the drop-down menu.

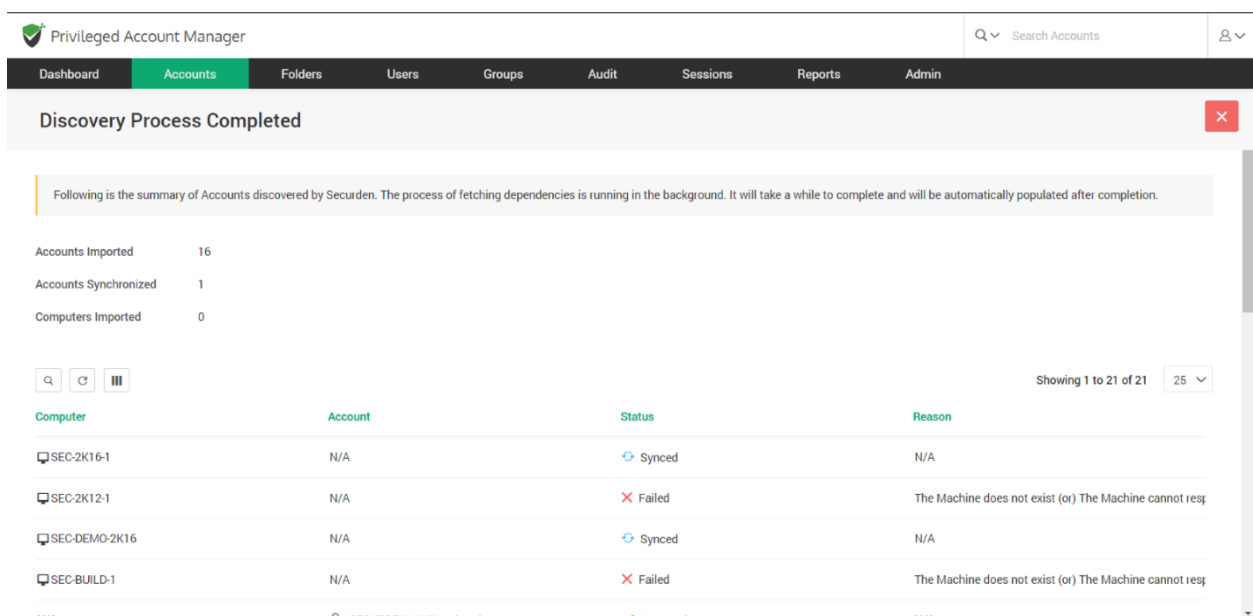
Important: If the selected account type doesn't have the appropriate attributes, then when importing, data loss is expected. Please ensure the selected account type has all the attributes required to avoid data loss.

Once the options are chosen, click **Import**. The discovery process will commence.



The screenshot shows the 'Privileged Account Manager' interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar on the right says 'Search Accounts'. Below the navigation bar, a message box titled 'Discovery Is In Progress' with a red close button contains the text: 'The process of discovering the OUs/Groups/Computers/Accounts as specified is in progress. It will take a while to complete the discovery process. The discovered accounts will be automatically populated to Securden inventory after completion.' Below this message, there is a large green progress bar consisting of four vertical bars of increasing height.

The discovery process typically takes some time. Once the process is over, a summary report of the process will be displayed.



The screenshot shows the 'Privileged Account Manager' interface after the discovery process is complete. The top navigation bar is the same. Below the navigation bar, a message box titled 'Discovery Process Completed' with a red close button contains the text: 'Following is the summary of Accounts discovered by Securden. The process of fetching dependencies is running in the background. It will take a while to complete and will be automatically populated after completion.'

Below the message box, the following summary is displayed:

Accounts Imported	16
Accounts Synchronized	1
Computers Imported	0

Below the summary, there are icons for search, refresh, and a list view. On the right, it says 'Showing 1 to 21 of 21' with a dropdown menu set to '25'.

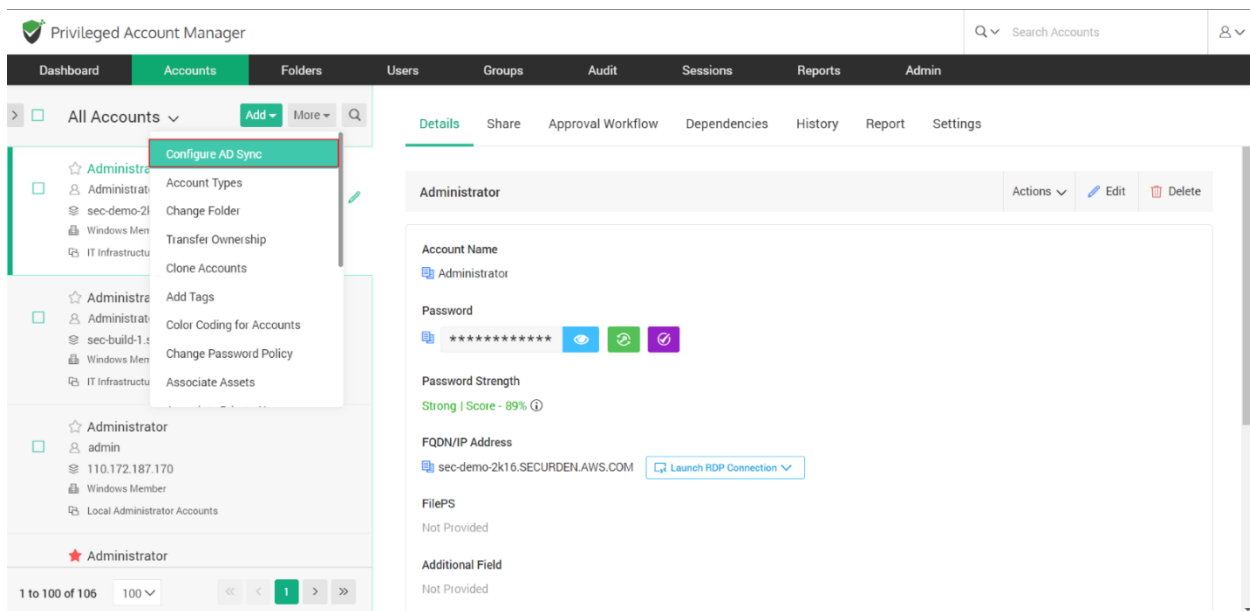
Computer	Account	Status	Reason
SEC-2K16-1	N/A	Synced	N/A
SEC-2K12-1	N/A	Failed	The Machine does not exist (or) The Machine cannot resp
SEC-DEMO-2K16	N/A	Synced	N/A
SEC-BUILD-1	N/A	Failed	The Machine does not exist (or) The Machine cannot resp

Details such as the number of accounts and computers imported, and accounts synchronized are displayed.

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.



In the window that opens, select **Synchronize Once** or **Synchronize Periodically**.

If you choose to synchronize once, you need to specify the time and date for scheduling the activity.

The screenshot displays the 'Privileged Account Manager' web interface. The top navigation bar includes 'Dashboard', 'Accounts' (selected), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' and a user profile icon are on the right. The left sidebar shows a list of account groups: 'Account Operators', 'All Domain Member Computers', 'AllUsers', 'AWSComputer', and 'Computers'. The main content area is titled 'Details Periodically Synchronize Accounts'. It contains a message about creating a scheduled task for synchronization. Below this is the 'Define Periodicity' section with two radio buttons: 'Synchronize Once' (selected) and 'Synchronize Periodically'. A note states: 'Note: The current time on the server in which Securden runs is 18 Apr 2023 11:42 hrs. The execution time you set here will follow the server time.' Below the note is a form to set the synchronization time: 'Synchronize accounts on DD/MM/YYYY at HH MM hrs'. A 'Save' button is at the bottom of the form.

If you choose to synchronize periodically, you need to specify the time and date for the first synchronization and the frequency of subsequent synchronizations.

The screenshot shows the Securden Unified PAM interface. The top navigation bar includes 'Dashboard', 'Accounts' (selected), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' is on the right. The left sidebar shows 'Account Groups' with a list of groups: 'Account Operators', 'All Domain Member Computers', 'AllUsers', 'AWSComputer', and 'Computers'. The main content area is titled 'Periodically Synchronize Accounts' and contains a 'Define Periodicity' section. This section has two radio buttons: 'Synchronize Once' (unselected) and 'Synchronize Periodically' (selected). A note states: 'The current time on the server in which Securden runs is 18 Apr 2023 11:42 hrs. The execution time you set here will follow the server time.' Below the note, there are input fields for 'Synchronize accounts periodically starting from' (DD/MM/YYYY), 'at' (HH), 'MM', and 'hrs'. There is also a field for 'Synchronize accounts every' followed by a 'Days' dropdown. A 'Save' button is at the bottom.

Manage Windows Service Accounts and their Dependencies

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.

The screenshot shows the Privileged Account Manager (PAM) interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. The 'Accounts' tab is active. On the left, the 'All Accounts' list is displayed with a search bar and filters for 'Folders', 'Tags', and 'Account Types'. The 'Service Accounts' folder is highlighted in red. The right pane shows the 'Details' tab for the 'Administrator' account, displaying fields like Account Name, Password, Password Strength (Strong | Score - 89%), FQDN/IP Address, FilePS, and Additional Field.

It will list down all the accounts that have dependencies. When you click a particular account, and then click the **Dependencies** tab in the right pane, you will see the list of all dependencies.

The screenshot shows the Privileged Account Manager (PAM) interface with the 'Dependencies' tab selected in the right pane. The left pane shows a list of accounts, including 'Administrator', 'sec-demo-2k16.SECURDEN.AWS...', 'Windows Member', 'IT Infrastructure/Local Accounts', 'sec-build-1.securden.aws.co...', 'Windows Member', 'IT Infrastructure', 'admin', '110.172.187.170', 'Windows Member', and 'Local Administrator Accounts'. The right pane displays the 'Dependencies' tab for the 'Administrator' account, showing a message: '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.' Below the message is a table with columns 'Type', 'Display Name', 'Name', and 'Computer Name'. The table is empty, showing 'No data found'. The bottom of the right pane includes a 'Help' section with a question mark icon and a paragraph explaining the dependency discovery process.

2. Alternatively, you can click any account available in the **Accounts** tab and then click the **Dependencies** tab in the right pane; you will see the list of all dependencies.

If you need to import recently added/configured dependencies to Securden, you can click **Fetch Now**. Securden will run the discovery process once again to fetch all the latest dependencies of the selected account.

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

If the password reset is not propagated to the services, you need to check and ensure the credentials provided for remote operations have admin privileges.

Troubleshooting Tips

Issue: One or more devices remain unreachable when running discovery on a distributed network. i.e., Error: Computer not reachable.

Possible cause 1: WMI service is not running on the remote computer, or the user might not have permission to access WMI services.

Troubleshooting:

Try starting WMI on the target computer. Follow the steps below:

1. Open the command prompt and execute the command ***net start winmgmt [/<switch>]***.
2. Use credentials of an administrator or a member of an administrator group to run WMI.

Possible cause 2: Port 135 not opened on the remote computer**Troubleshooting:**

Navigate to **Windows Firewall >> Advanced Settings** and create a new Inbound rule to open port 135.

Issue: Username or Password Incorrect

Possible Cause: When you provide the IP address, Securden can query the AD domain and check whether the specified credentials are correct. If they are found to be incorrect, then the error message is displayed.

Troubleshooting Tip:

Provide the correct set of credentials for accessing the AD. The account should at least have **READ** permission in the AD.

If you want to randomize the passwords of accounts discovered at the time of discovery, you need to provide the credentials of an account with password reset and verification privileges. By default, a domain admin account carries all the required privileges. If providing a domain admin account for running Securden is not desired, you can use a standard user account and delegate the required privileges manually in AD.

Issue: While running discovery on Windows servers, IIS App pools are not populated into Securden.

Possible cause 1: Connectivity issues between the web server, jump host, and the Securden server.

Troubleshooting Tip:

If you are running a separate web server using a jump host between the Securden server and the webserver, check whether connectivity exists between the servers using WIN RM.

If connectivity doesn't exist, try enabling WIN RM 5985 port on your firewall and check whether connectivity is established. If established, try running the discovery process again.

Possible cause 2: appcmd.exe is not enabled.

You can verify whether this is the cause if the following error message is displayed: *Unable to fetch dependent AppPools - WinRM: 'C:\Windows\System32\inetsrv\appcmd' is not recognized as an internal or external command.*

Troubleshooting Tip:

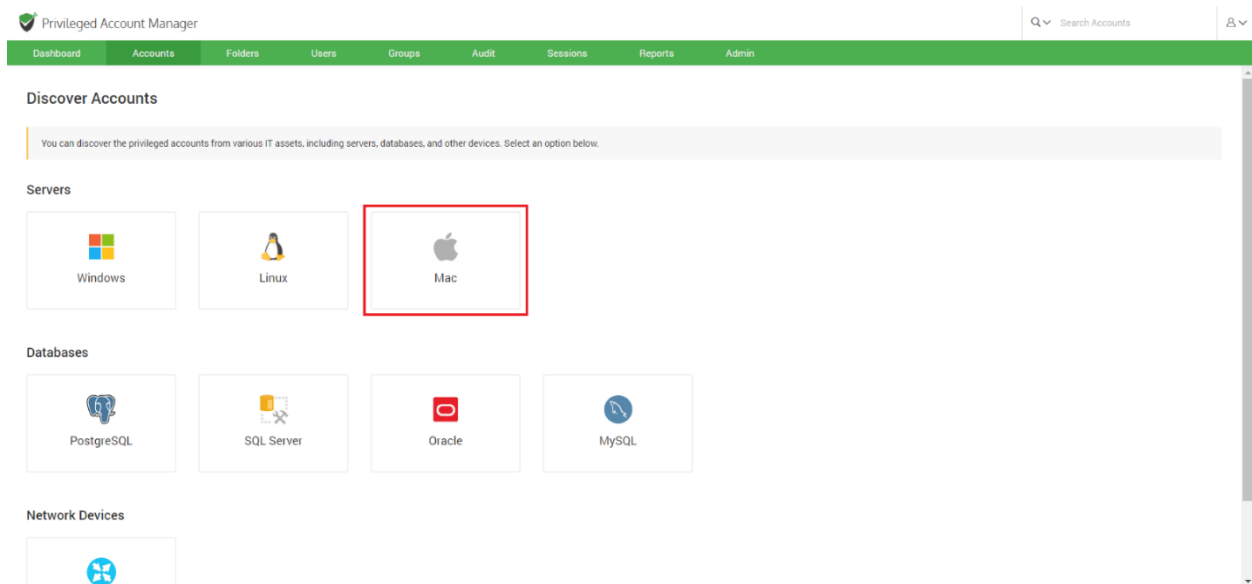
To fetch dependent App Pools, the tool **appcmd.exe** is used, and it needs to be enabled. Follow the steps below to enable appcmd.

1. Open **Control Panel** and navigate to **Turn Windows features on or off**.
2. Navigate to **Internet Information Service >> Web Management Tools** and enable **IIS Management Scripts and Tools**.
3. You can see **appcmd.exe** in the folder path **C:\Windows\System32\inetsrv**.
4. Add the folder path to the PATH system environment variable.

Run the app discovery again to check if the problem is resolved. If the problem persists, contact [**support@securden.com**](mailto:support@securden.com).

Discovering Privileged Accounts on Mac Devices

You can discover and add Mac devices and the accounts present in each of the devices. Navigate to **Accounts >> Add >> Discover Accounts** and then click **Mac** under **Servers** in the GUI to perform this step.



Note: Securden uses SSH for connecting to Mac devices. Hence, you should configure the firewall on your target devices to keep port 22 open.

Discovering from Mac devices is a two-step process.

Step 1: Establishing Connectivity

You need to establish connectivity between Securden and the Mac device. For Securden to connect with Mac-based devices and discover the accounts

present in them, you need to specify the IP address range of the devices and the channel through which the discovery needs to be performed.

You can discover devices from a single computer or a set of computers in an IP range.

If you choose **Single Computer**, you need to specify the **Hostname/IP address** of the target machine.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Mac Accounts [Back](#)

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**

Hostname/IP Address *

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

Select gateway or via channel ☒ Remote Gateway ☐ Unix Connector

Select Remote Gateway

Search remote gateway

[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

If you choose **Computer in IP Range**, you need to specify the **IP Range** of the target devices. I.e., you need to specify the **Start IP** and **End IP** of the range of devices to be scanned.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' and a user profile icon are on the right. The main heading is 'Discover Mac Accounts' with a red 'Back' button. A help box explains that Securden uses SSH for discovery and port 22 should be open. The 'Step 1: Enter Connectivity Details' section contains the following fields:

- Discover:** Radio buttons for 'Computers in IP range' (selected and highlighted with a red box) and 'Single Computer'.
- Start IP:** A text input field.
- End IP:** A text input field.
- Connection timeout (in seconds):** A text input field with the value '10'.
- Retry discovery process again after:** A checkbox labeled 'Retry discovery process again after: 5 hours'.
- Select gateway or via channel:** Radio buttons for 'Remote Gateway' (selected) and 'Unix Connector'.
- Select Remote Gateway:** A dropdown menu with the placeholder text 'Search remote gateway'.
- Buttons:** 'Next' (green) and 'Cancel' (white) buttons at the bottom.

A 'Help' section on the right provides additional context: 'You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.' It also mentions 'Discover through unix connector' for devices on different subnets.

Once the IP addresses of the devices have been specified, you need to provide the following details.

1. **Connection timeout:** The maximum time in seconds Securden can attempt to establish connectivity with the devices before terminating the process.
2. **Retry discovery process again:** If connectivity to one or more devices cannot be established at present, Securden can attempt to connect with the devices later. You need to specify the time (in hours) after which the attempt to connect should be made.

Discovering through Remote Gateway

If the devices belong to a different network than the Securden server, you can route the connection through a remote gateway.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. The main heading is 'Discover Mac Accounts' with a 'Back' button. A help section on the right explains that administrator credentials are needed for discovery and that separate discovery is required for each device. The main form area is titled 'Step 1: Enter Connectivity Details'. It has two radio buttons: 'Computers in IP range' (selected) and 'Single Computer'. Below these are input fields for 'Start IP' and 'End IP'. A 'Connection timeout(in seconds)' field is set to 10. A checkbox for 'Retry discovery process again after 5 hours' is present. Under 'Select gateway or via channel', the 'Remote Gateway' radio button is selected and highlighted with a red box. Below this, a dropdown menu is open, showing 'Select Remote Gateway' and 'Search remote gateway'. At the bottom are 'Next' and 'Cancel' buttons.

You can select the appropriate remote gateway from the drop-down and the discovery will happen through the selected gateway.

Discovering through a Unix Connector

If the devices you want to discover belong to a different subnet, you can try discovering them through Unix connectors.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Mac Accounts [Back](#)

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.

Select gateway or via channel ☐ Remote Gateway ☒ **Unix Connector**

Select Unix Connector
Search unix connector

[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

You can select a Unix connector from the drop-down and discovery will happen through the selected connector.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Mac Accounts [Back](#)

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
172.109.12.1 172.109.20.9

Connection timeout(in seconds) *
10

☒ Retry discovery process again after 5 hours.

Select gateway or via channel ☒ Remote Gateway ☐ Unix Connector

Select Remote Gateway
New York Data Center

[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Once all the required details have been provided, you can click **Next**.

Step 2: Enter Credentials and Discover

Securden needs to authenticate the connection with the devices to perform discovery. For this purpose, you can specify the root account credentials or sudo (Superuser Do) user credentials. Securden will also use the administrator credentials for performing remote actions like password verification and reset apart from account discovery.

You need to supply two sets of credentials, one for remote login and the other to fetch the accounts and onboard it to Securden.

1. Supply remote login credentials

You need to provide the login credentials of an administrator user on the target device for Securden to log in securely. You can choose between a **Password** or a **Public Key Infrastructure (PKI file)** as the authentication type.

If you choose a password-based authentication method, you need to specify the **Account Name** along with the corresponding **Password**.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Mac Accounts

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☒ Password ☐ PKI

Account Name *

Password *

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

[Advanced options](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you choose to authenticate using a PKI file, you have two options.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Mac Accounts [Back](#)

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☐ Password ☒ PKI

Account Name *

Private Key ☒ Select from Securden ☐ Select from your computer

Select from Securden Search Accounts

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

You can either choose an SSH key from Securden if available. You need to choose from the drop-down menu.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Mac Accounts [Back](#)

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☐ Password ☒ PKI

Account Name *

Private Key ☒ Select from Securden ☐ Select from your computer

Select from Securden Search Accounts

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

(or)

You can upload the key file from your computer.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Mac Accounts

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☐ Password ☒ PKI

Account Name *

Private Key ☐ Select from Securden ☒ Select from your computer

Select from your computer *

Choose a file Browse Passphrase

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you choose to upload a file from your computer, you need to provide the **passphrase** required to access the file.

Once the credentials for remote login are supplied, you need to specify the privileged credentials required to fetch the accounts present in the devices.

If the credentials required to fetch the accounts are the same as the credentials used for remote login, then you can select the checkbox named **Use remote login credentials as specified above**.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Supply remote login credentials

Authentication type ☐ Password ☒ PKI

Account Name *

Private Key ☐ Select from Securden ☒ Select from your computer

Select from your computer *

Choose a file Passphrase

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Password

[Advanced options](#)

accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

You can choose between **sudo** and **root** as the authentication type.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Supply remote login credentials

Authentication type ☐ Password ☒ PKI

Account Name *

Private Key ☐ Select from Securden ☒ Select from your computer

Select from your computer *

Choose a file Passphrase

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Password

[Advanced options](#)

accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you are using separate credentials for fetching accounts, you need to specify the account name and password for the same.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Account Name *

Private Key ☐ Select from Securden ☒ Select from your computer

Select from your computer *

Choose a file Browse Passphrase

Supply privileged credentials to fetch accounts

☐ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Account Name *

Password

Advanced options

Back Discover Cancel

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Important:

When choosing to use the same remote login credentials for fetching accounts:

1. For **root** authentication, you need not specify the account name or the password.
2. For **sudo** authentication:
 - a. If you chose password authentication for remote login, you need not specify your account name or password.
 - b. If you chose to authenticate with a PKI file in the previous step, you need to specify the password for fetching accounts.

Advanced Options

You have the options to add all the discovered accounts into a specific folder and assign them a specific account type. This will help mitigate the efforts required for classifying the accounts at a later time.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Account Name *

Private Key ☐ Select from Securden ☒ Select from your computer

Select from your computer *

Choose a file Passphrase

Supply privileged credentials to fetch accounts

☐ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Account Name *

Password

Advanced options

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

1. If you want to assign all the imported accounts a specific account type, you can select one from the drop down.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Choose a file Passphrase

Supply privileged credentials to fetch accounts

☐ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Account Name *

Password

Advanced Options

Account Type

Folder in Securden [\[Add Folder\]](#)

☐ Randomize passwords after accounts discovery ⓘ

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

2. If you want to add all the imported accounts to a folder, you can select one from the drop down.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Choose a file Password

Supply privileged credentials to fetch accounts

☐ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Account Name *

Search

- None-
- IT Infrastructure
 - API Test
 - Local Accounts
 - Open Connection
- None-

☐ Randomize passwords after accounts discovery ⓘ

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you want to create a new folder for this purpose, you need to click on **[Add Folder]**.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Choose a file Password

Supply privileged credentials to fetch accounts

☐ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Account Name *

Search

- None-
- IT Infrastructure
 - API Test
 - Local Accounts
 - Open Connection
- None-

☐ Randomize passwords after accounts discovery ⓘ

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

3. You have the option to assign strong and unique passwords to the accounts immediately after discovery.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Choose a file Browse Passphrase

Supply privileged credentials to fetch accounts

☐ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Account Name *

Password

Advanced Options

Account Type
Mac

Folder in Securden
--None-- [\[Add Folder\]](#)

☒ Randomize passwords after accounts discovery ⓘ

Back Discover Cancel

Randomize Passwords After Discovery
You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Note: The credentials used for authentication will not be randomized if this option is chosen.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Choose a file Browse Passphrase

Supply privileged credentials to fetch accounts

☐ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Account Name *

Password

Advanced Options

Account Type
Mac

Folder in Securden
--None-- [\[Add Folder\]](#)

☐ Randomize passwords after accounts discovery ⓘ

Back Discover Cancel

Randomize Passwords After Discovery
You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Once all the required parameters have been specified, click **Discover**.

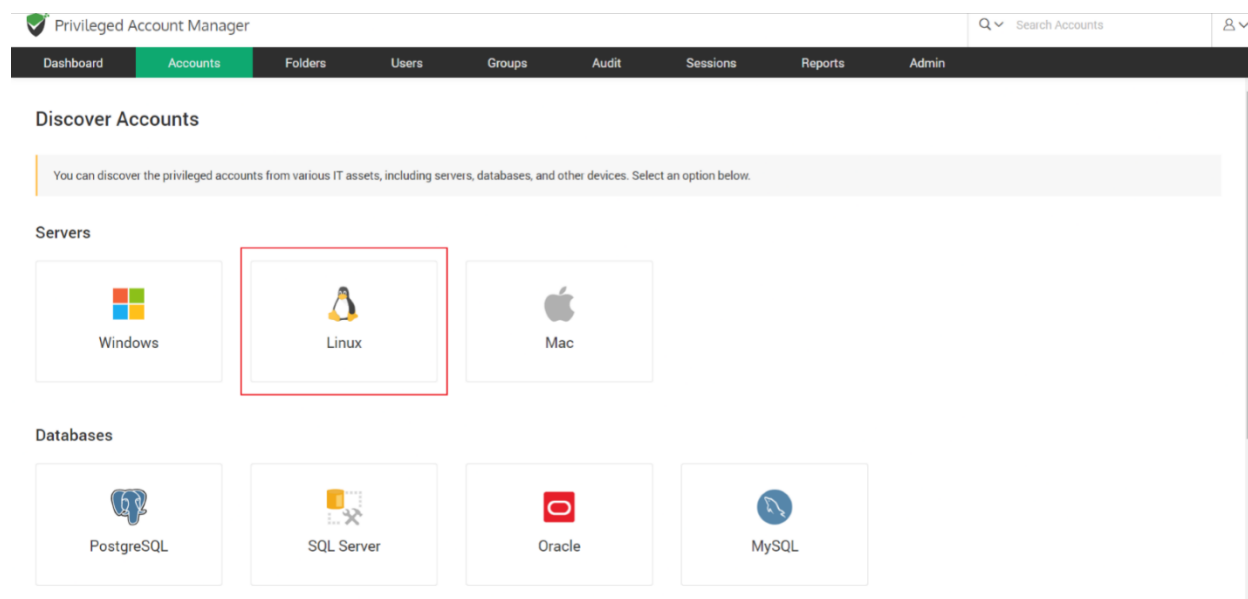
The process takes a few minutes to complete. Once it is completed, complete results with a list of accounts and their status is displayed. You can view how many accounts were successfully imported.

Discovering Privileged Accounts on Linux Devices

You can discover and add Linux devices and the accounts present in each of the devices. Discovering from Linux devices is a two-step process. First, you need to establish connectivity between Securden and the Linux server.

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

Note: Securden uses SSH for connecting to Linux devices. Hence, you should configure the firewall on your target devices to keep port 22 open.



Step 1: Establishing Connectivity

For Securden to connect with Linux-based devices and discover the accounts present in them, you need to specify the IP address range of the devices and the channel through which the discovery needs to be performed.

You have the option to discover devices from a single computer or from a set of computers in an IP range.

If you choose **Single Computer**, you need to specify the **Hostname/IP address** of the target machine.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. The 'Accounts' tab is selected. The main section is titled 'Discover Linux Accounts' with a 'Back' button. A help section on the right explains that administrator credentials are needed for discovery and that different credentials for different machines require separate discovery. The main form area is titled 'Step 1: Enter Connectivity Details'. It has two radio buttons: 'Computers in IP range' and 'Single Computer', with 'Single Computer' selected and highlighted by a red box. Below this, there is a text input field for 'Hostname/IP Address *' with the value '192.168.1.1'. A 'Connection timeout(in seconds) *' field is set to '10'. A checkbox for 'Retry discovery process again after 5 hours' is unchecked. There are two radio buttons for 'Select gateway or via channel': 'Remote Gateway' (selected) and 'Unix Connector'. Below these is a dropdown menu for 'Select Remote Gateway' with the placeholder text 'Search remote gateway'. At the bottom are 'Next' and 'Cancel' buttons.

If you choose **Computer in IP Range**, you need to specify the **IP Range** of the target devices. I.e., specify the **Start IP** and **End IP** of the range of devices to be scanned.

Note: If each machine in the IP range specified has different administrator credentials, you need to repeat the discovery separately for each device. In

such scenarios, importing accounts from CSV would be a better option than accounts discovery.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' and a user profile icon are on the right. The main heading is 'Discover Linux Accounts' with a '< Back' button. A help section on the right explains that administrator credentials are needed for discovery and that importing accounts from CSV is a better option than accounts discovery. The main form area is titled 'Step 1: Enter Connectivity Details'. It includes a 'Discover' section with two radio buttons: 'Computers in IP range' (selected) and 'Single Computer'. Below this are input fields for 'Start IP' (192.168.1.1) and 'End IP' (192.168.1.2). A 'Connection timeout(in seconds)' field is set to 10. There is a checkbox for 'Retry discovery process again after 5 hours'. The 'Select gateway or via channel' section has two radio buttons: 'Remote Gateway' (selected) and 'Unix Connector'. Below this is a 'Select Remote Gateway' dropdown menu with a search bar labeled 'Search remote gateway'. At the bottom are 'Next' and 'Cancel' buttons.

Once the IP addresses of the devices have been specified, you need to provide the following details:

1. **Connection timeout:** The maximum time in seconds Securden can attempt to establish connectivity with the devices before terminating the process.
2. **Retry discovery process again:** If connectivity to one or more devices cannot be established at present, Securden can attempt to connect with the devices at a later time. You need to specify the time (in hours) after which the attempt to connect should be made.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Linux Accounts

< Back

You can discover the Linux 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 * 172.168.72.1 End IP 172.168.73.5

Connection timeout(in seconds) * 10

☒ Retry discovery process again after 5 hours.

Select gateway or via channel ☒ Remote Gateway ☐ Unix Connector

Select Remote Gateway
--None--

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Discovering through Remote Gateway

If the devices belong to a different network than the Securden server, you can route the connection through a remote gateway. You can select the appropriate remote gateway from the drop-down and the discovery will happen through the selected gateway.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Linux Accounts

< Back

You can discover the Linux 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

Hostname/IP Address * 192.168.1.1

Connection timeout(in seconds) * 10

☐ Retry discovery process again after 5 hours.

Select gateway or via channel ☒ Remote Gateway ☐ Unix Connector

Select Remote Gateway
--None--

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Discovering through a Unix Connector

If the devices you want to discover belong to a different subnet, you can try discovering them through Unix connectors. You can select a Unix connector from the drop-down and discovery will happen through the selected connector.

The screenshot shows the 'Privileged Account Manager' interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' and a user profile icon are on the right. The main heading is 'Discover Linux Accounts' with a '< Back' button. A help section on the right explains that administrator credentials are needed for discovery and that Unix connectors can be used for different subnets. The main form area is titled 'Step 1: Enter Connectivity Details'. It has two radio buttons: 'Computers in IP range' and 'Single Computer' (selected). Below is a text field for 'Hostname/IP Address *' with the value '192.168.1.1'. Another text field for 'Connection timeout(in seconds) *' has the value '10'. A checkbox for 'Retry discovery process again after 5 hours.' is unchecked. Below that, 'Select gateway or via channel' has two radio buttons: 'Remote Gateway' and 'Unix Connector' (selected). At the bottom, there is a dropdown menu labeled 'Select Unix Connector' with the placeholder text 'Search unix connector'. At the very bottom are 'Next' and 'Cancel' buttons.

Once all the required details have been provided, you can click **Next**.

Step 2: Enter Credentials and Discover

Securden needs to authenticate the connection with the devices to perform discovery. For this purpose, you can specify the root account credentials or sudo (Superuser Do) user credentials. Securden will also use the administrator credentials for performing remote actions like password verification and reset apart from account discovery.

You need to supply two sets of credentials, one for remote login and the other to fetch the accounts and onboard it to Securden.

1. Supply remote login credentials

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Linux Accounts [Back](#)

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type: ☒ Password ☐ PKI

Account Name *
admin

Password *

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type: ☒ sudo ☐ root

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

You need to provide the login credentials of an administrator user on the target device for Securden to login securely.

- i. You need to specify the **Account Name** of the administrator account.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Linux Accounts [Back](#)

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☒ Password ☐ PKI

Account Name *
admin

Password *

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

- ii. You can choose between a **Password** or a **Public Key Infrastructure (PKI file)** as the authentication type.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Linux Accounts [Back](#)

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☒ Password ☐ PKI

Account Name *
admin

Password *

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you choose to authenticate using a PKI file, you have two options.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Linux Accounts

[< Back](#)

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☐ Password ☒ PKI

Account Name *
admin

Private Key ☒ Select from Securden ☐ Select from your computer

Select from Securden
Search Accounts

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

You can either choose an SSH key from Securden if available. You need to choose from the drop-down menu. (or)

You can upload the key file from your computer.

If you choose to upload a file from your computer, you need to provide the **passphrase** required to access the file.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Linux Accounts

[< Back](#)

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☐ Password ☒ PKI

Account Name *
admin

Private Key ☐ Select from Securden ☒ Select from your computer

Select from your computer *
Choose a file

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Once the credentials for remote login are supplied, you need to specify the privileged credentials required to fetch the accounts present in the devices.

If the credentials required to fetch the accounts are the same as the credentials used for remote login, then you can select the checkbox named **Use remote login credentials as specified above.**

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Select from your computer Choose a file Browse Passphrase

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Password *****

Advanced Options

Account Type Linux

Folder in Securden --None-- [Add Folder]

☐ Randomize passwords after accounts discovery ⓘ

Back Discover Cancel

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

You can choose between **sudo** and **root** as the authentication type.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Select from your computer

Choose a file Browse Passphrase

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Password

Advanced Options

Account Type
Linux

Folder in Securden
-None- [Add Folder]

☐ Randomize passwords after accounts discovery ⓘ

Back Discover Cancel

Randomize Passwords After Discovery
You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you are using separate credentials for fetching accounts, you need to specify the account name and password for the same.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☒ Password ☐ PKI

Account Name *
admin

Password *

Supply privileged credentials to fetch accounts

☐ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Account Name *

Password

[Advanced options](#)

Help
You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.
If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device, in such scenarios, importing accounts from CSV would be a better option than accounts discovery.
Discover through unix connector
If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.
Advanced Options
If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.
Randomize Passwords After Discovery
You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Important:

When choosing to use the same remote login credentials for fetching accounts:

1. For **root** authentication, you need not specify the account name or the password.
2. For **sudo** authentication:
 - a. If you choose password authentication for remote login, you need not specify your account name or password.
 - b. If you choose to authenticate with a PKI file in the previous step, you need to specify the password for fetching accounts.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type: ☐ Password ☒ PKI

Account Name*
admin

Private Key: ☒ Select from Securden ☐ Select from your computer

Select from Securden
Search Accounts

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type: ☒ sudo ☐ root

Password

[Advanced options](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Advanced Options

You have the options to add all the discovered accounts into a specific folder and assign them a specific account type. This will help mitigate the efforts required for classifying the accounts at a later time.

1. If you want to assign all the imported accounts a specific account type, you can select one from the drop down.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Private Key ☒ Select from Securden ☐ Select from your computer

Select from Securden
Search Accounts

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Password

Advanced Options

Account Type

Linux

Fedora

Linux

Ubuntu

[Add Folder]

☐ Randomize passwords after accounts discovery ⓘ

Back Discover Cancel

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

2. If you want to add all the imported accounts to a folder, you can select one from the drop down.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Private Key ☒ Select from Securden ☐ Select from your computer

Select from Securden
Search Accounts

Supply privileged credentials to fetch accounts

☒ Use remote login credentials as specified above

Authentication Type ☒ sudo ☐ root

Search

IT Infrastructure

API Test

Local Accounts

Open Connection

IT Infrastructure

[Add Folder]

☐ Randomize passwords after accounts discovery ⓘ

Back Discover Cancel

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you want to create a new folder for this purpose, you need to click on **[Add Folder]**.

3. You have the option to assign strong and unique passwords to the accounts immediately after discovery.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (selected), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' is on the right. The main content area is divided into sections:

- Private Key:** Radio buttons for 'Select from Securden' (selected) and 'Select from your computer'.
- Select from Securden:** A dropdown menu labeled 'Search Accounts'.
- Supply privileged credentials to fetch accounts:** A checked checkbox 'Use remote login credentials as specified above'.
- Authentication Type:** Radio buttons for 'sudo' (selected) and 'root'.
- Password:** A masked input field with a strength indicator.
- Advanced Options:**
 - Account Type:** A dropdown menu set to 'Linux'.
 - Folder in Securden:** A dropdown menu set to '-None-' with a '[Add Folder]' link.
 - Randomize passwords after accounts discovery:** A checked checkbox, highlighted with a red box.

At the bottom are 'Back', 'Discover', and 'Cancel' buttons. On the right, a sidebar titled 'Advanced Options' provides additional context for the 'Randomize Passwords After Discovery' option.

If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Note: The credentials used for authentication will not be randomized if this option is chosen.

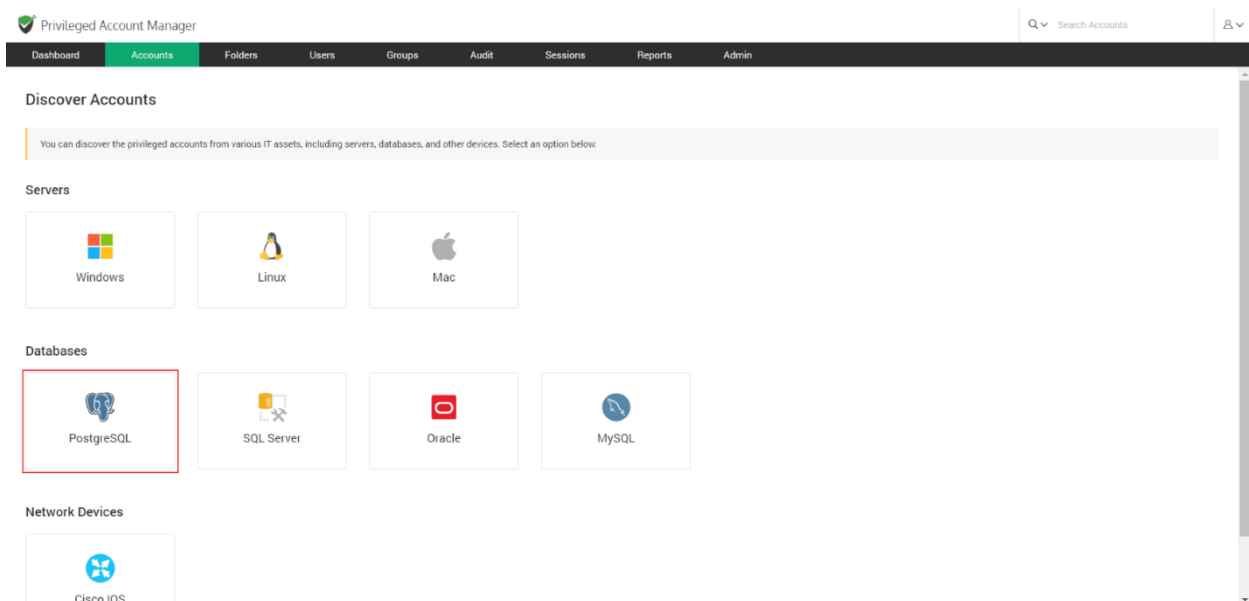
Once all the required parameters have been specified, click **Discover**. The process takes a few minutes to complete. Once it is completed, complete results with a list of accounts and their status is displayed. You can view how many accounts were successfully imported.

Discover and Import Accounts from Databases

Accounts stored in databases such as SQL servers, MySQL, PostgreSQL, and Oracle databases can be discovered and imported into Securden easily. You need to provide valid credentials to connect with the databases and import accounts into the PAM repository.

Discover Privileged Accounts from PostgreSQL Databases

The PostgreSQL instances and associated accounts can be discovered and added to Securden. To discover accounts in PostgreSQL databases, navigate to **Accounts >> Add >> Discover Accounts >> PostgreSQL**.



Discovering accounts from databases is a two-step process.

Step 1: Connecting to the Database

Before Securden discovers accounts from databases, it needs to establish connectivity between the database server and the Securden server. To establish connectivity, you need to furnish details such as the IP address and database port of the database instance.

IP Address: You can either run the discovery on a single computer or on a series of computers.

- 1) To discover from a single device, select **Single Computer**. You need to specify the IP address (or) the hostname of the required computer.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (selected), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar 'Search Accounts' and a user profile icon are on the right. The main heading is 'Discover PostgreSQL Accounts' with a 'Back' button. Below this is a descriptive text box: 'You can discover the PostgreSQL instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter a single instance too.' The 'Step 1: Enter Connectivity Details' section has three radio buttons: 'Discover', 'Computers in IP range', and 'Single Computer' (which is selected and highlighted with a red box). Below these are input fields for 'Hostname/IP Address *', 'Database Port *', and 'Default Database'. There are checkboxes for 'SSL' and 'Retry discovery process again after 5 hours'. A 'Connection timeout(in seconds) *' field is set to '10'. At the bottom are 'Next' and 'Cancel' buttons. A 'Help' section on the right explains the need for administrator credentials and mentions CSV import for multiple instances.

- 2) If you want to discover from a range of computers, select **Computers in IP Range**. You need to specify the start and end of the IP range.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover PostgreSQL Accounts

< Back

You can discover the PostgreSQL instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively you enter a single instance too.

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Single Computer

Start IP * End IP

Database Port * Default Database

☐ SSL

Connection timeout(in seconds) * 10

☐ Retry discovery process again after 5 hours.

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Note: If each instance in the IP range specified has different administrator credentials, you need to repeat the discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Database Port: You need to specify the port over which the database is serving.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover PostgreSQL Accounts

< Back

You can discover the PostgreSQL instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively you enter a single instance too.

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Single Computer

Start IP * End IP

Database Port * Default Database

☐ SSL

Connection timeout(in seconds) * 10

☐ Retry discovery process again after 5 hours.

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Default Database: You need to specify the default database of the MySQL instance running on your device(s).

The screenshot shows the 'Discover PostgreSQL Accounts' page in the Securden Privileged Account Manager. The page has a navigation bar with 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. The 'Accounts' tab is active. Below the navigation bar, there's a search bar and a user icon. The main content area is titled 'Discover PostgreSQL Accounts' and includes a 'Back' button. A help section on the right explains that administrator credentials are needed for discovery. The main form is titled 'Step 1: Enter Connectivity Details' and includes options for 'Discover' (Computers in IP range or Single Computer). It has input fields for 'Start IP', 'End IP', and 'Database Port' (which is highlighted with a red box and contains the text 'Default Database'). There are also checkboxes for 'SSL', a 'Connection timeout' field set to 10 seconds, and a 'Retry discovery process' checkbox set to 5 hours. 'Next' and 'Cancel' buttons are at the bottom.

Enforce SSL: You can enforce SSL while establishing a connection between Securden and PostgreSQL server. If you choose to enable this, you need to ensure that SSL connections are enabled in your PostgreSQL server. Additionally, you need to install a certified CA signed certificate in Securden. If the certificate of the domain controller is not signed by a certified CA, you need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the domain controller and all the intermediate certificates if any.

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover PostgreSQL Accounts

[Back](#)

You can discover the PostgreSQL instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter a single instance too.

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Single Computer

Start IP * End IP

Database Port * Default Database

☐ SSL

Connection timeout(in seconds) * 10

☐ Retry discovery process again after 5 hours.

[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Connection timeout: You need to specify the maximum time in seconds for which Securden will try to establish connectivity with your database instance.

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover PostgreSQL Accounts

[Back](#)

You can discover the PostgreSQL instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter a single instance too.

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Single Computer

Start IP * End IP

Database Port * Default Database

☐ SSL

Connection timeout(in seconds) * 10

☐ Retry discovery process again after 5 hours.

[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Retry discovery process again: If Securden is unable to connect to any or all the specified devices at present, you can schedule a re-attempt at discovery. You need to specify the time in hours after which the discovery process is attempted again.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' and a user profile icon are on the right. The main heading is 'Discover PostgreSQL Accounts' with a 'Back' button. A help section on the right explains that administrator credentials are needed for discovery and that separate discovery is required for each instance if using an IP range.

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Single Computer

Start IP * End IP

Database Port * Default Database

☐ SSL

Connection timeout(in seconds) * 10

☐ Retry discovery process again after 5 hours.

Step 2: Supply Administrator Credentials and Discover

Before Securden can discover accounts from the MySQL database, it needs to go through authentication. You need to specify the **username** and **password** of the administrator account.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar on the right says 'Search Accounts'. Below the navigation bar, the main heading is 'Discover PostgreSQL Accounts' with a red 'Back' button. The page is titled 'Step 2: Supply Credentials'. A message states: 'You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.' Below this, there are two input fields: 'Account Name *' with the value 'admin' and 'Password *' with masked characters. A red box highlights these fields. Below the password field is a link for 'Advanced options'. At the bottom are three buttons: 'Back', 'Discover' (highlighted), and 'Cancel'. On the right side, there is a 'Help' section with a question mark icon. It contains two sub-sections: 'Help' and 'Advanced Options'. The 'Help' section explains that administrator credentials are needed for discovery and that separate discovery is required for different instances. The 'Advanced Options' section explains that users can select account type classification and folders. Below this is a 'Randomize Passwords After Discovery' section, which explains that users can assign strong and unique passwords to discovered accounts.

Note: If each instance in the IP range specified has different administrator credentials, you need to repeat the discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

You can populate all the discovered accounts under a specific account type and/or a specific folder.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover PostgreSQL Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *

[Advanced options](#)

[Back](#) [Discover](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Account Type: You can select one of the compatible account types from the drop-down.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover PostgreSQL Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *

Advanced Options

Account Type
PostgreSQL

Folder in Securden
-None- [\[Add Folder\]](#)

☐ Randomize passwords after accounts discovery

[Back](#) [Discover](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you want to assign a different account type from the available list of types, you need to navigate to **Admin >> Account Management >> Account Types** and add a new custom account type or modify an existing custom account type according to your needs.

Folder: You can open the drop-down menu and select the required folder from the folder tree.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' and a user profile icon are on the right. The main heading is 'Discover PostgreSQL Accounts' with a red 'Back' button. The section is titled 'Step 2: Supply Credentials' with a note: 'You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.'

Form fields include:

- Account Name ***: A text input field containing 'admin'.
- Password ***: A password input field with masked characters and a show/hide toggle.
- Advanced Options**:
 - Account Type**: A dropdown menu set to 'PostgreSQL'.
 - Folder in Securden**: A dropdown menu currently showing '-None-' and highlighted with a red box. A link '(Add Folder)' is next to it.
 - ☐ **Randomize passwords after accounts discovery** (with a help icon).

At the bottom are 'Back', 'Discover' (in green), and 'Cancel' buttons. A 'Help' sidebar on the right provides instructions on supplying administrator credentials and details about advanced options and password randomization.

If you want to create a new folder, you can click **[Add Folder]** and create a new one.

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover PostgreSQL Accounts

[Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *

admin

Password *

Advanced Options

Account Type

PostgreSQL

Folder in Securden

~None~ [Add Folder](#)

☐ Randomize passwords after accounts discovery ⓘ

[Back](#) [Discover](#) [Cancel](#)

Help ⓘ

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Randomize Passwords After Discovery

Immediately after the discovery, you can assign secure and unique passwords to the accounts. If you select this option, Securden creates passwords for the accounts on the target devices according to the specified password rules.

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover PostgreSQL Accounts

[Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *

admin

Password *

Advanced Options

Account Type

PostgreSQL

Folder in Securden

~None~ [Add Folder](#)

☐ Randomize passwords after accounts discovery ⓘ

[Back](#) [Discover](#) [Cancel](#)

Help ⓘ

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

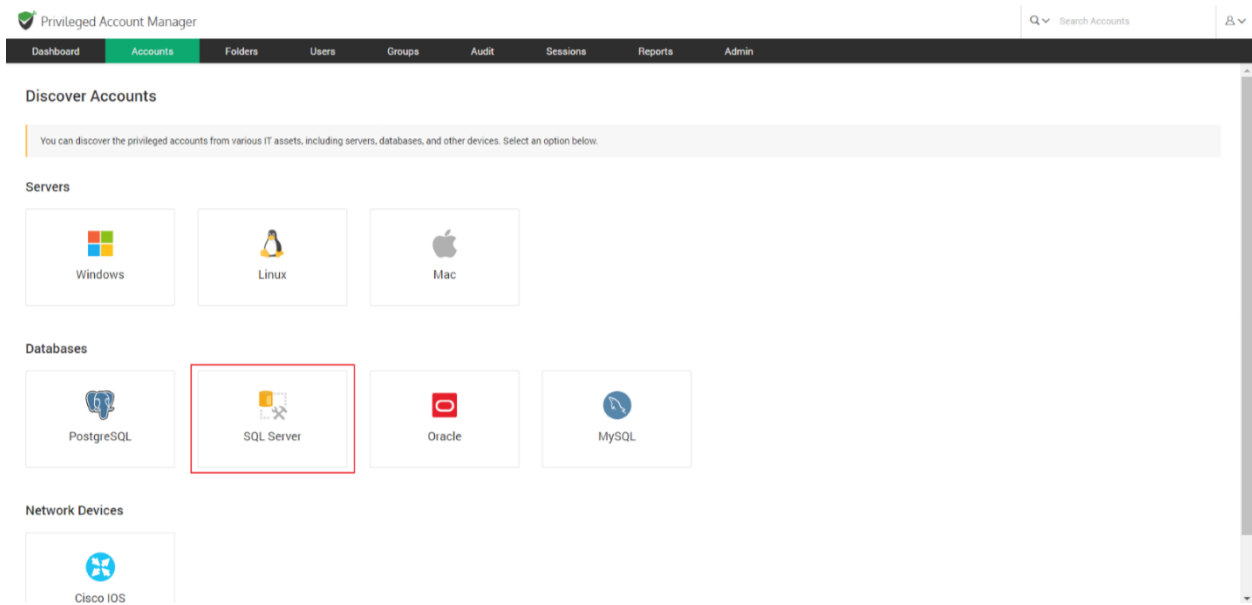
Once you have selected your preferences, click **Discover**.

The screenshot shows the 'Privileged Account Manager' interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar on the right says 'Search Accounts'. Below the navigation bar, the page title is 'Discover PostgreSQL Accounts' with a red 'Back' button. The main content area is titled 'Step 2: Supply Credentials' and contains a message: 'You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.' Below this, there are input fields for 'Account Name *' (with 'admin' entered) and 'Password *' (with masked characters). Under 'Advanced Options', there is a dropdown for 'Account Type' set to 'PostgreSQL' and another dropdown for 'Folder in Securden' set to '~None~'. A checkbox labeled 'Randomize passwords after accounts discovery' is unchecked. At the bottom, there are three buttons: 'Back', 'Discover' (highlighted with a red box), and 'Cancel'. On the right side, there is a 'Help' section with text explaining the need for administrator credentials and advanced options.

The process takes a few minutes to complete. Once it is completed, complete results with a list of accounts and their status is displayed. You can view how many accounts were successfully imported.

Discover Privileged Accounts from SQL Servers

You can connect to SQL server instances and discover the accounts present in each instance. To discover accounts in SQL servers, navigate to **Accounts >> Add >> Discover Accounts >> SQL Servers**.



Discovering accounts from SQL servers is a two-step process

Step 1: Connect to the SQL Servers

Before Securden can discover privileged accounts from your SQL server, it needs to establish connectivity with the SQL servers. You need to specify certain attributes for Securden to connect with the server.

IP address/Hostname

You have the option to connect to multiple instances of SQL servers and discover accounts in them. You have two options to achieve this.

- 1) You can select **Multiple Instances** and specify the individual IP addresses of the instances in comma-separated form.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover SQL Server Accounts

< Back

You can discover the SQL server instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter specific names of the instances or a single instance too.

Step 1: Enter Connectivity Details

Discover ☐ Computers in IP range ☒ Multiple Instances ☐ Single Instance

Enter instance names as comma separated.

Default Database

☐ SSL

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

- 2) If the instances have a series of consecutive IP addresses, you can select **Computers in IP range** and specify the start and end of the IP range.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover SQL Server Accounts

< Back

You can discover the SQL server instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter specific names of the instances or a single instance too.

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Multiple Instances ☐ Single Instance

Start IP *

End IP

Database Port *

Default Database

☐ SSL

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

- 3) Alternatively, you have the option to connect to a single SQL server instance and discover the accounts therein. Select **Single Instance** and specify the IP address or the hostname of the device and proceed.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover SQL Server Accounts

[Back](#)

You can discover the SQL server instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter specific names of the instances or a single instance too.

Step 1: Enter Connectivity Details

Discover ☐ Computers in IP range ☐ Multiple Instances ☒ Single Instance

Hostname/IP Address *

Database Port

Default Database

☐ SSL

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Database Port: You need to specify the port over which the database is serving.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover SQL Server Accounts

[Back](#)

You can discover the SQL server instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter specific names of the instances or a single instance too.

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Multiple Instances ☐ Single Instance

Start IP *

End IP

Database Port *

Default Database

☐ SSL

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Default Database: You need to specify the default database of the MySQL instance running on your device(s).

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

You can discover the SQL server instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter specific names of the instances or a single instance too.

Step 1: Enter Connectivity Details

Discover ☐ Computers in IP range ☐ Multiple Instances ☒ Single Instance

Hostname/IP Address *

192.168.72.2

Database Port

Default Database

☐ SSL

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Enforce SSL: You can enforce SSL while establishing a connection between Securden and SQL server. If you choose to enable this, you need to ensure that SSL connections are enabled in your SQL server. Additionally, you need to install a certified CA signed certificate in Securden. If the certificate of the domain controller is not signed by a certified CA, you need to import all the certificates that are present in the respective root certificate chain - that is the certificate of the domain controller and all the intermediate certificates if any.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover SQL Server Accounts [Back](#)

You can discover the SQL server instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter specific names of the instances or a single instance too.

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Multiple instances ☐ Single instance

Start IP * End IP

Database Port * Default Database

☐ SSL

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Connection timeout: You need to specify the maximum time in seconds for which Securden will try to establish connectivity with your database instance.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover SQL Server Accounts [Back](#)

You can discover the SQL server instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter specific names of the instances or a single instance too.

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Multiple instances ☐ Single instance

Start IP * End IP

Database Port * Default Database

☐ SSL

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Retry discovery process again: If Securden is unable to connect to any or all the specified devices at present, you can schedule a re-attempt at

discovery. You need to specify the time in hours after which the discovery process is attempted again.

The screenshot shows the Securden Privileged Account Manager web interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar and a user profile icon are on the right. The main heading is 'Discover SQL Server Accounts' with a red 'Back' button. A help box on the right explains that administrator credentials are needed for discovery. The main form area is titled 'Step 1: Enter Connectivity Details' and contains the following fields:

- Discover:** Three radio buttons: 'Computers in IP range' (selected), 'Multiple instances', and 'Single instance'.
- Start IP *:** A text input field.
- End IP:** A text input field.
- Database Port *:** A text input field.
- Default Database:** A text input field.
- SSL:** A checkbox that is currently unchecked.
- Connection timeout(in seconds) *:** A text input field with the value '10'.
- Retry discovery process again after:** A text input field with the value '5' and the unit 'hours'.

At the bottom of the form are two buttons: 'Next' (green) and 'Cancel' (grey).

Step 2: Supply Administrator Credentials and Discover

Before Securden can discover accounts from the MySQL database, it needs to go through authentication. You need to specify the **username** and **password** of the administrator account.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar on the right says 'Search Accounts'. Below the navigation bar, the main heading is 'Discover SQL Server Accounts' with a red 'Back' button. The current step is 'Step 2: Supply Credentials'. A message states: 'You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.' Below this is a form with two fields: 'Account Name *' with the value 'admin' and 'Password *' with masked characters. A red box highlights these fields. Below the form is a link for 'Advanced options' and three buttons: 'Back', 'Discover', and 'Cancel'. On the right side, there is a 'Help' section with a question mark icon. It contains two sections: 'Advanced Options' and 'Randomize Passwords After Discovery', both providing instructions on how to use these features.

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *

[Advanced options](#)

[Back](#) [Discover](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Note: If each instance in the IP range specified has different administrator credentials, you need to repeat the discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

You can populate all the discovered accounts under a specific account type and/or a specific folder.

The screenshot shows the 'Privileged Account Manager' interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar on the right says 'Search Accounts'. Below the navigation bar, the main heading is 'Discover SQL Server Accounts' with a red 'Back' button. The page is titled 'Step 2: Supply Credentials'. A message states: 'You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.' There are two input fields: 'Account Name *' with the value 'admin' and 'Password *' with masked characters. Below these is a link 'Advanced options' highlighted with a red box. At the bottom are three buttons: 'Back', 'Discover' (highlighted), and 'Cancel'. On the right side, there is a 'Help' section with a question mark icon. It contains text about supplying administrator credentials, a note about repeating discovery for different IP ranges, and sections for 'Advanced Options' and 'Randomize Passwords After Discovery'.

Account Type: You can select one of the compatible account types from the drop-down. If you want to assign a different account type from the available list of types, you need to navigate to **Admin >> Account Management >> Account Types** and add a new custom account type or modify an existing custom account type according to your needs.

Folder: You can open the drop-down menu and select the required folder from the folder tree.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover SQL Server Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *

admin

Search

- None-
- IT Infrastructure
 - API Test
 - Local Accounts
 - Open Connection
- None-

[Add Folder](#)

☐ Randomize passwords after accounts discovery ⓘ

[Back](#) [Discover](#) [Cancel](#)

Help ⓘ

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you want to create a new folder, you can click **[Add Folder]** and create a new one.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover SQL Server Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *

admin

Password *

Advanced Options

Account Type

SQL Server

Folder in Securden

-None- [Add Folder](#)

☐ Randomize passwords after accounts discovery ⓘ

[Back](#) [Discover](#) [Cancel](#)

Help ⓘ

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Randomize Passwords After Discovery

Immediately after the discovery, you can assign secure and unique passwords to the accounts. If you select this option, Securden creates passwords for the accounts on the target devices according to the password rules you specify.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover SQL Server Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *

Advanced Options

Account Type
SQL Server

Folder in Securden
-None- [Add Folder](#)

☒ Randomize passwords after accounts discovery ⓘ

[Back](#) [Discover](#) [Cancel](#)

Help ⓘ

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Once you have selected your preferences, click **Discover**.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover SQL Server Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *
.....

Advanced Options

Account Type
SQL Server

Folder in Securden
-None- [Add Folder](#)

☐ Randomize passwords after accounts discovery ⓘ

[Back](#) [Discover](#) [Cancel](#)

Help ⓘ
You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.
If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

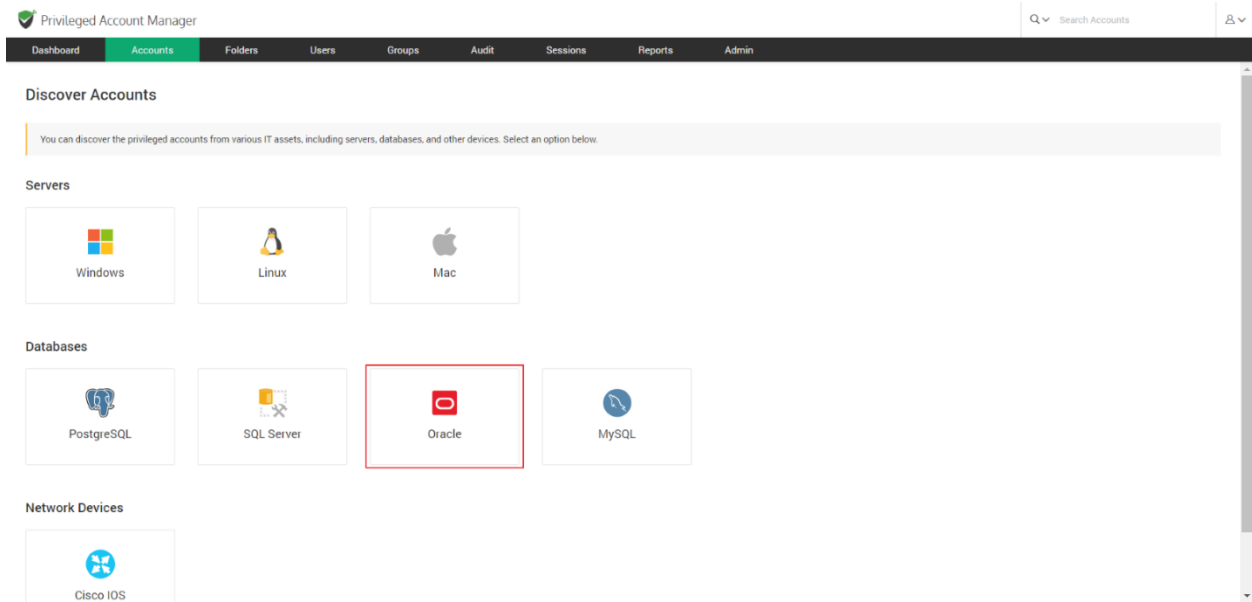
Advanced Options
If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery
You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

The process takes a few minutes to complete. Once it is completed, complete results with a list of accounts and their status are displayed. You can view how many accounts were successfully imported.

Discover Privileged Accounts from Oracle Databases

You can connect to your Oracle instances and discover accounts present in them. To discover accounts in Oracle databases, navigate to **Accounts >> Add >> Discover Accounts >> Oracle Database**.



Discovering accounts from databases is a two-step process.

Step 1: Connecting to the Oracle Database

Before Securden discovers accounts from databases, it needs to establish connectivity between the database server and the Securden server. To establish connectivity, you need to furnish details such as the IP address and database port of the database instance.

IP Address: You can either run the discovery on a single computer or on a series of computers.

- 1) To discover from a single device, select **Single Computer**. You need to specify the IP address (or) the hostname of the required computer.

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Oracle Accounts

You can discover the Oracle instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter a single instance too.

Pre-requisite: You need to download and install Oracle client library. [Refer to this section for details.](#)

Step 1: Enter Connectivity Details

Discover ☐ Computers in IP range ☒ **Single Computer**

Hostname/IP Address *

SID Service Name

Database Port *

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

2) If you want to discover from a range of computers, select **Computers in IP Range**. You need to specify the start and end of the IP range.

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Oracle Accounts

You can discover the Oracle instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter a single instance too.

Pre-requisite: You need to download and install Oracle client library. [Refer to this section for details.](#)

Step 1: Enter Connectivity Details

Discover ☒ **Computers in IP range** ☐ Single Computer

Start IP * End IP

SID Service Name

Database Port *

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

SID: The unique name that you use to identify your Oracle instance.

Privileged Account Manager

Q Search Accounts

Dashboard
Accounts
Folders
Users
Groups
Audit
Sessions
Reports
Admin

Discover Oracle Accounts

You can discover the Oracle instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter a single instance too.

Pre-requisite: You need to download and install Oracle client library. [Refer to this section for details.](#)

Step 1: Enter Connectivity Details

Discover
Computers in IP range
Single Computer

Hostname/IP Address *

SID
Service Name

Database Port *

Connection timeout(in seconds) *
10

☐ Retry discovery process again after 5 hours.

Next
Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Service Name: The alias given to your database for remote connection purposes.

Privileged Account Manager

Q Search Accounts

Dashboard
Accounts
Folders
Users
Groups
Audit
Sessions
Reports
Admin

Discover Oracle Accounts

You can discover the Oracle instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter a single instance too.

Pre-requisite: You need to download and install Oracle client library. [Refer to this section for details.](#)

Step 1: Enter Connectivity Details

Discover
Computers in IP range
Single Computer

Hostname/IP Address *

SID
Service Name

Database Port *

Connection timeout(in seconds) *
10

☐ Retry discovery process again after 5 hours.

Next
Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Database Port: You need to specify the port over which the database is serving.

The screenshot shows the 'Discover Oracle Accounts' page in the Securden Privileged Account Manager. The page has a dark navigation bar with the following tabs: Dashboard, Accounts (selected), Folders, Users, Groups, Audit, Sessions, Reports, and Admin. A search bar labeled 'Search Accounts' and a user profile icon are on the right. Below the navigation bar, the page title is 'Discover Oracle Accounts' with a 'Back' button. The main content area is titled 'Step 1: Enter Connectivity Details'. It includes a 'Discover' section with three radio buttons: 'Computers in IP range' (selected), 'Single Computer', and 'Discover'. Below this are input fields for 'Hostname/IP Address *', 'SID', and 'Service Name'. A 'Database Port *' field is highlighted with a red border. Below that is a 'Connection timeout(in seconds) *' field with the value '10'. At the bottom, there is a checkbox for 'Retry discovery process again after 5 hours' and 'Next' and 'Cancel' buttons. A 'Help' sidebar on the right provides additional information about the discovery process.

Discover Oracle Accounts Back

You can discover the Oracle instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter a single instance too.

Pre-requisite: You need to download and install Oracle client library. [Refer to this section for details.](#)

Step 1: Enter Connectivity Details

Discover ☐ Computers in IP range ☒ Single Computer

Hostname/IP Address *

SID Service Name

Database Port *

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Connection timeout: You need to specify the maximum time in seconds for which Securden will try to establish connectivity with your database instance.

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Oracle Accounts Back

You can discover the Oracle instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter a single instance too.

Pre-requisite: You need to download and install Oracle client library. [Refer to this section for details.](#)

Step 1: Enter Connectivity Details

Discover ☐ Computers in IP range ☒ Single Computer

Hostname/IP Address *

SID Service Name

Database Port *

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Retry discovery process again: If Securden is unable to connect to any or all the specified devices at present, you can schedule a re-attempt at discovery. You need to specify the time in hours after which the discovery process is attempted again.

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Oracle Accounts Back

You can discover the Oracle instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively, you enter a single instance too.

Pre-requisite: You need to download and install Oracle client library. [Refer to this section for details.](#)

Step 1: Enter Connectivity Details

Discover ☐ Computers in IP range ☒ Single Computer

Hostname/IP Address *

SID Service Name

Database Port *

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Step 2: Supply Administrator Credentials and Discover

Before Securden can discover accounts from the Oracle database, it needs to go through authentication. You need to specify the **username** and **password** of the administrator account.

The screenshot shows the 'Discover Oracle Accounts' page in the Securden Privileged Account Manager. The page title is 'Discover Oracle Accounts' with a red 'Back' button. Below the title, it says 'Step 2: Supply Credentials'. A message states: 'You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.' There are two input fields: 'Account Name *' with the value 'admin' and 'Password *' which is masked with asterisks. A red box highlights these two fields. Below the fields is a link for 'Advanced options' and three buttons: 'Back', 'Discover', and 'Cancel'. On the right side, there is a 'Help' section with a question mark icon. It contains two sections: 'Help' and 'Advanced Options'. The 'Help' section explains that administrator credentials are needed for scanning and that different credentials for different instances require separate discoveries. The 'Advanced Options' section explains that users can select specific account types and folders for discovery, and that Securden can generate passwords based on a specified policy after discovery.

Note: If each instance in the IP range specified has different administrator credentials, you need to repeat the discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

You can populate all the discovered accounts under a specific account type and/or a specific folder.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Oracle Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *

[Advanced options](#)

[Back](#) [Discover](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Account Type: You can select one of the compatible account types from the drop-down.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Oracle Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *

Advanced Options

Account Type
Oracle

Folder in Securden
-None- [Add Folder](#)

☐ Randomize passwords after accounts discovery

[Back](#) [Discover](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you want to assign a different account type from the available list of types, you need to navigate to **Admin >> Account Management >>**

Account Types and add a new custom account type or modify an existing custom account type according to your needs.

Folder: You can open the drop-down menu and select the required folder from the folder tree.

The screenshot shows the 'Privileged Account Manager' interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. The 'Accounts' tab is active. Below the navigation bar, the page title is 'Discover Oracle Accounts'. A red 'Back' button is in the top right corner.

The main content area is titled 'Step 2: Supply Credentials'. It contains a message: 'You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.' Below this, there are two input fields: 'Account Name *' with the value 'admin' and 'Password *' with a masked password. Below these is the 'Advanced Options' section, which includes a dropdown for 'Account Type' set to 'Oracle', a dropdown for 'Folder in Securden' set to '-None-' (highlighted with a red box), and a checkbox for 'Randomize passwords after accounts discovery' which is unchecked. A blue link '(Add Folder)' is next to the folder dropdown. At the bottom, there are three buttons: 'Back', 'Discover', and 'Cancel'.

On the right side, there is a 'Help' section with a question mark icon. It contains text about supplying administrator credentials and a note about repeating discovery for each instance. Below this is an 'Advanced Options' section with text about account type classification and folder selection. At the bottom of the help section is a 'Randomize Passwords After Discovery' section with text about assigning strong and unique passwords.

If you want to create a new folder, you can click **[Add Folder]** and create a new one.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Oracle Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *

Advanced Options

Account Type
Oracle

Folder in Securden
--None-- [Add Folder](#)

☐ Randomize passwords after accounts discovery ⓘ

[Back](#) [Discover](#) [Cancel](#)

Help ⓘ

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Randomize Passwords After Discovery

Immediately after the discovery, you can assign secure and unique passwords to the accounts. If you select this option, Securden creates passwords for the accounts on the target devices according to the password rules you specify.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Oracle Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *

Advanced Options

Account Type
Oracle

Folder in Securden
--None-- [Add Folder](#)

☐ Randomize passwords after accounts discovery ⓘ

[Back](#) [Discover](#) [Cancel](#)

Help ⓘ

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

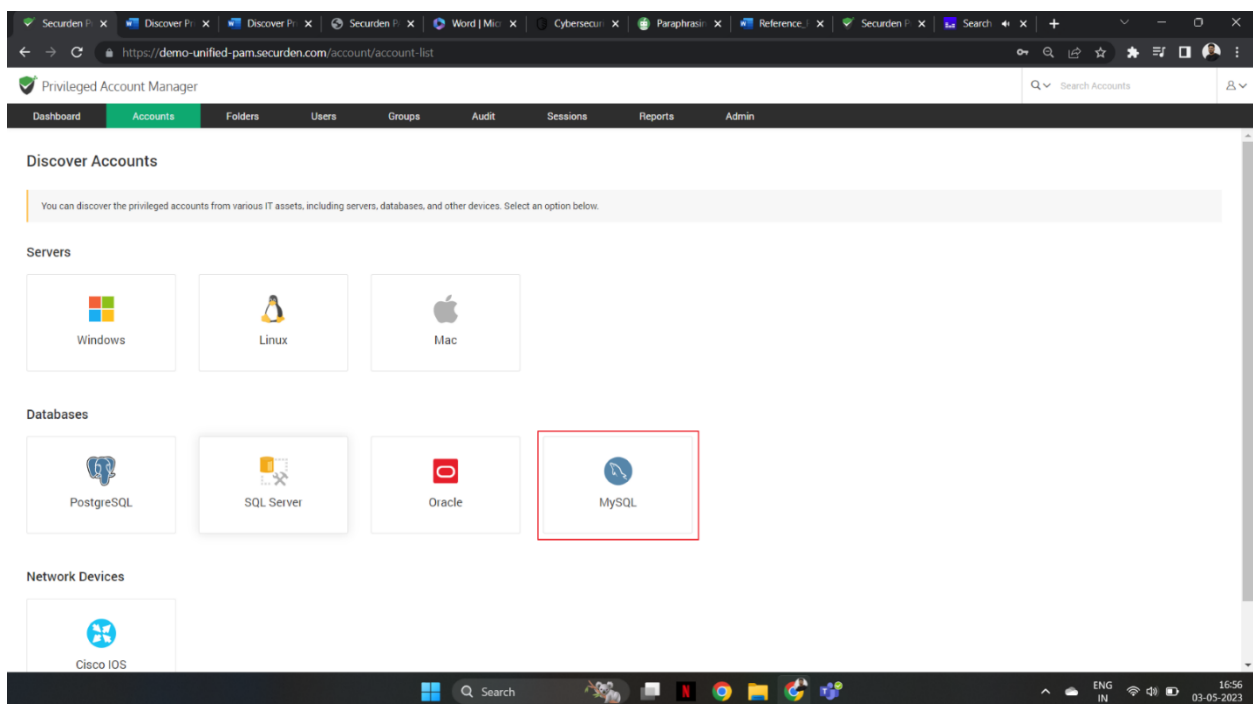
Once you have selected your preferences, click **Discover**.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar on the right says 'Search Accounts'. Below the navigation bar, the page title is 'Discover Oracle Accounts' with a 'Back' button. The main content area is titled 'Step 2: Supply Credentials' and contains a message: 'You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.' Below this, there are input fields for 'Account Name *' (with 'admin' entered) and 'Password *' (masked with dots). Under 'Advanced Options', there are dropdowns for 'Account Type' (set to 'Oracle') and 'Folder in Securden' (set to '-None-'). A checkbox 'Randomize passwords after accounts discovery' is unchecked. At the bottom are 'Back', 'Discover' (highlighted with a red border), and 'Cancel' buttons. On the right side, there is a 'Help' section with a question mark icon, followed by text explaining the need for administrator credentials and a note about repeating discovery for different instances. Below that is an 'Advanced Options' section explaining that account type and folder selection can save manual editing efforts. At the bottom of the help section is a 'Randomize Passwords After Discovery' section explaining that this option assigns strong and unique passwords to accounts immediately after discovery.

The process takes a few minutes to complete. Once it is completed, complete results with a list of accounts and their status is displayed. You can view how many accounts were successfully imported.

Discovering Privileged Accounts from MySQL Databases

The MySQL instances and associated accounts can be discovered and added to Securden. To discover accounts in MySQL instances, navigate to **Accounts >> Add >> Discover Accounts >> MySQL**.



Prerequisite: Before connecting to a MySQL connector and discovering accounts, you need to install MySQL Connector. Follow the steps below.

1. Ensure that the Securden server is connected to the internet.
2. Run a command prompt as Administrator.
3. Open a command prompt as Administrator and navigate to **Securden-Installation-Folder\bin** in the prompt.
4. Run '**installMySQLConnector.bat**'.

5. From services.msc, restart the Securden PAM Service.

Discovering accounts from databases is a two-step process.

Step 1: Connecting to the Database

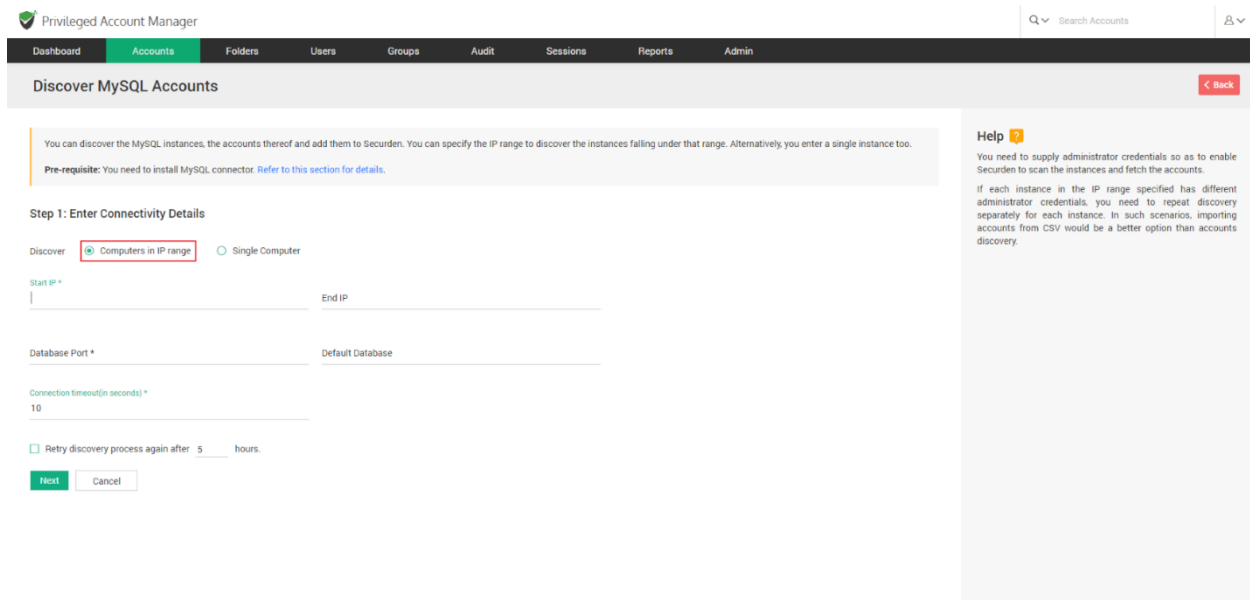
Before Securden discovers accounts from databases, it needs to establish connectivity between the database server and the Securden server. To establish connectivity, you need to furnish details such as the IP address and database port of the database instance.

IP Address: You can either run the discovery on a single computer or on a series of computers.

- 1) To discover from a single device, select **Single Computer**. You need to specify the IP address (or) the hostname of the required computer.

The screenshot shows the Securden Privileged Account Manager web interface. The top navigation bar includes 'Dashboard', 'Accounts' (selected), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' and a user profile icon are on the right. The main heading is 'Discover MySQL Accounts' with a 'Back' button. Below this, a message states: 'You can discover the MySQL instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively you enter a single instance too.' A 'Pre-requisite' note mentions installing the MySQL connector. The 'Step 1: Enter Connectivity Details' section has three radio buttons: 'Discover', 'Computers in IP range', and 'Single Computer' (which is selected and highlighted with a red box). Below these are input fields for 'Hostname/IP Address *', 'Database Port *' (with a 'Default Database' label), and 'Connection timeout(in seconds) *' (set to 10). A checkbox for 'Retry discovery process again after 5 hours' is also present. At the bottom are 'Next' and 'Cancel' buttons. A 'Help' section on the right explains the need for administrator credentials and mentions CSV import as an alternative to accounts discovery.

- 2) If you want to discover from a range of computers, select **Computers in IP Range**. You need to specify the start and end of the IP range.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover MySQL Accounts [Back](#)

You can discover the MySQL instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively you enter a single instance too.

Pre-requisite: You need to install MySQL connector. [Refer to this section for details.](#)

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Single Computer

Start IP * End IP

Database Port * Default Database

Connection timeout(in seconds) * 10

☐ Retry discovery process again after 5 hours.

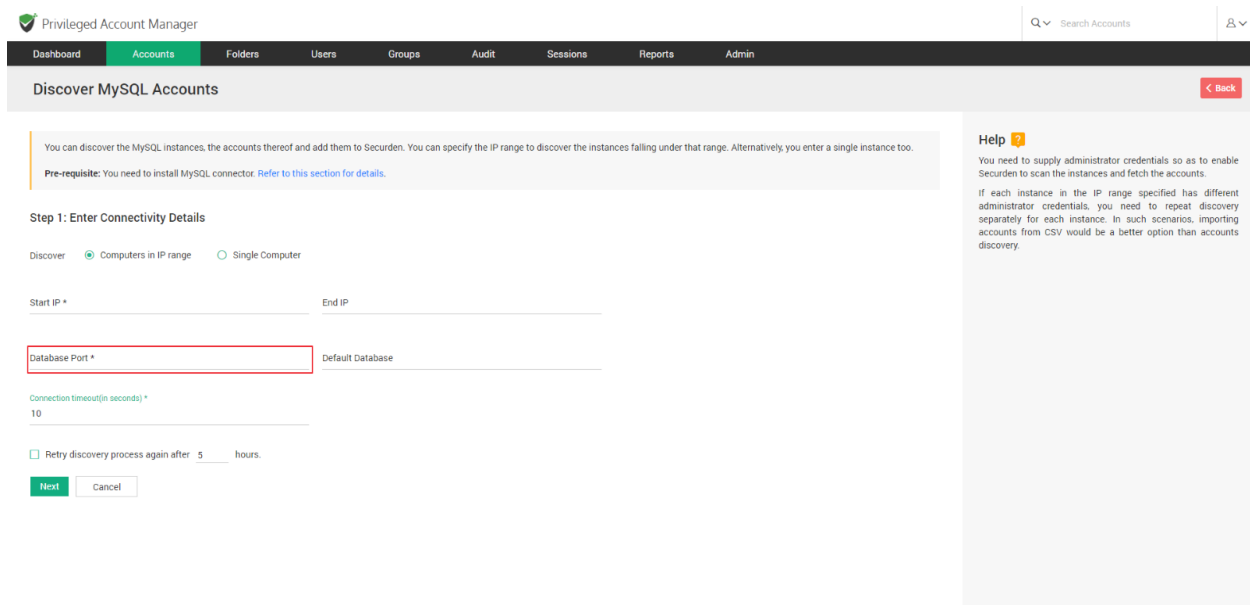
[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Database Port: You need to specify the port over which the database is serving.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover MySQL Accounts [Back](#)

You can discover the MySQL instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively you enter a single instance too.

Pre-requisite: You need to install MySQL connector. [Refer to this section for details.](#)

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Single Computer

Start IP * End IP

Database Port * Default Database

Connection timeout(in seconds) * 10

☐ Retry discovery process again after 5 hours.

[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Default Database: You need to specify the default database of the MySQL instance running on your device(s).

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover MySQL Accounts [Back](#)

You can discover the MySQL instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively you enter a single instance too.

Pre-requisite: You need to install MySQL connector. [Refer to this section for details.](#)

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Single Computer

Start IP * End IP

Database Port * **Default Database**

Connection timeout(in seconds) *
10

☐ Retry discovery process again after 5 hours.

[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Connection timeout: You need to specify the maximum time in seconds for which Securden will try to establish connectivity with your database instance.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover MySQL Accounts [Back](#)

You can discover the MySQL instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively you enter a single instance too.

Pre-requisite: You need to install MySQL connector. [Refer to this section for details.](#)

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Single Computer

Start IP * End IP

Database Port * Default Database

Connection timeout(in seconds) *
10

☐ Retry discovery process again after 5 hours.

[Next](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Retry discovery process again: If Securden is unable to connect to any or all the specified devices at present, you can schedule a re-attempt at discovery. You need to specify the time in hours after which the discovery process is attempted again.

The screenshot shows the 'Discover MySQL Accounts' page in the Securden Privileged Account Manager. The page has a dark navigation bar with links: Dashboard, Accounts (active), Folders, Users, Groups, Audit, Sessions, Reports, and Admin. A search bar and a user profile icon are on the right. The main content area is titled 'Discover MySQL Accounts' and includes a 'Back' button. A help sidebar on the right explains that administrator credentials are needed for discovery.

Discover MySQL Accounts

You can discover the MySQL instances, the accounts thereof and add them to Securden. You can specify the IP range to discover the instances falling under that range. Alternatively you enter a single instance too.

Pre-requisite: You need to install MySQL connector. [Refer to this section for details.](#)

Step 1: Enter Connectivity Details

Discover ☒ Computers in IP range ☐ Single Computer

Start IP * End IP

Database Port * Default Database

Connection timeout(in seconds) *

☐ Retry discovery process again after 5 hours.

Help ⓘ
You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.
If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Step 2: Supply Administrator Credentials and Discover

Before Securden can discover accounts from the MySQL database, it needs to go through authentication. You need to specify the **username** and **password** of the administrator account.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover MySQL Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *
.....

[Advanced options](#)

[Back](#) [Discover](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Note: If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

You can populate all the discovered accounts under a specific account type and/or a specific folder.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover MySQL Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *
.....

[Advanced options](#)

[Back](#) [Discover](#) [Cancel](#)

Help

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Account Type: You can select one of the compatible account types from the drop-down. If you want to assign a different account type from the available list of types, you need to navigate to **Admin >> Account Management >> Account Types** and add a new custom account type or modify an existing custom account type according to your needs.

The screenshot shows the 'Privileged Account Manager' web interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' is on the right. The main heading is 'Discover MySQL Accounts' with a red 'Back' button. The section is titled 'Step 2: Supply Credentials'.

A message states: 'You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.'

Fields for 'Account Name' (containing 'admin') and 'Password' (masked with dots) are present.

The 'Advanced Options' section includes:

- 'Account Type' dropdown menu with 'MySQL' selected (highlighted with a red box).
- 'Folder in Securden' dropdown menu with '--None--' selected and a '[Add Folder]' link.
- A checkbox for 'Randomize passwords after accounts discovery' which is currently unchecked.

At the bottom are 'Back', 'Discover' (green), and 'Cancel' buttons.

On the right, a 'Help' section provides instructions on supplying administrator credentials and advanced options for account discovery.

Folder: You can open the drop-down menu and select the required folder from the folder tree.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover MySQL Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Search

- None-
- IT Infrastructure
 - API Test
 - Local Accounts
 - Open Connection
- None-

[Add Folder](#)

☐ Randomize passwords after accounts discovery ⓘ

[Back](#) [Discover](#) [Cancel](#)

Help ⓘ

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you want to create a new folder, you can click **[Add Folder]** and create a new one.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover MySQL Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *

Advanced Options

Account Type
MySQL

Folder in Securden
-None- [Add Folder](#)

☐ Randomize passwords after accounts discovery ⓘ

[Back](#) [Discover](#) [Cancel](#)

Help ⓘ

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Randomize Passwords After Discovery

Immediately following discovery, you have the choice to assign the accounts secure and unique passwords. If you select this option, Securden creates passwords for the accounts on the target devices according to the password rules you specify.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. The 'Accounts' tab is selected. The main heading is 'Discover MySQL Accounts' with a 'Back' button. The section is titled 'Step 2: Supply Credentials'. A message states: 'You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.' Below this, there are input fields for 'Account Name *' (containing 'admin') and 'Password *' (masked with dots). Under 'Advanced Options', there are dropdowns for 'Account Type' (MySQL) and 'Folder in Securden' (-None-). A checkbox labeled 'Randomize passwords after accounts discovery' is highlighted with a red box. At the bottom are 'Back', 'Discover', and 'Cancel' buttons. A help sidebar on the right contains information about supplying administrator credentials, advanced options, and the 'Randomize Passwords After Discovery' feature.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover MySQL Accounts Back

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *
admin

Password *

Advanced Options

Account Type
MySQL

Folder in Securden
-None- [Add Folder]

☒ Randomize passwords after accounts discovery ⓘ

Back Discover Cancel

Help ⓘ

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Once you have selected your preferences, click **Discover**.

The screenshot shows the 'Privileged Account Manager' web interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' and a user profile icon are on the right. The main heading is 'Discover MySQL Accounts' with a red 'Back' button. The section is titled 'Step 2: Supply Credentials'. A message states: 'You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.' Below this, there are input fields for 'Account Name *' (containing 'admin') and 'Password *' (masked with dots). Under 'Advanced Options', 'Account Type' is set to 'MySQL' and 'Folder in Securden' is set to '-None-' with an '[Add Folder]' link. A checkbox 'Randomize passwords after accounts discovery' is unchecked. At the bottom are 'Back', 'Discover' (highlighted with a red box), and 'Cancel' buttons. A 'Help' sidebar on the right provides additional instructions and options.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover MySQL Accounts [Back](#)

Step 2: Supply Credentials

You need to supply administrator credentials so as to enable Securden to scan the databases and fetch the accounts.

Account Name *

admin

Password *

Advanced Options

Account Type

MySQL

Folder in Securden

-None- [Add Folder](#)

☐ Randomize passwords after accounts discovery ⓘ

[Back](#) [Discover](#) [Cancel](#)

Help ⓘ

You need to supply administrator credentials so as to enable Securden to scan the instances and fetch the accounts.

If each instance in the IP range specified has different administrator credentials, you need to repeat discovery separately for each instance. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

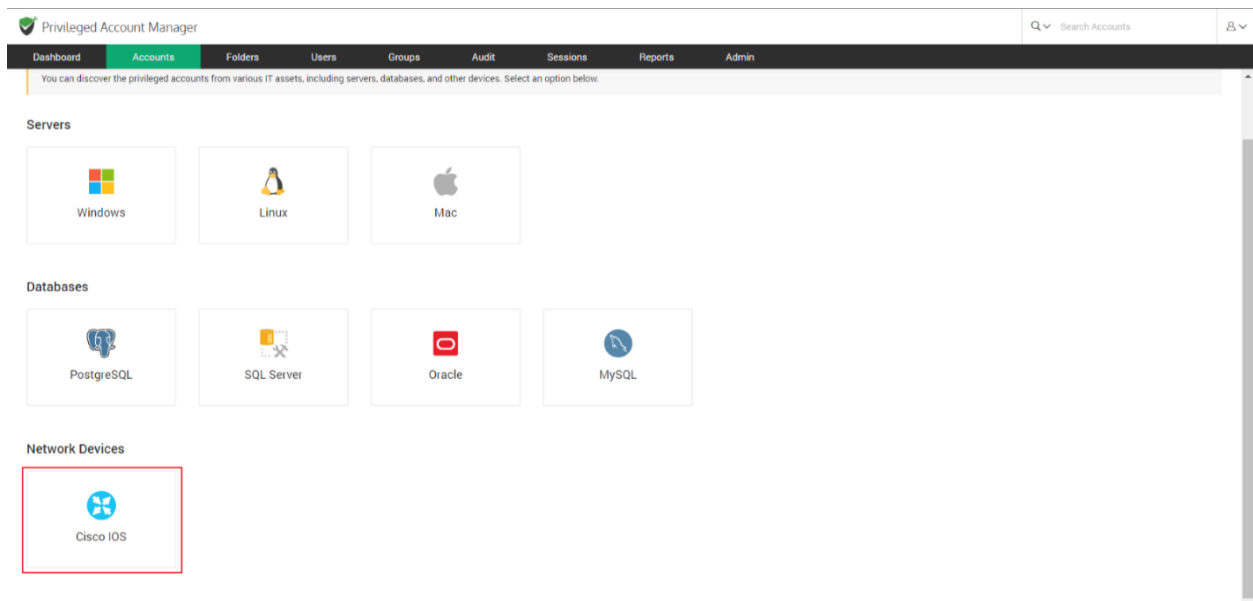
Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery if you choose this option. Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

The process takes a few minutes to complete. Once it is completed, complete results with a list of accounts, their status is displayed. You can view how many accounts were successfully imported.

Discovering and Importing accounts from Cisco IOS Devices

You can connect with network devices and discover the accounts present in them. To discover accounts from Cisco IOS devices, navigate to **Accounts >> Add >> Discover Accounts >> Cisco IOS Devices**.



Discovering accounts from network devices is a two-step process.

Step 1: Connecting to the Network Devices

For Securden to establish connectivity, you need to specify the IP addresses of the target network devices. You have the option to discover devices from a single device or from a set of devices in an IP range.

If you choose **Single Device**, you need to specify the **Hostname/IP address** of the target network device.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Cisco IOS Accounts Back

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

Step 1: Enter Connectivity Details

Discover ☐ Devices in IP range ☒ **Single Device**

Hostname/IP Address *

Connection timeout(in seconds) *

10

☐ Retry discovery process again after 5 hours.

Select gateway or via channel ☐ Remote Gateway ☒ Unix Connector

Select Unix Connector

Search unix connector

Next Cancel

Help

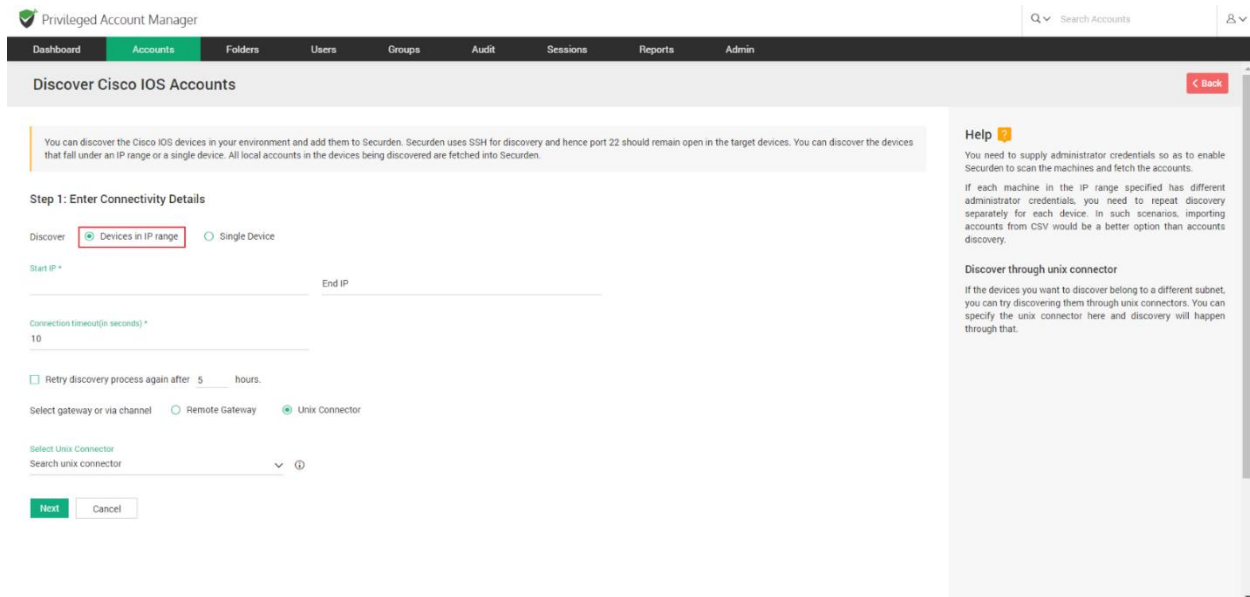
You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

If you choose **Devices in IP Range**, you need to specify the **IP Range** of the target devices. i.e., You need to specify the **Start IP** and **End IP** of the range of devices to be scanned.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Cisco IOS Accounts

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

Step 1: Enter Connectivity Details

Discover ☒ Devices in IP range ☐ Single Device

Start IP * End IP

Connection timeout(in seconds) * 10

☐ Retry discovery process again after 5 hours.

Select gateway or via channel ☐ Remote Gateway ☒ Unix Connector

Select Unix Connector

Search unix connector

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

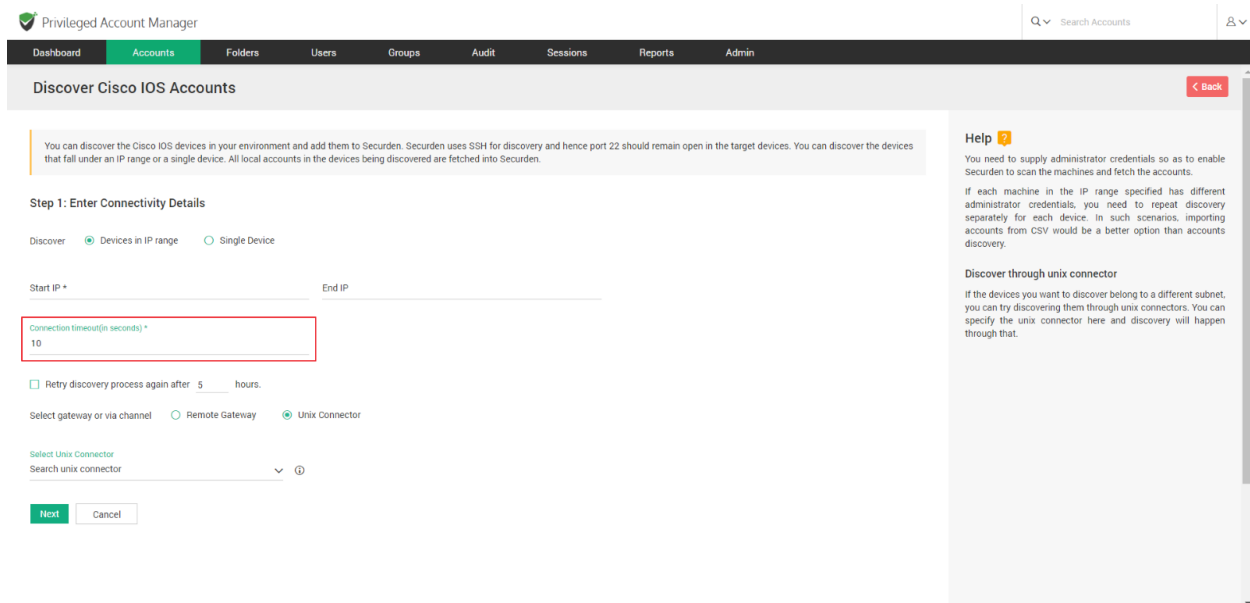
Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Once the IP addresses of the devices have been specified, you need to provide the following details.

Connectivity Timeout

The maximum time in seconds Securden can attempt to establish connectivity with the devices before terminating the process.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Cisco IOS Accounts

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

Step 1: Enter Connectivity Details

Discover ☒ Devices in IP range ☐ Single Device

Start IP * End IP

Connection timeout(in seconds) * 10

☐ Retry discovery process again after 5 hours.

Select gateway or via channel ☐ Remote Gateway ☒ Unix Connector

Select Unix Connector

Search unix connector

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Time delay for subsequent attempts

If connectivity to one or more devices cannot be established at present, Securden can attempt to connect with the devices at a later time. You need to specify the time (in hours) after which the attempt to connect should be made.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Cisco IOS Accounts

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

Step 1: Enter Connectivity Details

Discover ☒ Devices in IP range ☐ Single Device

Start IP * End IP

Connection timeout (in seconds) *
10

☒ Retry discovery process again after 5 hours.

Select gateway or via channel ☐ Remote Gateway ☒ Unix Connector

Select Unix Connector
Search unix connector

Next Cancel

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Discovering through Remote Gateway

If the devices reside in a different network than the Securden server, you can route the connection through a remote gateway. You can select the appropriate remote gateway from the drop-down and the discovery will happen through the selected gateway.

If no suitable gateway is available, navigate to **Admin >> Remote Sessions and Recordings >> Remote Gateway** and add the required gateway.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (selected), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' is on the right. The main heading is 'Discover Cisco IOS Accounts'. Below it, a help box explains that Securden uses SSH for discovery and port 22 should be open. The 'Step 1: Enter Connectivity Details' section contains the following fields and options:

- Discover:** Radio buttons for 'Devices in IP range' (selected) and 'Single Device'.
- Start IP:** A text input field.
- End IP:** A text input field.
- Connection timeout (in seconds):** A text input field with the value '10'.
- Retry discovery process again after:** A checkbox (unchecked) followed by a text input field with the value '5' and the unit 'hours'.
- Select gateway or via channel:** Radio buttons for 'Remote Gateway' (selected) and 'Unix Connector'.
- Select Remote Gateway:** A dropdown menu with the text 'Search remote gateway' and a downward arrow.
- Buttons:** 'Next' (green) and 'Cancel' (grey).

On the right side, there is a 'Help' section with a question mark icon. It contains two paragraphs: one about supplying administrator credentials and another about discovering through a Unix connector.

Discovering through a Unix Connector

If the devices you want to discover belong to a different subnet, you can try discovering them through Unix connectors. You can select a Unix connector from the drop-down and discovery will happen through the selected connector.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. The main heading is 'Discover Cisco IOS Accounts'. A red 'Back' button is in the top right corner.

Step 1: Enter Connectivity Details

Discover: ☒ Devices in IP range ☐ Single Device

Start IP * End IP

Connection timeout(in seconds) *

☐ Retry discovery process again after 5 hours.

Select gateway or via channel: ☐ Remote Gateway ☒ Unix Connector

Select Unix Connector
Search unix connector

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

To add a new Unix connector, navigate to **Admin >> Remote Distributors >> Unix Connector**.

Once all the required details have been provided, click **Next**.

Step 2: Enter Credentials and Discover

Securden needs to authenticate the connection with devices to perform discovery. You can specify the root account credentials or sudo (Superuser Do) user credentials for this purpose. Securden will also use the administrator credentials for performing remote actions like password verification and reset apart from accounts discovery.

Note: If each machine in the specified IP range has different administrator credentials, you need to repeat discovery separately for each device. In such

scenarios, importing accounts from files would be a better option than account discovery.

You need to supply two sets of credentials, one for remote log in and the other to fetch the accounts and onboard it to Securden.

Supply remote login credentials

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Cisco IOS Accounts

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☒ Password ☐ PKI

Account Name *
admin

Password *

Supply enable account credentials to fetch account

☐ Use remote login credentials as specified above, it has administrative privilege.

Account Name *

Password

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

You need to provide the credentials of an administrator user on the target device for Securden to login securely.

- i. You need to specify the **Account Name** of the administrator account.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Cisco IOS Accounts [Back](#)

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☒ Password ☐ PKI

Account Name *
admin

Password *

Supply enable account credentials to fetch account

☐ Use remote login credentials as specified above, it has administrative privilege.

Account Name *

Password *

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

- ii. You can choose between a **Password** or a **Public Key Infrastructure (PKI file)** as the authentication type.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Cisco IOS Accounts [Back](#)

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☐ Password ☒ PKI

Account Name *
admin

Private Key ☒ Select from Securden ☐ Select from your computer

Select from Securden
Search Accounts

Supply enable account credentials to fetch account

☐ Use remote login credentials as specified above, it has administrative privilege.

Account Name *

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you choose to authenticate using a PKI file, you have two options.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Cisco IOS Accounts

[< Back](#)

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type ☐ Password ☒ PKI

Account Name *
admin

Private Key ☒ Select from Securden ☐ Select from your computer

Select from Securden
Search Accounts

Supply enable account credentials to fetch account

☐ Use remote login credentials as specified above, it has administrative privilege.

Account Name *

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

You can either

1) choose an SSH key stored in Securden from the drop-down menu.

(or)

2) upload the key file from your computer.

If you choose to upload a file from your computer, you need to provide the **passphrase** required to access the file.

The screenshot shows the Securden Privileged Account Manager web interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar and user profile icon are on the right. The main heading is 'Discover Cisco IOS Accounts' with a '< Back' button. The page is titled 'Step 2: Enter Credentials and Discover'. A yellow box contains instructions: 'You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.'

Supply remote login credentials

Authentication type: ☐ Password ☒ PKI

Account Name *
admin

Private Key: ☐ Select from Securden ☒ Select from your computer

Select from your computer *
Choose a file: [Browse] Passphrase []

Supply enable account credentials to fetch account

☐ Use remote login credentials as specified above, it has administrative privilege.

Account Name *

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Credentials for Fetching Accounts

Once the credentials for remote login are supplied, you need to specify the administrator credentials which are required to fetch the accounts present in the devices.

If the account used for remote login has administrative privilege, then you can use the same credentials for fetching accounts. To use the same credentials, select the checkbox named **Use remote login credentials as specified above**.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discover Cisco IOS Accounts

[Back](#)

Step 2: Enter Credentials and Discover

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts. First, you should supply the credentials to remotely log in to the machine. Then you need to supply either the 'sudo' or 'root' credentials to discover the accounts from the machines.

Supply remote login credentials

Authentication type: ☒ Password ☐ PKI

Account Name *
admin

Password *

Supply enable account credentials to fetch account

☒ Use remote login credentials as specified above, it has administrative privilege.

Account Name *

Password *

Help

You need to supply administrator credentials so as to enable Securden to scan the machines and fetch the accounts.

If each machine in the IP range specified has different administrator credentials, you need to repeat discovery separately for each device. In such scenarios, importing accounts from CSV would be a better option than accounts discovery.

Discover through unix connector

If the devices you want to discover belong to a different subnet, you can try discovering them through unix connectors. You can specify the unix connector here and discovery will happen through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you are using separate administrator credentials for fetching accounts, you need to specify the account name and password for the same.

Important:

When choosing to use the same remote login credentials for fetching accounts,

1. For **Password** based authentication, you need not specify the account name or the password.
2. For **PKI** authentication, you need to specify the password of the account alone.

Advanced Options

You have the options to add all the discovered accounts into a specific folder and assign them a specific account type. This will help mitigate the efforts required for classifying the accounts at a later time.

1. If you want to assign a specific account type to all the imported accounts, you can select the required account type from the drop down.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

admin

Password *

Supply enable account credentials to fetch account

☐ Use remote login credentials as specified above, it has administrative privilege.

Account Name *

Password

Advanced Options

Account Type

Cisco IOS

Folder in Securden

-None-

☐ Randomize passwords after accounts discovery

Back Discover Cancel

through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

2. If you want to add all the imported accounts to a folder, you can select the required folder from the drop down.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

admin

Password *

Supply enable account credentials to fetch account

☐ Use remote login credentials as specified above, it has administrative privilege.

Account Name *

Password

Advanced Options

Account Type

Cisco IOS

Folder in Securden

-None-

☐ Randomize passwords after accounts discovery

Back Discover Cancel

through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you want to create a new folder for this purpose, you need to click on **[Add Folder]**.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

admin

Password *

Supply enable account credentials to fetch account

☐ Use remote login credentials as specified above, it has administrative privilege.

Account Name *

Password

Advanced Options

Account Type

Cisco IOS

Folder in Securden

-None- [Add Folder](#)

☐ Randomize passwords after accounts discovery ⓘ

Back Discover Cancel

through that.

Advanced Options

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.

Randomize Passwords After Discovery

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

3. You have the option to assign strong and unique passwords to the accounts at the time of discovery.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. The 'Accounts' tab is active. The main form is titled 'Discover' and contains the following fields and options:

- Username:** A text input field with the value 'admin'.
- Password:** A password input field with a strength indicator icon.
- Supply enable account credentials to fetch account:** A checkbox labeled 'Use remote login credentials as specified above, it has administrative privilege.' which is currently unchecked.
- Account Name:** A text input field.
- Password:** A password input field with a strength indicator icon.
- Advanced Options:**
 - Account Type:** A dropdown menu with 'Cisco IOS' selected.
 - Folder in Securden:** A dropdown menu with '-None-' selected. A link '[Add Folder]' is visible next to it.
 - Randomize passwords after accounts discovery:** A checkbox that is currently unchecked. It has a small information icon (i) to its right.

At the bottom of the form are three buttons: 'Back', 'Discover' (highlighted in green), and 'Cancel'.

On the right side of the interface, there is a sidebar with the following content:

- through that.**
- Advanced Options**

If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.
- Randomize Passwords After Discovery**

You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

Note: The credentials used for authentication will not be randomized if this option is chosen.

Once all the required parameters have been specified, click **Discover**.

The screenshot shows the Securden Privileged Account Manager web interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. Below the navigation bar, the 'Discover' button is highlighted with a red box. The form contains the following fields and options:

- admin** (text input)
- Password *** (password input with eye icon)
- Supply enable account credentials to fetch account**
 - ☐ Use remote login credentials as specified above, it has administrative privilege.
- Account Name *** (text input)
- Password** (password input with eye icon)
- Advanced Options**
 - Account Type**: Cisco IOS (dropdown menu)
 - Folder in Securden**: --None-- (dropdown menu with [Add Folder](#) link)
 - ☐ Randomize passwords after accounts discovery ⓘ
- Buttons**: Back, **Discover** (highlighted), Cancel

On the right side, there is a sidebar with the following content:

- through that.
- Advanced Options**
 - If you want the accounts being discovered fall under a specific account type classification and a folder, you select them as part of the advanced options. This will save some manual editing efforts after discovering the accounts.
- Randomize Passwords After Discovery**
 - You have the option to assign strong and unique passwords to the accounts immediately after discovery. If you choose this option, Securden generates passwords based on the password policy specified and assigns them to the accounts on target devices.

The process take a few minutes to complete. Once it is completed, complete results with a list of accounts, their status is displayed. You can view how many accounts were successfully imported.

Importing Accounts from CSV/XLSX Files

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

Formatting your File for Importing

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

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Import Accounts From File

This option helps you add multiple accounts at one go. The input for importing accounts may be in the form of a standard CSV file or an XLSX file. Typically each line in the file is added as an account and all the lines in the file should be consistent having the same number of fields.

CSV **XLSX**

Specify how each entry in your CSV has been separated

Delimiter
Comma Separated values

Classification ☒ Work ☐ Personal

Select the type under which the accounts are to be imported

Account Type
Windows Member

Choose a file **Browse**

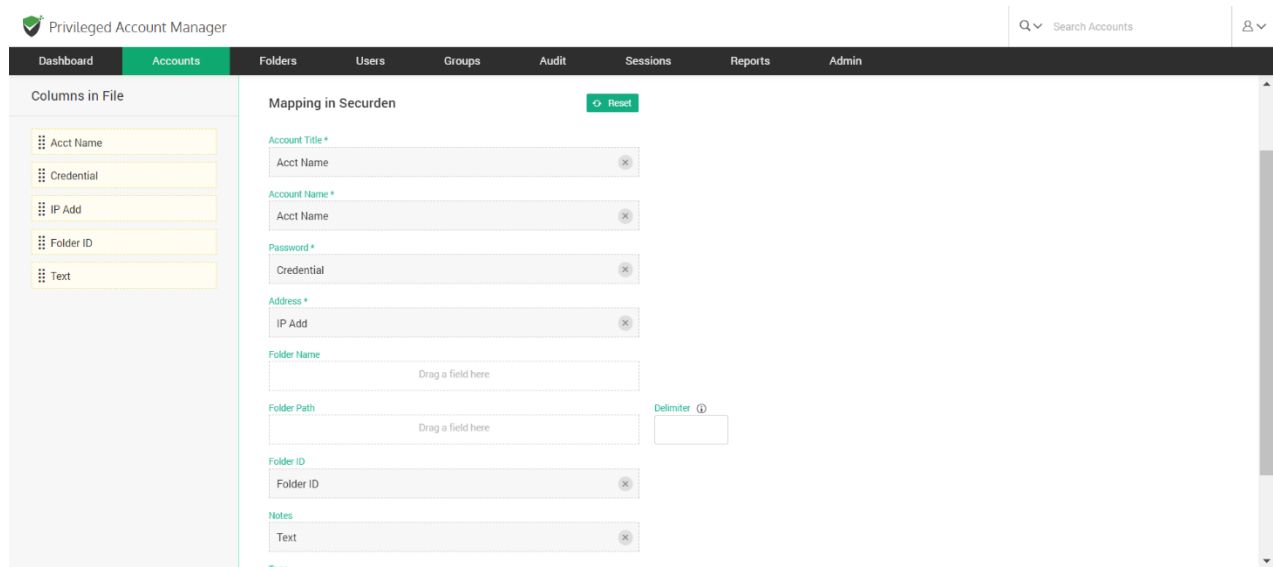
Choose Parent Folder

1. You need to select the type of file you want to import from.
2. If you select the file type **CSV**, you need to specify the delimiter used to separate different account attributes.
3. You need to select an account type that is suitable for all the accounts stored in the file. If such an account type doesn't exist, you need to create a suitable account type for this purpose. Navigate to **Admin >> Account Management >> Account Types** to add a new account type.
4. Once the account type is finalized, you need to browse and select the file you want to upload. Click **Browse** and select the required file on your computer and click **Open**.
5. You need to select a parent folder to which the imported accounts will be added.
6. Click **Next**.

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

Mapping

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



For example, you can map

Acct Name -- > Account Title

Acct Name ---> Account Name

Credential --> Password

IP Add - -> URL

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

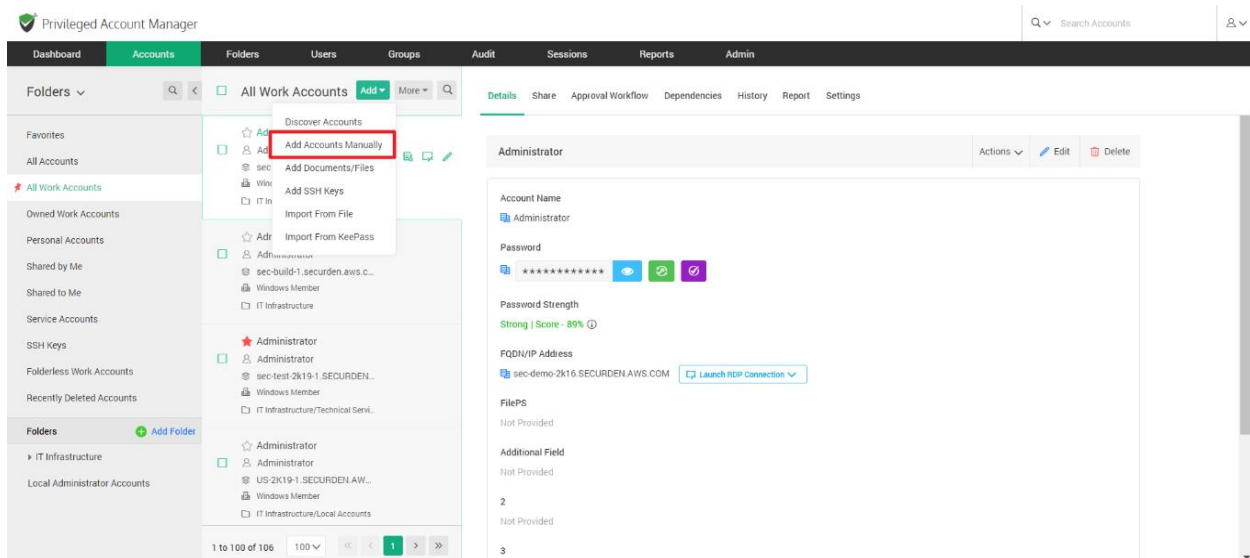
extra --> Extra (additional field added by creating a new account type)

grouping ---> Folders.

Adding Accounts Manually

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

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



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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Search Accounts

Add Account

☒ Work ☐ Personal

Account Title *

Account Type: Windows Member

Account Details

Account Name *

Password *

FQDN/IP Address *

Folder: --None--

FilePS *

Choose a file Browse

Additional Field

2

two

3

value1

abc

Choose a file Browse

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.

Account Name

depicts the username or login name of the account being added.

Password

enter the actual password of the account. Thereafter, Securden will manage the password.

FQDN/IP Address

enter the FQDN/IP Address of the machine to which this

Work Accounts

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

Personal Accounts

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

Note:

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

- 2) Personal Accounts cannot be viewed by any other user. Even the most privileged role like the Super Administrator would not have the ability to view personal accounts belonging to individual users.
- 3) You may disable users from creating and storing personal accounts. Navigate to **Admin >> Configurations** to configure this option.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Configurations

limited time-duration:

If new administrator users are created when a user makes use of temporary administrator privileges, would you like to remove the newly created user from the admin group? No [Change](#)

Technician Access

Would you like to configure the MFA system used in the organization to be the additional authentication factor during technician access by users? Yes [Change](#)

Do you want to restrict the time duration for Technician access? Once configured, users will have to specify a time duration (in minutes) within maximum duration specified. No restrictions [Change](#)

Personal

Do you want to allow your users to manage personal accounts? Allowed for All [Change](#)

Browser Extension

Do you want to allow automatic submission of credentials for directly logging in to websites using browser extension? Enabled for All [Change](#)

When accounts are shared with 'Open Connection' permission, do you want to allow automatic filling of credentials on websites using browser extension? Enabled for All [Change](#)

Do you want the Securden browser extension's auto-fill icon to be present in all input fields of the web pages? Disabled for All [Change](#)

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Add Account

☒ Work ☐ Personal

Account Title *

Account Type Windows Member

Account Details

Account Name * Password *

FQDN/IP Address * Folder -None-

FilePS * Choose a file Browse Additional Field

2 two 3 value1

abc Choose a file Browse

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.

Account Name

depicts the username or login name of the account being added.

Password

enter the actual password of the account. Thereafter, Securden will manage the password.

FQDN/IP Address

enter the FQDN/IP Address of the machine to which this

- **Account Title:** The account title helps uniquely identify the account added, this makes it easier to add to folders and share with users as well.
- **Account Type:** You can select an existing account type added in Securden or choose to create a new account type for the account being created. This helps classify the accounts for easy management and reporting. If you want to add a new type, you can do so from **Admin >> Account Management >> Account Types**.

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

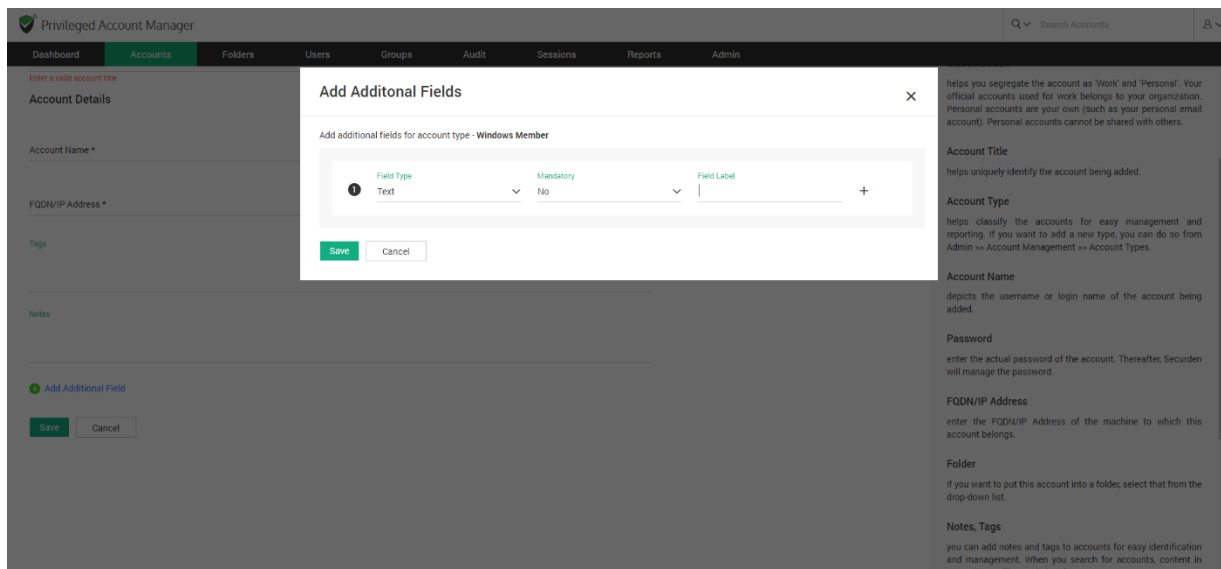
- **Account Name:** This depicts the username or login name of the account being added.
- **Password:** In this field you enter the actual password of the account. After doing so, Securden will take over the management of the password including periodic password resets if needed.
- **Folder:** If you want to add this account to a folder, you can select one of the existing folders in Securden or add a new folder by clicking on the **Add folder** option from the drop down.
- **File:** You can browse and select a file from your computer to attach with the account.
- **Notes and Tags:** You can add notes and tags to accounts for easy identification and management. When you want to search for accounts, content in notes / tags will come in handy.

Adding Additional Fields:

You can add any number of additional fields for a selected account type. The fields you add for a particular account type will be displayed for all accounts belonging to this account type.

Click on the **Add Additional Fields** to enter a text, password or file associated with the account.

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



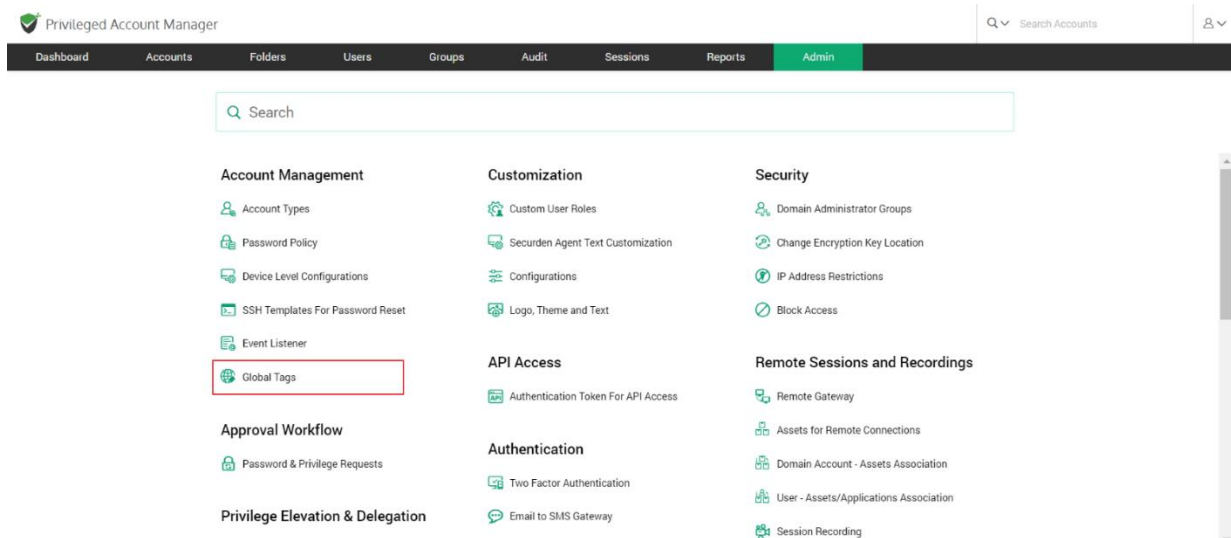
Once done with entering all the fields under Add Account click **Save** and your account will be added to Securden.

Global tags

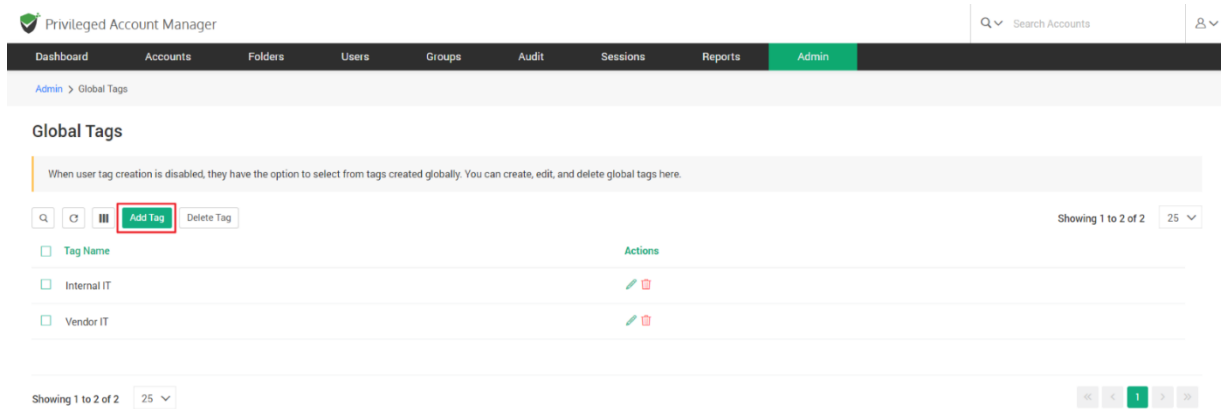
When user tag creation is disabled, they have the option to select from a list of globally available tags to associate with each account.

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

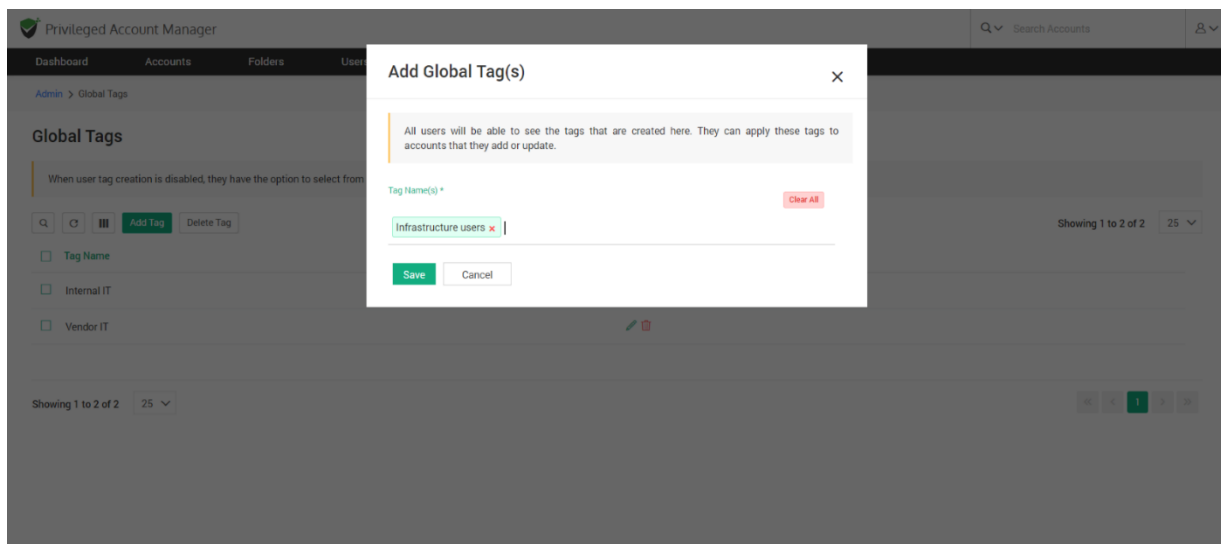
To configure Global tags, navigate to **Admin >> Account Management >> Global tags**.



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



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

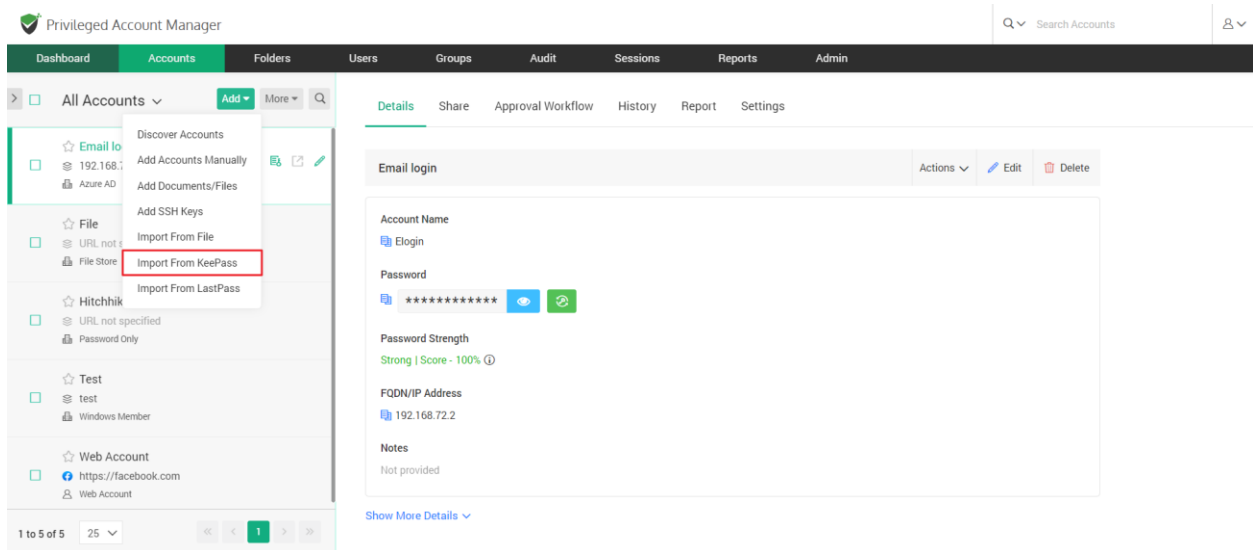


On configuring global tags, users can associate tags with accounts shared with them or owned by them. The globally created tags are displayed as a drop-down items when each account is created.

Importing accounts from KeePass

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

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



In the GUI that opens,

1. Select the appropriate file format – Either XML (2.X) OR XML (1.X)

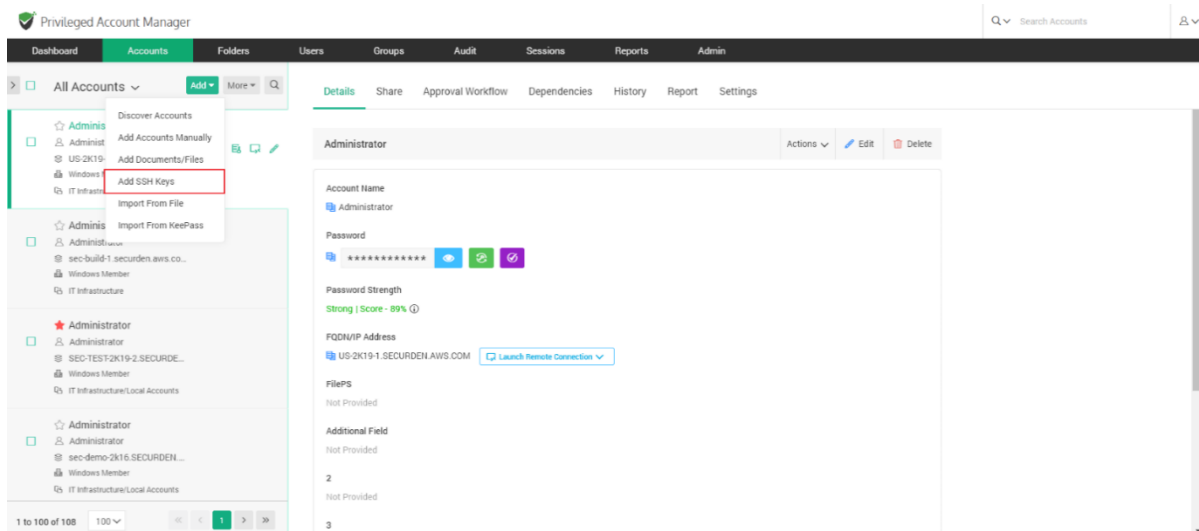
The screenshot shows the 'Privileged Account Manager' web interface. The top navigation bar includes 'Dashboard', 'Accounts' (highlighted), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar on the right says 'Search Accounts'. Below the navigation bar, there are two large buttons: 'XML (2.X)' with a green checkmark and 'XML (1.X)' with a grey circle. Underneath these buttons, there are radio buttons for 'Classification' with 'Work' selected and 'Personal' unselected. A section titled 'Select the type under which the accounts are to be imported' contains a dropdown menu for 'Account Type' currently set to 'Windows Member'. Below this is a section 'XML file to be imported' with a text input field containing the placeholder 'Browse and select the file exported from KeePass.' and a 'Browse' button. At the bottom, there are two checkboxes: 'Allow duplicates to be added.' (unchecked) and 'Create folders as in KeePass' (checked). Finally, there are 'Submit' and 'Cancel' buttons.

2. Choose whether the accounts imported should be classified as Work or Personal. (**Note:** Personal accounts cannot be shared)
3. Select the account type under which the accounts are to be imported.
4. Choose and upload the XML file.
5. When the checkbox **Create folders as in KeePass** is selected, the folder structure that was maintained in KeePass will be replicated in Securden.
6. Finally, choose the parent folder from the drop-down list and click **Submit**.

Add and Manage SSH Keys

The provision to manage SSH keys helps you store the keys securely, track their usage, and associate them with required Unix devices for authentication and remote access.

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



In the GUI that opens, enter the following details:

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Account Title * SSH Key 1 Account Type SSH Key

Account Details

Private Key * Choose a File Passphrase

PuTTY Private Key (.ppk) Choose a File PPK Passphrase

Folder --None--

Tags

Notes

Add Additional Field

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.

Account Name
depicts the username or login name of the account being added.

Password
enter the actual password of the account. Thereafter, Securden will manage the password.

FQDN/IP Address
enter the FQDN/IP Address of the machine to which this account belongs.

Folder
if you want to put this account into a folder, select that from the drop-down list.

Account Title: Helps uniquely identify the account being added.

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

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

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

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

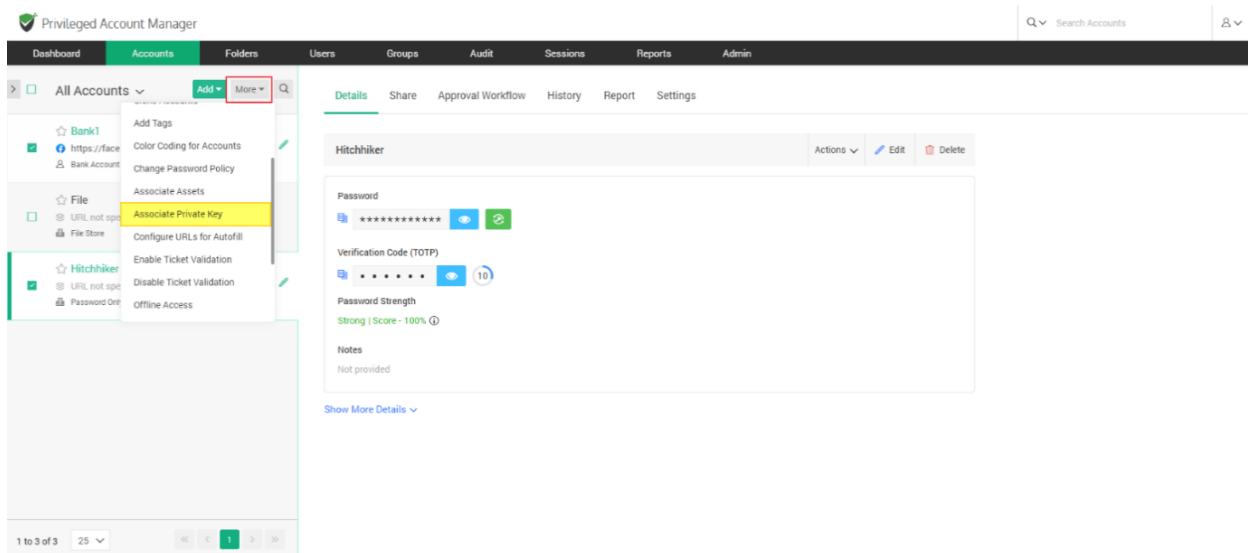
Folder: If you want to put this SSH Key account into a folder, select the required folder from the drop-down list.

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

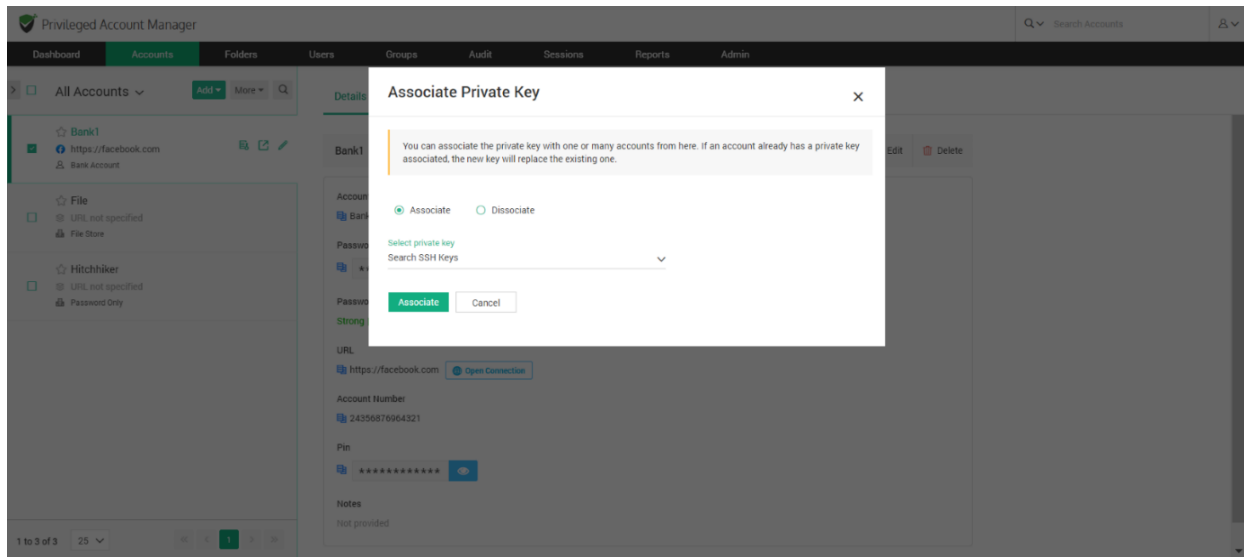
Once you enter all the details, click on **Save** to store the SSH Key.

Associating the SSH Keys to Accounts

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



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

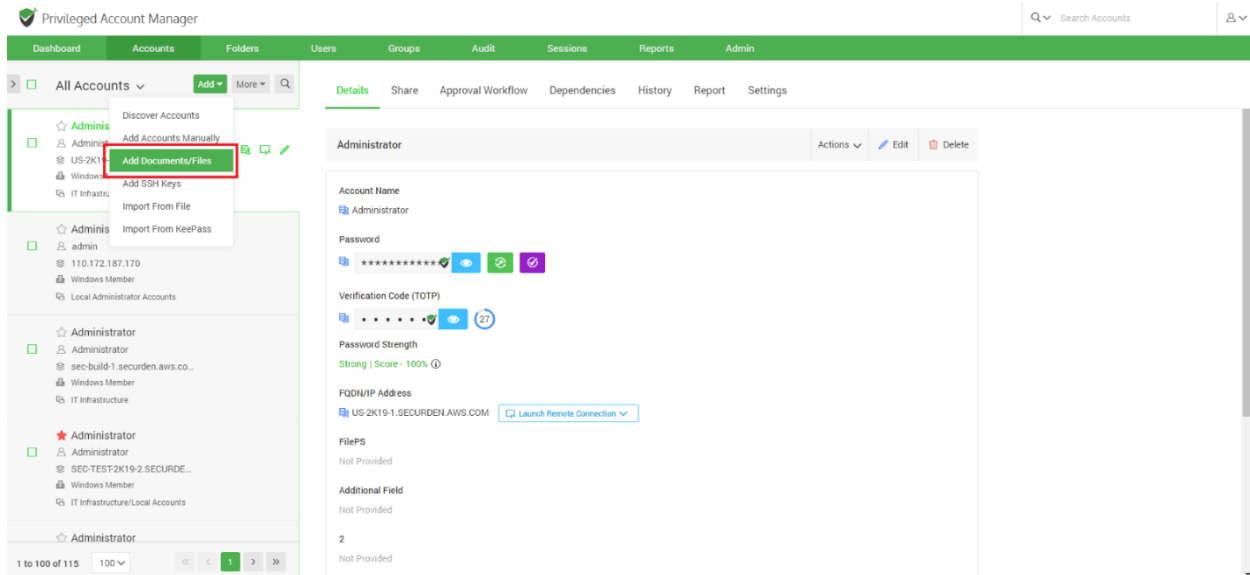


After associating the key, you can open direct connections with remote Unix devices using private key authentication.

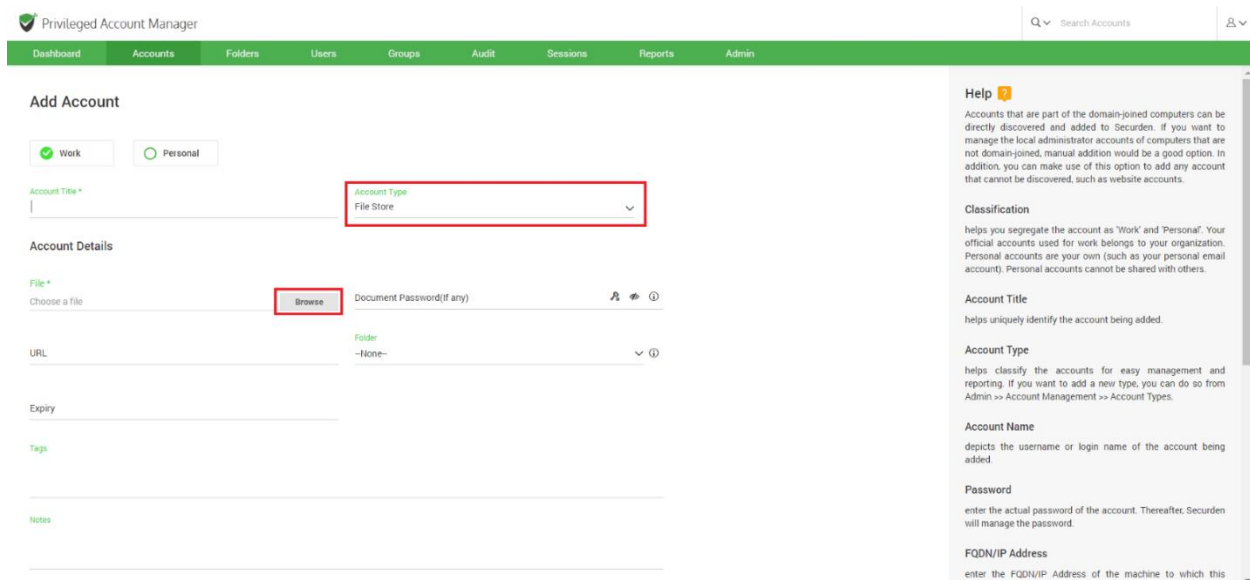
Add Documents/Files

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

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



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



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

Account Title: Provide a suitable title for identification purposes.

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

Browse: Select the required file from your device.

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

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

Add into a folder

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

Add Additional Fields

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

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

- Choose a Field type, either a text, password or file.

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

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

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

View Account Details, Passwords

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

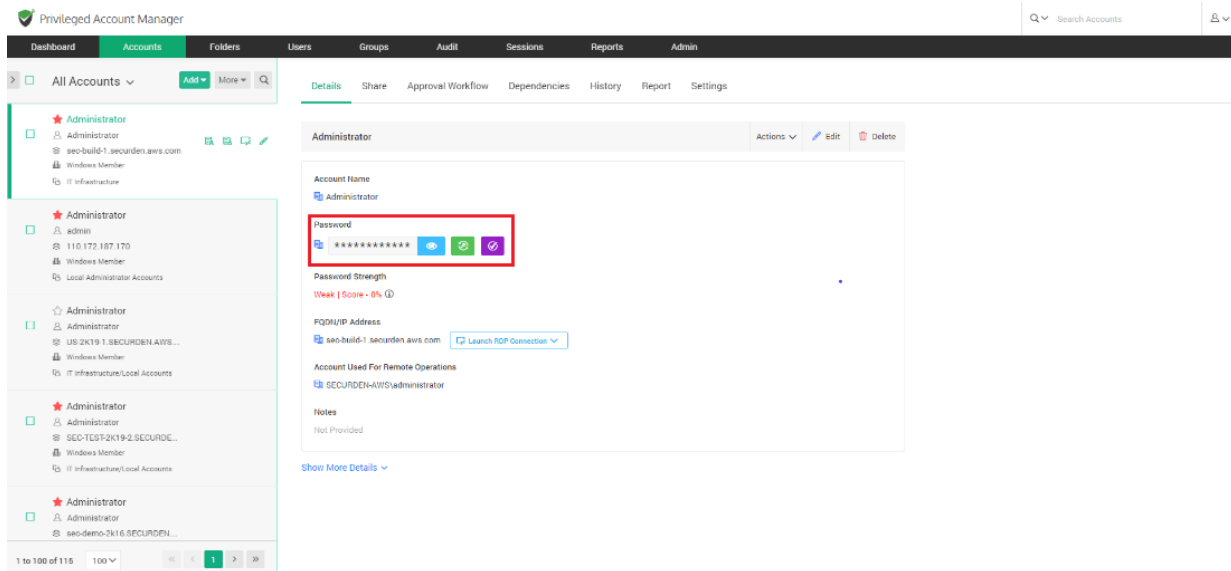
The basic details of an account are displayed on the right pane when you click on any account. This includes the account name, password, IP address and other security related information. The **Details** section provides a quick overview of the selected account in the inventory.

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

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

- **Account Name**

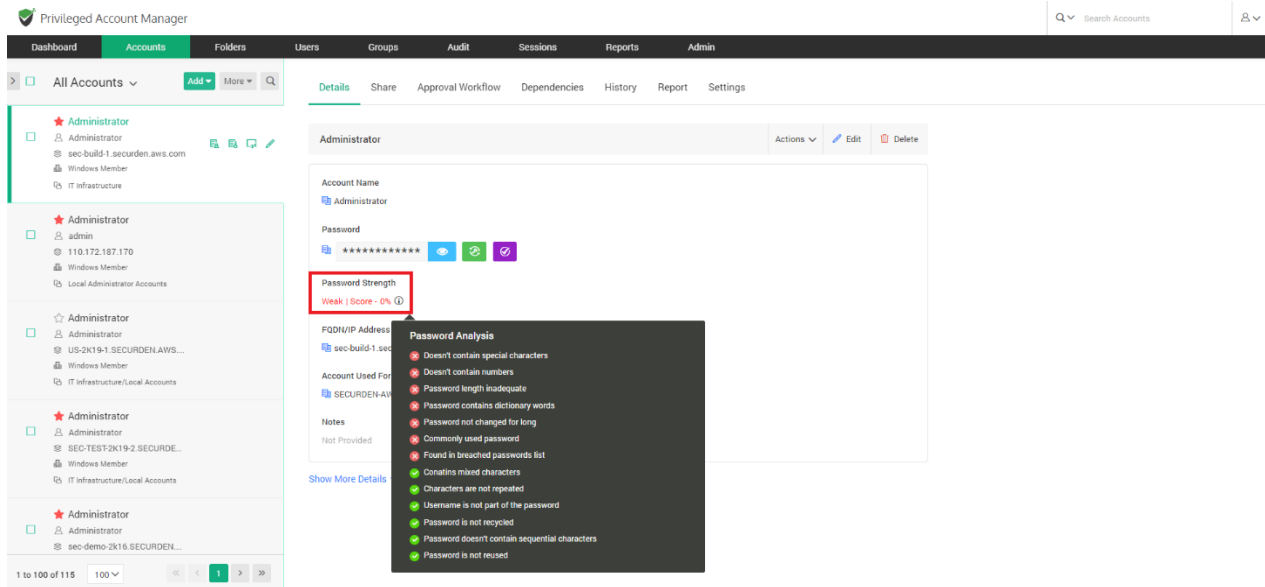
- **Password** - On the right side, next to the Password field, there are three options to Show/Hide Password, Change Password, and Verify Password.



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

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

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



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

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

Password Management Operations

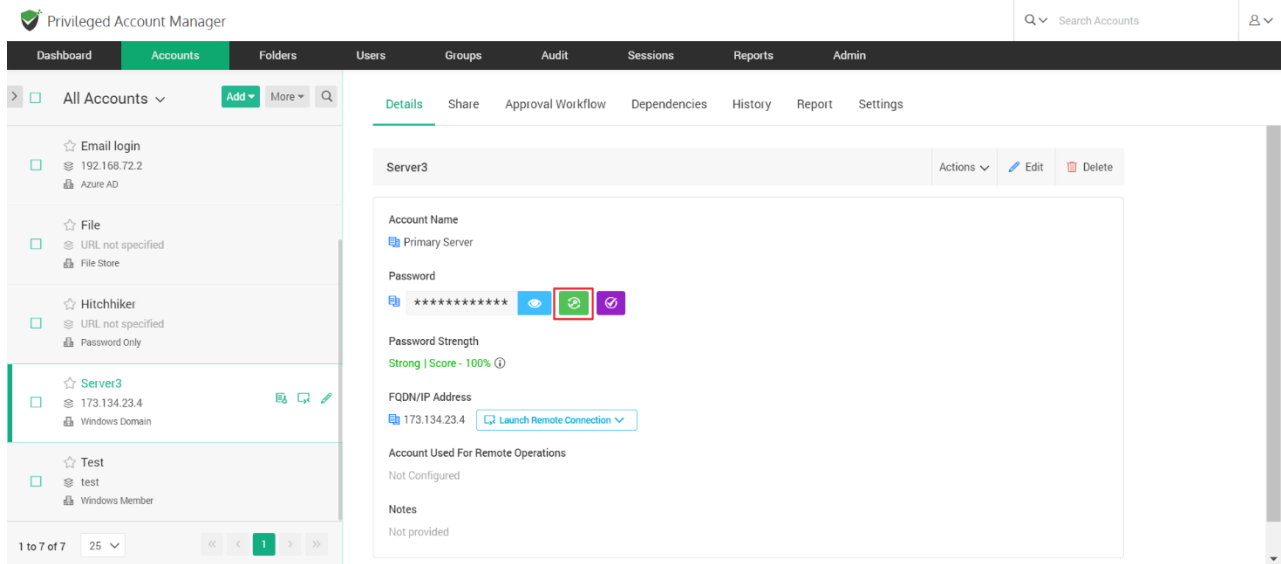
You can carry out certain operations like remote password resets and password changes in PAM.

Change Password

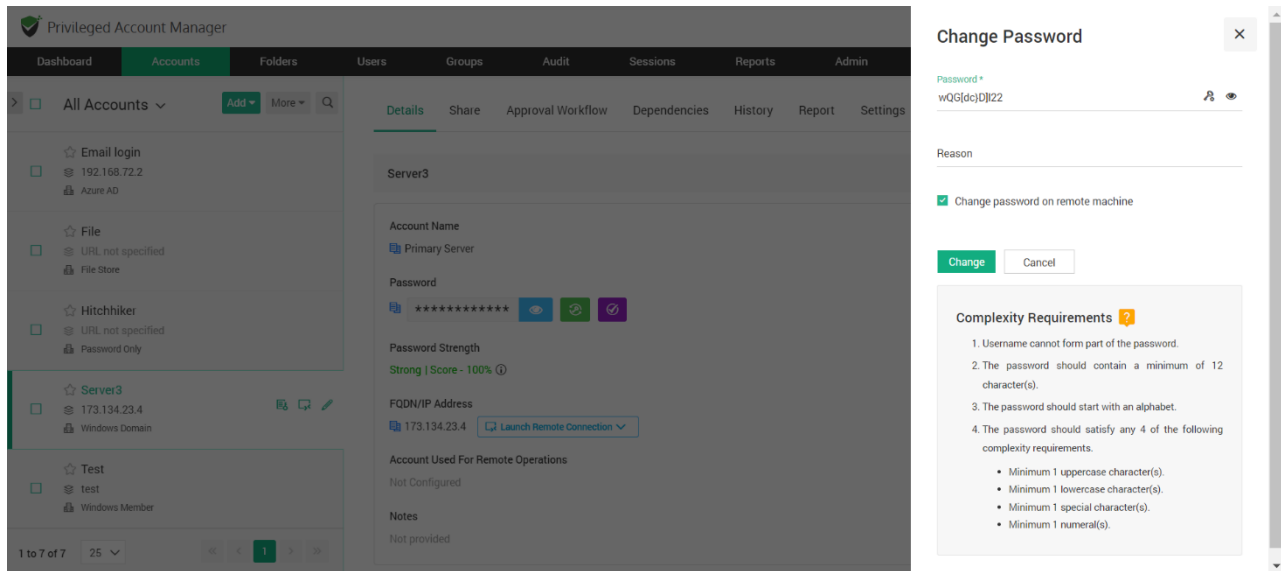
You can change the password of an account locally in Securden by navigating to the **Accounts** tab and selecting the account from the left panel whose password needs to be changed. On the right panel under the **Details** section,

on the right side of the **Password** field there are three options to Show/Hide Password, Change, and Verify the password.

Click on the **Change** password icon, a **Change Password** window opens.



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



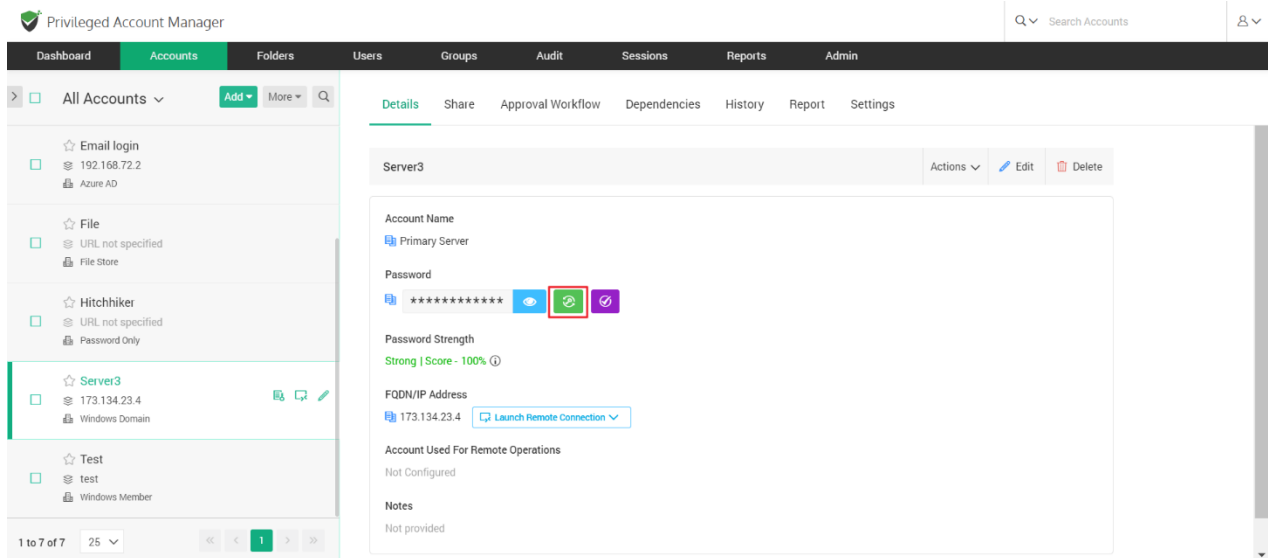
The new password being created must satisfy the complexity requirements so that the strength and robustness of the password is ensured.

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

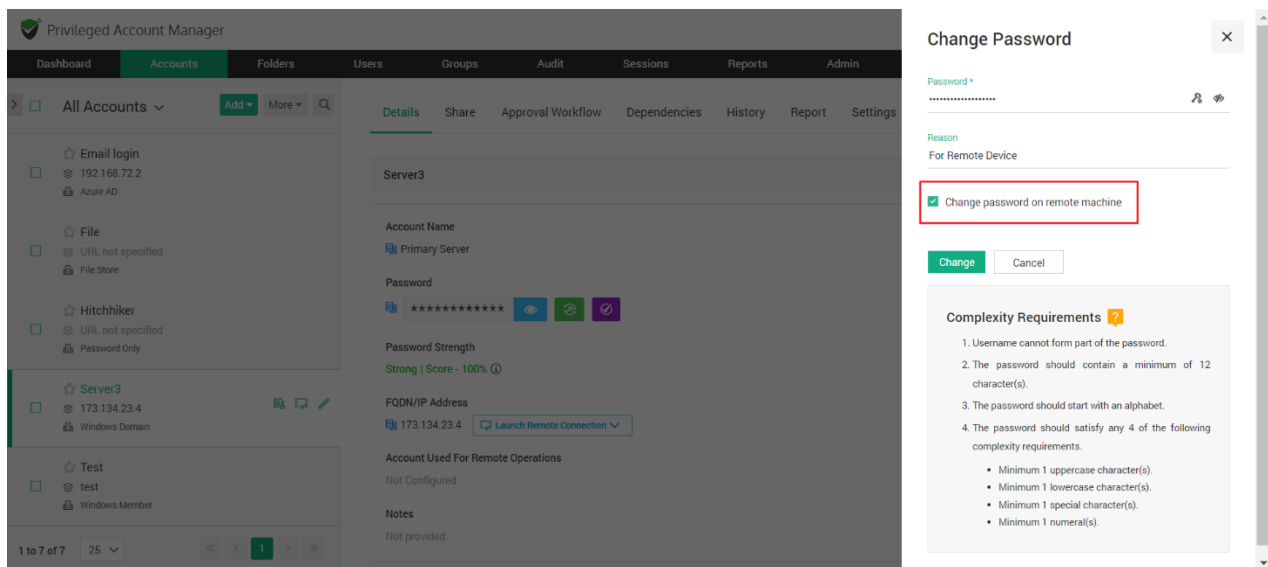
Remote Password Reset

With Securden, you can reset passwords of accounts on remote devices from the **Accounts >> Details** section in the GUI.

Select the account from the left panel and click on the **Details** tab and then click on the **Change** password icon next to the **Password** field.



In the pop-up window, change the password and then select the checkbox **Change password on remote machine**.

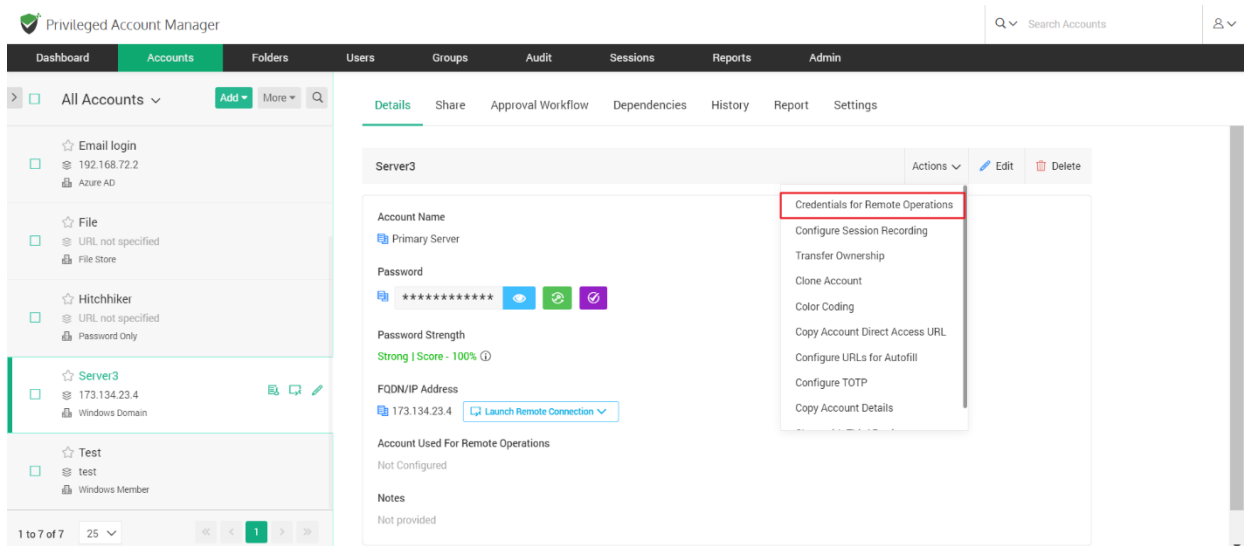


While resetting the passwords, you can take the help of Securden's password generator, which helps generate strong passwords. (**Generate password** is located beside the eye icon).

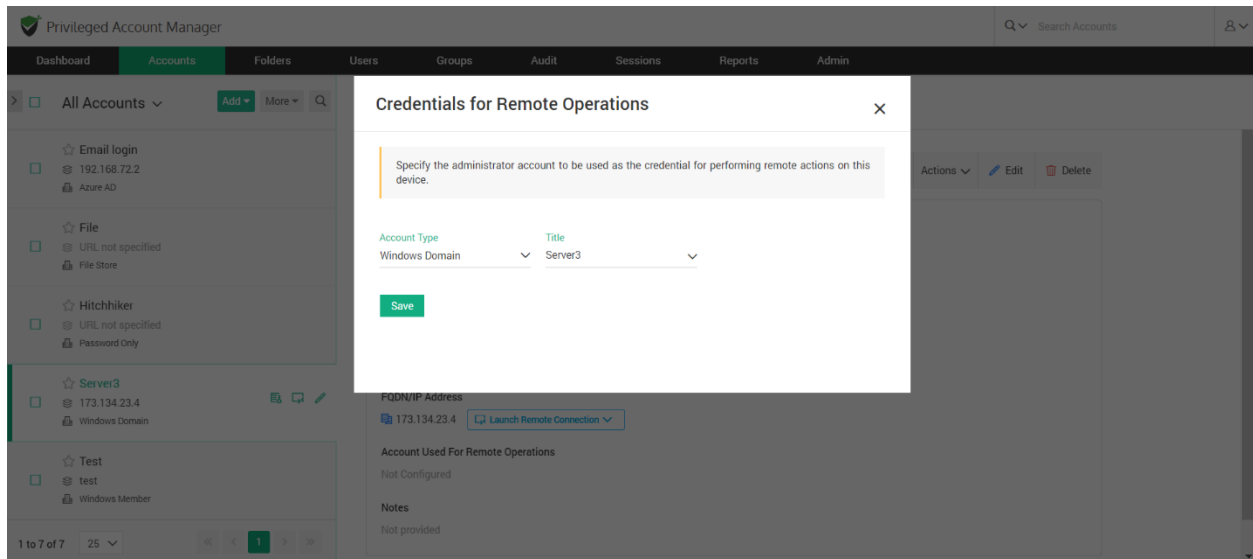
Remote password reset is supported for IT assets like servers, databases, and other network devices. To reset passwords of other accounts, you need to copy the generated password and manually carry out the password reset.

Troubleshooting Tip

Sometimes, the password is not reset successfully if the credentials for performing remote actions are not supplied. This can be resolved by supplying the required credentials in **Accounts >> Details >> Actions >> Credentials for Remote Operations**.



To perform remote actions on a particular device, select an account stored in Securden with the administrator credentials to log into the remote machine. Select the account from the drop-down then click **Save**.



Alternatively, navigate to **Admin >> Device Level Configurations** and select the device type and the device name. Click the **Remote Credentials** button on the right pane.

To perform remote actions on a particular device, specify the administrator account credentials. Select the account type, the account title, and then click **Save**.

The screenshot shows the 'Admin' tab in the Privileged Account Manager. The left sidebar lists 'Device Types' including AD Service Accounts, Cisco IOS, Linux, Mac, MySQL, Oracle, PostgreSQL, SQL Server, and Windows Domain. The main area displays a table of devices with columns for 'Device Types' and 'IP Address'. The table shows 5 devices, with the first one being '10.0.0.60'. Below the table, there are pagination controls showing '1 to 5 of 5' and a '25' dropdown. On the right, the 'Remote Credentials' section is active, showing a dropdown for 'Account Type' (Windows Domain) and a text field for 'Title' (SECURDEN-AWS\administrator).

Verifying Password

You can verify whether the password stored in Securden is in synchronization with the remote asset. To check if the password stored in Securden is the same as the actual password on the remote asset, click the **Verify** icon.

The screenshot shows the 'Accounts' tab in the Privileged Account Manager. The left sidebar lists 'All Accounts' with a search bar and a list of account types: Email login, File, Hitchhiker, Server3, and Test. The main area displays the details for 'Server3'. The details include: Account Name (Primary Server), Password (masked with asterisks), Password Strength (Strong | Score - 100%), FQDN/IP Address (173.134.23.4), Account Used For Remote Operations (Not Configured), and Notes (Not provided). There are icons for 'Edit' and 'Delete' next to the account name.

Troubleshooting Tips

If the verification fails, probable reasons are displayed to help you troubleshoot. Some of the common scenarios include:

- Credential mismatch between Securden and the target machine – One of the reasons of a password mismatch could be the fact that when the machine was imported into Securden, the password of the remote machine could have either been changed by selecting **Use username itself as password** during the account discovery process or the password on the remote device was changed manually by directly accessing it.
- Inadequate remote connection privileges – To verify the password, Securden initiates a remote connection to the target asset. For a user to verify the credentials, they need certain remote connection permissions. You need to provide these privileges to them for the required operating systems before they can verify credentials from PAM.
- The machine does not exist – The remote machine is offline or does not exist.
- The following firewall exceptions have not been made – The following default firewall ports should have been opened in the firewall to establish the respective connection:
 - SSH - 22
 - RDP - 3389
 - SQL - 1433

Password History

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

The screenshot displays the Privileged Account Manager interface. The left sidebar shows a list of accounts, with 'Server3' (IP: 173.134.23.4, Windows Domain) selected. The main panel shows the 'History' tab for this account, displaying a table of password changes.

Historical data related to password changes of this account are listed here. Information on 'who' changed the password and from 'where' are depicted along with the reason recorded for changing.

Password	Modified On	Modified By	Reason	Status
*****	24 Jul 2023 23:32	Securden Administrator		Success - Password Modified Loc...
*****	24 Jul 2023 23:32	Securden Administrator		Success - Password Modified Loc...

Showing 1 to 2 of 2

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

Manage Windows Dependencies and Service Accounts

During the Windows discovery process, Securden fetches and displays the services, scheduled tasks and IIS App pools that are making use of domain accounts. The dependencies of domain accounts are organized by the device on which they are running.

You can manage service accounts in two ways:

1. Navigate to **Accounts** and click **All Accounts**. Select **Service Accounts** from the drop-down. It will list down all the domain accounts with dependencies. When you click a particular account, and then click the **Dependencies** tab in the right pane, you will see the list of all dependencies.

The screenshot shows the Securden Privileged Account Manager interface. The left sidebar contains a 'Folders' section with a search bar and a list of folders. The 'Service Accounts' folder is selected and highlighted with a red box. The main pane displays a list of service accounts. The 'SECURDEN-AWS\administr...' account is selected. The right pane shows the 'Dependencies' tab, which is also highlighted with a red box. It displays a list of dependencies for the selected account, including services and scheduled tasks.

Service Accounts List:

Account Name	IP Address	Domain
Administrator	172.31.1.11	Windows Domain
SECURDEN-AWS\administr...		
SECURDEN-AWS\anish	172.31.1.11	Windows Domain
SECURDEN-AWS\bala	172.31.1.11	Windows Domain

Dependencies for SEC-2K12-1:

Type	Display Name	Name	Computer Name
Service	Active Directory Federation Servi...	adfsrv	SEC-2K12-1
Service	Device Registration Service	drs	SEC-2K12-1
Scheduled Task	Optimize Start Menu Cache Files...	Optimize Start Menu Cache Files...	SEC-2K12-1

Dependencies for SEC-2K16-1:

Type	Display Name	Name	Computer Name
Service	Active Directory Federation Servi...	adfsrv	SEC-2K16-1
Scheduled Task	CreateExplorerShellUnelevatedT...	CreateExplorerShellUnelevatedT...	SEC-2K16-1

Alternatively, you can click any domain account on the **Accounts** tab and then click the **Dependencies** tab in the right pane, you will see the list of all dependencies.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (selected), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar 'Search Accounts' is on the right. The left sidebar shows a tree view of accounts, with 'Administrator' selected. The main pane has tabs: 'Details', 'Share', 'Approval Workflow', 'Dependencies' (highlighted with a red box), 'History', 'Report', and 'Settings'. Below the 'Dependencies' tab, a message states: '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.' A table shows dependencies for 'US-2K19-1' (1 Dependencies):

Type	Display Name	Name	Computer Name
Scheduled Task	CreateExplorerShellUnelevatedTask	CreateExplorerShellUnelevatedTask	US-2K19-1

Below the table, a 'Help' section explains that Securden fetches dependencies from discovered computers and already discovered ones. The interface also shows pagination: 'Showing 1 to 1 of 1' and '100' items per page.

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.

Note: When a password on a domain account is changed and you want the related dependencies to be restarted immediately, navigate to **Admin >> Account Dependent Services** and select **Yes** for the question - *Do you want to restart the dependent services once password change gets propagated?*

Launching Remote Connections

Most organizations give staff, independent contractors, and third-party vendors remote administrative access to IT assets. If this access is not monitored, it opens the door for malicious insiders and outside attackers to exploit it. Furthermore, enabling direct remote access between end-user computers and the targeted IT assets might propagate security vulnerabilities.

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

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

Web-based and native connections:

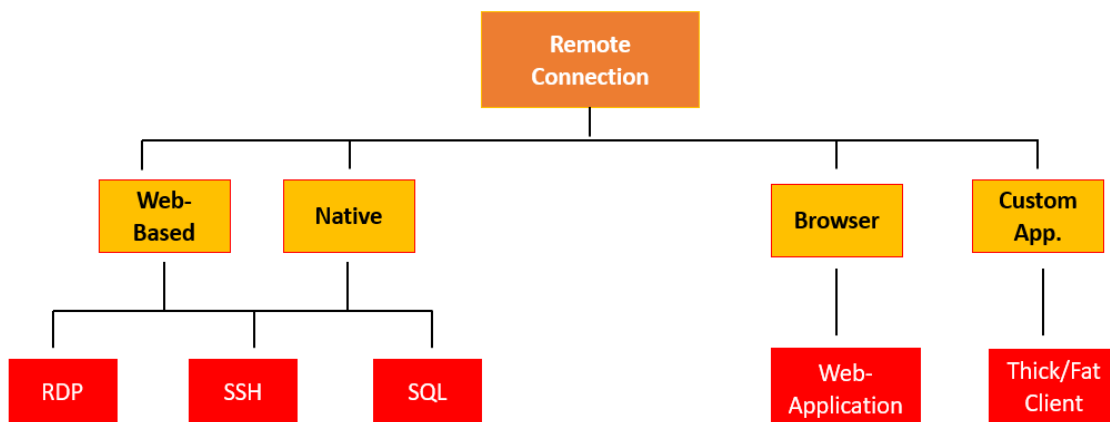
- RDP for establishing connection with Windows devices.
- SSH for establishing connection with Linux devices.
- SQL for establishing connection with Oracle and SQL database servers.

Brower-based connections

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

Connections to thick clients

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



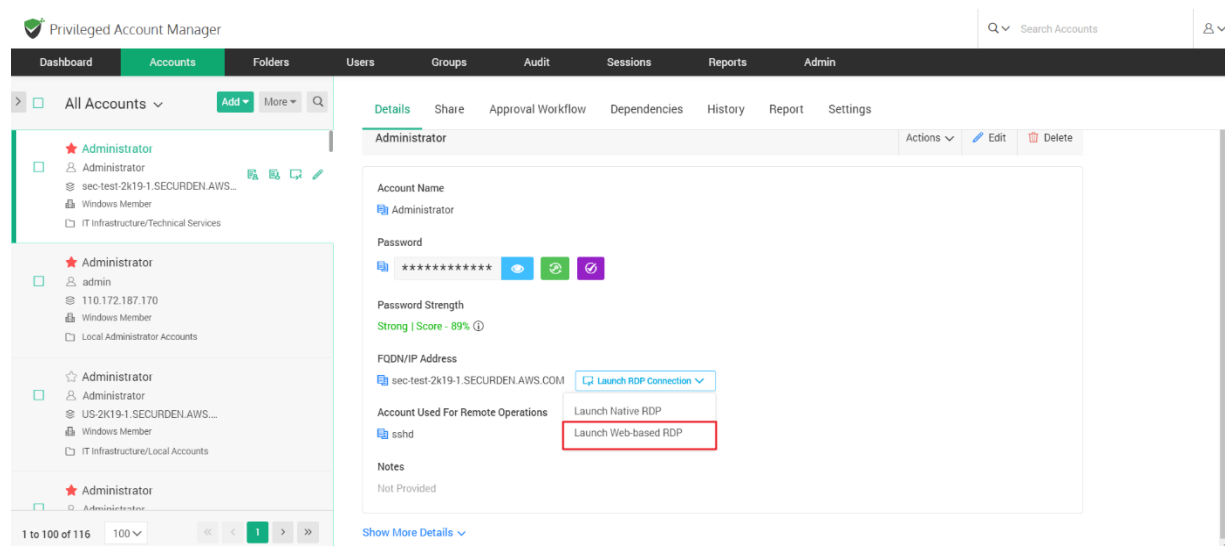
Web-Based Connections

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

The web-based connections use the Securden server as the starting point to launch connections to the target device. The target machine must be in the operability range to successfully launch web connections. In web-based connections, certain operations like file transfer, and audio and video recording are not supported.

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

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



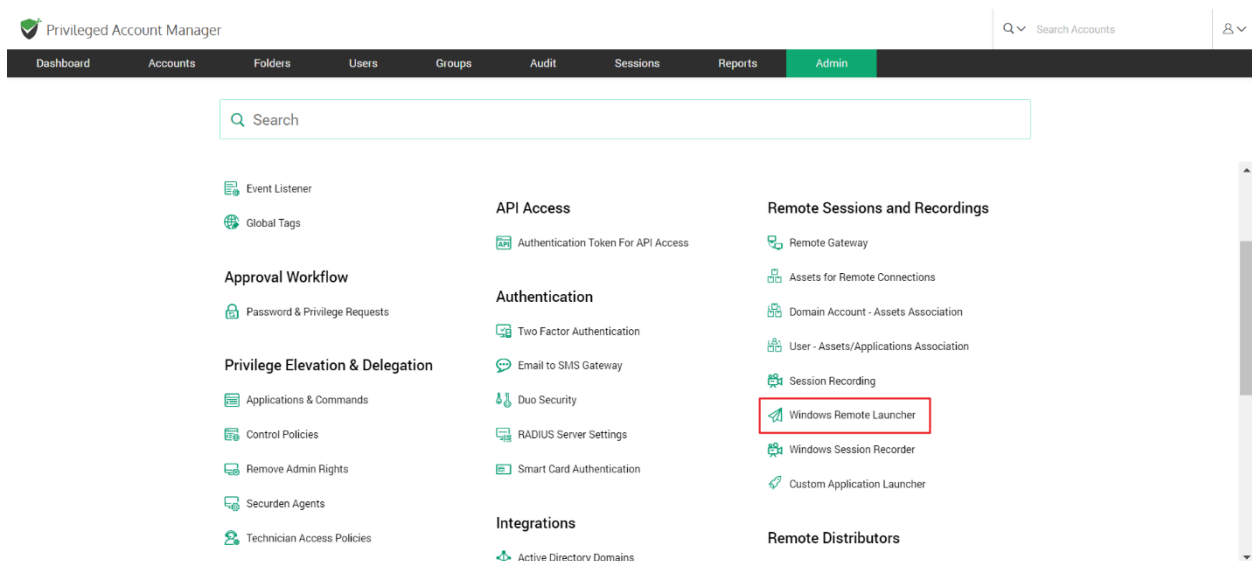
Here you can choose the asset you wish to connect to or specify the name. After you select the required asset, click **Connect** to launch the connection.

Using Native Client Applications

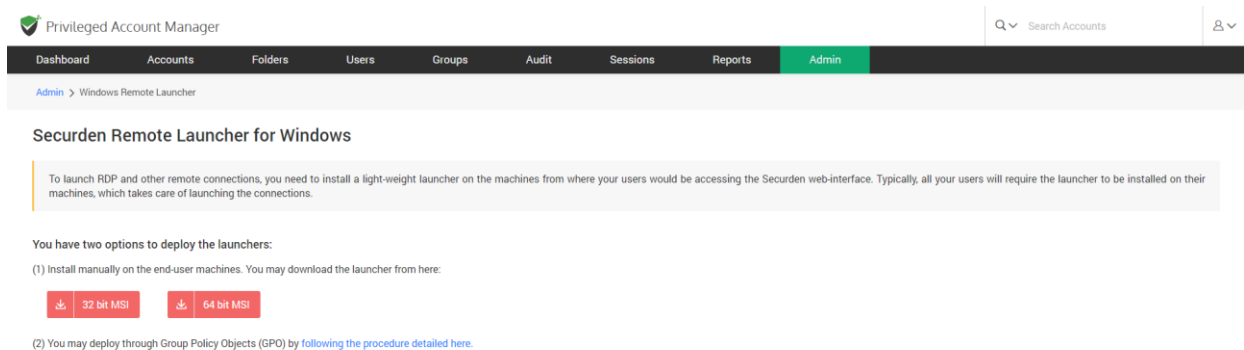
To use native client applications for RDP, SSH (PuTTY, SecureCRT etc.); SQL, a lightweight launcher application must be installed in all the end-user machines.

Installing Windows Remote Launcher for launching Native RDP connections

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

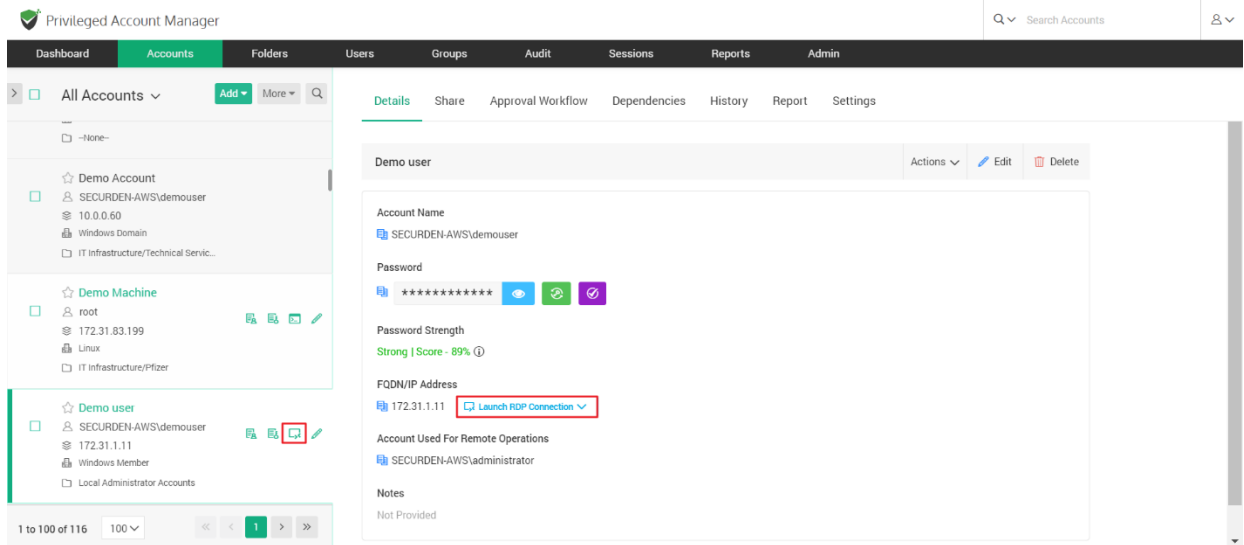


In the GUI that opens, you can follow the instructions provided to install the **Windows Remote Launcher**.



Launching Native RDP connections

RDP connections are mainly used to access Windows-based machines and network devices. Navigate to the Accounts section in the GUI, click the required account, click the **Launch RDP Connection** connection button appearing alongside the account information on the left-hand side. Alternatively, you can click the drop-down menu named **Launch RDP Connection** from within the Account to launch a connection.

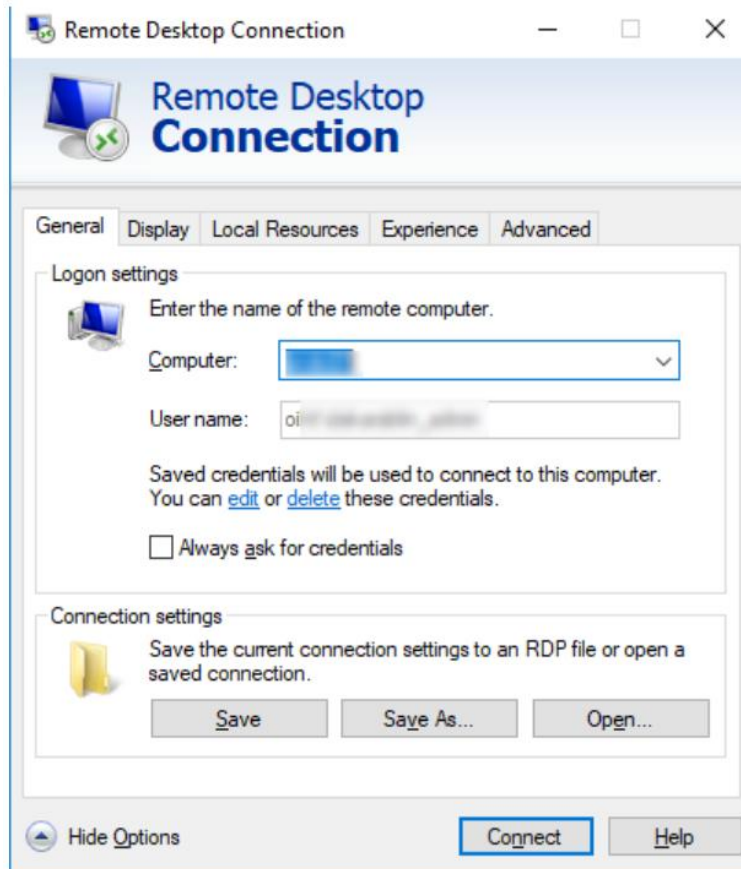


Native RDP Connections: Troubleshooting Checklist

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

Settings to be checked in mstsc app:

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



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

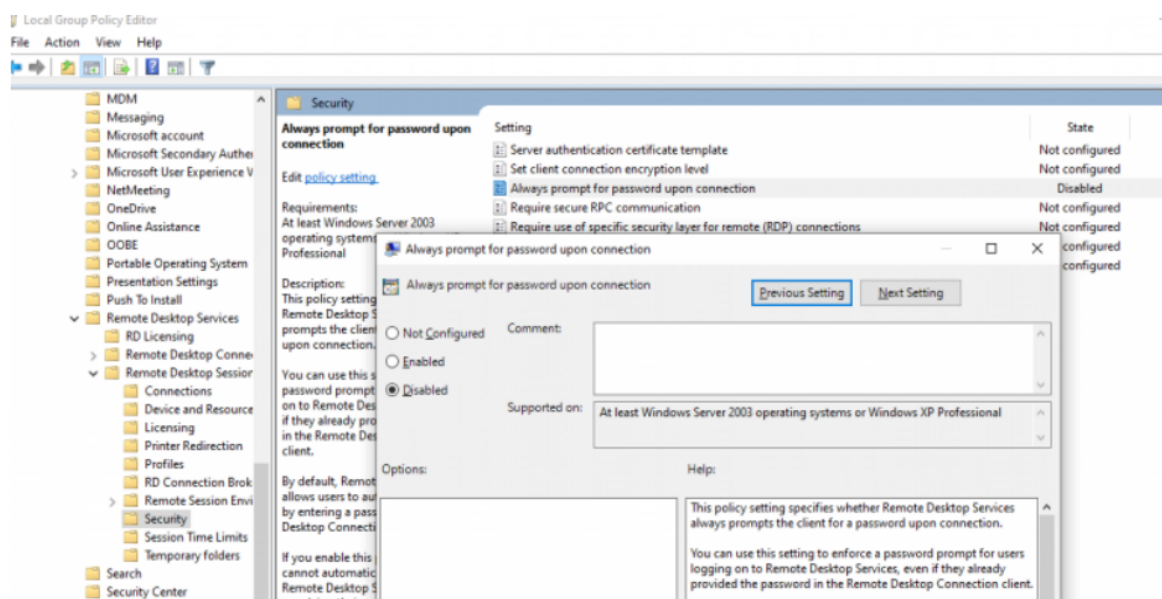
```

Default.rdp - Notepad
File Edit Format View Help
redirectsmartcards:i:1
redirectclipboard:i:1
redirectposdevices:i:0
autoreconnection enabled:i:1
authentication level:i:2
prompt for credentials:i:0
negotiate security layer:i:1

```

Group Policy: Always prompt for password upon connection.

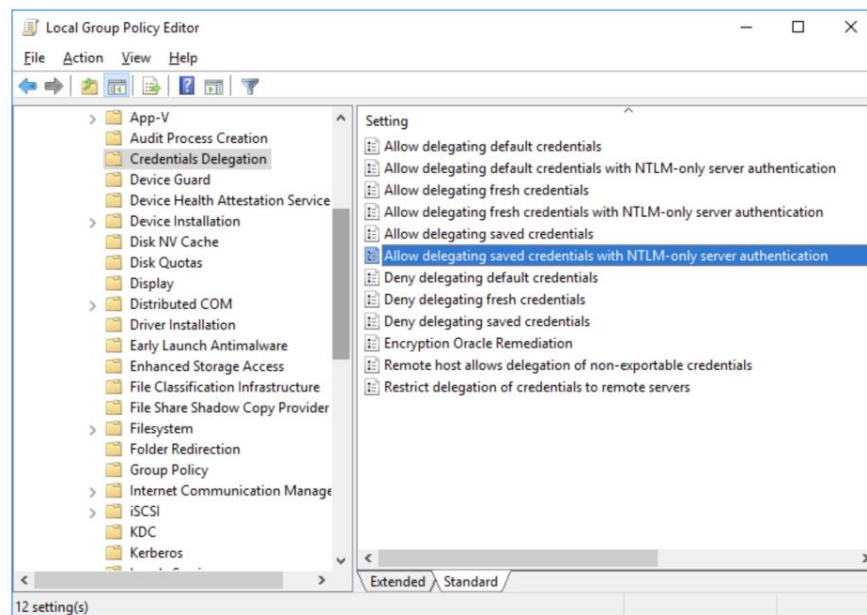
1. Open **Run** command and open gpedit.msc or gpmc.msc depending on your need.
2. Navigate to **Computer Configuration >> Administrative Templates >> Windows Components >> Remote Desktop Services >> Remote Desktop Session Host >> Security**. Look for the policy named **Always prompt for password upon connection**.



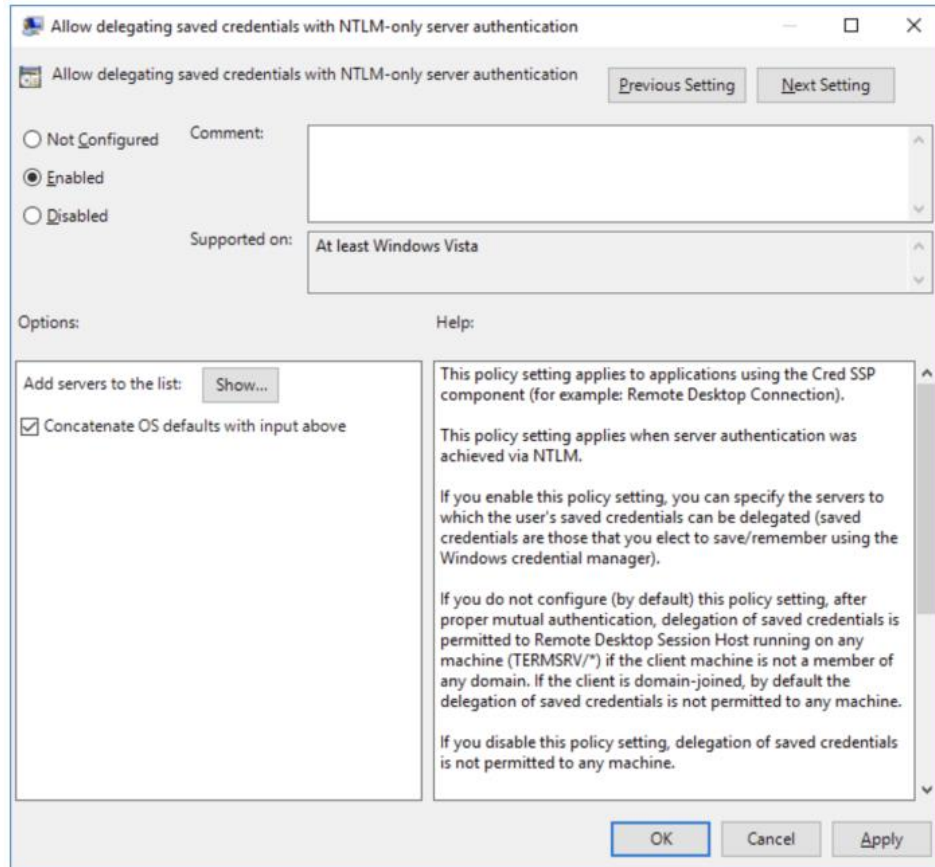
3. Double-click the policy and **disable** it.
4. Save the changes.
5. If a domain level policy is to be updated, you need to additionally run the command gpupdate/force in the command prompt as an administrator.

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

1. Open **Run** command and open gpedit.msc or gpmmc.msc depending on your need.
2. Go to **Computer Configuration >> Administrative Templates >> System >> Credentials Delegation**. Look for the policy named **Allow delegating saved credentials with NTLM-only server authentication**.



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



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

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

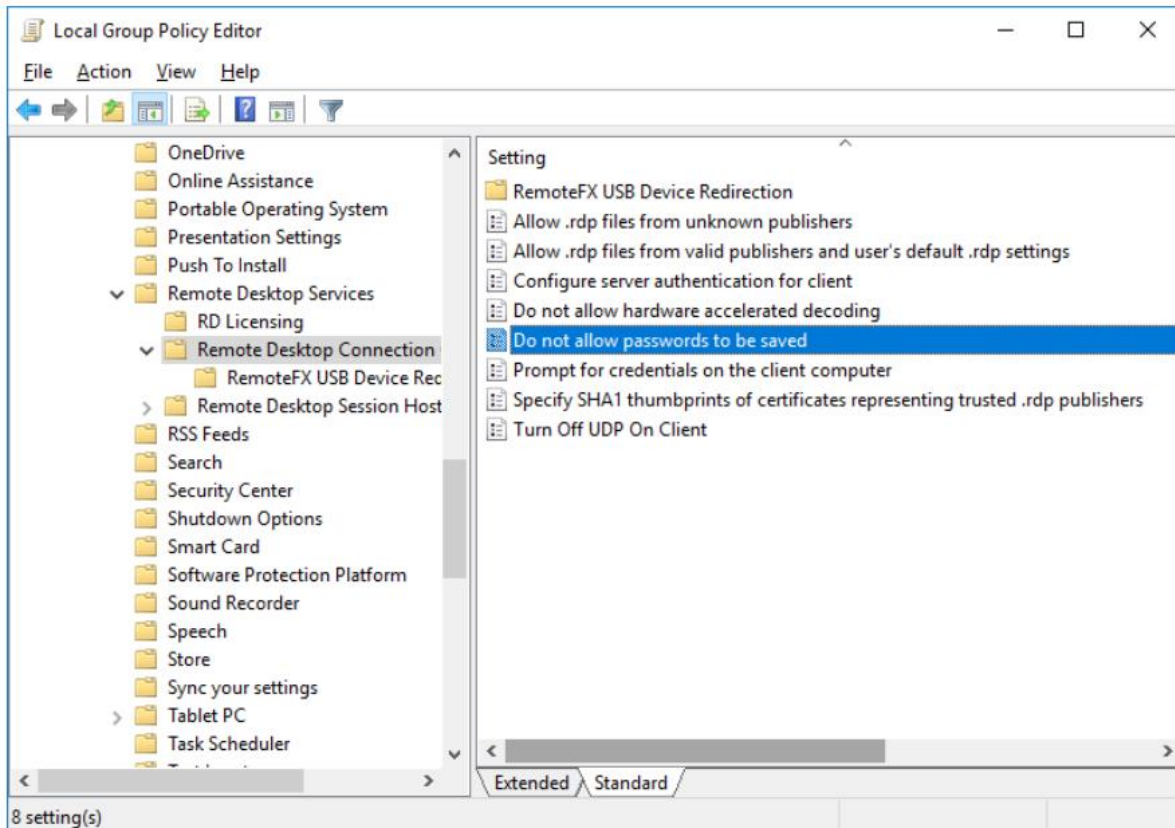
5. Save the changes.
6. If domain level policy is to be updated, you need to additionally run the command `gpupdate /force` in the administrator command prompt.

Group Policy: Deny delegation saved credentials

1. Open **Run** command and type `gpedit.msc` or `gpmc.msc` depending on your need.
2. Go to **Computer Configuration >> Administrative Templates >> System >> Credential Delegation**. Look for the policy named **Deny delegation saved credentials**.
3. Double-click the policy and **disable** it.
4. Save the changes.
5. If domain level policy is to be updated, you need to additionally run the command `gpupdate /force` in the administrator command prompt.

Group Policy: Do not allow passwords to be saved

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



3. Double-click the policy. **Disable** it.
4. Save the changes.
5. If domain level policy is updated, you need to additionally run the command `gpupdate /force` in the administrator command prompt.

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

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

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

3. Double-click the policy and **disable** it.
4. Save the changes.
5. If domain level policy is to be updated, you need to additionally run the command `gpupdate /force` in the administrator command prompt.

Launching Native SSH connection

The Native SSH connection can be launched via:

- PuTTY
- SecureCRT etc.

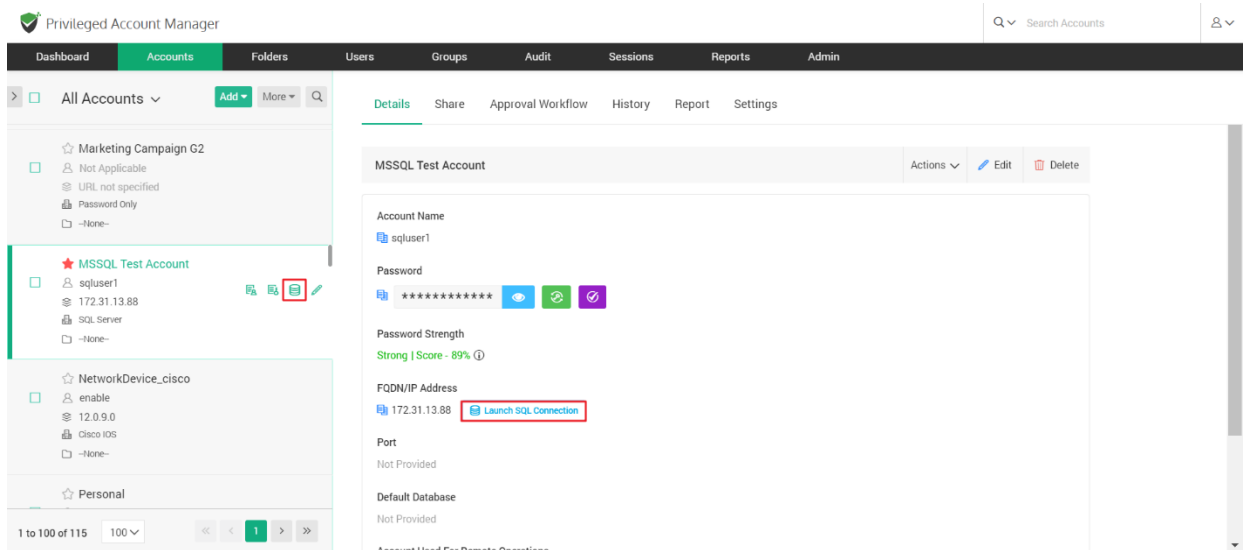
To launch PuTTY and SecureCRT connections you need the Securden Remote Launcher to be installed in the user's machine. The SSH connections are mainly used to connect to machines running Linux, Mac along with routers and other network devices.

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

Launching Native SQL connections

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

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



Launching connections to thick application clients

In addition to the default modes of launching web-based connections and through native clients, you can define custom application launchers to supply credentials and automatically launch any application, including thick application clients. Basically, you will be creating a profile for each such application capturing the input fields as found in the target application. You can configure the profile with placeholders to replace the required values from Securden repository at the time of launching the connections. You need to navigate to **Admin >> Remote Sessions and Recordings >> Custom Application Launcher** and configure the profiles.

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

Configure URLs for Autofill

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

The screenshot shows the Privileged Account Manager (PAM) interface. The top navigation bar includes Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin. The left sidebar shows a list of accounts under 'All Accounts'. The main panel displays the details for the 'Administrator' account. The 'Actions' menu is open, showing options like 'Credentials for Remote Operations', 'Configure Session Recording', 'Transfer Ownership', 'Clone Account', 'Color Coding', 'Copy Account Direct Access URL', 'Configure URLs for Autofill' (highlighted with a red box), 'Configure TOTP', and 'Share with Third Parties'.

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

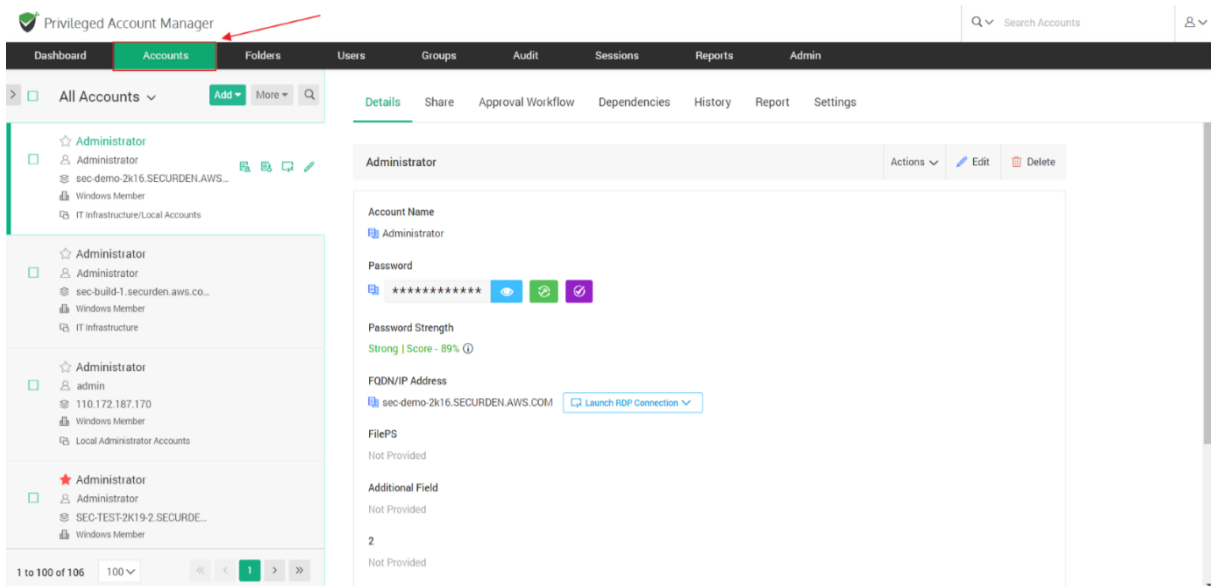
The screenshot shows the Privileged Account Manager (PAM) interface. The top navigation bar includes Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin. The left sidebar shows a list of accounts under 'All Accounts'. The 'More' menu is open, showing options like 'Change Folder', 'Transfer Ownership', 'Clone Accounts', 'Add Tags', 'Color Coding for Accounts', 'Change Password Policy', 'Associate Assets', 'Associate Private Key', and 'Configure URLs for Autofill' (highlighted with a red box). The main panel displays the details for the 'Administrator' account.

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

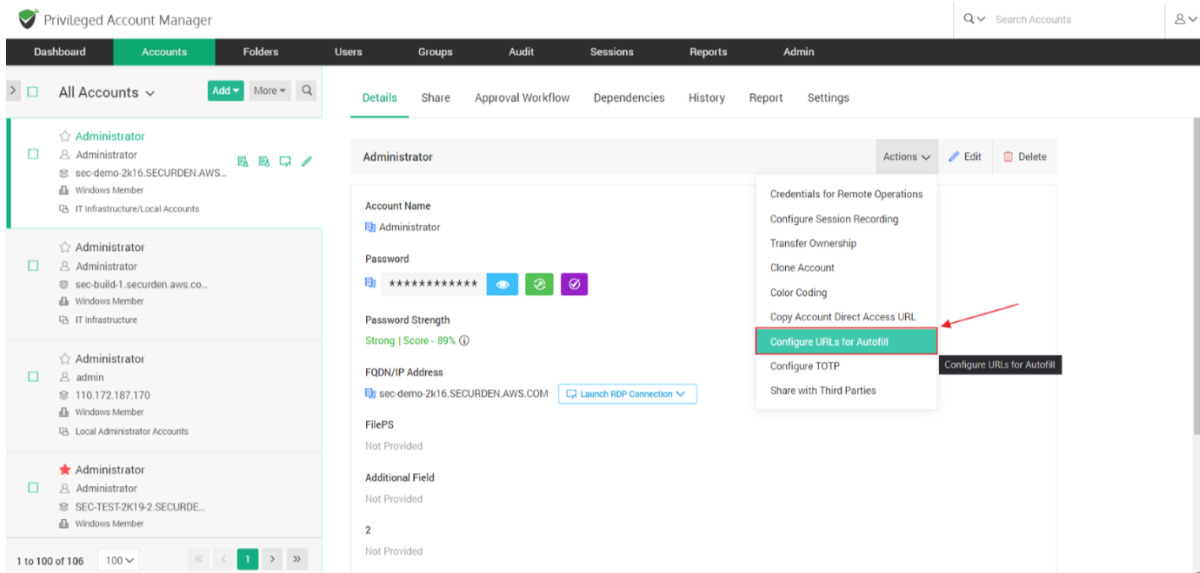
How to Add URLs to Accounts?

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

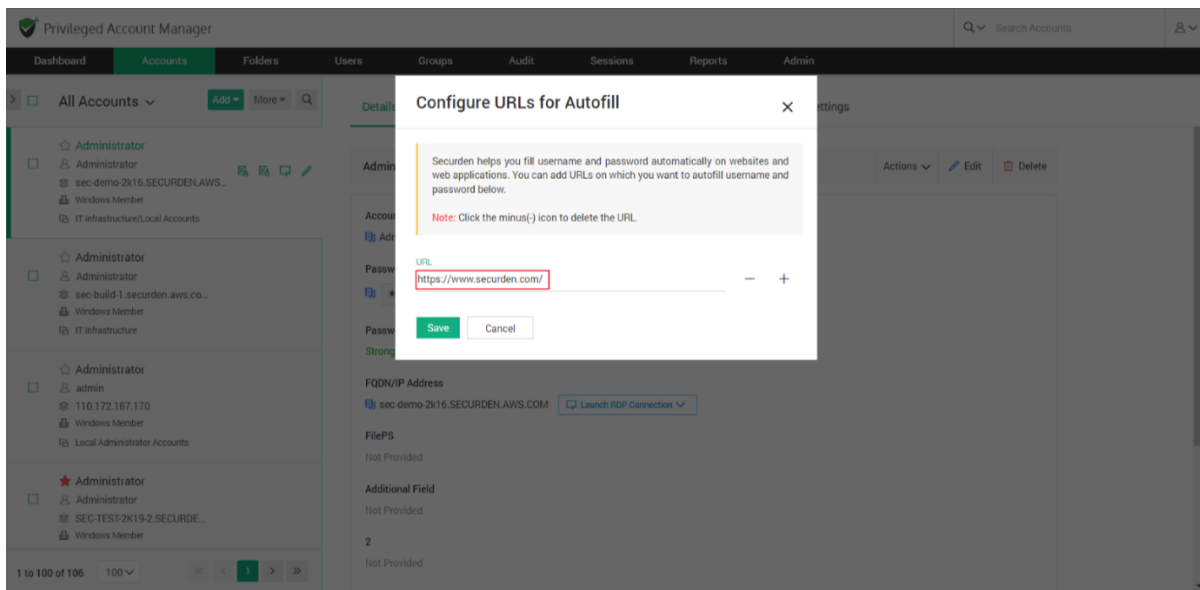
1. Navigate to Accounts tab and select the required account.



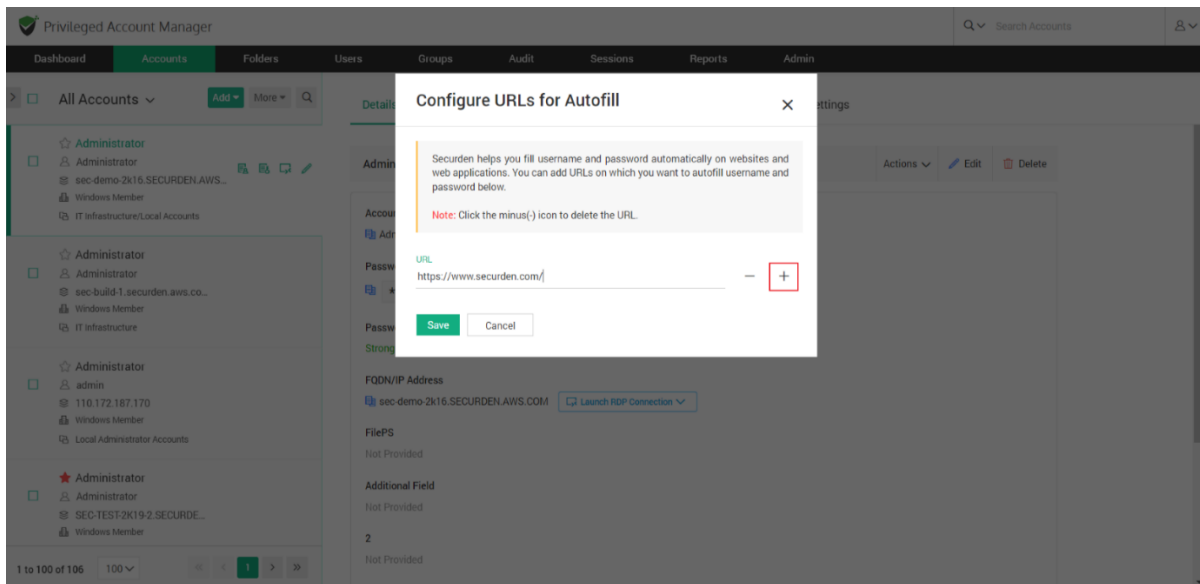
2. In the **Accounts** tab, navigate to **Actions >> Configure URLs for Autofill**.



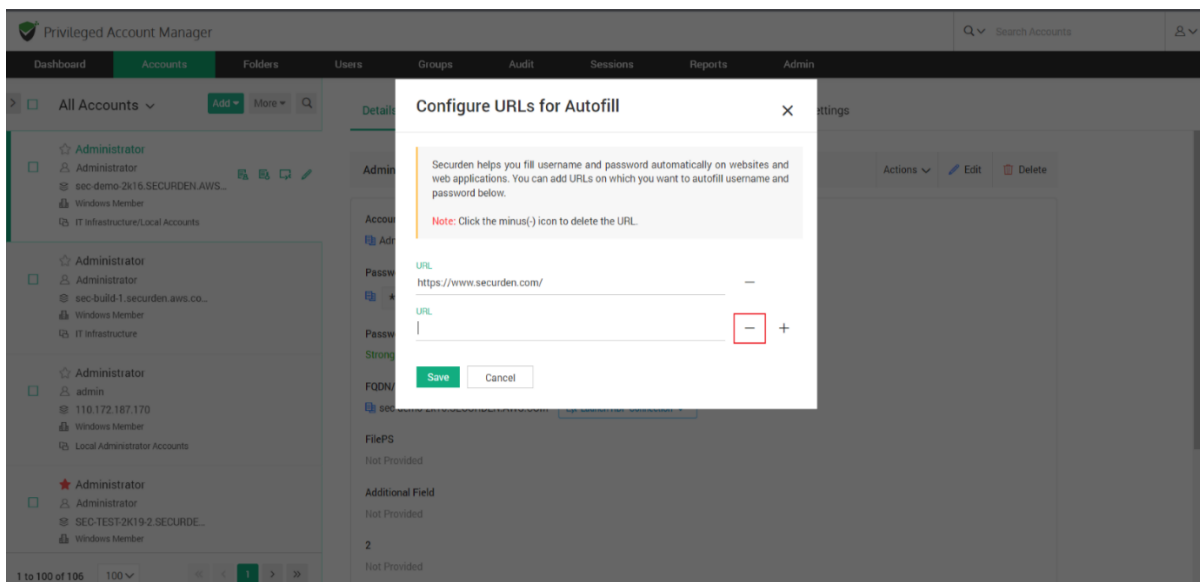
3. In the popup, you need to specify the URL on which username and password should be auto filled.



4. You can add multiple URLs on which the account credentials can be auto filled. Click on the + sign to add a second URL.



5. To remove a URL, click on the - symbol.



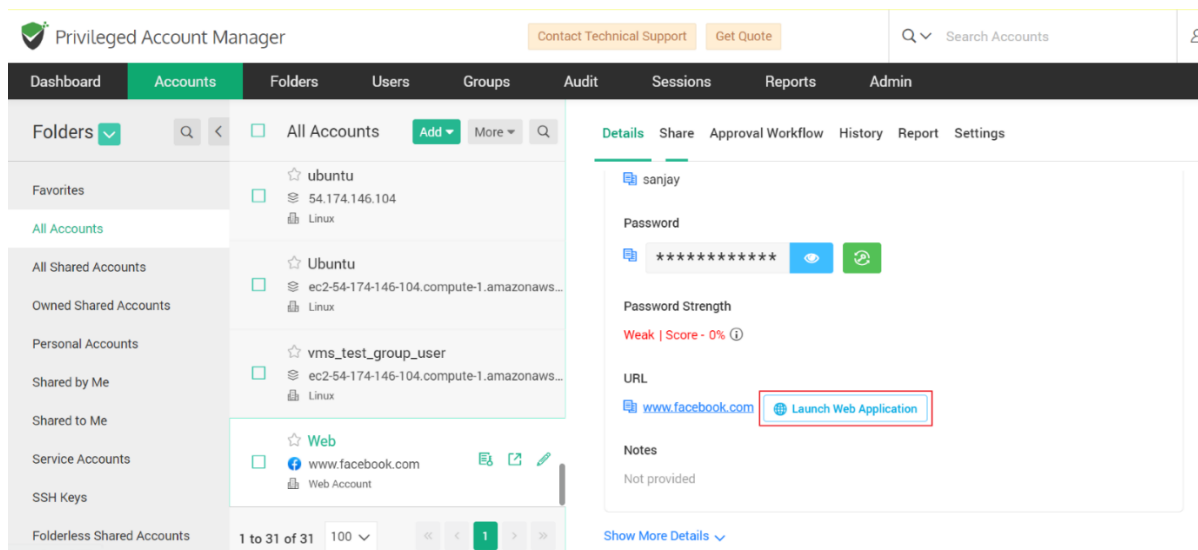
6. Once you have configured all the URLs you want, click **Save**.

How to auto fill credentials on the website?

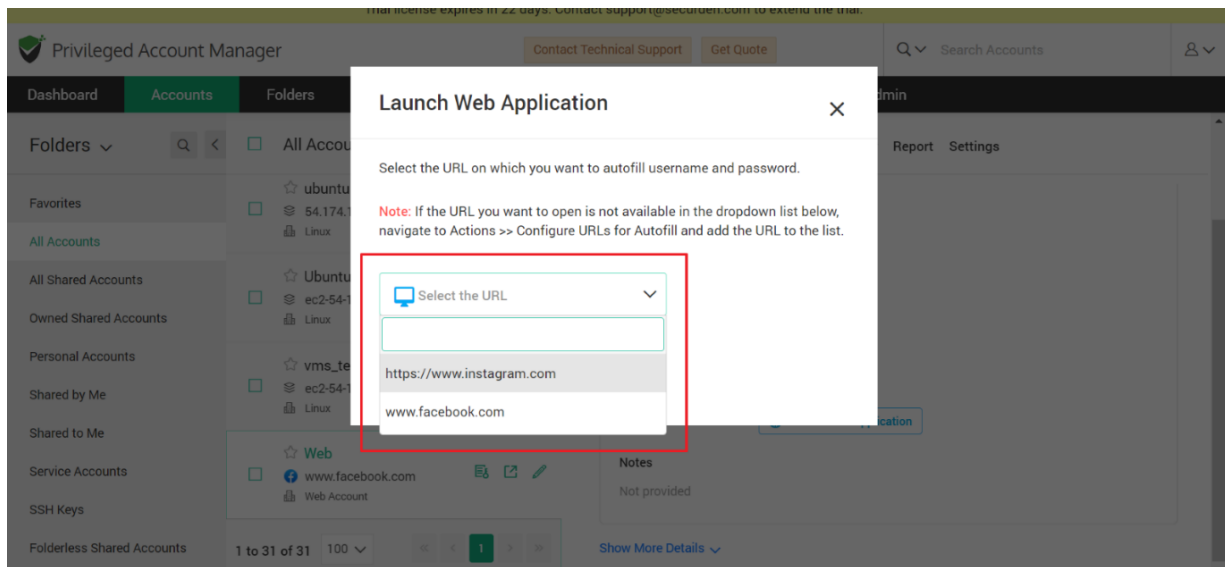
Note: You need to install the Securden Browser Extension on the required browser to be able to utilize the auto fill feature. To install the browser extension, navigate to **Admin >> General >> Browser Extension**.

Once the URLs are configured, you can connect to the webpage or web application by navigating to **Accounts** tab.

In the accounts tab, select the required account and click on **Launch Web Application**.



In the window that opens, all the added URLs to the selected account will be available in the drop down.



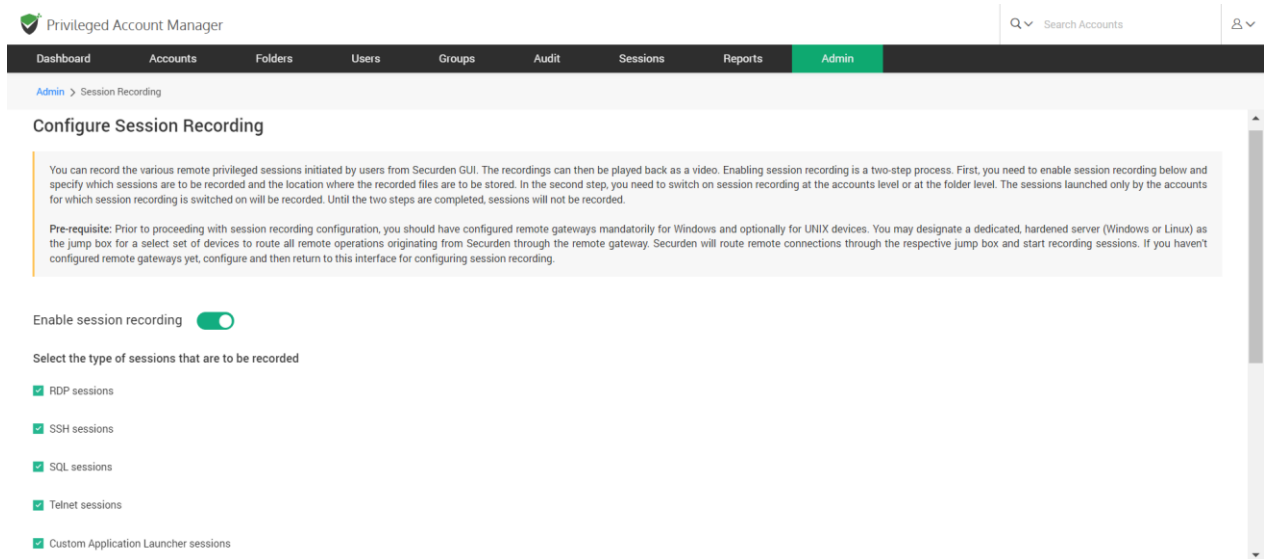
You can select the required URL and the web application/webpage will be opened and the credentials will be auto filled.

Enable Session Recording for Accounts

You can record the various remote privileged sessions initiated by users from Securden's GUI. The recordings can then be played back as a video.

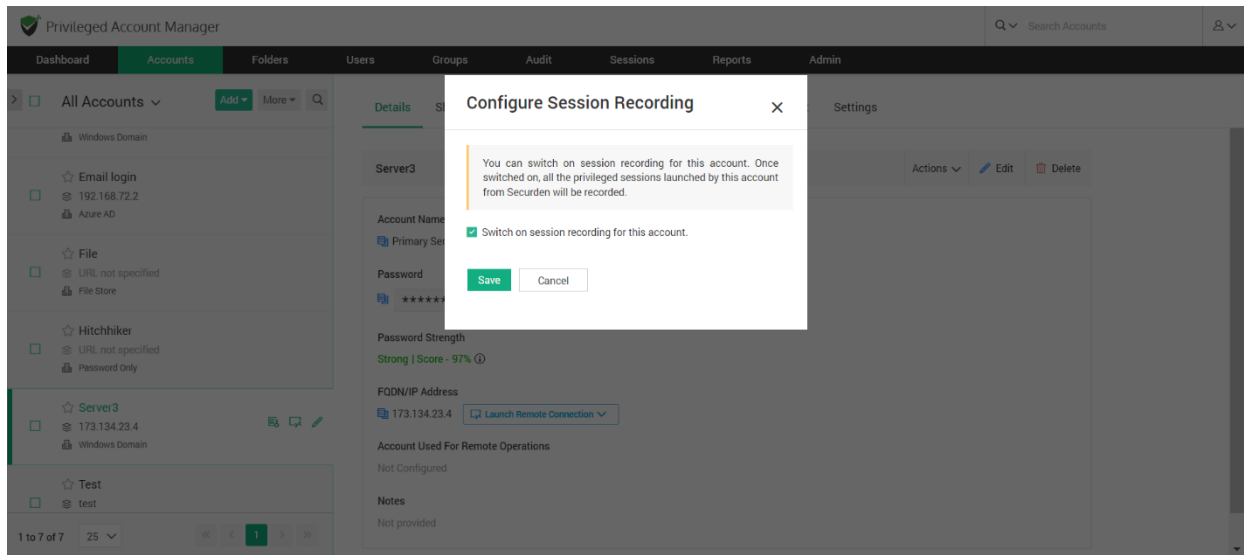
Configuring session recording is a two-step process.

Step 1: Configure session recording globally by navigating to **Admin >> Remote Sessions and Recordings >> Session Recording**. Specify which type of sessions are to be recorded and the location where the recorded files are to be stored.



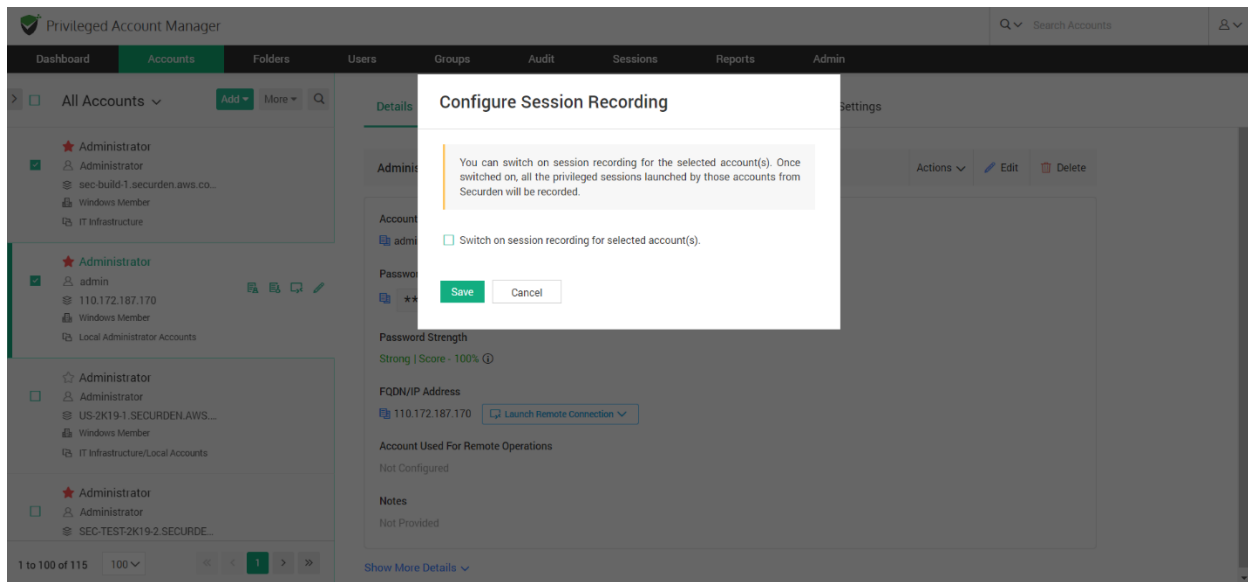
Step 2: Switch on session recording at the accounts level or at the folder level. The sessions launched using the accounts for which session recording is switched on will be recorded.

Navigate to the account for which you want to enable session recording. Under **Actions**, select **Configure Session Recording**. Once switched on, all the privileged sessions launched by this account from Securden will be recorded and stored in the specified location.



Pre-requisite: Prior to proceeding with the 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. Securden will route remote connections through the respective jump box and start recording sessions.

To enable session recording for multiple accounts at the same time, navigate to **Accounts** tab and select the required accounts.



Go to **More >> Configure Session Recording**, select the checkbox, and click **Save**.

Managing Access Permissions

Share Accounts with Users/Groups

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

1. You can search and add the users and groups with whom the account must be shared.

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

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

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

Launching Connections without revealing the Credentials

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

All Accounts Add More

Email login
192.168.72.2
Azure AD

File
URL not specified
File Store

Hitchhiker
URL not specified
Password Only

Server3
173.134.23.4
Windows Domain

Test
test
Windows Member

1 to 7 of 7 25 << < 1 > >>

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

Help ?

- '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.

How to modify share permissions?

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

All Accounts Add More

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

Administrator
sec-demo-2k16.SECURDEN.AWS.COM
Windows Member

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

Administrator
SEC-TEST-2K19-2.SECURDEN.AWS.COM
Windows Member

1 to 25 of 37 25 << < 1 > >>

Details Share Approval Workflow Dependencies History Report Settings

Share Account Remove Share

Showing 1 to 1 of 1 25

Username	Manage	Modify	View	Open Contr
Chris R				✓

Chris R

Showing 1 to 1 of 1 25 << < 1 > >>

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

How does Securden trace accounts shared at multiple levels?

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

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

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

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

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions **Reports** Admin

User Access Report < Back

Report Export: [Export](#) | [Schedule Export](#)

Access Snapshot

Showing 1 to 5 of 5

Username	Login Name	Role	Email	Domain
Destro Shax	destro	Super Administrator	destro@gmail.com	Local
Frankel Lampard	Frank	Account Manager	frenkid@gmail.com	Local
Jonathan Ridge	John R	Administrator	john@gmail.com	Local
Perry Theplat	Perry	Account Manager	perry@prey.com	Local
Securden Administrator	admin	Administrator	localadmin@securden.com	Local

Showing 1 to 5 of 5

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

Privileged Account Manager

Dashboard Accounts Folders

Securden Administrator

Report > User Access Report > Securden Administrator

Access Details

Account Title Account Address

Domain Admin 192.164.23.1

Email login 192.168.72.2

File

Hitchhiker

Server3 173.134.23.4

Test test

Showing 1 to 6 of 6

Trace the sharing mechanism

check how the sharing has actually taken effect. This report helps you trace all the levels in which the account has been shared. It tells you the share permission that is effective at present and shows all the other share permissions disregarded as per the least privilege principle.

The specific sharing level that has taken effect:

Account owner	Username	Share Type
Account Title Server3	Securden Administrator	Manage

This account has been shared at the following levels too. These levels have been disregarded:

Folder owner	Folder Name	Username	Share Type
Folder Name Fruit	Securden Administrator	Manage	

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

Synchronization of Groups in AD with Securden

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

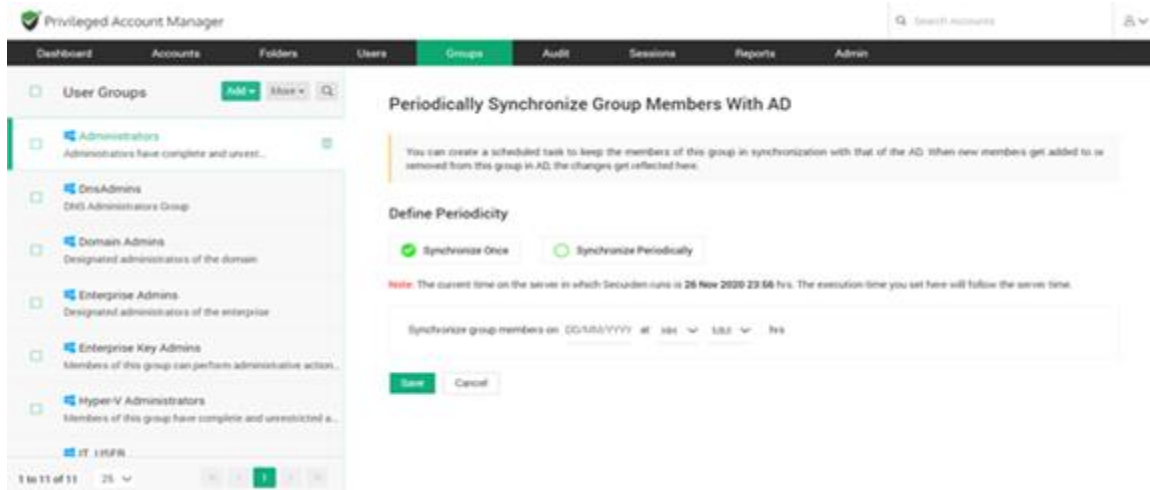
You have shared an account with a group imported from AD. The group originally has only 10 members. A new user is added to the group in AD and now the members total up to 11. Will the 11th member automatically get the access permissions associated with the group?

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

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

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

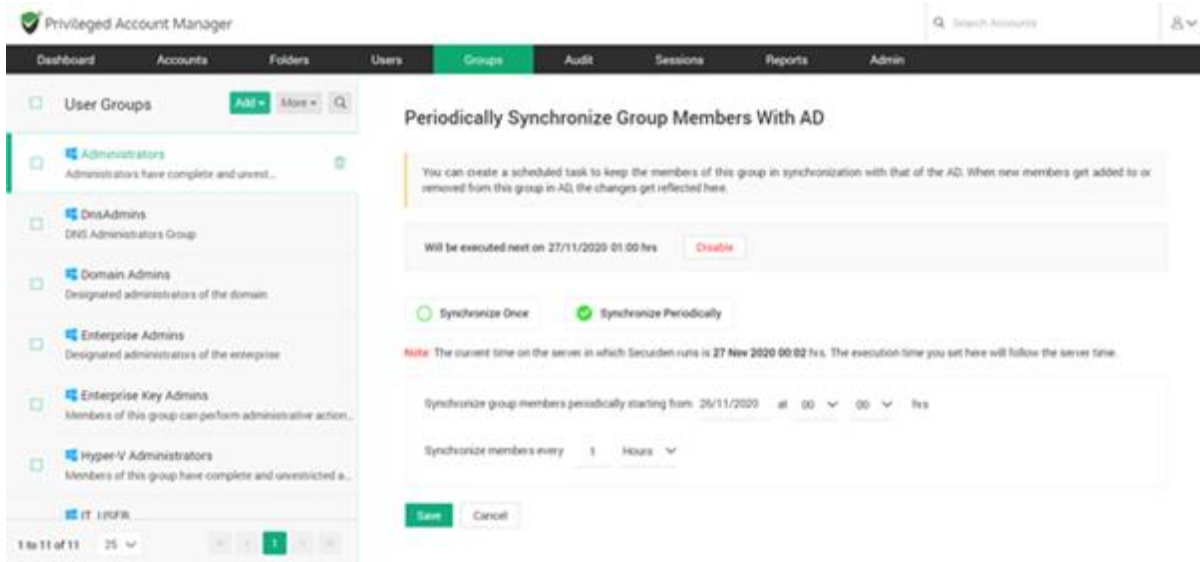
You can either schedule the synchronization activity for a one-time run or create scheduled tasks to run periodically and ensure regular synchronization.



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

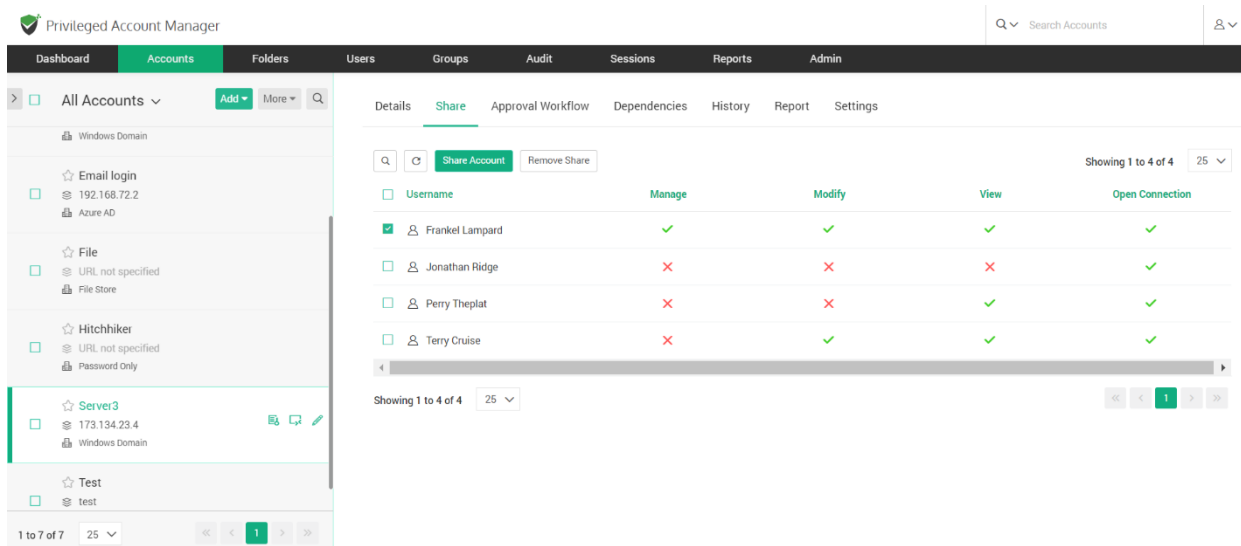
Once enabled, you can navigate to the **Schedule Sync** section to view the next planned schedule.

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



Remove Share Permission

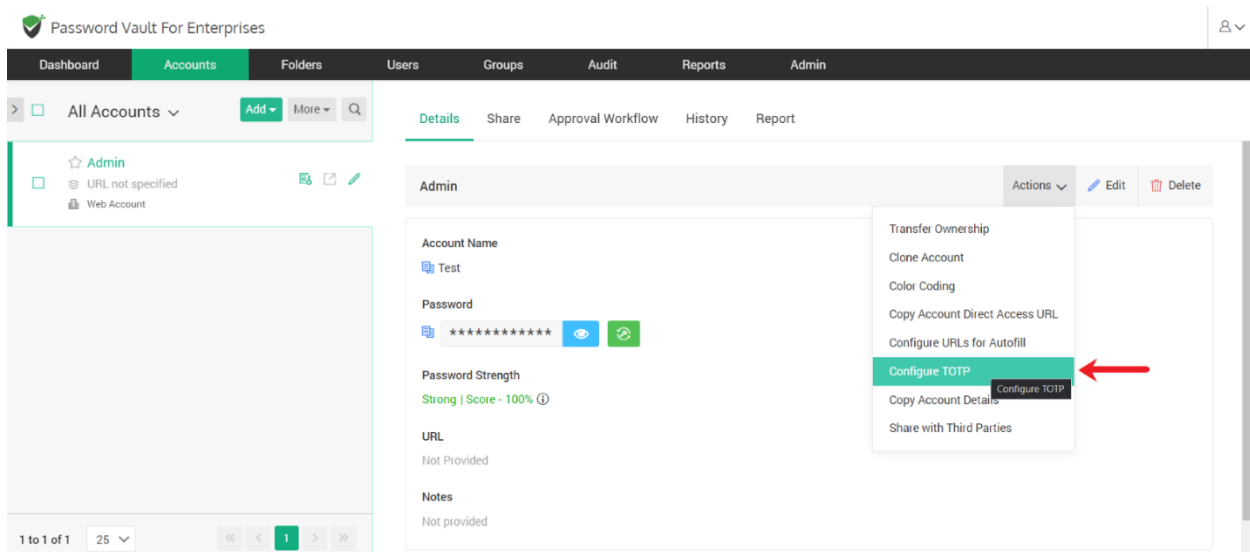
If you want to revoke the share permission from a user or group of users, navigate to the **Share** panel, select the users or groups for whom you want to terminate the account access, and then, click the **Remove Share** button.



Configuring Shared MFA Tokens

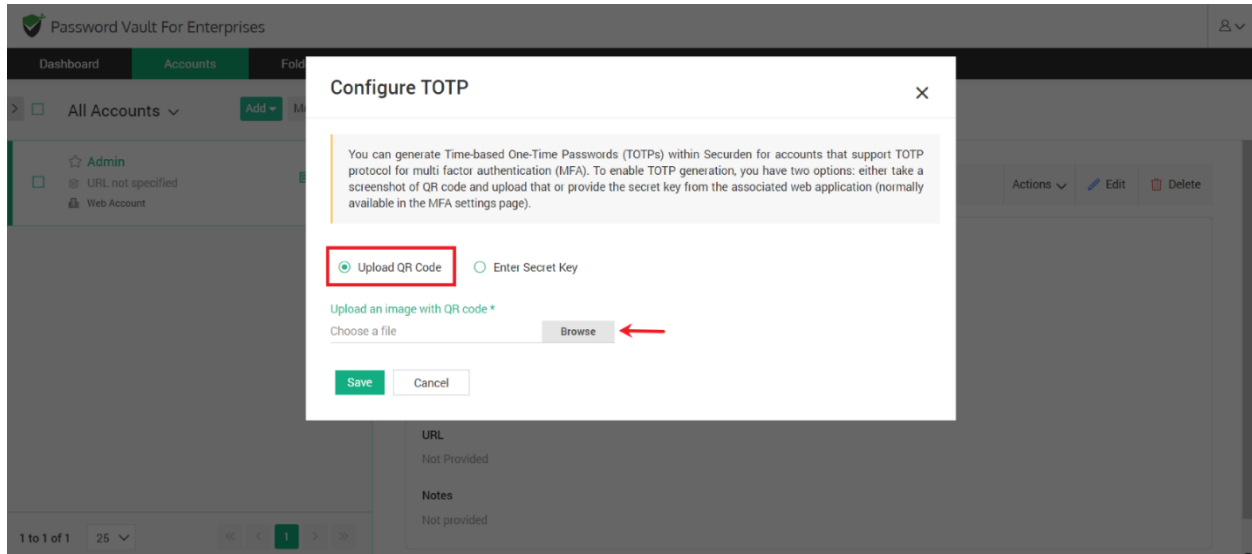
Securden readily integrates with TOTP-generating applications like Google Authenticator, Microsoft Authenticator, and others using either secret keys or QR codes. After integrating, the TOTP will be generated in the Securden interface.

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

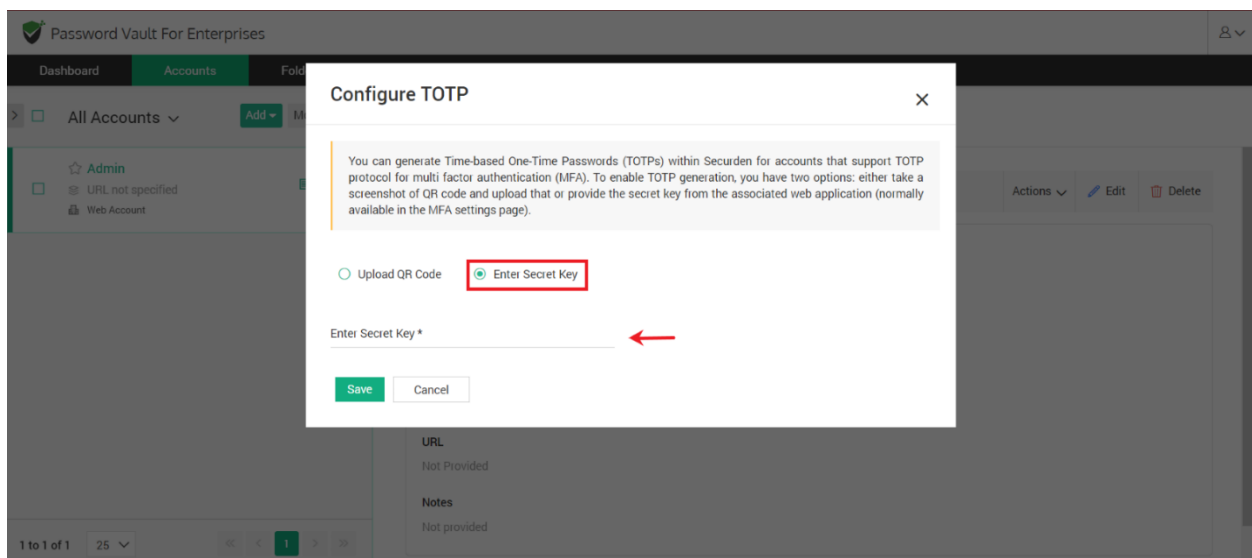


In the window that opens, you need to select between the two options available. You can configure TOTP generation by using either a QR code or the secret key from the MFA application.

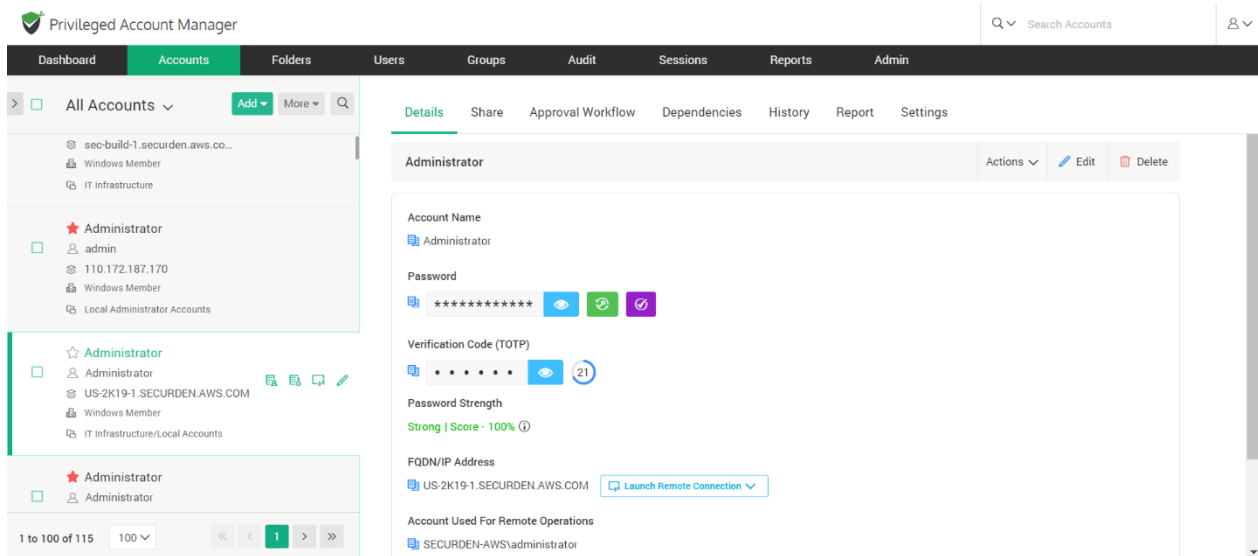
1. If you choose to use a QR code, you need to upload an image containing the QR code. Select **QR code** and click on **Browse**. Select and upload the required image. Click **Save**



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



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



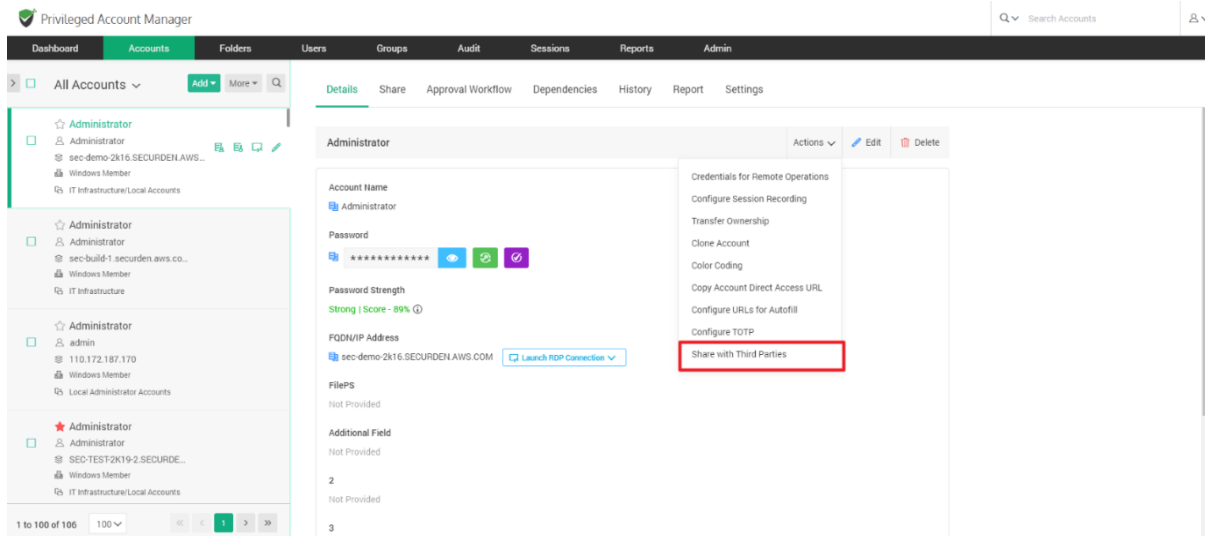
When you share the account with a user or a group, the associated TOTP will be shared alongside the credentials.

Share Accounts/Passwords with Third Parties

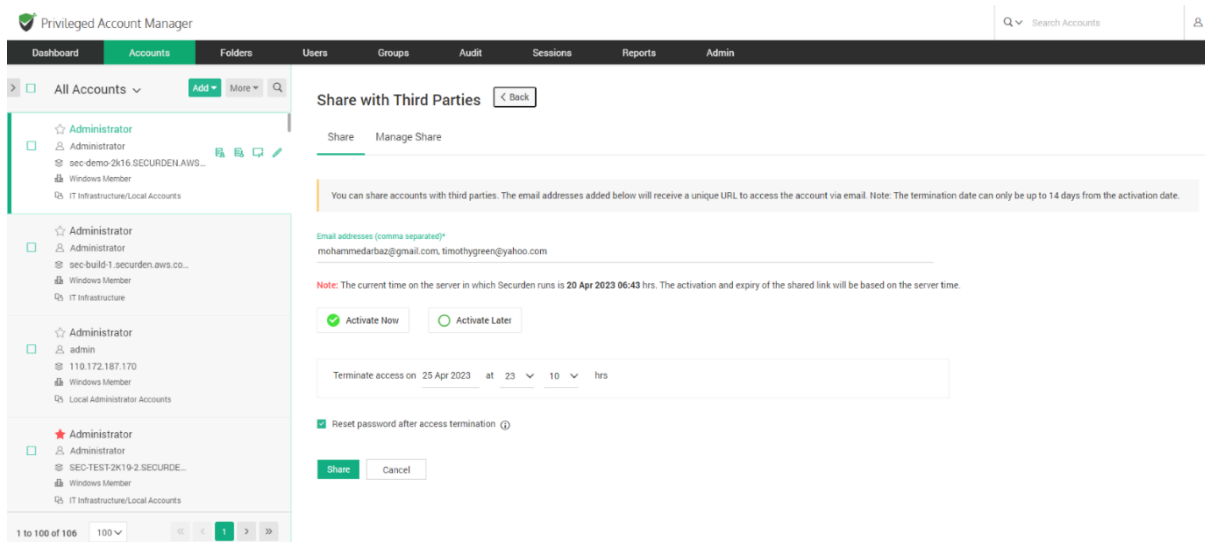
Any user in Securden can share accounts owned by them/shared with them to a third-party user outside the organization. They need the email addresses of the third parties who need access to the account.

Pre-requisite: To send accounts to external user emails, you need to configure the email server settings which are available under **Admin >> General >> Mail Server Settings**.

To share an account, navigate to **Accounts >> Select the account to be shared >> Actions >> Share with Third Parties**

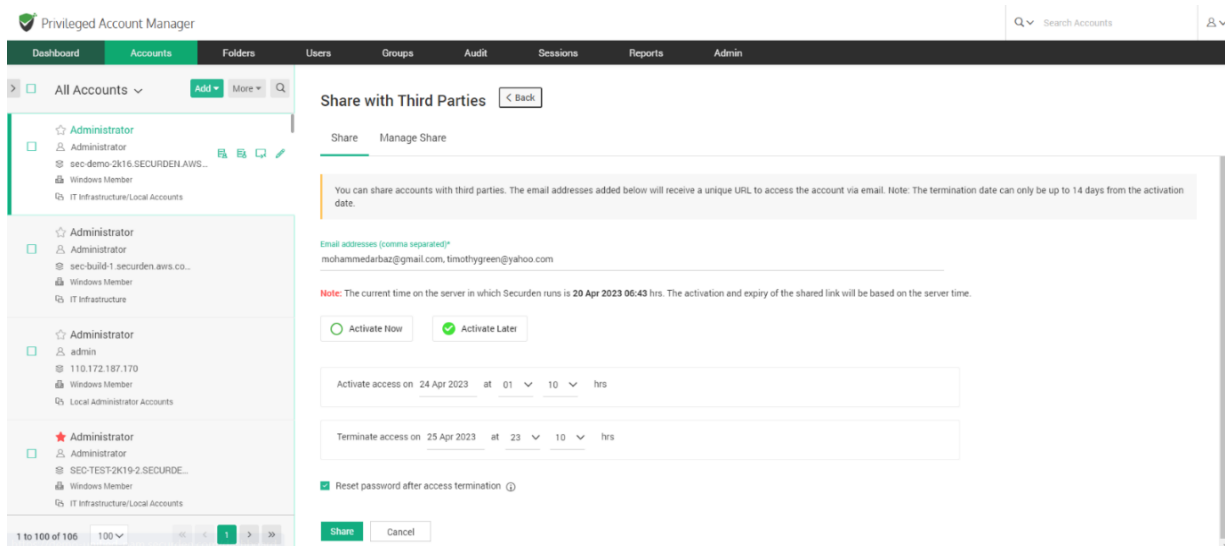


This opens the GUI shown below:



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

- **Email addresses:** You need to specify the email address of the third-party user. If you are sending this account to more than one recipient, you must specify their email addresses in a comma-separated format.
- **Activate Now:** You can select this option to allow the third-party to access the account immediately after sharing it.
- **Activate Later:** You can select this option to allow the third party to access the account at a specified date and time.



- **Terminate access:** You must specify when the account access should be revoked from the third-party. Specify the date and time after which they will be unable to access the shared account.
- **Reset password after access termination:** Enabling this checkbox will ensure that the password of the remote machine is changed after the third-party access is revoked.

Once you have set up the access duration and password reset configurations, click on **Share** to send the account as a HTML link to the third party.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Owned Work Acc... Add More

Share with Third Parties Back

Share Manage Share

You can share accounts with third parties. The email addresses added below will receive a unique URL to access the account via email. Note: The termination date can only be up to 14 days from the activation date.

Email addresses (comma separated)*
timothygreen@yahoo.com

Note: The current time on the server in which Securden runs is 29 Apr 2023 10:11 hrs. The activation and expiry of the shared link will be based on the server time.

Activate Now Activate Later

Terminate access on DD/MM/YYYY at HH MM hrs

Reset password after access termination

Share Cancel

Terminating Third Party Access

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Owned Work Acc... Add More

Share with Third Parties Back

Share Manage Share

Terminate Access

Showing 1 to 1 of 1 25

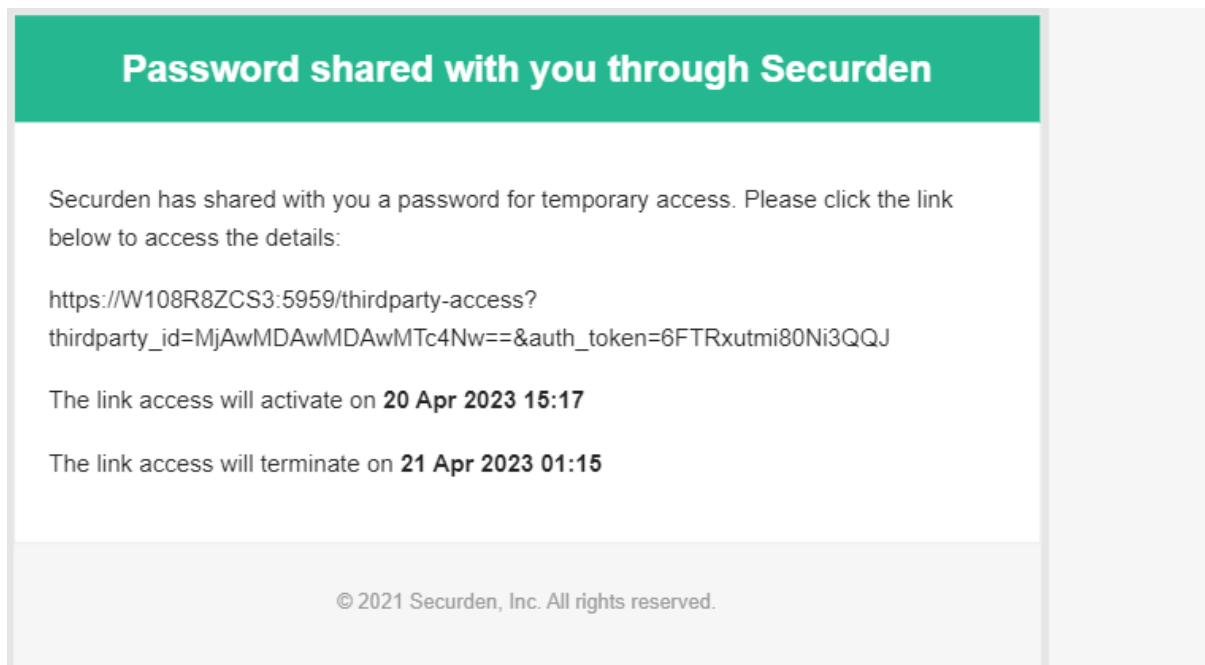
Email	Activate access on	Terminate access on	Status	Shared By
shyam@securden.com	20 Apr 2023 10:08	25 Apr 2023 01:10	Yet to Activate	Securden Administrator

Showing 1 to 1 of 1 25

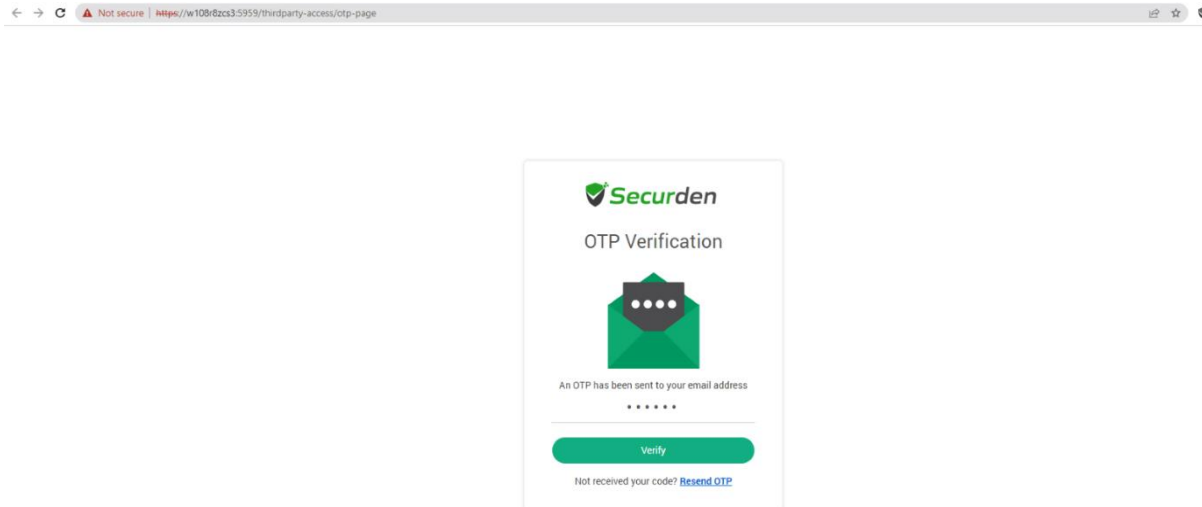
If required, you can select the email of the user and **Terminate Access** to the account. This will end their access regardless of the time-duration defined.

How external users access the shared account

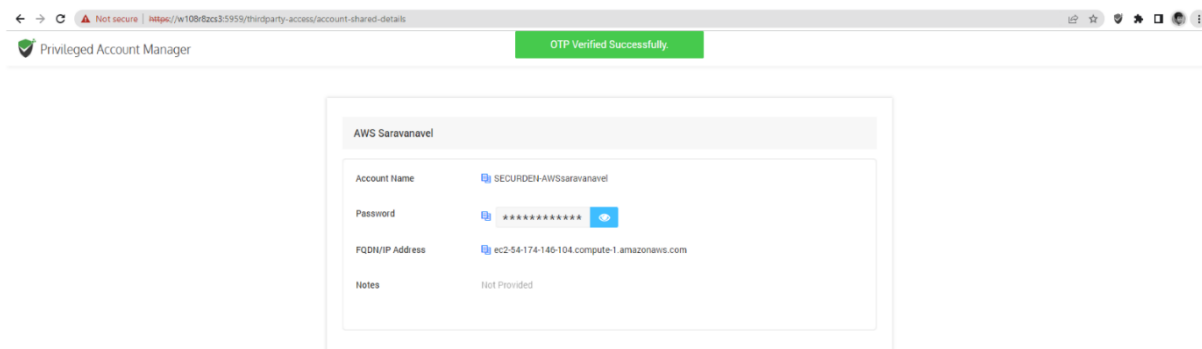
The external user who receives the shared account will find a link in their email id as shown below.



Upon clicking the link, they will be taken to a Securden OTP verification page. This OTP can be found in the inbox of the external user.



On entering the OTP and clicking **Verify**, they will be able to access the account shared with them.



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

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

Copy Account Direct Access URL

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

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

Just-in-time Access through Approval Workflows

You can establish an additional layer of security for sensitive accounts by enforcing your users to go through approval workflows. This also serves as just-in-time access provisioning mechanism. Whenever the passwords of such accounts are to be accessed, users will have to raise a request and select administrators or account managers, who are designated as **Approvers** and will grant time-limited access. At the end of the usage period, the password will be automatically reset.

This feature comes with adequate provisions to handle various scenarios such as obtaining permission in advance, granting automated approvals, etc.

Configuring approval workflow

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

The screenshot shows the Securden Privileged Account Manager interface. The left sidebar lists accounts under 'All Accounts'. The main content area is titled 'Approval Workflow' and contains a description of the approval process, a 'Designate Approvers' section with a search box, and options to 'Add Second Level Approvers', 'Add Exclusion List', and 'Configure Automatic Approval'.

Designate Approvers

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

This screenshot shows the 'Approval Workflow' tab with designated approvers. The 'Designate Approvers' section lists 'Jonathan Ridge (John Ridge)' and 'IT Team'. The 'Second Level Approvers' section lists 'Securden Administrator (admin)'. The 'Third Level Approvers' section lists 'Destro Shax (destro)'. Each section has a 'Clear All' button.

Exclusion List

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

The screenshot displays the Securden Unified PAM web interface. The left sidebar shows a list of accounts under 'All Accounts', with 'Email login' selected. The main panel is titled 'Approval Workflow' and contains the following sections:

- Designate Approvers:** A section for specifying administrators who can approve password access requests. It includes a search bar with the text 'Jonathan Ridge (John R)' and a 'Clear All' button.
- Add Second Level Approvers:** A section for adding additional approvers.
- Exclusion List:** A section for specifying users or user groups to be granted direct access to the password without going through the approval process. It includes a search bar with the text 'Perry Theplat (Perry)' and a 'Clear All' button.
- Configure Automatic Approval:** A section for configuring automatic approval. It includes a checkbox for 'Configure Automatic Approval' (which is checked), a radio button for 'All times during the day' (which is selected), and a time interval selector showing '00' and '00' with 'and' in between.

A 'Save' button is located at the bottom of the configuration panel.

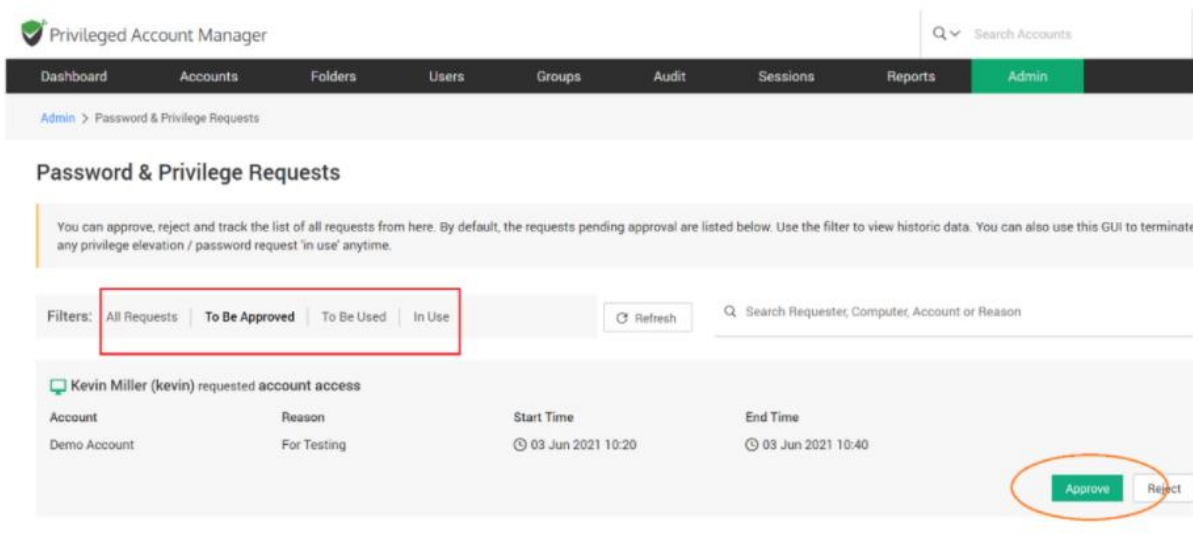
Configure Automatic Approval

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

Managing Access Requests

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

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



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

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

Important Note:

- Once a user starts accessing the application after receiving approval, concurrent controls kick in. No other user, including the administrator, super administrator, and account owner, would be able to access the application until the access is surrendered or terminated, or expired. If another user attempts to access the account in use, they will see the message **In exclusive use by another user**.
- If the periodic password reset is configured for an account and at the time of the reset execution the account is used by a user, in this scenario the password reset task will not be executed for the account.

Accounts Report

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

Details that the report captures:

Password usage statistics - Data shown here includes password retrievals, remote connections launched and password auto-fills on websites.

Account usage statistics - The data in this report highlights the number of times the selected account has been used and by which user.

Access Details - A list of all the users who had accessed the account.

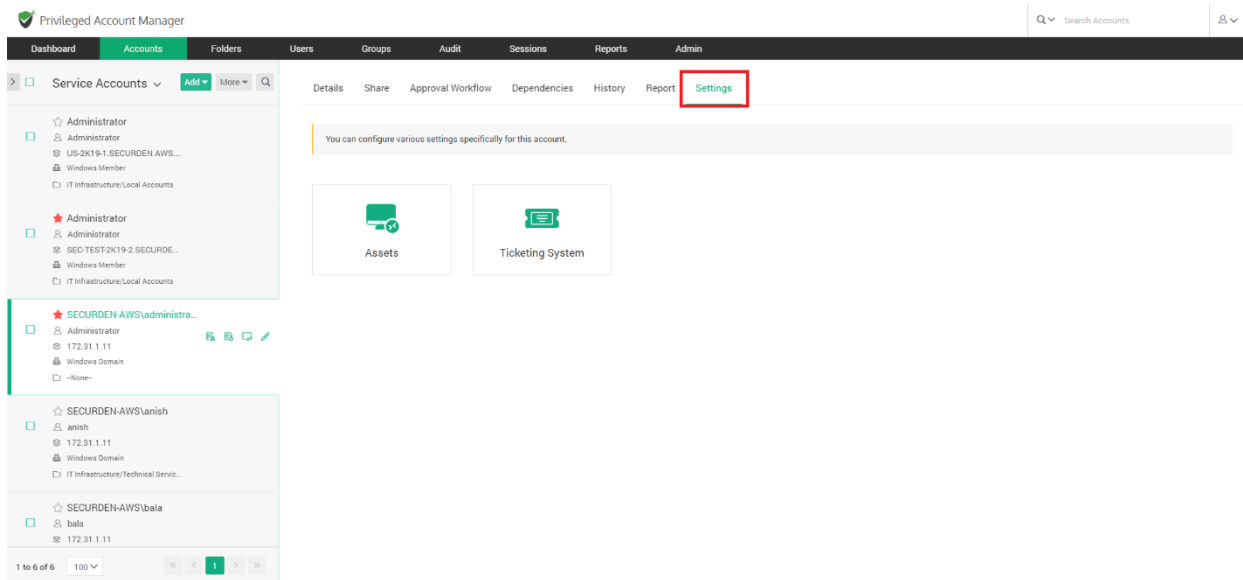
Account Activity - Lists out all the activities performed on the account by users.

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

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

Account Settings

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



Assets

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

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

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Service Accounts

- Administrator
 - Administrator
 - US-2K19-1.SECURDEN-AWS...
 - Windows Member
 - IT Infrastructure/Local Accounts
- SECURDEN-AWS/administra...
 - Administrator
 - SEC-TEST-2K19-2.SECURDE...
 - Windows Member
 - IT Infrastructure/Local Accounts
- SECURDEN-AWS/anish
 - anish
 - 172.31.1.11
 - Windows Domain
 - IT Infrastructure/Technical Serv...
- SECURDEN-AWS/bala
 - bala
 - 172.31.1.11

1 to 6 of 6 100

Assets

You can list down here the computers and other IT assets to which remote connections could be launched using this domain account.

Asset Identifier Asset Connection Type Actions

test	172.31.1.12	RDP	
------	-------------	-----	--

Showing 1 to 1 of 1 25

Add Assets

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Service Accounts

- Administrator
 - Administrator
 - US-2K19-1.SECURDEN-AWS...
 - Windows Member
 - IT Infrastructure/Local Accounts
- SECURDEN-AWS/administra...
 - Administrator
 - SEC-TEST-2K19-2.SECURDE...
 - Windows Member
 - IT Infrastructure/Local Accounts
- SECURDEN-AWS/anish
 - anish
 - 172.31.1.11
 - Windows Domain
 - IT Infrastructure/Technical Serv...
- SECURDEN-AWS/bala
 - bala
 - 172.31.1.11

1 to 6 of 6 100

Add Assets

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

Connection Type *
Select

Asset Identifier*

IP Address*

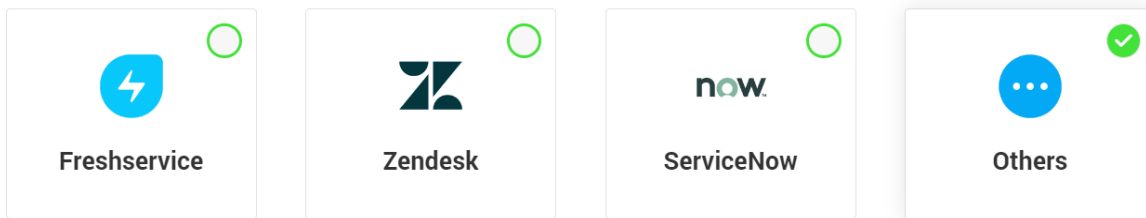
Add Cancel

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

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

Enforcing Ticketing System Validation

Securden integrates with web-based ticketing systems. The integration helps trace specific activities like password retrieval in Securden to corresponding entries in the ticketing system. Securden validates the ticket ID provided by users either by matching the RegEx pattern of the ticket ID or directly accessing the ticketing system through API calls to see if there is a matching ticket found to be open. Out of the box, Securden integrates with Freshservice, Zendesk, and ServiceNow. However, you can integrate with any ticketing system through RegEx pattern validation.



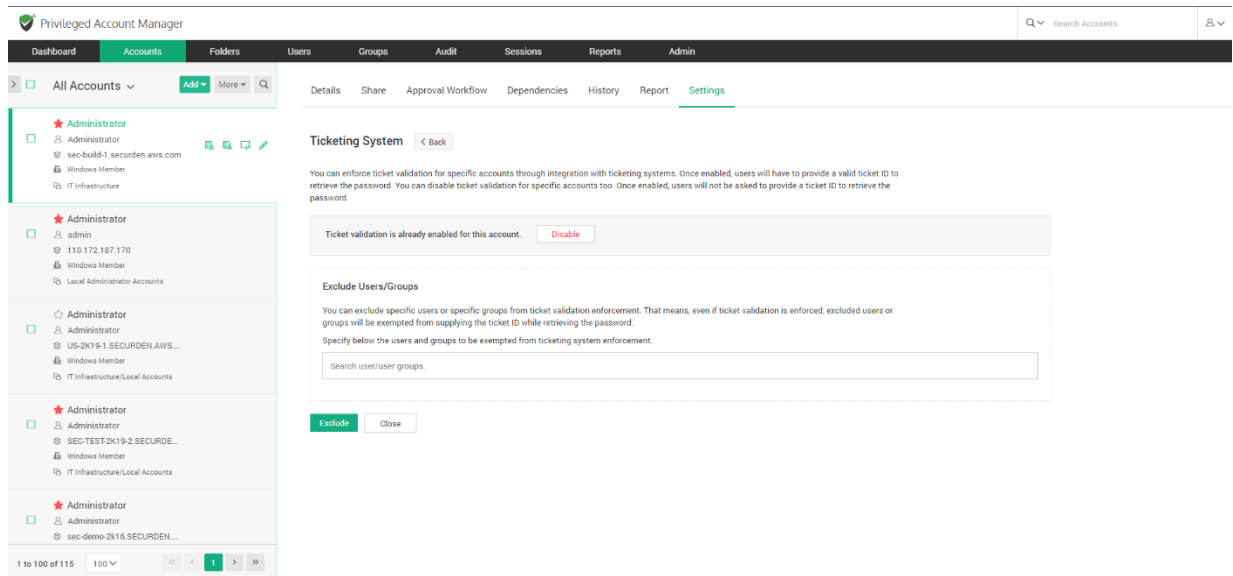
Note: After configuring ticketing system here, you need to enable it at the account/folder level for the required accounts/folders.

Enabling it at the account/folder level

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

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

You can exclude specific users or specific groups from ticket validation enforcement. That means, even if ticket validation is enforced, excluded users or groups will be exempted from supplying the ticket ID while retrieving the password.



Account Actions

Clone Account

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

The screenshot shows the Securden Unified PAM interface. The left sidebar displays a list of accounts under 'All Accounts'. The main panel shows the details for an 'Administrator' account. The 'Actions' menu is open, and the 'Clone Account' option is highlighted with a red box. The account details include:

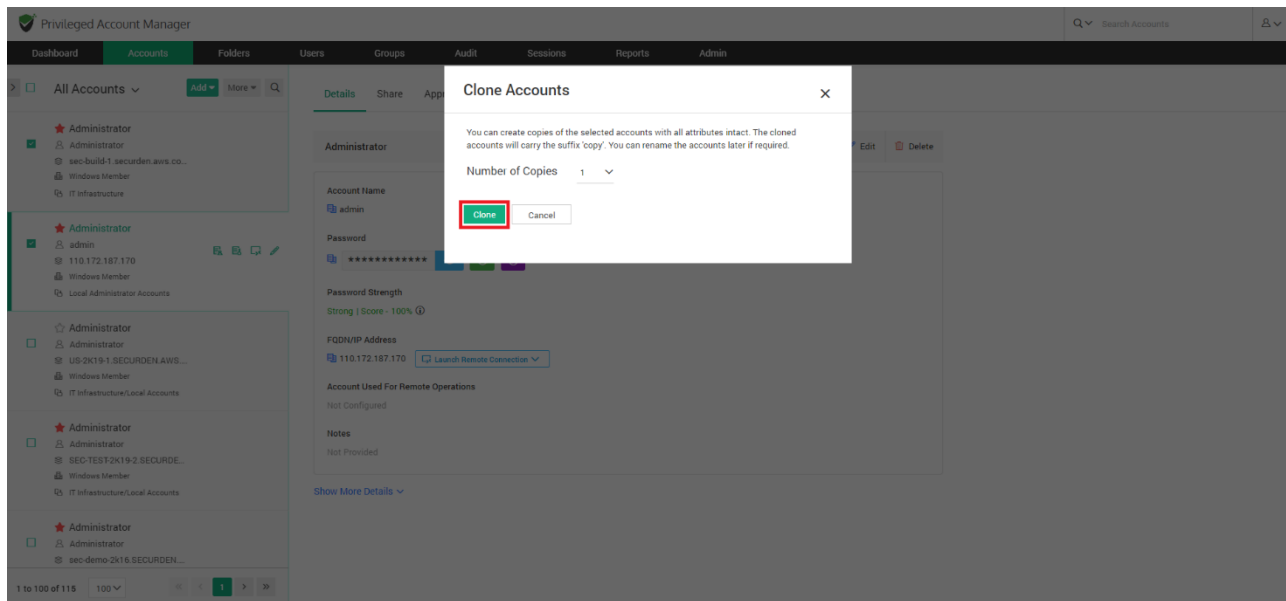
- Account Name:** Administrator
- Password:** [Masked]
- Password Strength:** Weak | Score - 0%
- FQDN/IP Address:** sec-build-1.securden.aws.com
- Account Used For Remote Operations:** SECURDEN-AWS/administrator

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

The screenshot shows the Securden Unified PAM interface. The left sidebar displays a list of accounts under 'All Accounts'. The 'More' menu is open, and the 'Clone Accounts' option is highlighted with a red box. The main panel shows the details for an 'Administrator' account. The account details include:

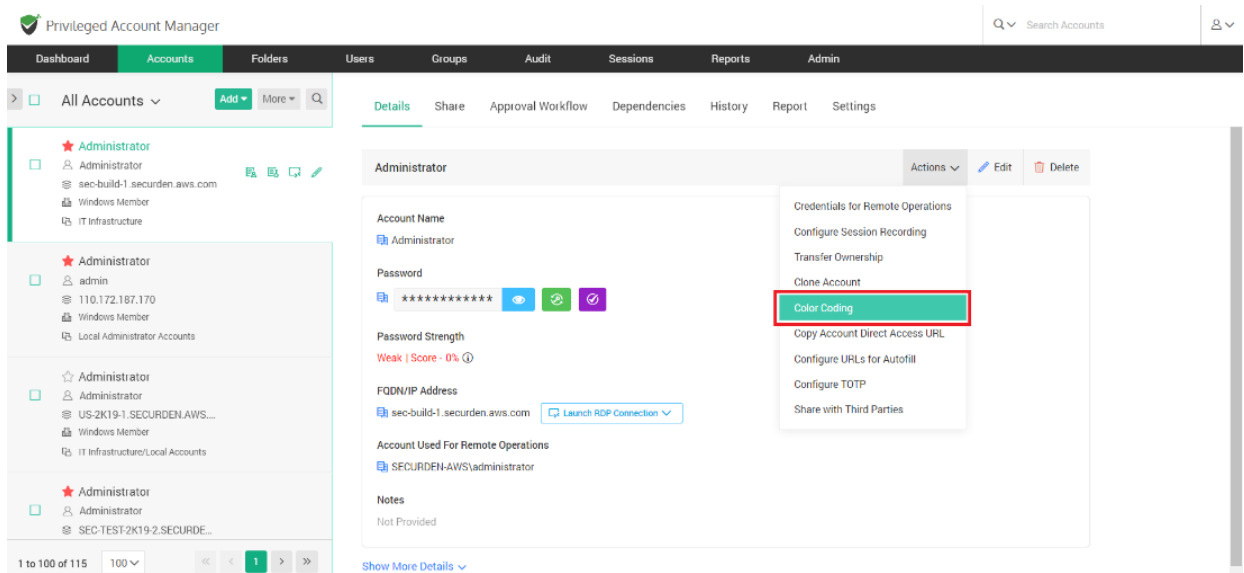
- Account Name:** admin
- Password:** [Masked]
- Password Strength:** Strong | Score - 100%
- FQDN/IP Address:** 110.172.187.170
- Account Used For Remote Operations:** Not Configured

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

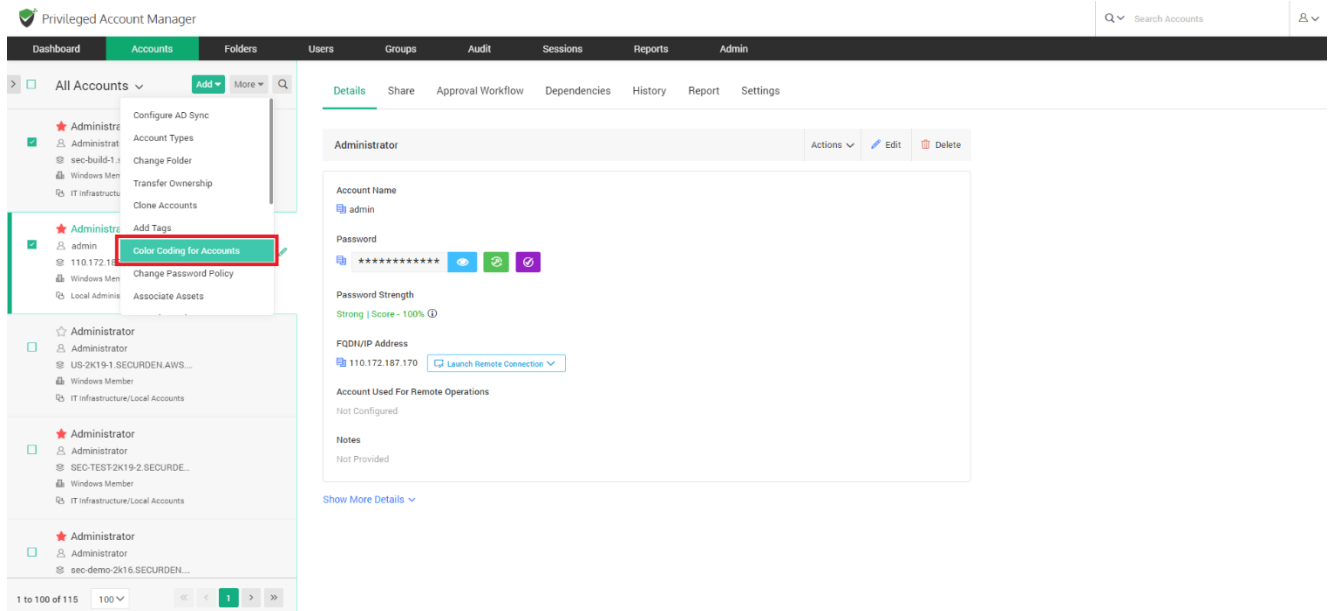


Color Coding

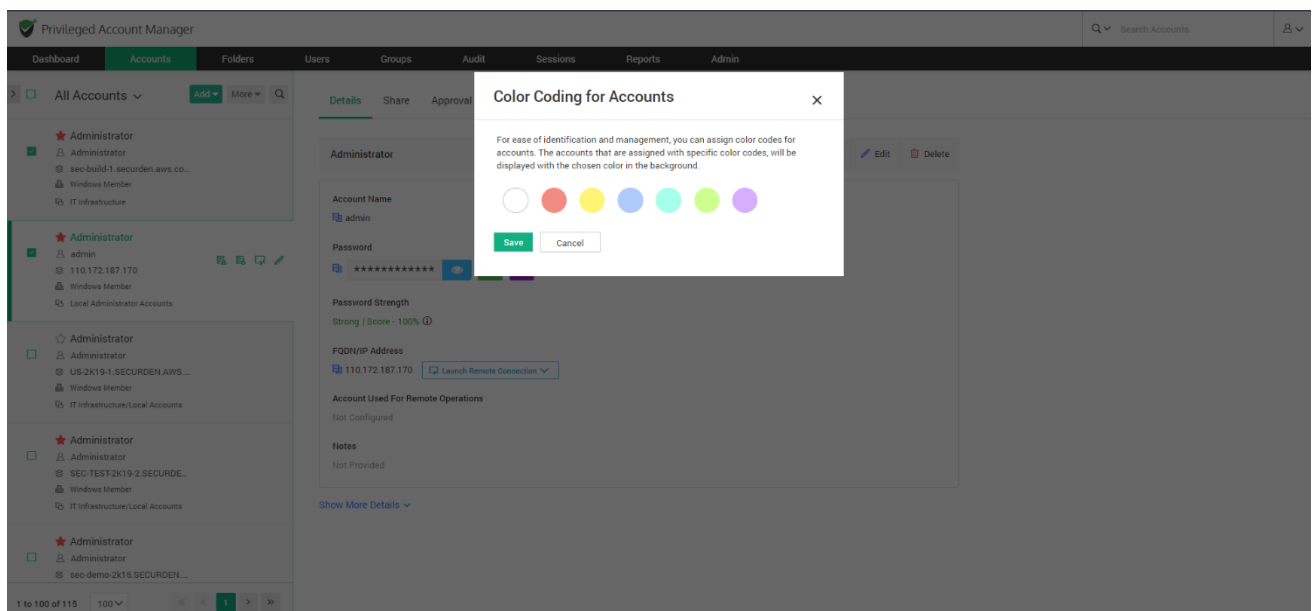
Designed for ease of identification and management, you can assign a color code for an account. Once a color is selected, the account will be displayed with the chosen color in the background. Select the account that you want to color code. Navigate to **Actions >> Color Coding**.



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

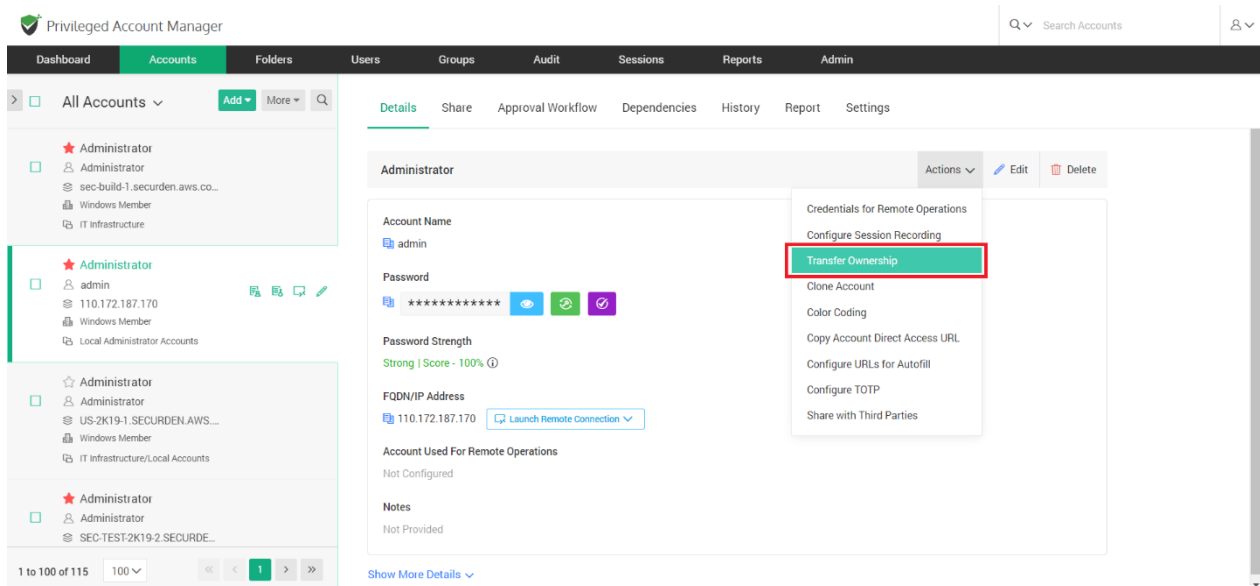


Select the desired color and click **Save**.

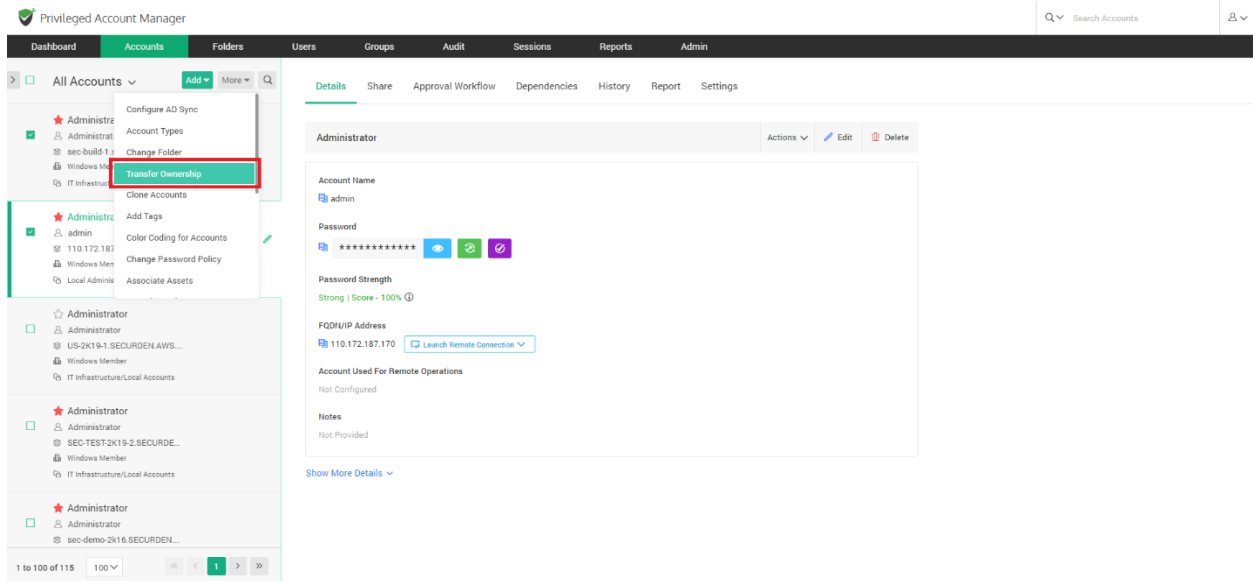


Transfer Ownership

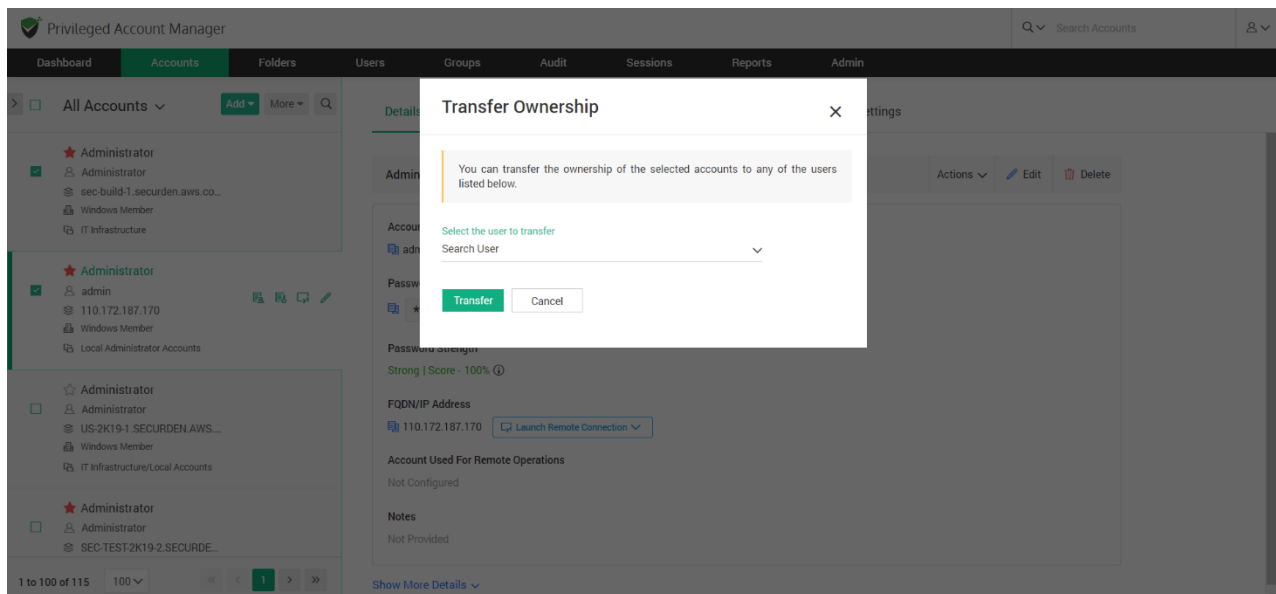
You can transfer the ownership of a particular account to any of the users in Securden. In such an event, the transferer will lose access to the accounts and folders already owned and the transferee will get complete ownership of those accounts and folders. Select the required accounts and navigate to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



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



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



Performing Operations on Multiple Accounts

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

Configuring AD Sync

You can synchronize the accounts in AD with Securden manually or configure periodic synchronization. To manually synchronize it, navigate to **Accounts >> More >> Configure AD Sync**.

On the left, you will find the Account Groups present in AD. On the right side of the interface, you have two tabs **Details** and **Periodically Synchronize Accounts**.

The screenshot displays the 'Privileged Account Manager' interface. The top navigation bar includes 'Dashboard', 'Accounts' (selected), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar and user profile icon are on the right. Below the navigation bar, the 'Accounts' section is active, showing a list of 'Account Groups' on the left and a 'Details' view for 'Account Operators' on the right.

Account Groups List (Left):

- Account Operators**: Members can administer domain user an... (SECURDEN.AWS.COM)
- All Domain Member Computers**: Group description not given in AD (SECURDEN.AWS.COM)
- AllUsers**: Group description not given in AD (SECURDEN.AWS.COM)
- AWSComputer**: Group description not given in AD (SECURDEN.AWS.COM)
- Computers**: Default container for upgraded computer accounts (SECURDEN.AWS.COM)

Details View (Right):

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

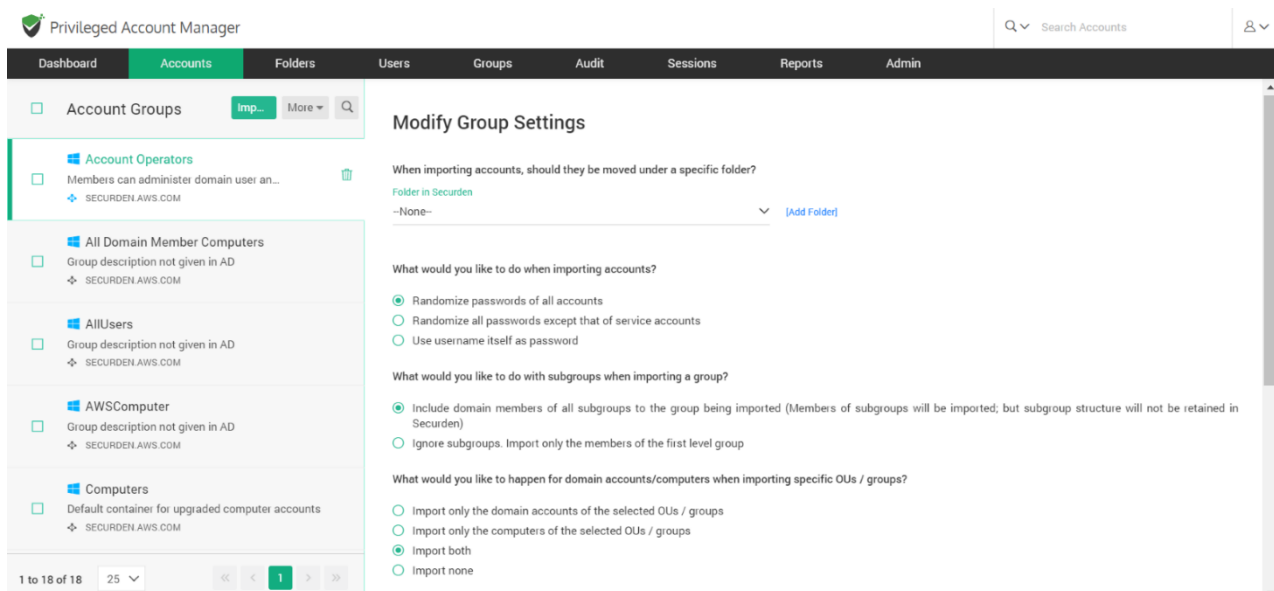
Buttons: Sync Members, Group Settings

Footer: 1 to 18 of 18, 25, 1

Details

Under the **Details** tab, you have the options to sync members and view the group settings. Once you click **Sync Members**, the discovery process begins and fetches the domain accounts that are discovered by Securden. The process of fetching dependencies will take a while to complete and will be automatically populated after completion.

On clicking the **Group Settings** button, you will get to modify the group settings. You can select the required choices and click **Save**.



Periodically Synchronize Accounts

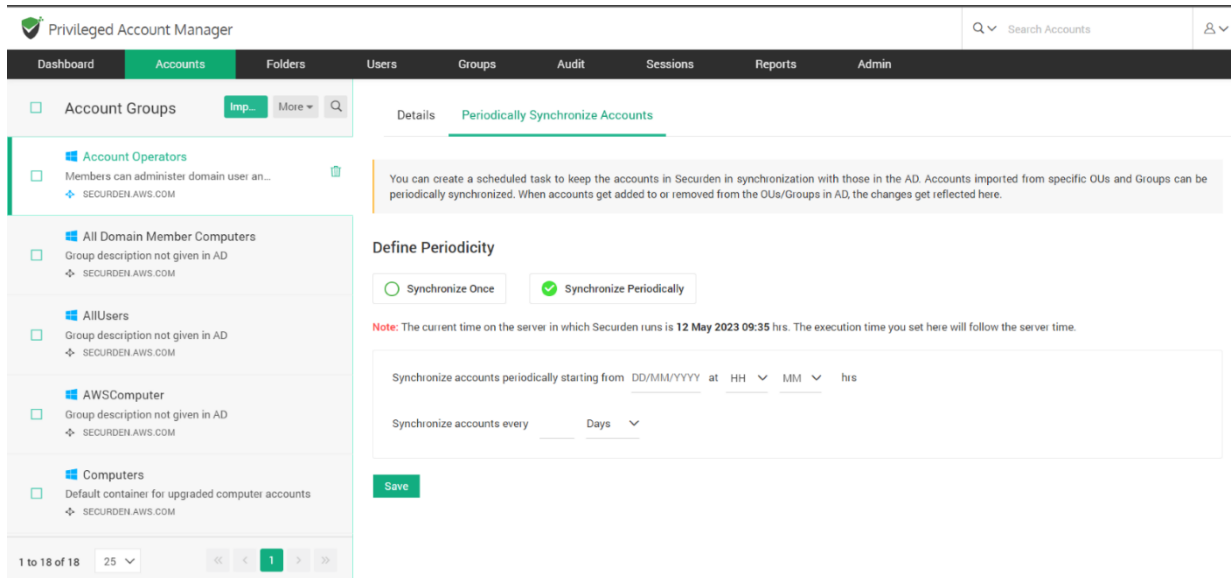
You can create a scheduled task to keep the accounts in Securden in synchronization with those in the AD. Accounts imported from specific OUs and Groups can be periodically synchronized. When accounts get added to or

removed from the OUs/Groups in AD, the changes automatically get reflected in Securden.

You have two options, **Synchronize Once** and **Synchronize Periodically**. If you want to synchronize once, you need to mention the date and time at which the sync should occur and click **Save**.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts' (selected), 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' and a user profile icon are on the right. The left sidebar shows a list of account groups under 'Account Groups', including 'Account Operators', 'All Domain Member Computers', 'AllUsers', 'AWSComputer', and 'Computers'. The main content area is titled 'Details Periodically Synchronize Accounts'. It contains a note about creating a scheduled task for synchronization. Below this is a 'Define Periodicity' section with two radio buttons: 'Synchronize Once' (selected) and 'Synchronize Periodically'. A red note indicates the current server time is 12 May 2023 09:35 hrs. Below the note is a form to set the synchronization time: 'Synchronize accounts on DD/MM/YYYY at HH MM hrs'. A green 'Save' button is at the bottom.

If you want to synchronize periodically, you also need to mention the frequency of synchronization in days. After entering the required inputs, click **Save**.



Add and Manage Account Types

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

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

Creating a new account type

To create a new account type, navigate to **Admin >> Account Management >> Account Types**. You need to select between **Work** and **Personal** type

account and click **Add Account Type**. Enter a name for the new account type being created. The name you enter here will uniquely identify the type. Adding a description to the type would help further in this aspect.

The screenshot shows the 'Add Account Type' form in the Privileged Account Manager. The interface includes a top navigation bar with 'Privileged Account Manager' and a search bar. Below the navigation bar is a menu with 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin' (highlighted in green). The breadcrumb trail is 'Admin > Account Types > Add Account type'.

The form itself is titled 'Add Account Type' and contains the following fields:

- Name ***: A text input field with the placeholder 'New Account Type'.
- Description**: A text input field.
- Password Policy**: A dropdown menu with 'Securden Policy' selected.
- Template**: A dropdown menu with 'Select Template' selected.
- Primary Fields**: A section containing two rows:

	Mandatory	
Password	No	▼
URL	No	▼
- Identifiers**: A section with no visible content.

Associate a password policy

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

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

Associate a Template

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

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

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

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

Define the Fields

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

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

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

The screenshot shows the 'Privileged Account Manager' interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin' (highlighted). Below the navigation bar, the breadcrumb trail is 'Admin > Account Types > Add Account type'. A 'Select Template' dropdown is visible. The main content area is divided into two sections: 'Primary Fields' and 'Identifiers'.

Primary Fields:

Field	Mandatory
Password	No
URL	No

Identifiers:

Field	Visibility	Mandatory
Notes	Show	No
Tags	Show	No
Account Expiration Date	Hide	No

At the bottom of the form, there is a green '+ Add Fields' button and a 'Save' button next to a 'Cancel' button.

Primary Fields

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

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

Additional Fields

You can create any number of customized additional fields as required. To create additional fields, click the **Add Fields** button. When creating additional fields, you have the option to specify the field type - Text, Password, or File Store. While **Text** represents a text field, **Password** helps mask the value from being displayed in plain text. **File Store** type allows you to browse and choose files.

Managing Account Types

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

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

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Account Types

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.

Work Personal

Search Add Account Type Delete Account Types More Actions Showing 1 to 20 of 20 25

Type Name	Description	Template Name	Password Policy
Azure AD	Azure AD		Securden policy
Bank Account	Bank Account		Securden policy
Cisco IOS	Cisco IOS	Cisco IOS	Securden policy
File Store	File Store	File	Not Available

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

Delete Account Types

You can delete any custom account types created. Select the types to be deleted and then click the button **Delete Account Types**. You can also click the **Delete** icon present at the RHS of each entry.

The screenshot shows the 'Privileged Account Manager' interface. A confirmation dialog is open, asking: 'This will permanently delete the account type(s). Do you want to proceed?' with 'OK' and 'Cancel' buttons. The background interface shows the 'Account Types' section under the 'Admin' tab. A table lists various account types with columns for 'Type Name', 'Description', 'Template Name', and 'Password Policy'. The 'API Credential' and 'Azure AD' types are checked for deletion.

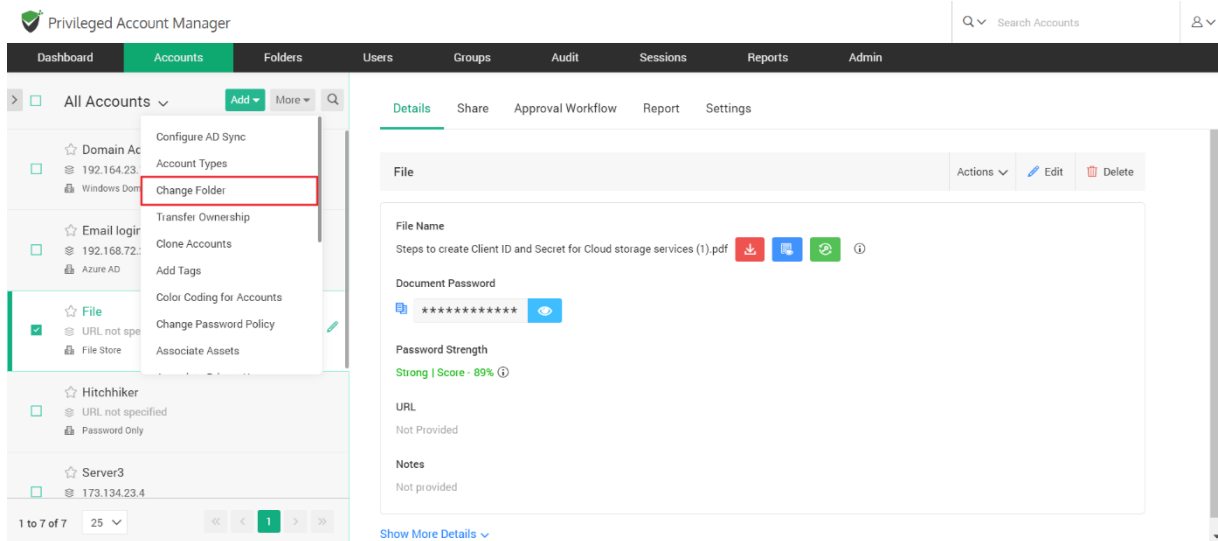
Type Name	Description	Template Name	Password Policy
<input checked="" type="checkbox"/> API Credential	API Credential	API Credential	Securden policy
<input checked="" type="checkbox"/> Azure AD	Azure AD		Securden policy
<input type="checkbox"/> Bank Account	Bank Account		Securden policy
<input type="checkbox"/> Cisco IOS	Cisco IOS	Cisco IOS	Securden policy
<input type="checkbox"/> File Store	File Store	File	Not Available

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

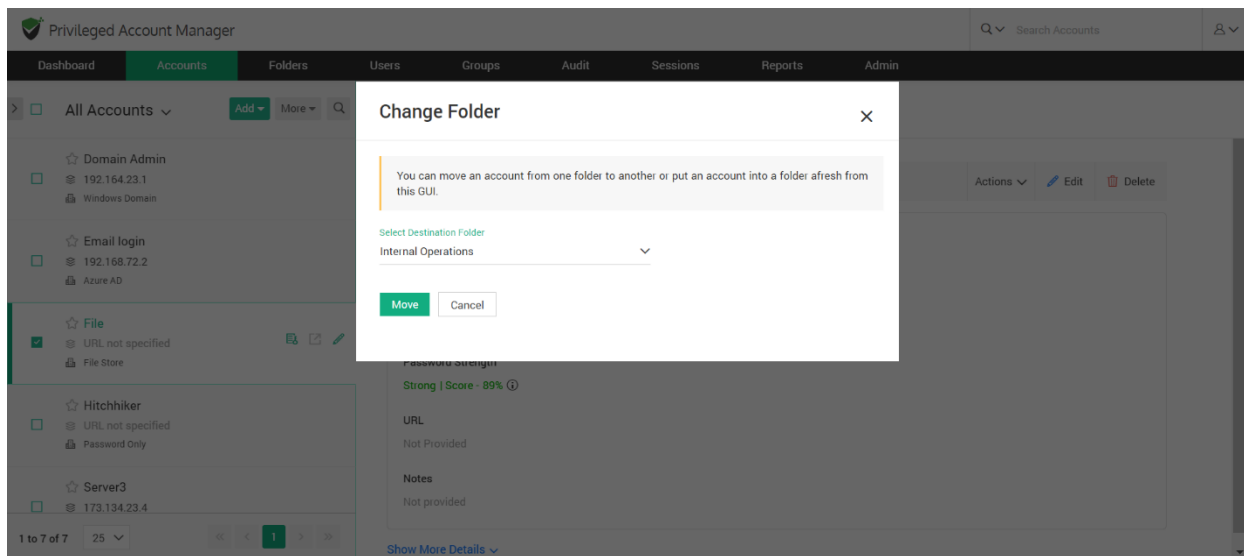
The default system defined account types cannot be deleted. They can only be disabled.

Change Folder

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

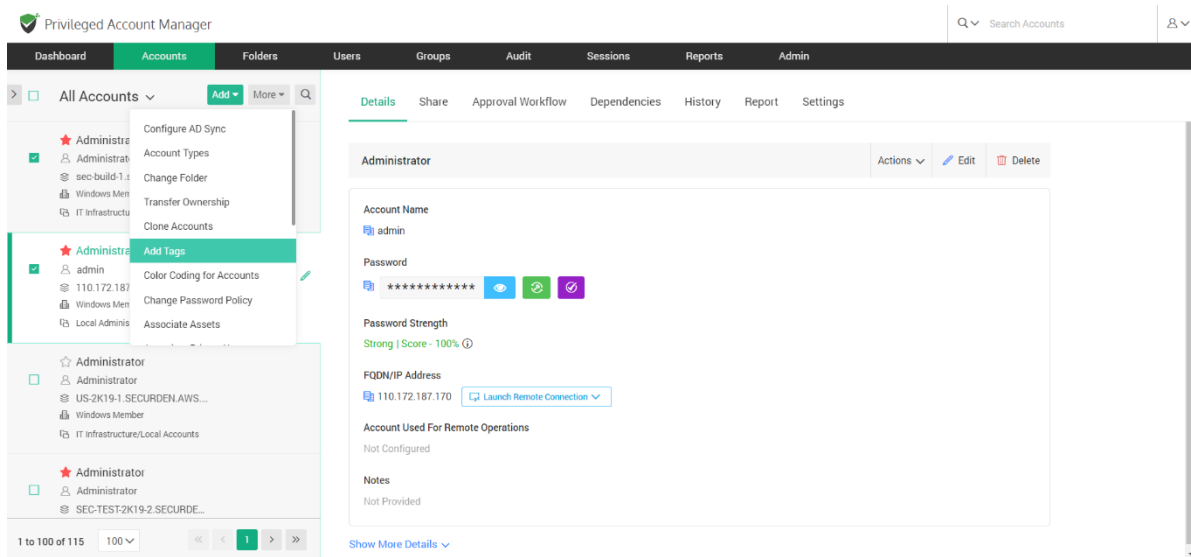


In the popup that opens, choose the folder to which the account(s) are to be moved, and then click **Move**.

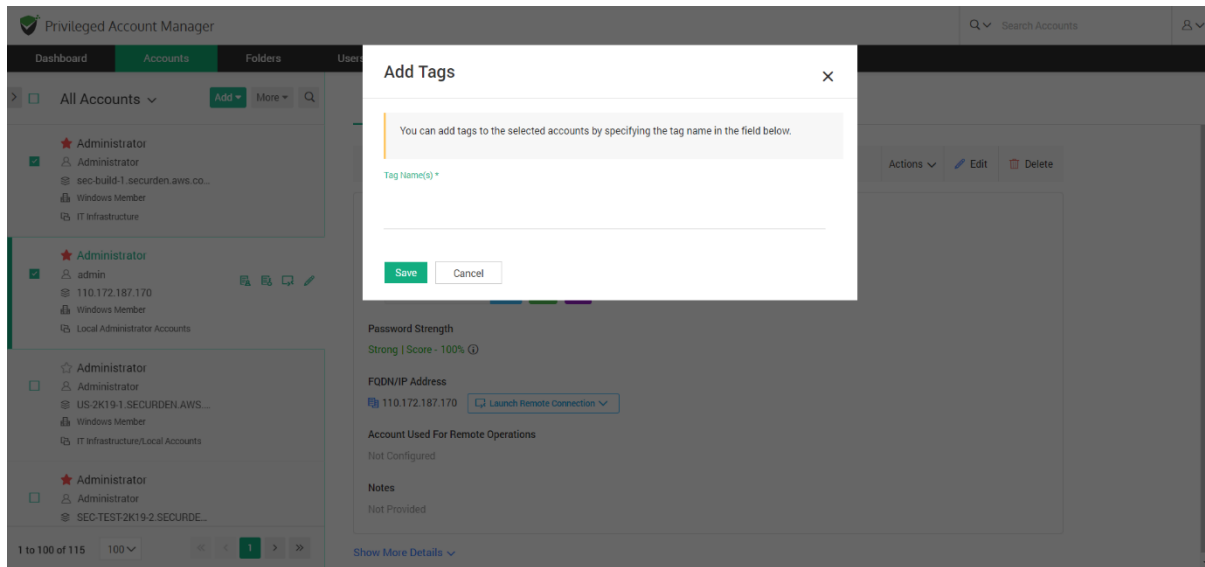


Add Tags

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

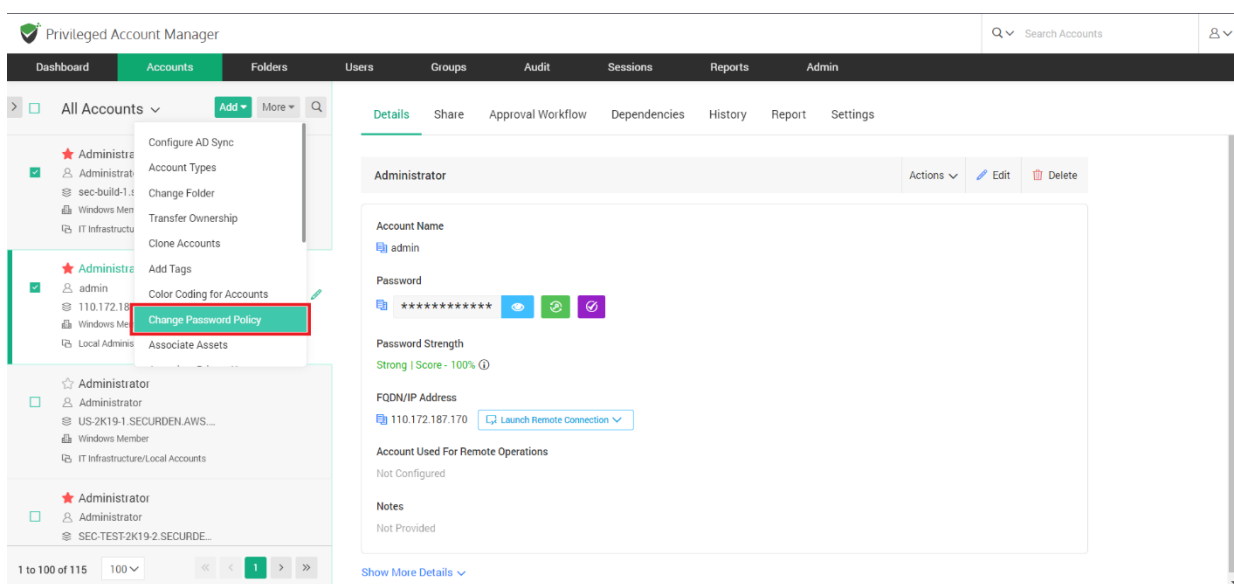


Select the account(s), enter the tag name(s), and click **Save**.

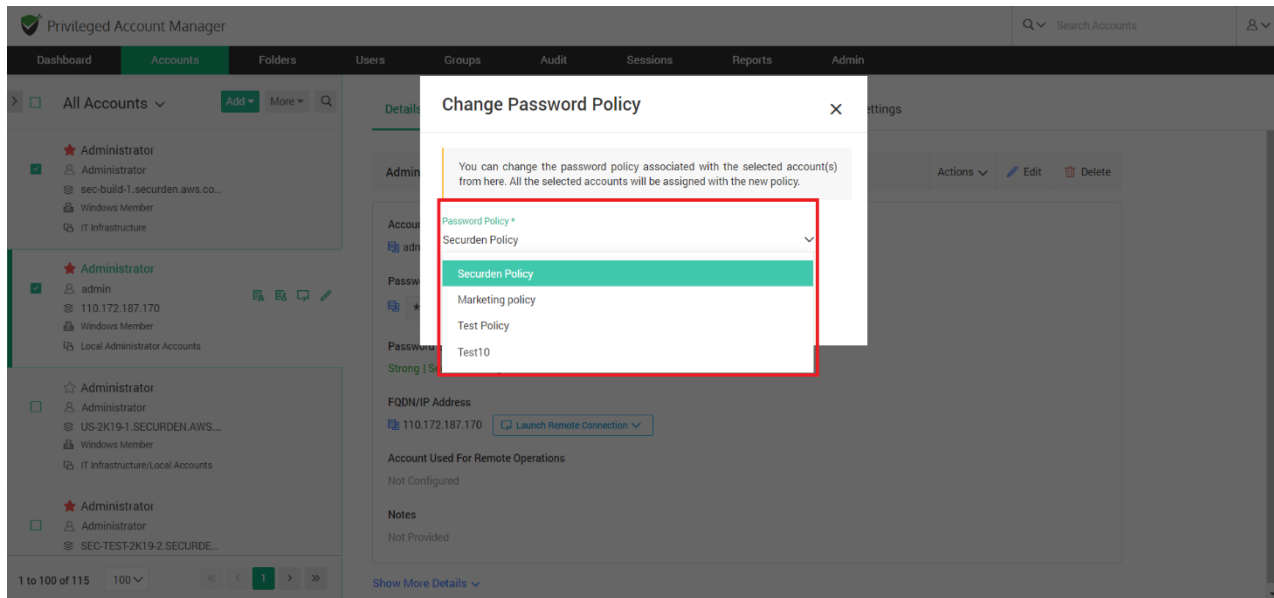


Change Password Policy

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

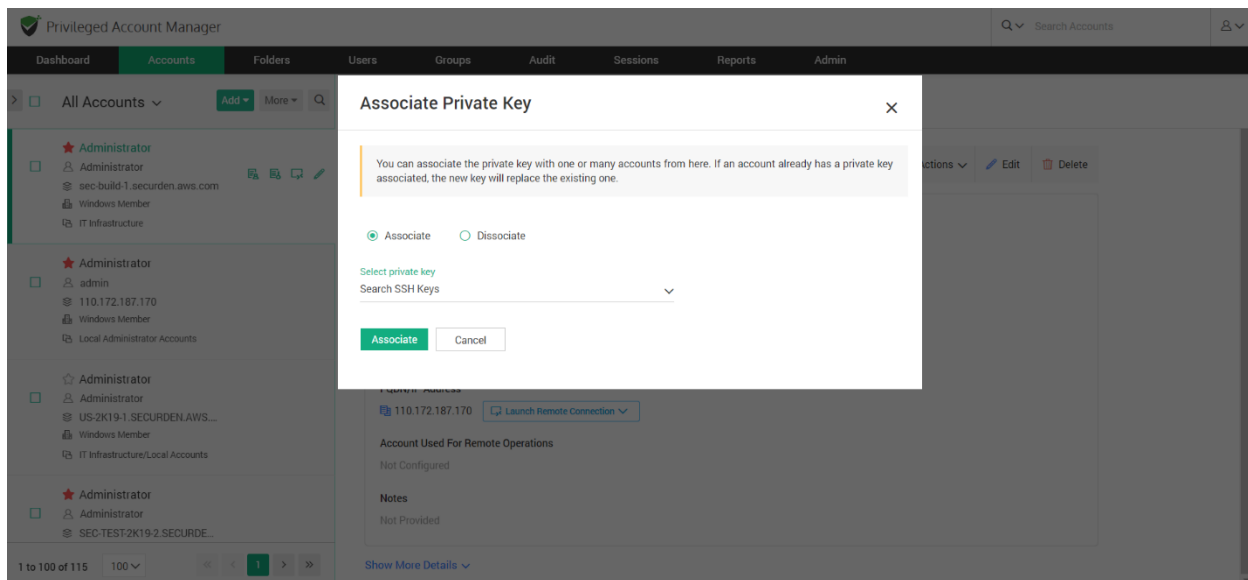


Select the account(s), click the option **Change Password Policy**, and then choose the policy to be applied from the drop-down. After selecting, click **Change Policy** to apply the policy to the account(s).



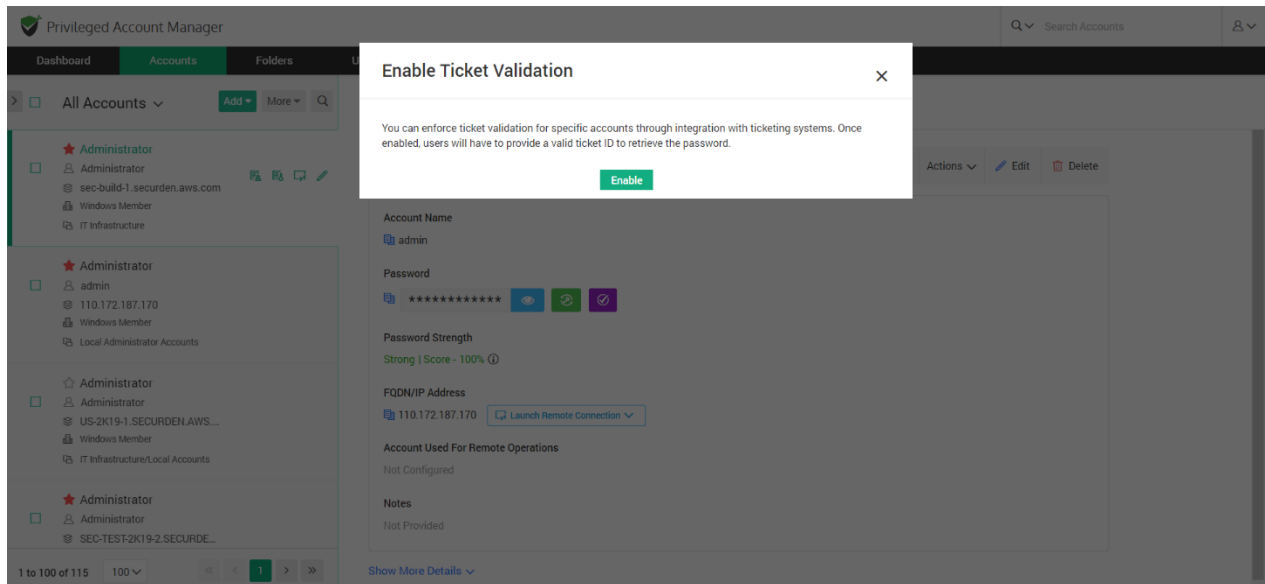
Associate Private Key

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



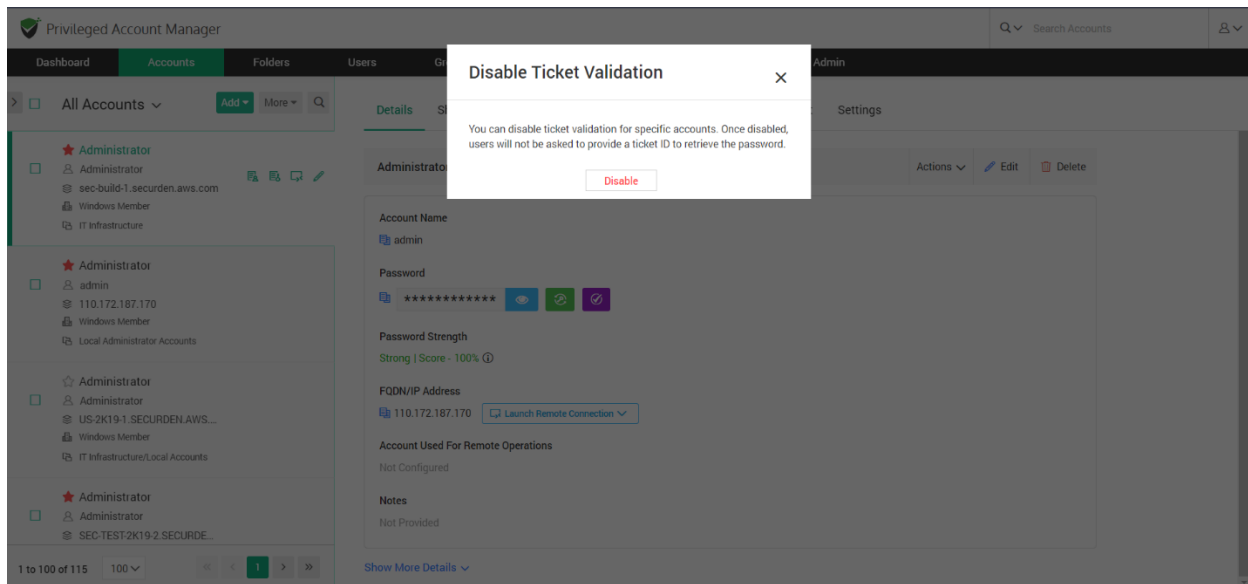
Enable Ticket Validation

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



Disable Ticket Validation

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



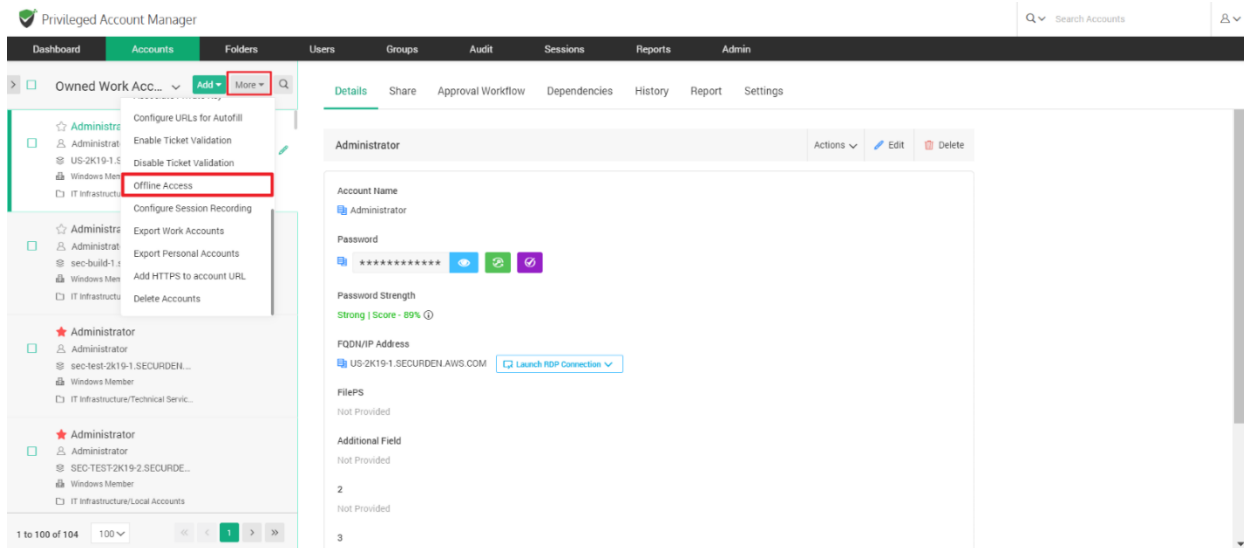
Offline Access

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

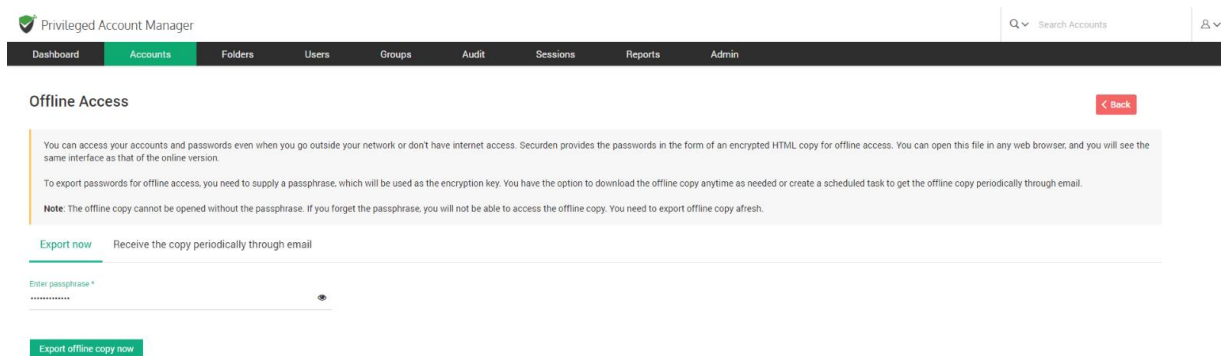
To export passwords for offline access, you need to supply a passphrase, which will be used as the encryption key. You have the option to download the offline copy anytime as needed or create a scheduled task to get the offline copy periodically through email.

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

End-users can save an offline copy of all the accounts they have access to. Users need to navigate to **Accounts >> More >> Offline Access**.



Users can export the account at once from the **Export now** tab, they need to enter a passphrase while exporting the offline copy. This passphrase will be used to open the offline copy of passwords.



Once you have decided a strong passphrase, key it in and click **Export offline copy now**.

The screenshot shows the 'Offline Access' page in the Securden Privileged Account Manager. The page has a dark navigation bar with links: Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin. The 'Accounts' link is active. In the top right, there is a search bar labeled 'Search Accounts' and a user profile icon. The main content area is titled 'Offline Access' and includes a 'Back' button. Below the title, there is a text box explaining that users can access accounts and passwords offline using an encrypted HTML copy. It also mentions that a passphrase is required for encryption and that the offline copy cannot be opened without it. Below this, there are two radio buttons: 'Export now' (selected) and 'Receive the copy periodically through email'. Under the 'Export now' option, there is a text input field labeled 'Enter passphrase *' with a password strength indicator. At the bottom, the 'Export offline copy now' button is highlighted with a red rectangular box.

Receive the offline copy through email

Users can choose to export their passwords in an offline copy to their email id. Users who wish to export a copy once can select **Export Once**.

They then need to select the date and time at which an offline copy of passwords should be sent to them.

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

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.

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

Export now Receive the copy periodically through email

Define Periodicity

☒ Export Once ☐ Export Periodically

Note: The current time on the server in which Securden runs is 20 Apr 2023 10:44 hrs. The execution time you set here will follow the server time.

Export passwords and email the encrypted offline copy on: 21 Apr 2023 at 01:05 hrs

Enter passphrase *

Save

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

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

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

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.

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

Export now Receive the copy periodically through email

Define Periodicity

☐ Export Once ☒ Export Periodically

Note: The current time on the server in which Securden runs is 20 Apr 2023 10:44 hrs. The execution time you set here will follow the server time.

Export passwords and email the encrypted offline copy periodically starting from: 21 Apr 2023 at 01:15 hrs

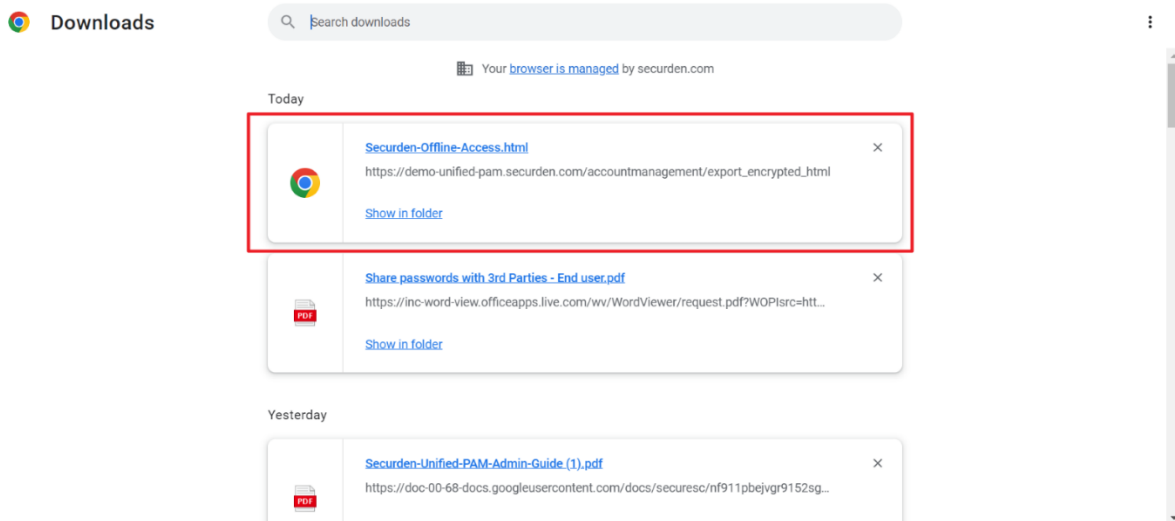
Export passwords every 2 Months

Enter passphrase *

Save

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

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



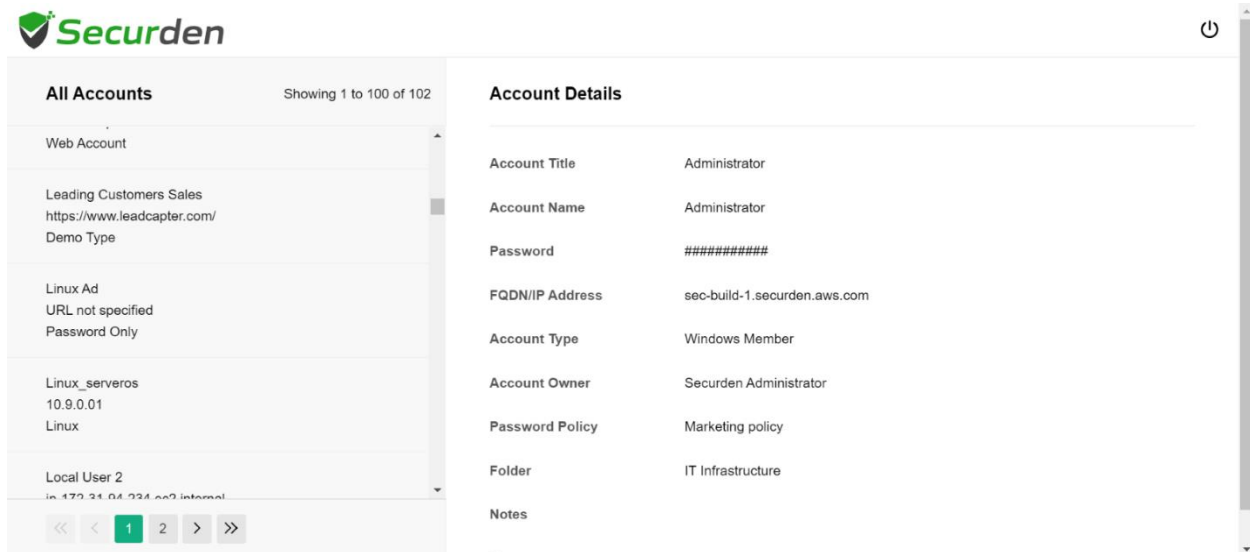
To open the encrypted HTML file, users have to enter the passphrase that they keyed in on configuring offline access.



Securden Offline Access

Proceed

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

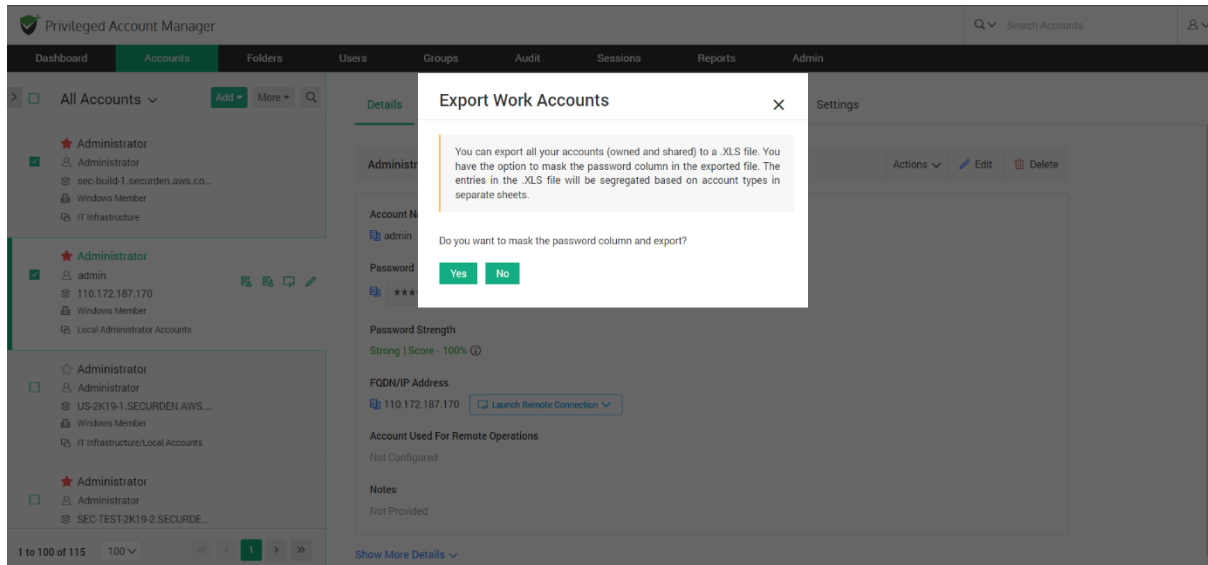


The screenshot displays the Securden web interface. On the left, under 'All Accounts', a list of accounts is shown, including 'Web Account', 'Leading Customers Sales', 'Linux Ad', 'Linux_serveros', and 'Local User 2'. The 'Account Details' panel on the right shows the following information for the selected account:

Field	Value
Account Title	Administrator
Account Name	Administrator
Password	#####
FQDN/IP Address	sec-build-1.securden.aws.com
Account Type	Windows Member
Account Owner	Securden Administrator
Password Policy	Marketing policy
Folder	IT Infrastructure
Notes	

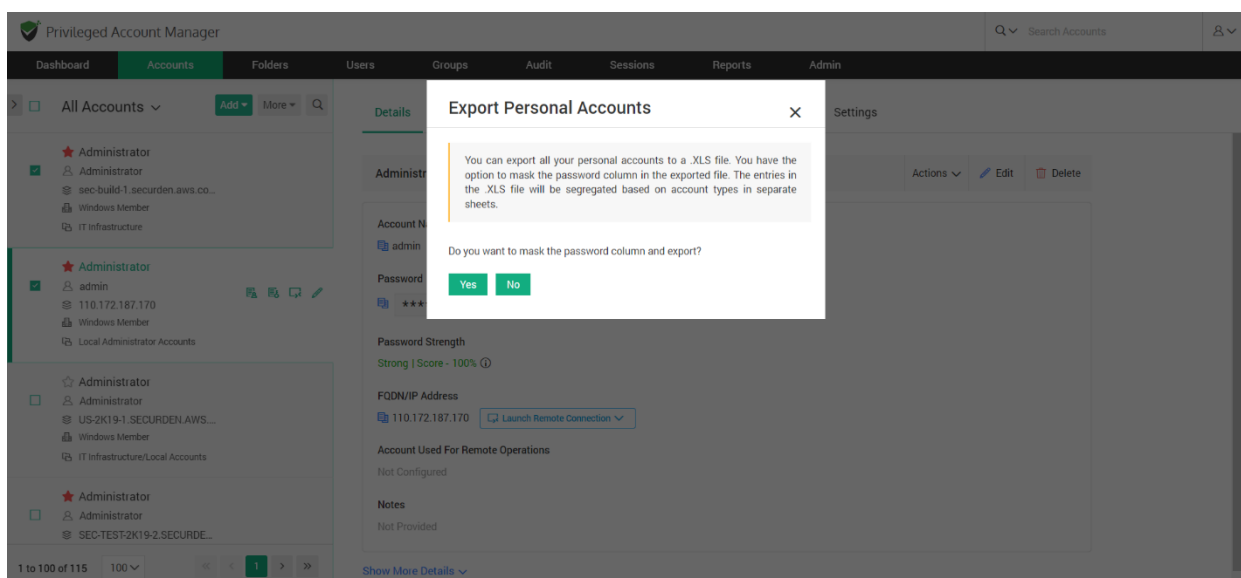
Export Work Accounts

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



Export Personal Accounts

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

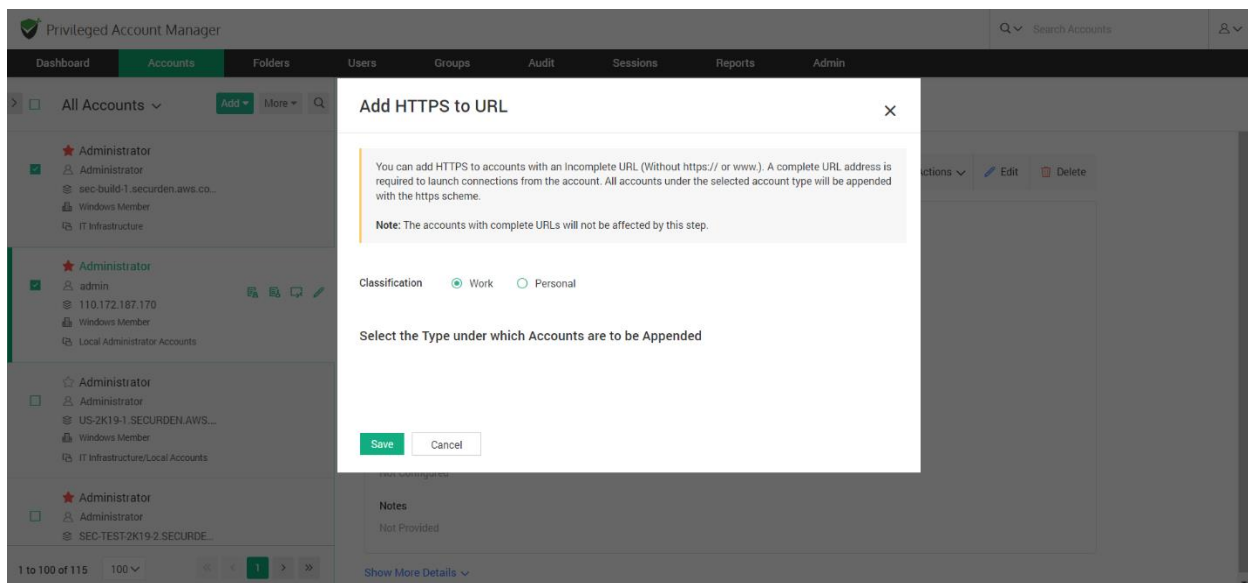


Add HTTPS to account URL

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

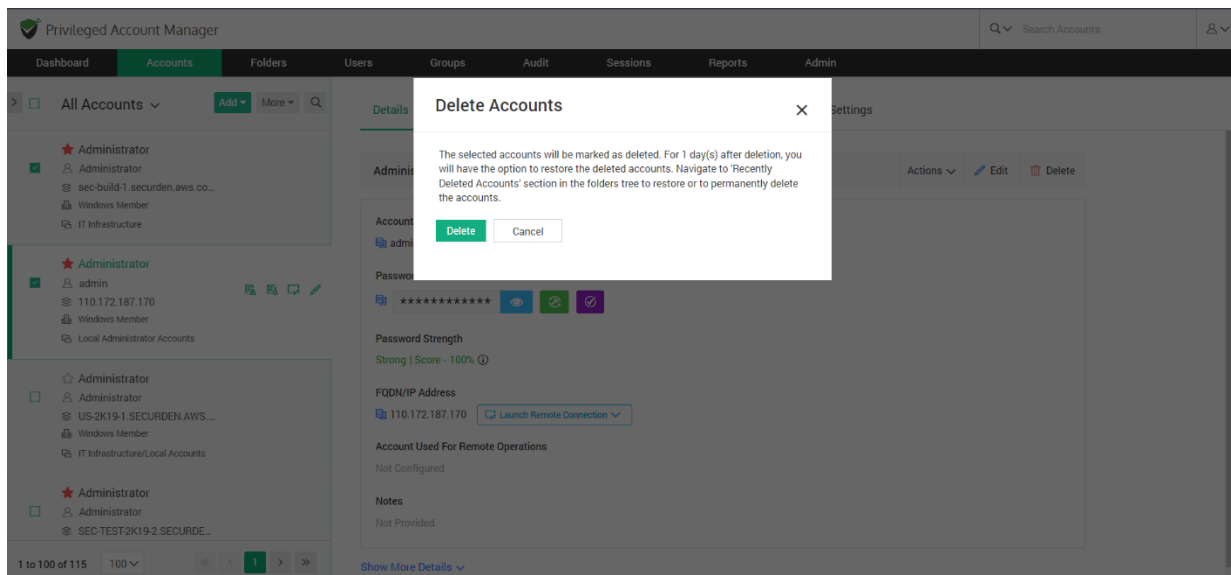
Note: The accounts with complete URLs will not be affected by this step.

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



Delete Accounts

You can delete one or more accounts at once by navigating to **Accounts >> More >> Delete Accounts**. The selected accounts will be marked as deleted. For 1 day(s) after deletion, you will have the option to restore the deleted accounts. Navigate to **Recently Deleted Accounts** section in the folders tree to restore or to permanently delete the accounts.



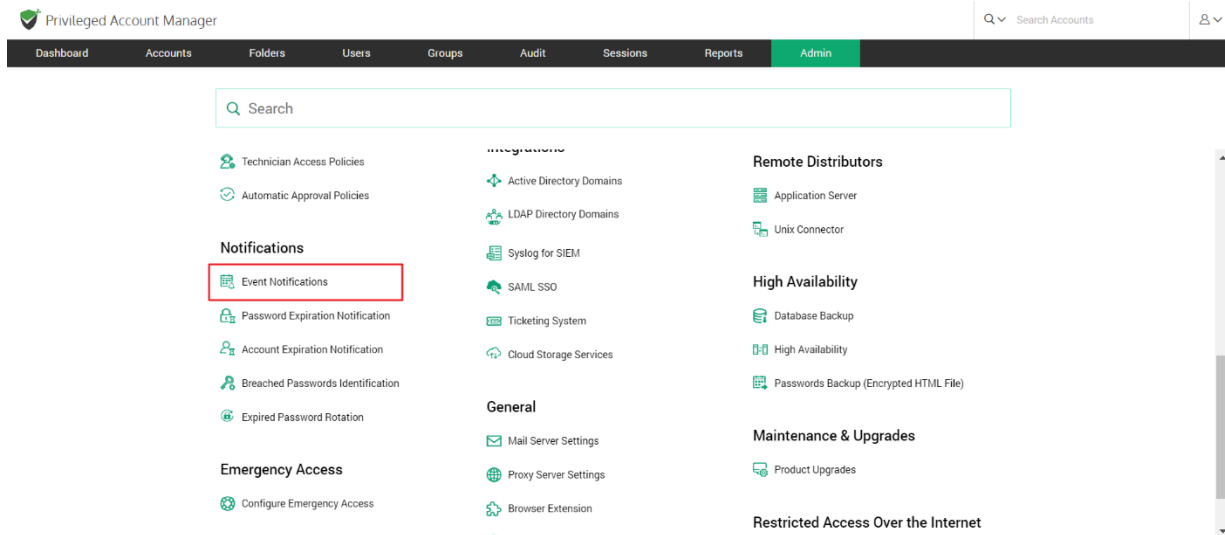
Section 6: Notifications

Event Notification

You can choose to send or receive email alerts upon the occurrence of any specific event like password retrieval, addition, deletion, and other modification activities. You can choose which events you would like to get alerted about. The notifications can be sent out in real-time as and when the event occurs or as a consolidated email once a day.

Configure Event Notifications

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



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

Selecting Events

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

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

Event 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.

Configure Notifications ☒

Select the events for which you want to receive notifications from the list below.

Events related to actions on accounts

Clear All

Remote Connection Established X Account Deleted X

Events related to user activities

Clear All

User Deleted X 2FA Disabled X

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

When do you want to get Notified?

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

Who to Notify?

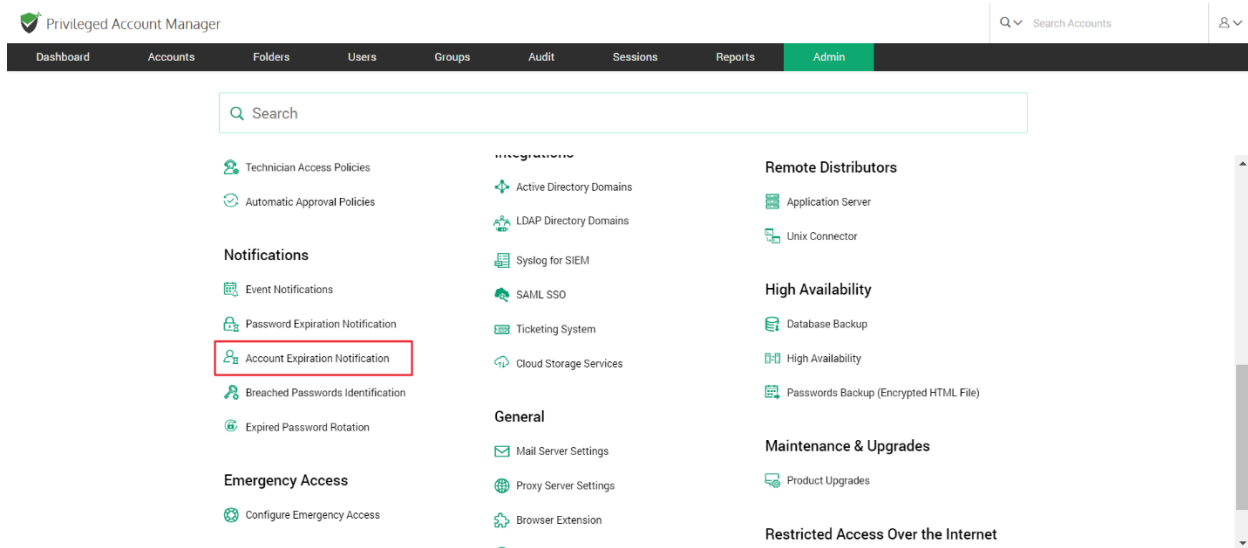
- You can trigger the notification upon the occurrence of the selected events to any specific user(s) or usergroup(s). You may even choose to trigger notifications for certain specific roles of users too - for example, 'All Administrators', 'All Auditors', etc.
- You can also send notifications to people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

Account Expiration Notification

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

Configure Account Expiration Notification

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



Enable Expiration Notification to view the configuration options.

To Configure Account Expiration Notification, follow these steps.

The Notification Schedule

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

Who to Notify?

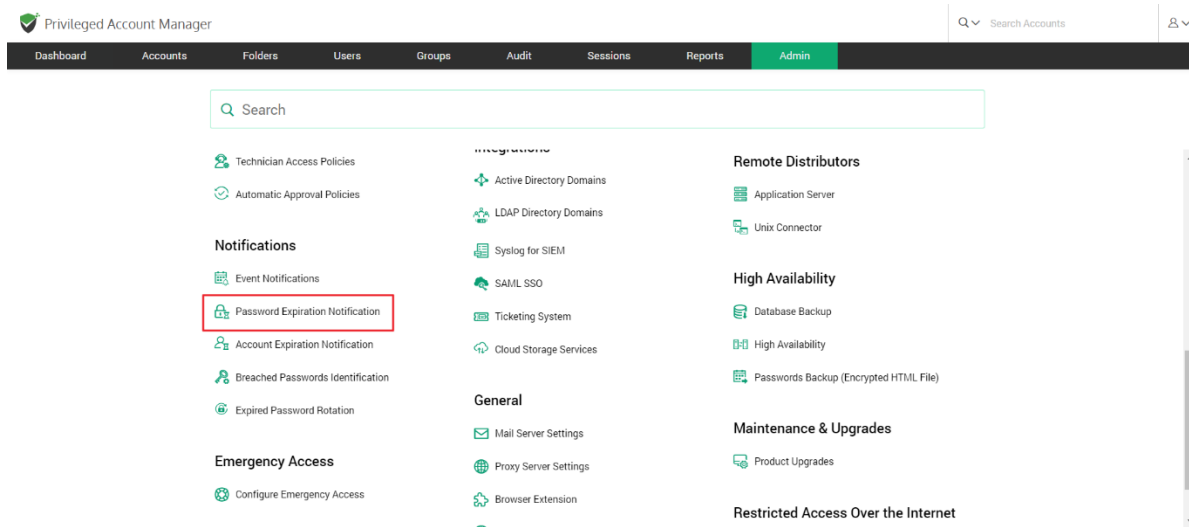
- You can trigger the notification upon the occurrence of the selected events to any specific user(s) or usergroup(s). You may even choose to trigger notifications for certain specific roles of users too - for example, **All Administrators, All Auditors**, etc.
- You can also send notifications to people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

Password Expiration Notification

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

Configuring Password Expiration Notification

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



Enable Expiration Notification to view the configuration options.

To Configure Password Expiration Notification, follow these steps

The Notification Schedule

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

Who to Notify?

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

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

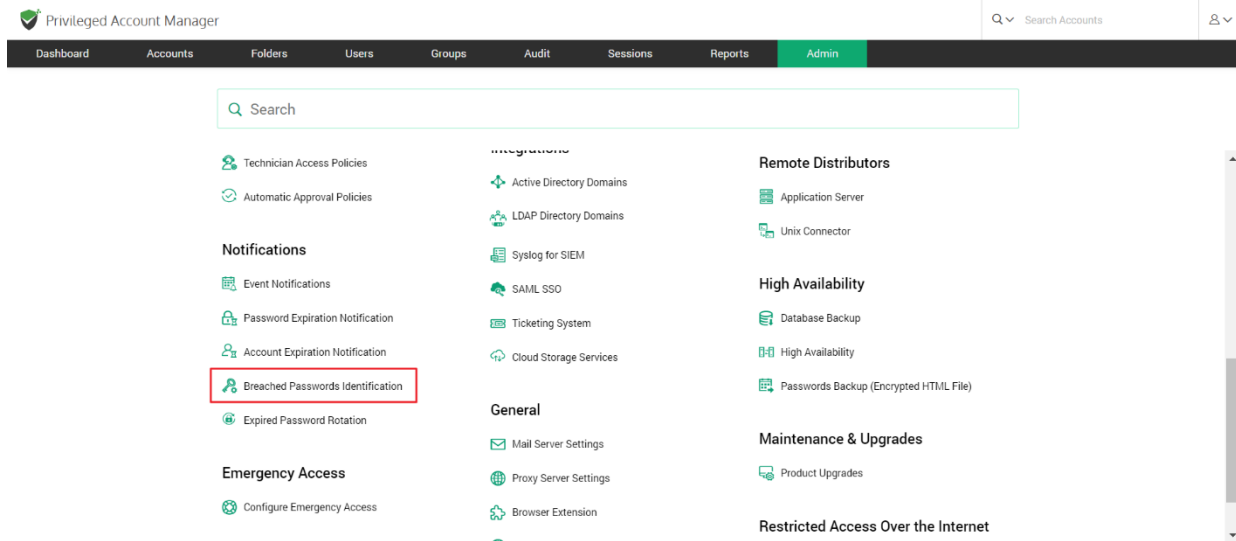
Breached Password Identification

Passwords exposed in various data breaches worldwide are publicly available as a data dump. Many times, users are not aware when their passwords are exposed in credential spilling attacks. If a breached password is being used, it may lead to a spate of cyberattacks. To prevent such incidents, Securden can periodically scan the dump and check if any of the passwords stored in the product matches with the passwords that have been exposed in known data breaches. You can configure how often Securden should check for breached passwords. Whenever usage of a breached password is detected, email alerts will be sent to administrators, auditors, respective account owners, and other specified users.

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

Configuring Breached Password Identification

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



Enable breached password Identification to view the configuration options.

To configure Breached Password Identification, follow these steps.

Periodicity of checks

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

Breached Passwords Identification

Passwords exposed in various data breaches worldwide are publicly available as a data dump. Many times, users are not aware when their passwords are exposed in credential spilling attacks. If a breached password is being used, it may lead to a spate of cyberattacks. To prevent such incidents, Securden can periodically scan the dump and check if any of the passwords stored in the product matches with the passwords that have been exposed in known data breaches. You can configure how often Securden should check for breached passwords. Whenever usage of a breached password is detected, email alerts will be sent to administrators, auditors, respective account owners, and any other specific users.

Important Note:

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

Enable Breached Passwords Identification (Periodic Check) ☒

Verification Schedule

Enter Periodicity (in days) *

7

Enable Email Alerts Upon Identification ☐

Save

Cancel

Who to Notify?

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

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

Expired Password Rotation

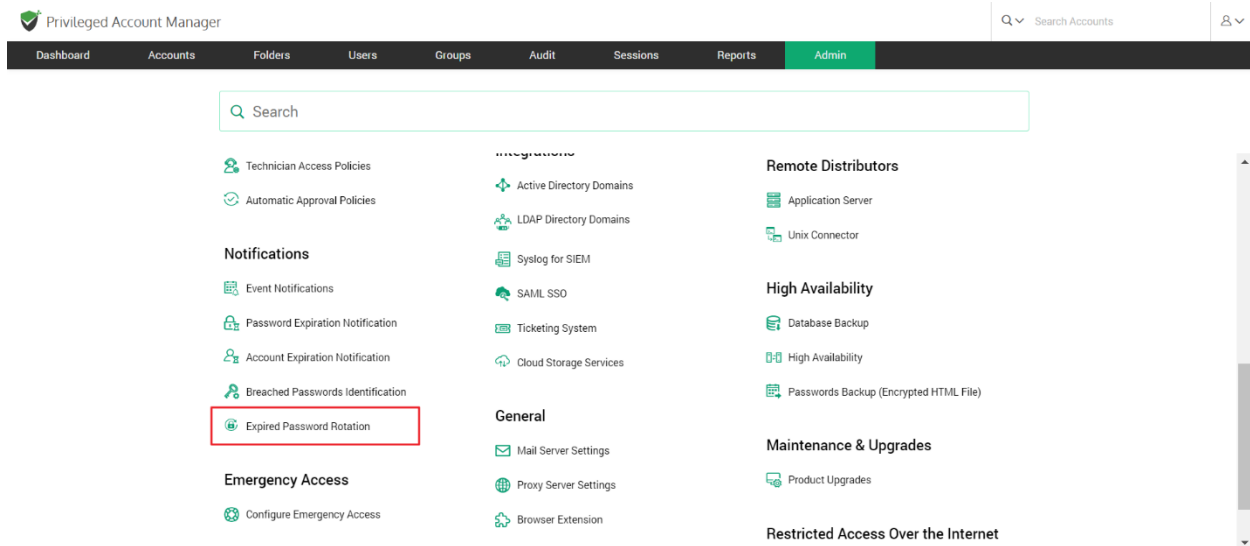
When passwords expire or are about to expire, Securden can automatically rotate them for accounts remote password reset is enabled. You can indicate the number of days until the password expires that the password rotation should be tried, as well as the number of attempts.

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

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

Configuring Password Rotation

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



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

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

If you choose **On Expiration Date**,

- You need to provide the frequency of password reset attempts, which can be as low as a minute.
- You should also specify the maximum number of attempts to be made to reset a password in **Number of retries**.

- You can choose to **Reset the already expired password**. Securden will try to reset the expired passwords at the time of configuration.

If you choose **Prior to Expiration**,

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

Event Listener

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

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

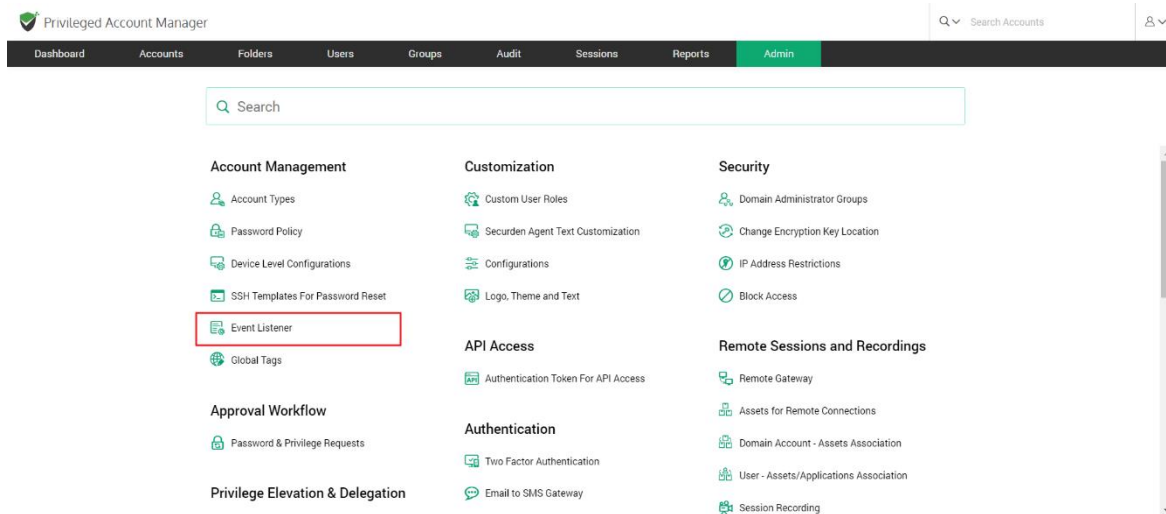
You can trigger the automated follow-up action(s) upon the occurrence of any specific event or a sequence of events in Securden. For example, when the password of an account is retrieved or changed, you can trigger a follow-up action automatically. Typically, Securden keeps listening for the event to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

and triggers the script defined by you to initiate the follow-up action.

Creating the event listener

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

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



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

Privileged Account Manager

Search Accounts




Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Event Listener

Event Listener

You can trigger an action after the occurrence of any specific event or a sequence of events in Securden. For example, when the password of an account is changed, you can trigger a follow-up action automatically. The followup action could be defined in the form of a script or as an API task making use of third-party APIs. The wizard below helps you to define the listener and the desired follow up action.

Q G III **Add Listener** Delete Listener Showing 1 to 1 of 1 25

Listener Name	Description	Conditional Event Type	Status	Actions
Telecom		Account Added to Folder	[Pending For Approval]	  

Showing 1 to 1 of 1 25

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Event Listener > Add Event Listener

Add Event Listener

The wizard below helps you create a listener specifying the conditions upon which it should trigger the followup action. You can also define the desired followup action in the form of a script or an API task.

Listener Name*
List1

Description

Conditional Event Type
Search event type

Trigger the Listener for the Events from

☐ All Accounts ☐ Account Types

Save **Cancel**

Help

You can trigger an action after the occurrence of any specific event or a sequence of events in Securden. For example, when the password of an account is changed, you can trigger a follow-up action automatically. The followup action could be defined in the form of a script (any Windows executable such as .bat, .exe, .ps1, .vbs etc.) or as an API task making use of third-party REST APIs.

Summary of steps:

- Specify the event type for which you want to trigger the listener (Conditional Event Type)
- Specify if you want the listener to be triggered for all accounts or accounts belonging to a specific type
- Granularly select specific accounts by creating conditional criteria (optional)
- Define the desired followup action (post listener trigger) in the form of a script or a task using third-party APIs

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

Provide a Name and description for the Listener

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Event Listener > Add Event Listener

Add Event Listener

The wizard below helps you create a listener specifying the conditions upon which it should trigger the followup action. You can also define the desired followup action in the form of a script or an API task.

Listener Name*	Description
Password Script	Run a script when a remote device password is change

Conditional Event Type

Password Reset in Remote Machine

Trigger the Listener for the Events from

☐ All Accounts
 ☐ Account Types

Save **Cancel**

Help

You can trigger an action after the occurrence of any specific event or a sequence of events in Securden. For example, when the password of an account is changed, you can trigger a follow-up action automatically. The followup action could be defined in the form of a script (any Windows executable such as .bat, .exe, .ps1, .vbs etc.) or as an API task making use of third-party REST APIs.

Summary of steps:

- Specify the event type for which you want to trigger the listener (Conditional Event Type)
- Specify if you want the listener to be triggered for all accounts or accounts belonging to a specific type
- Granularly select specific accounts by creating conditional criteria (optional)
- Define the desired followup action (post listener trigger) in the form of a script or a task using third-party APIs

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

How to pass parameters in the follow-up action script or API task?

Specify the event type to trigger the listener

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Event Listener > Add Event Listener

Conditional Event Type

Search event type

Trigger the Listener for the Events from

☒ All Accounts ☐ Account Types

Save Cancel

- Specify if you want the listener to be triggered for all accounts or accounts belonging to a specific type
- Granularly select specific accounts by creating conditional criteria (optional)
- Define the desired followup action (post listener trigger) in the form of a script or a task using third-party APIs

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

How to pass parameters in the follow-up action script or API task?

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

You may use the following placeholders

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

Specify account types for listener to be triggered

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

Click on **All Accounts** to trigger an event for all accounts.

Click on **Account Types** and select the type from the drop-down list.

Granularly select specific accounts

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

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

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

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

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

Condition:

Equals mean the **Value** specified is an exact match to the account's attribute.

Contains mean the **Value** specified is a part of the account's attribute.

Does Not Contain means the **Value** specified is not a part of the account's attribute.

To add a criterion, you can click on “+” at the RHS.

To remove a criterion, you can click on “-” at the RHS.

Define the desired follow-up action

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

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

The screenshot shows the 'Privileged Account Manager' Admin console. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin' (highlighted). The breadcrumb trail is 'Admin > Event Listener > Add Event Listener'. Below this, there are tabs for 'All Accounts' and 'Account Types'. The main content area is titled 'Granularly Select Accounts' and includes a link 'Specify Attributes for Granular Selection'. The section 'Define the Followup Action (Post Listener Trigger)' is active, showing a dropdown menu with 'Third-party REST APIs' selected. On the right, a sidebar provides additional information: 'Define the desired followup action (post listener trigger) in the form of a script or a task using third-party APIs', a 'Prerequisite' note about internet connectivity, a section on 'How to pass parameters in the follow-up action script or API task?', and a list of placeholders: Account Title, Account Name, Account ID, and Address.

Setting up follow-up actions with a script

Summary of steps:

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

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

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

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

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Event Listener > Add Event Listener

Script

If the script needs another program to invoke it from the command prompt, the same could be provided here as the 'Pre Command' below.

Examples

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

Example 1: "C:\Program Files\python\python.exe" <Uploaded python file> "%ACCOUNT_NAME%" "%OLD_PASSWORD%" "%ACCOUNT_PASSWORD%"

Example 2: <Uploaded batch file> "%ACCOUNT_NAME%" "%OLD_PASSWORD%" "%ACCOUNT_PASSWORD%"

Pre Command

Select the Script File *

Choose a file:

Parameters to be Passed

Save Cancel

You may use the following placeholders

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

You may use the following placeholders:

- Account Title
{%ACCOUNT_TITLE%}
- Account Name
{%ACCOUNT_NAME%}
- Address
{%ACCOUNT_ADDRESS%}
- Account Old Password
{%OLD_PASSWORD%}
- Account Password
{%ACCOUNT_PASSWORD%}
- Folder Name
{%FOLDER_NAME%}
- Name of the account for remotely logging in to the IT asset
{%REMOTE_LOGIN_ACCOUNT_NAME%}
- Password of the remote login account
{%REMOTE_LOGIN_ACCOUNT_PASSWORD%}

- Name of the account that has privileges to do remote operation
{%PRIVILEGED_ACCOUNT_NAME%}
- Password of the privileged account
{%PRIVILEGED_ACCOUNT_PASSWORD%}

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

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

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

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

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

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

DELETE deletes a resource at a specified URL.

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

To enter multiple Headers or Parameters use the **+** sign.

To remove a Header or Parameter use the **-** sign.

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

- API headers are like **an extra source of information for each API call you make** to represent the meta-data associated with an API request and response.
- API parameters are **the variable parts of a resource**. They determine the type of action you want to take on the resource. Each parameter has a name and value type.

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

Event listener actions

You can configure event listeners added in Securden, you can choose to Delete, Edit, or Clone an event listener.

The screenshot shows the Securden Privileged Account Manager Admin interface. The top navigation bar includes Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin (highlighted). Below the navigation bar, the breadcrumb trail is Admin > Event Listener. The main heading is Event Listener. A descriptive text box explains that users can trigger actions after specific events or sequences of events, such as password changes, and provides a wizard to define these listeners and actions. Below this, there is a table of listeners. The table has columns for Listener Name, Description, Conditional Event Type, Status, and Actions. One listener is listed: 'Telecom' with the description 'Account Added to Folder' and status '[Pending For Approval]'. The Actions column for this listener contains icons for cloning, deleting, editing, and deleting. At the bottom, there are pagination controls showing 'Showing 1 to 1 of 1' and a page number '1'.

Event Listener

You can trigger an action after the occurrence of any specific event or a sequence of events in Securden. For example, when the password of an account is changed, you can trigger a follow-up action automatically. The followup action could be defined in the form of a script or as an API task making use of third-party APIs. The wizard below helps you to define the listener and the desired follow up action.

Search, Refresh, Add Listener, Delete Listener

Showing 1 to 1 of 1 25

Listener Name	Description	Conditional Event Type	Status	Actions
Telecom	Account Added to Folder		[Pending For Approval]	Clone, Delete, Edit, Delete

Showing 1 to 1 of 1 25

Navigation: << < 1 > >>

Delete a listener - To delete listeners, select them from the list and click **Delete Listener** OR delete them individually using the **<Red icon>** in **Actions**.

View Listener - gives you a brief of the Listener name, Event type, Trigger action, and Description. To access this, click on the **view icon**.

Clone Listener - To create a listener with similar details to an existing one, use the **clone icon**. This takes you to the Add listener configuration with all the pre-filled details of the clone, change the fields as needed and click **Save**.

Edit Listener - To edit a listener, click on the **edit icon**. This lets you change any field you have entered while adding the listener.

Section 7: API Access

APIs for Programmatic Access

Identities are present everywhere and in every piece of IT. Apart from the passwords, keys, and other credentials used by humans, every organization has to deal with a lot of machine identities, credentials embedded on scripts and applications, and so on. Securden provides APIs for programmatic access of the data stored in the product. Scripts, applications, and configuration files that require credentials can access the Securden database and fetch the data, thus eliminating the dangerous practice of hard-coding of credentials. API access is regulated through a token-based authentication mechanism.

To programmatically access an account through API, you need an URL and the Auth Token. The token can be a static one or dynamic and valid for a specified time duration or forever. The access can be restricted from specific IP addresses or FQDNs. Also, tokens can be applicable only for a specific list of operations.

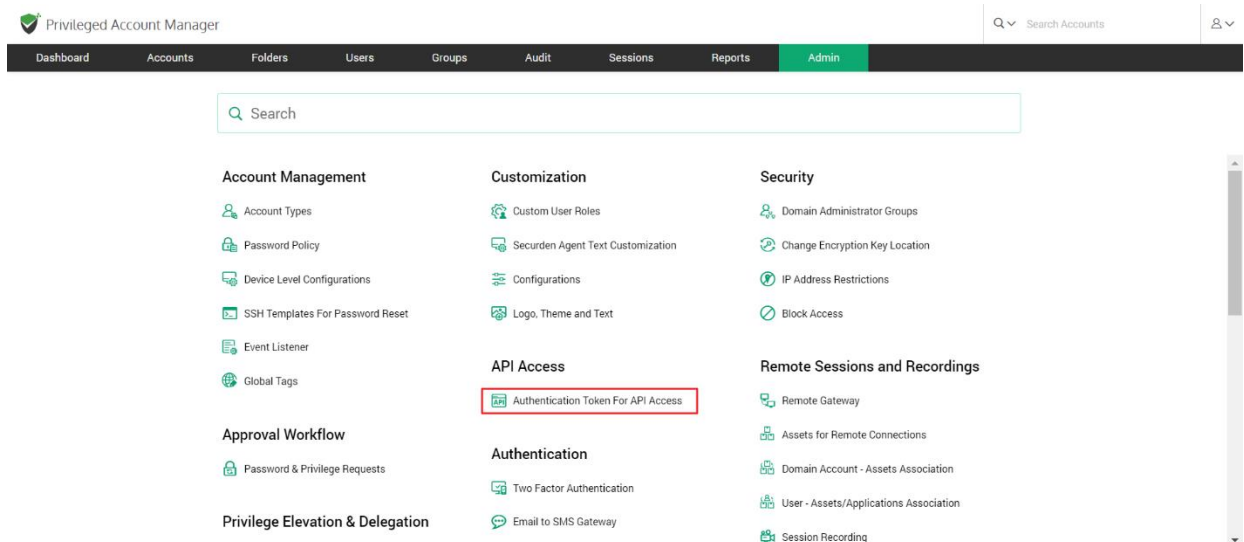
As mentioned above, you require two things for API access:

- Authentication token
- Access URL

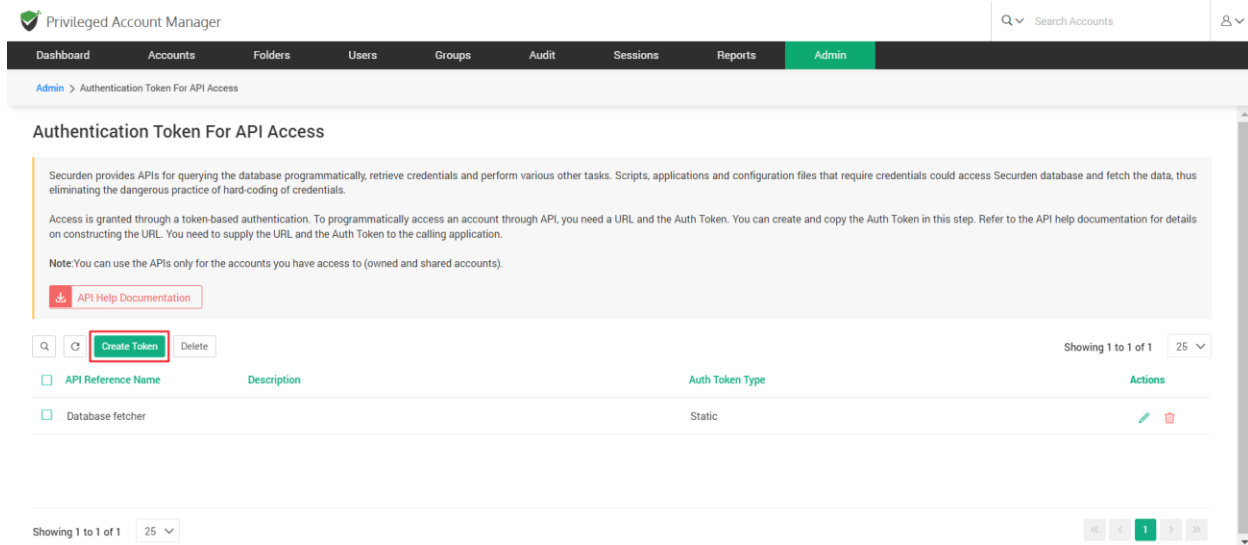
You need to create the authentication token in the GUI and then construct the URL referring to our API reference guide. You need to supply the URL and the Auth Token to the calling application.

How to create the authentication tokens for APIs?

To create tokens for APIs, **navigate to Admin >> API Access >> Authentication Token for API Access** section.



In the GUI that opens, click the button **Create Token**.



Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Authentication Token For API Access

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 Help Documentation](#)

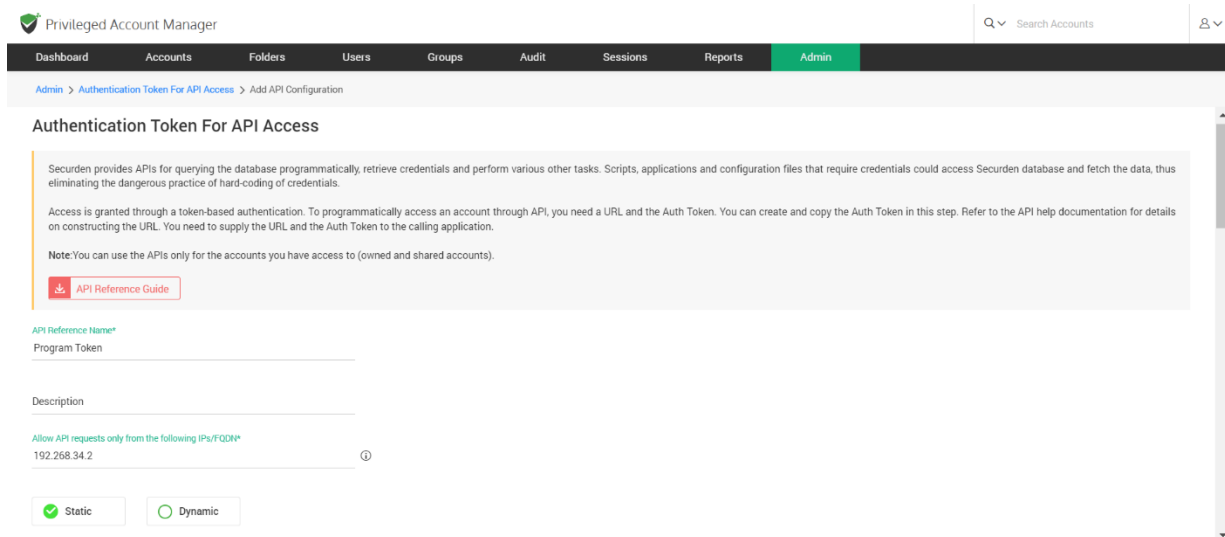
Search Create Token Delete

Showing 1 to 1 of 1 25

API Reference Name	Description	Auth Token Type	Actions
Database fetcher		Static	Edit Delete

Showing 1 to 1 of 1 25

In the GUI that opens, you need to enter the following information:



Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Authentication Token For API Access > Add API Configuration

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 Guide](#)

API Reference Name*

Program Token

Description

Allow API requests only from the following IPs/FQDN*

192.268.34.2 ⓘ

☒ Static ☐ Dynamic

Token name and description

Enter a name for the token being created. This **API Reference Name** helps you uniquely identify the token when using it in APIs. A description will help in tracking the purpose of the token.

Token access restrictions

If you want to restrict the token usage only from specific IP addresses, you may enter the same in the field "Allow API requests from the following IPs/FQDN". You can enter individual IP addresses in comma separated form or an IP range or FQDNs or CIDR notations.

Examples:

Specific IP Address: 191.224.1.22

IP Range: 224.1.1.10:224.1.2.1

CIDR Notation: 192.168.1.30/24

Token type

You can choose to create a static token or a dynamically changing one. Select your choice **Static** or **Dynamic** as required.

The screenshot displays the 'Admin' section of the Privileged Account Manager interface. The top navigation bar includes links for Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin (which is highlighted). A search bar for accounts is also present. The breadcrumb trail indicates the current path: Admin > Authentication Token For API Access > Add API Configuration.

The main content area is divided into two sections:

- Token Validity:** This section contains two radio buttons: 'Set to Never Expire' (which is currently selected) and 'Valid Up To'. Below these, a text field shows 'Auth Token is valid up to 08 Aug 2023 at 02:15 hrs'.
- Token Applicability:** This section includes a descriptive text: 'You can specify the operations for which the token generated here would be applicable. In other words, the API, with this token, cannot be used for operations other than the ones selected below.' It features a checkbox for 'Select All operations' and a list of specific operations, each with its own checkbox:
 - Password Management (checkbox selected)
 - Password Retrieval (checkbox selected)
 - Change Password (checkbox selected)
 - Remote Password Reset (checkbox selected)
 - Generate Password (checkbox selected)
 - Get Password Policy Details (checkbox selected)

Token lifetime

You can also decide about the lifetime of the token being created. Static tokens can be created with a permanent validity **Set to Never Expire** or can be created to be valid for a predefined date and time. Select the option **Valid Upto** and set the validity date. Dynamic token will have a short lifespan in minutes.

Token scope

You can define the scope of the token being created by restricting the operations for which the token generated here would be applicable. In other words, the API, with this token, cannot be used for operations other than the ones selected in scope. To define the scope, select the required operations under **Token Applicability**.

The screenshot shows the 'Privileged Account Manager' interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin' (highlighted in green). A search bar on the right says 'Search Accounts'. Below the navigation bar, the breadcrumb trail reads 'Admin > Authentication Token For API Access > Add API Configuration'.

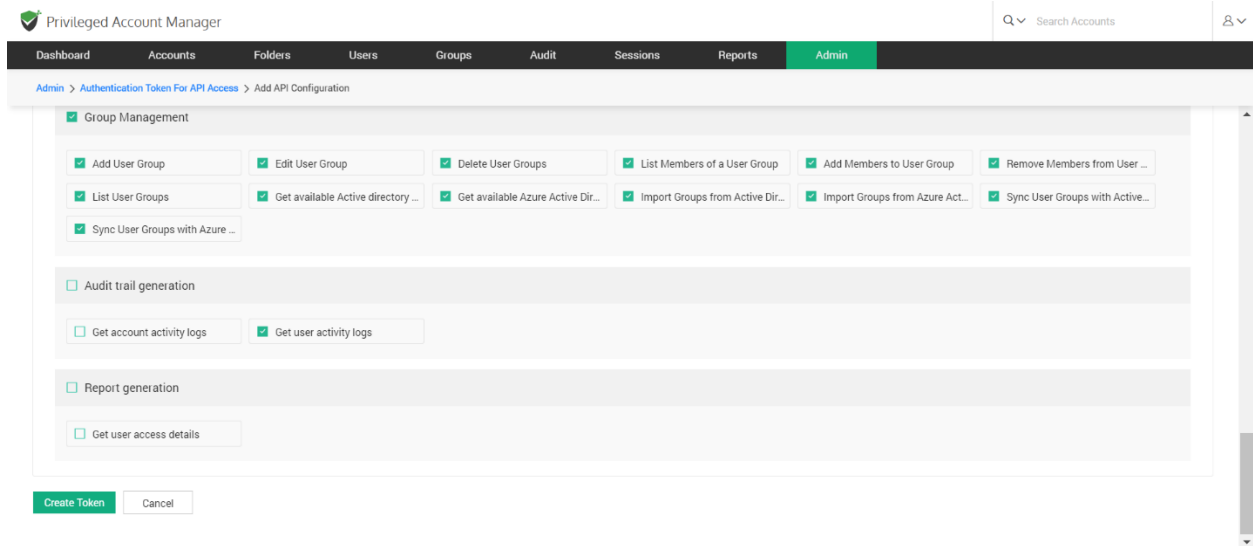
The main content area is titled 'Token Applicability'. It contains a sub-header 'You can specify the operations for which the token generated here would be applicable. In other words, the API, with this token, cannot be used for operations other than the ones selected below.'

Under 'Token Applicability', there are two main sections:

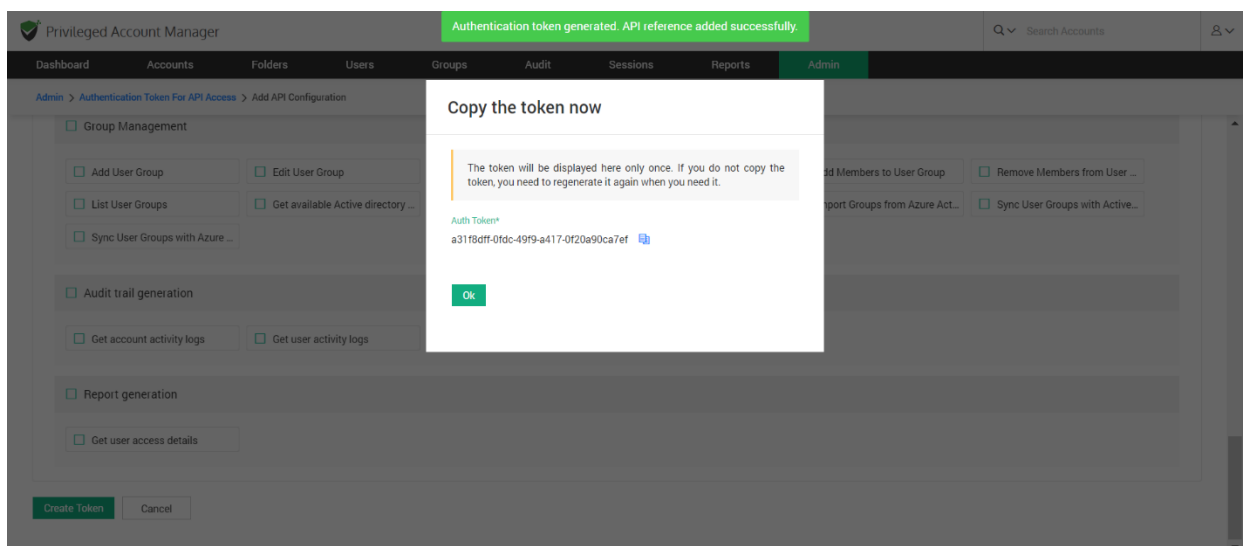
- Select All operations** (checkbox)
- Password Management** (checkbox)
 - ☒ Password Retrieval
 - ☒ All My Accounts (Owned and Shared) ☐ Specific Accounts
 - ☐ Change Password
 - ☐ Remote Password Reset
 - ☐ Generate Password
 - ☐ Get Password Policy Details
- Account Management** (checkbox)
 - ☐ Add Account
 - ☒ Edit Account
 - ☒ Delete Accounts
 - ☐ Share Account
 - ☒ Remove Share
 - ☐ View Account Share Permissi...
 - ☐ List Accounts (Owned and Sh...
 - ☐ Get Account details
 - ☐ Approval Workflow
 - ☐ File Retrieval
 - ☐ Additional File Retrieval
 - ☐ List Existing Tags (Owned, Sh...
 - ☐ Transfer Account Ownership

Create the token and copy the static token

After defining the scope, proceed to create the token.



If you have chosen the type **Static**, you will be prompted to copy the token to the clipboard. The token will be displayed only once and you can't refer to that again if you don't copy it.



Getting dynamic tokens

Dynamic auth tokens can be obtained programmatically. Typically, you will obtain it as explained below. You will have to pass the credentials to access Securden as arguments.

GET /api/get_auth_token

Input data (arguments): login_name (String), password (String), domain_name

(Default authentication will be local)

Example (if you are using Curl):

```
curl -k -X GET
```

```
"https://pamdemo.com/api/get_auth_token?login_name=admin&password=admin&domain_name=xyz"
```

Edit, Delete, Update, Regenerate Tokens

You can use the **Actions** column on the APIs page to delete the tokens that are no longer needed. Similarly, you can edit the static tokens and extend their lifetime (validity period). In such cases, you will have to update and regenerate the token.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Authentication Token For API Access

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 Help Documentation](#)

Search Create Token Delete Showing 1 to 1 of 1 25

API Reference Name	Description	Auth Token Type	Actions
Database fetcher		Static	Edit Delete

Showing 1 to 1 of 1 25

Token creation is the first step in API access. You need to construct the URL for use by applications, scripts, and configuration files.

Constructing the URL for API Access

To programmatically access an account through API, you need a URL with the Auth token. You have created the auth token through the steps detailed above. You can create the URL by following the steps detailed in the API Help Documentation present in **Admin >> API Access >> Authentication Token for APIs**. The documentation explain how the URL is to be constructed and the arguments to be passed for various operations.

Section 8: Folder Management

Organize Accounts with Folders

You can create folders and group **Accounts** for easy and efficient management. At any point of time, a specific account could be a member of only one folder. This means, an account cannot be a member of multiple folders. Grouping accounts into folders lets you perform actions like remote password resets for multiple accounts grouped in the folder at one go. You can also define a hierarchical structure with any number of folders and sub-folders.

You can add folders to Securden in two ways:

1. Add manually
2. Import from a file

Manually Adding Folders

Navigate to **Folders >> Add**. Provide the following details to create a folder.

Folder Name

You need to provide a name that uniquely identifies the folder. This name will appear on the left-hand side of the interface. The name will help you distinguish between folders while adding, deleting, and modifying accounts.

Description

You can also provide a description to further help classify the accounts for easy management.

Parent Folder

- If you want to create a stand-alone folder, leave this option as **--None--**.
- If you want to create a new subfolder to an existing folder, you should specify the existing parent folder by choosing the required folder from the drop-down list.

Inheritance of Share Permissions

- Once you select a parent folder, you will have the option to choose whether to inherit permissions from it or not. Select **Yes** if you want to inherit permissions. This means that the users and user groups having access to the parent folders will now have access to the subfolder with the same level of access permissions.
- Select **No** if you don't want the subfolder to inherit permissions granted to the parent folder.

- Choosing to inherit share permission will mean users who have shared access to the parent folder will now have access to the new folder with the same permissions (View/Modify/Manage). But, users with whom you explicitly share the new folder will only obtain access permissions to the new folder.
- You can choose to switch inheritance **On** or **Off** anytime.

Notes

- You can add notes to a folder for classification, marking ownership, and sharing user guidelines.
- You can also add any miscellaneous remarks related to the folder and its content.

Add Accounts to the Folder

You can add accounts to the folder at the time of creation. An account could remain a member of one folder at a time. This means the same account cannot be added to multiple folders at the same time. Also, note that if inheritance mode is switched on, parent folders and the new folder will have the same share permission. That means, users who have access to the accounts stored in the parent folder(s), will get access to the accounts being added in this step.

Import Folders from Files

In situations where multiple folders are to be added, you have the option to import them from a file.

Navigate to **Folders >> More >> Import Folders from Files**.

You can either import folders from a CSV file or an Excel sheet.

Privileged Account Manager

Search Accounts

Dashboard Accounts **Folders** Users Groups Audit Sessions Reports Admin

Import Folders From File

CSV

XLSX

Specify how each entry in your CSV has been separated

Delimiter

Comma Separated values

Choose a file Browse

Choose Parent Folder *

--None--

Help

A note on creating the folder data to be imported:

Securden offers the flexibility to create folders in bulk. Based on your requirements, you can have the following columns in the input file.

Folder Name, Description, Folder ID, Parent Folder ID, Inherit Parent Folder Share permission, Notes

- Of the above, 'Folder Name' alone is mandatory. Other columns are optional.
- 'Folder ID' is some unique number that you can give to identify each folder being created. This is just for reference purpose while importing. The ID will not be displayed in the GUI.
- 'Parent Folder ID' is used to make any folder entry being added as the sub-folder of another folder. You need to give the 'Folder ID' of the parent folder here. If there is no parent folder (you want to add the folder directly under the root folder), enter '0'.
- Inherit Parent Folder Share Permission - if you want to make use of inheritance, enter 'Yes'. Otherwise, enter 'No'.
- Choose Parent Folder - Your administrators have enabled

- For CSV files, you need to specify how the values have been separated. You can choose between comma-separated values and tab-separated values. This is not required in the case of Excel Sheet (XLSX) files.

Privileged Account Manager

Search Accounts

Dashboard Accounts **Folders** Users Groups Audit Sessions Reports Admin

Import Folders From File

CSV XLSX

Choose a file Browse

Choose Parent Folder *
--None--

Next Cancel

Help

A note on creating the folder data to be imported:

Securden offers the flexibility to create folders in bulk. Based on your requirements, you can have the following columns in the input file.

Folder Name, Description, Folder ID, Parent Folder ID, Inherit Parent Folder Share permission, Notes

- Of the above, 'Folder Name' alone is mandatory. Other columns are optional.
- 'Folder ID' is some unique number that you can give to identify each folder being created. This is just for reference purpose while importing. The ID will not be displayed in the GUI.
- 'Parent Folder ID' is used to make any folder entry being added as the sub-folder of another folder. You need to give the 'Folder ID' of the parent folder here. If there is no parent folder (you want to add the folder directly under the root folder), enter '0'.
- Inherit Parent Folder Share Permission - if you want to make use of inheritance, enter 'Yes'. Otherwise, enter 'No'.
- Choose Parent Folder - Your administrators have enabled

- Choose the file from your computer by clicking on **Browse**.
- If the imported folder is not a subfolder of a parent folder, leave the Parent Folder as **--None--**. If the folder is a subfolder, select the parent folder from the drop-down.

Note: If your administrators have enabled the configuration to enforce the selection of a parent folder while adding/editing a folder, you will only be able to import folders only as subfolders to folders for which you have **Manage** permission or to the folders you own.

A note on creating the folder data to be imported:

Based on your requirements, you can have the following columns in the input file.

Folder Name, Description, Folder ID, Parent Folder ID, Inherit Parent Folder Share permission, Notes

- Of the above, **Folder Name** is mandatory. Other columns are optional.

- **Folder ID** is an unique number that you can give to identify each folder being imported. This is just for reference purposes while importing. The ID will not be displayed in the GUI.
- **Parent Folder ID** is used to make any folder entry being added as the sub-folder of another folder. You need to give the **Folder ID** of the parent folder here. If there is no parent folder (you want to add the folder directly under the root folder), enter **0**.
- **Inherit Parent Folder Share Permission** - if you want to make use of inheritance, enter **Yes**. Otherwise, enter **No**.

Following are some sample entries:

IT Infrastructure, Description, 1,0, yes

Systems, Admin Team, 2, 1, yes

Windows, Tier 1 Team, 3, 2, yes

Linux, Tier 2 Team, 4, 2, no

This will create a folder structure as below:

IT Infrastructure

|

|__**Systems**

|

|__**Windows**

|

|__Linux

Enable and Disable Inheritance

You can enable and disable permission inheritance whenever you want. You can select multiple folders and configure inheritance permission by navigating to **Folders >> More >> Enable or disable Inheritance for Sub-Folders**.

The screenshot shows the Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders' (selected), 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' and a user profile icon are on the right. The left sidebar shows a tree view with 'Folders' expanded, containing 'IT Infrastr...' and 'Local Ac...'. A context menu is open over the 'Folders' section, showing options: 'Import Folders From File', 'Share Folders', 'Enable or Disable Inheritance for ...' (highlighted), and 'Delete Folders'. The main content area shows the 'Accounts' tab for the 'IT Infrastructure' folder. It displays metadata: Folder Name (IT Infrastructure), Description (-None-), Notes (-None-), Folder ID (1000000001098), and Owner (Securden Administrator). Below this is a message: '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.' At the bottom, there are buttons for 'Add Accounts', 'Move Accounts', and 'Remove Accounts', along with a pagination indicator 'Showing 1 to 4 of 4' and a table with columns 'Account Title', 'Account Name', 'Address', and 'Type'. The table contains one entry: 'Administrator' with 'Administrator' as the name, 'sec-build-1.securden.aws.com' as the address, and 'Windows Member' as the type.

You can also modify inheritance settings for a specific folder by navigating to **Folders >> Share**. This option is visible only when the selected folder is a sub-folder. This option is not valid for parent folders and stand-alone folders.

Quick Access Options

In addition to selecting a parent folder while adding a folder using manual method and when importing from files, you can also create subfolders from the quick access pane on the left side of the Folders GUI. If you hover the pointer over a folder, you will see two icons. One with the folder symbol and the other with a settings symbol.

1. The Folder icon represents **Add Sub Folder**.
2. The Settings icon has three different options. **Edit**, **Transfer Ownership**, and **Delete**.

Add Sub Folder

If you click the Folder icon, you will be redirected to the add folder page and the parent folder section will be auto-filled. You will still have to provide the other required information as mentioned in the **Manually Adding Folders** section.

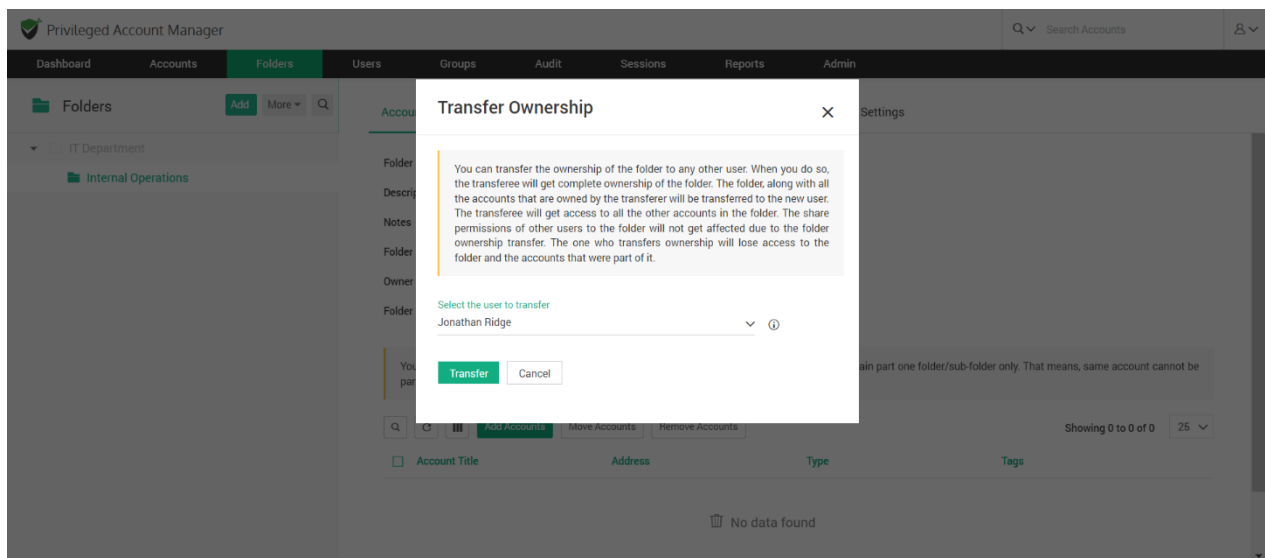
Edit

In this section, you can alter the details of a folder while retaining the accounts added to it. All the details of a folder can be altered.

If a folder having subfolders is edited, the new details will be enforced to the subfolders automatically.

Transfer Ownership

You can transfer the ownership of an entire folder to another user instead of transferring the accounts one by one. In such an event, the Transferer will lose access to the accounts in the folder and the Transferee will get complete ownership of the accounts in the folder. The share permissions of other users will not be affected due to an ownership transfer.

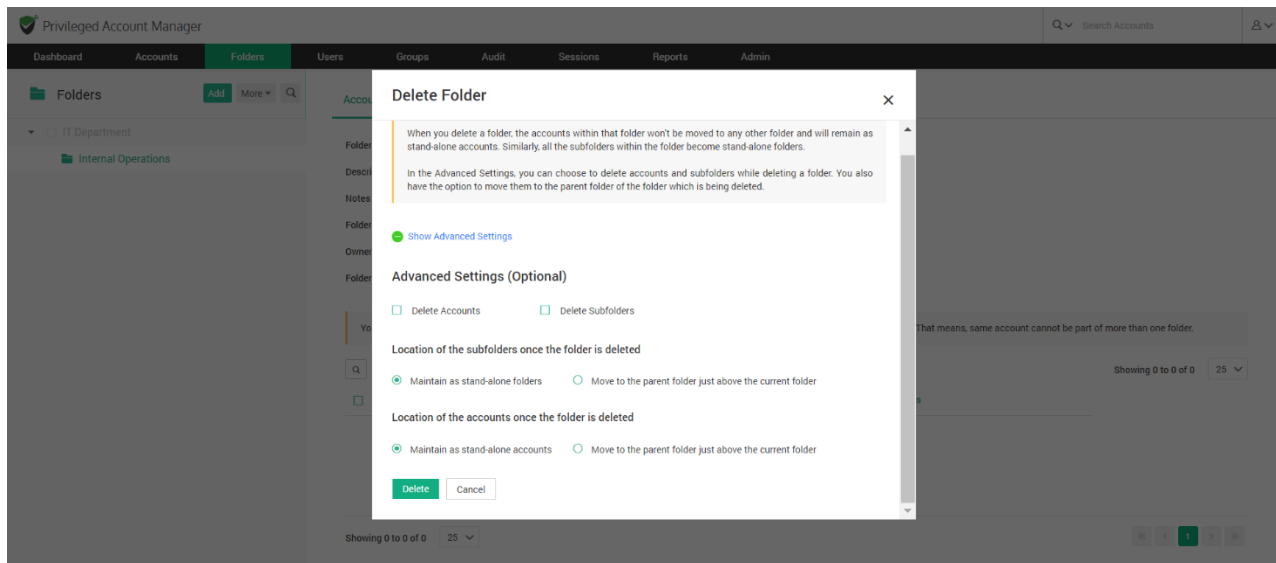


By default, Folders can only be transferred to Super Administrators, Administrators, and Account Managers. In the case of users with custom roles, the transferee should have add, edit, delete and share folder permissions.

To transfer the ownership of a folder, select the transferee from the list of users and click **Transfer**.

Delete

When you delete a folder, the accounts within that folder won't be moved to any other folder and will remain as stand-alone accounts. Similarly, all the subfolders within the folder become stand-alone folders.



In Advanced Settings, you can choose to

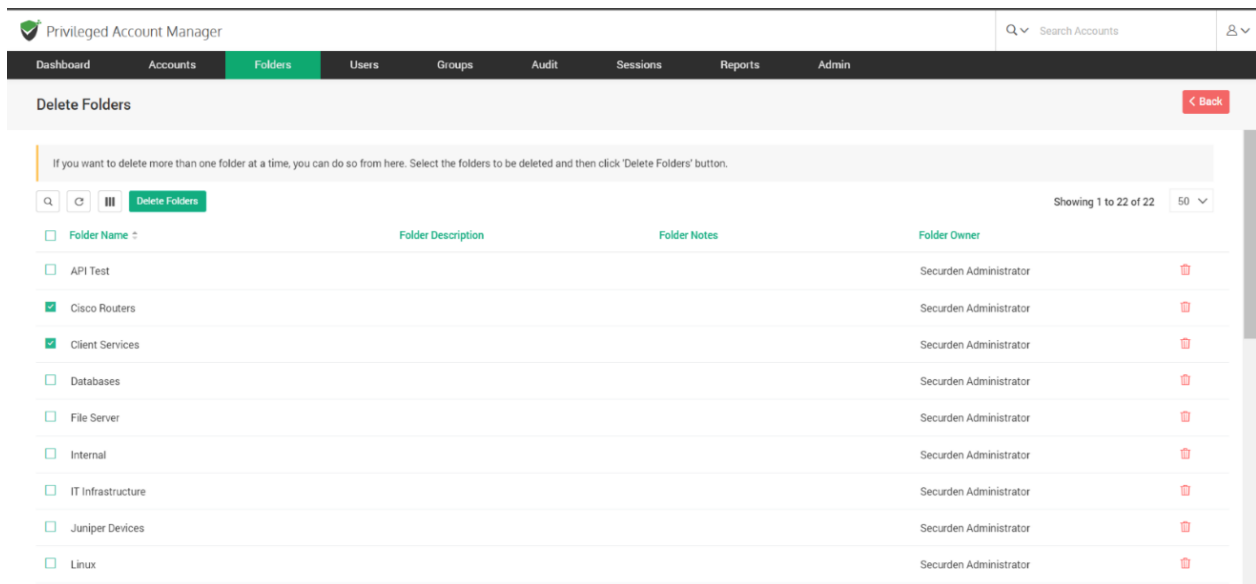
1. Delete the accounts inside the Folder.
2. Delete SubFolders and subsequently delete the accounts in SubFolders.

You can choose to maintain the folders and accounts as stand-alone or move them to the parent folder just above them in case you choose the accounts or the subfolders to not be deleted.

Deleting Multiple Folders

You can delete multiple folders at once. Navigate to **Folders >> More >> Delete Folders**.

Select the folders you want to delete and click **Delete Folders**.



Privileged Account Manager

Dashboard Accounts **Folders** Users Groups Audit Sessions Reports Admin

Delete Folders [Back](#)

If you want to delete more than one folder at a time, you can do so from here. Select the folders to be deleted and then click 'Delete Folders' button.

Showing 1 to 22 of 22 50

<input type="checkbox"/> Folder Name	Folder Description	Folder Notes	Folder Owner	
<input type="checkbox"/> API Test			Securden Administrator	
<input checked="" type="checkbox"/> Cisco Routers			Securden Administrator	
<input checked="" type="checkbox"/> Client Services			Securden Administrator	
<input type="checkbox"/> Databases			Securden Administrator	
<input type="checkbox"/> File Server			Securden Administrator	
<input type="checkbox"/> Internal			Securden Administrator	
<input type="checkbox"/> IT Infrastructure			Securden Administrator	
<input type="checkbox"/> Juniper Devices			Securden Administrator	
<input type="checkbox"/> Linux			Securden Administrator	

Manage Accounts in a Folder

You can add, search, move, and delete accounts by opening any folder for which you have **Manage** permission. An account can be a part of only one folder at any given time.

When you select a folder, the details such as the Folder Name, Description, Notes, Folder ID, and Owner (User name) will be displayed.

Below these details, the list of all accounts inside the folder will be displayed. The attributes of each account such as Account Title, Account Name, etc will

be displayed. You can change which attribute to display by clicking on the **Column Chooser** icon.

You can view the list in batches of 25, 50, and 100 accounts at a time. To set the preferred batch size click on the drop-down button on the right-hand side of the Showing x to y of y.

The screenshot shows the Privileged Account Manager (PAM) interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders' (selected), 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar 'Search Accounts' is on the right. The left sidebar shows a tree view with 'IT Infrastructure' and 'Local Administrator Accounts'. The main panel displays details for the 'IT Infrastructure' folder, including its name, description, notes, ID, and owner. Below this, a message states: '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.' At the bottom, there are buttons for 'Add Accounts', 'Move Accounts', and 'Remove Accounts', along with a search bar and a dropdown for 'Showing 1 to 4 of 4' with a batch size of 25.

Add Accounts

In addition to adding accounts at the time of folder creation, you can add accounts to a folder at any time. You can add accounts to a folder only if it is not already a part of another folder.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders' (selected), 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' and a user profile icon are on the right. On the left, a sidebar shows 'Folders' with a tree view containing 'IT Infrastructure' and 'Local Administrator Accounts'. The main area is titled 'Add Accounts to the Folder'. It displays 'Folder Name' as 'IT Infrastructure' and 'Folder Description' as 'Yet to give a description'. A note states: '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.' Below this, there is a 'Fetch Accounts Based On' dropdown menu currently set to 'Select'. A search input field below the dropdown says 'Search and select required account(s) here'. At the bottom are 'Save' and 'Cancel' buttons.

To add accounts to a folder,

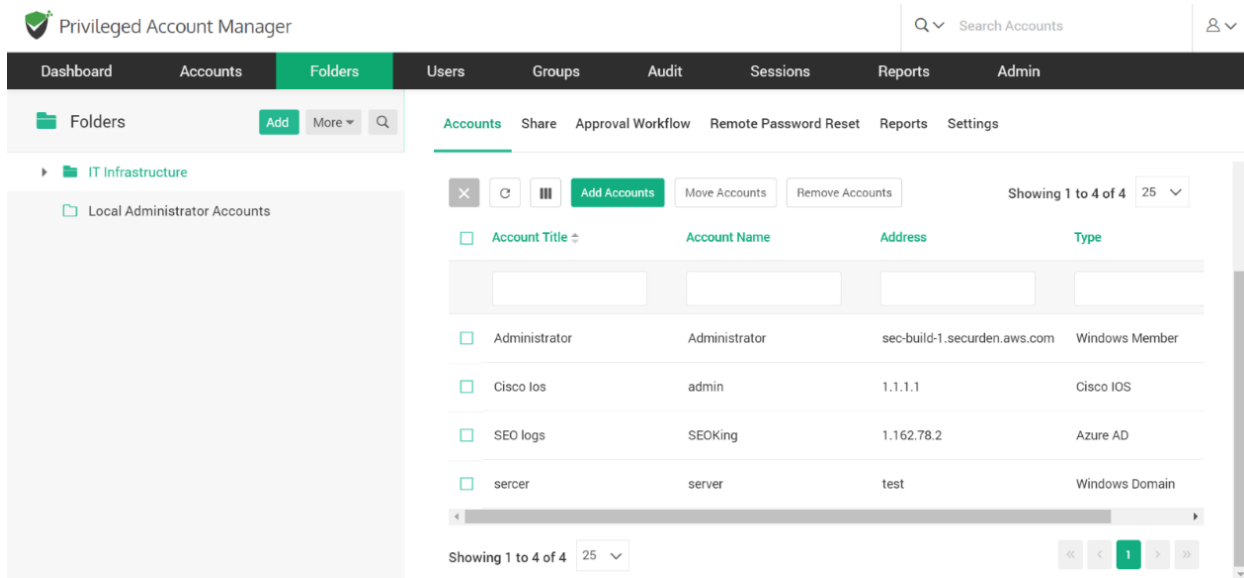
1. Click on **Add Accounts**.
2. Here you can fetch a list of accounts based on any attribute such as Account Title, Account Name, DNS/IP address, Account Type, Notes, and Tags.
3. Once you select the attribute, Securden will fetch accounts and display the list of accounts based on its attribute.

For example, if you choose DNS/IP address as the attribute, Then a list of all accounts in this DNS/IP address will be displayed for you to select the required accounts..


4. If you want to clear a selection, click on 'x' of the selected account. If you want to clear all the selected accounts, click on '**Clear all**'.
5. Once the required accounts are selected, Click '**Save**'.

Search Accounts

You can search for accounts based on different attributes. This feature comes in handy when there are numerous accounts inside a folder.



To search for accounts,

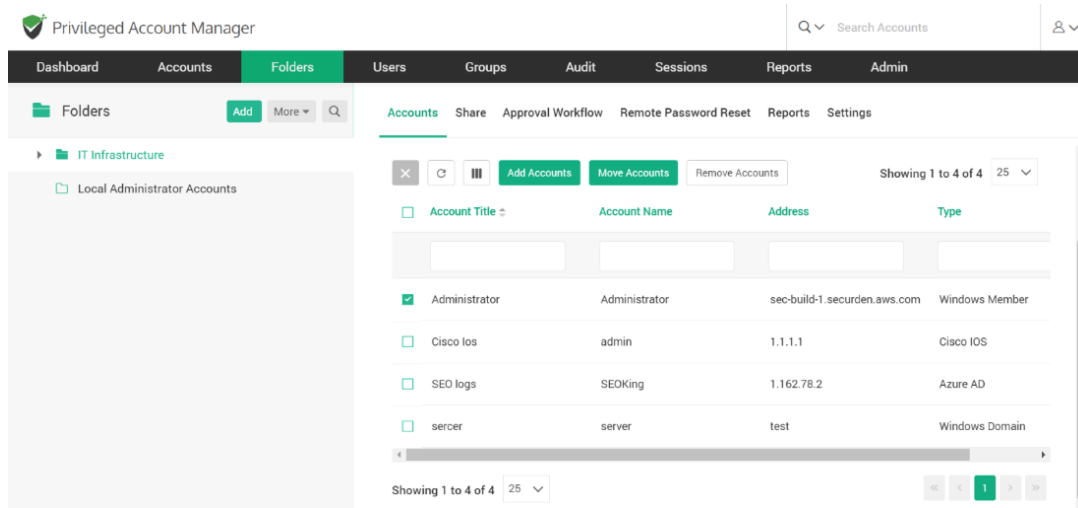
1. Click on the **Magnifying glass**  icon present in Folders >> Accounts.
2. Give the input attribute(s) to search for.
3. From the list, you can select the accounts you want. If you want to select all accounts from the search result, click on the checkbox beside **Account Title**.

Move Accounts

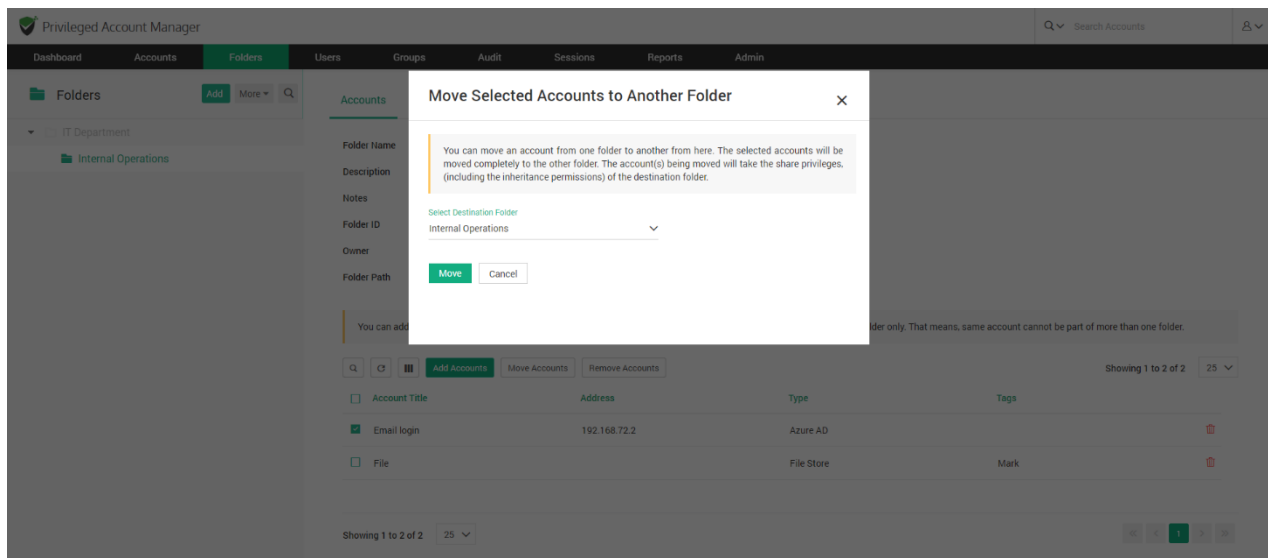
You can move accounts from one folder to another, however an account can only be a part of one folder at a time. The accounts being moved will have the same share permissions and the inheritance preferences of the destination folder.

To move accounts from one folder to another,

1. Open the folder in which the accounts are currently present.
2. Select the accounts you want to move.

3. Click on **Move Accounts**.

4. In the GUI that pops up, select the destination folder.

5. Click **Move**.

Remove Accounts

You can remove the accounts from a folder and make them stand-alone accounts.

To remove accounts from a folder,

1. Open the required folder.
2. Select the accounts you want to remove.
3. Click on **Remove Accounts**
4. In the confirmation window, Click **OK**

The screenshot displays the Privileged Account Manager (PAM) interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders' (highlighted), 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar for 'Search Accounts' is on the right. Below the navigation bar, the 'Folders' section shows a tree view with 'IT Infrastructure' and 'Local Administrator Accounts'. The main content area is titled 'Accounts' and features a table with columns: 'Account Title', 'Account Name', 'Address', and 'Type'. The table lists four accounts: 'Administrator' (checked), 'Cisco Ios', 'SEO logs', and 'server'. Above the table are buttons for 'Add Accounts', 'Move Accounts', and 'Remove Accounts'. The 'Remove Accounts' button is highlighted. The table also includes a 'Showing 1 to 4 of 4' indicator and a '25' dropdown menu.

Account Title	Account Name	Address	Type
<input checked="" type="checkbox"/> Administrator	Administrator	sec-build-1.securden.aws.com	Windows Member
<input type="checkbox"/> Cisco Ios	admin	1.1.1.1	Cisco IOS
<input type="checkbox"/> SEO logs	SEOKing	1.162.78.2	Azure AD
<input type="checkbox"/> server	server	test	Windows Domain

Share Folders

You can share multiple accounts at the same time by sharing a folder with Users and Groups. In addition to sharing accounts, you are also sharing the folder with well-defined privileges.

There are different folder management privileges and account management privileges in Securden. When you want to share a folder, you can select what privileges you want to grant to the users/groups with whom you want to share the folder.

Note: When viewing the share settings of a sub-folder, the share permission settings will be displayed. You can turn inheritance of permissions On and Off as required from here.

Folder Management Privileges

- 'View Folder Details' privilege allows the users/groups to simply view the folder properties. They are not allowed to modify anything.
- 'Add Accounts to Folder' privilege allows the users/groups to view the folder properties as well as add accounts to the folder.
- 'Manage Folder' privilege grants all permissions - view, modify properties, share the folder with others and add accounts.

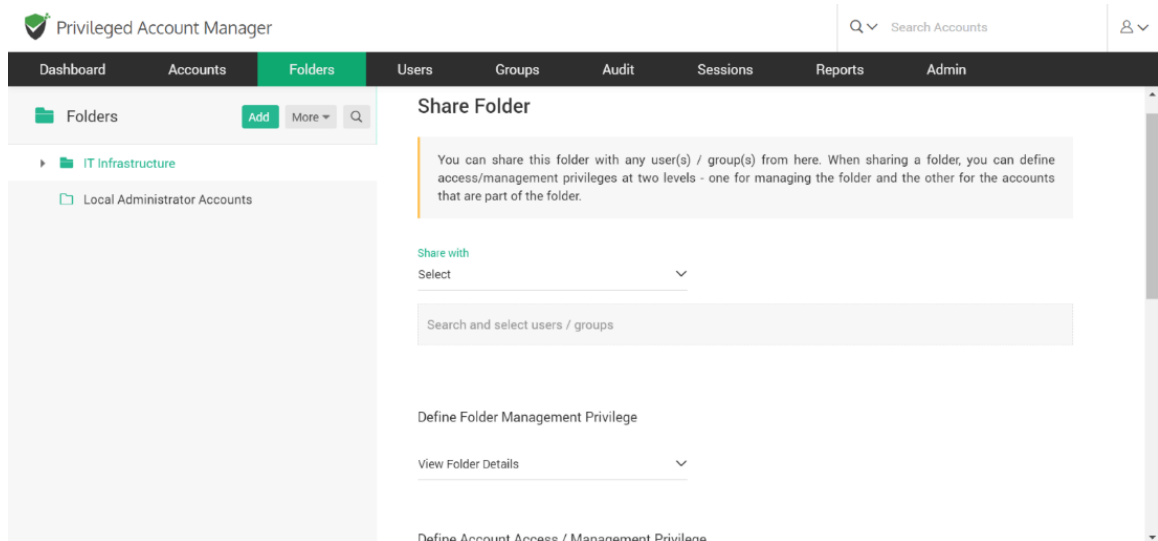
Account Access / Management Privileges

- 'Open Connection' allows launching RDP, SSH sessions with target machines, and auto-filling credentials for web applications without showing the underlying password in plain text in the GUI.

- **View** allows the user to view the details as well as the password.
- **Modify** allows editing the password.
- **Manage** grants all privileges including subsequent share permissions.

To **Share** a Folder,

1. Navigate to **Folders >> <Folder Name> >> Share >> Share Folder.**
2. Select Users or Groups by clicking on the drop-down named **Share with.**
3. You can select the users/groups with whom you want to share by traversing the list from '**Search and Select Users/Groups**'. You can add multiple users and groups at the same time.
4. To remove a user/group from the selected list click on the **x**. If you want to clear all the selected users/groups, click on **Clear All**.



5. Define the folder management privileges and the account management privileges according to the definitions from above.
6. Click **Save**.

Share Multiple Folders

1. Navigate to **Folders >> More >> Share Folders**.
2. Select the folders you want to share.

The screenshot shows the 'Share Multiple Folders' page in the Securden Privileged Account Manager. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders' (highlighted), 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar and a user profile icon are on the right. Below the navigation bar, the page title 'Share Multiple Folders' is displayed with a 'Back' button. A message states: 'You can share more than one folder with users or groups. Just select the required folders to be shared and click the button 'Share Folders'.' Below this, there is a table with columns: 'Folder Name', 'Folder Description', 'Folder Notes', and 'Folder Owner'. The table lists six folders: 'API Test', 'Cisco Routers', 'Client Services', 'Databases', and 'File Server', all owned by 'Securden Administrator'. A 'Share Folders' button is visible in the top left of the table area. A pagination control shows 'Showing 1 to 22 of 22' and a dropdown for '100'.

Folder Name	Folder Description	Folder Notes	Folder Owner
<input type="checkbox"/> API Test			Securden Administrator
<input type="checkbox"/> Cisco Routers			Securden Administrator
<input type="checkbox"/> Client Services			Securden Administrator
<input type="checkbox"/> Databases			Securden Administrator
<input type="checkbox"/> File Server			Securden Administrator

3. You can choose to not disturb existing shares and append the new share permissions wherever applicable. Doing so will imply that the share

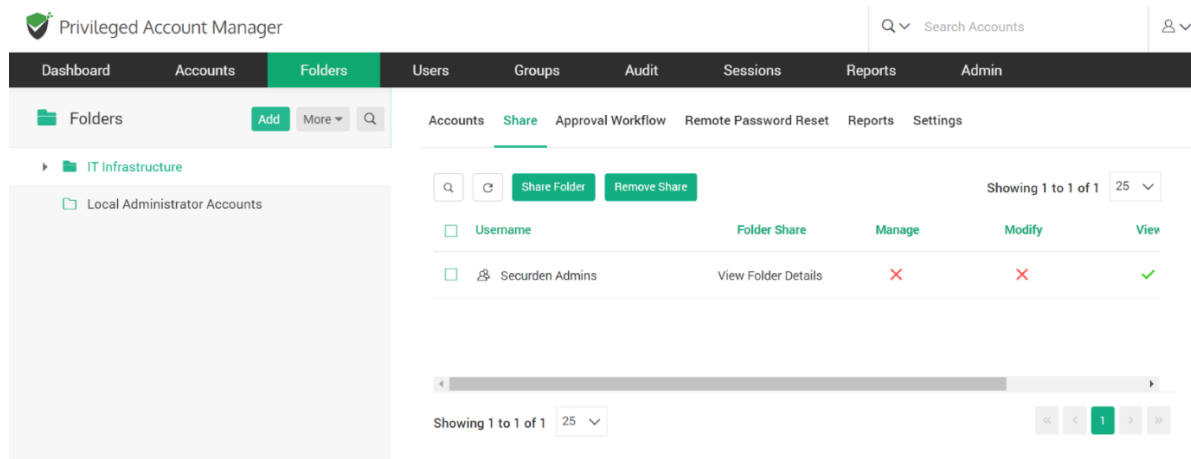
permissions can only be elevated. If a lower level of permission is selected, it will not take effect.

4. Define the folder and account management privileges by selecting the appropriate options. *To learn more about the different levels of permissions, refer to the sections above.*

Remove Share for a Folder

To **Remove** a Share, Navigate to **Folders >> Share**.

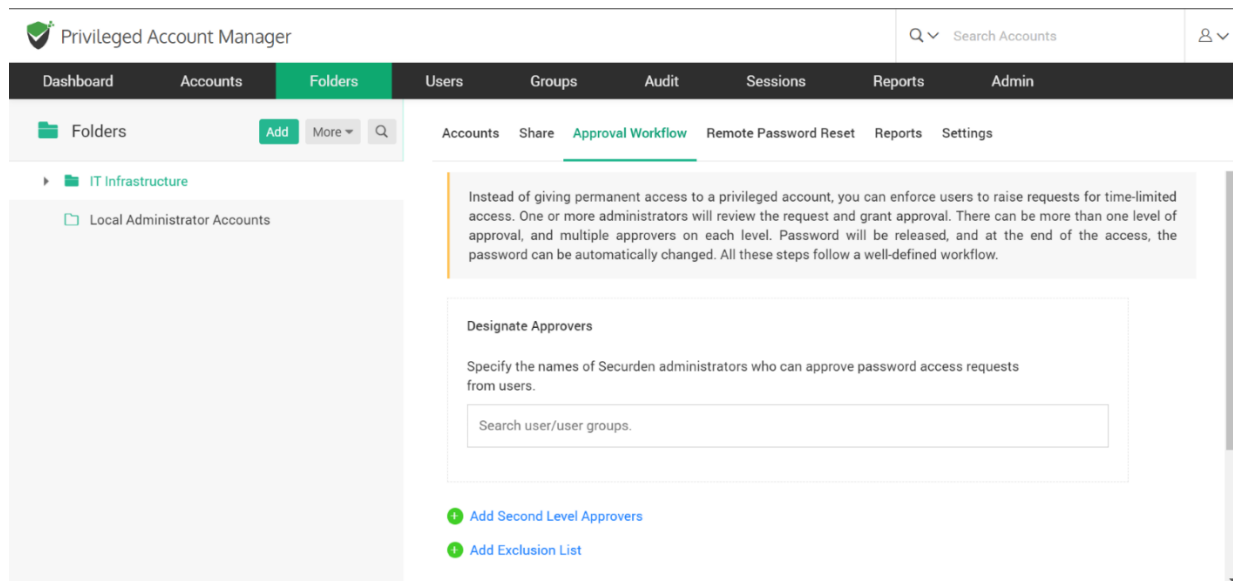
1. Select the user by clicking on the check box.
2. Click **Remove Share**.
3. Click OK on the confirmation dialog box.



Configure Approval Workflow for Folders

Instead of granting standing access to users, you can enforce just-in-time access at the folder level by using the approval workflow in Securden.

When users need access, they can place requests. One or more administrators will review before approving the request. There can be more than one level of approval with multiple approvers in each level. Upon approval, the password will be released. When the access ends, the password will be auto changed.



To **Designate Approvers**,

1. Navigate to **Folders >> Approval Workflow >> Designate Approvers**.
2. You can search for a specific user or a user group. You can select multiple users and user groups as approvers at the same time.
3. To remove a certain User or a User Group from the selection, click on x. To clear all selections, click **Clear All**.
4. To designate second level of approvers, click on **Add Second Level Approvers**. Follow steps 2 and 3 to designate the second-level approvers.

The request will reach the second-level approvers only after it is approved by the first-level approvers.

To designate subsequent levels of approvers, follow the same steps as above.

Exclusion List

You can grant direct access to passwords for any users or groups without going through the approval process, by adding them to the exclusion list.

To create an exclusion list,

1. Click on **Add Exclusion List**.
2. Search for the users/user groups and select the ones to be added to the list.
3. To remove a certain user or a user group from the selection, click on x.
To clear all selections, click **Clear All**.

To automatically renew the passwords after the access is terminated, click on the checkbox named **Change Password After Use**.

In a situation where the approver(s) might not be available to approve requests, you can configure automatic approval of requests.

1. Click the checkbox named **Configure Automatic Approval**.
2. You can choose between approving requests throughout the day or between certain hours.

Click **Save**.

To Remove/Edit a designated approver after configuring approval workflow, you can click 'Edit' from **Folders >> Approval Workflow**.

To reset the configurations, you can click **Disable** from the same GUI.

Configure Automated, Periodic Remote Password Resets

You can configure to reset the passwords of accounts contained in the folder by navigating to **Folders >> <Folder Name> >> Remote Password Reset**. There are two options to choose from when you schedule a password reset for a folder.

1. **Reset Once**
2. **Reset Periodically**

You can reset once on a specific date and time or you can configure a periodic reset to be taken in intervals as low as an hour.

If you choose '**Reset Once**', follow the steps to schedule a backup

1. Specify the date of reset from the calendar by clicking on the date format text.
2. Specify the time of reset in the format [hh mm].
3. Specify how often to retry password reset.
4. Specify the maximum number of resets to be attempted.

If you choose **Reset Periodically**, follow the steps to schedule backups

1. Specify the date of the first reset from the calendar by clicking on the date format text.

2. Specify the time of the first reset in the format [hh mm].
3. Specify the periodicity of password reset. You can configure a periodicity as low as an hour.
4. Specify the maximum number of resets to be attempted.

You can select options shown to notify the folder owner and the users with shared manage access. You can also include recipients to notify by specifying their email addresses in comma separated form.

To disable an already existing schedule, click on **Disable**. Click **Save**.

Troubleshooting Tips

- 1) **Issue:** Issue with Domain Admin accounts. The user has put them in a folder and has been using remote password reset functionality, but when it runs it shows the following error.

Error: Possible reasons: (1) Invalid credentials. (2) Remote connection privileges for this account could have been disabled on the remote computer.

Password on both side (Securden and AD) is the same and the user uses a domain admin account for remote.

Solution:

One possible reason could be that WMI connectivity might not be available. We use WMI protocol for password resets and verifications. By default, WMI

remains disabled for all local users except for the built-in administrator accounts.

You may follow the steps below to enable WMI access on a specific Windows machine:

<https://www.securden.com/documents/WMI-Access-for-All-Users.pdf>

In case you wish to enable WMI on multiple machines, you may refer to the link below:

<https://www.securden.com/documents/WMI-Access-For-All-Users-GPO.pdf>

2) **Issue:**

I am trying to let local admin accounts from a PC, and I get an error "The username/password does not exist (or) the user does not have the remote launch or remote."

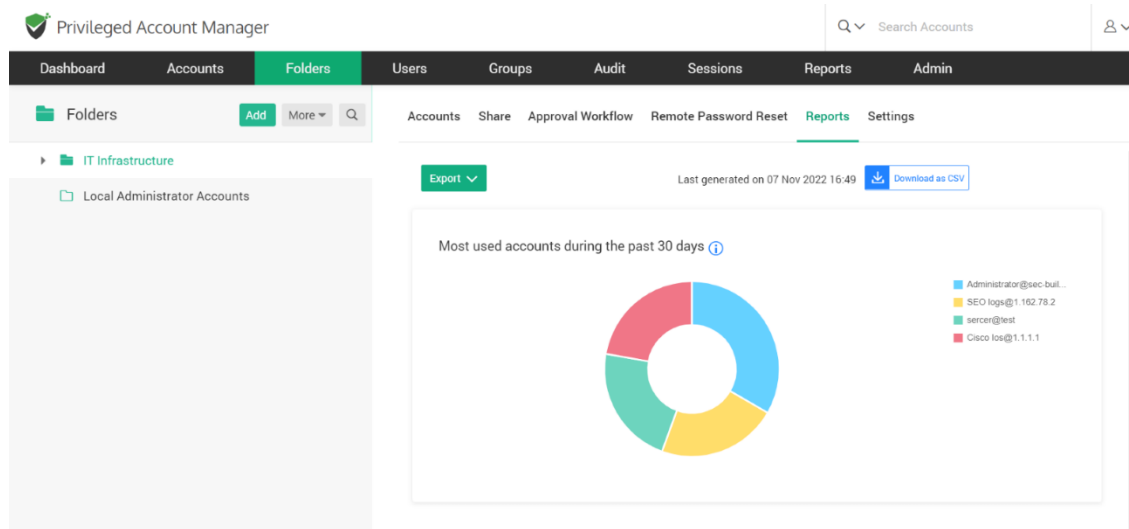
Solution: It might be an account permission issue. Try to re-run the discovery by providing a domain admin credential.

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

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

Folder Reports

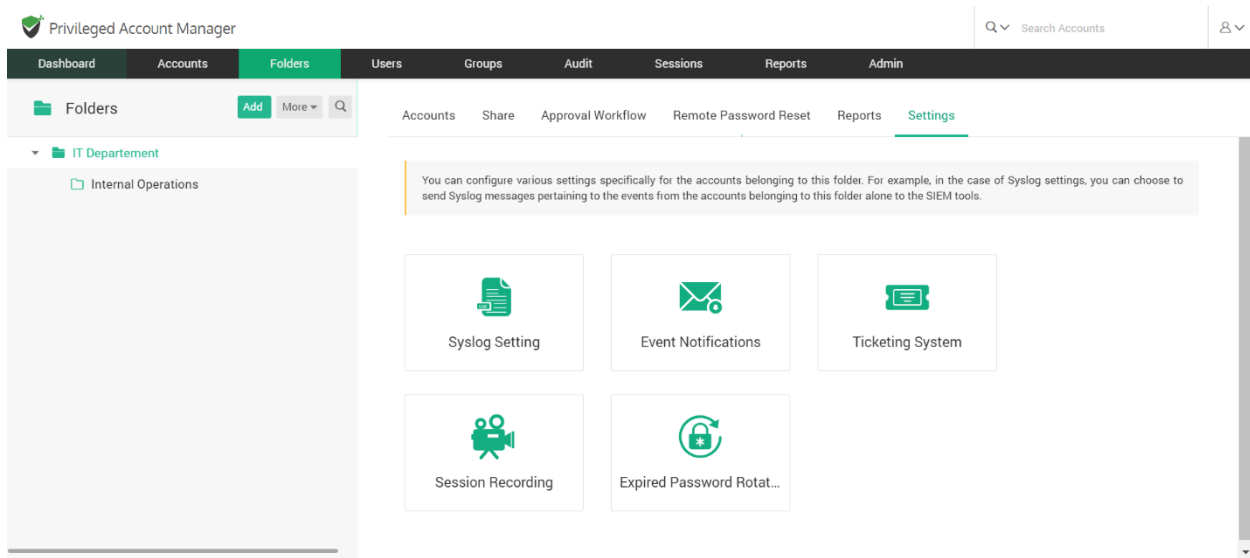
You can generate and view various actionable reports with the data specific to the selected folder.



You can view the most used accounts, most active users, accounts and activity trails of the selected folder.

Folder Settings

Certain settings such as session recording, syslog settings, etc., can be configured for accounts at a folder level in addition to being configured at an account level. For example, in the case of Syslog settings, you can choose to send Syslog messages pertaining to the events from the accounts belonging to this folder alone to the SIEM tools.



Syslog Settings

You can configure Syslog preferences for Folders. Navigate to **Folders >> Select a Folder >> Settings >> Syslog Settings**.

Pre-requisite: You need to configure the Syslog settings from **Admin >> Syslog for SIEM** to be able to access this folder level setting.

You can select the account related activities for which you want to maintain a Syslog.

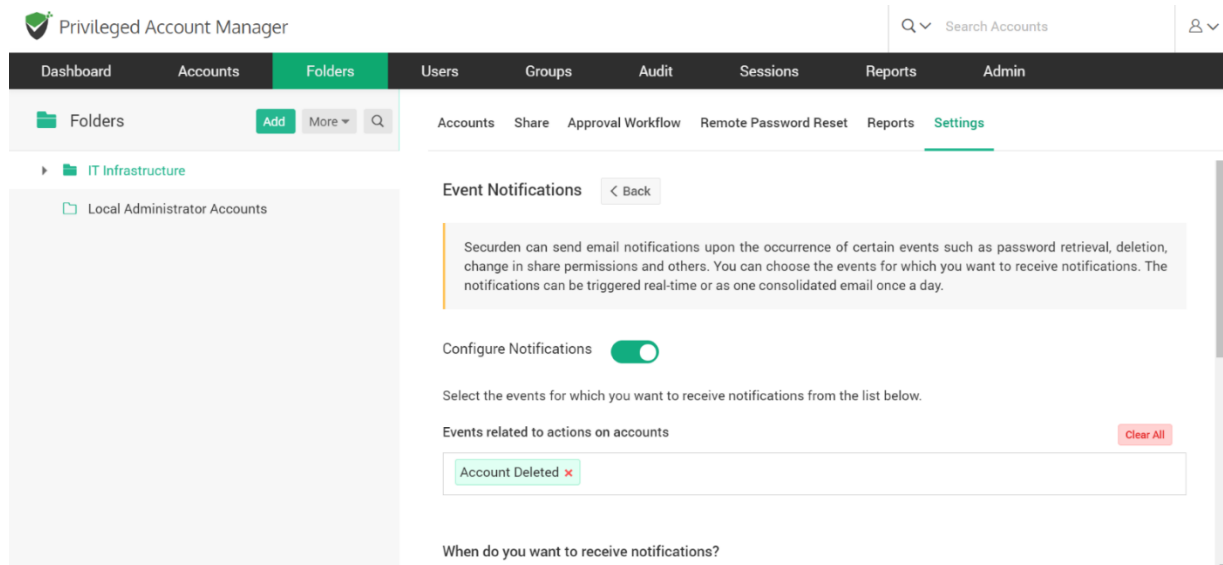
The folder-specific settings will get the preference over the global settings that were configured in **Admin >> Syslog for SIEM**.

Event Notification at a Folder level

When certain events occur, such as password recovery at the folder level, deletion, or changes in sharing permissions, Securden can send email notifications. You have the option of selecting which events you want to be notified about. The notifications can be sent out in real-time or as a consolidated email once a day.

Configuring Event Notifications

To start setting your preferences in receiving notifications, you need to toggle the Configure Notifications button. You will see a field named **Events related to actions on accounts**.



To add events, click on **Select Events** under **Events related to actions on accounts** and select the events you want to get notified about from the list.

The selected events will be shown in a green box and can be deselected by clicking on the **x** present adjacent to the event. To clear all selected events, click on the **Clear All** button.

When to Notify?

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

Who to Notify?

You can choose who receives notification emails by selecting the options in the checklist present under **Send Notifications to**. If you select **All**

Administrators, users with **Administrator** or **Super Administrator** designation will be notified.

If you select **All Auditors**, the users with auditor role designated to them will be notified.

You can also configure to notify specific users or a group of users by selecting **Select Users/Groups**.

You can send notifications to people who are not registered users in Securden by specifying their email address in the box named **Others (specify email address)**. When more than one email address needs to be notified, separate the emails with a comma(,).

Click **Save**.

Ticketing System integration at a Folder level

To use the ticketing system for a folder and its accounts, you need to configure the ticketing system from **Admin >> Ticketing System**.

Once the ticketing system has been configured, you can toggle this feature **On** for specific accounts and folders. Navigate to **Folders >> Settings >> Ticketing System** to toggle this feature **On** or **Off**.

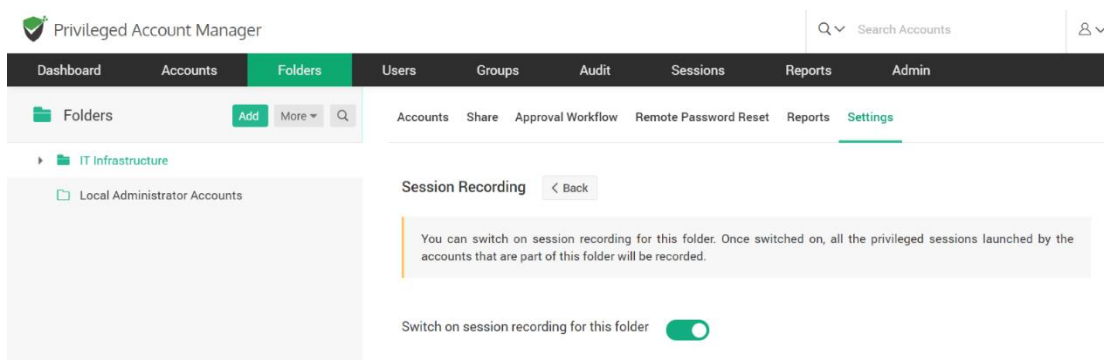
Exclusion List

You can exclude specific users or groups, with whom the folder is shared, from going through the ticket validation by including them in the exclusion list.

Session Recording at the Folder level

You can switch ON the session recording feature at the folder level. Doing this records a video copy of remote sessions launched from all accounts that are a part of the folder.

Note: Switching this feature ON is a second step of configuring session recording in Securden. You need to configure preferences in **Admin >> Remote Sessions and Recordings >> Session Recording** before you can turn this feature ON for the folder of your choice.

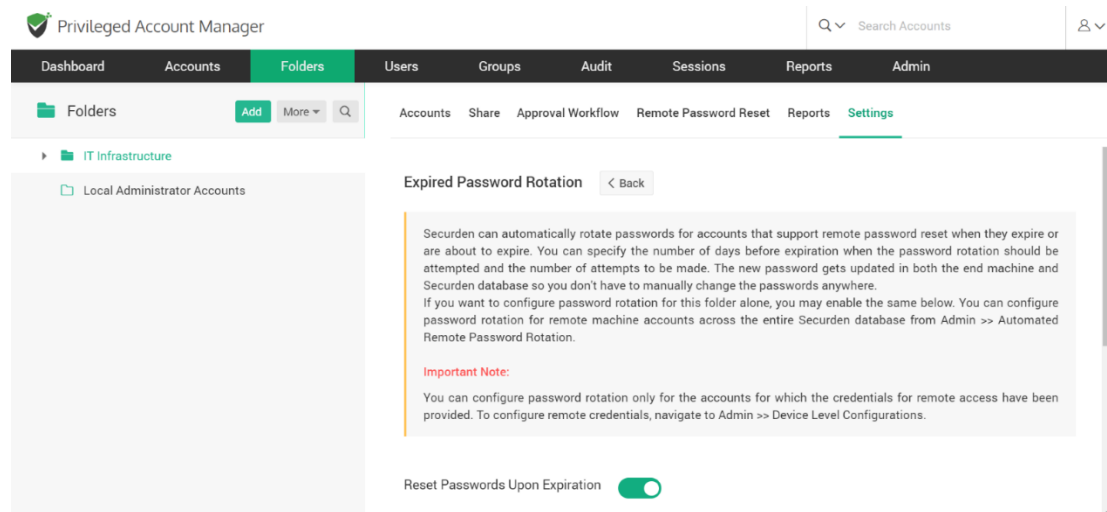


Expired Password Rotation

When passwords expire or are about to expire, Securden can automatically rotate them for you without manual intervention. You can indicate the number of days until the password expires after which password rotation will be tried, as well as the number of attempts.

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

If you only want to configure password rotation for the accounts contained within a folder, you may do it from **Folders >> Settings >> Expired Password Rotation**.



You can set password rotation for remote machine accounts across the entire Securden database by navigating to **Admin >> Automated Remote Password Rotation**.

Important Note: You can configure password rotation only for the accounts for which the credentials for remote access have been provided. To configure remote credentials, navigate to **Admin >> Device Level Configurations**.

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

If you choose **On Expiration Date**

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

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin. The left sidebar shows a tree view with Folders, IT Department, and Internal Operations. The main content area is titled 'Remote Password Reset' and contains an 'Important Note' about configuring password rotation. Below the note, there are several configuration options: 'Reset Passwords Upon Expiration' (checked), 'Reset Passwords' (radio buttons for 'On Expiration Date' and 'Prior to Expiration'), 'Retry password reset every' (3 Hours), 'Number of retries' (1), and a checkbox for 'Reset the already expired passwords'. At the bottom, there are 'Save' and 'Cancel' buttons.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Folders Add More

IT Department

Internal Operations

Accounts Share Approval Workflow Remote Password Reset Reports Settings

accounts across the entire Securden database from Admin >> Automated Remote Password Rotation.

Important Note:
You can configure password rotation only for the accounts for which the credentials for remote access have been provided. To configure remote credentials, navigate to Admin >> Device Level Configurations.

Reset Passwords Upon Expiration ☒

Reset Passwords: ☒ On Expiration Date ☐ Prior to Expiration

Retry password reset every 3 Hours

Number of retries 1

☐ Reset the already expired passwords

Save Cancel

If you choose **Prior to Expiration**,

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

The screenshot shows the 'Settings' page for 'Reset Passwords Upon Expiration' in the Privileged Account Manager. The interface includes a top navigation bar with 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin'. A search bar and user profile icon are on the right. The left sidebar shows a tree view with 'IT Department' and 'Internal Operations'. The main content area has tabs for 'Accounts', 'Share', 'Approval Workflow', 'Remote Password Reset', 'Reports', and 'Settings'. The 'Settings' tab is active, showing the 'Reset Passwords Upon Expiration' toggle switch turned on. Below this, there are radio buttons for 'On Expiration Date' and 'Prior to Expiration', with 'Prior to Expiration' selected. A text field shows '3 days prior to the date of expiration.' Below that, a dropdown menu for 'Retry password reset every' is set to '5 Hours'. Another dropdown for 'Number of retries' is set to '2'. There are two checkboxes: 'Reset the already expired passwords' (unchecked) and 'Consider only the passwords that are about to expire.' (checked). At the bottom are 'Save' and 'Cancel' buttons.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Folders Add More

IT Department

Internal Operations

Accounts Share Approval Workflow Remote Password Reset Reports Settings

Reset Passwords Upon Expiration ☒

Reset Passwords: ☐ On Expiration Date ☒ Prior to Expiration

Reset passwords 3 days prior to the date of expiration.

Retry password reset every 5 Hours

Number of retries 2

☐ Reset the already expired passwords

☒ Consider only the passwords that are about to expire.

Save Cancel

Precedence of user-level privilege

When a user is part of a group, and if an account is shared with different levels of privileges with that group, and as well as the individual user, the privilege granted on the user-level will take precedence over the privilege granted on a group-level.

For example, let us say there is an account, user, and group named *Account1*, *UserA*, and *Group1* respectively.

Consider,

- UserA is a member of Group1
- Account1 is shared with 'Open Connection' permission individually to UserA
- Account1 is shared with **Modify** permission to Group1

Then, the UserA will only have **Open Connection** access to Account1, and not **Modify** access.

Precedence of least privilege

When an account/folder is shared with many groups with different privileges, and if same user is a member of all those groups, the user can access the account/folder only with the 'least level of privilege' given amongst the groups.

For example, let us say there is an account, folder, user, and groups named *Account1*, *Folder1*, *UserA*, *Group1*, and *Group2* respectively.

Consider,

- UserA is a member of both Group1 and Group2.
- Account1 is shared with 'Manage' permission to Group1 and 'Modify' permission to Group2.

Now, the UserA will only have 'Modify' access over Account1, and not 'Manage' permission.

Precedence of account-level access over the folder-level

If a folder and an account has been shared with different levels of privileges to a user, and even if the same account is present within that folder, the user will still have account-level access over that folder and will not be able to access it with folder-level permission.

For example, let us say there is an account, folder, user, and groups named Account1, Folder1, UserA, Group1, and Group2 respectively.

Consider,

- Account1 is a part of Folder1.
- UserA is a part of both Group1 and Group2.
- Group1 has 'Manage' (folder-level) permission over Folder1, and Group2 has 'View' (account-level) permission over Account1, which is inside Folder1.

Now, the UserA will only have account-level **View** access to Account1 and will not be able to access the account with folder-level **Manage** access.

Section 9: Audits

Securden captures all activities in the form of audit trails. You can view and search the trails to find 'who' did 'what' and 'when'. In addition, you can also gain security insights with various analytical reports. activities capture the activities on the accounts. User activities capture the activities of the Users. To view the audit trails, navigate to the '**Audit**' tab in the GUI. The trails are classified into three categories:

- Account activities
- User activities
- Session activities

Account activities:

Account activities include all the activities related to the accounts that occur in Securden like changes in passwords account addition, deletion, modification and, so on. Activities across all accounts are recorded and can be tracked. It displays the dates and times that an account or file is handled, as well as the names of users who have retrieved, modified, or added it.

Navigate to **Audit>> Account Activities** to view account logs.

The screenshot shows the Securden Privileged Account Manager interface. The top navigation bar includes Dashboard, Accounts, Folders, Users, Groups, Audit (selected), Sessions, Reports, and Admin. The Audit tab is active, displaying 'Account Activities' (highlighted with a red box), 'User Activities', and 'Session Trails'. A message states: 'All activities performed in general are captured here as audit trails.' Below this, there are buttons for 'Export' and 'Schedule Export'. The table shows audit records with columns: Account Title, Account Address, Activity Type, Performed By, Performed From, Performed At, and Reason. The records show various folder modifications and account sharing actions performed by the Securden Administrator.

Account Title	Account Address	Activity Type	Performed By	Performed From	Performed At	Reason
IT Department (Folder)	N/A	Folder modified	Securden Administrator	W10PF2YAS0P	26 Jul 2023 00:05	Modified : Name
Internal Operations (Folder)	N/A	Folder added	Securden Administrator	W10PF2YAS0P	26 Jul 2023 00:00	
IT Departement (Folder)	N/A	Folder modified	Securden Administrator	W10PF2YAS0P	26 Jul 2023 00:00	Modified : Name
Server3	173.134.23.4	Account shared with user	Securden Administrator	W10PF2YAS0P	25 Jul 2023 12:11	Shared to Terry Cruise. Shar...
Server3	173.134.23.4	Account shared with user	Securden Administrator	W10PF2YAS0P	25 Jul 2023 12:10	Shared to Frankel Lampard...
Server3	173.134.23.4	Account shared with user	Securden Administrator	W10PF2YAS0P	25 Jul 2023 12:09	Shared to Jonathan Ridge ...
Server3	173.134.23.4	Account password changed lo...	Securden Administrator	W10PF2YAS0P	24 Jul 2023 23:32	

Filtering data from audit records:

You can acquire a concise report by filtering and viewing only the records that satisfy your criteria. To filter, click on the **Search** tab. You can search through the audit filter with the following labels:

Parameter	Description
Performed by	The user who performed the operation.
Performed from	The name of the device where the operation was done.
Performed at	The time at which the operation took place.
Activity type	The type of action performed by the user.

Username	The name of the user who triggered the action.
Reason	The reason behind the particular activity is noted and displayed.
Account Title	The name of the account on which the user performed the activity.
Account address	The IP address of the device on which the account activity was performed.

For instance, If deletion of password occurs in a particular account and you want to see them, you can view them in the account activities and with the help of the available filters you can view the exact data you require.

Column chooser:

You have the option to select which columns are displayed under account activity audits. Click the column chooser icon – shown below.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups **Audit** Sessions Reports Admin

Account Activities User Activities Session Trails

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

Search Filter Export Schedule Export Showing 1 to 7 of 7 25

Account Title	Account Address	Activity Type	Performed By	Performed From	Performed At	Reason
Cisco	192.168.72.2	Account added	Securden Administrator	W10PF2YAS0P	11 Apr 2023 18:43	
Skype	N/A	Application Launcher added	Securden Administrator	W10PF2YAS0P	11 Apr 2023 18:43	
Zoom	N/A	Application Launcher added	Securden Administrator	W10PF2YAS0P	11 Apr 2023 18:42	
N/A	N/A	User Asset Associations for launching ...	Securden Administrator	W10PF2YAS0P	11 Apr 2023 18:42	User
Custom Gateway (Remote Gateway)	N/A	Remote Gateway Modified	Securden Administrator	W10PF2YAS0P	11 Apr 2023 18:42	
N/A	N/A	User Asset Associations for launching ...	Securden Administrator	W10PF2YAS0P	11 Apr 2023 18:40	User
N/A	N/A	Asset for launching remote connection...	Securden Administrator	W10PF2YAS0P	11 Apr 2023 18:40	Sequel

Showing 1 to 7 of 7 25

The search columns can display different label columns according to the requirements of the user. At a time, any six columns can be selected for display from the following nine categories – **Account Title, Account Name, Account Address, Activity Type, Performed By, Performed From, Performed At, Performed Over, Reason.**

The screenshot shows the 'Privileged Account Manager' interface. The 'Audit' tab is selected, displaying a table of account activities. A 'Column Chooser' sidebar is open on the right, allowing users to select which columns to display in the table. The table has columns for Account Title, Account Address, Activity Type, Performed By, Performed From, and Performed At. The activities listed include Cisco, Skype, Zoom, and various gateway and asset associations, all performed by the Securden Administrator on April 11, 2023.

Account Title	Account Address	Activity Type	Performed By	Performed From	Performed At
Cisco	192.168.72.2	Account added	Securden Administrator	W10PF2YASGP	11 Apr 2023 18:43
Skype	N/A	Application Launcher added	Securden Administrator	W10PF2YASGP	11 Apr 2023 18:43
Zoom	N/A	Application Launcher added	Securden Administrator	W10PF2YASGP	11 Apr 2023 18:42
N/A	N/A	User Asset Associations for launching ...	Securden Administrator	W10PF2YASGP	11 Apr 2023 18:42
Custom Gateway (Remote Gateway)	N/A	Remote Gateway Modified	Securden Administrator	W10PF2YASGP	11 Apr 2023 18:42
N/A	N/A	User Asset Associations for launching ...	Securden Administrator	W10PF2YASGP	11 Apr 2023 18:40
N/A	N/A	Asset for launching remote connection...	Securden Administrator	W10PF2YASGP	11 Apr 2023 18:40

Showing 1 to 7 of 7

For instance, if you want to have a report solely consisting of activity type and who it was performed by, you can select those columns and download the report. An example screenshot is attached below:

This screenshot shows the same 'Privileged Account Manager' interface, but with a custom report view. The 'Export' button has been clicked, and a dropdown menu is visible, showing options for PDF, CSV, and XLSX. The table now displays only two columns: 'Activity Type' and 'Performed By'. The activities listed are the same as in the previous screenshot, but only the 'Performed By' column is visible, showing 'Securden Administrator' for all entries.

Activity Type	Performed By
Account added	Securden Administrator
Application Launcher added	Securden Administrator
Application Launcher added	Securden Administrator
User Asset Associations for launching remote connections modified	Securden Administrator
Remote Gateway Modified	Securden Administrator
User Asset Associations for launching remote connections added	Securden Administrator
Asset for launching remote connections added	Securden Administrator

Showing 1 to 7 of 7

Exporting the filtered data:

After the screening process of audit trails and securing the required audit, it can be exported for various investigation purposes. Navigate to the '**Export**' tab and select the required format.

There are three formats available and they are:

- PDF
- CSV
- XLSX

Click on the **Download as** to get the report to your system. The date and time at which the report was generated is also displayed.

Schedule Export of Account and User activities:

The exporting of audit data can be scheduled on a periodic basis or at once, in a time frame by selecting the required report format. To download the report, the link will be sent to the specified recipients. Navigate to the **Schedule Export** tab.

Firstly, the report format must be selected among the three options which are **PDF, CSV, XLSX**. Then the interval must be specified by choosing **Export Once** or **Export Periodically** according to the needs of the user.

Note: The execution time you set will follow the current time indicated in the server in which Securden runs and the current timing along with the date is displayed.

The date and the timing of the export must be specified in the formats of DD/MM/YYYY and in the 24 hour format HH:MM respectively. The same can be notified to different levels of users:

- Administrators
- Super Administrators
- Auditors
- Select users/groups

After selecting the recipients, click **Save**.

Privileged Account Manager

Contact Technical Support Get Quote

Search Accounts

Dashboard Accounts Folders Users Groups **Audit** Sessions Reports Admin

Periodically Export [Account Activities](#) > [Activities on Accounts Report](#) > Periodically Export [Back](#)

Select Report Format

☒ PDF ☐ CSV ☐ XLSX

Specify the Interval

☐ Export Once ☒ Export Periodically

Note: The current time on the server in which Securden runs is 10 Apr 2023 16:06 hrs. The execution time you set here will follow the server time.

Export periodically starting from DD/MM/YYYY at HH MM hrs

Export every Days

Notify

☐ Administrators

☐ Super Administrators

☐ Auditors

☐ Select users/groups

Save

The only difference when you export periodically is that you need to specify the periodicity in terms of **Days, Months and Hours**.

The screenshot shows the 'Periodically Export' configuration page in the Securden Privileged Account Manager. The page has a top navigation bar with 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit' (highlighted), 'Sessions', 'Reports', and 'Admin'. Below the navigation bar, there are links for 'Account Activities', 'Activities on Accounts Report', and 'Periodically Export'. A red '< Back' button is in the top right corner. The main content area is titled 'Periodically Export' and contains two sections: 'Select Report Format' and 'Specify the Interval'. In 'Select Report Format', there are three buttons: 'PDF' (selected with a green checkmark), 'CSV', and 'XLSX'. In 'Specify the Interval', there are two buttons: 'Export Once' and 'Export Periodically' (selected with a green checkmark). Below these buttons, a note states: 'Note: The current time on the server in which Securden runs is 10 Apr 2023 16:10 hrs. The execution time you set here will follow the server time.' The 'Export periodically starting from' section has dropdowns for 'DD/MM/YYYY', 'at HH', 'MM', and 'hrs'. The 'Export every' section has a dropdown for 'Days' and a text input field.

For instance, If you want to avail the audit report in a CSV form you can easily export and download them. Also if you want them to be exported everyday at 10.00 AM, you can customize and schedule the time and get them exported in any format you expect.

Notify

Navigate to the **Schedule Export** tab and under that you can find the set of users, to whom the link will be sent to download certain reports. When we want to track specific audit events, then upon their occurrence we can notify the required users.

Privileged Account Manager

Dashboard Accounts Folders Users Groups **Audit** Sessions Reports Admin

Periodically Export < Back

Account Activities > Activities on Accounts Report > Periodically Export

Note: The current time on the server in which Securden runs is 26 Jul 2023 08:24 hrs. The execution time you set here will follow the server time.

Export on DD/MM/YYYY at HH MM hrs

Notify

☒ Administrators

☐ Super Administrators

☐ Auditors

☐ Select users/groups

Others (specify email address)

Save

User activities

All the activities performed by the users in Securden are recorded as audit trails under User activities. The number of users in any organization varies from time-to-time. Some users may leave the organization but the activities they performed before leaving will get captured here and can be utilized if any information is needed.

For instance, If a user is leaving your organization, it is high-time the passwords accessed by him might be exposed. So, to avoid any such circumstances, Securden allows you to view the activities performed by a particular user and change them. To help ease that process, you can have a variety of filters and search icon.

Navigate to **Audit >> User Activities**.

Privileged Account Manager

Q Search Accounts

8

DashboardAccountsFoldersUsersGroupsAuditSessionsReportsAdmin

Account ActivitiesUser ActivitiesSession Trails

All activities performed by the users in Securden are captured here as audit trails.

Q

🔍

📄

Export

Schedule Export

Showing 1 to 25 of 443

25

Performed By	Performed From	Performed At	Activity Type	Username	Reason
System (Schedule)	localhost	26 Jul 2023 01:01	Schedule task execution ended	N/A	Database Backup
System (Schedule)	localhost	26 Jul 2023 01:01	Database backup completed	N/A	Database Backup
System (Schedule)	localhost	26 Jul 2023 01:00	Database backup initiated	N/A	Database Backup
System (Schedule)	localhost	26 Jul 2023 01:00	Scheduled task execution started	N/A	Database Backup
Securden Administrator	W10PF2YAS0P	25 Jul 2023 12:11	User added	Terry Cruise	
Securden Administrator	W10PF2YAS0P	25 Jul 2023 11:57	Session recording enabled	N/A	
Securden Administrator	W10PF2YAS0P	25 Jul 2023 11:57	Session recording disabled	N/A	
System (Schedule)	localhost	25 Jul 2023 09:07	Schedule task execution ended	N/A	Database Backup

Click on the **Search** icon. Among the plethora of activities performed by each of the users, the search option helps to filtrate and acquire the relevant trails. To facilitate the search process, six different parameters are available.

Parameter	Description
Performed by	The role of the user who performed the operation.
Performed from	The name of the device where the operation was done.
Performed at	The time at which the operation took place.
Activity type	The type of action performed by the user.

Username	The name of the user who triggered the action.
Reason	The reason behind the particular activity is noted and displayed.

Session Trails:

All activities performed in a Securden browser session are captured here as audit trails. A session here means the window of activity between login and logout. Every detailed activity from the beginning of the session to the ending is captured.

For instance, If you are an IT admin in your company and you want to know the reason for a particular password issue requested by your employee, you can easily reach out to session activities and view the session from the start to the end and find out the reason.

To get audits from session activities, navigate to **Audit >> User Activities**.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups **Audit** Sessions Reports Admin

Account Activities User Activities **Session Trails**

All activities performed in a Securden browser session are captured here as audit trails. A session here means the window of activity between login and logout.

Session Filter: All Sessions (Filter) Search Session: Search Specific Session (Search Session)

Showing 1 to 25 of 365 25

Activity Type	Performed At	Account Title	Account Address	Username	Reason
Securden Administrator - W10PF2YAS0P (24 Jul 2023 23:00 - Live session) (12 Activities)					
Folder modified	26 Jul 2023 00:05	IT Department (Folder)	N/A		Modified : Name
Folder added	26 Jul 2023 00:00	Internal Operations (Folder)	N/A		
Folder modified	26 Jul 2023 00:00	IT Departement (Folder)	N/A		Modified : Name
Account shared with user	25 Jul 2023 12:11	Server3	173.134.23.4		Shared to Terry Cruise. Shared with '...
User added	25 Jul 2023 12:11			Terry Cruise	

Filters in Session activities:

You have a couple of filters like **Session filter** and **search session** with which you can dil down the report and acquire the exact data you want. In **Session Filter**, you have

- All sessions
- Live sessions
- Concluded sessions

To filter out and search the exact audit data you require, click on the search icon. To facilitate the search process, six different parameters are available as seen above in the account and user activities.

Export and scheduled export:

You can also avail the export and schedule export option like the other audit tabs as explained above.

Event notification:

Securden can send email notifications upon the occurrence of certain events such as password retrieval, deletion, change in share permissions and others. You can choose the events for which you want to receive notifications. The notifications can be triggered real-time or as one consolidated email once a day. This is further explained in the admin section.

For instance, if you need to know all the addition and deletion activities performed by all users and accounts in your organization, you can choose to receive notifications for that particular event. You can also customize the time of receiving notifications like if you want them at the time of occurrence or consolidated notification once in a day.

Section 10: 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 and specify which type of sessions are to be recorded (RDP, SSH, SQL, Telnet, etc.) 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.

Prerequisite: Before proceeding with session recording configuration, you should have optionally configured **remote gateways** for Windows and 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.

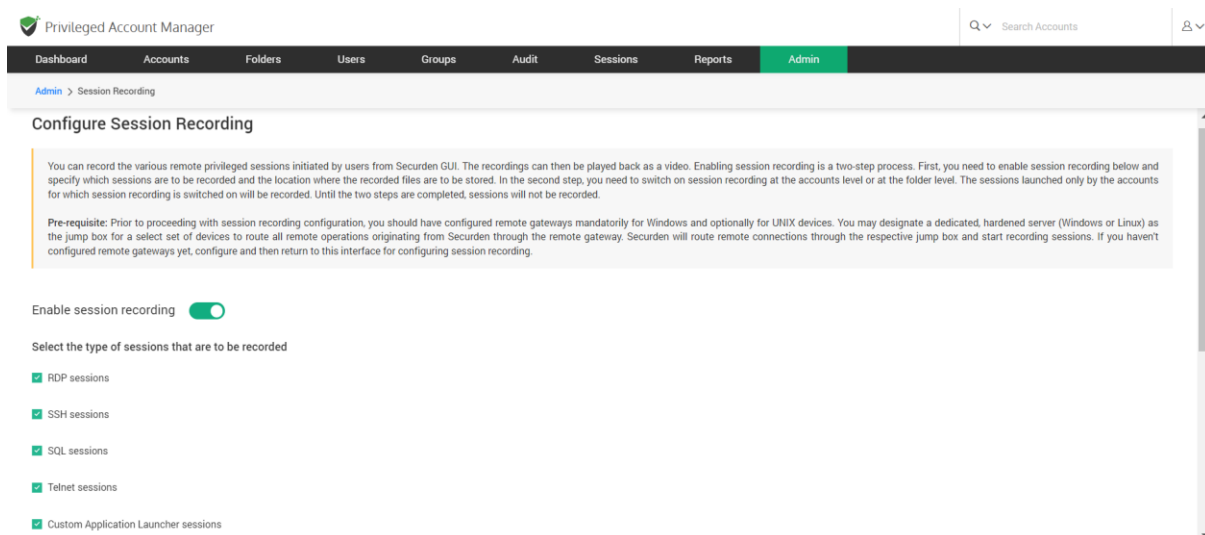
Steps to configure session recording

An overview of steps to configure session recording is to first enable the session recording and then specify the type of sessions to be recorded. Secondly, pick the location where they will be stored. To record sessions on remote computers, deploy the advanced recorder for windows.

Step 1: Enable session recording

To enable session recording, navigate to **Admin >> Remote sessions and recordings >> Session recording configuration** to perform this step.

Toggle the session recording slider as depicted in the below screenshot.

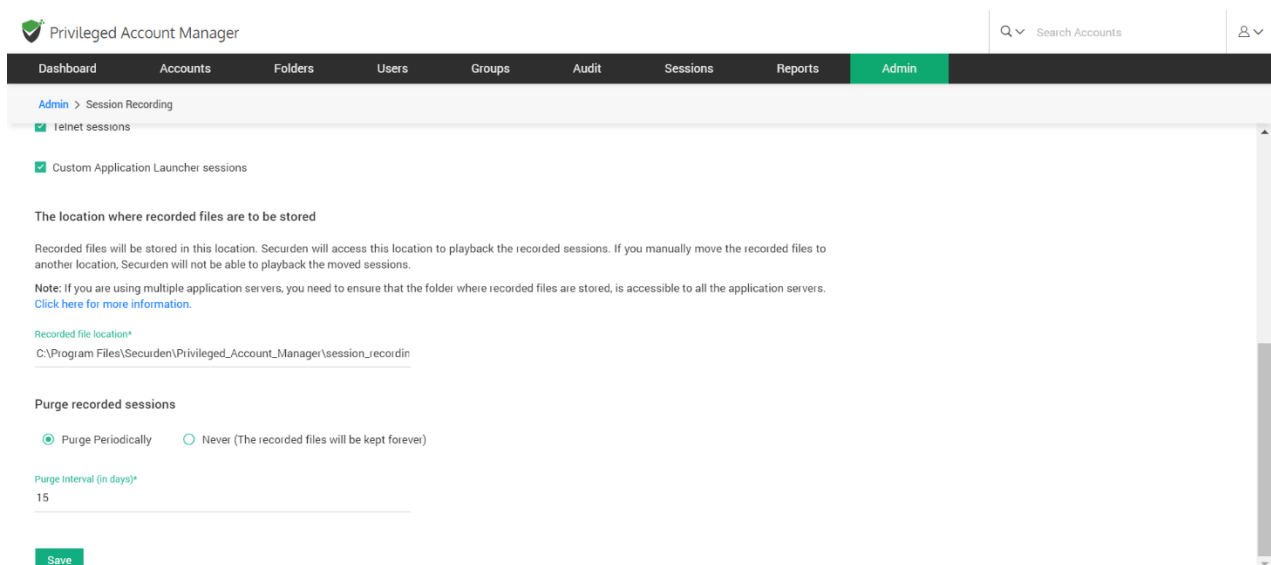


Step 2: Specify the type of Session to be recorded

You can choose to record specific types of sessions alone. You can select any of the required sessions from the list displayed on the interface - RDP, SSH, SQL, and Telnet sessions.

Note: Only the type of sessions selected here will be recorded, provided session recording is enabled for the respective account.

Step 3: Select the location where the recordings should be stored



The screenshot shows the 'Admin' tab in the Privileged Account Manager interface. The breadcrumb trail is 'Admin > Session Recording'. Under the 'Session Recording' section, there are two checkboxes: 'Telnet sessions' (checked) and 'Custom Application Launcher sessions' (checked). Below these, a section titled 'The location where recorded files are to be stored' contains explanatory text and a note about multiple application servers. A text input field labeled 'Recorded file location*' contains the path 'C:\Program Files\Securden\Privileged_Account_Manager\session_recordin'. Below this, the 'Purge recorded sessions' section has two radio buttons: 'Purge Periodically' (selected) and 'Never (The recorded files will be kept forever)'. A 'Purge interval (in days)*' input field contains the value '15'. A green 'Save' button is at the bottom left.

You can browse and choose a location on your device, network, or shared drive, on your cloud storage service. Recorded files will be stored in this location. Securden will access this location to playback the recorded sessions.

Note: If you are using multiple application servers, you need to ensure that the folder where recorded files are stored, is accessible to all the application servers.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Session Recording

☒ Telnet sessions

☒ Custom Application Launcher sessions

The location where recorded files are to be stored

Recorded files will be stored in this location. Securden will access this location to playback the recorded sessions. If you manually move the recorded files to another location, Securden will not be able to playback the moved sessions.

Note: If you are using multiple application servers, you need to ensure that the folder where recorded files are stored, is accessible to all the application servers. [Click here for more information.](#)

Recorded file location*

C:\Program Files\Securden\Privileged_Account_Manager\session_recordin

Purge recorded sessions

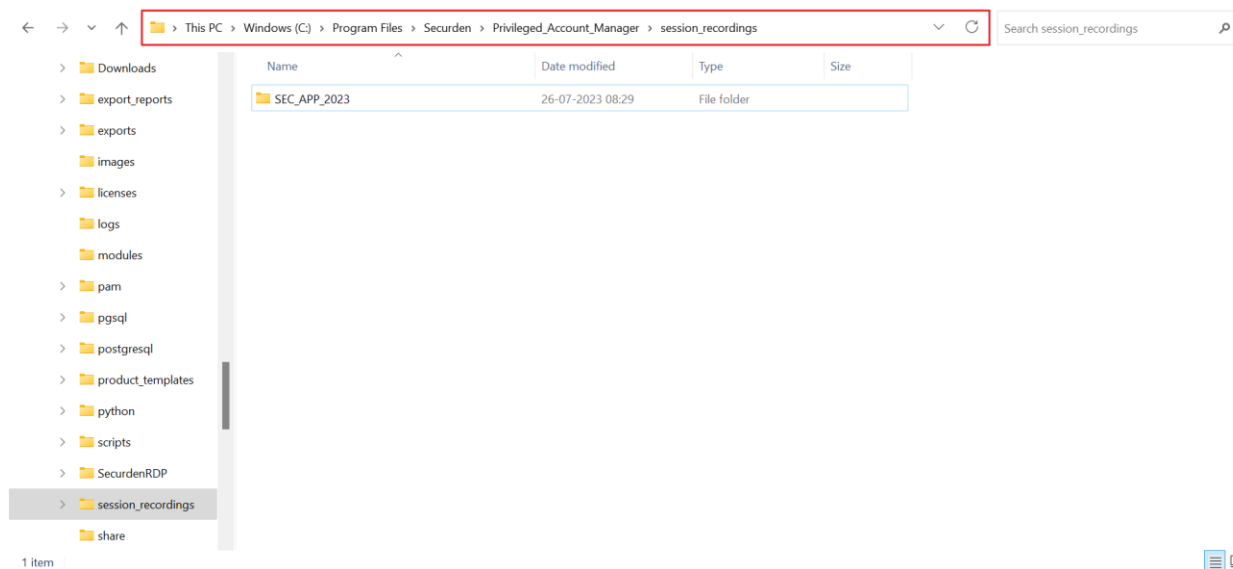
☒ Purge Periodically ☐ Never (The recorded files will be kept forever)

Purge interval (in days)*

15

Save

Note: If you manually move the recorded files to another location, Securden will not be able to playback those moved sessions when you try to.



Storing recorded sessions on a shared drive

If you are using multiple application servers, you need to ensure that the folder where recorded files are stored, is accessible to all the application servers. If you choose to store them on a shared drive, ensure that the user accounts used to run **Securden PAM Service** on all application servers have read/write access to the folder. To do this, in **services.msc**, search for **Securden PAM Service** and **Securden PAM Web Service**, go to 'Log On' tab, and enter the account which has read/write permission to the shared folder. Do this for all application servers as needed.

Purge recorded sessions

You can choose to delete recorded sessions periodically. This can be done by enabling the purge option and then choosing a time interval to automatically purge the files recorded in that gap, for example, if 15 days is chosen as the interval, recorded files will be deleted from the system after every 15 days.

To do this step Navigate to **GUI >> Admin >> Remote sessions and recordings >> Session recording** and scroll down.

The screenshot shows the 'Admin' section of the Securden Privileged Account Manager. The breadcrumb trail is 'Admin > Session Recording'. The page contains the following configuration options:

- Storage Location:** Two radio buttons are present: 'Device Storage/Network Drive' (unselected) and 'Cloud Storage' (selected).
- Cloud Storage Identifier:** A text input field with a dropdown arrow, labeled 'Cloud Storage Identifier*' and 'Search Cloud Storage Identifier'.
- Folder Path:** A text input field labeled 'Folder Path*'.
- Purge recorded sessions:** Two radio buttons: 'Purge Periodically' (selected) and 'Never (The recorded files will be kept forever)' (unselected).
- Purge Interval:** A text input field labeled 'Purge Interval (in days)*' with the value '15' entered.
- Save Button:** A green button labeled 'Save' at the bottom left.

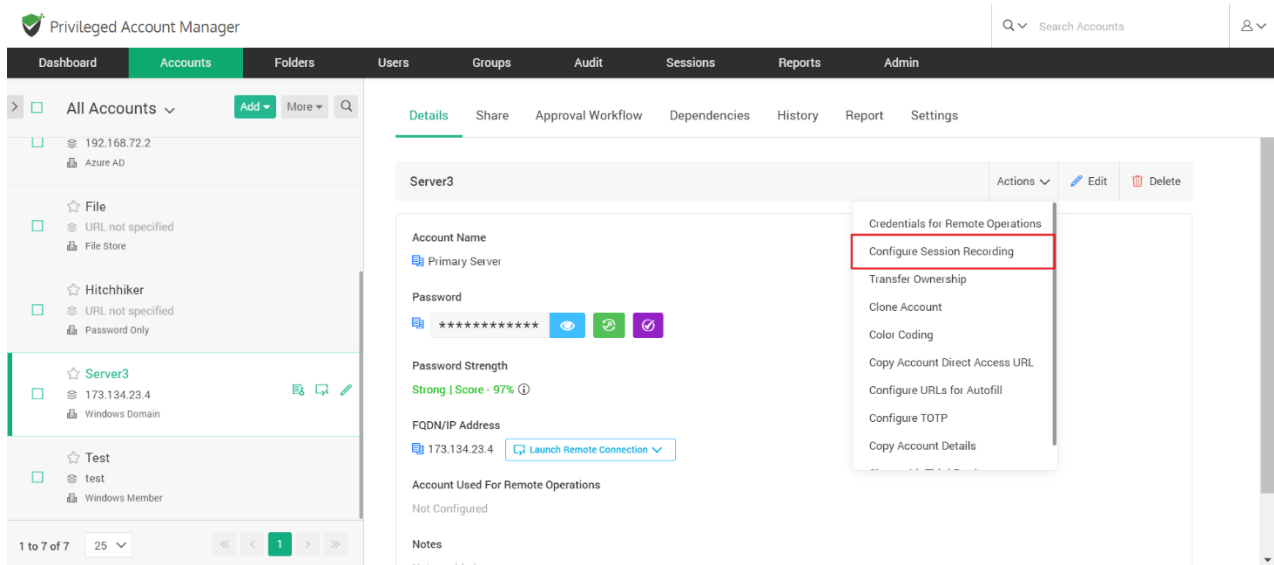
At the top of the interface, there is a search bar labeled 'Search Accounts' and a user profile icon.

Note: If you select the option to **Never**, the recorded files may be kept forever and occupy storage space over time.

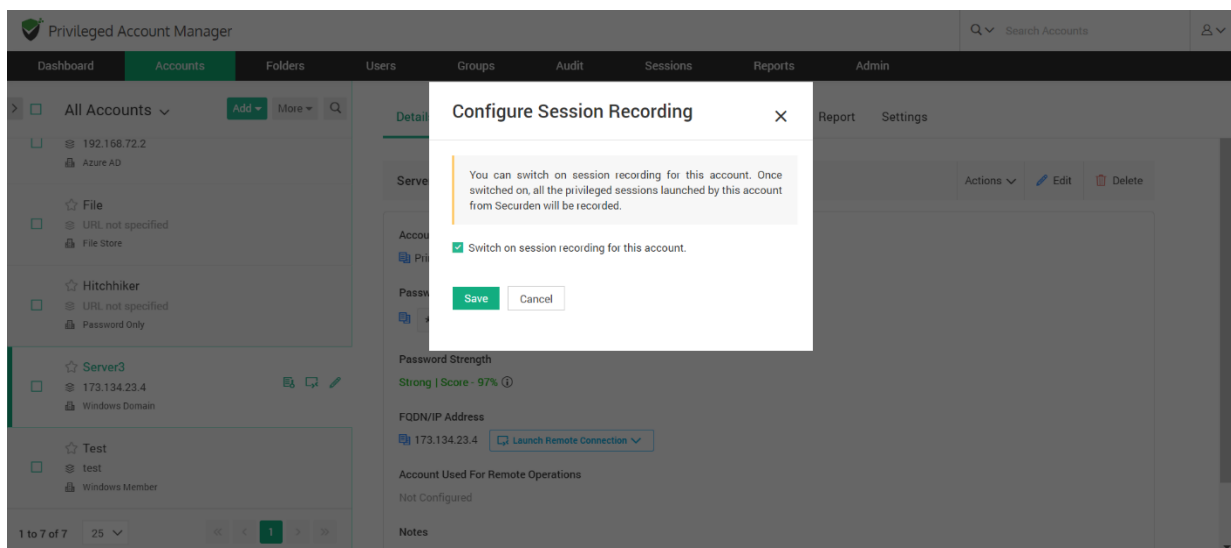
Step 4: Enable session recording at the account level

Specific accounts can be chosen to playback sessions launched from them. The sessions launched only for those accounts will be available for playback later.

Navigate to **Accounts >> Choose an account to be recorded >> Actions >> Configure session recording.**



You can enable session recording for that specific account using the checkbox and save changes.



Playback recorded sessions

Securden records the privileged sessions launched by the users and stores the recorded files. You can playback the recordings anytime.

Step 1: Ensure that session recording is enabled from **GUI >> 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.

To playback recorded sessions Navigate to Sessions >> **Recorded Sessions**.

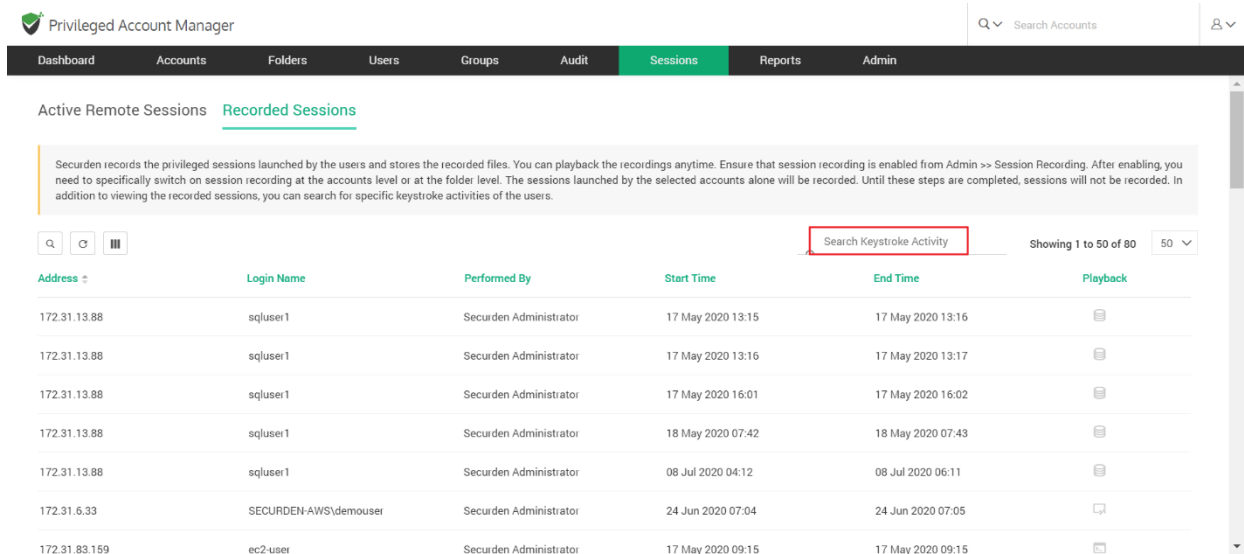
The screenshot displays the Securden Privileged Account Manager web interface. The top navigation bar includes links for Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions (highlighted), Reports, and Admin. A search bar for accounts and a user profile icon are also present. Below the navigation bar, the 'Recorded Sessions' tab is selected under the 'Active Remote Sessions' section. A descriptive text box explains that Securden records privileged sessions and provides instructions on enabling session recording at the account or folder level. Below this, a table lists recorded sessions with columns for Address, Login Name, Performed By, Start Time, End Time, and a Playback icon. The table shows seven sessions performed by the Securden Administrator, with timestamps ranging from May 17, 2020, to July 8, 2020. A search bar for keystroke activity and a pagination control (Showing 1 to 50 of 80) are located above the table.

Address	Login Name	Performed By	Start Time	End Time	Playback
172.31.13.88	sqluser1	Securden Administrator	17 May 2020 13:15	17 May 2020 13:16	[Playback Icon]
172.31.13.88	sqluser1	Securden Administrator	17 May 2020 13:16	17 May 2020 13:17	[Playback Icon]
172.31.13.88	sqluser1	Securden Administrator	17 May 2020 16:01	17 May 2020 16:02	[Playback Icon]
172.31.13.88	sqluser1	Securden Administrator	18 May 2020 07:42	18 May 2020 07:43	[Playback Icon]
172.31.13.88	sqluser1	Securden Administrator	08 Jul 2020 04:12	08 Jul 2020 06:11	[Playback Icon]
172.31.6.33	SECURDEN-AWS\demouser	Securden Administrator	24 Jun 2020 07:04	24 Jun 2020 07:05	[Playback Icon]
172.31.83.159	ec2-user	Securden Administrator	17 May 2020 09:15	17 May 2020 09:15	[Playback Icon]

You can search and select the 'Playback' option beside each session on the right, to watch the entire recorded session. There are no prerequisites needed for playback, they occur on a web-based media player.

Search by keystroke activity

In addition to viewing recorded sessions, you can search for specific keystroke activities of the users. A keystroke is the press of a single key on the keyboard. If a user has used the searched Keystroke, he will be listed on the search.



Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit **Sessions** Reports Admin

Active Remote Sessions Recorded Sessions

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.

Search Keystroke Activity Showing 1 to 50 of 80 50

Address	Login Name	Performed By	Start Time	End Time	Playback
172.31.13.88	sqluser1	Securden Administrator	17 May 2020 13:15	17 May 2020 13:16	
172.31.13.88	sqluser1	Securden Administrator	17 May 2020 13:16	17 May 2020 13:17	
172.31.13.88	sqluser1	Securden Administrator	17 May 2020 16:01	17 May 2020 16:02	
172.31.13.88	sqluser1	Securden Administrator	18 May 2020 07:42	18 May 2020 07:43	
172.31.13.88	sqluser1	Securden Administrator	08 Jul 2020 04:12	08 Jul 2020 06:11	
172.31.6.33	SECURDEN-AWS\demouser	Securden Administrator	24 Jun 2020 07:04	24 Jun 2020 07:05	
172.31.83.159	ec2-user	Securden Administrator	17 May 2020 09:15	17 May 2020 09:15	

Monitor remote sessions

You can monitor and shadow the remote sessions launched by the users using Securden PAM. The list of sessions that are active at the moment is shown. You may view the sessions and if needed, terminate any active session.

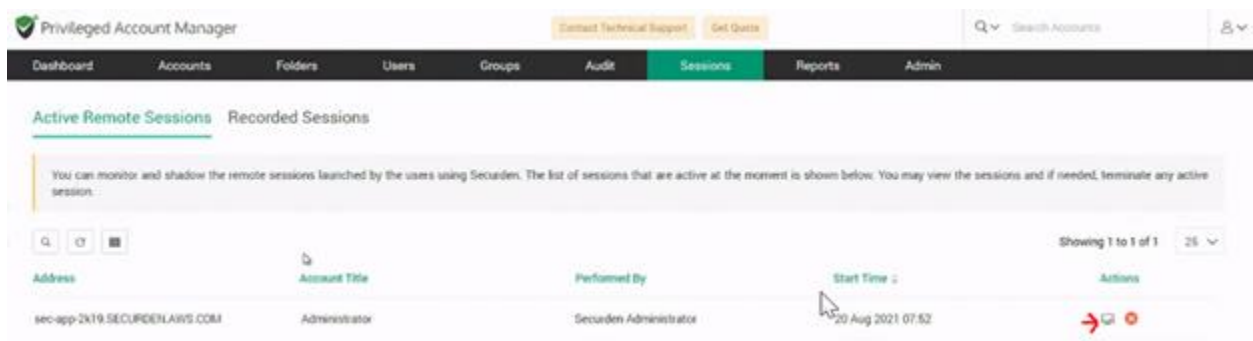
Navigate to **Sessions >> Active Remote sessions** to monitor remote sessions.

Note: You must refresh the sessions page to see sessions in progress.

The screenshot shows the Securden Privileged Account Manager web interface. The browser address bar indicates the URL is <https://w1040r68s3-5959/sessions/active-remote-sessions>. A yellow banner at the top states: "Trial license expires in 18 days. Contact support@securden.com to extend the trial." The main navigation bar includes tabs for Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions (highlighted in green), Reports, and Admin. Below the navigation bar, there are two tabs: "Active Remote Sessions" (selected) and "Recorded Sessions". A message box explains: "You can monitor and shadow the remote sessions launched by the users using Securden. The list of sessions that are active at the moment is shown below. You may view the sessions and if needed, terminate any active session." Below this message is a table with the following columns: Address, Account Title, Performed By, Start Time, and Actions. The table is currently empty, displaying "No data found". At the bottom of the page, there is a search bar and a "Showing 0 to 0 of 0" indicator. The Windows taskbar at the bottom shows the date as 18-04-2023 and the time as 16:00.

You can shadow the live session using the first icon actions if you have the admin rights to do so. You can also choose to terminate that session if required using the red cross under actions.

To do this, click on the **Monitor** icon beside the active session under **Actions**.



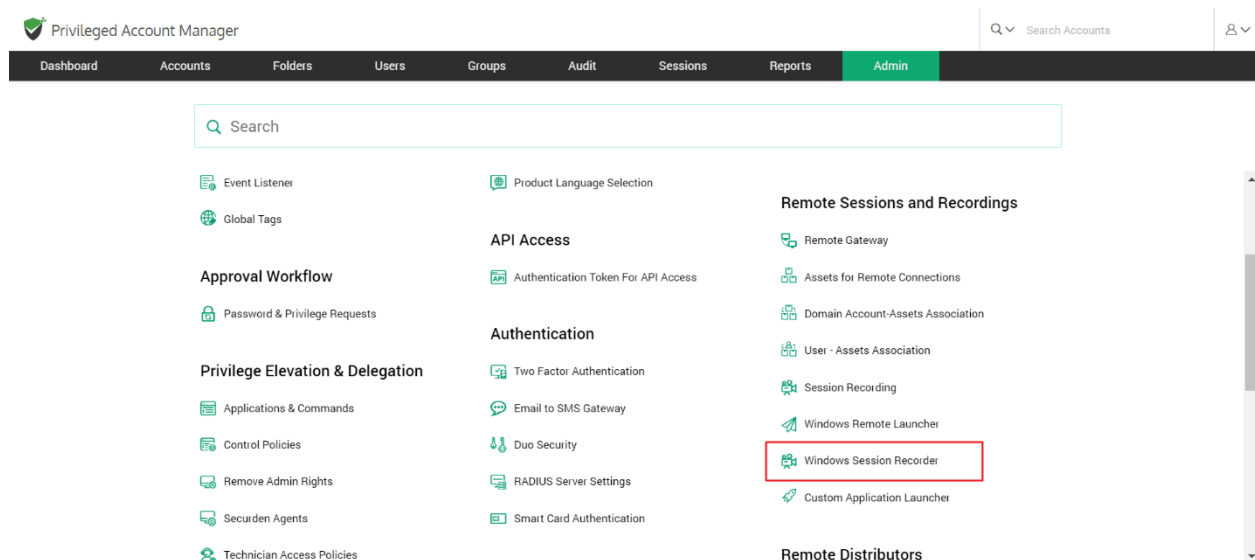
Then you will be asked if you want to shadow the session, on clicking '**Shadow the session**', you will be directed to a live screen where you can monitor the active session.

Advanced Recorder for Windows

Session recorder is a utility software that enables you to record remote sessions on your computer including the ones launched outside securden.

Deploy advanced session recorderIP If you wish to record sessions on remote computers, the session recorder from Securden can be installed manually on your computer to record all sessions.

To do this step Navigate to **Admin >> Remote sessions and recordings >> Windows session recorder.**



You can choose to download and install either the 32x bit or the 64x bit installer according to your system configurations OR follow the detailed instructions to install through GPO by clicking **follow the procedure detailed here.**

Section 11: Configuring the Remote Gateway

By default, all remote sessions launched from end user machines are tunneled through the Securden server, which acts as the gateway. There will not be any direct connectivity between the end user machines and the target device.

For enhanced security, you may route all remote operations originating from Securden through a single, dedicated gateway (instead of Securden server acting as the gateway). Once configured, Securden will route all operations, including remote connections, session recording, and password resets through the gateway.

When should you consider deploying a remote gateway?

You should consider deploying a remote gateway in the following scenarios:

- If you want to manage the IT assets/accounts that are distributed across multiple networks with interconnectivity.
- If you want to route all remote operations through a common gateway instead of direct connections to target devices from endpoints.
- If you want to record remote sessions

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 configure a remote gateway?

Gateway configuration is a four-step process:

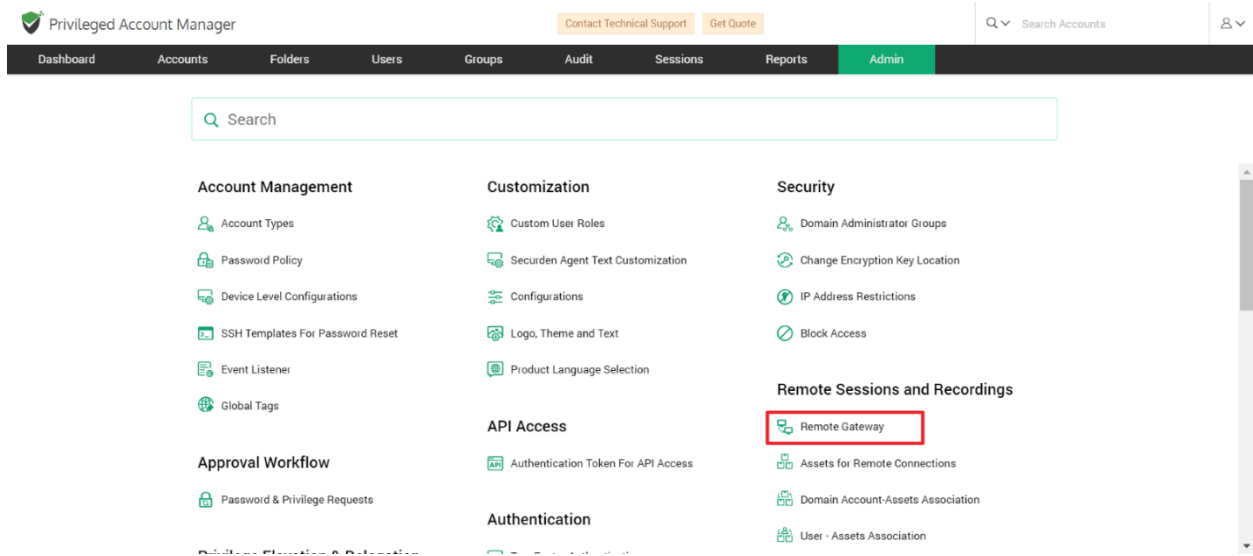
1. Create a remote gateway in Securden
2. Deploy Securden Session Manager and/or Securden Application Server
3. Associate devices with the remote gateway
4. Associate domains with the remote gateway

Summary: You need to create an entity called the remote gateway in Securden, deploy one or both the Securden Session Manager/Application Server and then associate the gateways with the required devices/domains in Securden. The steps are explained in detail in the sections that follow.

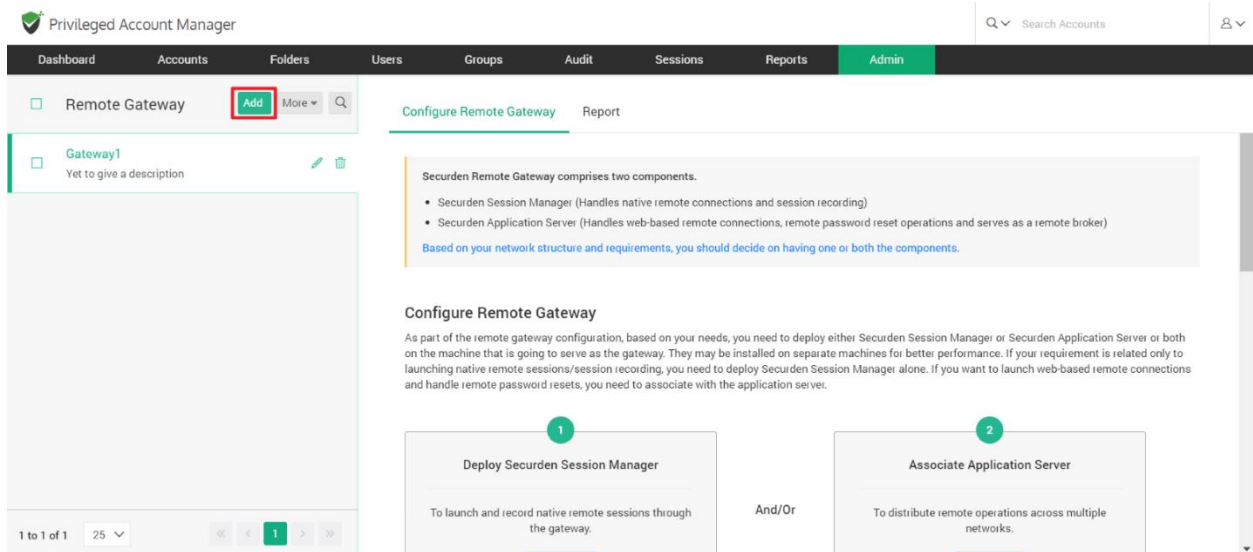
Step 1: Create a remote gateway

Prior to carrying out any configuration, you first need to add the required gateway as an entity giving it a name and description. Securden remote gateway is a virtual entity - something similar to a folder that holds files. So, you will first give it a name and description. In the next step, you will go about carrying out the actual configuration of the gateway.

To add a gateway, navigate to **Admin >> Remote Sessions and Recordings >> Remote Gateway**



In the Remote Gateway page that opens, click on **Add** to create a new remote gateway.



In the GUI that opens, enter the following details:

The screenshot shows the 'Add Remote Gateway' page in the Securden Privileged Account Manager. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin' (highlighted in green). There are links for 'Contact Technical Support' and 'Get Quote'. A search bar for 'Search Accounts' and a user profile icon are also present.

Add Remote Gateway

Securden remote gateway is a virtual entity - something similar to a folder that holds files. You will create the gateway giving it a name and description here. In the next step, the actual configuration of the gateway will have to be done. The gateway will hold two components - Securden Session Manager and Securden Application Server.

Remote Gateway Name *
Network systems RG

Description
To connect to remote network systems

Save **Cancel**

Remote Gateway Name: Helps you to uniquely identify the gateway you create.

- **Description:** A brief explanation of the purpose of that specific remote gateway.

On filling in the name and description fields, click '**Save**' to add the remote gateway in Securden.

Step 2: Configure the Remote Gateway

As part of the 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. They may be installed on separate machines for better performance.

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

Deploy Securden Session Manager (SSM)

To launch remote sessions and record them, you need to deploy Securden Session Manager (SSM), a lightweight tool on the machine that is identified to serve as the gateway. You need to choose the machine first and then deploy the SSM package.

Prerequisite: The server in which you want to deploy SSM should have already been discovered/added to Securden. In the interface, you can only choose from the already available accounts. If the server has not yet been added to Securden, add/discover and then follow the step below.

To deploy SSM, navigate to **Admin >> Remote Sessions and Recordings >> Remote Gateway** and select the required gateway.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Remote Gateway Add More

- Australia Data Center Connect fast
- Belgium DC Yet to give a description
- Dubai Data Center Yet to give a description
- Gateway A** A
- India Data center Yet to give a description
- London DC Yet to give a description
- New York Data Center Yet to give a description

1 to 7 of 7 25

Configure Remote Gateway Report

Securden Remote Gateway comprises two components.

- Securden Session Manager (Handles native remote connections and session recording)
- Securden Application Server (Handles web-based remote connections, remote password reset operations and serves as a remote broker)

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

Configure Remote Gateway

As part of the 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. They may be installed on separate machines for better performance. If your requirement is related only to launching native remote sessions/session recording, you need to deploy Securden Session Manager alone. If you want to launch web-based remote connections and handle remote password resets, you need to associate with the application server.

1 Deploy Securden Session Manager

To launch and record native remote sessions through the gateway.

2 Associate Application Server

Application Server has already been configured and associated.

And/Or

Associate Devices, Domains with Remote Gateway

After configuring the remote gateway, you need to associate the container with the required devices (IT assets) or domains. Once configured, all remote connections originating from the respective devices will go

In the RHS, you will see the GUI consisting of the steps to **Deploy Securden Session Manager**.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Remote Gateway Add More

- Australia Data Center Connect fast
- Belgium DC Yet to give a description
- Dubai Data Center Yet to give a description
- Gateway A** A
- India Data center Yet to give a description
- London DC Yet to give a description
- New York Data Center Yet to give a description

1 to 7 of 7 25

Deploy Securden Session Manager

To launch remote sessions and record them, you need to deploy Securden Session Manager (SSM), a lightweight utility on a Windows machine. In the steps below, you need to choose the machine/device first. Then download and install Securden Session Manager on the machine/device selected. The machine acts as the landing server for SSM.

Step 1: Select the machine to install SSM

The server in which you want to deploy SSM should have been already discovered/added to Securden. You can only choose from the already available accounts. If the server has not yet been added to Securden, you can directly install the MSI from Step 2. Once the MSI is installed, the server will be automatically shown in the list in Securden.

Select and Configure

Step 2: Install Securden Session Manager (.msi)

Download and install this lightweight tool on the machine selected in Step 1 above.

Follow these instructions to deploy SSM.

SecurdenSessionManager.msi (404)

Step 3: Configure SSH Tunneling (Optional)

If you access Securden Session Manager from the internet, it is recommended that you download and configure SSH tunneling. This optional configuration acts as an additional Security step when you connect to the Securden Session Manager. If you do not access the Session Manager through the internet, you can simply skip this configuration.

Instead of opening the RDP port of Securden Session Manager to the internet, you can configure SSH tunneling in front of the RDP port. Once configured, users will be connecting to the SSH tunnel port instead of the RDP port. This can be configured either in the same server where Securden Session Manager is installed or on a different server.

Follow these detailed instructions to configure SSH tunneling.

SecurdenCustomService.zip

In the GUI that opens, you need to perform the following actions:

1) Select the machine in which you will be deploying SSM

2) Download the SSM package and deploy it on the machine selected. Select the machine to install SSM

3) (Optional) Configure SSH tunneling

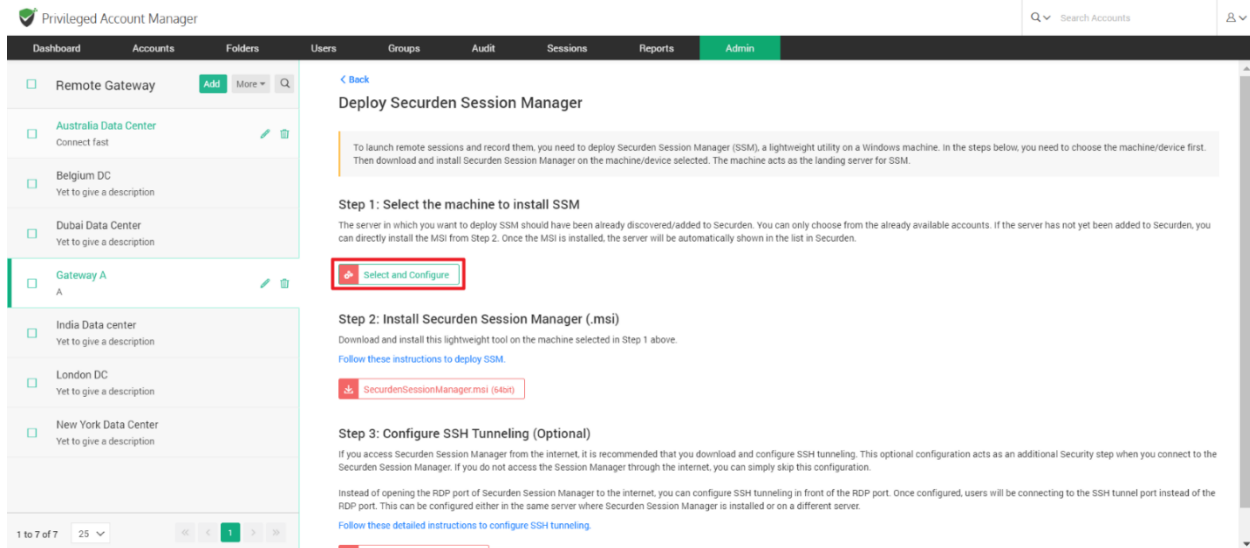
1: Select the machine in which you will be deploying SSM

In this step, you need to select a machine where you would like to install the Securden Session Manager. In addition, you need to specify an account using which connections are to be established with the machine.

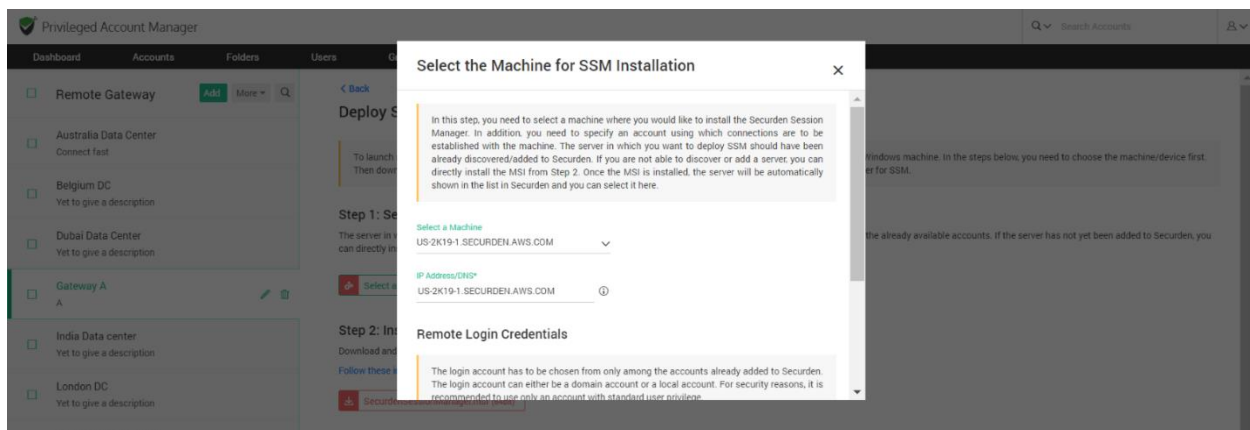
Pre-requisite: The machine/server in which you want to deploy SSM should have been already discovered/added to Securden. You will only be able to select from the machines/servers that are listed in the drop-down.

If you are not able to discover or add a server, you can directly install the MSI from Step 2. Once the MSI is installed, the server will be automatically shown in the list in Securden and you can select it here.

To select the machine where SSM should be deployed, click “**Select and Configure**” as shown in the screenshot below.



In the GUI that opens up, you need to select a machine discovered and added to Securden. Once you select the intended machine, you need to enter its IP address or DNS to enable Securden to connect to the device.



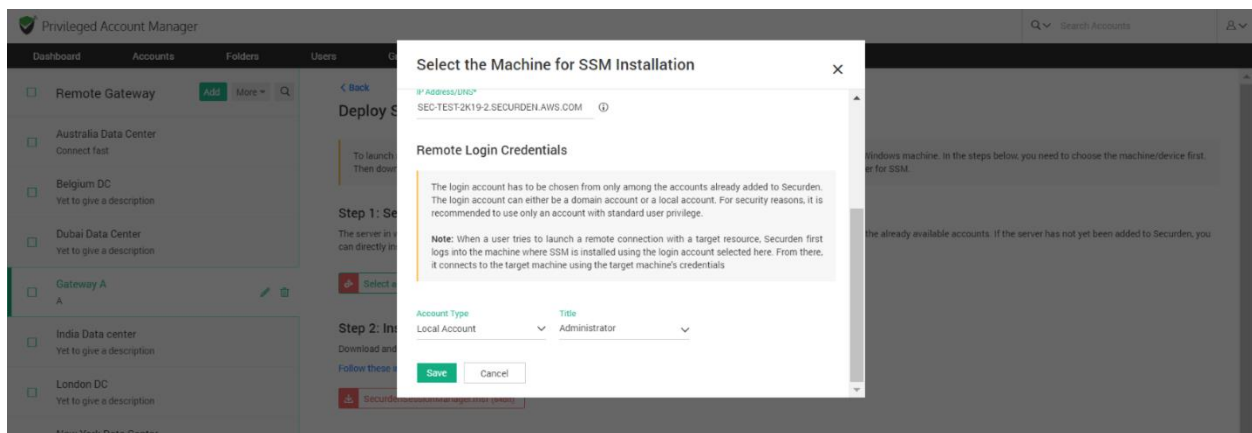
Input remote login credentials - In addition to the IP address, you need to specify an account using which connections are to be established with the machine.

Typically, when a user tries to launch a remote connection with a target resource, Securden first logs into the machine where SSM is installed using

the login account selected here. From there, it connects to the target machine using the target machine's credentials.

The remote login account has to be chosen from only among the accounts already added to Securden. The login account can either be a domain account or a local account.

Note: For security reasons, it is recommended to use only an account with standard user privilege.



You need to select the Account Type, the Account title for the required account and click **"Save"**.

2: Install the Securden Session Manager (.msi)

After completing Step 1, you are ready to install the SSM package on the machine identified above. Download the .msi package from the GUI and follow the instructions given in the document link provided in the interface.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Remote Gateway Add More Q

- Australia Data Center Connect fast
- Belgium DC Yet to give a description
- Dubai Data Center Yet to give a description
- Gateway A** A
- India Data center Yet to give a description
- London DC Yet to give a description
- New York Data Center Yet to give a description

1 to 7 of 7 25 < 1 >

Deploy Securden Session Manager

[Back](#)

To launch remote sessions and record them, you need to deploy Securden Session Manager (SSM), a lightweight utility on a Windows machine. In the steps below, you need to choose the machine/device first. Then download and install Securden Session Manager on the machine/device selected. The machine acts as the landing server for SSM.

Step 1: Select the machine to install SSM

The server in which you want to deploy SSM should have been already discovered/added to Securden. You can only choose from the already available accounts. If the server has not yet been added to Securden, you can directly install the MSI from Step 2. Once the MSI is installed, the server will be automatically shown in the list in Securden.

[Select and Configure](#)

Step 2: Install Securden Session Manager (.msi)

Download and install this lightweight tool on the machine selected in Step 1 above.

[Follow these instructions to deploy SSM.](#)

[SecurdenSessionManager.msi \(64bit\)](#)

Step 3: Configure SSH Tunneling (Optional)

If you access Securden Session Manager from the internet, it is recommended that you download and configure SSH tunneling. This optional configuration acts as an additional Security step when you connect to the Securden Session Manager. If you do not access the Session Manager through the internet, you can simply skip this configuration.

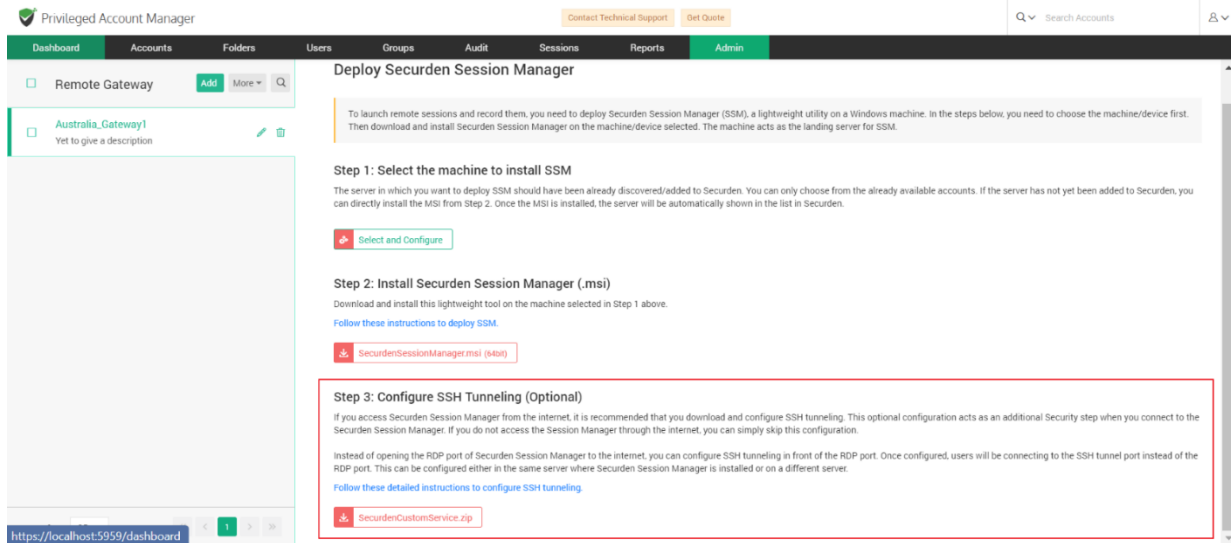
Instead of opening the RDP port of Securden Session Manager to the internet, you can configure SSH tunneling in front of the RDP port. Once configured, users will be connecting to the SSH tunnel port instead of the RDP port. This can be configured either in the same server where Securden Session Manager is installed or on a different server.

[Follow these detailed instructions to configure SSH tunneling.](#)

3: Configure SSH Tunneling (Optional)

If you do not access the Session Manager through the internet, you can simply skip this configuration.

If you access Securden Session Manager from the internet, it is recommended that you download and configure SSH tunneling. This optional configuration acts as an additional Security step when you connect to the Securden Session Manager.



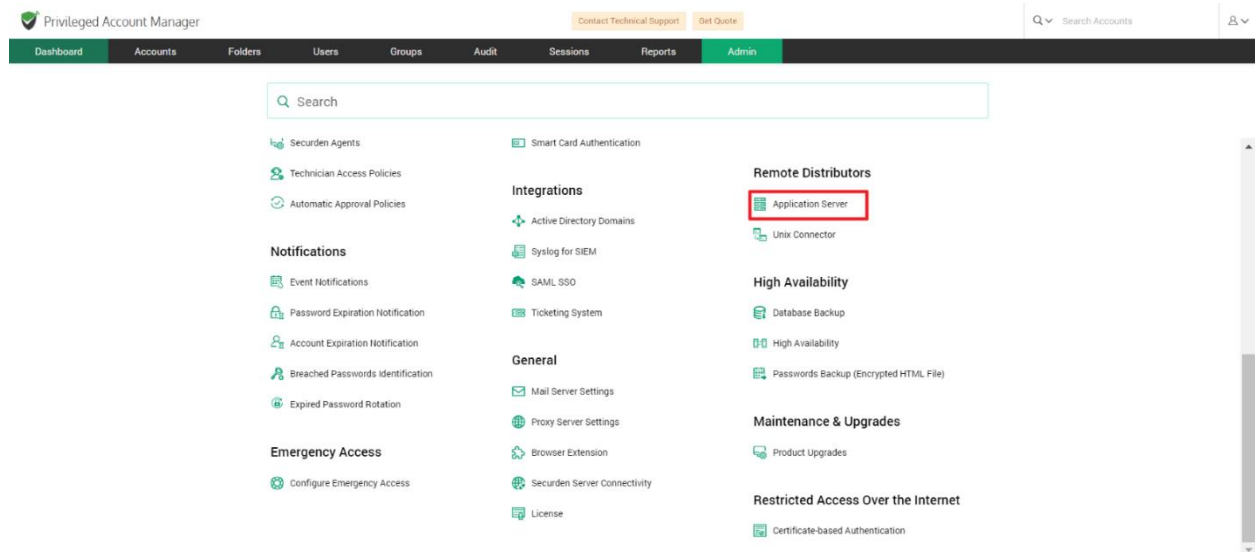
Instead of opening the RDP port of Securden Session Manager to the internet, you can configure SSH tunneling in front of the RDP port. Once configured, users will be connecting to the SSH tunnel port instead of the RDP port. This can be configured either in the same server where Securden Session Manager is installed or on a different server.

Follow the detailed instructions available on the GUI to configure SSH tunnelling.

Associate an Application Server

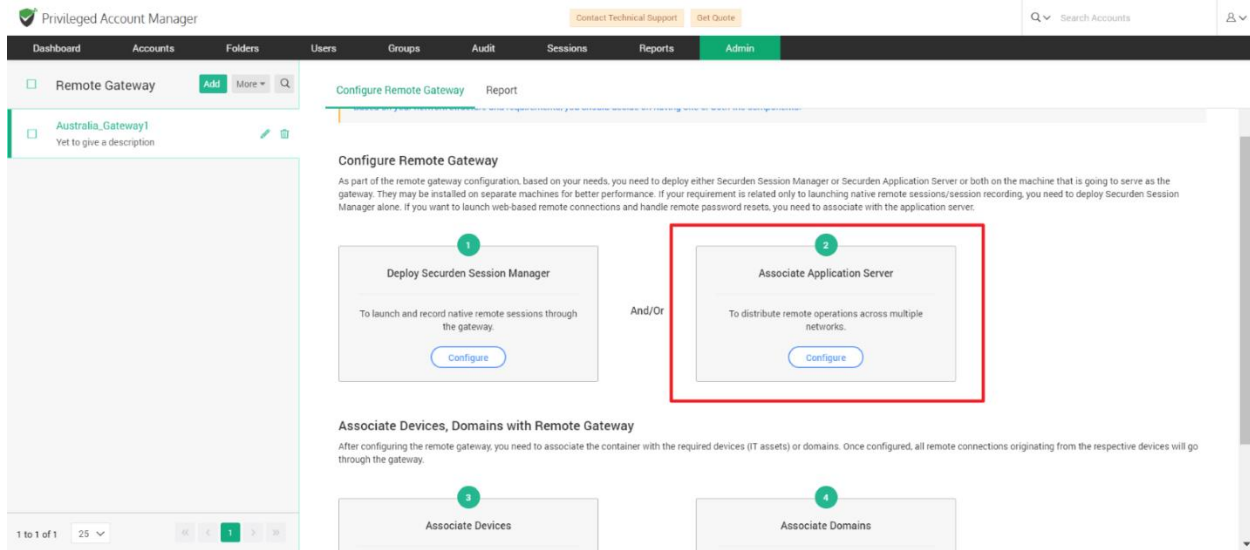
If you have decided to deploy a Securden application server as well (for reasons explained on components selection above), you need to associate each such application server with a remote gateway. Once the association is done, all remote connections originating from the application servers will be routed through the gateway.

Prerequisite: You should have added at least one Application Server before proceeding further. If you haven't added any yet, navigate to **Admin >> Remote Distributors >> Application Server**.

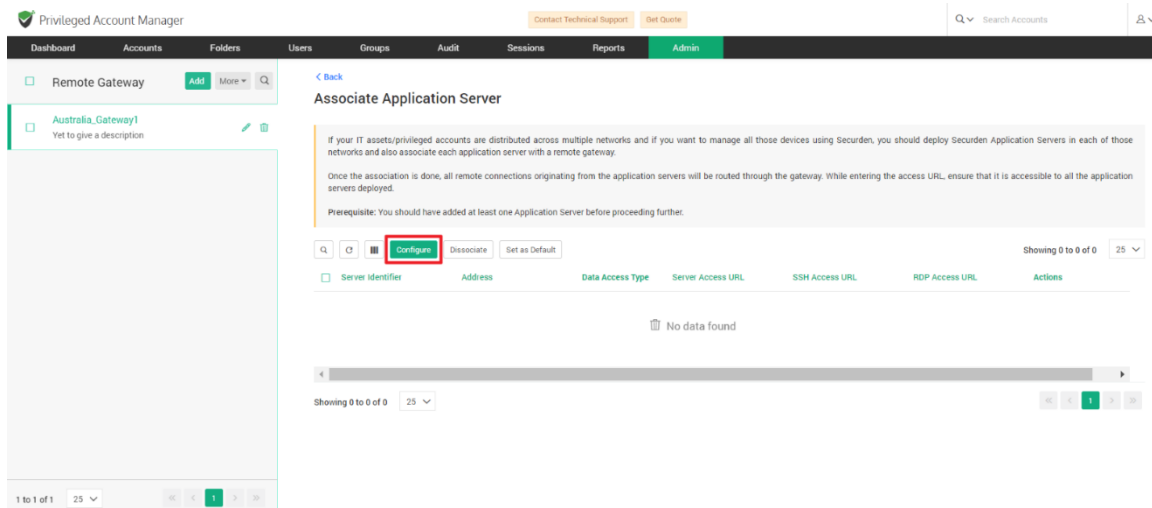


To associate an existing application server with the remote gateway, navigate to **Admin >> Remote Sessions and Recordings >> Remote Gateway** and select the required gateway.

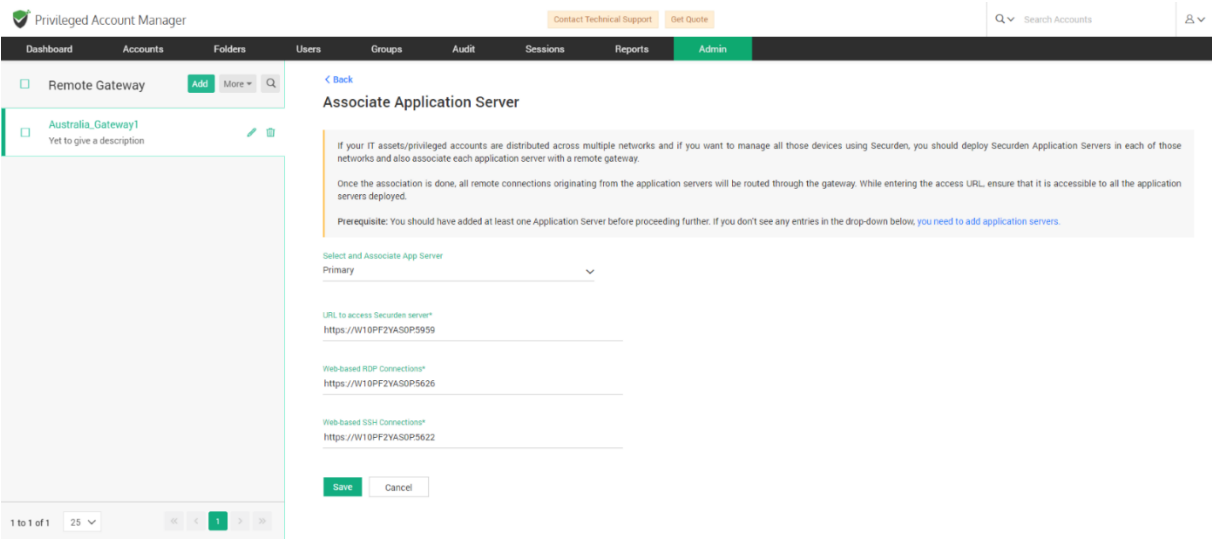
In the RHS, you will see the **Configure Remote Gateway** section. Within that you will see the option to **Associate Application Server**. Click the **Configure** button.



In the GUI that opens, you can see all application servers associated with the selected gateway. If there are no application servers added, you need to select **Configure**.

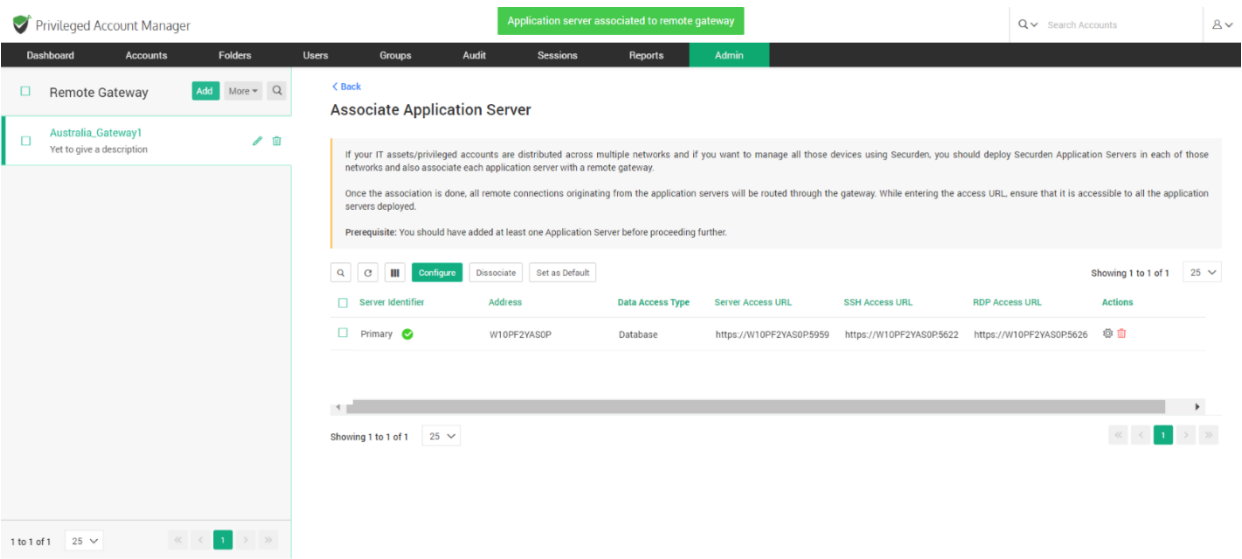


Once you select the required application server, you will need to supply the URLs shown below.

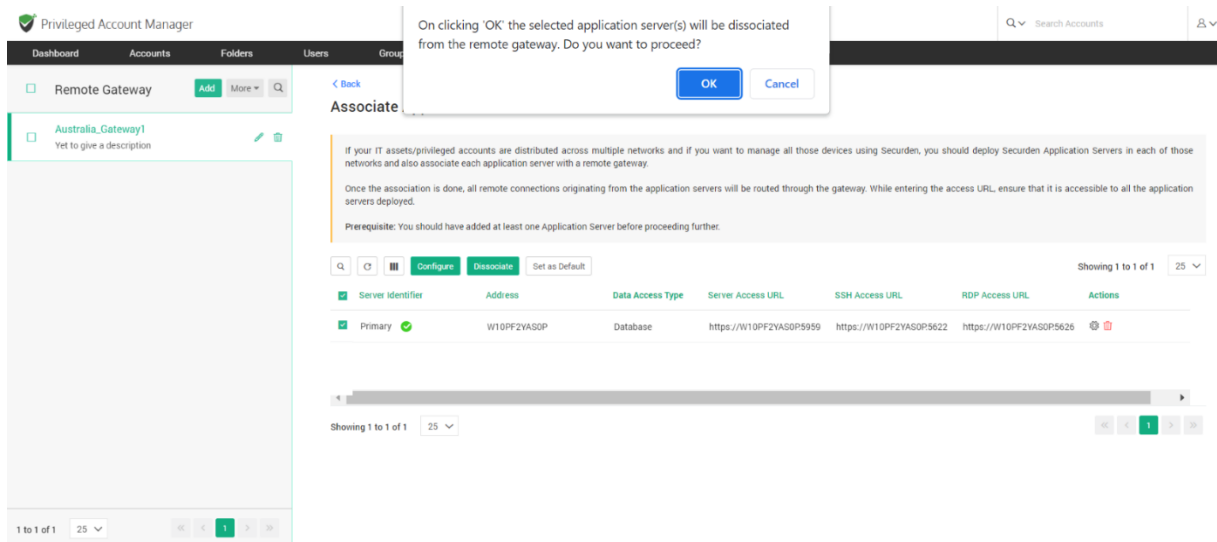


The URL through which the Securden server could be connected, and the URLs for web-based RDP and SSH connections. Ensure that all the URLs supplied are correct.

Click **Save**. You will now be able to see that the application server has been associated with the selected gateway and listed.



You can choose to select a configured application server and dissociate it if needed. Click on the gateway you need to dissociate and click **Dissociate**. You can then click **OK** on the precautionary popup that appears.



Step 3: Associate the required devices

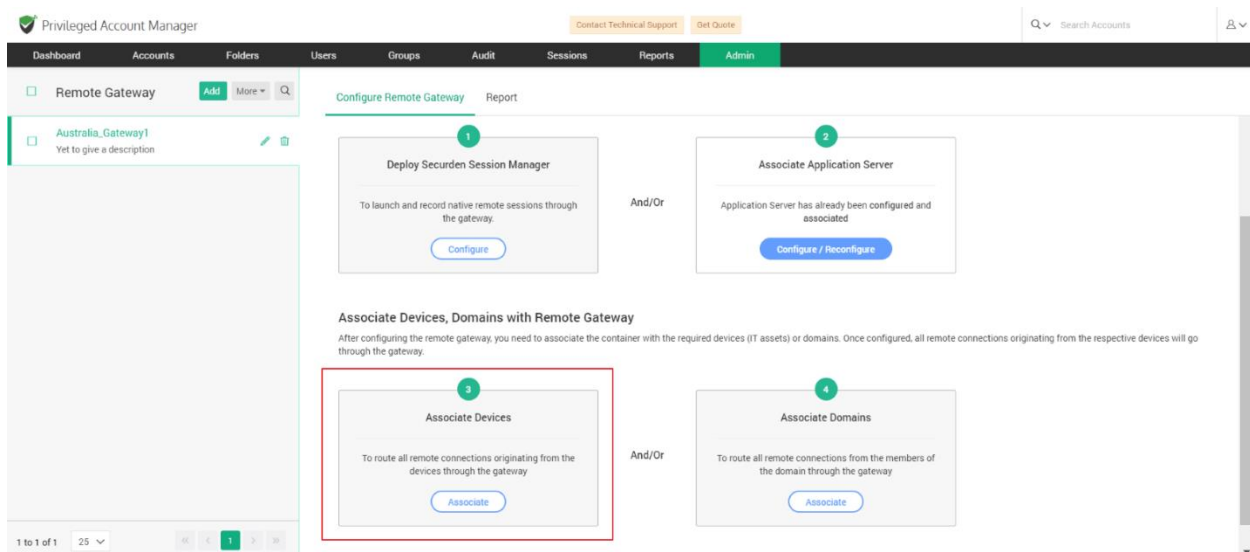
Steps 1 and 2 above mark the creation of the remote gateway, which is like a container.

Once you have created the Container, you need to associate it with the required devices (IT assets) or domains. Once configured, all remote connections originating from the respective devices will go through the gateway associated with them.

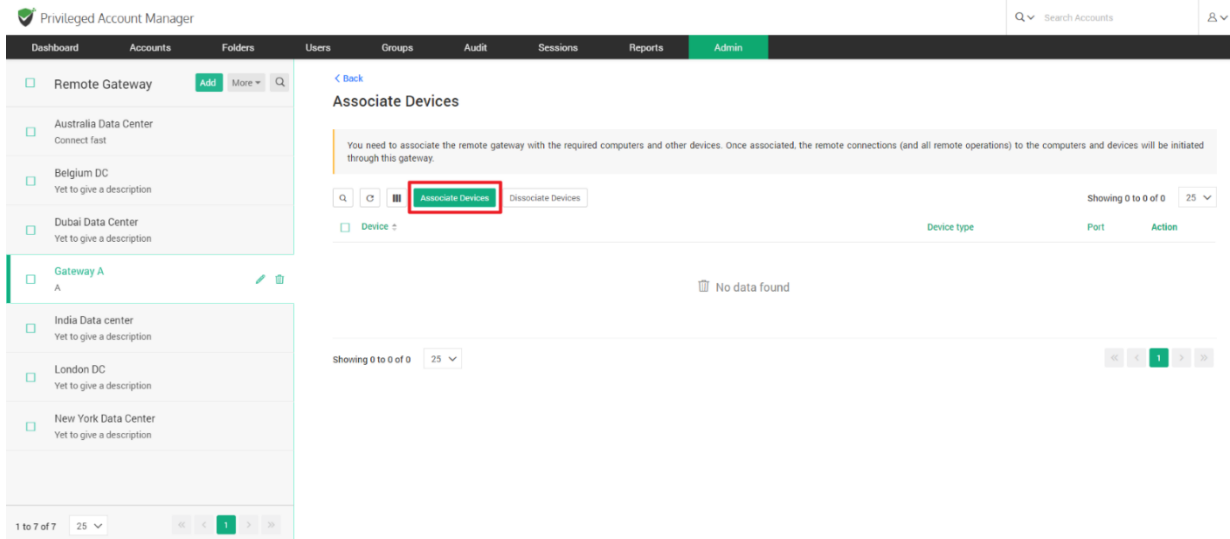
Prerequisite: You can only associate the devices and domains that are already added to Securden.

To associate devices and/or domains with the gateway, navigate to **Admin >> Remote Sessions and Recordings >> Remote Gateway** and select the required gateway.

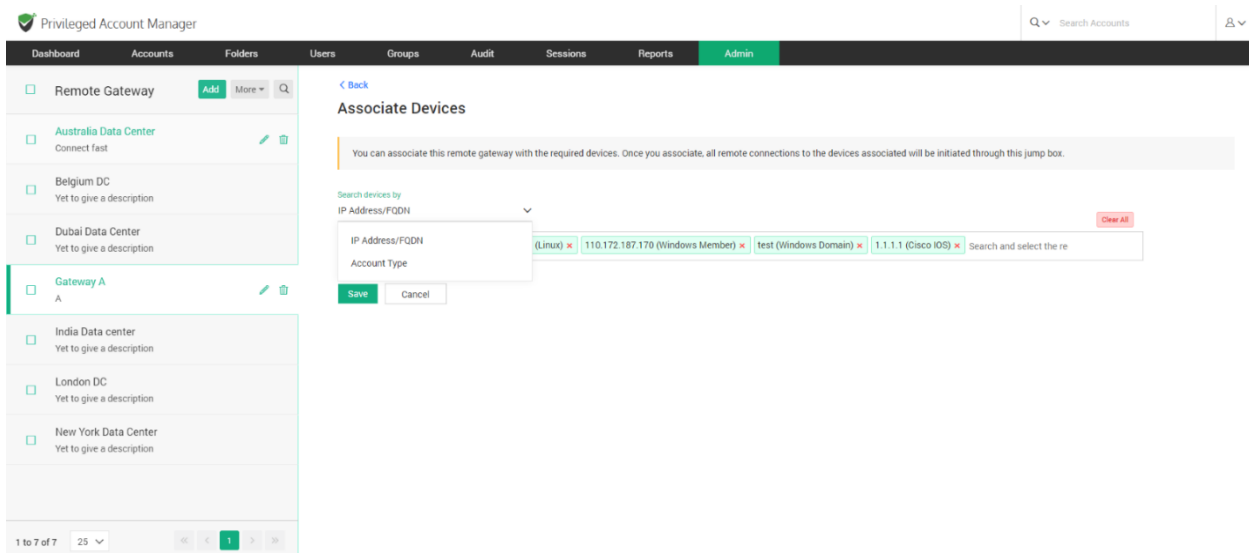
In the RHS, you will see the **Configure Remote Gateway** section. Within that you will see the option to **Associate Devices**. Click the **Associate** button.



In the GUI that opens, you can see all devices associated with the selected gateway. If there are no devices added, you need to select the button **Associate Devices**.



Then do a search for the required devices using the search filters. You can either search for devices based on their IP Address/FQDN or their Account Type.



You may select as many devices as you want. To clear a selected device, click the 'x' beside the device, to clear all selected devices use the 'Clear all' icon to the right.

On selecting the devices to be associated with the gateway, click **Save**.

Step 4: Associate the required domains

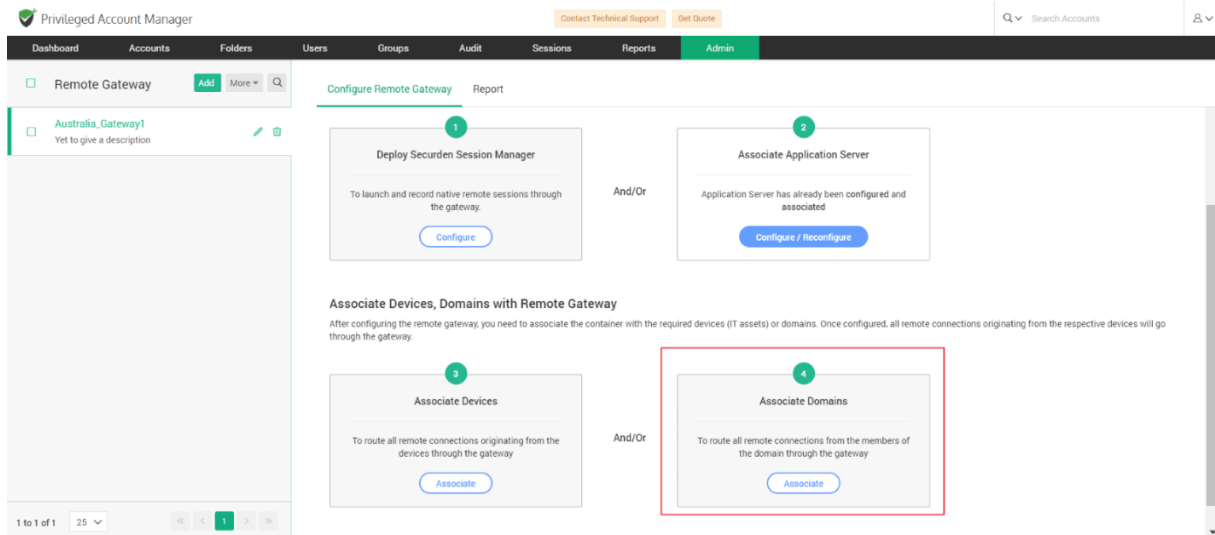
Once you have created the Container, you need to associate it with the required domains. Once configured, all remote connections originating from the respective domains will go through the gateway associated with them.

You have the option to associate specific devices alone and/or an entire domain. When a domain is associated with the gateway, all remote connections originating from the members of the domain will go through the gateway. When adopting a combination approach (associating both devices and domains), in case you have configured a different remote gateway for any of the computers that are part of the domain, the device level configuration will take effect for that computer alone.

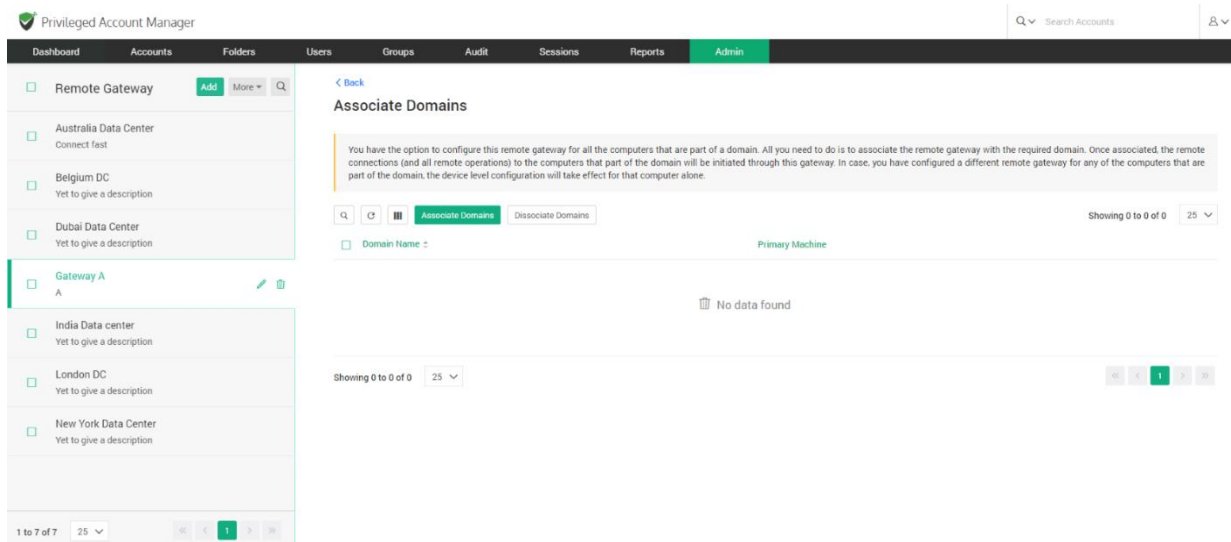
Prerequisite: You can only associate the domains that are already added to Securden.

To associate domains with the gateway, navigate to **Admin >> Remote Sessions and Recordings >> Remote Gateway** and select the required gateway.

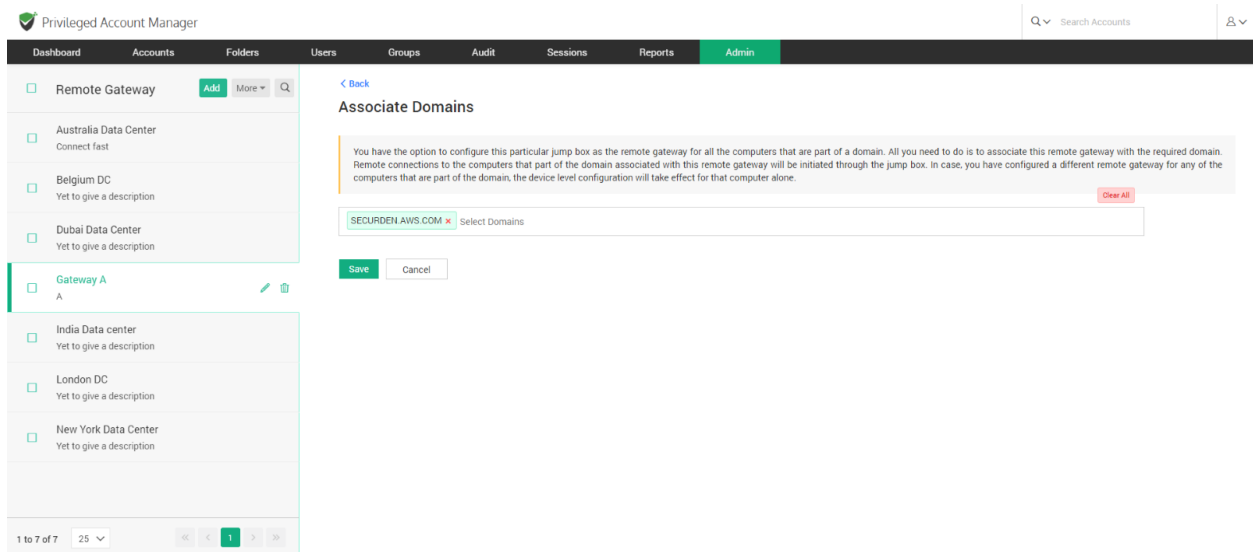
In the RHS, you will see the **Configure Remote Gateway** section. Within that you will see the option to **Associate Domains**. Click the “**Associate**” button.



In the GUI that opens, you can see all domains associated with the selected gateway. If there are no devices added, you need to select the button **Associate Domains**.



You may search and select as many domains as you want. To clear a selected domain click the **x** beside the device, to clear all selected domains use the **Clear all** icon to the right.



On selecting the domains to be associated with the gateway, click **Save**.

These steps complete the configuration for a single remote gateway. You may repeat the steps and configure multiple gateways.

Verify remote gateway configuration and associations

Once you complete all the steps above, you can verify all associations in the form of a report. Securden depicts the list of all devices and domains associated with the remote gateway. You can also view the Securden packages (Application server and/or Securden Session Manager) associated with the gateway.

To view the report, navigate to **Admin >> Remote Sessions and Recordings >> Remote Gateway** and select the required gateway. In the RHS, you will see the 'Report' section.

The screenshot shows the Securden Unified PAM Admin interface. The top navigation bar includes Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin (highlighted). The left sidebar lists various Remote Gateways, including Gateway A. The main content area is titled 'Configure Remote Gateway' and features a 'Report' button highlighted with a red box. Below this, there are two sections: 'Devices associated with this remote gateway' and 'Domains associated with this remote gateway'. The 'Devices' section displays a table with columns for Device Name, Device Type, and Port, showing three entries. The 'Domains' section displays a table with columns for Domain Name and Primary Machine, showing one entry.

Device Name	Device Type	Port
10.0.0.1	Windows Workgroup	
10.0.0.60	Windows Domain	
110.172.187.170	Windows Member	

Domain Name	Primary Machine
SECURDEN.AWS.COM	

Editing an existing remote gateway

The existing remote gateways, their configurations, device/domain associations can be edited anytime by visiting the same pages in the same way they were configured.

To configure the remote gateway name and description, Navigate to **Admin >> Remote Sessions and Recordings >> Remote Gateway**, select the required gateway and click the edit icon.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Remote Gateway Add More

Australia_Gateway1
Yet to give a description

Configure Remote Gateway Report

Securden Remote Gateway comprises two components.

- Securden Session Manager (Handles native remote connections and session recording)
- Securden Application Server (Handles web-based remote connections, remote password reset operations and serves as a remote broker)

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

Configure Remote Gateway

As part of the 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. They may be installed on separate machines for better performance. If your requirement is related only to launching native remote sessions/session recording, you need to deploy Securden Session Manager alone. If you want to launch web-based remote connections and handle remote password resets, you need to associate with the application server.

1 Deploy Securden Session Manager
To launch and record native remote sessions through the gateway.
[Configure](#)

And/Or

2 Associate Application Server
Application Server has already been configured and associated.
[Configure / Reconfigure](#)

Associate Devices, Domains with Remote Gateway

After configuring the remote gateway, you need to associate the container with the required devices (IT assets) or domains. Once configured, all remote connections originating from the respective devices will go

To configure the associated devices/domains and app servers, re-configure the required attributes the same way they were added.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Remote Gateway Add More

Australia Data Center
Connect Test

Belgium DC
Yet to give a description

Dubai Data Center
Yet to give a description

Gateway A
A

India Data center
Yet to give a description

London DC
Yet to give a description

New York Data Center
Yet to give a description

Configure Remote Gateway Report

Securden Remote Gateway comprises two components.

- Securden Session Manager (Handles native remote connections and session recording)
- Securden Application Server (Handles web-based remote connections, remote password reset operations and serves as a remote broker)

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

Configure Remote Gateway

As part of the 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. They may be installed on separate machines for better performance. If your requirement is related only to launching native remote sessions/session recording, you need to deploy Securden Session Manager alone. If you want to launch web-based remote connections and handle remote password resets, you need to associate with the application server.

1 Deploy Securden Session Manager
To launch and record native remote sessions through the gateway.
[Configure](#)

And/Or

2 Associate Application Server
Application Server has already been configured and associated.
[Configure / Reconfigure](#)

Associate Devices, Domains with Remote Gateway

After configuring the remote gateway, you need to associate the container with the required devices (IT assets) or domains. Once configured, all remote connections originating from the respective devices will go through the gateway.

3 Associate Devices
To route all remote connections originating from the devices through the gateway.
[Associate / Disassociate](#)

And/Or

4 Associate Domains
To route all remote connections from the members of the domain through the gateway.
[Associate / Disassociate](#)

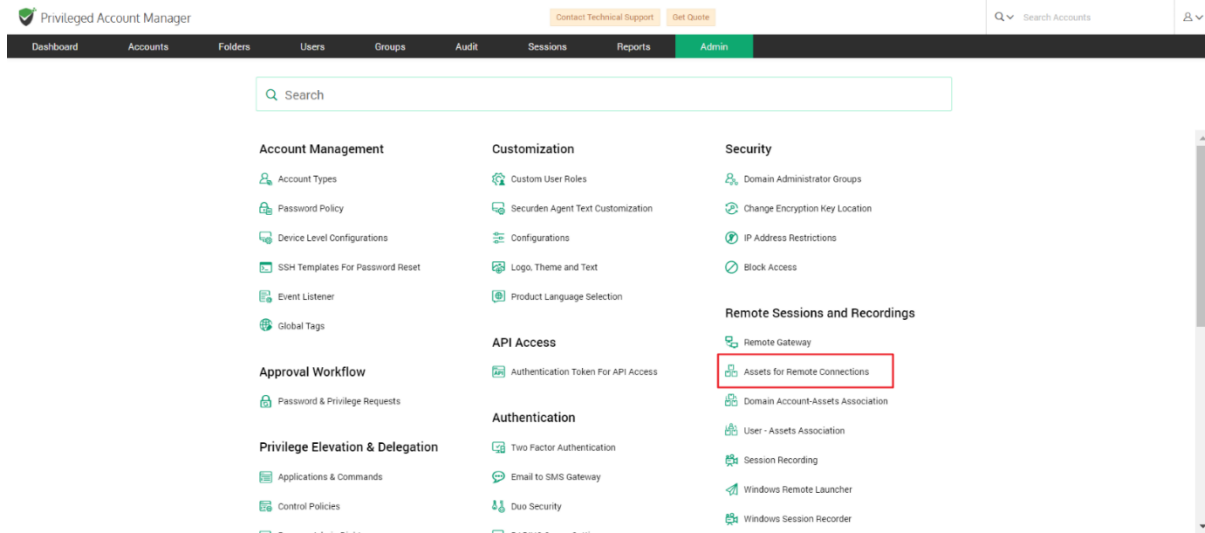
Add Assets for Remote Connections

Domain accounts are often used to remotely connect to computers and various other IT assets. Any domain account can be configured to remotely connect to multiple IT assets. In such scenarios, creating an association between the domain accounts and the list of IT assets it could connect to, becomes necessary.

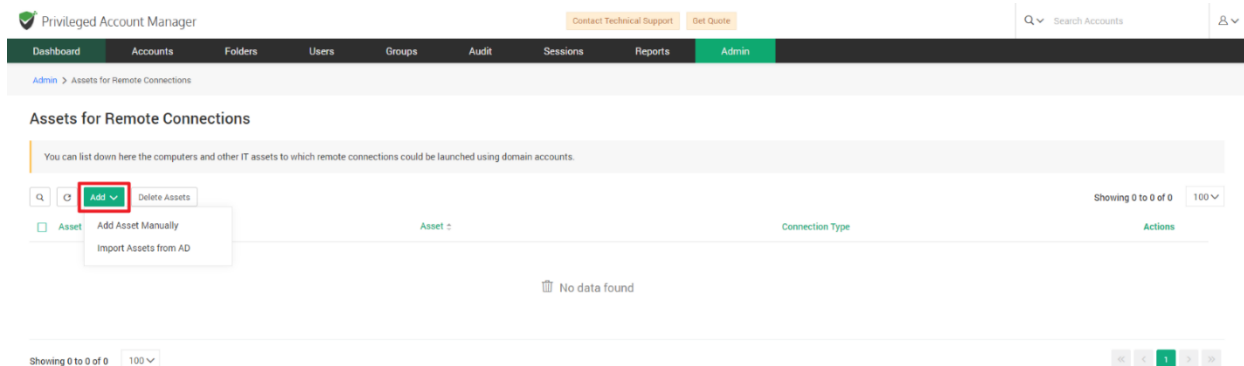
Prior to creating such an association, the IT assets are to be added to Securden. You may add all such computers and other IT assets in this section.

While adding the IT asset, you can specify how the device can be connected (RDP/SSH/SQL) and the device's connectivity details. As mentioned above, the assets added here need to be associated with the required domain accounts - that is, with specific users/user groups and accounts/folders in Securden.

To add the assets that are to be remotely accessed, navigate to **Admin >> Remote Sessions and Recordings >> Assets for Remote Connections**.



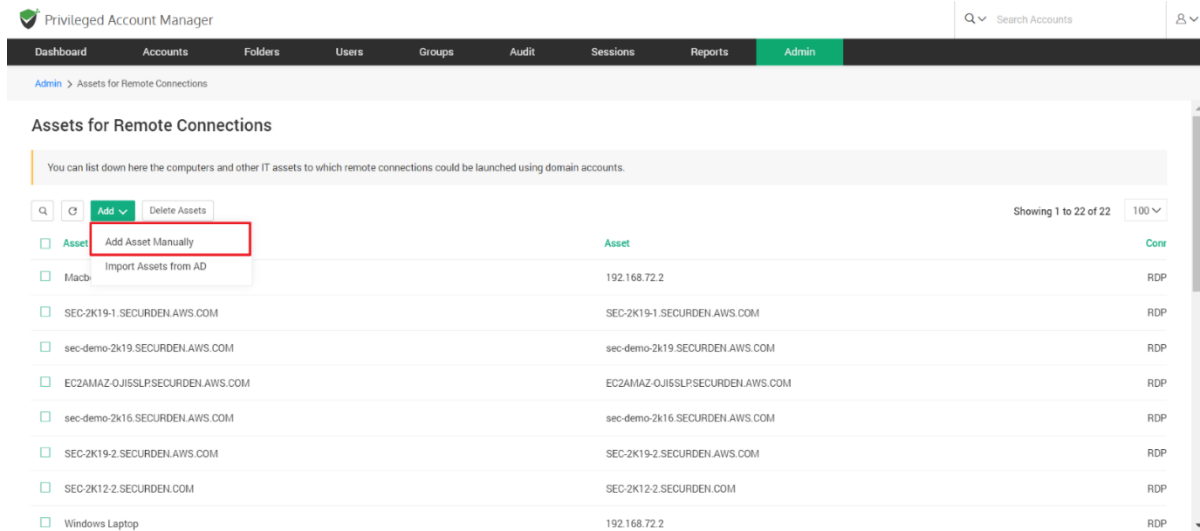
In the GUI that opens, click **Add**.



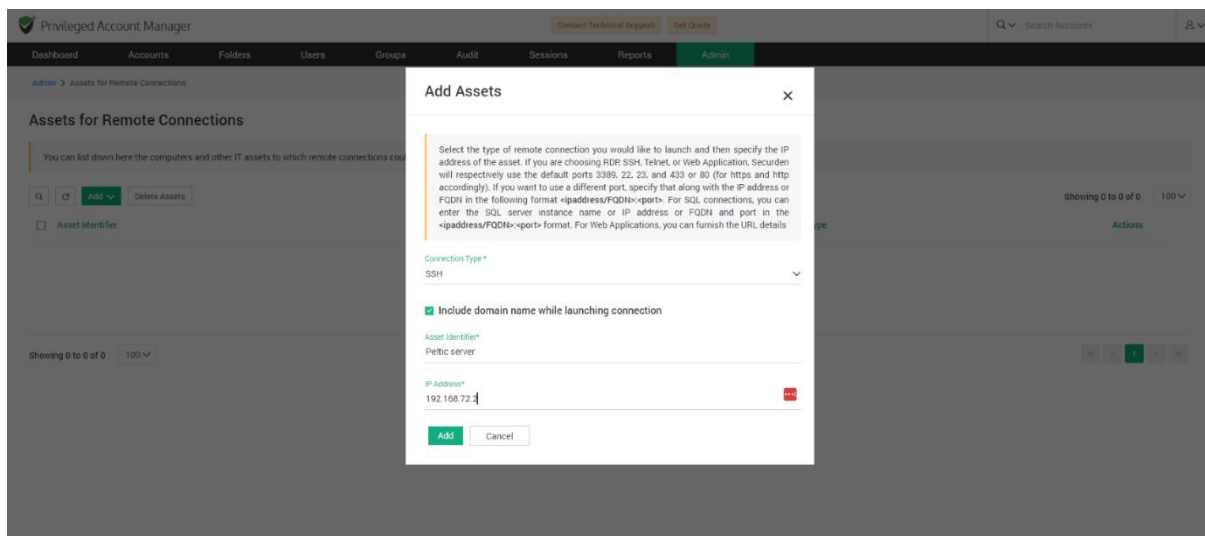
You have the option to either add assets manually by supplying the connectivity details or import them from your directory. Both options are elaborated below.

Add Assets Manually

You can add the required IT assets manually one at a time. Click on **Add Asset Manually**.



In the GUI that opens, you need to specify the attributes associated with the asset.



Provide the following attributes associated with the asset:

- **Connection type:** You can specify what type of connection the asset will be connected with from the options available in the drop-down.

If you choose RDP, SSH, or Telnet, Securden will use the default ports 3389, 22, and 23 respectively. If you want to use a different port, specify that along with the IP address in the following format <ipaddress>:<port>. For SQL connections, you can either enter the SQL server instance name or the IP address and port in <ipaddress>:<port> format.

Note: For SSH connections, you have the additional option to include the domain name while launching a connection.

- **Asset Identifier:** Enter a name for the IT asset being added in this field. This helps in uniquely identifying the asset for launching remote connections.
- **IP address:** Finally, specify the IP address of the asset.

Import Assets from AD

The other option is to import the required IT assets from the Active Directory domain. You can import select devices, OUs, or Groups in any manner as needed. To import assets, click “**Import Assets from AD**”. The import is a two-step process.

Step 1: Establish connectivity

Securden scans your Active Directory domain and obtains the OUs, Groups and computers in the domain. It fetches the computer objects and adds them here as assets for launching RDP connections.

To establish connectivity with your domain you need to specify the following:

Domain: Select from an active directory domain added in securden

Domain IP address: Enter the IP address or the FQDN of the domain

Remote gateway (Optional): You can choose to route the connection with the domain using a remote gateway added in Securden. If you wish to add a new remote gateway, navigate to **Admin >> Remote Sessions and Recordings >> Remote Gateway**

Connection Mode: You can specify if you wish to connect securely using an SSL connection by clicking the checkbox.

Administrator Credentials: You need to supply the administrator credentials which will be used to connect to the domain and authenticate.

You can either enter the username and password of the account which will be used to connect to the domain, or alternatively select an account already added to Securden.

On completion, click **Next**

The page that appears will allow you to select the OUs/Groups/Computers from the domain. You can search and select the required assets and add them to Securden.

Once you complete the step 2 above, the imported IT assets will appear in the list on the page **Admin >> Remote Sessions and Recordings >> Assets for Remote Connections**.

As previously mentioned, the assets added here need to be associated with the required domain accounts. Typically, the asset is associated with specific users/user groups and accounts/folders in Securden.

This can be done from Admin >> Remote Sessions and Recordings >> Domain Account - Assets Association. Once the association is made, the asset will appear in the list of remote session launch options for the specific domain account for the specific users.

Domain Accounts - Asset Associations

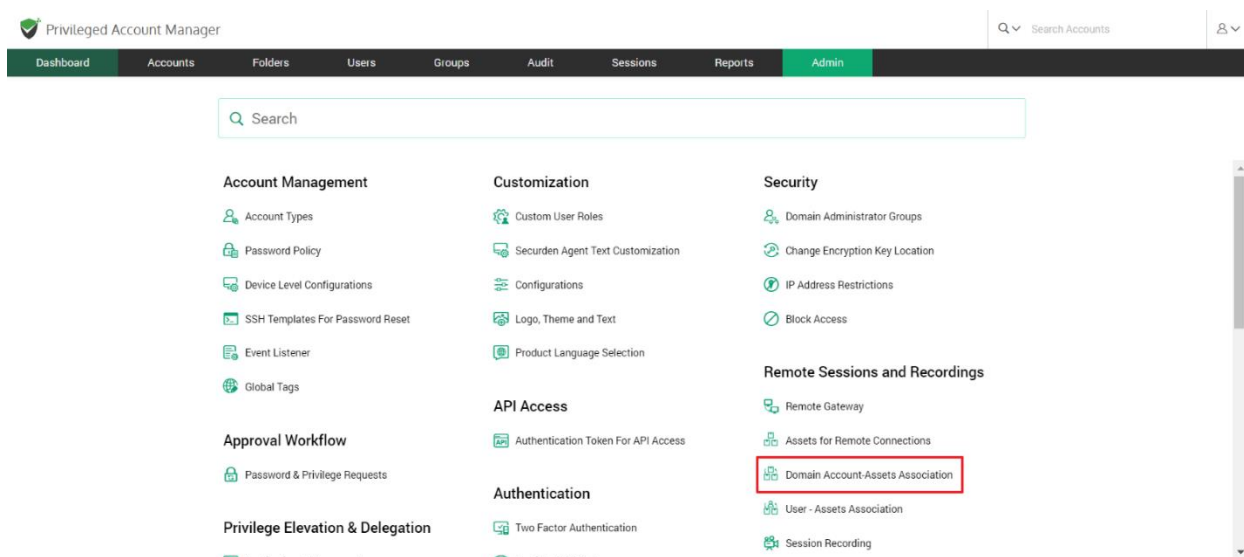
If any domain account is used to remotely connect to multiple IT assets, creating an association between the domain accounts and the list of IT assets it could connect to, becomes necessary.

Typically, an asset is associated with specific users/user groups and accounts/folders in Securden. That means, you will specify 'who' can launch a remote connection to 'what' asset using 'which' domain account.

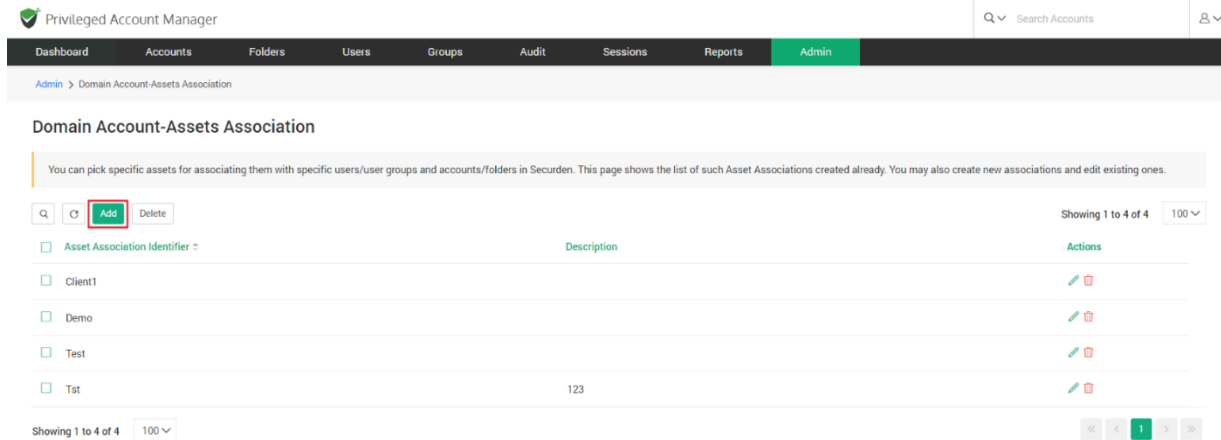
Once the association is made, the asset will appear in the list of remote session launch options for the specific domain account for the specific users. You can create any number of such associations from this section.

Adding Asset Associations

To add a new asset association configuration, navigate to **Admin >> Remote Sessions and Recordings >> Domain Account - Asset Association**



In the GUI that opens, all added domain-asset associations will be listed. You can choose to add a new association. Click on **Add**.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Domain Account-Assets Association

Domain Account-Assets Association

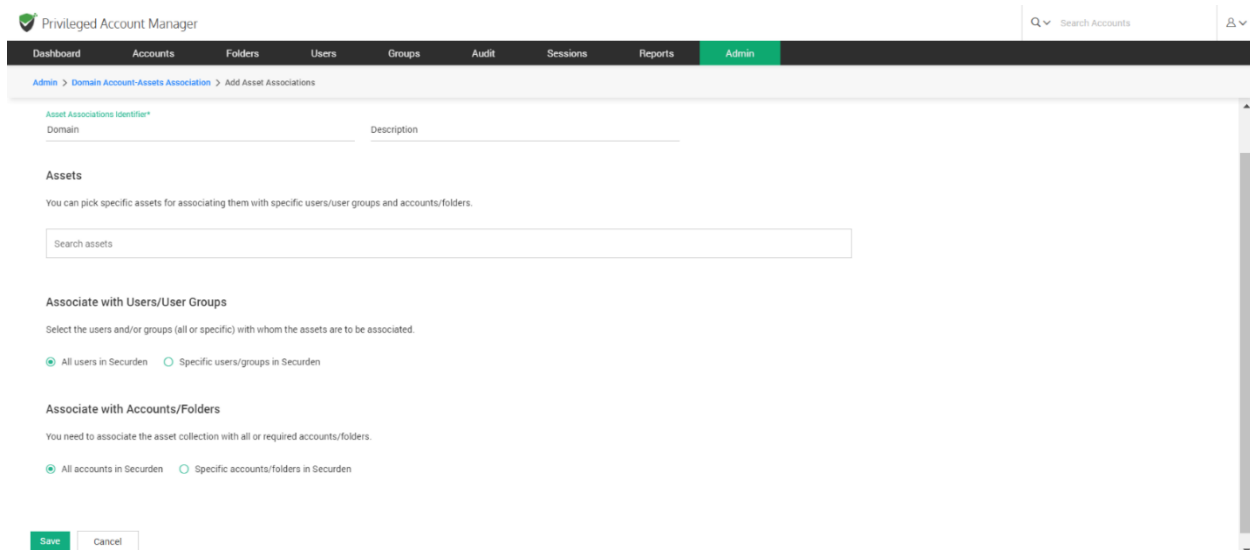
You can pick specific assets for associating them with specific users/user groups and accounts/folders in Securden. This page shows the list of such Asset Associations created already. You may also create new associations and edit existing ones.

Q **Add** Delete

Asset Association Identifier	Description	Actions
Client1		
Demo		
Test		
Tst	123	

Showing 1 to 4 of 4 100

In the GUI that opens, you need to fill in certain attributes – like an identification name for the association etc.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Domain Account-Assets Association > Add Asset Associations

Asset Associations Identifier* Description

Domain

Assets

You can pick specific assets for associating them with specific users/user groups and accounts/folders.

Search assets

Associate with Users/User Groups

Select the users and/or groups (all or specific) with whom the assets are to be associated.

☒ All users in Securden ☐ Specific users/groups in Securden

Associate with Accounts/Folders

You need to associate the asset collection with all or required accounts/folders.

☒ All accounts in Securden ☐ Specific accounts/folders in Securden

Save Cancel

The fields to be filled are explained below:

Asset Association Identifier - Provide a name for the new mapping being created. The name you enter here helps uniquely identify the asset-account association.

Description - Provide a Description for this association.

Select the Assets - You can pick one or more assets for associating them with specific users/user groups and accounts/folders.

Securden will display all the Assets that were already added in the drop-down list in the field under “Assets”. Search the drop-down and add the asset you want to associate with the Users/User groups and Accounts/Folders. You can select any number of assets.

The screenshot displays the 'Privileged Account Manager' interface. The top navigation bar includes links for Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin (which is currently selected). Below the navigation bar, the breadcrumb trail reads: Admin > Domain Account-Assets Association > Add Asset Associations. The main form area is titled 'Asset Associations Identifier*' and contains a table with two columns: 'Domain' and 'Description'. Below this table, there is a section titled 'Assets' with the instruction: 'You can pick specific assets for associating them with specific users/user groups and accounts/folders.' This section includes a search bar with the text 'Office Desktop', 'SEC-2K12-1.SECURDEN.AWS.COM', and a 'Search assets' button. To the right of the search bar is a 'Clear All' button. Below the 'Assets' section, there are two sections: 'Associate with Users/User Groups' and 'Associate with Accounts/Folders'. Each section has a radio button option for 'All' and 'Specific' users/accounts/folders in Securden. At the bottom of the form, there are 'Save' and 'Cancel' buttons.

Associate with User/User Groups

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Domain Account-Assets Association > Add Asset Associations

Assets

You can pick specific assets for associating them with specific users/user groups and accounts/folders.

Office Desktop SEC-2K12-1.SECURDEN.AWS.COM Search assets Clear All

Associate with Users/User Groups

Select the users and/or groups (all or specific) with whom the assets are to be associated.

☐ All users in Securden ☒ Specific users/groups in Securden Clear All

Administrator (Administrator) Josh Fraser (Josh) Search user/group

Associate with Accounts/Folders

You need to associate the asset collection with all or required accounts/folders.

☒ All accounts in Securden ☐ Specific accounts/folders in Securden

Save Cancel

You can choose to associate the selected assets with all the users and groups in Securden by selecting the option **All users in Securden**. You can also associate the assets with specific users and groups by selecting the option **Specific users/groups in Securden**.

If you select **Specific users/groups in Securden**, all the users and groups present in Securden will be displayed in the drop-down list. Search and add all the users and groups you want to associate with the selected assets.

Associate with Accounts/Folders

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Domain Account Assets Association > Add Asset Associations

You can pick specific assets for associating them with specific users/user groups and accounts/folders.

Office Desktop x SEC-2K12-1.SECURDEN.AWS.COM x Search assets Clear All

Associate with Users/User Groups

Select the users and/or groups (all or specific) with whom the assets are to be associated.

☐ All users in Securden ☒ Specific users/groups in Securden Clear All

Administrator (Administrator) x Josh Fraser (Josh) x Search user/group

Associate with Accounts/Folders

You need to associate the asset collection with all or required accounts/folders.

☐ All accounts in Securden ☒ Specific accounts/folders in Securden Clear All

Databases x Cisco Routers x Search account/folder

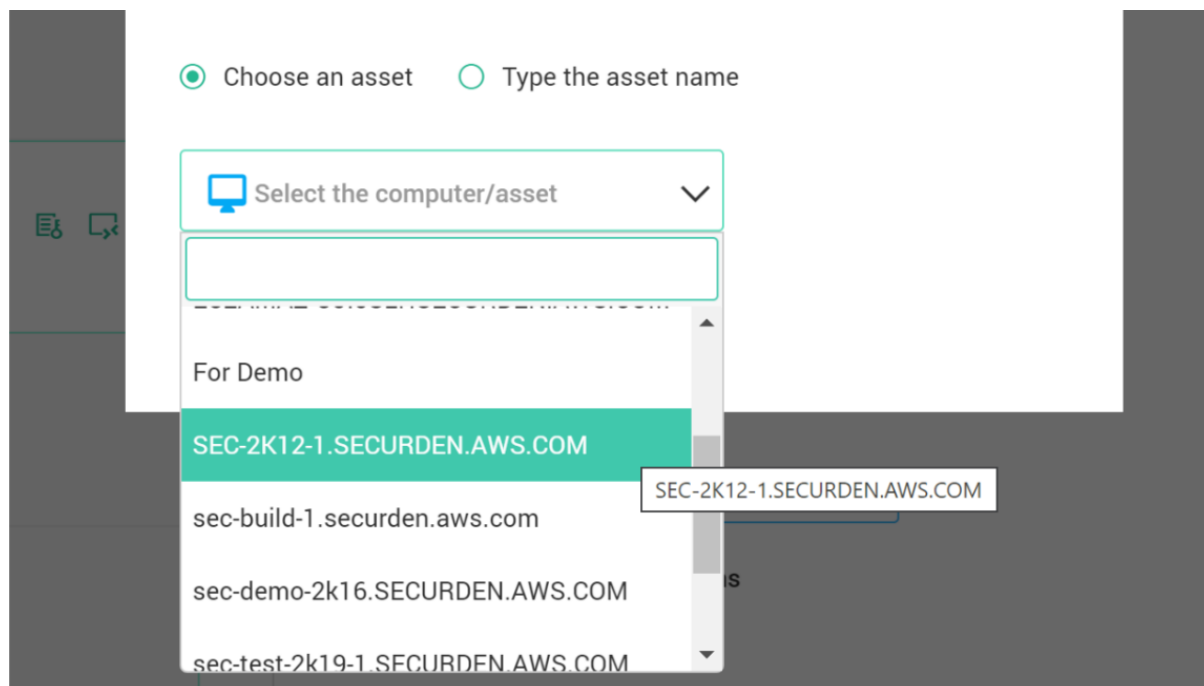
Save Cancel

The final step in the association process is to link the assets and users/groups selected above with the required accounts/folders.

You can choose to associate the selected assets with all the accounts and folders in Securden by selecting the option **All accounts in Securden**. You can also associate the assets with specific accounts and folders by selecting the option **Specific Accounts/Folders in Securden**.

If you select **Specific accounts/folders in Securden**, all the accounts and folders present in Securden will be displayed in the drop-down list. Search and add all the accounts and folders you want to associate with the selected assets. Once you've associated the selected assets with users/accounts, click **Save**.

Once this association is completed, when launching a connection using a domain account, the associated asset will appear in the drop-down as shown below:

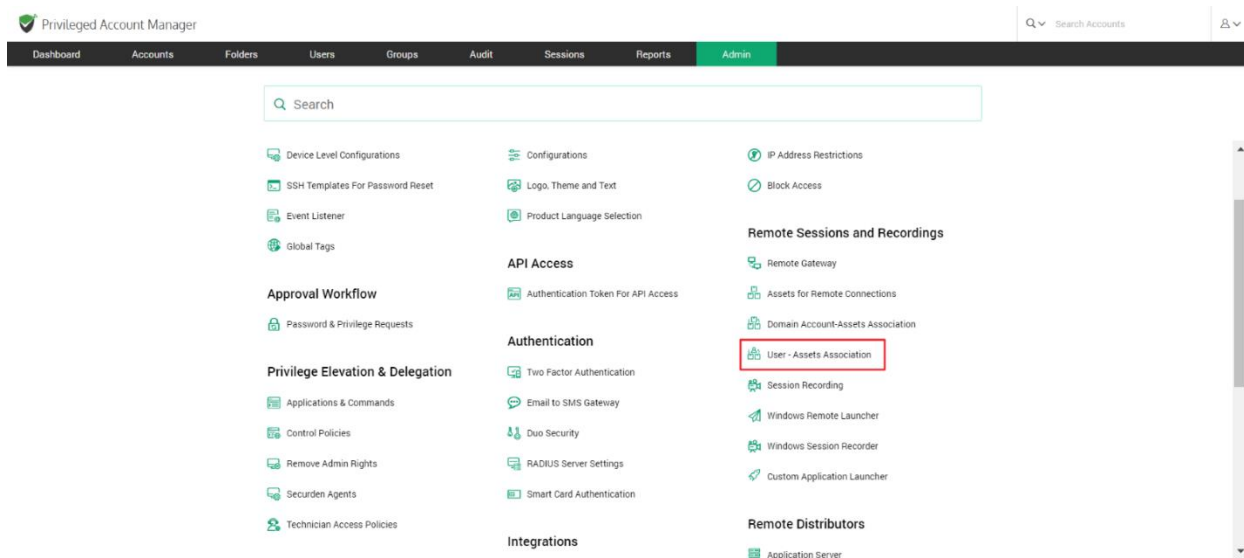


User – Assets/Application Association

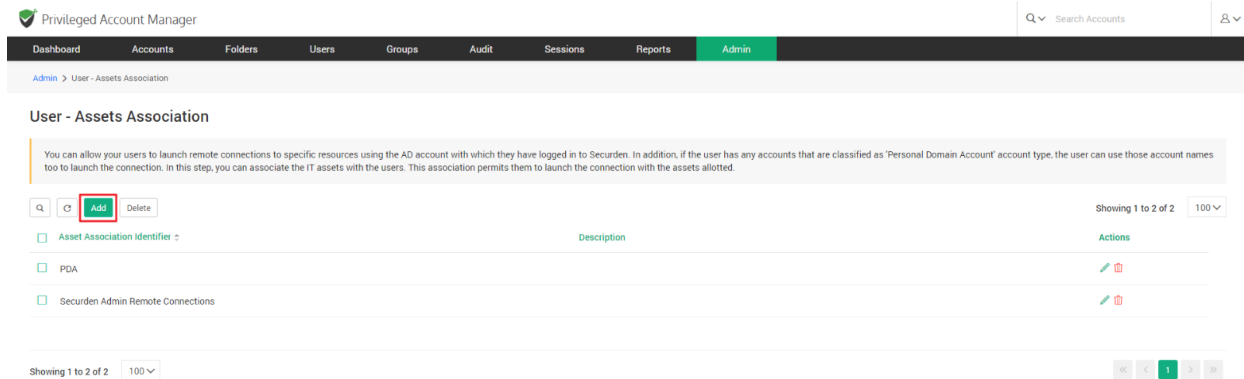
You can allow your users to launch remote connections to specific resources using the AD account with which they have logged in to Securden. In addition, if the user has any accounts that are classified as 'Personal Domain Account' account type, the user can use those account names too to launch the connection. In this step, you can associate the IT assets with the users. This association permits them to launch the connection with the assets allotted.

Additionally, you can also associate the applications with the users. This association permits them to launch the connection with the thick client applications allotted.

To associate assets/applications with users, navigate to **Admin >> Remote Sessions and Recordings >> User – Assets/Applications Association**



In the GUI that opens, click on **Add** to add a new user-asset/app association.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > User - Assets Association

User - Assets Association

You can allow your users to launch remote connections to specific resources using the AD account with which they have logged in to Securden. In addition, if the user has any accounts that are classified as 'Personal Domain Account' account type, the user can use those account names too to launch the connection. In this step, you can associate the IT assets with the users. This association permits them to launch the connection with the assets allotted.

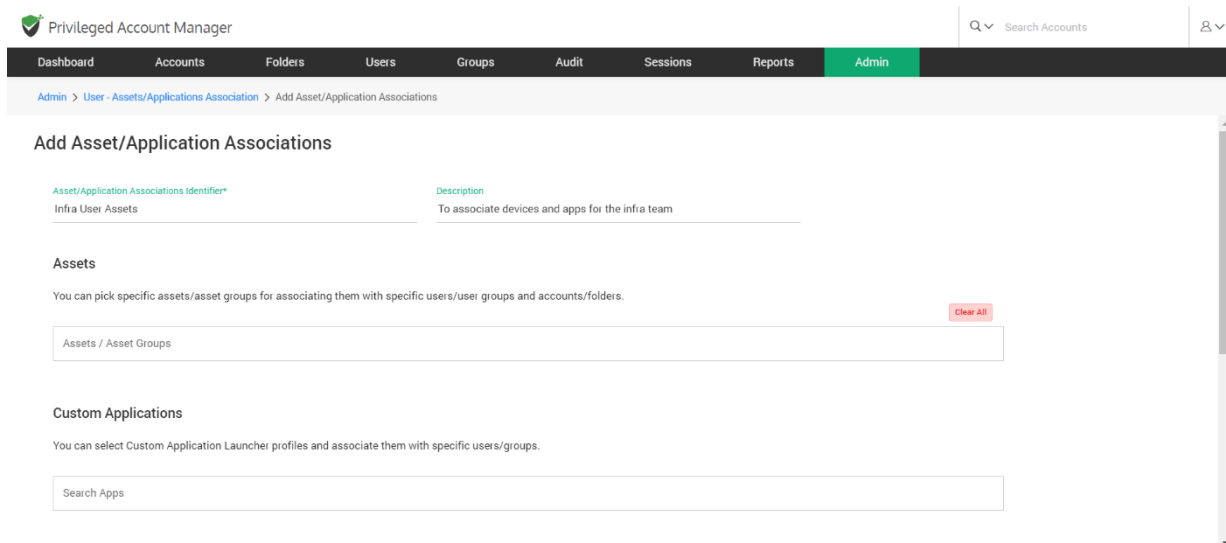
Q C **Add** Delete

Showing 1 to 2 of 2 100

Asset Association Identifier	Description	Actions
PDA		
Securden Admin Remote Connections		

Showing 1 to 2 of 2 100

In the page that opens, you can associate assets with users the same way assets were associated with domain accounts.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > User - Assets/Applications Association > Add Asset/Application Associations

Add Asset/Application Associations

Asset/Application Associations Identifier* Description

Infra User Assets To associate devices and apps for the infra team

Assets

You can pick specific assets/asset groups for associating them with specific users/user groups and accounts/folders.

Assets / Asset Groups Clear All

Custom Applications

You can select Custom Application Launcher profiles and associate them with specific users/groups.

Search Apps

You need to enter the following details on the page:

Asset Association Identifier - Provide a name for the new mapping being created. The name you enter here helps uniquely identify the asset-account association.

Description - Provide a Description for this association.

Select the Assets - You can pick one or more assets for associating them with specific users/user groups and accounts/folders.

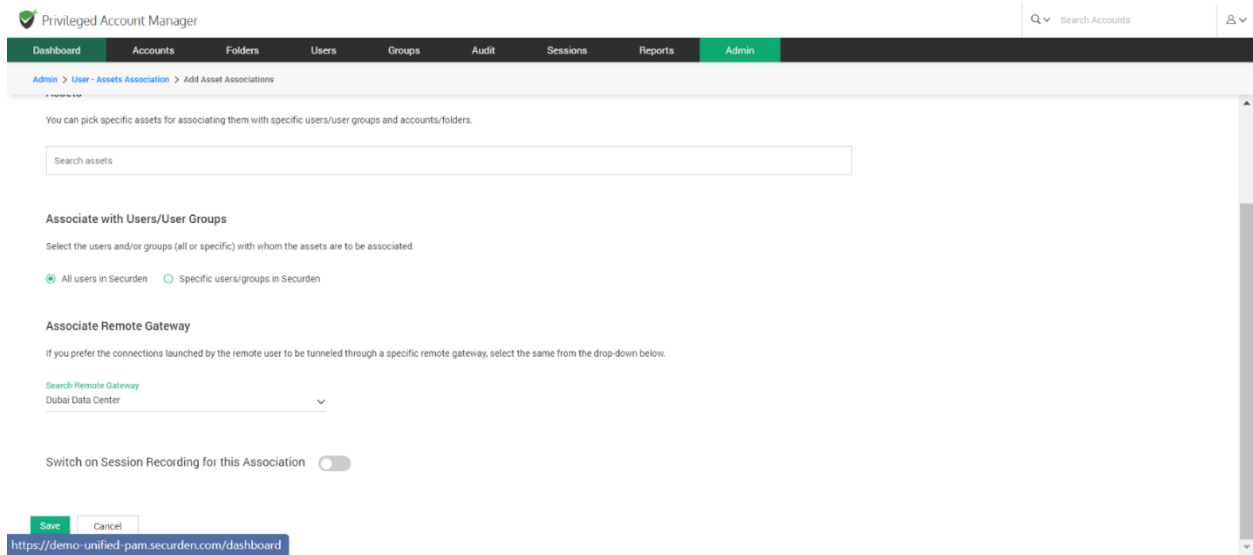
Securden will display all the Assets that were already added in the drop-down list in the field under **Assets**. Search the drop-down and add the asset you want to associate with the Users/User groups and Accounts/Folders. You can select any number of assets.

Select the Custom Applications - You can pick one or more custom applications for associating them with specific users/user groups and accounts/folders.

Pre-requisite: You should have added custom app launcher profiles under **Admin >> Remote sessions and recordings >> Custom application launcher**.

Search the drop-down and add the application you want to associate with the Users/User groups and Accounts/Folders. You can select any number of custom applications.

Associate a remote gateway – You can choose to tunnel the connections launched by the remote user through a specific remote gateway, select the same from the drop-down on the page.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > User - Assets Association > Add Asset Associations

You can pick specific assets for associating them with specific users/user groups and accounts/folders.

Search assets

Associate with Users/User Groups

Select the users and/or groups (all or specific) with whom the assets are to be associated.

☒ All users in Securden ☐ Specific users/groups in Securden

Associate Remote Gateway

If you prefer the connections launched by the remote user to be tunneled through a specific remote gateway, select the same from the drop-down below.

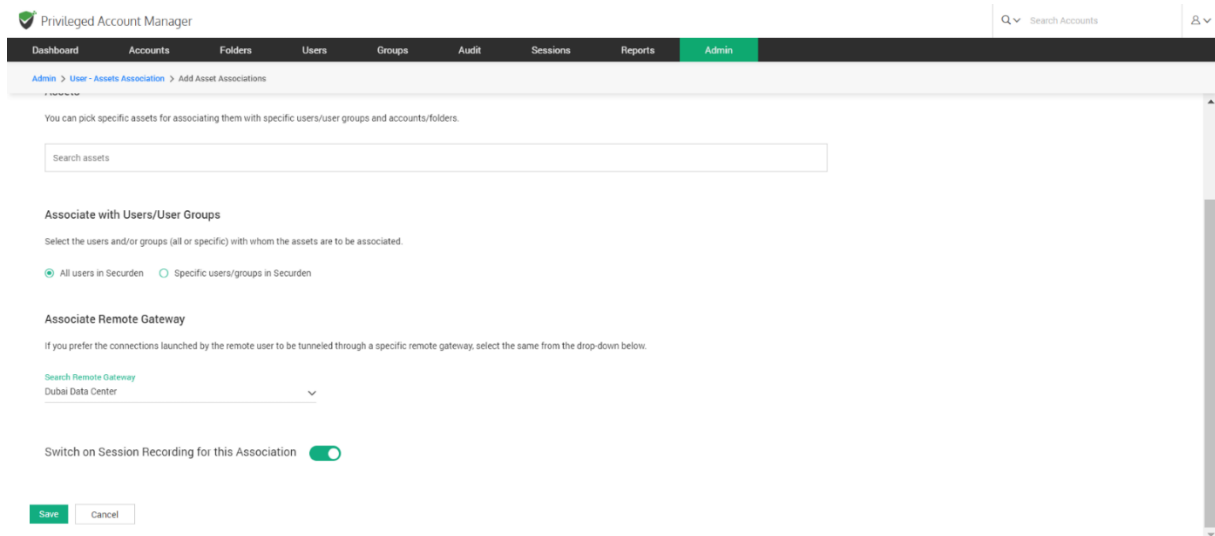
Search Remote Gateway
Dubai Data Center

Switch on Session Recording for this Association ☐

Save Cancel

<https://demo-unified-pam.securden.com/dashboard>

You have the option to record all the sessions launched using the associated remote gateway by the selected users. Enable the switch if you wish to do so.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > User - Assets Association > Add Asset Associations

You can pick specific assets for associating them with specific users/user groups and accounts/folders.

Search assets

Associate with Users/User Groups

Select the users and/or groups (all or specific) with whom the assets are to be associated.

☒ All users in Securden ☐ Specific users/groups in Securden

Associate Remote Gateway

If you prefer the connections launched by the remote user to be tunneled through a specific remote gateway, select the same from the drop-down below.

Search Remote Gateway
Dubai Data Center

Switch on Session Recording for this Association ☒

Save Cancel

On filling all the fields, click **Save**.

Custom Application Launcher

Securden facilitates launching connections with remote IT assets and applications. In addition to the default modes of launching web-based connections and through native clients, you can define custom application launchers to supply/autofill credentials and automatically launch any application, including thick application clients.

Creating a custom launcher basically involves creating a profile for each such application capturing the input fields as found in the target application. The profile will have placeholders to replace the required values from Securden repository at the time of launching the connections.

To create/configure the application launcher profile, navigate to **Admin >> Remote Sessions and Recordings >> Custom Application Launcher**.

In the page that opens, you can create new app launcher profiles or configure existing launcher profiles.

Create an app launcher profile

To create a new application launcher profile, click on **Add App Launcher Profile**.

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Custom Application Launcher

Custom Application Launcher

Securden facilitates launching connections with remote IT assets and applications. In addition to the default modes of launching web-based connections and through native clients, you can define custom application launchers to supply credentials and automatically launch any application, including thick application clients. Basically, you will be creating a profile for each such application capturing the input fields as found in the target application. The profile will have placeholders to replace the required values from Securden repository at the time of launching the connections.

Q Add App Launcher Profile Delete

Showing 1 to 1 of 1 25

Launcher profile	Description	Status
Zoom	Launch zoom from Securden	Active

Showing 1 to 1 of 1 25

Securden requires various details related to the application for which the profile is being created.

Typically, you need to know the exact name of the data input form (as appearing on the Window), the order of the input data fields, and the type of those fields. Once you have these details in hand, you may proceed to create the profile.

Privileged Account Manager

Q Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Custom Application Launcher > Add Application

Add Application Launcher Profile

You need to create a profile for each application to be launched from Securden GUI. Specify the name of the application, the file path where it is located, and the exact order in which the application expects input/credentials to launch connections. You may make use of placeholders to fetch data (like account name, password, domain name etc.) at runtime from Securden database.

Application Profile Name* DBVisualizer

Description To launch DBViz from Securden

Authentication Type ⓘ

☐ Authenticate using Account Credentials ☐ Authenticate using User Credentials

Application Launch Type

☐ Native App ☐ Custom App ☐ Open App ☐ Autofill on next window ☐ Google Chrome ☐ Microsoft Edge

Help ⓘ

Securden requires various details related to the application for which the profile is being created. Typically, you need to know the exact name of the data input form (as appearing on the Window), the order of the input data fields, and the type of those fields. Once you have these details handy, you may proceed creating the profile.

Application Profile Name

Helps uniquely identify the application profile.

Application Launch Type

The type of application for which you are creating this launcher profile. You may create this profile for native applications, and custom applications as required. If neither option is selected, launching a connection will simply launch the application file.

Native App - You can use this option to launch applications that are built using languages specific to Windows. These include C#, Visual Basic. These apps are designed to specifically run on Windows platforms.

In the GUI that opens, the following fields need to be filled:

Application Profile Name: The name that you enter here helps you uniquely identify the application profile being created. This name will appear on the remote connection launching section in Securden. Your users will identify the launch option through this name.

Description (Optional): A brief of the app launcher for a quick overview, this could explain the purpose of this launcher profile.

Authentication Type

- Authenticate using Account Credentials

If you select this option, you need to specify the account types for which this custom application launcher profile is applicable. Once the profile is created, it will be automatically added to the list of available connections for all accounts of the selected type and the account credentials will be used for authentication

- Authenticate using User Credentials

Once the application launcher profile is created, it should be associated with the required users. Credentials of the associated user will be used for authentication. To associate the profile, navigate to **Admin >> Remote Sessions and Recordings >> User - Assets/Applications Association**

Once you have filled these fields, you need to select an **Application Launch Type**

The screenshot shows the 'Add Application Launcher Profile' form in the Securden Privileged Account Manager. The form includes a navigation bar with tabs for Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin. The 'Admin' tab is selected. The form has a breadcrumb trail: Admin > Custom Application Launcher > Add Application. The main form area is titled 'Add Application Launcher Profile' and contains a description: 'You need to create a profile for each application to be launched from Securden GUI. Specify the name of the application, the file path where it is located, and the exact order in which the application expects input/credentials to launch connections. You may make use of placeholders to fetch data (like account name, password, domain name etc.) at runtime from Securden database.' The form fields include: 'Application Profile Name*' (with a sub-label 'App Profile A'), 'Description', 'Application Launch Type' (with radio buttons for Native App, Custom App, Open App, Autofill on next window, Google Chrome, and Microsoft Edge), 'Application Identifier / Application file path*', 'Arguments', 'Input Form Name*', 'Total Time Delay for Filling Data (in milli seconds)*', a checkbox for 'Take connections through Remote Gateway', 'Account Type *', and a 'Search Account Type' field. A help sidebar on the right provides information about placeholders and application profile names.

Help

Securden requires various details related to the application for which the profile is being created. Typically, you need to know the exact name of the data input form (as appearing on the Window), the order of the input data fields, and the type of those fields. Once you have these details handy, you may proceed creating the profile.

Place Holders

You may use the following placeholders for replacing the attributes in the respective field name in application login page. Additional fields associated with an account type can also be given a placeholder.

- {%ACCOUNT_NAME%} - Account name
- {%ACCOUNT_PASSWORD%} - Password
- {%ACCOUNT_ADDRESS%} - Address
- {%ACCOUNT_TOTP%} - TOTP (if configured).
- {%FOLDER_NAME%} - Folder name
- {%DOMAIN_NAME%} - Domain name
- {%NETBIOS_NAME%} - Netbios
- {%DISTINGUISHED_NAME%} - Distinguished name

Application Profile Name

Helps uniquely identify the application profile.

Application Identifier

Helps uniquely identify the application for launching connections in the GUI.

This is the type of application for which you are creating this launcher profile. You may create this profile for native applications, custom applications or explore other options as required.

- Native Applications:** Generally, Windows applications possessing one or more drop-downs, text-boxes, password fields and action buttons are called native applications in Securden. Securden can easily identify the fields of native windows apps. If you are familiar with the exact values the fields in your application would hold, you may select the option **Native Apps**. SQL server studio is a typical example of a native app.

- **Custom Applications:** Applications that have a more complex field pattern can be classified as custom applications. Zoom, Skype, any other app/web-app are examples of custom applications.
- **Open Application:** If you wish to simply launch/open an application without needing to input credentials and other fields in it, you may select the option **Open App**.
- **Autofill on next window:** If you want to autofill credentials on active applications, you can select the checkbox Autofill in the next active application. Although, while launching a connection using this method, applications will not be launched. Instead, Securden will autofill credentials in the next active application window (the window that opens when you press Alt+Tab). You need to ensure that the appropriate window is manually launched beforehand and is the next active window.

Important Note: The autofill option simply changes the input focus to the next active application regardless of its type and autofill the credentials. For example, if the next active application happens to be a notepad, it will autofill the credentials there too. So, exercise care in selecting this option. If you are granting access with 'Open Connection' permission to an account, enabling this option may result in auto-filling credentials (in plain text) on any application and might potentially reveal the credentials.

- **Google Chrome/Microsoft Edge:** If you wish to launch a chrome or edge browser you can select this option. Securden auto-fills the fields known for the Chrome/Edge profile so you can fill the rest with ease.

Application Identifier/Application file path: This is an important configuration parameter. You need to specify the name of the custom application you want to launch (for example, test.exe. The application should be in the system path) OR the exact file path of the application (for example, C:\example\testapp.exe). This application should be available on all the client machines from which users would try to launch the application from Securden.

Arguments (Optional): If the application requires any arguments to be passed for launch, you may enter the same here. For example, some applications might require IP addresses to launch the application. In such cases, you may pass the required value as an argument as shown below:

/h {%ACCOUNT_ADDRESS%}

Input form name: Exact name of the data input form of the application (as appearing on the Window)

Time Delay for Filling Data: While launching connections, the application might take time to launch. To handle such scenarios, you can configure time delay in milliseconds for Securden to start filling the data.

Account Type: This represents the **Account Type** in Securden. The custom profile being created, will be applicable only for the selected account type.

Creating a native app launcher profile

Native app launcher profiles will require you to fill in the order of input data fields and enter the field value. Each input action has to be defined according to the order in which they will be filled.

The screenshot displays the 'Add Application' configuration page in the Securden Privileged Account Manager. The interface includes a top navigation bar with tabs like Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin. The 'Admin' tab is active. Below the navigation bar, the breadcrumb trail shows 'Admin > Custom Application Launcher > Add Application'.

The main configuration area is titled 'Account Type' and includes a search bar with 'Web Account' selected. Below this, the 'Application Launch Type' is set to 'Native App' (indicated by a selected radio button). The 'Input Data Order' section contains a table with three rows of input fields:

Field Type	Field Name	Element Selection	Time Delay (in milliseconds)
Drop Down	Select Server	1	2000
Text Box	Server Name	Field Value (%ACCOUNT_NAME%)	3000
Password	Credential	Field Value (%ACCOUNT_PASSWORD%)	

Below the table, there is an 'Add Fields' button and 'Save' and 'Cancel' buttons. On the right side of the interface, there is a help panel with sections: 'Helps uniquely identify the application for launching connections in the GUI.', 'Arguments', 'Input Form Name', 'Time Delay for Filling Data', 'Account Type', 'Application Launch Type', and 'Take connections through Remote Gateway'.

The steps to follow while entering each input action is as follows:

- Firstly, select the field type – this can either be a text field, a button, a password or a drop-down.
- Then, enter the name of the field that appears on the application.
- Specify Field Value and Select Element

If the field type in your application form is of the type **Drop Down** you will have to take care of **Element Selection**.

Element Selection for drop-down allows you to select the entries from the drop-down. If you enter the element value as '0', the first entry in the drop down will be selected. 1 will choose the second entry and so on.

If the field type in your application form is of the type **Text-box** you will have to take care of **Specify Value**.

In the case of text fields, you can specify the value to be filled in for the specific input field. It could be the account name, password, or any other value. When specifying the value, you have the option to use placeholders as explained below.

The values for the placeholders will be taken by Securden at runtime:

You may use placeholders for replacing the attributes in the respective field name in application login page.

{%ACCOUNT_NAME%} - to be replaced with the respective "Account name" at runtime

{%ACCOUNT_PASSWORD%} - to be replaced with the account's password at runtime

{%ACCOUNT_ADDRESS%} - to be replaced with the respective account's "IP Address" at runtime

{%ACCOUNT_TOTP%} - to be replaced with the respective account TOTP token at runtime (if configured)

{%DOMAIN_NAME%} - to be replaced with the domain name of the mentioned account

{%NETBIOS_NAME%} - to be replaced with the NetBIOS name of the account mentioned.

- Specify **Time delay**

Wherever you want Securden to wait for a few milliseconds before filling the respective data while launching the application, you may add **Time Delay** in milliseconds.

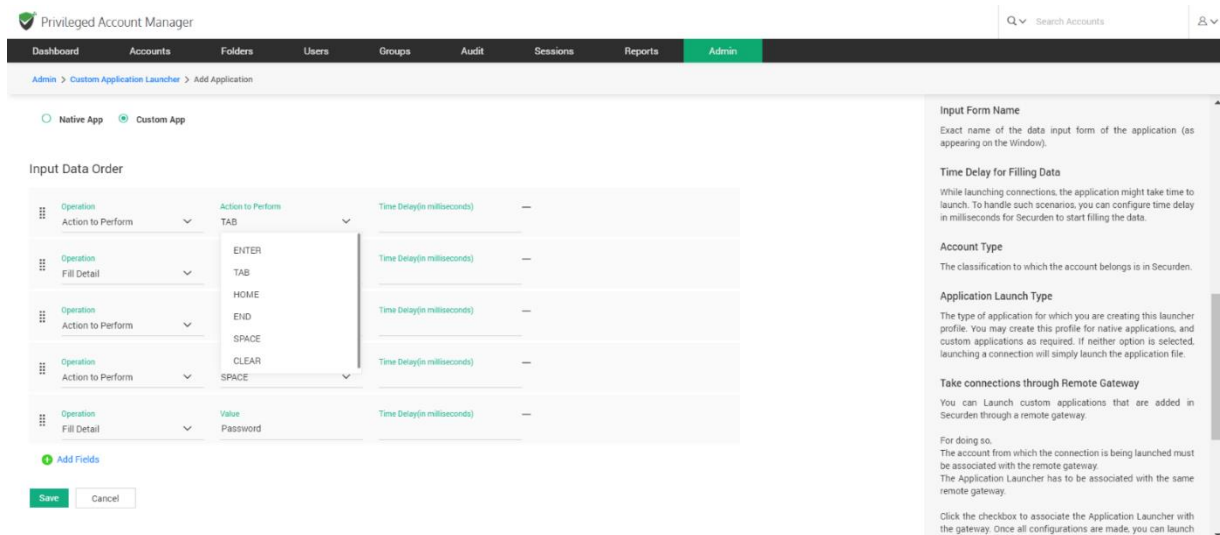
Once you have defined the Input Data Order, click **Save** to add the native app launcher profile in Securden. The native application can now be directly launched from Securden.

Creating a custom app launcher profile

Custom app launcher profiles require you to fill in the order of input data fields and enter the field value, similar to the native app launcher. Each input action has to be placed according to the order in which they will be filled in the application.

The steps to follow while entering the input data order is as follows:

- Firstly, select the **Action to Perform** - This lets you perform actions like clicking TAB, ENTER, SPACE etc. on the application.
- Then select the **Fill Detail** operation and specify the value that will be filled in after the selected action is performed.
- Repeat the input actions in the order that they will be carried out.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Custom Application Launcher > Add Application

☐ Native App ☒ Custom App

Input Data Order

Operation	Action to Perform	Time Delay (in milliseconds)
Operation	Action to Perform	Time Delay (in milliseconds)
Operation	Fill Detail	Time Delay (in milliseconds)
Operation	Action to Perform	Time Delay (in milliseconds)
Operation	Action to Perform	Time Delay (in milliseconds)
Operation	Fill Detail	Time Delay (in milliseconds)

[Add Fields](#)

Input Form Name

Exact name of the data input form of the application (as appearing on the Window).

Time Delay for Filling Data

While launching connections, the application might take time to launch. To handle such scenarios, you can configure time delay in milliseconds for Securden to start filling the data.

Account Type

The classification to which the account belongs is in Securden.

Application Launch Type

The type of application for which you are creating this launcher profile. You may create this profile for native applications, and custom applications as required. If neither option is selected, launching a connection will simply launch the application file.

Take connections through Remote Gateway

You can Launch custom applications that are added in Securden through a remote gateway.

For doing so, The account from which the connection is being launched must be associated with the remote gateway. The Application Launcher has to be associated with the same remote gateway.

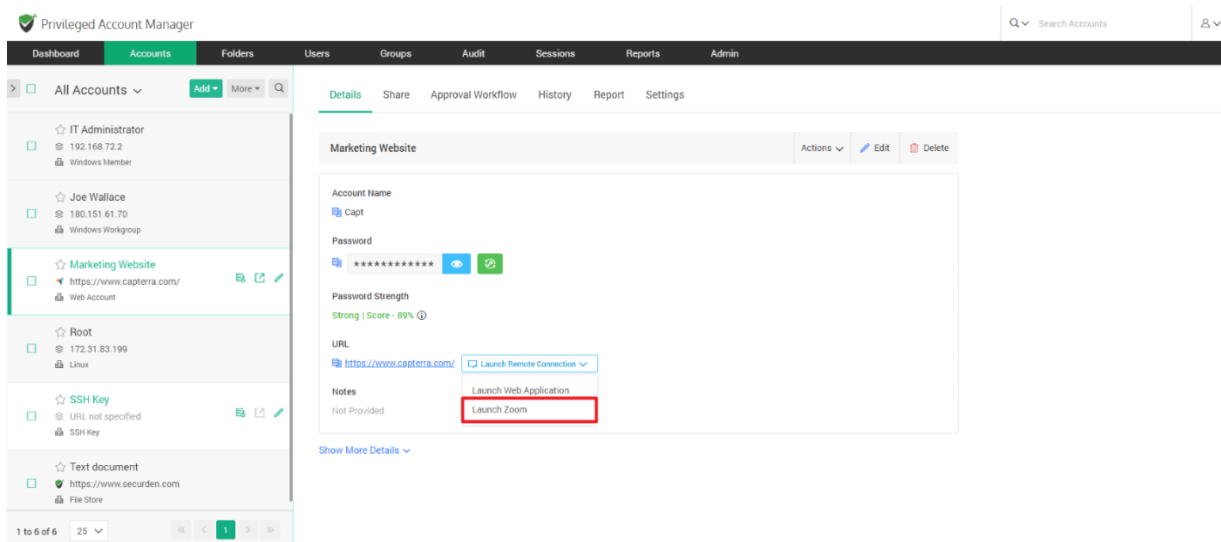
Click the checkbox to associate the Application Launcher with the gateway. Once all configurations are made, you can launch a custom application in the remote desktop client Privileged

You have to carry out these steps for each input action added to the launcher. Once you have defined the Input Data Order, click **Save** to add the custom

app launcher profile in Securden. The custom application can now be directly launched from Securden.

Launching Remote Connections Using the Custom Launcher

Once you create the app launcher profile, the custom app launcher will be available in the remote access drop-down for accounts with the specified account type.



You can click that and directly launch the connection.

Take connections through Remote Gateway

You can launch custom applications that are added in Securden through a remote gateway. As a pre-requisite, the account from which the connection is being launched must be associated with a remote gateway.

Click the checkbox **Take connections through the remote gateway**.

The screenshot shows the 'Add Application' form in the Securden Privileged Account Manager. The 'Take connections through Remote Gateway' checkbox is highlighted with a red box. The form includes the following fields and sections:

- Application Profile Name***: Dvill app launcher
- Description**: (Empty text area)
- Application Launch Type**:
 - ☐ Native App
 - ☐ Custom App
 - ☐ Open App
 - ☐ Autofill on next window
 - ☒ Google Chrome
 - ☐ Microsoft Edge
- Application Identifier / Application file path***: C:\Program Files\Google\Chrome\Application\chrome.exe
- Input Form Name***: Untitled - Google Chrome (Incognito)
- Total Time Delay for Filling Data (in milliseconds)***: (Empty text area)
- Take connections through Remote Gateway**: ☒ (highlighted with a red box)
- Account Type ***: (Empty text area)
- Input Data Order**:

Operation	Action to Perform	Operation Time Delay (in milliseconds)
Action to Perform	TAB	

On the right side, there is a 'Place Holders' section with a list of placeholders for replacing attributes in the application login page:

- {%ACCOUNT_NAME%} - Account name
- {%ACCOUNT_PASSWORD%} - Password
- {%ACCOUNT_ADDRESS%} - Address
- {%ACCOUNT_TOTP%} - TOTP (if configured)
- {%FOLDER_NAME%} - Folder name
- {%DOMAIN_NAME%} - Domain name
- {%NETBIOS_NAME%} - Netbios
- {%DISTINGUISHED_NAME%} - Distinguished name

Once all configurations are made, you can launch the custom application through the remote gateway. You can create a Remote Gateway from **Admin >> Remote Sessions and Recordings >> Remote Gateway**

Configure an existing app launcher profile

You have the option to clone, edit, or delete a previously created app launcher profile. This can be done using the action buttons highlighted below.

Privileged Account Manager

Q

Search Accounts

Dashboard

Accounts

Folders

Users

Groups

Audit

Sessions

Reports

Admin

Admin

Custom Application Launcher

Custom Application Launcher

Securden facilitates launching connections with remote IT assets and applications. In addition to the default modes of launching web-based connections and through native clients, you can define custom application launchers to supply credentials and automatically launch any application, including thick application clients. Basically, you will be creating a profile for each such application capturing the input fields as found in the target application. The profile will have placeholders to replace the required values from Securden repository at the time of launching the connections.

Q

C

Add App Launcher Profile

Delete

Showing 1 to 2 of 225

Launcher profile	Description	Status	
<input type="checkbox"/> Zoom		✓ Active	<div><div></div><div></div><div></div></div>
<input type="checkbox"/> Skype		✓ Active	<div><div></div><div></div><div></div></div>

Showing 1 to 2 of 225

<

<

1

>

>

Section 12: Privilege Elevation and Delegation (PEDM)

Privilege Elevation and Delegation helps in eliminating administrator rights on servers and endpoints. Instead of granting shared administrative access to servers, you can establish policy-based controls to allow standard users to access required servers.

Securden takes care of elevating the applications for standard users. Similarly, you can eliminate local administrator rights on endpoints and elevate applications for standard users. In Linux devices, you can allow users to run specific commands with SUDO privileges in Linux.

PEDM - Summary of Steps

1. Deploy the Securden agent on the servers, endpoints
2. Discover/add applications, processes, and commands
3. Create application control policies
4. Remove admin rights across endpoints

Step 1: Deploy Securden Agent on Computers

To elevate and delegate privileges, you need to deploy Securden agents on servers and endpoints. The agent takes care of elevating the pre-approved applications and processes for standard users. The agent also allows users to request temporary access to applications/ temporary full admin access.

Securden agent can be deployed in two ways:

You can deploy Securden agents on endpoints and servers either manually or in bulk using Group Policy Objects.

Agent for Windows Machines

Navigate to Admin >> Privilege Elevation and Delegation >> Securden Agents >> Install Windows Agent to download the agents for 32-bit, 64-bit MSI and install them manually in the remote machine.

Agent Installation Using GPO

1. Connect to the domain group policy editor (gpmc.msc from Domain Controller)
2. Select all the OUs/Groups that contain the computers (endpoints and servers) in which agents must be installed.
3. Create a GPO for the selected OUs/Groups
4. 4. Add InstallAgent.vbs as a startup script in the GPO with the following parameters:

MSIPATH = Location of the MSI file (accessible to all the endpoints and servers)

SERVER = Name of the host (FQDN / DNS) where Securden server is running

PORT = Securden server port

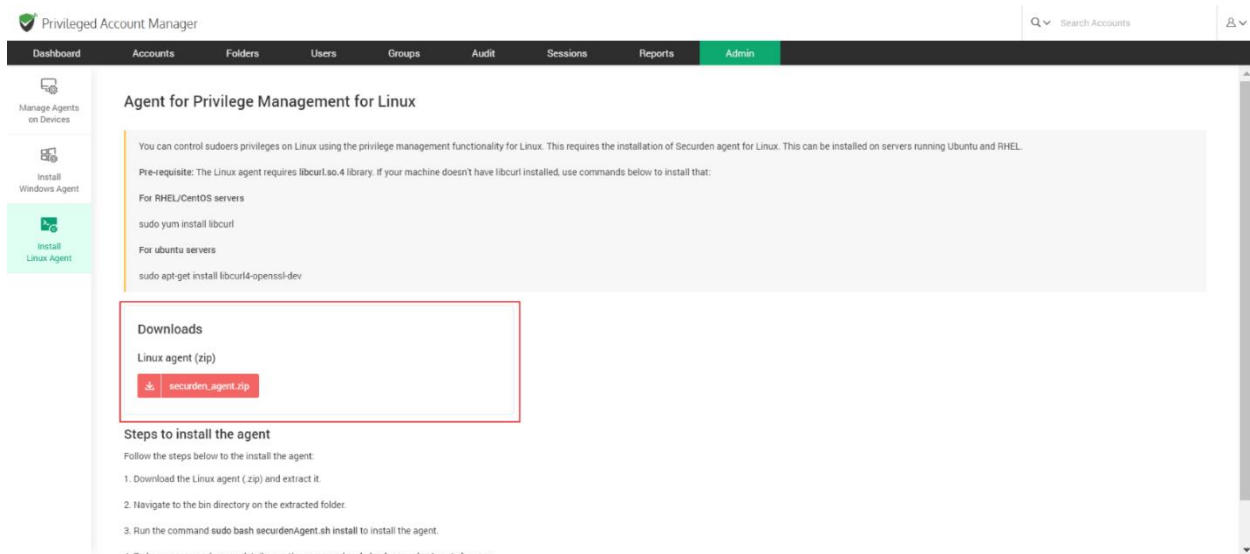
Example

```
/MSIPATH:"\\SECURDEN-SERVER\\Executable\\SecurdenAgent.msi"
/SERVER:"SECURDEN-SERVER" /PORT:"5151"
```

5. Securden Agent will be deployed on the computers (endpoints and servers) during the next restart.

Agent for Linux Machines

To install agents for Linux machines, click **Install LinuxAgent** and download the zip file.



Prerequisite: The Linux agent requires **libcurl.so.4** library. If your machine doesn't have libcurl installed, you may make use of the commands below to install that:

For RHEL/CentOS servers

sudo yum install libcurl

For ubuntu servers

sudo apt-get install libcurl4-openssl-dev

Steps to install the agent:

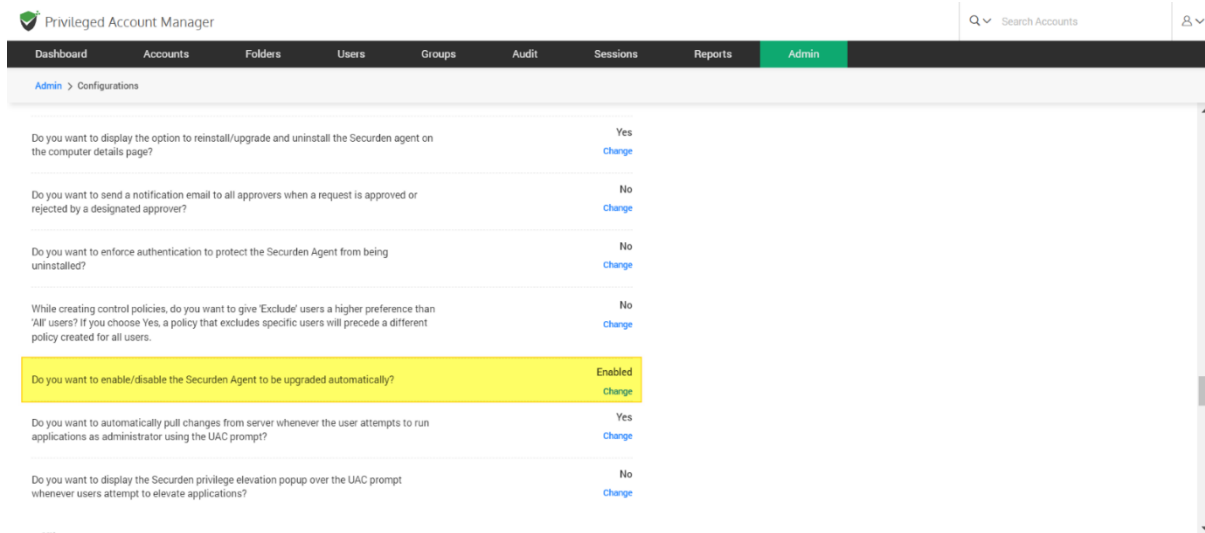
1. Download the Linux agent (.zip) and extract it.
2. Navigate to the bin directory on the extracted folder.
3. Run the command `sudo bash securdenAgent.sh install` to install the agent.
4. To know command usage details, run the command `sudo bash securdenAgent.sh usage`.

Upgrading the Securden Agent

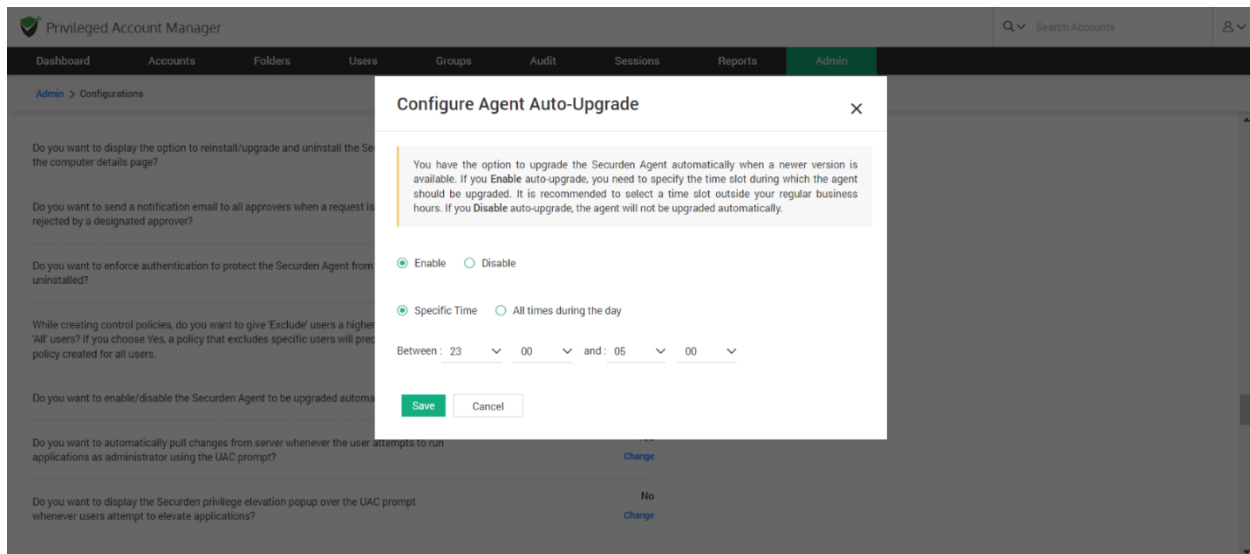
Once a new version of Securden Agent is available, Securden takes care of automatically upgrading the existing agent to the latest one.

As a pre-requisite, you need to have the agent version <xyz> or higher installed and have an active connection with the internet.

You have the provision enable/disable, auto-upgrades of the Securden agent. Navigate to Admin >> Configurations and select **Provision to auto-upgrade the Securden agent**



In the GUI that opens, you can enable the auto-upgrade feature and select a time slot outside business hours to perform the upgrade.



Once the endpoint connects to the server, it will automatically upgrade the agent and all privilege controls and policies are retained on the machine.

Step 2: Discover / Add Applications, Processes, Commands

The essential aspect of privilege elevation and delegation is elevating the privileges for applications (in Windows) and allowing users to run specific commands with SUDO privileges in Linux.

To ensure that least privilege enforcement does not impact productivity, Securden provides the application control feature. You can 'whitelist' the trusted applications that can be installed/run with elevated privileges by standard users. The term 'application' refers to any Windows process/executable. When you install the Securden agent on Windows endpoints and servers, the applications that normally require admin privileges are automatically discovered and added here. You can also add applications manually.

In the case of Linux, you need to add the commands that are allowed or not allowed to be run with SUDO privileges. You can review the list and add any other application or command that needs to be controlled.

There are two ways in which you can add applications (in Windows) to Securden:

1. Discovering and automatically adding applications

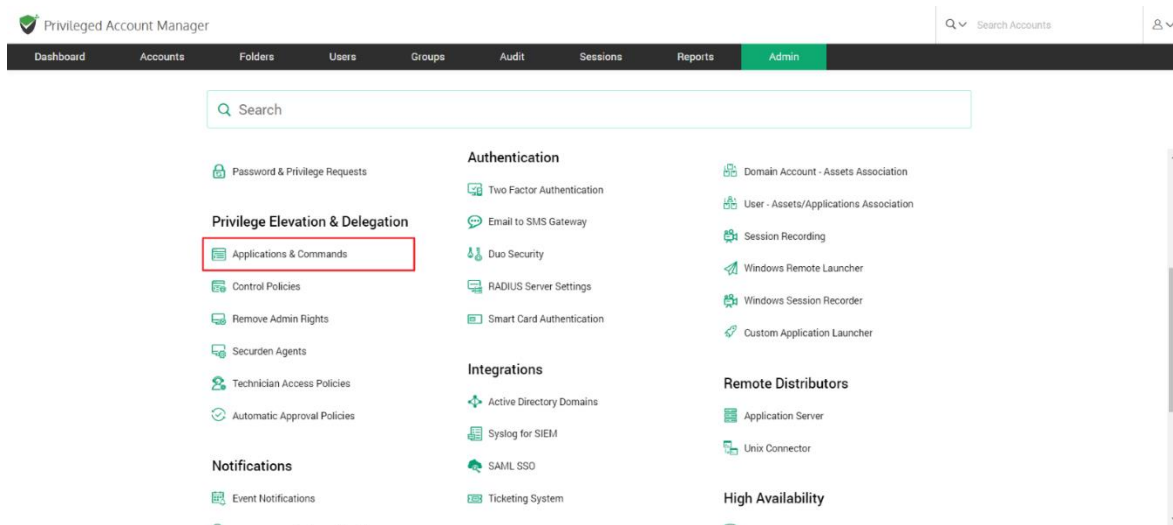
2. Manually adding applications

Automatic Discovery of Applications

When you install Securden agents on endpoints and servers, the agents automatically start discovering the applications running at that time on the computers and add them to the applications inventory.

However, the discovery process is not an instant one; applications are discovered over a period of time. Typically, it takes about a couple of weeks to complete the process. This is because the agent discovers and adds only the applications that require elevated privileges and not all processes/applications unnecessarily.

You can view the discovered applications in the **Admin >> Privilege Elevation and Delegation >> Applications and Commands** section.



In the GUI that opens, all discovered applications are listed.

Privileged Account Manager

Dashboard

Accounts

Folders

Users

Groups

Audit

Sessions

Reports

Admin

Admin > Applications & Commands

Applications and Commands for Privilege Elevation

The essential aspect of privilege elevation and delegation is temporarily elevating the privileges for applications (in Windows) and allowing users to run with specific commands SUDO privileges in Linux. This page serves as the inventory of all such applications and commands. When you install the Securdn agent on Windows endpoints and servers, the applications that normally require admin privileges are discovered and added here. You can also manually add applications. In the case of Linux, you need to add the commands that are to be allowed or not allowed to be run with SUDO privileges. You can review the list and add any other application or command that needs to be controlled. You can define the policy (how should they be elevated) as part of the 'Control Policies' section.

Note: When an existing application or command is edited by an administrator, the change has to be approved by one of the other available administrators.

Q

+

≡



















Y

Add

Delete

Showing 1 to 6 of 6

100 ▼

Name ↕	Description	Type	Status	Actions
CTF Loader (ctfmon.exe)	Imported through Securdn Agent	Application (.exe)	✓ Active	  
Disk Space Cleanup Manager for Windows (cleanmgr.exe)	Imported through Securdn Agent	Application (.exe)	✓ Active	  
Dism Host Servicing Process (DismHost.exe)	Imported through Securdn Agent	Application (.exe)	✓ Active	  
Host Process for Windows Tasks (taskhostw.exe)	Imported through Securdn Agent	Application (.exe)	✓ Active	  
Lenovo.Vantage.AddinHost.Am064 (Lenovo.Vantage.SmartDisplayAdd...)	Imported through Securdn Agent	Application (.exe)	✓ Active	  
Windows Logon User Interface Host (LogonUI.exe)	Imported through Securdn Agent	Application (.exe)	✓ Active	  

Adding Applications Manually

While the automatic discovery takes time, if you want to instantly add applications, you can manually add them. To add applications, navigate to **Admin >> Privilege Elevation and Delegation >> Applications** and Commands section in the GUI and click the button **Add**.

Privileged Account Manager

Dashboard

Accounts

Folders

Users

Groups

Audit

Sessions

Reports

Admin

Q

Search Accounts

Admin > Applications & Commands

Applications and Commands for Privilege Elevation

The essential aspect of privilege elevation and delegation is temporarily elevating the privileges for applications (in Windows) and allowing users to run with specific commands SUDO privileges in Linux. This page serves as the inventory of all such applications and commands. When you install the Securen agent on Windows endpoints and servers, the applications that normally require admin privileges are discovered and added here. You can also manually add applications. In the case of Linux, you need to add the commands that are to be allowed or not allowed to be run with SUDO privileges. You can review the list and add any other application or command that needs to be controlled. You can define the policy (how should they be elevated) as part of the 'Control Policies' section.






















Note: When an existing application or command is edited by an administrator, the change has to be approved by one of the other available administrators.

Q

Add

Delete

Showing 1 to 7 of 7 100

Name	Description	Type	Status	Actions
CTF Loader (ctfmon.exe)	Imported through Securen Agent	Application (.exe)	Active	  
Disk Space Cleanup Manager for Windows (cleanmgr.exe)	Imported through Securen Agent	Application (.exe)	Active	  
Dism Host Servicing Process (DismHost.exe)	Imported through Securen Agent	Application (.exe)	Active	  
Host Process for Windows Tasks (taskhostv.exe)	Imported through Securen Agent	Application (.exe)	Active	  
Lenovo Vantage.AddInHost.Amd64 (LenovoVantage-SmartDisplay.AddIn.exe)	Imported through Securen Agent	Application (.exe)	Active	  
Task Manager (Taskmgr.exe)	Imported through Securen Agent	Application (.exe)	Active	  
Windows Logon User Interface Host (LogonUI.exe)	Imported through Securen Agent	Application (.exe)	Active	  

Showing 1 to 7 of 7 100

In the GUI that opens, you need to define the Windows applications through multiple attributes so Securden can identify them.

The screenshot shows the 'Privileged Account Manager' interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin' (highlighted in green). Below the navigation bar, the breadcrumb trail reads 'Admin > Applications & Commands > Add Applications and Commands'. The main heading is 'Add Applications and Commands'. A yellow callout box contains the following text: 'This step actually helps Securden in identifying the applications and commands to be elevated. In the case of Windows applications, try to define them through multiple attributes so that Securden is able to identify them perfectly. In the case of Linux, you can define the commands that are to be run with (or not to be run with) SUDO privileges. To add commands, choose the option 'Linux Command' in the Type.' The form fields include: 'Name*' with the value 'Microfoz', 'Description' with the value 'Notepad alternative', 'Type' with a dropdown menu showing 'Application (.exe)', and 'Attributes' with a table containing one row: 'Attribute' (Publisher / Digital Signature) and 'Value*'. At the bottom of the form are 'Save' and 'Cancel' buttons, and a 'Help' link with a question mark icon.

You need to specify the following details:

Name: Provide a name to uniquely identify this application/command in Securden.

Description: You can optionally give the application a brief description.

Type: Type of application (exe/msi/msc etc.)

Attributes: Attributes could be digital signatures, actual file path, original file name and hash value of files. You may provide any number of attributes as desired that would help Securden identify the application.

Once you have filled in all the details, click **Save**.

Adding Linux Commands

For controlling which commands can be run (or cannot be run) with **SUDO** privileges on Linux machines, you need to add the commands in Securden.

Navigate to **Admin >> Privilege Elevation and Delegation >> Applications and Commands** section in the GUI and click the button **Add** and select **Linux Command** for type.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Applications & Commands > Add Applications and Commands

you can define the commands that are to be run with (or not to be run with) SUDO privileges. To add commands, choose the option 'Linux Command' in the Type.

Name*

Admin command Description

Type

Linux Command

Linux Command

Ensure to specify the command with its absolute path. You can also pass parameters with the command.

Example 1: /usr/bin/apt-get

Example 2: /usr/bin/apt-get install python2

Command*

/usr/bin/apt-get install python2

Save Cancel

Ensure to specify the command with its absolute path. You can also pass parameters with the command.

Examples:

/usr/bin/apt-get

/usr/bin/apt-get install python2

--

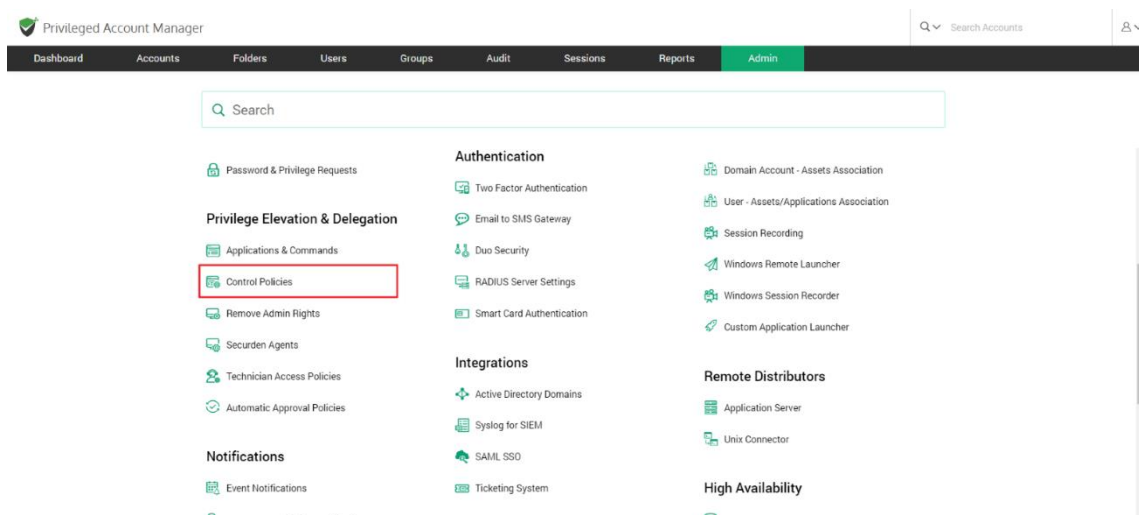
Step 3: Create Control Policies

After adding applications/commands, you need to define policies for a seamless, on-demand elevation of applications for standard users. This is basically, specifying the list of applications that are to be elevated for specific users on specific computers.

For example, you can create a policy whitelisting the ADUC application and associate it with computers in 'Department A' for 'User X' and 'User group Y.' ADUC will be elevated for User X and all users of group Y on the computers in Department A.

Similarly, in the case of Linux, you can specify the commands that can be run with SUDO privileges by specific users/groups on specific computers. Application control policies created here are to be associated with the needed computers and users or user groups.

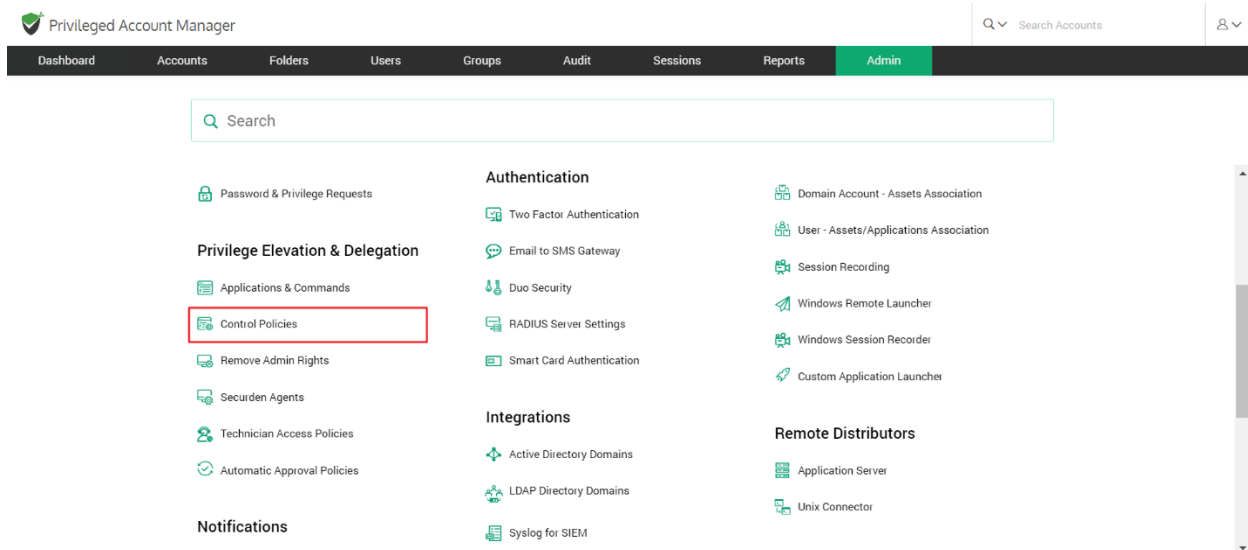
To add application control policies, navigate to **Admin >> Privilege Elevation and Delegation >> Control Policies** section in the GUI.



You need to create policies separately for domain-joined computers, non-domain computers, and Linux.

Creating Domain and Non-domain Control Policies

To create a control policy, Navigate to **Admin >> Privilege Elevation and Delegation >> Control Policies**



In the GUI that opens, click **Add Policy** and select domain control policy for domain joined machines and non-domain policy for workgroup/external computers.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Control Policies

Control Policies

This step helps you to define policies for seamless, on-demand elevation of applications for standard users (in Windows) and elevation of specific commands with SUDO privileges on Linux. Control policies created here are to be associated with the needed computers and users or user groups. For example, you can create a policy whitelisting the ADUC application and associate it with computers in 'Department A' for 'User X' and 'Usergroup Y'. ADUC will be elevated for User X and all users of the group Y on the computers in Department A. The control policy created by one administrator will have to be approved by anyone of the other available administrators. Similarly, in the case of Linux, you can specify the commands that can be run with SUDO privileges by specific users/groups on specific computers.

Search Add Policy Delete Policies

Showing 0 to 0 of 0 100

Name	Type	Privilege Elevation	Status	Actions
No data found				

Showing 0 to 0 of 0 100

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Control Policies > Add Application Policy

Control Policy Name*
Cleanmgrapplications

Description

Application Elevation Preference

☒ Elevate with local administrator privilege ☐ Elevate with domain administrator privilege ☐ Elevate with system privilege ☐ Blacklist

Select Applications

Select the applications that should form part of this policy.

Disk Space Cleanup Manager for Windows (cleanmgr.exe) Search application

Associate Policy with Domain Computers in Securden

☒ All domain computers ☐ Specific domain computers

Associate Policy with Users or Accounts in Securden

☒ All domain users/accounts ☐ Include specific domain users/groups/accounts/folders ☐ Exclude specific domain users/groups/accounts/folders

Save Cancel

https://localhost:5959/dashboard

Please refer to the section below for help with creating Application Control Policies.

Privilege Elevation Precedence

Application control policies can be created and associated with

- Specific users
- Specific groups
- All users
- All users except 'Excluded' ones

You can select the required application elevation preference to whitelist or blacklist applications for the selected users.

While whitelisting, you can grant different levels of privileges to the users based on the requirements. These include, system level privileges, domain privileges, and local admin privileges.

If two different policies affect the same user, the policy in effect will be based on the following order of user/group precedence:

Specific Users >> Specific Groups >> All Users / Excluded Users

Note: By default policies associated with all users will be prioritized over the policy created by excluding specific users. However, this order of priority between All users and Excluded users can be interchanged. Navigate to the configurations section to set the order of priority between All users and Excluded users.

If the two policies assigned have the same user/group precedence, the application control policy in effect will be based on the following order of privilege precedence:

Blacklist >> Local Admin Privilege >> Domain Admin Privilege >> System Privilege

For example, User A and User B have an application control

Step 1: Enter the following details in the interface

Control Policy Name: The name that you enter here helps you uniquely identify the control policy being created. This name will appear on the control policies list.

Description: An overview of the control policy describing what it does and then why this policy has been created

Step 2: Choose the level of elevation for the application(s)

Elevate with local admin privilege: Selecting this lets you run the application with local admin rights.

Elevate with system privilege: If you want to elevate services and processes within Windows that need the capability to log on internally with system privilege, select this option.

Blacklist: This option is to block usage of the application.

Step 3: Select the applications that are to be part of the policy

You can use the **Search application** field to select the required applications from the list or enter the application name and select it.

Step 4: Associating the policy with domain/non-domain computers

The next step is to specify the list of computers on which this policy should take effect. You can choose to have all domain/non-domain computers follow this policy or choose a specific set of computers to adhere to it.

Step 5: Associate policy with specific users/accounts

The final step is to associate the policy with the required domain users/user groups or domain accounts/folders (in the case of domain policy) and accounts/folders (in the case of non-domain policy). That means the policy will take effect on the users/groups/accounts/folders selected here on the

computers chosen in the previous step.

Step 6: Once done with all the steps, proceed to click '**Save**'.

Important Note: For security reasons, the application control policy created by one administrator will have to be approved by any one of the other available administrators. Securden sends notifications to the approvers, who can review applications and approve/reject the request from the "Control Policies" page. Until the policy gets approval, it will not take effect.

Linux Commands Policy

You have the option to specify if a command is to be allowed to be run with SUDO privileges or not by specific users or groups on specific computers. Linux command policies help achieve that.

To add application control policies, navigate to **Admin >> Privilege Elevation and Delegation >> Control Policies** section in the GUI and select **Linux Command Policy**.

Select the option "**Grant SUDO Privilege**" to allow running the command and "**Deny SUDO Privilege**" to restrict the usage of the command.

Select the commands that are to be part of the policy

You can use the "**Select Commands**" field to select the required commands from the list, or enter the command name and select it.

Associate policy with specific accounts/folders

The final step is to associate the policy with the required accounts/folders. That means the policy will take effect on the accounts/folders selected here.

Technician Access Policies

IT help desk technicians often log on to end-user machines with administrative privileges to carry out certain tasks. This leads to various security and operational issues. To overcome such issues, Securden helps you define '**Technician Access Policies**'.

Typically, you can create policies authorizing specific technicians to perform administrative tasks on specific endpoints. Technicians can log on to end-user machines with standard user privileges and offer the required assistance. Their privilege will be elevated on-demand temporarily. You can specify the computers on which specific technicians can have technician access.

Create technician access policies

To create a technician access policy,

Navigate to **Admin>> Privilege Elevation and Delegation >> Technician Access Policies**

You need to create policies for domain-joined computers and non-domain computers separately. When creating the policy, you need to **select Domain Policy** or **Non-domain Policy** as required.

Follow the steps below to create a technician policy

The policy creation involves specifying the computers on which specific technicians should be able to access to perform various operations. The process is quite flexible - you can allow a technician or a group of technicians to access all computers or only specific computers. The technician could be a **user** or a **group** in Securden.

To create a policy, click **Add Policy** and select **Add Domain Policy** or **Non-domain Policy** as needed.

In the GUI that opens, enter the following information:

Technician policy name: The name that you enter here helps you uniquely identify the policy being created.

Description: A brief of the policy for a quick overview

Select the computers and computer groups the technician could access

All the OUs and Groups imported from AD will be displayed as **Computer Groups** in Securden. In this step, you will specify the computers and computer groups that you want to authorize the technician to access and carry out the tasks. You can allow access to all computers or only for specific computers.

Associate policy with the technician

The final step is to associate the policy with the required technicians or groups. The 'technician' could be a 'user' or a 'group' in Securden. You can select either all 'users' or specific users/groups alone. For example, you can designate all members of the IT Help Desk group to access the computers selected in the previous step.

- To associate the policy with all domain users and accounts enable **All domain users/accounts imported in Securden**
- To select users or groups, use the **search user/group** and choose from the list of users/groups.

Finally, **Save** the changes.

Approval for policies

On completing this step, your technician access policy created will be reserved for review and approval by another administrator. You can check the approval status on the technician policies page. Approved policies will be shown as '**Active**'.

How to approve policies?

Administrators can approve the policies created by other administrators from **Admin >> Privilege Elevation and Delegation >> Technician Access Policies**. Administrators will receive email notifications when a policy is

created and awaits approval

How do technicians commence access?

When a technician wants to access an endpoint, the technician must use the Securden tray icon present in the machine. (See the icon shown inside the red circle in the image below).

Upon clicking the tray icon, the technician will see a menu in which **Start Technician Access** will be one of the options. When that option is clicked, the technician will be prompted to enter credentials for authentication. The technician has to enter his/her domain account credentials to authenticate. Upon successful authentication, technician access will start.

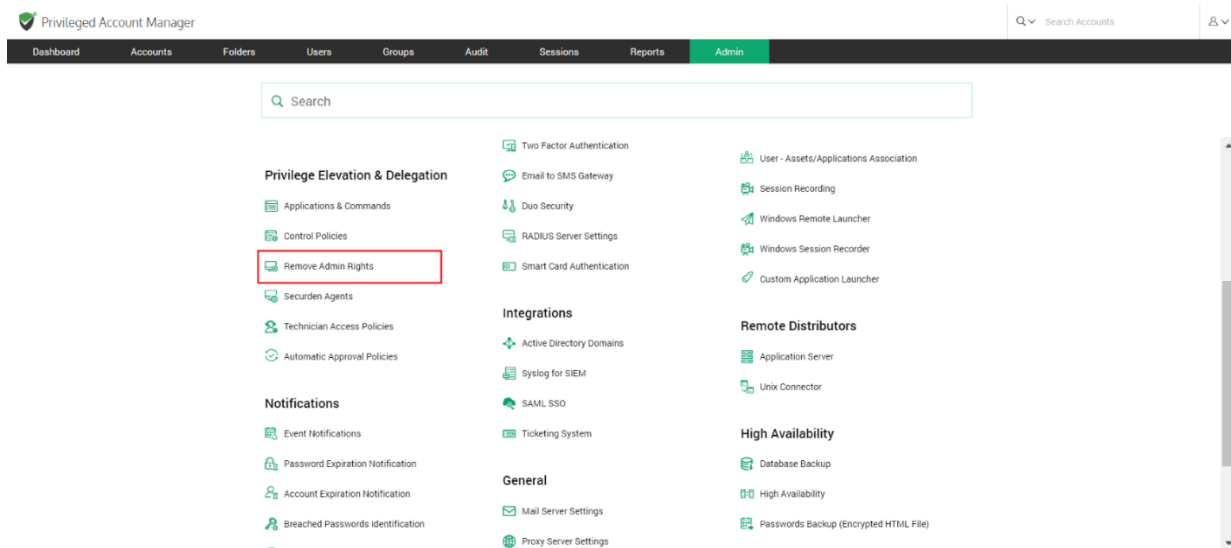
The technician will have administrative access and can carry out the required tasks. To elevate applications the technician should use **Run as Administrator** instead of **Run with Securden Privilege**. When doing so, the technician will see the UAC prompt, but along with that Securden screen will also overlay as shown in the screenshot below:

Finally, the technician must click **End Technician Access** access available in the tray icon menu.

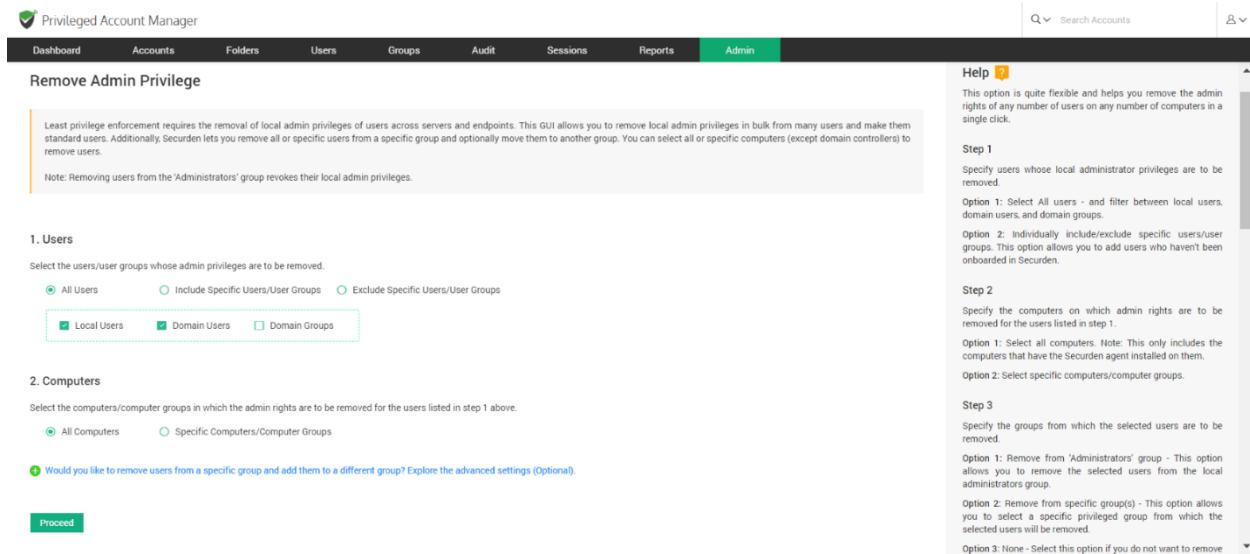
Eliminate Local Admin Rights

Along with the device discovery, the Securden agent captures the list of local administrator accounts on each computer. This helps you decide which devices require least privilege enforcement. Least privilege enforcement requires the removal of local admin rights of users across servers and endpoints.

Navigate to **Admin >> Privilege Elevation and Delegation Management >> Remove Admin Rights**



In addition to removing local admin privileges, this GUI allows you to remove users from any group on devices and add them to a different group.



Remove Admin Privilege

Least privilege enforcement requires the removal of local admin privileges of users across servers and endpoints. This GUI allows you to remove local admin privileges in bulk from many users and make them standard users. Additionally, Securden lets you remove all or specific users from a specific group and optionally move them to another group. You can select all or specific computers (except domain controllers) to remove users.

Note: Removing users from the 'Administrators' group revokes their local admin privileges.

1. Users

Select the users/user groups whose admin privileges are to be removed.

☒ All Users ☐ Include Specific Users/User Groups ☐ Exclude Specific Users/User Groups

☒ Local Users ☒ Domain Users ☐ Domain Groups

2. Computers

Select the computers/computer groups in which the admin rights are to be removed for the users listed in step 1 above.

☒ All Computers ☐ Specific Computers/Computer Groups

? Would you like to remove users from a specific group and add them to a different group? Explore the advanced settings (Optional).

Proceed

Help

This option is quite flexible and helps you remove the admin rights of any number of users on any number of computers in a single click.

Step 1

Specify users whose local administrator privileges are to be removed.

Option 1: Select All users - and filter between local users, domain users, and domain groups.

Option 2: Individually include/exclude specific users/user groups. This option allows you to add users who haven't been onboarded in Securden.

Step 2

Specify the computers on which admin rights are to be removed for the users listed in step 1.

Option 1: Select all computers. Note: This only includes the computers that have the Securden agent installed on them.

Option 2: Select specific computers/computer groups.

Step 3

Specify the groups from which the selected users are to be removed.

Option 1: Remove from 'Administrators' group - This option allows you to remove the selected users from the local administrators group.

Option 2: Remove from specific group(s) - This option allows you to select a specific privileged group from which the selected users will be removed.

Option 3: None - Select this option if you do not want to remove

This option is quite flexible and helps you manage the admin rights of any number of users on any number of computers with a single click.

Step 1: Selecting Target Users

You need to specify the users for whom you want to manage privileges. You have two options going forward.

Option 1: Select All users - and filter between local users, domain users, and domain groups.

Option 2: Individually include/exclude specific users/user groups. This option allows you to add users who haven't been onboarded in Securden.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Remove Admin Rights

Remove Admin Privilege

Least privilege enforcement requires the removal of local admin privileges of users across servers and endpoints. This GUI allows you to remove local admin privileges in bulk from many users and make them standard users. Additionally, Securden lets you remove all or specific users from a specific group and optionally move them to another group. You can select all or specific computers (except domain controllers) to remove users.

Note: Removing users from the 'Administrators' group revokes their local admin privileges.

1. Users

Select the users/user groups whose admin privileges are to be removed.

☐ All Users
 ☐ Include Specific Users/User Groups
 ☒ Exclude Specific Users/User Groups

Enter User/User Group Name

jake matthew Admin Group

2. Computers

Help

This option is quite flexible and helps you remove the admin rights of any number of users on any number of computers in a single click.

Step 1

Specify users whose local administrator privileges are to be removed.

Option 1: Select All users - and filter between local users, domain users, and domain groups.

Option 2: Individually include/exclude specific users/user groups. This option allows you to add users who haven't been onboarded in Securden.

Step 2

Specify the computers on which admin rights are to be removed for the users listed in step 1.

Option 1: Select all computers. Note: This only includes the computers that have the Securden agent installed on them.

Option 2: Select specific computers/computer groups.

Step 3

Specify the groups from which the selected users are to be removed.

Option 1: Remove from 'Administrators' group - This option allows you to remove the selected users from the local administrators group.

Option 2: Remove from specific group - This option allows

Step 2: Selecting Target Devices

Specify the computers on which rights are to be managed for the users selected in step 1. You have two options going forward.

Option 1: Select all computers. Note: This only includes the computers that have the Securden agent installed on them.

Option 2: Select specific computers/computer groups.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Search Accounts

Jake x Matthew x Admin Group x

2. Computers

Select the computers/computer groups in which the admin rights are to be removed for the users listed in step 1 above.

☐ All Computers ☒ Specific Computers/Computer Groups

Enter Computer/Computer Group Name

W10PF2YASDP x

3. Remove from Group

Select the groups from which the users (specified in step 1 above) are to be removed. If you know of any other groups with excess privileges, select those specific groups too.

☒ Remove from 'Administrators' group ☐ Remove from specific group(s) ☐ None

Step 3
Specify the groups from which the selected users are to be removed.
Option 1: Remove from 'Administrators' group - This option allows you to remove the selected users from the local administrators group.
Option 2: Remove from specific group(s) - This option allows you to select a specific privileged group from which the selected users will be removed.
Option 3: None - Select this option if you do not want to remove users from any group

Step 4
Specify the groups to which users removed in Step 3 are to be added into.
Option 1: Add to the 'Users' group - This option allows you to add the users removed into the default 'Users' group, making them standard users with no admin privilege.
Option 2: Add to a specific group - This option allows you to add the users removed into a specific group/groups of your choice. Select the groups where you wish to add the users.
Option 3: None - Select this option if you do not want to add the users removed from group(s) specified in Step 3 to any other group(s).

Step 3: Specify Source Groups

Selected users might be a part of groups with admin privileges in the selected devices. Specify the groups from which the selected users are to be removed. You have three options going forward.

Option 1: Remove from 'Administrators' group - This option allows you to remove the selected users from the local administrators group.

Option 2: Remove from specific group(s) - This option allows you to select a specific privileged group from which the selected users will be removed.

Option 3: None - Select this option if you do not want to remove users from any group

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

☐ All Computers ☒ Specific Computers/Computer Groups

Enter Computer/Computer Group Name

W10PF2V8SP X

3. Remove from Group

Select the groups from which the users (specified in step 1 above) are to be removed. If you know of any other groups with excess privileges, select those specific groups too.

☐ Remove from 'Administrators' group ☒ Remove from specific group(s) ☐ None

Enter Group Name ☒ Default Group ☐ Custom Group

Administrators X

4. Add to Group

Option 3: None - Select this option if you do not want to remove users from any group

Step 4

Specify the groups to which users removed in Step 3 are to be added into.

Option 1: Add to the 'Users' group - This option allows you to add the users removed into the default 'Users' group, making them standard users with no admin privilege.

Option 2: Add to a specific group - This option allows you to add the users removed into a specific group/groups of your choice. Select the groups where you wish to add the users.

Option 3: None - Select this option if you do not want to add the users removed from group(s) specified in Step 3 to any other group(s).

Step 4: Specify Destination Group

Specify the groups to which users removed in Step 3 are to be added into. You have three options going forward.

Option 1: Add to the 'Users' group - This option allows you to add the users removed into the default 'Users' group, making them standard users with no admin privilege.

Option 2: Add to a specific group - This option allows you to add the users removed into a specific group/groups of your choice. Select the groups where you wish to add the users.

Option 3: None - Select this option if you do not want to add the users removed from group(s) specified in Step 3 to any other group(s).

The screenshot shows the 'Admin' section of the Securden Privileged Account Manager interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin' (highlighted). A search bar for 'Search Accounts' and a user profile icon are on the right. The main content area is titled '4. Add to Group' and contains the following text: 'Select the groups from which the users (specified in step 1 above) are to be added to the group. If you know of any other groups with excess privileges, select those specific groups too.' Below this text are three radio buttons: 'Add to the 'Users' group', 'Add to specific group(s)' (which is selected), and 'None'. Further down, there is a section for 'Enter Group Name' with two tabs: 'Default Group' (selected) and 'Custom Group'. Under the 'Default Group' tab, there is a text input field containing the word 'Users' and a blue button with a plus sign. At the bottom left of the form area is a green 'Proceed' button.

Once you've selected and specified all the required options, click on **Proceed**. The selected users will be added/removed for specific/all devices based on your configurations.

Section 13: Customization

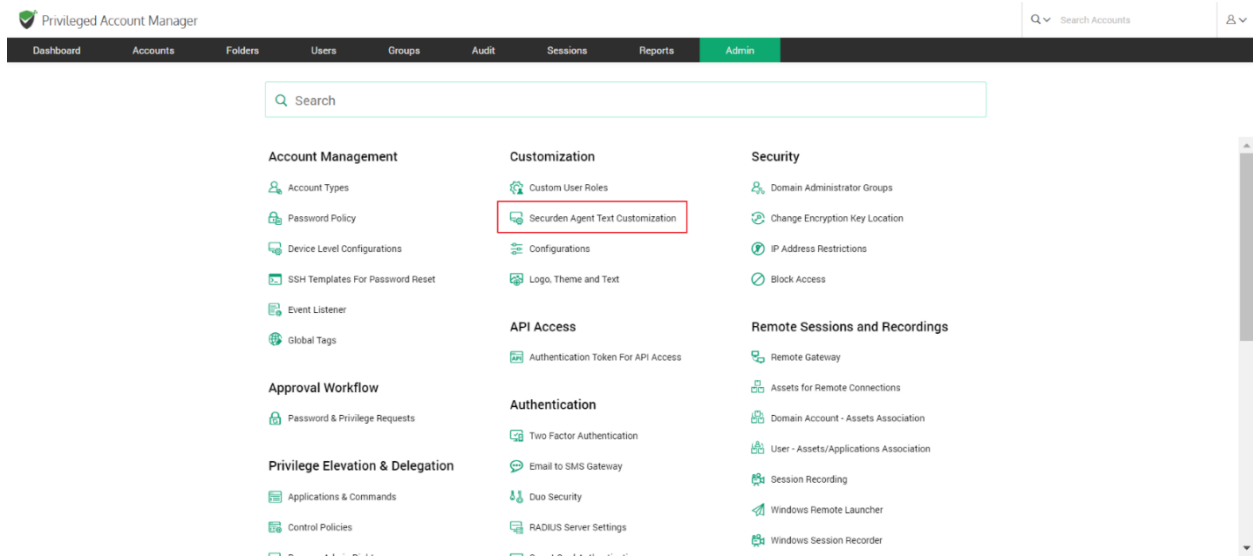
Customize Securden PAM

You can customize Securden PAM to suit your organization's unique needs. Securden allows you to create custom user roles, granularly switch on and switch off certain features, add your company logo, modify the text appearing at certain places, select the display language of product interface, and so on. Navigate to **Admin >> Customization** section to check the various customization options.

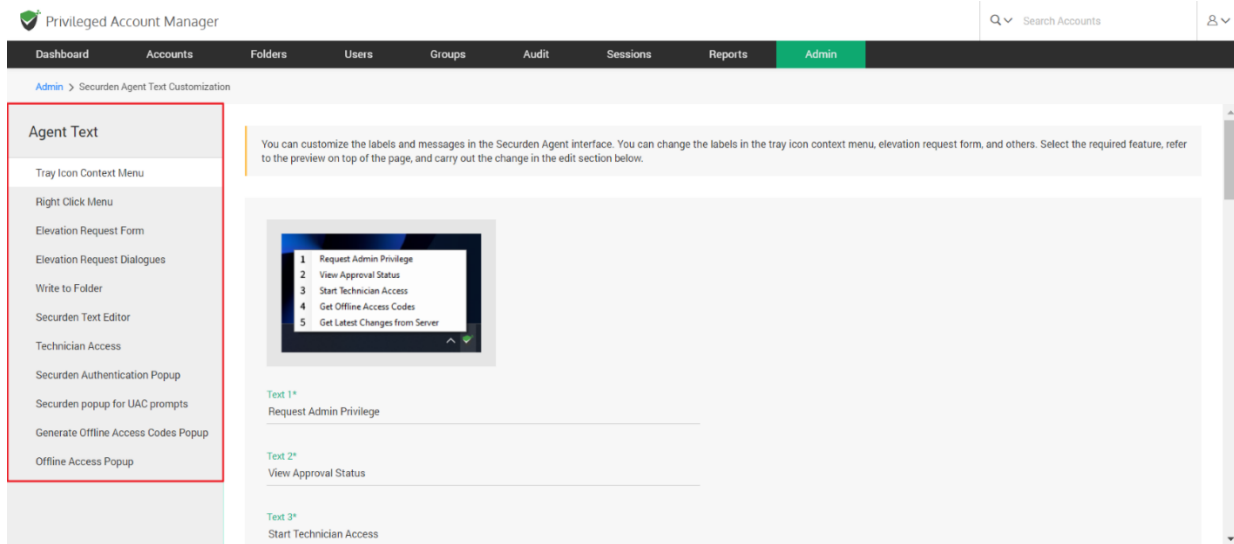
Securden Agent Text Customization

If you are using the Privilege Elevation and Delegation feature, you would be deploying the Securden agent on endpoints and servers. The agent displays various labels, context menus, and forms. You can customize the message text and labels appearing in the Securden agent interface. You can change the labels in the tray icon context menu, elevation request form, Securden text editor, and others.

To customize the agent text, navigate to **Admin >> Customization >> Securden Agent Text Customization**.



In the GUI that opens you have the following option to customize within the Securden Agent:



The LHS menu lists the different types of messages related to the Securden agent. The different types of customizable items are:

- **Tray icon context menu** – The tray icon appears on right clicking the Securden Agent icon available on the taskbar tray.
- **Right Click Menu** – The right click menu appears when you right-click any application that requires admin permissions to be run
- **Elevation Request Form** – The elevation request form is the form that pops-up when a user requests admin access – either for a specific application or time-restricted full admin access.
- **Elevation Request Dialogues** – Elevation request dialogues are those that appear on requesting access to an application. These dialogues usually depict messages to notify the user of a restricted application.
- **Write to Folder** – This dialogue box appears when trying to paste content from the clipboard directly to a folder.
- **Securden Text Editor** - This dialogue box appears when trying to paste content from the clipboard directly to a folder.
- **Technician Access** – This includes all the dialogues that appear during technician access.
- **Securden Authentication Pop-up** – The securden authentication pop-up appears when a user has to login using their user credentials for the device to confirm their identity.
- **Securden Pop-up for UAC Prompts** – The pop-up appears when bypassing the Windows UAC prompt.
- **Generate Offline Access Codes Pop-up** – This pop-up appears when a user attempts to generate access codes for privilege elevation during offline scenarios.
- **Offline Access Pop-up** – This pop-up appears when a user uses offline codes for privilege elevation when the agent is disconnected from the Securden server.

You will see the related screenshots in each section. In the text fields below the respective screenshots, you can customize the text in the text fields.

Configurations

Securden lets you comprehensively enable, disable, and configure all the features that are part of the solution. You can make necessary modifications to the required features from the **Configurations tab** available under **Admin >> Customization**.

Defaults selection

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

While importing users from the Active directory, you can assign role to the users. You have the option to select which role users are imported with. When you click change, it shows the list of default roles and custom roles available. You can choose from the list of roles. The users which gets imported after changing the role will acquire that role.

While importing user groups from AD/Azure AD, do you want to configure automatic synchronization with Securden groups?

You can automatically synchronize the user groups in Securden with that of Active Directory. Automatic synchronization is applicable only for the user groups imported after saving this configuration. When users are added or

deleted in AD, the same gets reflected here. You can also define the synchronization interval.

When you click change, a GUI with two options 'Configure' and 'No' appears. When you select No, automatic synchronization will be disabled. If you select 'Configure'

A GUI named 'Configure Automatic Group Synchronization' appears. You can customize the time interval with which the synchronization should happen. After selecting the time interval click on '**Save**' to see the changes.

When synchronizing user groups with AD in Securden, do you want to remove the users (from the group) who remain disabled in AD? If you select 'No' for this option, the disabled users in AD will only be disabled in Securden too. They will not be removed from the respective group.

Securden allows you to remove the imported users who are disabled in the Active directory. If you don't want them to be removed you can just disable them.

When you click change, a GUI with two options Yes and No appears. If you select Yes, the disabled users in the Active Directory will be removed. If you select No, the disabled users in AD will only be disabled in Securden too. They will not be removed from the respective groups.

Do you want to receive an email alert on the remaining user license count (when you can add less than 5 users)?

Securden allows up to 5 free users. You have the option to receive email alert on the remaining user license when the added user count is less than 5. When you click change, a confirmation box will appear saying Yes and No. You'll receive email alerts if you select Yes and if you select No, it will be disabled.

Do you want to enable hotkeys?

Hotkeys here are nothing but the shortcut keys used inside the Securden UI. Securden has many hotkeys like ctrl+shift+U for copying account name, ctrl+shift+P for copying password, ctrl+shift+S for opening advanced search etc.

When you click change, a list with options like **Enable for all**, **Disable for all** and **Customize** appears. You can enable hotkeys for a custom list of users by selecting customize. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added below.

You can enable hotkeys for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added below.

Do you want to send email alerts to users on user addition?

Securden sends email alerts to the users upon adding them. It is not mandatory. If you want to disable it, you can do it in the configuration section.

When you click change, it comes with the dropdown that says **Yes** and **No**. If you want to send email alerts, you can select **Yes** and if you don't want you can select **No**.

Do you want to send email alerts when users are added in specific roles?

Securden has the flexibility to send email alerts to specific roles. It is totally customizable.

When you click change, it shows options like No and Customize. You can choose from the options given. If you don't want to send email, you can select No. If you want to customize, you can select customize and make the required customization from the respective section.

Do you want to include the username of the creator and the time of creation as a footer in PDF reports?

Securden allows you to generate reports in the form of PDF. You have the option to include the username of the creator and the time of creation as a footer in PDF reports.

When you click change, a GUI with two options Yes and No appears. If you want to include the details in PDF, you can select Yes. If you don't want to include the details, you can select No.

Password Policy

Would you like to enforce password policy during account addition and local password resets?

Securden allows you to enforce password policy during account addition and local password resets.

When you click change, a GUI with two options Yes and No appears. If you select Yes, password policy will be enforced and if you click No, it will not be enforced.

You can enforce complexity rules for the passphrase to be used for offline access. Select a password policy to be enforced for that purpose.

Securden allows you to create and enforce the complexity rules for passphrase to be used for offline access. You have the option to specify and enforce an existing password policy for the passphrase used to encrypt the offline copy. When you click change, a GUI named 'Change Password Policy for Offline Access' appears. You have to enter password policy by clicking the drop- down and click '**Change policy**' to enforce them.

RESTful API

Do you want to allow API access for all users?

Securden allows you to have API access for all users. You can disable it for all and also customize it as desired. All these can be done in the **Admin>>Configurations section**.

When you click change, a dialog box with four options 'Allow for all', 'Deny for all', 'Deny for Users & Auditors' and 'Customize' appears. When you select 'Allow for all', all users will be allowed access and if you select 'Deny for all', all users will be denied from using API access. If you select 'Deny for Users & Auditors', only the Users & Auditors will be denied. If you select customize,

You can enable API access for a custom list of users. If you select 'Allow', this configuration will be applicable only to the users/groups added below. If you select 'Deny', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

Account Management

Do you want to enforce folder selection while adding/editing accounts?

Securden allows you to enforce folder selection while adding/editing accounts. You have the option to enable/disable/customize the folder selection.

When you click change, a confirmation box with three options Enable for all, Disable for all and Customize appears. If you select enable for all, the folder selection will be enforced for all the users and if you select disable for all it will be disabled for all the users.

If you select customize, you can enforce folder selection while adding/editing accounts for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added.

Do you want to display the account details page in expanded form by default?

Securden allows you to display the account details page in expanded form by default. You can enable display of account details page in expanded form for a custom list of users.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', It will be displayed for all users. If you select 'Disable for all', it will not be displayed for anyone. If you select Customize,

You can enable display of account details page in expanded form for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added.

Do you want to enforce users to provide reason while retrieving passwords?

Securden allows you to enforce users to provide reason while retrieving passwords. If you don't want to enforce it for all the users and you want to customize it for specific users/Groups, you can go ahead and do it.

When you click change, a dialog box with three options **Enable for all**, **Disable for all** and **Customize** appears. If you select **Enable for all**, all users will be providing reasons while retrieving passwords and if you select 'Disable for all', this option will be disabled. If you select **Customize**,

You can enforce providing reason while retrieving passwords for a custom list of users . If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added.

Do you want to enforce users to provide reason while launching remote connections using the remote launch icon

Securden allows you to enforce users to provide reason while launching remote connections using the remote launch icon. You can disable it and also can customize it for specific Users/Groups.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', it will be enforced for all the users and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize',

You can enforce providing reason while launching remote connections via the remote launch button for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Finally click '**save**' to show changes.

Do you want to enforce users to provide reason while changing password?

Securden allows users to provide reason while changing passwords. You can disable it for all the users and also can customize it for specific Users/Groups..

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', it will be enforced for all the users and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears

You can enforce providing reason while changing passwords for a custom list of users . If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click '**Save**' to show changes.

Do you want to enforce users to provide a reason while deleting accounts and folders?

Securden allows users to provide a reason while deleting accounts and folders. You can disable it for all the users and also can customize it for specific Users/Groups.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', it will be enforced for all the users and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears

You can enforce a custom list of users to provide a reason while deleting accounts and folders. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click '**Save**' to show changes.

Do you want to set password change on remote machines as the default option?

Securden allows users to set password change on remote machines as the default options. You can disable it for all the users and also can customize it for specific Users/Groups. .

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', it will be enforced for all the users and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears

You can set password change as a default when logging into remote machines.. If you select 'Allow', this configuration will be applicable only to the users/groups added below. If you select 'Deny', this configuration will be

applicable to all users/groups except the ones added. Click '**save**' to show changes.

Do you want to display Recently Deleted Accounts by default?

Securden allows users to display Recently Deleted Accounts by default. You can disable it for all the users and also can customize it for specific Users/Groups.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', it will be enforced for all the users and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears

You can set password change as a default when logging into remote machines.. If you select 'Allow', this configuration will be applicable only to the users/groups added below. If you select 'Deny', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

Do you want to restrict the time duration for password access requests as a part of 'Approval Workflow'? Once configured, users will have to specify a time duration (in minutes) within the maximum duration specified

Securden allows an option to restrict the time duration for password access requests as a part of 'Approval Workflow'.

When you click change, a GUI 'Configure Maximum Time Duration for Password Access' appears. If you want to restrict time limit, select 'Restrict Time Duration' you can specify the upper limit (in minutes) within which users can request access for password and if you don't want, you can select 'No restriction'. Click '**save**' to show changes.

Do you want to deny account addition permission (work accounts) to the users with roles 'User' and 'Auditor'?

Securden have the option to deny account addition permission (work accounts) to the users with roles 'User' and 'Auditor'.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, users with roles 'Users' and 'Auditors' will be denied account addition permission and if you select No, users will not have any such restrictions.

Do you want to allow users with the roles 'User' and 'Auditor' to import accounts from files?

Securden allows users with the roles 'Users' and 'Auditor' to import accounts from files. If you don't want you can just disable it.

When you click change, a confirmation box will appear saying Yes and No.

If you click Yes, users with roles 'Users' and 'Auditors' will be allowed to import accounts from files and if you select No, users will not have any such permissions.

Do you want to allow users with roles 'User' and 'Auditor' to edit the details of accounts that are shared to them with 'Manage' privilege?

Securden allows users with the roles 'Users' and 'Auditor' to edit the details of accounts that are shared to them with 'Manage' privilege. If you don't want you can just disable it.

When you click change, a confirmation box will appear saying Yes and No.

If you click Yes, users with roles 'Users' and 'Auditors' will be allowed to edit the details of accounts that are shared to them with 'Manage' privilege and if you select No, users will not have any such permissions.

Do you want to allow users (irrespective of the role) to view the 'Password History' of accounts if the share permissions allow them to view passwords?

Securden allows users(irrespective of the role) to view the 'Password History' of accounts if the share permissions allow them to view passwords. If you don't want you can just disable it.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', it will be enforced for all the users and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can allow a custom list of users to view 'Password History' of accounts if they already have view permission. If you select 'Allow', this configuration will be applicable only to the users/groups added below. If you select 'Deny', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

Do you want to deny account sharing permission to the users with the roles 'User' and 'Auditor'?

Securden have the option to deny account sharing permission to the users with roles 'User' and 'Auditor'. If you don't want you can just disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, users with roles 'Users' and 'Auditors' will be denied account sharing permission to the users with the roles 'User' and 'Auditor' and if you select No, users will not have any such restrictions.

Do you want to enforce selection of a parent folder while adding/editing folders?

Securden allows you to enforce selection of a parent folder while adding/editing folders. If you don't want you can disable it.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', it will be enforced for all the users and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can enforce parent folder selection while adding/editing folders for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

During folder creation, do you want to enable 'permissions inheritance from parent folders' by default?

Securden allows you to enable 'permissions inheritance from parent folders' by default during folder creation. If you don't want you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, 'permission inheritance from parent folders' will be enabled by default during folder creation and if you select No, it will be disabled.

Do you want to enforce 'permissions inheritance from parent folders', while creating or editing a folder?

Securden allows you to enable 'permissions inheritance from parent folders' while creating or editing a folder. If you don't want you can disable it.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', it will be enforced for all the users and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can enforce parent folder inheritance for specific users/groups. You can do this by selecting the list of users/groups and enable/disable parent folder inheritance. Click '**save**' to show changes.

Do you want to restrict users with roles 'User' and 'Auditor' from deleting the accounts owned by them?

Securden have the option to restrict users with roles 'User' and 'Auditor' from deleting the accounts owned by them. If you don't want you can just disable it.

When you click change, a confirmation box will appear saying Yes and No.

If you click Yes, users with roles 'User' and 'Auditor' will be restricted from deleting the accounts and if you select No, it will be disabled.

Upon clicking a folder in the 'Accounts' list view, do you want to show the accounts belonging to its sub-folders?

Securden have the option to show the accounts belonging to its sub-folders upon clicking a folder in the 'Accounts' list view. If you don't want you can just disable it.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', it will be enforced for all the users and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can enable viewing of accounts belonging to the sub-folders while clicking a folder in the 'Accounts' list view a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click **'save'** to show changes.

Do you want to show the folders tree in collapsed mode on the 'Folders' tab?

Securden have the option to show the folders tree in collapsed mode on the 'Folders' tab. If you don't want you can just disable it.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', it will be enabled for all the users and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can apply this setting for specific users or a group alone. Select the names of users and groups here. If you select 'Enable', this configuration will be applicable only to the users/groups added. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click **'save'** to show changes.

Do you want to show the folders tree structure in 'Accounts' view in compact form collapsing the entries by default?

Securden have the option to show the folders tree structure in 'Accounts' view in compact form collapsing the entries by default. If you don't want you can disable it.

When you click change, a confirmation box will appear saying Yes and No.

If you click Yes, the folders tree structure in 'accounts' view in compact form collapsing the entries by default will be shown and if you select No, it will be disabled.

Do you want to allow users to add multiple accounts with the same account title?

Securden allows users to add multiple accounts with the same account title. If you don't want, you can just disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, users can add multiple accounts with the same account title and if you select No, it will be disabled.

When ticketing system validation is enforced, do you want to enforce ticket ID validation during remote password reset operation?

Securden have the option to enforce ticket ID validation during remote password reset operation when ticketing system validation is enforced. If you don't want you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, ticket ID validation during remote password reset operation will be enabled and if you select No, it will be disabled.

How long (in days) would you like to keep the recently deleted accounts before permanently deleting them?

Securden allows an option to keep the recently deleted accounts before permanently deleting them for a period of time. You can specify the time period (in days).

When you click change, a GUI appears 'Recently Deleted Accounts Restoration'. You can specify the maximum number of days the recently deleted accounts to be kept for recovery. During this time window, you will have the option to recover. After that, the accounts will be permanently deleted. At last, click '**save**' to show changes.

Do you want the system default folders to be shown on the Accounts page?

Securden have the option to show the system default folders on the Accounts page. If you don't want.

When you click change, a dialog box with two options 'Yes' and 'Customize' appears. If you select Yes, the system default folders will be shown on the Accounts page and if you select Customize, a GUI appears

The list of default system folders is shown below. Select the ones that you want to see on the 'Accounts' page. The greyed-out items in the list cannot be disabled.

When searching for folders, do you want to include sub-folders in the search result?

Securden have the option to include sub-folders in the search result when searching for folders. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No.

If you click Yes, sub-folders will be included in the search result when searching for folders and if you select No, it will be disabled.

Do you want allow your users to create their own tags while adding or editing work accounts?

Securden allows your users to create their own tags while adding or editing work accounts. If you don't want, you can disable it.

When you click change, a dialog box with three options 'Allow for all', 'Deny for all' and 'Customize' appears. If you select 'Allow for all', users will be allowed to create their own tags while adding or editing work accounts and if you select 'Deny for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can enable or disable specific users/groups from creating custom tags. Disabled users/groups will only be able to utilize existing tags while creating/editing accounts. Click '**save**' to show changes.

Do you want to customize the account details displayed in the 'Accounts' list view?

Securden allows you to customize the account details displayed in the 'Accounts' list view. If you don't want, you can disable it or even customize it. This can be done in the **Admin >> Configurations section**.

When you click change, a dialog box with two options 'No' and 'Customize' appears. If you select 'No', the account details cannot be customized in the 'Accounts' list view. If you select 'Customize', a GUI appears.

You have the option to select/deselect the account details displayed in the 'Accounts' list. The Account Title is displayed by default and cannot be disabled. Click **'save'** to show changes.

Do you want to display the account title shown on the web interface in multiple lines?

Securden allows you to display the account title shown on the web interface in multiple lines. If you don't want to display, you can just disable it.

When you click change, a confirmation box will appear saying Yes and No.

If you click Yes, the account title shown on the web interface will be displayed in multiple lines and if you select No, it will be disabled.

Remote Connections

When launching remote connections using a domain account, a list of FQDN/IP addresses will be displayed to which you can connect. Do you want to show the address of the domain account in the list?

Securden have the option to show the address of the domain account in the list. When launching remote connections using a domain account, a list of FQDN/IP addresses will be displayed to which you can connect. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you select Yes, the address of the list will be shown in the list and if you want to disable it, you can select No.

When launching remote connections with specific addresses (FQDN/IP Address) using a domain account, do you want to display the list of permitted account addresses a user has access to?

Securden allows you to display the list of permitted account addresses a user has access to, When launching remote connections with specific addresses (FQDN/IP Address) using a domain account. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you select Yes, the list of permitted account addresses a user has access to will be displayed and if you want to disable it, you can select No.

When launching remote connections using a domain account, do you want to allow users to type the name of IT asset to be connected?

Securden allows users to type the name of IT asset to be connected when launching remote connections using a domain account. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you select Yes, users will be allowed to type the name of IT asset to be connected and if you want to disable it, you can select No.

Do you want to allow remote Telnet connections? When the Telnet window is opened, Securden fills the credentials (password might get printed on the command window). Telnet protocol has its inherent security limitations that have limited its usefulness in environments where the network cannot be fully trusted. The use of Telnet over the public internet should be avoided as it carries the risk of eavesdropping. Allow this only after carefully considering the security aspects.

Securden have the option to allow remote Telnet connections. If you don't want, you can disable it.

Do you want to disable any type of remote connections available in Securden?

Securden allows you to disable any type of remote connections available. If you don't want, you can disable it or even customize it.

When you click change, a dialog box with two options 'No' and 'Customize' appears. If you select 'No', the option to disable any type of remote connections available will be denied. If you select 'Customize', a GUI appears.

Securden supports various protocols for launching remote connections. You may enable or disable any protocol as needed. Every connection type listed below is enabled by default, except Windows Telnet & Putty Telnet connections.

To disable a protocol, unselect it from the list below.

If you select to have Telnet connections, you need to additionally enable Telnet connections from Admin >> Customization >> Configurations >> Remote Connections. You can select up to five details to be shown in the details list.

Do you want to enable Bypass alerts from the securden agent when RDP connection is not launched through securden session manager?

Securden allows you to enable Bypass alerts from the securden agent when RDP connection is not launched through securden session manager. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you select Yes, Bypass agents from the Securden agent will be enabled and if you want to disable it, you can select No.

Do you want to enable the Securden agent to confirm its presence with the server? If yes, specify the time interval in which the agent tries contacting the server.

Securden allows you to enable the Securden agent to confirm its presence with the server. If you don't want, you can disable it.

You can specify the upper time limit (in minutes) within which the agent should contact the server to confirm its presence, on exceeding which an audit is captured. You can turn it off by selecting disable. Click '**save**' to show changes.

Export Accounts

Do you want to allow your users to export their work accounts as .xlsx file?

Securden allows your users to export their work accounts as .xlsx file. If you don't want, you can disable it or even customize it.

When you click change, a dialog box with three options 'Allow for all', 'Deny for all' and 'Customize' appears. If you select 'Allow for all', users will be allowed to export their work accounts as .xlsx file and if you select 'Deny for

all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can allow a custom list of users to export their work accounts as .xlsx file. If you select 'Allow', this configuration will be applicable only to the users/groups added below. If you select 'Deny', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

Do you want to allow your users to export their personal accounts as .xlsx file?

Securden allows your users to export their personal accounts as .xlsx file. If you don't want, you can disable it or even customize it.

When you click change, a dialog box with three options 'Allow for all', 'Deny for all' and 'Customize' appears. If you select 'Allow for all', users will be allowed to export their personal accounts as .xlsx file and if you select 'Deny for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can allow a custom list of users to export their personal accounts as .xlsx file. If you select 'Allow', this configuration will be applicable only to the users/groups added below. If you select 'Deny', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

Do you wish to conceal the password column when users export their work accounts as .xlsx file?

Securden have the option to conceal the password column when users export their work accounts as .xlsx file. If you don't want, you can disable it or you can even customize it.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', the password column will be concealed when users export their work accounts as .xlsx file and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can conceal the password column while exporting work accounts as .xlsx file for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

Do you want to allow offline access for your users? If allowed, they will be able to download their data as an encrypted HTML file.

Securden have the option to allow offline access for your users. If allowed, they will be able to download their data as an encrypted HTML file. If you don't want, you can disable it and you can even customize it.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', your users will

be allowed offline access and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can allow offline access for a custom list of users. If you select 'Allow', this configuration will be applicable only to the users/groups added below. If you select 'Deny', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

Privilege Management

Would you like to automatically approve admin privilege elevation requests?

Securden allows you to automatically approve admin privilege elevation requests. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, admin privilege elevation requests will be automatically approved and if you select No, it will be disabled.

•

Would you like to allow applications to be elevated with domain admin privilege?

Securden have an option to elevate the applications with domain admin privilege. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, applications will be elevated with domain admin privilege and if you select No, it will be disabled.

Do you want to allow discovery of applications running on endpoints and servers upon installing Securden agents?

Securden allows discovery of applications running on endpoints and servers upon installing Securden agents. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, discovery of applications running on endpoints and servers will be enabled upon installing Securden agents and if you select No, it will be disabled.

On clicking the Securden agent tray icon on endpoints, what options would you like to show?

Securden allows to show the options by clicking the Securden agent tray icon on endpoints. If you don't want, you can disable it or even customize it.

When you click change, a dialog box with three options 'Application elevation for endusers', 'Technician access', and 'Both' appears. If you select 'Application elevation for endusers', only this option will be enabled and if you

select 'Technician access', technician access option will be enabled in the agent tray icon. When you select 'Both', you can avail both options.

Securden agent can fetch the latest changes from the server periodically at a specified interval. Would you like to set that time interval (in minutes) here?

Securden agent can fetch the latest changes from the server periodically at a specified interval. It allows to set that time interval (in minutes) here.

When you click change, a GUI 'Data Fetch Interval' appears. You can specify the time interval (in minutes) at which the Securden agent will periodically fetch data from the server. Click '**save**' to show changes.

Do you want to allow users to edit username on the authentication screen shown by Securden agent?

Securden allows users to edit username on the authentication screen shown by Securden agent. If you don't want, you can disable it.

•

When you click change, a confirmation box will appear saying Yes and No. If you select Yes, users will be allowed to edit the username on the authentication screen shown by Securden agent and if you want to disable it, you can select No.

Securden agent discovers running processes periodically. Do you want to create applications for the discovered processes?

Securden agent discovers running processes periodically. It allows you to create applications for the discovered processes. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you select Yes, applications can be created for the discovered processes and if you don't want to disable it, you can select No.

Do you want to display the option to reinstall/upgrade and uninstall the Securden agent on the computer details page?

Securden allows you to display the option to reinstall/upgrade and uninstall the Securden agent on the computer details page. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you select Yes, the option to reinstall/upgrade and uninstall the Securden

agent on the computer details page will be displayed and if you don't want it, you can select No.

Do you want to send a notification email to all approvers when a request is approved or rejected by a designated approver?

Securden have an option to send a notification email to all approvers when a request is approved or rejected by a designated approver. If you don't want, you can disable it

When you click change, a confirmation box will appear saying Yes and No. If you select Yes, notification email will be sent to all approvers and if you don't want, you can select No.

Do you want to enforce authentication to protect the Securden Agent from being uninstalled?

Securden provides an option to enforce authentication to protect the Securden Agent from being uninstalled. If you don't want, you can disable it.

When you click change, a GUI 'Set Authentication for Agent Uninstallation' appears. In that you can enforce a password requirement to prevent users from uninstalling the Securden Agent. To set a password requirement, click 'Yes' and enter a password. By clicking 'No', users will be able to uninstall the Agent directly. The best practice is to set a password to stop the Agent from being uninstalled. Click '**save**' to show changes.

While creating control policies, do you want to give 'Exclude' users a higher preference than 'All' users? If you choose Yes, a policy that excludes specific users will precede a different policy created for all users.

Securden gives you an option to 'Exclude' users a higher preference than 'All' users while creating control policies. If you don't want , you can disable it.

When you click change, a confirmation box will appear saying Yes and No.

If you select Yes, a policy that excludes specific users will precede a different policy created for all users and if you want to disable it, you can select No.

Do you want to enable/disable the Securden Agent to be upgraded automatically?

Securden has the option to enable/disable the Securden Agent to be upgraded automatically. If you don't want, you can disable it.

When you click change, a GUI 'Configure Agent Auto-Upgrade' appears. You have the option to upgrade the Securden Agent automatically when a newer version is available. If you Enable auto-upgrade, you need to specify the time slot during which the agent should be upgraded. It is recommended to select a time slot outside your regular business hours. If you Disable auto-upgrade, the agent will not be upgraded automatically. Click '**save**' to show changes.

Do you want to automatically pull changes from server whenever the user attempts to run applications as administrator using the UAC prompt?

Securden allows you to automatically pull changes from server whenever the user attempts to run applications as administrator using the UAC prompt. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No.

If you select Yes, changes will be pulled automatically from server and if you don't want, you can disable it.

Do you want to display the Securden privilege elevation popup over the UAC prompt whenever users attempt to elevate applications?

Securden allows you to display the Securden privilege elevation popup over the UAC prompt whenever users attempt to elevate applications. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No.

If you select Yes, the Securden privilege elevation popup will be displayed and if you don't want, you can disable it.

Offline Access

Do you want to allow automatic approval for privilege elevation requests if the user is on the automatic approval list?

Securden allows automatic approval for privilege elevation requests if the user is on the automatic approval list. If you don't want, you can disable it or even customize it.

When you click change, a confirmation box will appear saying Yes and No.

If you click Yes, automatic approval for privilege elevation requests if the user is on the automatic approval list will be enabled and if you select No, it will be disabled.

Do you want to allow offline automatic approval for privilege elevation requests if the user who is raising the request has already generated offline access codes?

Securden allows offline automatic approval for privilege elevation requests if the user who is raising the request has already generated offline access codes.

You can specify the maximum number of codes a user can generate and use to raise approval requests for temporary elevated access in offline scenarios. You can choose to apply this setting for any specific purpose as below. You have the option to specify the maximum time duration the user can have elevated access. Click '**save**' to show changes.

Do you want to allow users to regenerate offline codes? Even if you choose 'No', Users included in Automatic Approval Policies will be able to regenerate offline codes.

Securden allows users to regenerate offline codes. Even if you choose 'No', Users included in Automatic Approval Policies will be able to regenerate offline codes. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, users will be able to regenerate offline codes and if you select No, it will be disabled.

Do you want to allow privilege elevation in offline scenarios using access codes generated by the admin?

Securden allows privilege elevation in offline scenarios using access codes generated by the admin.

You can choose to allow users to use an Admin-Generated offline code for temporarily elevating specific applications or for gaining full admin access or both. You have the option to specify the maximum time duration the user can have elevated access. Click '**save**' to show changes.

Temporary Full Admin Access

Do you want to restrict the time duration for elevation requests? Once configured, users will have to specify a time duration (in minutes) within the maximum duration specified.

Securden have the option to restrict the time duration for elevation requests. Once configured, users will have to specify a time duration (in minutes) within maximum duration specified.

You can specify the upper limit (in minutes) within which users can request access for elevated access. Click '**save**' to show changes.

When allowing users to request for extending their elevated access, do you want to specify a restriction on the maximum time duration (in minutes)? If specified, users will be able to ask for an extension within the duration specified.

Securden have the option to specify a restriction on the maximum time duration (in minutes) when allowing users to request for extending their elevated access. If specified, users will be able to ask for an extension within the duration specified.

You can specify the upper time limit (in minutes) within which users can ask for an extension of the elevated access. For example, if you specify 30

minutes, users will be able to request an extension for 30 minutes or less. Click '**save**' to show changes.

Would you like to configure which privilege elevation requests can be raised by users? If set to 'Full Admin Access', they would only be able to raise requests for full admin access and not for specific applications. If set to 'For a Specific Application', they would only be able to raise requests for accessing specific applications and not for full admin access. To allow raising requests for the two, set the configuration to 'Both'.

Securden allows you to configure which privilege elevation requests can be raised by users.

When you click change, a dialog box with three options 'Application Access', 'Full Admin Access' and 'Both' appears. If set to 'Full Admin Access', they would only be able to raise requests for full admin access and not for specific applications. If set to 'For a Specific Application', they would only be able to raise requests for accessing specific applications and not for full admin access. To allow raising requests for the two, set the configuration to 'Both'.

When you grant temporary full administrator rights, the explorer process would be killed. Would you like to restart it when the user gains administrator rights?

Securden allows you like to restart it when the user gains administrator rights. When you grant temporary full administrator rights, the explorer process would be killed. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, the process will be restarted when the user gains administrator rights and if you select No, it will be disabled.

When granting temporary full administrator rights, would you like to add the user to the administrator group for the session? This will make the user a full administrator for the limited time-duration.

Securden allows you to add the user to the administrator group for the session when granted temporary full administrator rights. This will make the user a full administrator for the limited time-duration. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, the user will be added to the administrator group for the session and if you select No, it will be disabled.

If new administrator users are created when a user makes use of temporary administrator privileges, would you like to remove the newly created user from the admin group?

Securden allows you to remove the newly created user from the admin group, If new administrator users are created when a user makes use of temporary administrator privileges. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, the newly created user from the admin group will be removed and if you select No, it will be disabled.

Technician Access

Would you like to configure the MFA system used in the organization to be the additional authentication factor during technician access by users?

Securden allows you to configure the MFA system used in the organization to be the additional authentication factor during technician access by users. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, the MFA system used in the organization to be the additional authentication factor during technician access by users will be configured and if you select No, it will be disabled.

Do you want to restrict the time duration for Technician access? Once configured, users will have to specify a time duration (in minutes) within the maximum duration specified.

Securden have the option to restrict the time duration for Technician access. Once configured, users will have to specify a time duration (in minutes) within the maximum duration specified.

When you click change, a GUI appears. In that, you can specify the upper limit (in minutes) within which users can request access for technician access. Click **'save'** to show changes.

Personal

Do you want to allow your users to manage personal accounts?

Securden allows your users to manage personal accounts. If you don't want, you can disable it or even customize it.

When you click change, a dialog box with three options 'Allow for all', 'Deny for all' and 'Customize' appears. If you select 'Allow for all', users will be allowed to export their personal accounts as .xlsx file and if you select 'Deny for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can allow a custom list of users to manage personal accounts. If you select 'Allow', this configuration will be applicable only to the users/groups added below. If you select 'Deny', this configuration will be applicable to all users/groups except the ones added. Click 'save' to show changes.

Browser Extension

Do you want to allow automatic submission of credentials for directly logging in to websites using browser extension?

Securden allows your users to export their personal accounts as .xlsx file. If you don't want, you can disable it or even customize it.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', the password column will be concealed when users export their work accounts as .xlsx file and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

When accounts are shared with 'Open Connection' permission, do you want to allow automatic filling of credentials on websites using browser extension?

Securden allows automatic filling of credentials on websites using browser extension when accounts are shared with 'Open Connection' permission. If you don't want, you can disable it or even customize it. This can be done in the **Admin >> Configurations section**.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', automatic filling of credentials on websites using browser extension will be allowed and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can enable automatic filling of credentials on websites using browser extension when accounts are shared with 'Open Connection' permission for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

Do you want the Securden browser extension's auto-fill icon to be present in all input fields of the web pages?

Securden allows browser extension's auto-fill icon to be present in all input fields of the web pages. If you don't want, you can disable it or even customize it.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', Securden's browser extension's auto-fill icon will be present in all input fields of the web pages for all Users/Groups and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears.

You can enable Securden autofill icon to be filled in all input fields on websites. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click '**save**' to show changes.

Mobile App

Do you want to enable MFA for Securden mobile application?

Securden allows you to enable Multi Factor Authentication for Securden mobile application. You can disable it or you can also customize it for specific Users/Groups.

When you click change, a dialog box with three options 'Enable for all', 'Disable for all' and 'Customize' appears. If you select 'Enable for all', it will be enforced for all the users and if you select 'Disable for all', it will be denied for all the users. If you select 'Customize', a GUI appears

You can enable MFA for Securden mobile application for a custom list of users. If you select 'Enable', this configuration will be applicable only to the users/groups added below. If you select 'Disable', this configuration will be applicable to all users/groups except the ones added. Click '**Save**' to show changes.

General

Do you want to check the Active Directory port before initializing the connection with the AD? If yes, specify the time duration in seconds after which the check times out.

Securden provides an option to check the Active Directory port before initializing the connection with the AD. You can specify the time duration in seconds after which the check times out. If you don't want, you can disable it or even customize it.

When you click change, a GUI appears. In that, you can specify the time duration (in seconds) within which a response from the Active Directory domain controller is expected. Click '**save**' to show changes.

What should be the default application logging level setting?

Do you want to run password verification schedule everyday?

Securden have an option to run password verification schedule everyday. If you don't want, you can disable it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, the option to run password verification schedule everyday will be enabled and if you select No, it will be disabled.

Do you want to disable local authentication in Securden? In case, you choose not to allow local authentication, no local user will be able to login into Securden.

Securden have an option to disable local authentication. In case, you choose not to allow local authentication, no local user will be able to login into Securden. If you don't want, you can disable it or even customize it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, the option to disable local authentication will be enabled and if you select No, it will be disabled.

Do you want to display 'forgot password' option in Securden login GUI? In case, you choose not to allow this, no one in your organization, including the super administrator will see 'forgot password' link.

Securden allows an option to display 'forgot password' in Securden login GUI. In case, you choose not to allow this, no one in your organization, including the super administrator will see 'forgot password' link. If you don't want, you can disable it or even customize it.

When you click change, a confirmation box will appear saying Yes and No. If you click Yes, the option to display 'forgot password' in Securden login GUI will be enabled and if you select No, it will be disabled.

Do you want to customize the footer section for emails generated by Securden?

Securden allows you to customize the footer section for emails generated. If you don't want, you can disable it or even customize it.

When you click change, a GUI appears. In that You have the option to modify the footer section in emails generated by Securden. You can customize the existing copyright text and the footer message. Click '**save**' to show changes.

How long should the web session be active (in minutes) when things are idle?

Securden allows you to specify the maximum time (in minutes) should the web session be kept active when things are idle. You have the option to keep the session active indefinitely too.

When you click change, a GUI named 'Change Inactivity Timeout' appears. In that, you can choose 'Keep Active Indefinitely' if you want to keep the session alive or choose 'Specify Session Timeout' if you want to customize the maximum time. You have the option to logout the session on closing the browser. You can select the checkbox if you want to enable it. Click '**save**' in the end.

What should be the default date and time display format?

You can define the specific format in which the date and time should be displayed in the GUI. There is a list of various time and date formats available and you can choose from it.

When you click change, a GUI with a list of date and time display format appears. You can choose the desired format from the list. Click '**save**' to show changes.

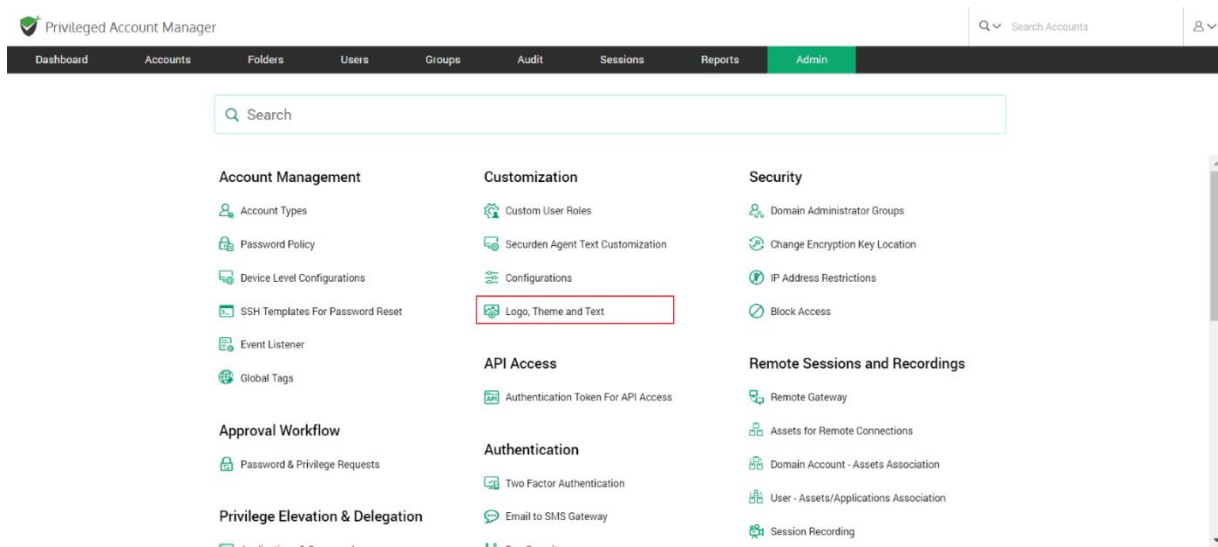
Do you want to disable the Super Administrator role?

Securden has 5 pre-defined user roles which includes user, auditor, account manager, administrator and super administrator. Super administrator is a kind of break glass account. They will not have any access control. They will be able to just view all the data stored in the application. If you don't want a super administrator role, you can disable it.

When you click change, a dialog box comes up with two options 'enable' and 'disable'. If you want a super administrator role you can click enable and if you don't want, you can disable it.

Changing Logo, Theme, and Text

You can replace the Securden logo that appears in the login page and throughout the GUI with your own logo. Navigate to **Admin >> Customization >> Logo, Theme and Text**.



Click on Logo and you can upload your logo which will replace the Securden logo that appears throughout the GUI. The logo can be uploaded in the PNG or JPG format.

Login Page Text

You can change the text that appears on the Securden login screen, including the product name and description. If you want to display any information or instructions on the login screen for your end-users or prompt them to agree to certain terms and conditions related to the usage of the product, you may do so here.

Click the **Admin >> Customization >> Logo, Theme and Text >> Login Page Text**.

The screenshot shows the Securden Admin interface. At the top, there's a header with the Securden logo and 'Privileged Account Manager'. Below the header is a navigation bar with tabs: Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin (which is highlighted). Under the Admin tab, there's a sub-menu with 'Admin > Logo, Theme and Text'. In this sub-menu, 'Login Page Text' is selected. The main content area has a heading 'You can change the text that appears on the Securden login screen, including the product name and description. If you want to display any information or instructions on the login screen for your end-users or prompt them to agree for certain terms and conditions related to the usage of the product, you may do so from here.' Below this, there are two text input fields. The first is labeled 'Product Name (in 50 characters or less)' and contains the text 'Privileged Account Manager'. The second is labeled 'Description (in 250 characters or less)' and contains the text 'Securely store, protect, and automate management of all high privileged account passwords. Control and monitor admin access to critical IT assets.' At the bottom, there's a toggle switch for 'Show Instructions/Terms and Conditions' which is currently turned off. Below the toggle are 'Save' and 'Cancel' buttons. At the very bottom, there's a URL bar showing 'https://localhost:5959/dashboard'.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Logo, Theme and Text

Logo Login Page Text Color Theme Securden Agent

You can change the text that appears on the Securden login screen, including the product name and description. If you want to display any information or instructions on the login screen for your end-users or prompt them to agree for certain terms and conditions related to the usage of the product, you may do so from here.

Product Name (in 50 characters or less)
Privileged Account Manager

Description (in 250 characters or less)
Securely store, protect, and automate management of all high privileged account passwords. Control and monitor admin access to critical IT assets.

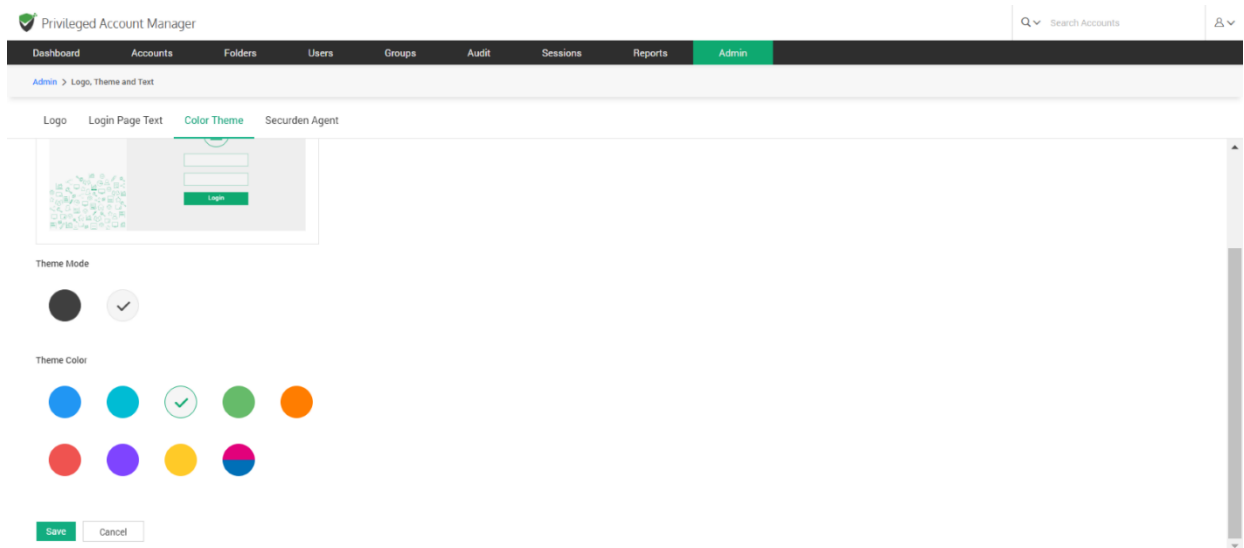
Show Instructions/Terms and Conditions ☐

Save Cancel

https://localhost:5959/dashboard

Color Theme

By default, Securden web interface follows the green color theme. You may change it and assign a different color theme by selecting a color below. The theme you set here will be the default theme for your organization and take effect for all users. However, end users can overwrite this and can choose a theme of their choice for their own views. If any of your users have already changed their theme, the change you make here will not take effect for them.



Click on **Admin >> Customization >> Logo, Theme and Text >> Color Theme**

After selecting the theme mode and theme color, click on the Save button. “Product color theme changed successfully” will be displayed on top of the screen after it is saved.

Securden Agent Theme

By default, Securden agents follows the green color theme. You may select and assign a different color theme from the options available below. The selected option will be applied to all the agents deployed on devices and will be considered as the default agent theme for your organization. You might want to display certain terms and conditions for using the Securden agent on endpoints and mandate users to agree to the terms. These terms and conditions are displayed while requesting privilege elevation. You can choose to disable the display of terms and conditions too, if this is not needed for your organization.

The screenshot displays the Securden Privileged Account Manager Admin interface. The top navigation bar includes links for Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin (which is currently selected). A search bar for accounts and a user profile icon are also present. Below the navigation bar, the breadcrumb trail shows 'Admin > Logo, Theme and Text'. The main content area has tabs for Logo, Login Page Text, Color Theme, and Securden Agent (which is active). A descriptive text block explains that the default theme is green and that terms and conditions can be displayed or disabled. Below this, there are two sections: 'Agent Theme' and 'Top Band Color'. Each section contains a grid of color circles. In the 'Agent Theme' section, the green circle is selected with a checkmark. In the 'Top Band Color' section, the green circle is also selected with a checkmark. At the bottom, there is a 'Show Terms and Conditions' toggle switch, which is currently turned off. Finally, there are 'Save' and 'Cancel' buttons.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Logo, Theme and Text

Logo Login Page Text Color Theme Securden Agent

By default, Securden agents follows the green color theme. You may select and assign a different color theme from the options available below. The selected option will be applied to all the agents deployed on devices and will be considered as the default agent theme for your organization. You might want to display certain terms and conditions for using the Securden agent on endpoints and mandate users to agree to the terms. These terms and conditions are displayed while requesting privilege elevation. You can choose to disable the display of terms and conditions too, if this is not needed for your organization.

Agent Theme

Top Band Color

Show Terms and Conditions ☐

Save Cancel

Product Language Selection

Securden supports multiple languages, and you can select the desired language here. The language of the machine in which Securden is installed is taken as the system default language. From the list of supported languages, you can select the ones required for your organization. You can then select one of the languages as the 'default' selection for your organization. When you do so, all your users will see the product in that language. Individual users will have the option to select any language from the list of languages approved by you.

Navigate to **Admin>> Customizations >> Product Language Selection**.

The screenshot shows the Securden Admin interface. At the top, there's a header with the Securden logo and 'Privileged Account Manager'. Below the header is a navigation bar with tabs: Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin (which is highlighted). Below the navigation bar is a breadcrumb trail: Admin > Product Language Selection. The main content area is titled 'Product Language Selection'. It contains a paragraph explaining that Securden supports multiple languages and that the language of the machine is the system default. Below this is a section titled 'Pick Desired Languages' with a sub-header 'Securden supports the following languages at present. Select the ones that are required for your organization. End users will get the option to use one of the languages selected by you.' There are three toggle switches: English (Default) is turned on, French is turned on, and Deutsch is turned off. Below this is a section titled 'System Default Language' with a sub-header 'You can specify one of the languages selected above as the system default language. The language that is set as the default language will appear for all your users. However, they can later override the default selection and use one of the languages approved by you.' There is a dropdown menu showing 'English' and a 'Change' button next to it.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Product Language Selection

Product Language Selection

Securden supports multiple languages and you can carry out the desired language selection here. The language of the machine in which Securden is installed, is taken as the system default language. From the list of supported languages, you can select the ones required for your organization. You can then select one of the languages as the 'default' selection for your organization. When you do so, all your users will see the product in that language. Individual users will have the option to select any language from the list of languages approved by you.

Pick Desired Languages

Securden supports the following languages at present. Select the ones that are required for your organization. End users will get the option to use one of the languages selected by you.

English (Default) ☒

French ☒

Deutsch ☐

System Default Language

You can specify one of the languages selected above as the system default language. The language that is set as the default language will appear for all your users. However, they can later override the default selection and use one of the languages approved by you.

English [Change](#)

The screen will display the languages that are currently supported by Securden. You will have to select the language from Pick Desired Languages according to your organization's requirements. Once the desired language is enabled, a message "Language Activated Successfully" will be displayed on top of the screen. When you disable any language, it will display the message - **Language deactivated successfully**. End users will get the option to use one of the languages selected by you.

The languages available and supported by Securden at present are:

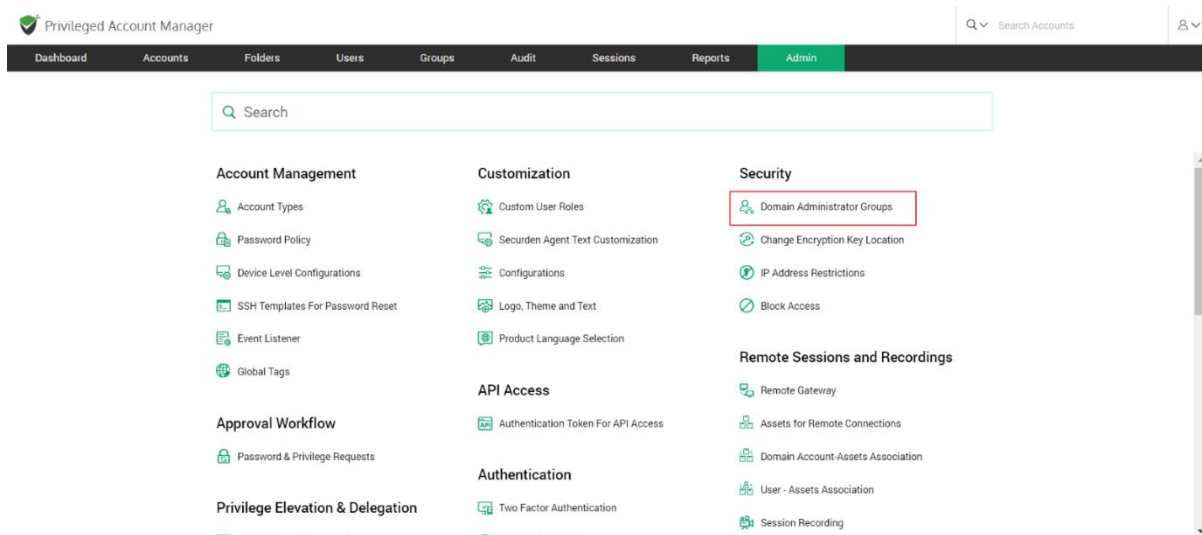
- English
- French
- Deutsch

Then you can specify one of the languages selected above as the System Default Language. The language selected as default here will appear for all your users. However, they can later override the default selection and use one of the languages approved by you.

Section 14: Security Settings

You can carry out certain security settings to protect the Securden installation and control access to the interface.

Monitor Changes to Domain Admin Groups

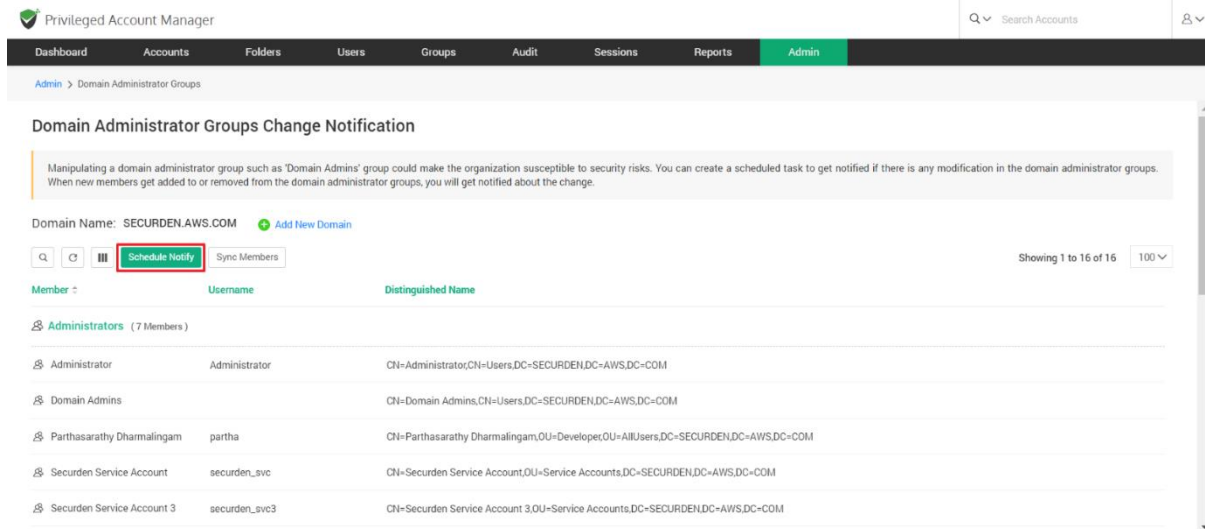


Manipulating a domain administrator group such as the **Domain Admins** could make the organization susceptible to security risks. You can create a scheduled task to get notified if there is any modification to the domain administrator groups. When new members get added to or removed from the domain administrator groups, you will get notified about the change. Securden can monitor the changes to the domain admin groups of all the

Active Directory domains added to the product. You can create a scheduled task to periodically monitor and send notifications.

How to Schedule Notifications?

To Schedule Notifications, Navigate to **Admin >> Security >> Domain Administrator Groups**. In the GUI that opens, click the button **Schedule Notify**.



You have two options here - carry out the check once (Notify Once) at the required timeslot and trigger notification (or) carry out the check at periodic intervals (Notify Periodically). Select the required option in GUI.

You can choose to send notifications to all Administrators or all Super administrators or to both administrators and super administrators. Select the checkbox as needed. You can even add email addresses directly in comma separated form in the **Specific Email Address** field.

When you navigate to **Admin >> Security >> Domain Administrator Groups** section in the GUI, it typically shows the list of all administrator groups present in the selected domain. You can click the button **Sync Members** to view the latest data anytime.

As mentioned above, you can monitor the changes to domain admin groups for multiple domains. You can add the domains to be monitored by clicking the button **Add New Domain**.

The screenshot displays the Privileged Account Manager interface. The top navigation bar includes links for Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin (highlighted in green). A search bar labeled 'Search Accounts' is on the right. Below the navigation bar, the breadcrumb trail reads 'Admin > Domain Administrator Groups'.

The main content area is titled 'Domain Administrator Groups Change Notification'. It contains a warning message: 'Manipulating a domain administrator group such as 'Domain Admins' group could make the organization susceptible to security risks. You can create a scheduled task to get notified if there is any modification in the domain administrator groups. When new members get added to or removed from the domain administrator groups, you will get notified about the change.'

Below the warning, the 'Domain Name' is set to 'SECURDEN.AWS.COM'. A red box highlights the '+ Add New Domain' button. To the right of the domain name are buttons for 'Schedule Notify' and 'Sync Members'.

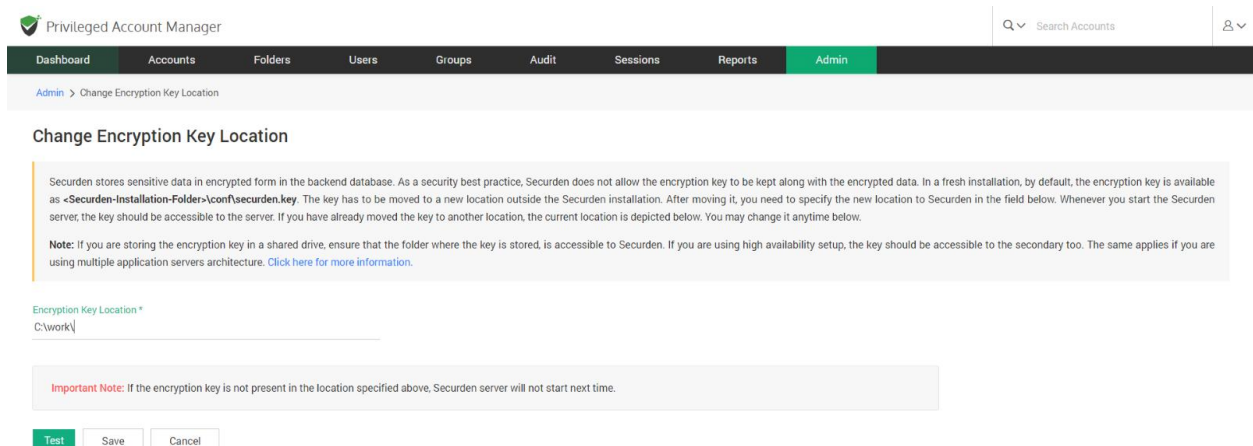
A table lists the domain administrator groups. The table has columns for 'Member', 'Username', and 'Distinguished Name'. The first row is a header for 'Administrators (7 Members)'. The subsequent rows list individual group members.

Member	Username	Distinguished Name
Administrators (7 Members)		
Administrator	Administrator	CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM
Domain Admins		CN=Domain Admins,CN=Users,DC=SECURDEN,DC=AWS,DC=COM
Parthasarathy Dharmalingam	partha	CN=Parthasarathy Dharmalingam,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM
Securden Service Account	securden_svc	CN=Securden Service Account,OU=Service Accounts,DC=SECURDEN,DC=AWS,DC=COM
Securden Service Account 3	securden_svc3	CN=Securden Service Account 3,OU=Service Accounts,DC=SECURDEN,DC=AWS,DC=COM

At the bottom right, it says 'Showing 1 to 16 of 16' with a dropdown menu set to '100'.

Change the Encryption Key Location

Every installation of Securden is protected with a unique encryption key. By default, this encryption key is located at <securden installation folder>/conf/securden.key for evaluation purposes. Securden doesn't allow the encryption key and the encrypted data to reside in the same location to ensure security. Hence, the key has to be moved outside the Securden installation folder.



The screenshot shows the Securden Admin interface. The top navigation bar includes 'Dashboard', 'Accounts', 'Folders', 'Users', 'Groups', 'Audit', 'Sessions', 'Reports', and 'Admin' (highlighted). Below the navigation bar, the breadcrumb trail reads 'Admin > Change Encryption Key Location'. The main heading is 'Change Encryption Key Location'. A text box explains that Securden stores sensitive data in encrypted form and that the encryption key must be moved to a new location outside the installation folder. It notes that the key should be accessible to the server and that the current location is depicted below. A note specifies that if the key is stored in a shared drive, it must be accessible to the secondary server in a high availability setup. Below this, the 'Encryption Key Location' field is shown with the value 'C:\work\'. At the bottom, there is an 'Important Note' stating that if the key is not present in the specified location, the Securden server will not start next time. Finally, there are three buttons: 'Test', 'Save', and 'Cancel'.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions 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 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.

Test Save Cancel

When deploying the product to production, Securden enforces moving the key out of the installation folder. The encryption key is essential to start the Securden server. If the key is not present in the new location, Securden server won't start. After moving the key to some other secure location, you need to specify the new location as explained below:

To specify the new location,

1. Navigate to **Admin >> Security >> Change Key location.**
2. Specify the location.
3. Click **Test** to check whether the key is found in the specified location.
4. If the floating screen states “Securden encryption key not found in the path specified”, check if the key is found in the new location.
5. If the encryption key was found in the specified location, A floating screen will appear containing a message stating **Encryption key found in the path specified.**
6. Click **Save.**

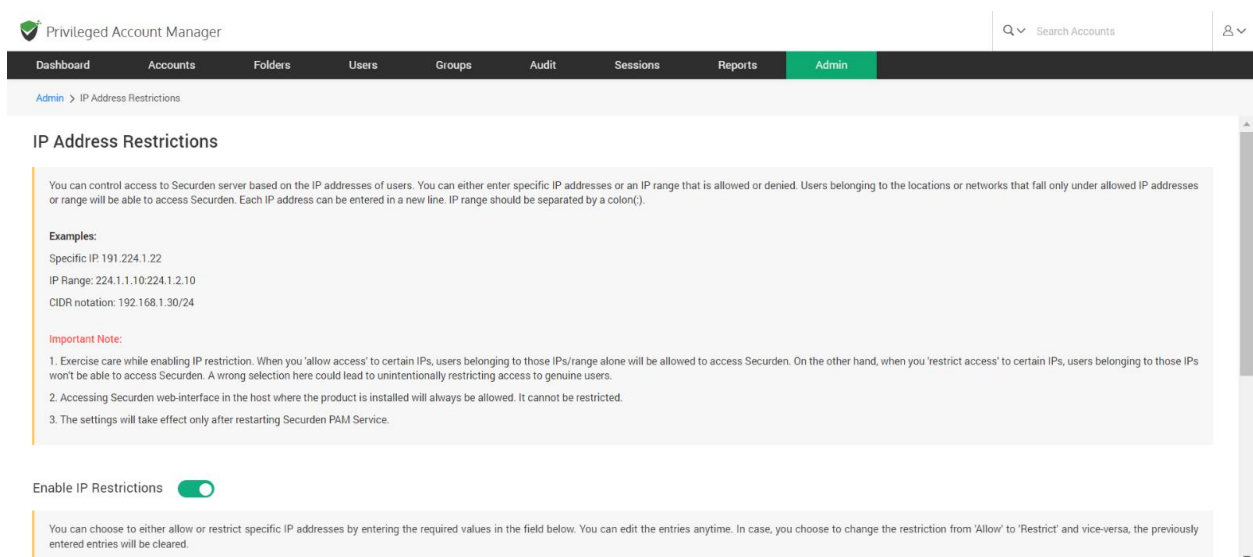
Note: If the server fails to start, you can view the current location of the encryption key by opening the Securden_key.location file using any text editor. This file is located at <Securden Installation folder>/conf/Securden_key.location. You need to have the encryption key in the location specified in this file for the Securden server to start.

IP Address Restriction

Securden gives you the option to control and restrict access to Securden Server based on the user's IP address. You can either enter specific IP addresses or an IP range that is allowed or denied. Users belonging to the locations or networks that fall only under allowed IP addresses or range will be able to access Securden.

Enable IP Restrictions

To Enable IP Restrictions, navigate to **Admin >> Security >> IP Address Restrictions >> Enable IP Restrictions** and move the toggle **Enable IP Restrictions** to green.



Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > IP Address Restrictions

IP Address Restrictions

You can control access to Securden server based on the IP addresses of users. You can either enter specific IP addresses or an IP range that is allowed or denied. Users belonging to the locations or networks that fall only under allowed IP addresses or range will be able to access Securden. Each IP address can be entered in a new line. IP range should be separated by a colon(:).

Examples:

Specific IP: 191.224.1.22

IP Range: 224.1.1.10:224.1.2.10

CIDR notation: 192.168.1.30/24

Important Note:

1. Exercise care while enabling IP restriction. When you 'allow access' to certain IPs, users belonging to those IPs/range alone will be allowed to access Securden. On the other hand, when you 'restrict access' to certain IPs, users belonging to those IPs won't be able to access Securden. A wrong selection here could lead to unintentionally restricting access to genuine users.
2. Accessing Securden web-interface in the host where the product is installed will always be allowed. It cannot be restricted.
3. The settings will take effect only after restarting Securden PAM Service.

Enable IP Restrictions ☒

You can choose to either allow or restrict specific IP addresses by entering the required values in the field below. You can edit the entries anytime. In case, you choose to change the restriction from 'Allow' to 'Restrict' and vice-versa, the previously entered entries will be cleared.

Here you choose either to allow access or to restrict access.

Enter one or multiple IP addresses. Each IP address can be entered in a new line. IP range should be separated by a colon (:).

Examples:

Specific IP: 191.224.1.22

IP Range: 224.1.1.10:224.1.2.10

CIDR notation: 192.168.1.30/24

Note:

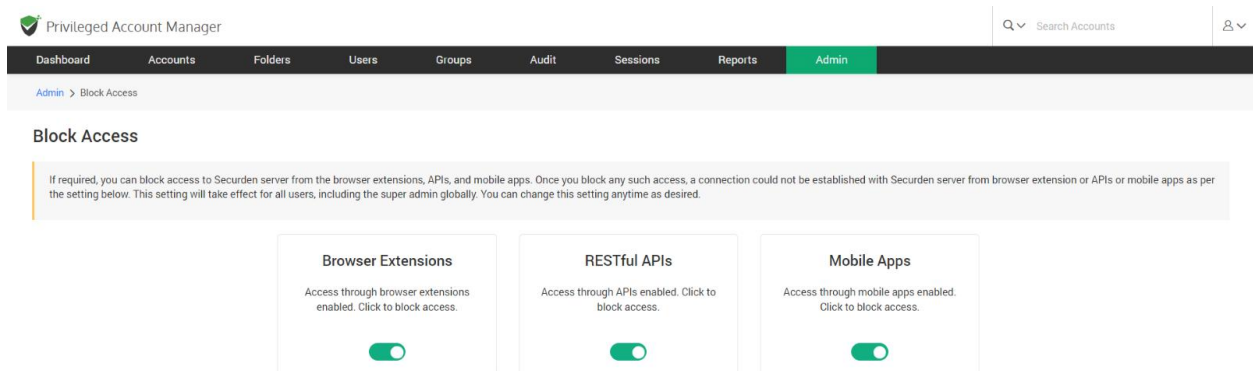
- Exercise care while enabling IP restriction. When you allow access to certain IPs, users belonging to those IPs/ranges alone will be allowed to access Securden. On the other hand, when you restrict access to certain IPs, users belonging to those IPs won't be able to access Securden. A wrong selection here could lead to unintentionally restricting access to genuine users.
- Accessing the Securden web interface in the host where the product is installed will always be allowed. It cannot be restricted.

Finally, click "Save". The settings will take effect only after restarting Securden PAM Service.

Block Access through API, Extensions, Mobile Apps

Securden allows you to block and filter access to its server from extensions, API, and mobile applications. Once you block any such access, a connection could not be established with the Securden server from browser extension or APIs or mobile apps as per the setting below. This setting will take effect for all users, including the super admin globally. You can change this setting anytime as desired.

To block access, navigate to **Admin >> Security >> Block Access**.



You can block access through browser extensions, APIs, or mobile apps by moving the green toggle to red.

You can change this setting anytime as required

Section 15: Emergency Access Settings

Configure Emergency Access

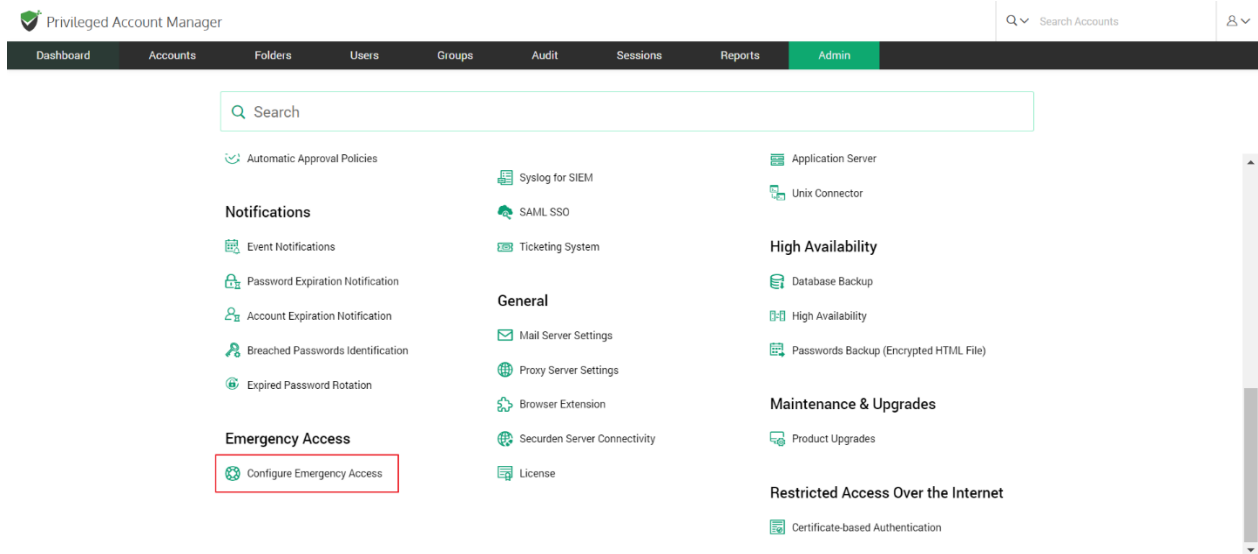
Emergency access, as the name implies, is used in highly critical and urgent situations. For instance, imagine the scenario when an administrator who has access to an IT resource is away and your team requires immediate access to the device. The emergency access feature helps in this scenario to gain access in a hassle-free manner with a well-defined workflow.

How does emergency access work?

You can enable a designated list of users as 'Emergency Access Users' allowing them to access all passwords (work accounts) stored in Securden, breaking the usual access controls during emergency situations. When an emergency access requirement arises, any of the designated users will first declare emergency and get access after the predefined mandatory waiting period. In the meantime, all administrators will be notified of the situation.

Configuring emergency access

To configure emergency access, navigate to **Admin >> Emergency Access >> Configure Emergency Access**.



In the GUI that opens, you can designate the users who should get the emergency access privilege. You can define the maximum time duration until which the user should have emergency access.

As an additional control, you can define a mandatory waiting period (in minutes) until the person should wait before gaining emergency access. All administrators will be notified when someone wants to gain emergency access.

Move the toggle **Enable Emergency Access** to turn on emergency access. You will see two options namely, **All users** and **Specific users**. As the name itself implies, **All users** option grants the emergency access privilege to all the users. On the other hand, if you want to grant the privilege only to certain specific users or groups of users, you need to choose the option **Specific users**.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports **Admin**

Admin > Configure Emergency Access

Emergency Access Configurations

You can enable a designated list of users to access all passwords (work accounts) stored in Securden, breaking the usual access controls. This is to meet password access needs during certain emergencies. In this interface, you can designate the users who should get the emergency access privilege. You can define the maximum time duration until which the user should have emergency access. As an additional control, you can define a mandatory waiting period (in minutes) until the person should wait before gaining emergency access. All administrators will be notified when someone wants to gain emergency access.

Enable Emergency Access ☒

Select the users who can make use of emergency access

☒ All Users ☐ Specific Users

Emergency access duration minute(s)

Wait for minutes(s) after emergency access is initiated.

When you choose the **Specific users**, you need to select the users or groups from the list. You can define the maximum duration up to which a user can avail emergency access. Specify the duration in minutes. As a security best practice, to guard against any possible misuse of the provision, you can enforce a mandatory waiting period for anyone to gain access after **breaking the glass**. During this window, notifications will go to all administrators, who can revoke access if any suspicious motive is found. You can define the waiting time in minutes. After configuring these values, click **Save**.

The above steps complete the emergency access configuration. The configuration done by one administrator has to be approved by another administrator. The approval can be done from the same page in the GUI. When another administrator logs in, the link to approve or reject the request will be visible as shown below.

How to initiate emergency access?

When an emergency access requirement arises, the designated user(s) can initiate the access from **Admin >> Emergency Access >> Initiate Emergency Access**. In the GUI that opens, the user has to justify why emergency access is needed. As per the emergency access configuration, the user will get access.

Section 14: Disaster Recovery Settings

Database Backup

To ensure uninterrupted access to passwords even in the unlikely event of a disaster, you can take a backup of the entire database and store it in a secure location. If something goes wrong with the existing installation, you can do a quick recovery of data. Backup can be taken anytime on-demand and at periodic intervals by creating a scheduled task.

Configuring Backup

To configure database backup, navigate to **Admin >> High Availability >> Database Backup** section in the GUI. There are two options to choose from when scheduling a backup. You can choose to take a backup once whenever required or at periodic intervals.

If you want to take a backup instantly, you can click on **Backup Now**. If you choose **Take Backup Once**, follow the steps below:

1. Select the date and time when you want to take backup once.
2. If needed, change the backup destination from its default location by providing the destination folder path. When the backup file is to be stored in another machine, you can specify the network path to that

destination.

3. Specify the maximum number of backups to be retained in that location. For example, if you specify this as 5, only the most recent 5 backup copies will be retained. Click **Save**

If you choose 'Take Backup Periodically', follow the steps below to create a scheduled task:

1. Choose the date and time of the first backup.
2. Thereafter, you can schedule backups on an hourly, daily, weekly, and monthly basis. Choose an option between 'Hours', 'Days', 'Weeks', and 'Months' from the drop-down menu. Specify the number of hours/days/weeks/months in the adjacent space.
3. If needed, change the backup destination from its default location by providing the destination folder path. When the backup file is to be stored in another machine, you can specify the network path to that destination.
4. Specify the maximum number of backups to be retained in that location. For example, if you specify this as 5, only the most recent 5 backup copies will be retained.
5. Click **Save**

Disabling the Database Backup

You can use the disable option to delete an already existing backup schedule along with its configurations.

Important Note: Every installation has a randomly generated, unique encryption key, using which sensitive data are encrypted and stored in the database. By default, the encryption key is located at <Securden-Installation-Folder>/conf/securden.key. Securden doesn't allow the encryption key and encrypted data to reside together. It has to be moved to some other location. When you start the Securden server, the key should be available in the path specified every time. Otherwise, the server won't start, and you won't be able to access the passwords.

This encryption key is needed to restore the data from the backup copy. If you don't have the encryption key, data cannot be restored. Ensure that you have a copy of the encryption key for disaster recovery.

Steps for Data Recovery

In the event of a disaster, you can restore the data and the configurations from a backup file.

Important Note: The backup data is encrypted using the same encryption key as the original. For data restoration, Securden requires access to the encryption key.

Ensure the key is available at the location specified in the current(new) installation of Securden. By default, the encryption key is located at <Securden-Installation-Folder>/conf/securden.key.

You can also identify the current location of the encryption key by navigating to **Admin >> Security >> Change encryption key location**, and hovering the pointer over the “i” icon (or) Open the file named Securden_key.location using a text editor. This file can be found at <Securden installation folder>/conf/Securden_key.location

To Recover the backed-up data, follow the steps below

- Install Securden in a new machine without disturbing the existing installation.
- Stop the Securden server.
 - Open services.msc
 - Navigate to Securden PAM Service.
 - **Stop** the service.
- Open Command Prompt by clicking on 'Run as Administrator'.
- Navigate to <Securden-Installation-Folder>/bin.
- In the cmd window, use the following command.

➤ RestoreDatabase.exe <enter the full path of the backup file>

➤ Example: RestoreDatabase.exe

C:\ProgramFiles\Securden\PAM\exports\PostgreSQL_Backups\Securden_postgresql_db_backup_2019-05-22-11-48-22.zip

- Start Securden PAM service from services.msc. (You can safely ignore the other service named Securden Web Service, which is automatically taken care of).

Backup of Passwords as an Encrypted HTML File

As an additional backup option, super administrators can take a backup of all passwords in the form of an encrypted HTML file. These HTML files can be opened using a web browser. A passphrase has to be provided at the time of configuring the schedule. This passphrase will be used as the encryption key. Whenever the file has to be opened, the passphrase has to be supplied. The passphrase is not stored anywhere.

The encrypted HTML file contains work accounts only. The personal accounts of the users cannot be backed up. As mentioned above, only super administrators can create the schedule. Administrators can view the schedules created by a super administrator.

To configure backup of passwords as an encrypted HTML file, navigate to **Admin >> High Availability >> Password Backup** (Encrypted HTML file). You will see options to configure backup once or periodically.

You can also specify the location where the encrypted HTML file should be stored and in the case of periodic backup, how many copies to be retained. If you specify 5, the most recent five backfiles will be retained.

Section 16: High Availability

[High Availability configuration steps are also available as separate guides for the default PostgreSQL as the backend database and optional MS SQL server as the backend separately. You may refer to them if needed.]

Configure High Availability

Securden comes with High availability architecture to ensure uninterrupted and a reliable supply of credentials. Configuring High Availability (with PostgreSQL database as the backend) To configure high availability in Securden Unified PAM, 2 or more servers have to be deployed.

1. Primary server with bundled PostgreSQL database.
2. One secondary standby server with bundled PostgreSQL database.
3. One more application server without a database (optional).

Securden uses an active-active approach to high availability support. A primary server and a secondary server will be active at the same time and will have their own databases. In the event of a primary server going down, users can connect to the secondary standby server. Additionally, any number of application servers can be deployed for load distribution.

Two types of secondary servers can be deployed and both have different use cases. You may choose one of the options below:

Case 1: Automatic failover with active standby. When the secondary server is deployed as a standby server, the database will be replicated and periodically synchronized with the primary server database. You will be able to enable automatic failover only when one of the secondary servers deployed is of this type. Only one such server can be deployed and it has to be deployed in the same subnet as the primary server for the automatic failover to work.

Case 2: Load distribution using application servers without database. You can also deploy a secondary server as an application server without a database. The secondary server will only have the securden application installed and not a database. Since there is no separate database other than the one in the primary server, automatic failover will not be possible. This type of secondary server is useful when you need to deploy more than one secondary server. It is mainly used for load distribution by ensuring no single server bears too much demand and reduces application response time for users.

Notes

1. For automatic failover to work, the database port (5858) of the standby server must be accessible from the primary application server. Also, ensure that the standby server is in the same subnet as that of the primary server.
2. The primary and secondary servers must be running the same version of Securden. Navigate to User Details (User icon at the top right corner) >> About >> Version to check the current product version. Contact Securden Support if you need any assistance.

Pre-requisites: A primary server with Securden Unified PAM up and running and using the bundled PostgreSQL database. Refer to our installation guide to install the application.

Summary of Steps

Step 1: Setting up a secondary server

Step 2: Configuring High Availability in the primary server.

Step 3: Downloading and Transferring the high availability package.

Step 4: Configuring the Secondary server.

Step 5: Verifying the high availability setup

Step 1: Setting up a Secondary Server

1. Identify a machine that would act as a secondary server. Consider the current Securden Unified PAM installation as the primary server.
2. Install Securden Unified PAM on the chosen machine. Refer to our installation guide if you need help with the installation process.

Note: Make sure both the machines are running the same version of Securden Unified PAM.

Navigate to User Details (On the top right corner) >> About >> Version to check for the current product version. Contact Securden Support for any Assistance.

Step 2: Configuring HA in the primary server

1. Navigate to Admin>> High Availability in the GUI of Securden Unified PAM in the primary server.
2. Click the 'Configure Secondary Application Server' button and enter the following details regarding the secondary server.

Server Identifier - Provide a name that helps identify the secondary application server.

Address - hostname/ IP address of the machine where the secondary server instance has been installed.

Secondary Type - Two types of secondary servers can be deployed: Application server without database and Standby Server. Select **Standby** and click **Save**.

STEP 3: Downloading and deploying the high availability package

1. Once the details of the secondary server have been saved, a pop-up with the title 'Download and Deploy the High Availability Package' will appear in which you will have an option to download the package as a zip file.

You can also download the package from the main High Availability GUI too. Navigate to **Admin >> High Availability >> High Availability**. In this GUI you will have the download option right next to the secondary server in the server list.

2. Transfer the downloaded zip file to the secondary server.

STEP 4: Configuring the secondary server

1. Stop the server if it is running. Open windows service manager (run services.msc) and stop Securden PAM Service.
2. Put the High availability package under the "<Securden Installation folder(Secondary)>/bin" directory.
3. Open Command Prompt with administrator privileges and navigate to the "< Securden Installation folder(Secondary)>/bin" directory.

Then execute the following command: ApplyHAPackage.exe-<Secondary server Identifier>.zip

4. Securden secondary server shares the same encryption key as the primary server. Ensure the location of securden.key as mentioned in "<Securdensecondary installation folder>/conf/securden_key.location" is accessible from the secondary server. (You can open securden_key.location with any text editor)
5. Start the service again on the secondary server. To start the service, open Windows service manager (run services.msc) and start Securden PAM service.

Securden High availability setup is now ready.

STEP 5: Verifying High availability

1. Navigate to admin>>High availability in the GUI of the primary server.
2. Check the status column for the secondary server. If the status shows "Running", It means high availability is available working properly.

Deploying additional secondary application servers without DB (Optional)

You can deploy any number of secondary application servers without database. You need to deploy additional servers only if you need to distribute the load between multiple servers. To deploy additional secondary application servers without database, follow Step 1 through Step 5 again and except for "Standby" as secondary type in Step 2, select "App server without DB"

Troubleshooting Tip

Status column for the secondary shows "Data sync in progress" for a long time or **Data replication to standby stopped.**

Solution

This issue can occur when the database port (5858) of the primary server is not accessible from the secondary standby server or vice-versa. Run the following Telnet commands to verify these connections:

In secondary server: Telnet <primary server address> 5858

In primary server: Telnet <secondary server address> 5858

If these two connections are not working, you should be able to resolve it by creating an inbound firewall rule to allow access to the database port in both primary and secondary standby servers.

To add an inbound rule,

1. Open "Windows Defender Firewall with Advanced security"
2. Go to Inbound Rules and select New Rule. Add the following rule.
3. Rule Type: Port
4. Protocols and Port: TCP, 5858
5. Action: Allow the connection
6. Profile: Domain, Private, Public
7. Name(Example): TCP5858
8. Click Finish

Configuring High availability with MS SQL Server as the Backend Database

To configure High availability in Securden Unified PAM, you will need two or more application servers and a database server with MS SQL server installed. Securden enables the configuration of multiple application servers for high availability. You can configure any number of application servers as a measure to ensure high availability. In the event of the primary server going down, Users can connect to a secondary server.

To provide high availability for the Database, you need to set up your MS SQL server database with SQL clustering or AlwaysOn High availability groups.

Prerequisites: A primary server with Securden Unified PAM and MS SQL database should be installed and kept running. Refer to our Installation guide to install the application. You can refer to the **Optional: Change Backend database to MS SQL server** section in the document to set up an MS SQL Server as the backend database.

Summary of Steps

Step 1 Setting up a secondary server

Step 2 Configuring High Availability in the primary server.

Step 3 Downloading and Transferring the high availability package.

Step 4 Configuring the Secondary server.

Step 5 Verifying the high availability setup

STEP 1: Setting up a Secondary Server

1. Identify a machine that would act as a secondary server. Consider the current Securden Unified PAM installation as the primary server.
2. Install Securden Unified PAM on the chosen machine. Refer to the installation guide if you need help with the installation process.

Note: Make sure both the machines are running the same version of Securden Unified PAM. Navigate to User Details (On the top right corner) >> About >> Version to check for the current product version. Contact Securden

Support for any assistance.

STEP 2: Configuring HA in the Primary Server

1. Navigate to Admin>> High Availability in the GUI of Securden Unified PAM in the primary server.
2. Click the 'Configure Secondary Application Server' button and enter the following details regarding the secondary server.
 - a. Server Identifier - Provide a name that helps identify the secondary application server.
 - b. Address - hostname/ IP address of the machine where the secondary server instance has been installed.

STEP 3: Downloading and Transferring the Download Package

1. Once the details of the secondary server have been saved, a pop-up with the title **Download and Deploy the High Availability Package** will appear in which you will have an option to download the package as a zip file.

You can also download the package from the main High Availability GUI too. Navigate to Admin>>High Availability>> High availability. In this GUI you will have the download option right next to the secondary server in the server list.

2. Transfer the downloaded zip file to the secondary server.

STEP 4: Configuring the secondary server

1. Stop the server if it is running. Open windows service manager (run services.msc) and stop Securden PAM Service.
2. Put the High availability package under the "`<Securden Installation folder(Secondary)>/bin`" directory.
3. Open Command Prompt with administrator privileges and navigate to the "`< Securden Installation folder(Secondary)>/bin`" directory.

Then execute the following command: `ApplyHAPackage.exe-<Secondary server Identifier>.zip`

4. Securden secondary server shares the same encryption key as the primary server.

Ensure the location of securden.key as mentioned in "`<Securden secondary installation folder>/conf/securden_key.location`" is accessible from the secondary server. (You can open `securden_key.location` with any text editor)

5. Start the service again on the secondary server. To start the service, open Windows service manager (run services.msc) and start Securden PAM service. Securden High availability setup is now ready.

STEP 5: Verifying High availability

1. Navigate to admin>>High availability in the GUI of the primary server.
2. Check the status column for the secondary server. If the status shows "Running", It means high availability is available working properly.

Troubleshooting Tips

Issue: The secondary server fails to start after startup.

Solution 1:

Make sure both the machines are running the same version of Securden Unified PAM. Navigate to User Details (On the top right corner) >> About >> Version to check for the current product version. Contact Securden Support for any Assistance.

Solution 2:

Verify the location of the encryption key in the secondary server. Whenever Securden is run, the key should be accessible to the server. Otherwise, the server won't start. Securden secondary server shares the same encryption key as the primary server. Ensure the location of securden.key as mentioned in "<Securden secondary installation folder>/conf/securden_key.location" is accessible from the secondary server. (You can open securden_key.location with any text editor)

Solution 3:

Database port (1433) of MS SQL and web server port (5959) should be accessible from the secondary server. Run the following telnet commands in your secondary server to verify the connections

Telnet <database server address> 1433

Telnet <primary server address> 5959

If any of the ports are inaccessible, you can resolve it by creating an inbound firewall rule for that particular port in the primary server or the database server.

To add an inbound rule,

1. Open "Windows Defender Firewall with Advanced security"
2. Go to Inbound Rules and select New Rule. Add the following rule.
3. Rule Type: Port
4. Protocols and Port: TCP,<Port Number>
5. Action: Allow the connection
6. Profile: Domain, Private, Public
7. Name(Example): TCP5959
8. Click **Finish**

Section 17: Distributed Architecture

Remote Distributors

To manage networks distributed across multiple locations, you can make use of the remote distributors in Securden. The remote distributors are Application servers for Windows and Unix Connectors for Linux.

Configure Application Servers for Distributed Networks

As part of product deployment, Securden offers the flexibility to deploy multiple application servers to take care of certain specific needs such as IT infrastructure spread across multiple networks. If your IT assets/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 servers deployment is a three-step process - first, you need to add the required application servers, then associate each application server with a remote gateway, and finally associate the IT assets in each network with the gateway.

Adding an application server

Prerequisite: Identify the Windows machine(s) in which you will be deploying the Securden Application Server(s). Typically, you would need machines with the same specifications as that of Securden installation.

Step 1: Enter details about the application server

In this step, you will simply be creating an identifier for each of the application servers (also called secondary servers) you want to add.

To enter the details, Navigate to **Admin >> Remote Distributors >> Application Server** and click the button **Create Application Server**. In the GUI that opens, enter the following details:

Server identifier: Server identifier is just a name that helps identify the specific application server. The machines where you install application servers should be able to access the database running with the Securden primary server.

Address: You need to specify the hostname/IP address of the machine where the application server instance has been installed. Whenever you add or change the IP address or hostname of the machines where you have installed application servers, you need to restart the Securden

primary server. Ensure that the standby server is in the same subnet as that of the primary server for failover to work.

When you click **Save**, you will see a pop-up, which will provide you the link to download the application server package as a .zip file. Follow the instructions on that page before downloading the zip file. You need to restart the Securden primary server before downloading the zip. (You will see the title 'download high availability package'. It represents the application server package download).

Step 2: Deploy application server package on the designated Machine

You need to deploy the zip file you have downloaded in step 1 above on the machine which has been identified for the purpose of deploying the application Server.

Pre-requisites:

- The application server should be able to access the port of the primary server (default 5959) through the primary server's address you have specified on server settings.
- The application server should be running the same product version of Securden primary server. Contact Securden support if you need any assistance.

Carry out the following steps in the machine where you have installed the application server:

- Stop the Securden PAM Service

- Unzip the application server package (high availability package downloaded above) under **<Securden AppServer installation folder>/bin** directory.
- Open a command prompt with Administrator privileges and navigate to **<Securden AppServer installation folder>/bin** directory. Then execute the following command: **ApplyHAPackage.exe HA-<name>.zip**
- Securden AppServer server shares the same encryption key as that of the Primary installation. Ensure the location of securden.key as mentioned in "**<Securden Secondary installation folder>/conf/securden_key.location**" is accessible from the secondary Machine.
- Start the service. Securden high availability setup is now ready.

Step 3: Associate application server with a remote gateway

After configuring the application server, you need to associate it with a remote gateway. This can be done from **Admin >> Remote Sessions and Recordings >> Remote Gateway**.

In the GUI that opens, select the required remote gateway and then select **Associate Application Server** and click **Configure**. In that page, the list of all available application servers would be displayed. You need to select this application server and click **Save**.

After completing this association, you need to associate the devices and/or domains that you want to manage through this application server. Typically, this is an association between Application Servers → Remote Gateway → IT Infrastructure to be Managed. This association is to be done through step 3 in the Remote Gateway configuration page.

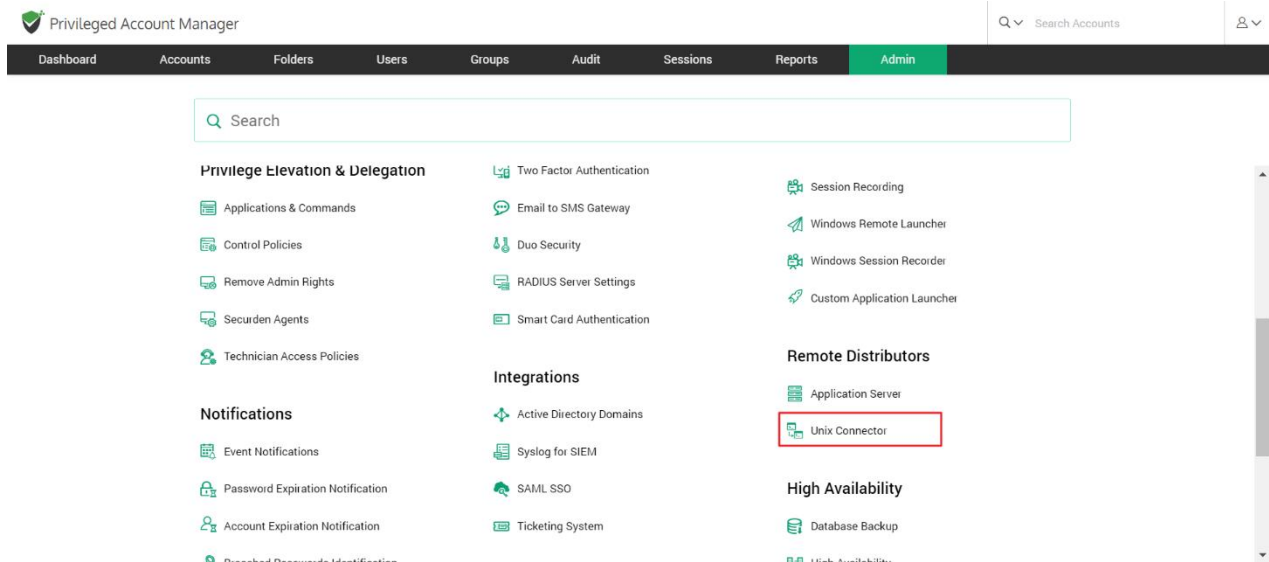
Once this is done, the application server would be fully ready to manage the respective network.

Unix Connector

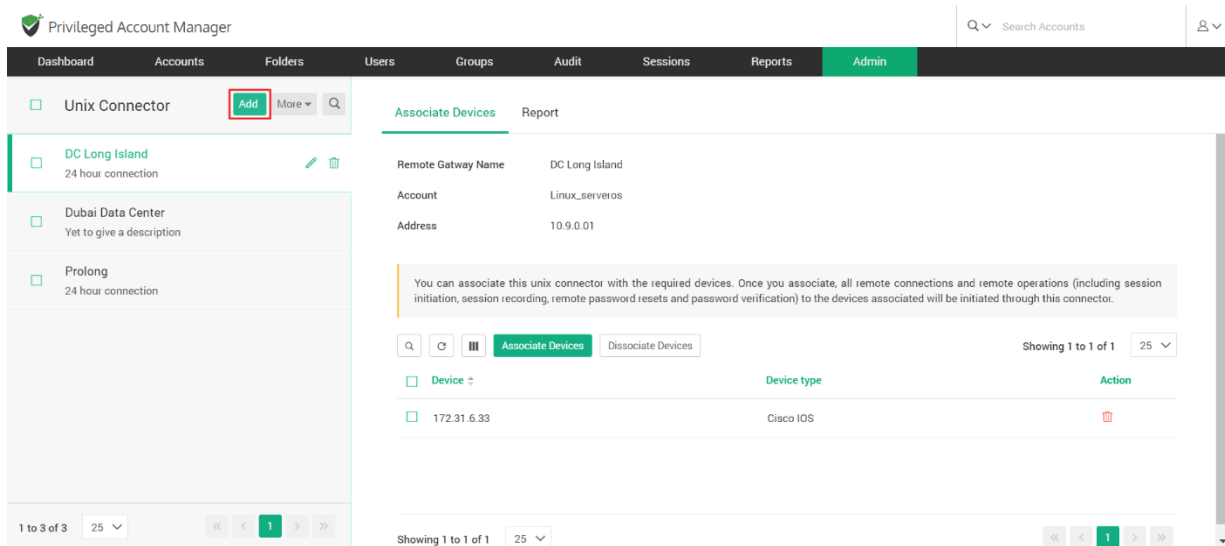
You can associate this Unix connector with the required devices. Once you associate, all remote connections and remote operations (including session initiation, session recording, remote password resets and password verification) to the devices associated will be initiated through this connector.

Add a Unix Connector

Navigate to **Admin >> Remote Distributors >> Unix Connector** to add and manage Unix connectors.



In the GUI that opens, click on **Add**.



To add a new Unix Connector, you need to specify the following details:

The screenshot shows the 'Privileged Account Manager' interface with the 'Admin' tab selected. The main heading is 'Add Unix Connector'. A yellow warning box states: 'The server that is being designated as a unix connector, should have been already discovered/added to Securden. You can only choose from the already available accounts. If the server has not yet been added to Securden, add/discover and then follow the steps below.' The form contains the following fields:

- Unix Connector Name ***: A text input field with the value 'Lin32'.
- Description**: A text input field.
- IP Address**: A dropdown menu showing '54.174.146.104'.
- Remote Login Credentials**: A dropdown menu with the option 'Select account from device' and the selected value 'Linux Demo'.

At the bottom of the form are two buttons: 'Save' (in green) and 'Cancel'.

Unix Connector Name: This name is used to uniquely identify the connector added in Securden.

Description: (Optional) You can choose to add a brief description of the connector.

IP Address: Specify the IP address of the server/machine that will act as the Unix Connector.

Remote Login Credentials: Supply the remote login credentials to authenticate into the server/machine that acts as the Unix Connector.

Once added, click **Save** and the connector will be added to the list.

Section 18: Reports

Securden Unified PAM provides comprehensive reports for detailed insights on password management and user activities. The easy-to-understand graphs and tables display activity status and summaries related to password management.

Click the **Reports** tab and select your preferred report to proceed. The reports are broadly classified into four categories namely:

1. Standard Reports
2. Concise Reports
3. Password Security Analysis
4. Exported Reports

Standard Reports

Insights related to accounts stored

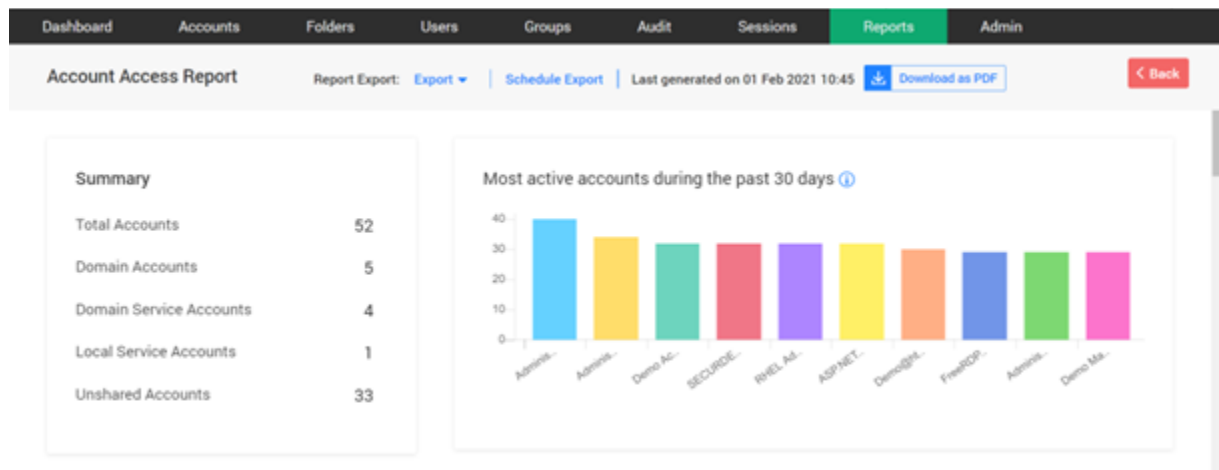
Account Access Report

To access this report, navigate to **Reports >> Standard Reports >> Account Access**. The account access report shows '**who**' are all linked to a

particular account along with '**how**' many of them share that account. The various access entitlements given to the shared users are also displayed.

In the Summary, the number of accounts are displayed categorically and on the other side the bar-graph further highlights the most active accounts during a month. The data shown in the graph includes password retrievals, remote connections launched and password auto-fills on websites.

When you click on any bar on the graph, it specifies the account address, account title and their level of usage.



Trace accounts/folders shared with users or groups

From the Access Snapshot, you get the list of accounts present in the product. Once you click on a particular account, you get the details of users who have access for that account. When an account is shared at multiple levels (such as

account/folder with user or group), Securden follows the least privilege principle in showing the account.

When sharing occurs at multiple levels, at times, you might want to check how the sharing has actually taken effect - how a user is getting access to an account. Account Access Report helps you trace all the levels in which the account has been shared. It tells you the share permission that is effective at present and shows all the other share permissions disregarded as per the least privilege principle.

You may use **Reports >> Account Access Report** for this purpose. Based on this finding, you would be able to take corrective action in case of any deviations.

The screenshot displays the Securden Privileged Account Manager interface. A modal window titled "Trace the sharing mechanism" is open, showing an "Account Access Report" for the "RHEL Admin Account". The report explains the least privilege principle and lists the specific sharing level that has taken effect.

Trace the sharing mechanism

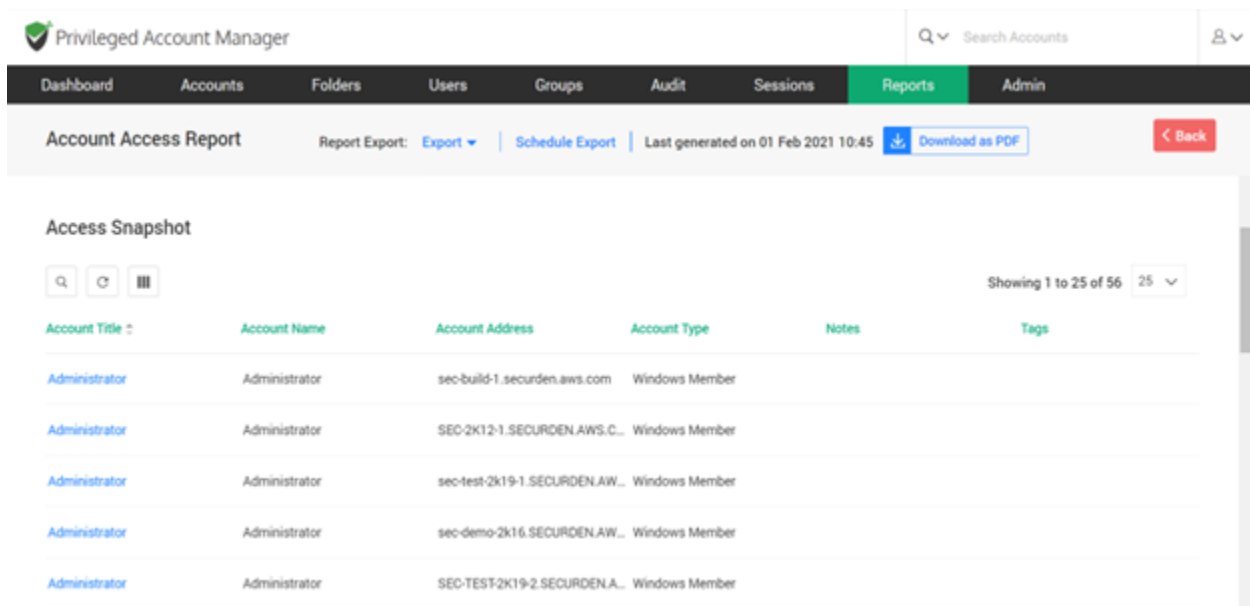
When an account is shared at multiple levels (such as account/folder with user or group), Securden follows the least privilege principle in showing the account. When sharing occurs at multiple levels, at times, you might want to check how the sharing has actually taken effect. This report helps you trace all the levels in which the account has been shared. It tells you the share permission that is effective at present and shows all the other share permissions disregarded as per the least privilege principle.

The specific sharing level that has taken effect:

Account Title	Username	Share Type
RHEL Admin Account	Josh Fraser	Manage

Access Snapshot

When you click on the **Account title**, the page navigates to the **Access details** screen. The access details screen shows the modes of privileges assigned to the user; **Manage, Modify, View and Open Connection**.



The screenshot displays the Privileged Account Manager interface. At the top, there is a navigation bar with tabs: Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports (highlighted in green), and Admin. Below the navigation bar, the 'Account Access Report' section is visible, showing options for 'Report Export: Export' and 'Schedule Export', along with a 'Download as PDF' button and a '< Back' button. The main content area is titled 'Access Snapshot' and contains a table with the following columns: Account Title, Account Name, Account Address, Account Type, Notes, and Tags. The table lists five entries, all with 'Administrator' as the Account Name and 'Windows Member' as the Account Type. The Account Address for each entry is unique, starting with 'sec-build-1.securden.aws.com' and ending with 'SEC-TEST2K19-2.SECURDEN.AW...'. The table also includes a search bar, a refresh icon, and a pagination control showing 'Showing 1 to 25 of 56' with a dropdown menu set to '25'.

Account Title	Account Name	Account Address	Account Type	Notes	Tags
Administrator	Administrator	sec-build-1.securden.aws.com	Windows Member		
Administrator	Administrator	SEC-2K12-1.SECURDEN.AWS.C...	Windows Member		
Administrator	Administrator	sec-test-2k19-1.SECURDEN.AW...	Windows Member		
Administrator	Administrator	sec-demo-2k16.SECURDEN.AW...	Windows Member		
Administrator	Administrator	SEC-TEST2K19-2.SECURDEN.A...	Windows Member		

Account Activity Report

To access this report, navigate to **Reports >> Standard Reports >> Account Activity**. The report indicates about the activities performed on any particular account. The screen displays a graph that shows account access during the past week and a piechart that specifies the type distribution. The type distribution throws light upon the number of activities performed on the account.

The Activity Snapshot, through the search filter, enables you to view the string of activities performed on the accounts in a brief manner.



Once you click on an account, you will get a detailed report on the usage, access, and activities related to that account. The screen shows Password usage statistics and Account usage statistics from which you can see details about password retrievals, remote connections launched, and password auto-fills on websites. Account Activity displays the details of users who have carried out activities on the account, along with the reasons involved.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions **Reports** Admin

Account Activity Report Report Export: [Export](#) | [Schedule Export](#) | Last generated on 08 Sep 2022 08:54 [Download as PDF](#) [Preview PDF](#) [Back](#)

Activity Snapshot

Showing 1 to 25 of 136 25

Account Title	Account Name	Account Address	Account Type	Notes	Tags
SECURDEN-AWS\vm_test_no_pass	vm_test_no_pass	172.31.1.11	Windows Domain		
vm_test_group_user	vm_test_group_user	ip-172-31-94-234.ec2.internal	Linux		
SECURDEN-AWS\vm_test_account	vm_test_account	172.31.1.11	Windows Domain		
SECURDEN-AWS\VMS_Disabled_User	VMS_Disabled_User	172.31.1.11	Windows Domain		
SECURDEN-AWS\user3	user3	172.31.1.11	Windows Domain		
SECURDEN-AWS\user2	user2	172.31.1.11	Windows Domain		
SECURDEN-AWS\user1	user1	172.31.1.11	Windows Domain		
Ubuntu	ubuntu	54.152.7.121	Linux		
Linux Demo	ubuntu	54.174.146.104	Linux		

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions **Reports** Admin

SECURDEN-AWS\vm_test_no_pass [Back](#)

[Report](#) > [Account Activity Report](#) > SECURDEN-AWS\vm_test_no_pass

Details on the usage, access and activities related to this account are depicted in the form of reports here.

Password usage statistics

Account usage statistics

Account Activity

Showing 1 to 8 of 8 50

Performed By	Performed From	Activity Type	Performed At	Reason
--------------	----------------	---------------	--------------	--------

Password Compliance Report

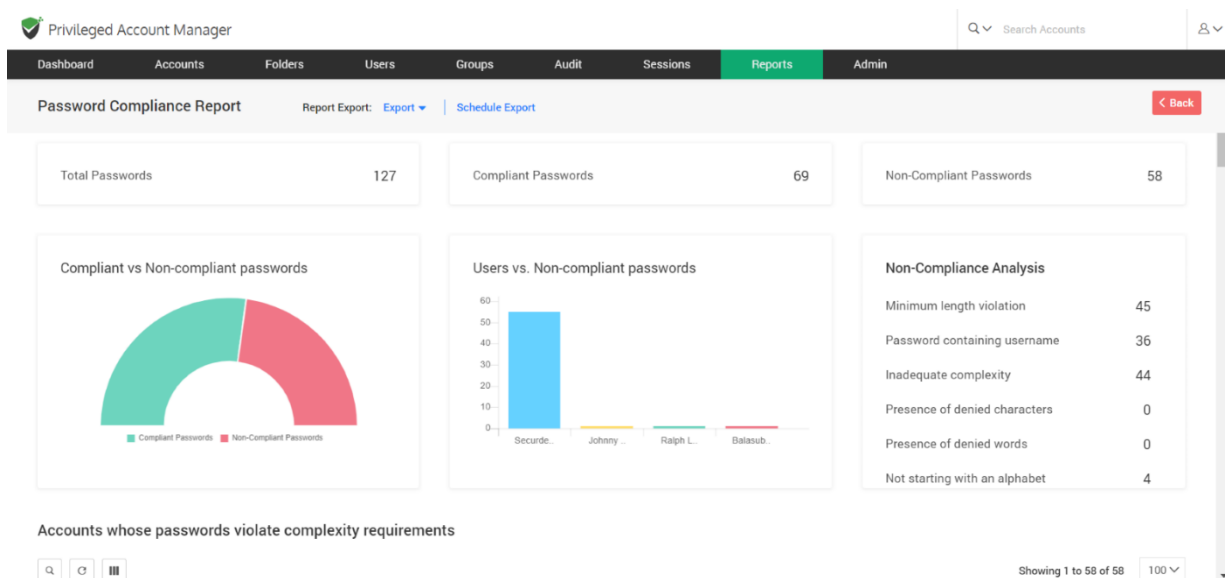
To access this report, navigate to **Reports >> Standard Reports >> Password Compliance**.

The passwords that do not comply with the IT policy of the organization are reported. Securden aids in checking the passwords of the account with the

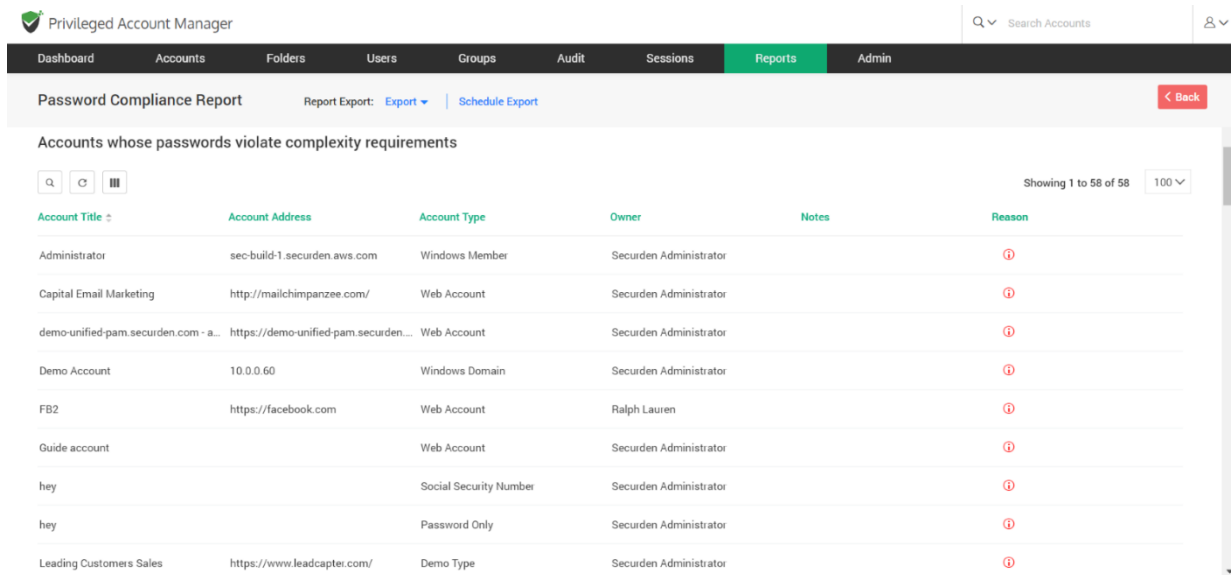
respective password policies and represents the compliance status in the report. Accounts which are excluded from any policy are not included in the report.

The report showcases the summary which includes the number of passwords in the three categories namely, **Total Passwords**, **Compliant Passwords**, and **Non-Compliant Passwords**.

The bar graphs and pie charts show us the comparison between Compliant and Non-compliant passwords, Users and Non-compliant passwords respectively. The Non-compliance analysis further lists the policies which are deviated in the password generated. The search filter enables users to locate the accounts whose passwords violated the complexity requirements. The complexity requirements that were not satisfied by the account are displayed in the reason column.



The expiration dates can be noted for the accounts from the Compliant passwords table.



Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions **Reports** Admin

Password Compliance Report Report Export: [Export](#) | [Schedule Export](#) [Back](#)

Accounts whose passwords violate complexity requirements

Showing 1 to 58 of 58 100

Account Title	Account Address	Account Type	Owner	Notes	Reason
Administrator	sec-build-1.securden.aws.com	Windows Member	Securden Administrator		
Capital Email Marketing	http://mailchimpzanee.com/	Web Account	Securden Administrator		
demo-unified-pam.securden.com - a...	https://demo-unified-pam.securden...	Web Account	Securden Administrator		
Demo Account	10.0.0.60	Windows Domain	Securden Administrator		
FB2	https://facebook.com	Web Account	Ralph Lauren		
Guide account		Web Account	Securden Administrator		
hey		Social Security Number	Securden Administrator		
hey		Password Only	Securden Administrator		
Leading Customers Sales	https://www.leadcaptes.com/	Demo Type	Securden Administrator		

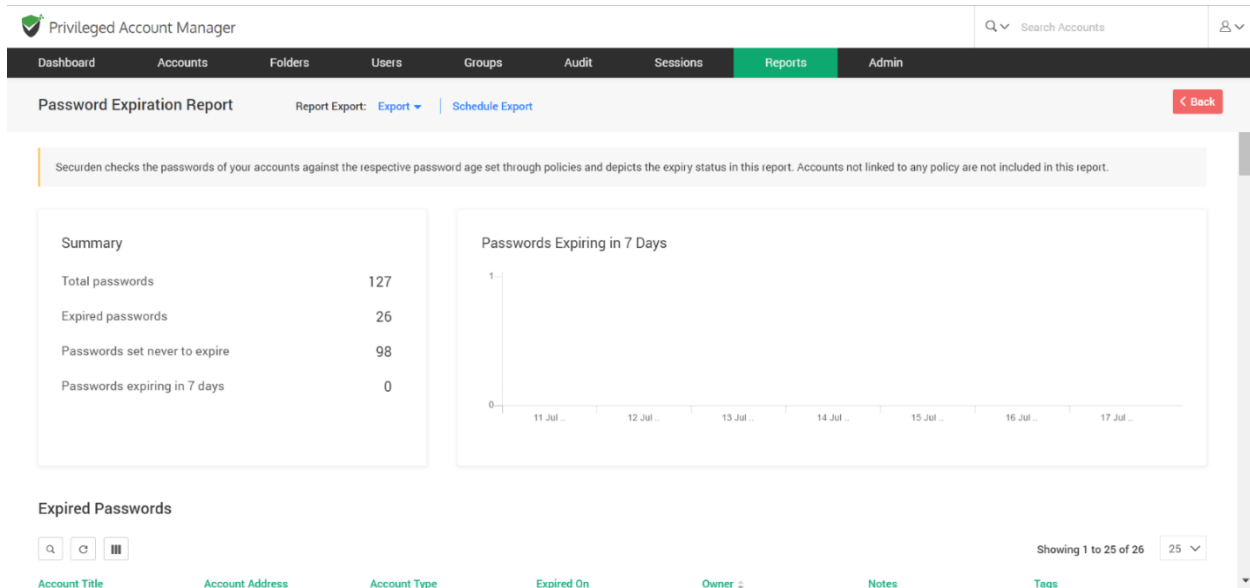
Password Expiry Report

To access this report, navigate to **Reports >> Standard Reports >> Password Expiry**.

Securden checks the passwords of your accounts against the respective password age set through policies and depicts the expiry status in this report. Accounts not linked to any policy are not included in this report.

The graph in the GUI gives the update on passwords expiring in seven days. The three sets of tables, **Expired Passwords**, **Passwords that will expire**

in seven days, Passwords set never to expire give information about account details along with expiration dates and notes if any.



Analysis of user access and activities in Securden

User Access Report

To access this report, navigate to **Reports >> Standard Reports >> User Access**. The **User Access Report** provides you organization-wide information on the list of access entitlements for a specific user. You can select any user and view the information. The user access report is the inverse version of Account Access reports.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions **Reports** Admin

User Access Report Report Export: [Export](#) | [Schedule Export](#) | Last generated on 08 Mar 2021 07:25 [Download as PDF](#) [Preview PDF](#) [Back](#)

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	62
Local Users	23
Active Directory Users	34
Disabled Users	2

Role distribution

Users vs. Account Ownership

Access Snapshot

Showing 1 to 50 of 64

Username	Role	Email
Duncan Hume	Account Manager	duncan@securden.com
Timothy	Account Manager	shyamsenthil9925@gmail.com
Securden Administrator	Administrator	localadmin@securden.com
Vito Canale	Administrator	vito.canale@ofgem.gov.uk
Michele Tammaro	Administrator	michele.tammaro@ofgem.gov.uk
Bala Govind	Administrator	sakthi@securden.com
sanjay	Auditor	sanjay@securden.com
Demo User	Demo Role	demouser@securden.com
Perry The Platypus	Special Agent	shyamsenthil9925@gmail.com

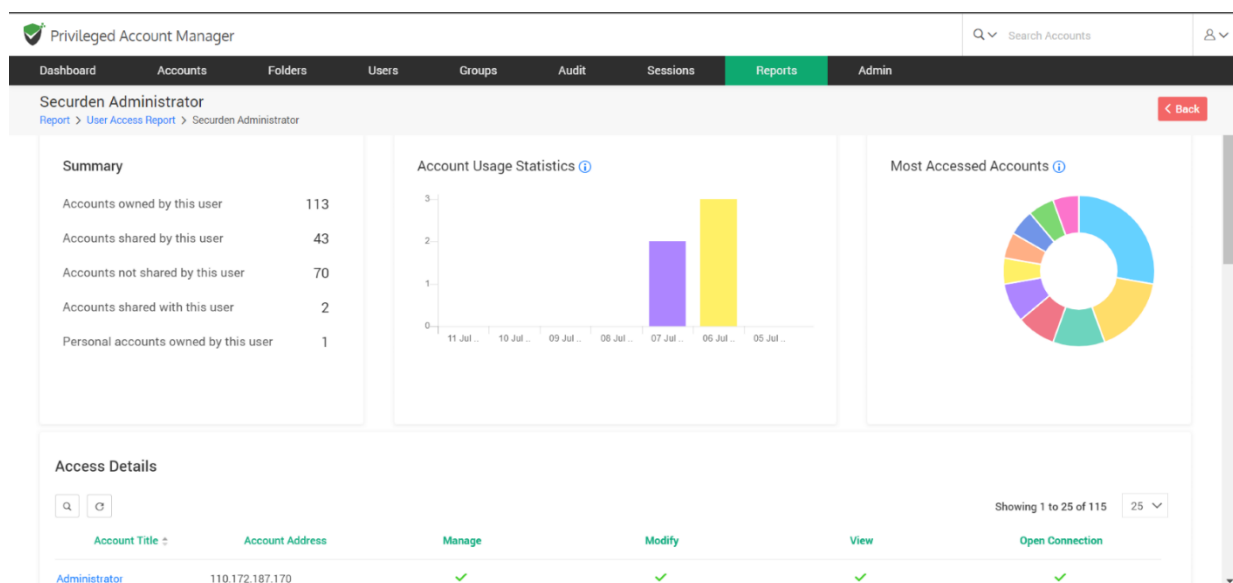
How is the user getting access to an account?

When an account is shared at multiple levels (such as account/folder with user or group), Securden follows the least privilege principle in showing the account. When sharing occurs at multiple levels, at times, you might want to

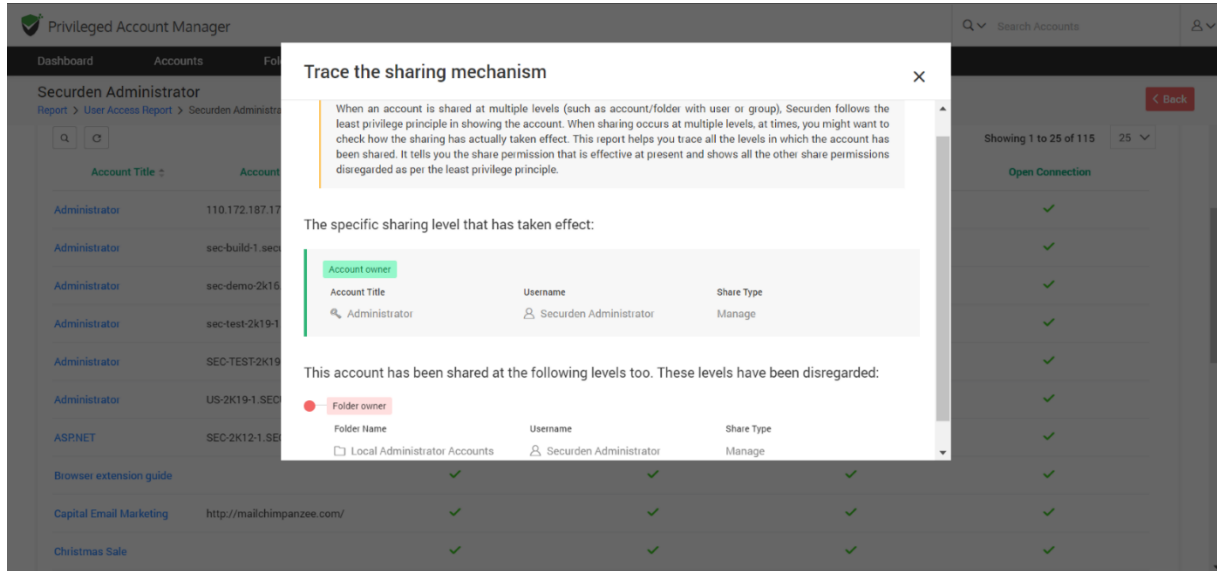
check how the sharing has actually taken effect - how a user is getting access to an account.

You may use **Reports >> User Access Report** for this purpose. Under the **Access Snapshot**, you get the details of users along with the accounts they have access to. Once you click on a username, you will be directed to a page that shows account usage statistics, and access details of that user.

If you are taking a User Access Report, click the name of the user (listed under Access Snapshot) who has access to an account you want to verify. Then click the required account name under Access Details



You will see a pop-up that shows **Trace the sharing mechanism**. It shows details regarding the account's access. Based on this finding, you would be able to take corrective action in case of any discrepancy.



User Activities Report

To access this report, navigate to **Reports >> Standard Reports >> User Activity**. The User Activity Report depicts the activities performed by users in Securden. Click the respective username in the activity snapshot table to view the access details. The two bar graphs in the GUI display the frequent logins and usage of accounts during a 30-day time period. The **Activity Snapshot** further gives us more details about the user, their role along with their email id.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions **Reports** Admin

User Activity Report Report Export: [Export](#) | [Schedule Export](#) [Back](#)

This report depicts the activities performed by users in Securden. Click the respective username in the table below to view the access details.

Frequent logins to Securden during the past 30 days

User	Frequency
Securden	10
Test Ab.	3

Users vs. Most accounts access during the past 30 days

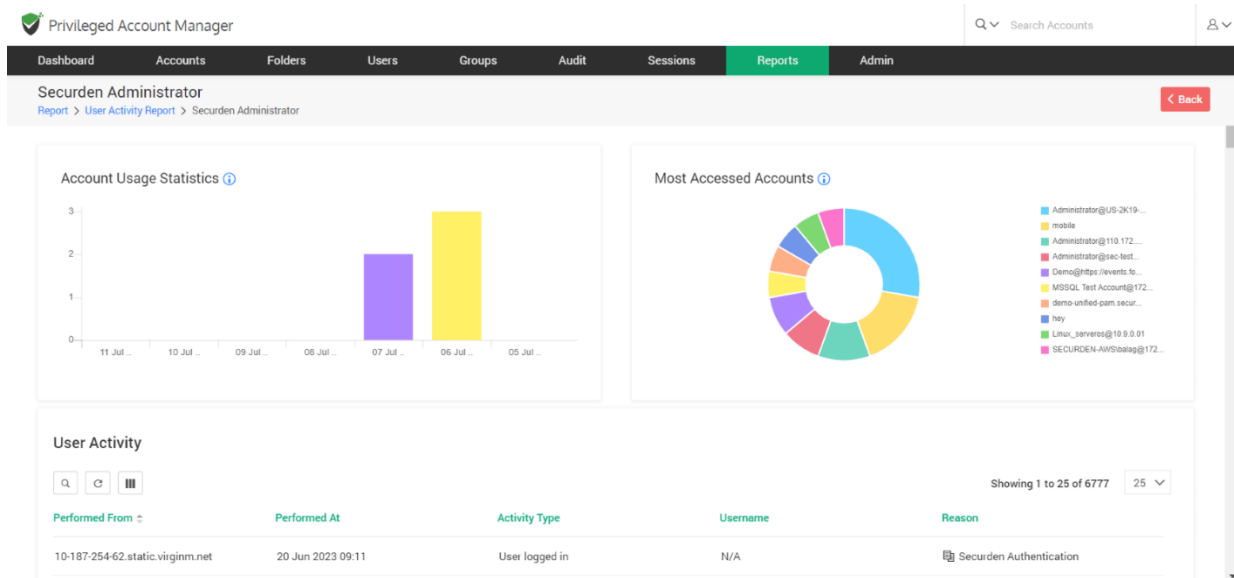
User	Access Count
Securden	130
Test Ab.	10

Activity Snapshot

Showing 1 to 50 of 64

Username	Role	Email
Duncan Hume	Account Manager	duncan@securden.com
Timothy	Account Manager	shyamsenthil9925@gmail.com
Securden Administrator	Administrator	localadmin@securden.com
Vito Canale	Administrator	vito.canale@ofgem.gov.uk
Michele Tammaro	Administrator	michele.tammaro@ofgem.gov.uk
Bala Govind	Administrator	sakthi@securden.com
sanjay	Auditor	sanjay@securden.com
Demo User	Demo Role	demouser@securden.com
Perry The Platypus	Special Agent	shyamsenthil9925@gmail.com

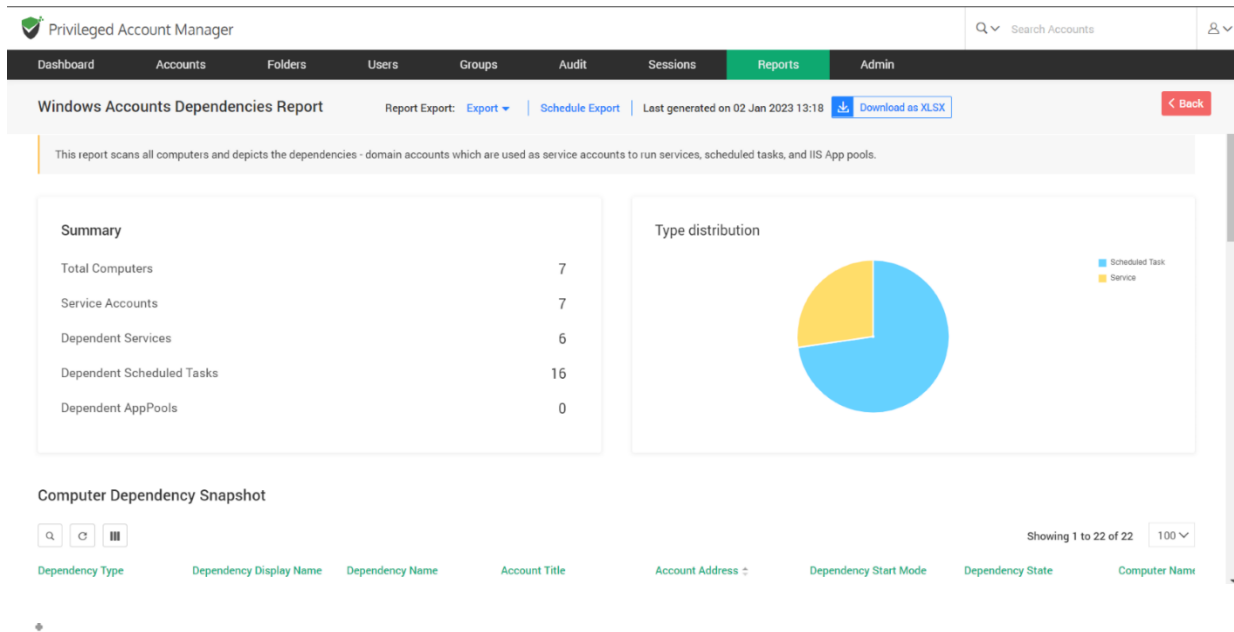
To get a user activity report, click on a username present under Activity Snapshot, and then you will be directed to a page that displays account usage statistics, user activity, account activity, groups that the user belongs to, directly shared folders, and group shared folders to that particular user.



Complete Visibilities on Windows Dependencies

Windows Accounts Dependencies Report

To access this report, navigate to **Reports >> Standard Reports >> Dependencies**. This report scans all computers and depicts the dependencies - domain accounts which are used as service accounts to run services, scheduled tasks, and IIS App pools. The pie chart shows the type distribution of scheduled tasks and services. The computer dependency snapshot table lists out the details about the dependency type and other details including the name of the computer.



Processes and Software

Processes and Software Inventory

To access this report, navigate to **Reports >> Standard Reports >> Processes and Software >> Processes and Software Inventory**. This report presents an inventory of all processes and software installed on each computer. Securden discovers the processes and the software installed on endpoints and servers on which the Securden agent is installed. The list of computers is displayed along with the processes that had run until the time of discovery in the 'Processes' table. The list of computers along with the software installed on each of them is displayed in the 'Software' table.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions **Reports** Admin

Processes and Software Inventory Report Export: [Export](#) | [Schedule Export](#) Last generated on 29 Sep 2021 06:59 [Download as PDF](#) [Preview PDF](#) [Back](#)

This report presents an inventory of all processes and software installed on each computer. Securden discovers the processes and the software installed on endpoints and servers on which the Securden agent is installed. The list of computers is displayed along with the processes that had run until the time of discovery in the 'Processes' table. The list of computers along with the software installed on each of them is displayed in the 'Software' table.

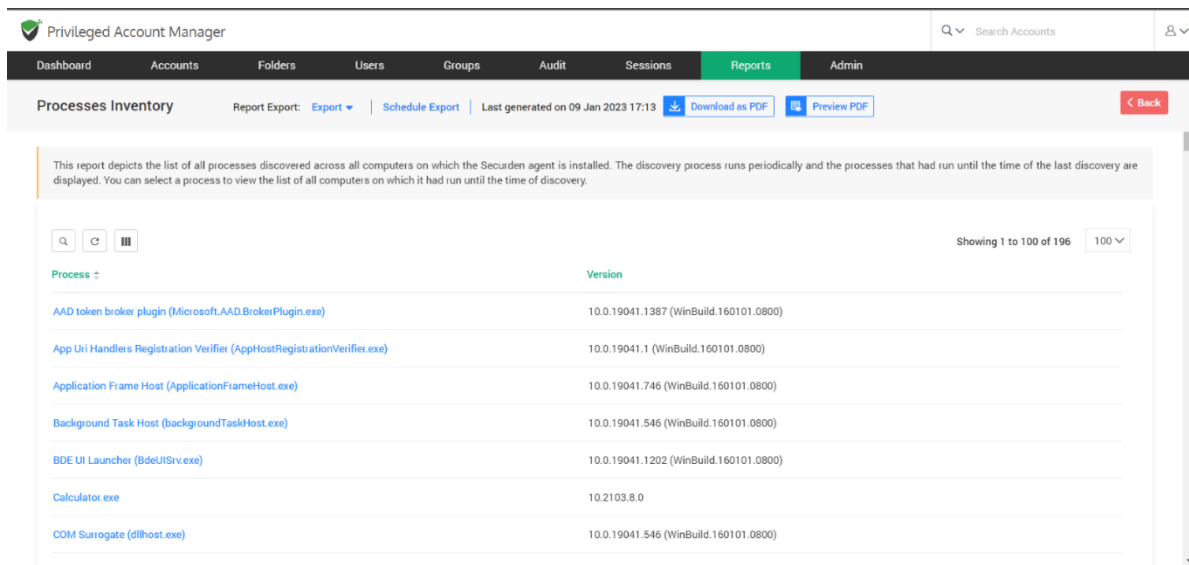
System Processes run on this Computer

Showing 1 to 25 of 199 25

Process	Version	Publisher	Last Run	Computer
SEC-SUPPORT-2 (25 Processes)				
Microsoft Edge (msedge.exe)	97.0.1072.62	Microsoft Corporation	18 Jan 2022 14:54	SEC-SUPPORT-2
Google Chrome (chrome.exe)	97.0.4692.71	Google LLC	18 Jan 2022 14:52	SEC-SUPPORT-2
Runtime Broker (RuntimeBroker.exe)	10.0.19041.746 (WinBuild.160101.0800)	Microsoft Windows	18 Jan 2022 14:51	SEC-SUPPORT-2
Microsoft Outlook Communications (HxTsr...	16.0.14326.20544		18 Jan 2022 14:51	SEC-SUPPORT-2
PWA Identity Proxy Host (identity_helper.ex...	97.0.1072.62	Microsoft Corporation	18 Jan 2022 14:51	SEC-SUPPORT-2

Processes Inventory

To access this report, navigate to **Reports >> Standard Reports >> Processes and Software >> Processes Inventory**. This report depicts the list of all processes discovered across all computers on which the Securden agent is installed. The discovery process runs periodically and the processes that had run until the time of the last discovery are displayed. You can select a process to view the list of all computers on which it had run until the time of discovery.



Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions **Reports** Admin

Processes Inventory Report Export: [Export](#) | [Schedule Export](#) Last generated on 09 Jan 2023 17:13 [Download as PDF](#) [Preview PDF](#) [Back](#)

This report depicts the list of all processes discovered across all computers on which the Securden agent is installed. The discovery process runs periodically and the processes that had run until the time of the last discovery are displayed. You can select a process to view the list of all computers on which it had run until the time of discovery.

Showing 1 to 100 of 196

Process	Version
AAD token broker plugin (Microsoft.AAD.BrokerPlugin.exe)	10.0.19041.1387 (WinBuild.160101.0800)
App UI Handlers Registration Verifier (AppHostRegistrationVerifier.exe)	10.0.19041.1 (WinBuild.160101.0800)
Application Frame Host (ApplicationFrameHost.exe)	10.0.19041.746 (WinBuild.160101.0800)
Background Task Host (backgroundTaskHost.exe)	10.0.19041.546 (WinBuild.160101.0800)
BDE UI Launcher (BdeUISrv.exe)	10.0.19041.1202 (WinBuild.160101.0800)
Calculator.exe	10.2103.8.0
COM Surrogate (dllhost.exe)	10.0.19041.546 (WinBuild.160101.0800)

Software Inventory

To access this report, navigate to **Reports >> Standard Reports >> Processes and Software >> Software Inventory**. This report depicts the list of all software installed across all computers on which the Securden agent is installed. The discovery process runs periodically and the software that was found installed until the time of the last discovery is displayed. You can select a software to view the list of all computers on which it was installed until the time of discovery.

Privileged Account Manager | Search Accounts | Admin

Dashboard | Accounts | Folders | Users | Groups | Audit | Sessions | **Reports** | Admin

Software Inventory | Report Export: [Export](#) | [Schedule Export](#) | [Back](#)

This report depicts the list of all software installed across all computers on which the Securden agent is installed. The discovery process runs periodically and the software that were found installed until the time of the last discovery are displayed. You can select a software to view the list of all computers on which it was installed until the time of discovery.

Showing 1 to 25 of 38 | 25

Software	Version	Publisher
Google Chrome	97.0.4692.71	Google LLC
Greenshot 1.2.10.6	1.2.10.6	Greenshot
Intel(R) Chipset Device Software	10.1.18460.8229	Intel Corporation
Intel(R) Chipset Device Software	10.1.18460.8229	Intel(R) Corporation
KeePass Password Safe 2.49	2.49	Dominik Reichl
Lenovo Vantage Service	3.10.26.0	Lenovo Group Ltd.
McAfee LiveSafe	16.0 R41	McAfee, LLC

Securden Agents on Computer

To access this report, navigate to **Reports >> Standard Reports >> Processes and Software >> Securden Agents on Computers**. This report shows the list of computer names and agent versions installed on each computer.

Privileged Account Manager | Search Accounts | Admin

Dashboard | Accounts | Folders | Users | Groups | Audit | Sessions | **Reports** | Admin

Computer Agent versions | Report Export: [Export](#) | [Schedule Export](#) | [Back](#)

This report shows the list of computer names and agent versions installed on each computer.

Computer agent version snapshot

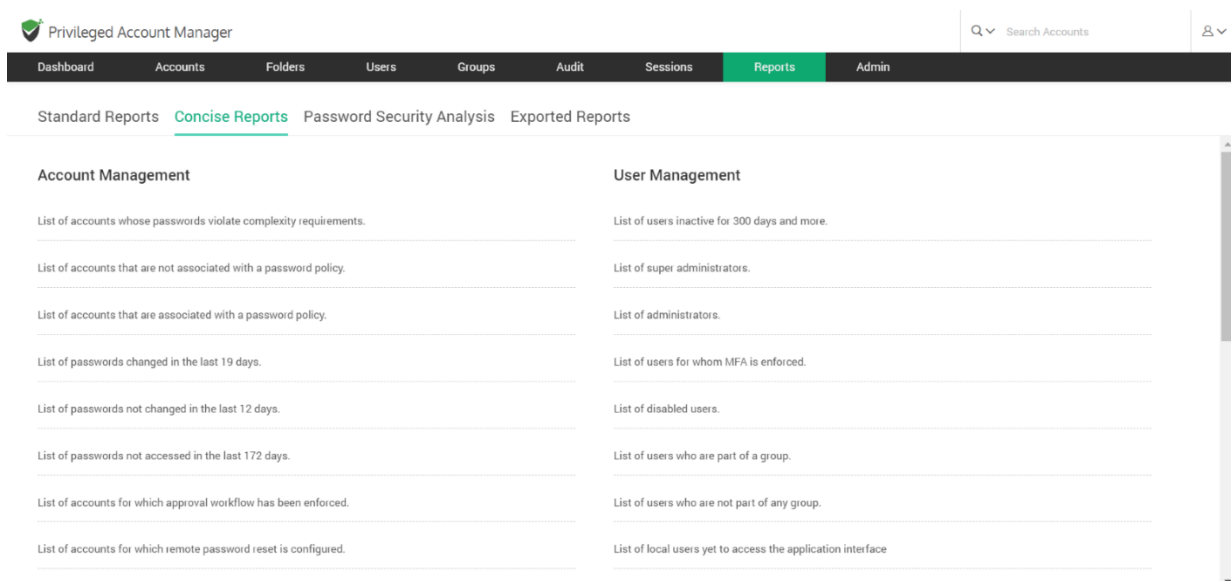
Showing 1 to 3 of 3 | 25

Agent Version	Last Connected Time	Operating System
5.7.9	18 Jan 2022 14:53	Windows 10 Pro
5.5.8	09 Sep 2020 04:01	Windows Server 2016 Datacenter
5.0.3	11 Jul 2020 15:45	Windows Server 2019 Datacenter

Showing 1 to 3 of 3 | 25

Concise Reports

Concise Reports provide you 'to the point' information on specific topics. For example, if you want to know the list of passwords that were changed during the past X number of days, the concise reports will get you the details quickly.



Concise reports consists of different categories:

Account Management

The account management section deals with the list of accounts and password related matters. This includes violation of password complexity requirements, password policies and expiry duration etc.,

User Management

The user management section deals with the list of many user activities. This includes inactive users, super admins, disabled users, users part of group and those who are not part of any groups.

My Accounts

This section deals with the list of accounts:

1. Owned by you
2. Shared by you
3. Shared with you

Folder Management

The folder management section deals with a list of folders owned, shared by you, not shared with anyone and also folders for which approval workflow has been enforced.

My Folders

This section deals with a list of folders:

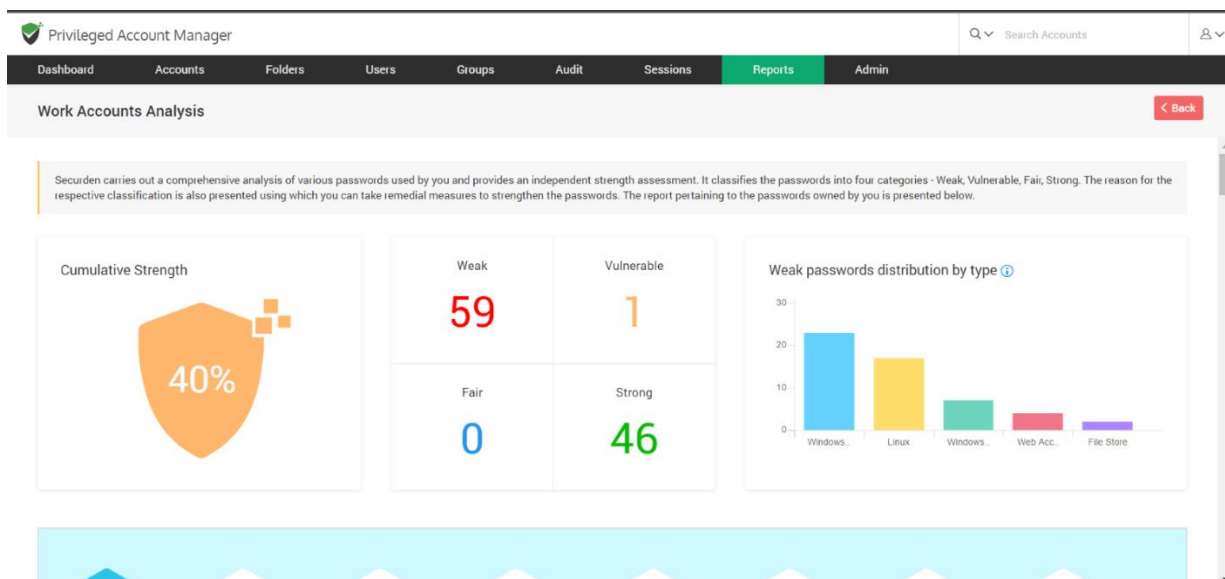
1. Owned by you
2. Shared by you
3. Shared with you

Password Security Analysis

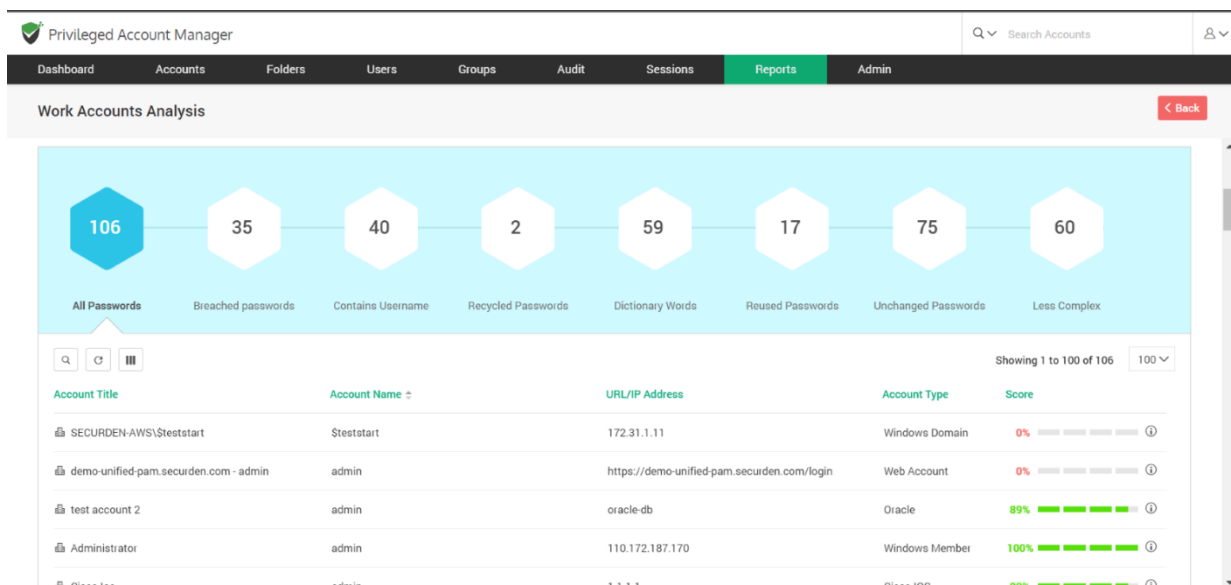
Work Account Analysis

To access this report, navigate to **Reports >> Password Security Analysis >> Work Accounts Analysis**.

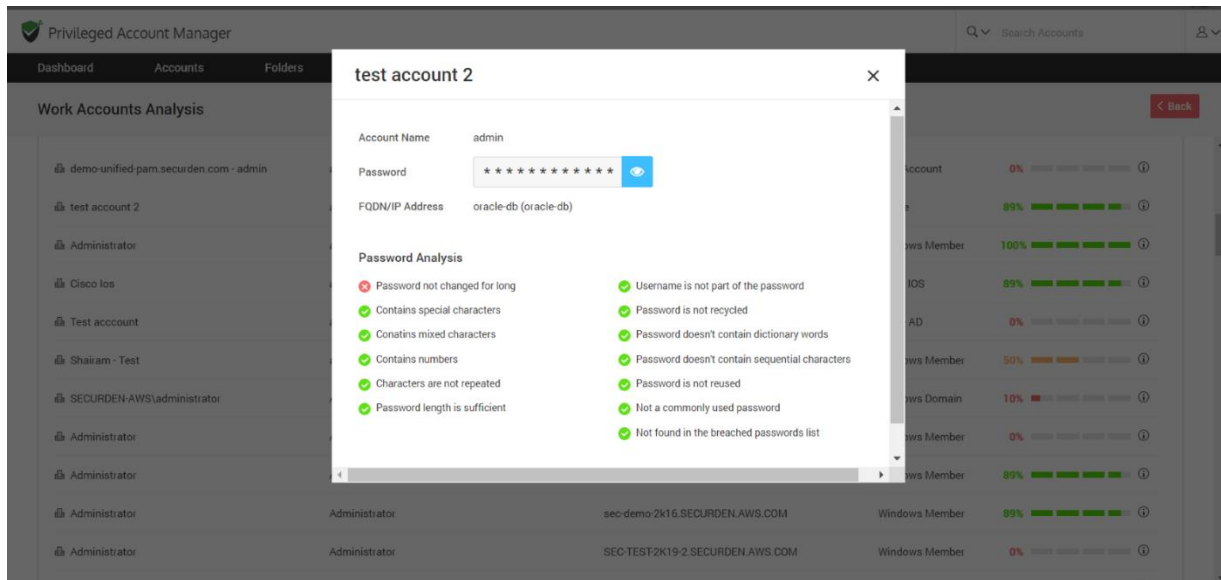
Securden carries out a comprehensive analysis of various passwords used by you and provides an independent strength assessment. It classifies the passwords into four categories - Weak, Vulnerable, Fair, Strong. The reason for the respective classification is also presented, using which you can take remedial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



The cumulative strength password indicates the overall strength of the various passwords in terms of the percentage. The bar graph of weak passwords distribution by type depicts a quick summary of the weak passwords belonging to different account types. The types that have the most number of weak passwords are also displayed on the screen.



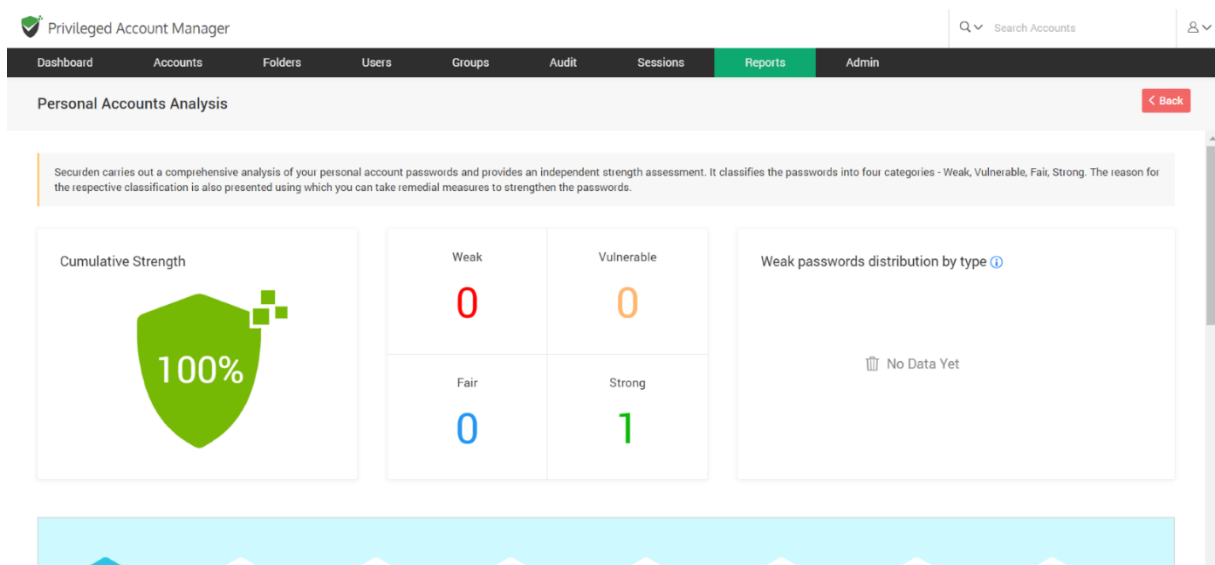
The hexagons display the category of password (such as breached passwords, less complex passwords, reused passwords, etc.,) and show the table with account details and strength score of the password (in percentage). The score column further tells us which criterias have been satisfied by that password and gives a detailed password analysis for each account.



Personal Account Analysis

To access this report, navigate to **Reports >> Password Security Analysis >> Personal Accounts Analysis**.

This report keeps track of the personal account passwords and provides an analysis about the activities performed with those accounts.



Exported Reports

To access these reports, navigate to **Reports >> Exported Reports**. You can view the reports already exported in various formats and download them. The different types of reports which were already exported are displayed here along with the date of download and the user who generated it. Click on **Configure Export Location** to change the location for the exported reports.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions **Reports** Admin

Standard Reports Concise Reports Password Security Analysis Exported Reports

You can view the reports already exported in various formats and download them.

Showing 1 to 25 of 27
25

Report Name	Generated By	Date	Download / Preview
Activities on Accounts Report (PDF)	Securden Administrator	10 Apr 2023 06:08	Download Preview
Account Access Report (PDF)	Securden Administrator	23 Mar 2023 15:52	Download Preview
Processes Inventory (PDF)	Securden Administrator	09 Jan 2023 17:13	Download Preview
Windows Accounts Dependencies Report (XLSX)	Securden Administrator	02 Jan 2023 13:18	Download
Windows Accounts Dependencies Report (XLSX)	Securden Administrator	02 Jan 2023 13:17	Download
Windows Accounts Dependencies Report (CSV)	Securden Administrator	02 Jan 2023 13:13	Download
Activities on Accounts Report (PDF)	Securden Administrator	04 Nov 2022 09:30	Download Preview
Windows Accounts Dependencies Report (PDF)	Securden Administrator	07 Oct 2022 10:25	Download Preview

Section 19: Miscellaneous

Change Database

If you want to change the backend database to MS SQL Server, you can change your backend database from the default PostgreSQL to MS SQL server. When you change the backend, you will be starting afresh - that means, your existing data in PostgreSQL will not be migrated. To change the backend database from the default PostgreSQL to MS SQL Server, follow the steps below:

- Stop **Securden 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

Store Encryption Keys on Securosys HSM

You can configure an HSM device and store the Securden encryption key for additional security. HSM is an encrypted, security-hardened device used for storing, generating, and rotating encryption keys. You need to provide certain details of your HSM device and configure it before storing the Securden encryption key in your HSM device.

Prerequisite: You need to take a backup of your entire database along with the encryption key before starting the HSM configuration process.

Step 1: Stopping the Securden PAM service on Primary and Secondary servers

Navigate to services.msc and **Stop** the **Securden PAM service**. If you have configured secondary application servers in your organization, you need to stop the Securden PAM service on all the secondary servers.

Step 2: Configuring the HSM

Navigate to <Securden installation folder>/bin and locate **ConfigureHSM.exe**.

Open **ConfigureHSM.exe** and provide the following details:

1. **HSM Provider Name:** The name of your HSM provider. You can select Securosys from the drop-down menu.
2. **DLL File Path:** Securden integrates with your HSM provider through their **primus.dll** file. You need to specify the location of this file in this field.
3. **HSM Slot ID:** The partition in which the Securden encryption key should be stored.
4. **HSM Slot Password:** The credential required for accessing the HSM and storing the encryption key in the slot mentioned above.
5. **Encryption Key Label:** The name with which the Securden encryption key should be stored in the HSM.

Once the required details are provided, click **Configure**.

Important:

After configuring the HSM,

1. The entire database will be decrypted using your current key and encrypted using a new key which is stored in your HSM.
2. You need to take a fresh backup of your database since your previous backup copies cannot be restored, since the encryption key is different.
3. If you had configured secondary servers of any type before configuring the HSM, they would not work as intended after the process is completed. This is because of the encryption key mismatch between the primary server and the secondary server. You need to re-configure all

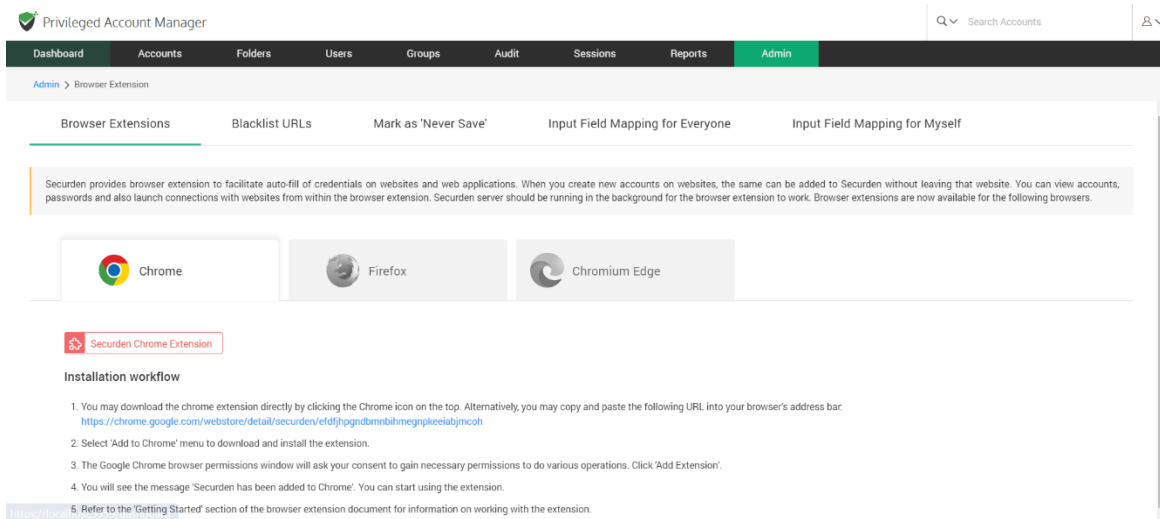
secondary servers (Remote distributors and high availability servers) and deploy the application server package once again.

4. Securden primary and secondary servers share the same HSM keys. You need to ensure that HSM keys (hsm_1.key, hsm__2.key, and hsm_3.key) are located in the default (Securden\conf) folder.

Browser Extensions

Securden provides browser extensions to facilitate auto-fill of credentials on websites and web applications. When you create new accounts on websites, the same can be added to Securden without leaving that website. You can view accounts, passwords and also launch connections with websites from within the browser extension. Securden server should be running in the background for the browser extension to work. Extensions are available for Chrome, Firefox, and Chromium-based Edge browsers.

Navigate to **Admin >> General >> Browser Extensions** to download the extensions.



The steps to install different browser extensions are given below:

Chrome

- You may download the chrome extension directly from the GUI. Alternatively, you may copy and paste the following URL into your browser's address bar:

<https://chrome.google.com/webstore/detail/securden/efdfjhpgnbmnbihtmegnpkeeiabjmcoh>

- Select the 'Add to Chrome' menu to download and install the extension.
- The Google Chrome browser permissions window will ask for your consent to gain the necessary permissions to do various operations. Click Add Extension.
- You will see the message 'Securden has been added to Chrome'. You can start using the extension.

Firefox

- You may download the chrome extension directly from the GUI. Alternatively, you may copy and paste the following URL into your browser's address bar: <https://addons.mozilla.org/enUS/firefox/addon/securden/>
- Click the 'Add to Firefox' menu to download and install the extension.
- The Mozilla Firefox browser permissions window will ask for your consent to gain the necessary permissions to do various operations. Click 'Add'.
- You will see the message 'Securden has been added to Firefox'. You can start using the extension.

Chromium Edge

- You may download the chrome extension directly from the GUI. Alternatively, you may copy and paste the following URL into your browser's address bar: Securden - Chrome Web Store ([google.com](https://chrome.google.com/webstore/detail/securden))
- Select the 'Add to Chrome' menu to download and install the extension.
- The Chromium Edge browser permissions window will ask for your consent to gain the necessary permissions to do various operations. Click 'Add Extension'.
- You will see the message 'Securden has been added'. You can start using the extension.

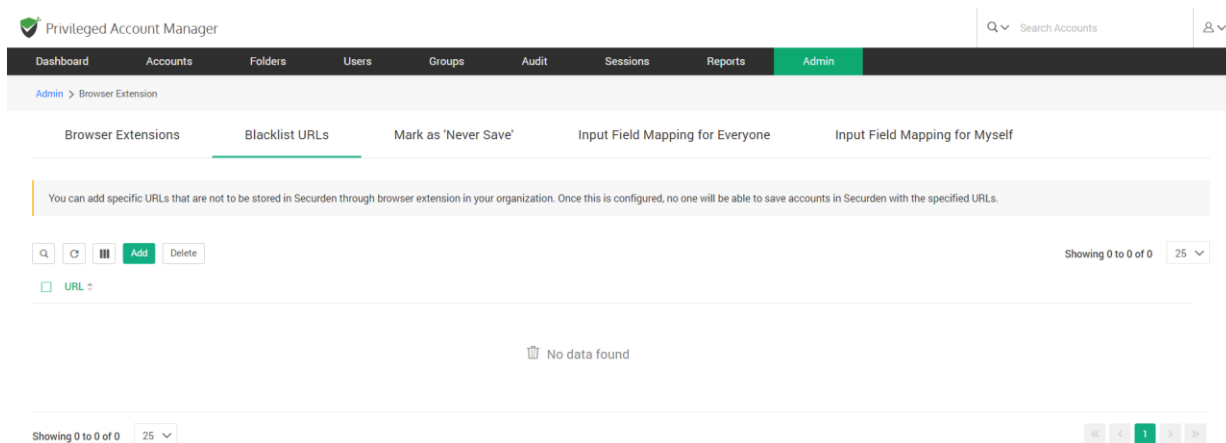
In addition to installing browser extensions, you can do certain configurations related to the usage of the extensions.

Blacklist URLs

Once you install the extension, whenever you create a new account/password on a website, it usually prompts you to add the accounts to Securden inventory. There might be requirements where you wouldn't need certain accounts to be added to Securden. You can handle such scenarios through the blacklist URLs option.

This option Securden allows you to add (and delete) specific URLs that are not to be stored in Securden through the browser extension in your organization.

Navigate to **Admin >> General >> Browser Extension >> Blacklist URLs** page and click the **Add** button.



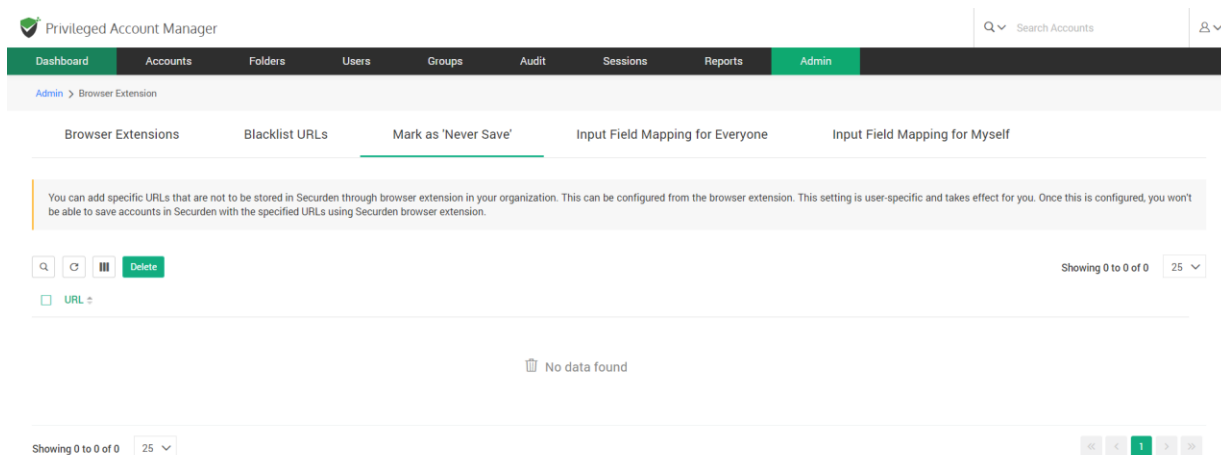
Once this is configured, no one will be able to save accounts in Securden with the specified URLs.

Mark as Never Save

This feature is similar to the Blacklist URL option and allows you to define specific URLs that are not to be stored in Securden through the browser extension. While the Blacklist URLs option takes effect globally across the organization for all users, the 'Never Save' option is user-specific and doesn't affect the entire organization.

Typically, the URLs that are marked not to be saved in Securden (setting you will see in the extension) will be listed on this page.

Navigate to **Admin >> General >> Browser Extension >> Never Save** page to manage such URLs.



You can add specific URLs that are not to be stored in Securden through browser extension in your organization. This can be configured from the

browser extension. This setting is user-specific and takes effect for you. Once this is configured, you won't be able to save accounts in Securden with the specified URLs using Securden browser extension.

Moving Securden Installation from One Machine to Another

If you want to move the Securden installation from one machine to another (for example, moving a test setup to production), you may follow the steps below:

Prerequisite: Securden installation is guarded by a unique encryption key. When you move the installation, you need to take care of the key as well. The new installation would require the key. By default, the encryption key is available as `<Securden-Installation-Folder>\conf\securden.key`. In production instances, we enforce changing the key location. If you have changed it from **Admin >> Security >> Change Encryption Key**

Location, you need to ensure that the key is present in the location specified.

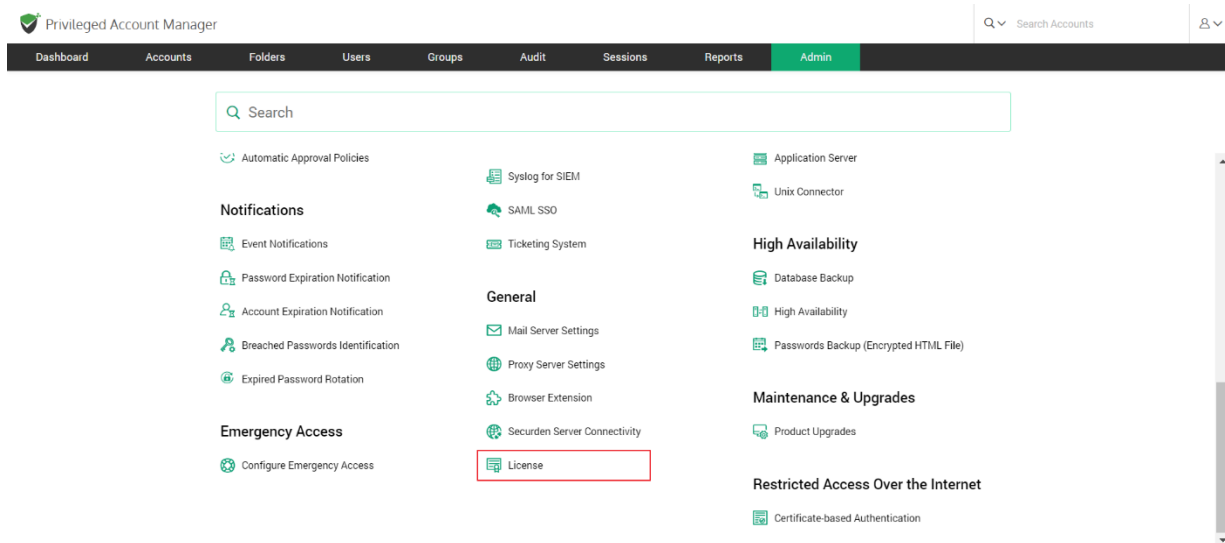
To move Securden from one server to another follow the steps below.

- Stop the "Securden PAM Service" from services.msc
- Copy the entire Securden installation folder
- Paste it on the new server

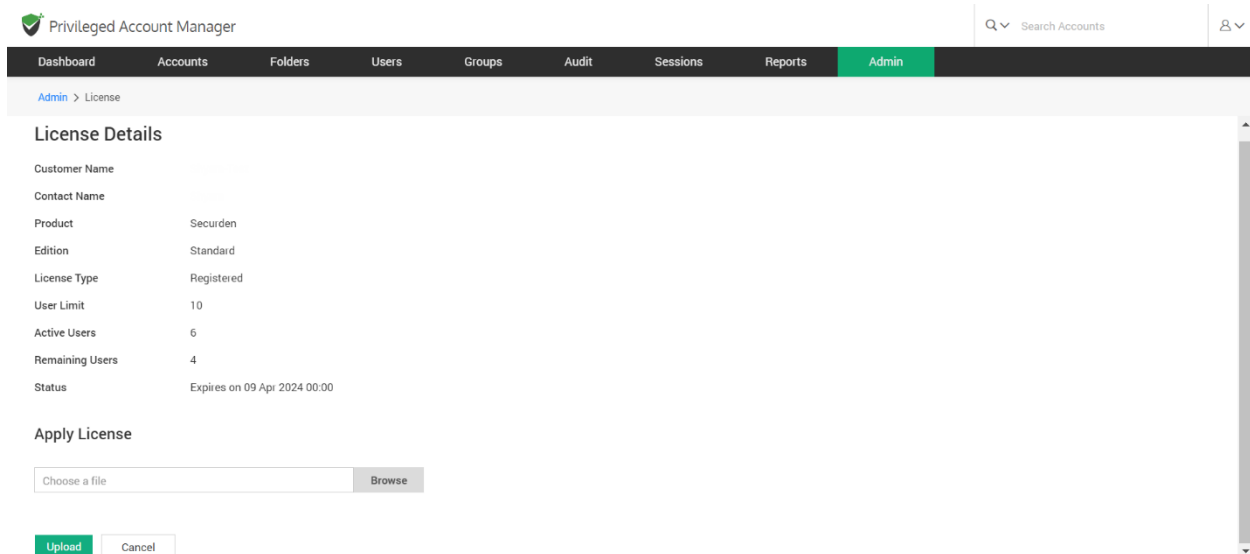
- Open a command prompt, run with admin privileges, and navigate to **<Securden Installation Folder>/Privileged_Access_Manager/bin folder**
- Execute the command `SecurdenServiceInstaller.exe install`
- Start the "Securden PAM Service" from `services.msc`

Section 20: Product License Key

You can apply the Securden license key and get information about the existing license from **Admin >> General >> License** section.



In the License details page, the following details are displayed:



Customer Name: The name of the organization for which the product is licensed

Contact Name: Contact person within the company

Product: The name of the product purchased from Securden.

Edition: Product edition name

License Type: This indicates if you are a registered user or if you are using the trial version.

User Limit: The number of users that can be onboarded into Securden.

Active Users: The number of users that are currently onboarded into the solution.

Remaining Users: The number of users who can be added into Securden.

Addons: Product addons, if any.

Status: The number of days until expiration is displayed here. To add a new license, you can use the browse button to search for that license and upload the same

Renewing the PAM license

To renew the license, you may reach out to support@securden.com. You will receive a license file that you need to unzip (.txt) and upload. You can click **Browse** and select the downloaded file.