Securden

Endpoint Privilege Manager (EPM)

Administrator Guide

Table of Contents

Getting Started 5

Starting the EPM Server 5

Launching Web Interface 5

SECTION 1: General Configuration Settings **6**

Configure Mail Server Settings 6

Proxy Server Settings 8

Securden Server Connectivity 9

Integrating Active Directory Domains 13

Import Domain Controllers Certificate 16

SECTION 2: User Management **17**

Onboarding Users to WPM 17

Import Users from Active Directory 17

Import from Azure AD 25

Import from File 30

Add Users Manually 34

Privilege Elevation Approvers for Users 53

User Report 55

Groups 57

Import User Groups from AD 58

Import User Groups from Azure AD 64

Add User Groups Manually 68

Configure Periodic Synchronization of Groups 70

Configure Multi-Factor Authentication 73

Activate TFA 74

Mail OTP 77

Google Authenticator/ Microsoft Authenticator/ TOTP Authenticator 77
Self-support any TOTP Authenticator 78
RADIUS Authentication 79
Email to SMS Gateway Configuration 81
Yubikey 82
Enforcement Options 85
Selective MFA Enforcement 86
Configure SAML-based SSO 89

SECTION 3: Privilege Management Configurations 97
Step 1: Deploy Securden Agent on Computers 97
Manual Installation 98
Agent Installation Using GPO 98
Discover Workstations (Optional) 100
Computer Groups 103
Importing groups from AD 104
Manually Adding Computer Groups 107
Add Members 108
Synchronizing with AD 108
Step 2: Discover and Add Applications 110
Automatic Discovery of Applications 111
Adding Applications Manually 111
Step 3: Define Application Control Policies 115
Adding a Domain-policy 116
Add a non-domain policy 120
Step 4: Remove Local Admin Rights 120
Move Users from One Group to Another 123
Technician Access Policies 124

SECTION 4: Privilege Elevation 135
Privilege Elevation Scenarios (for Users) 135
Scenario 1: Elevating Privileges for Whitelisted Applications 135
Scenarios 2 & 3 : Requesting Elevated Access 139
Monitor Changes to Domain Admin Group 145
Privilege Elevation Requests 147
Approving requests 149
Automatic Approval Policies.. 150
Adding a domain approval policy 151
Adding a non-domain approval policy 153
Privilege Elevation in Offline Scenarios 156
Management Operations from Computers Tab 169
Monitor the Securden Agent 169
Application Policies for Specific Computers 170
Computer Specific Reports 172

SECTION 5: High Availability 174
Configure High Availability 174
Configuring High Availability with PostgreSQL backend 174
Configuring High availability with MS SQL backend database 182
Database Backup 188
Steps for Data Recovery 192

SECTION 6: Audit, Compliance & Reports 194
Standard Reports.. 195
Exported reports... 223
Event Notifications 224

SECTION 7: Miscellaneous 228

Admin Dashboard 228

Customize Securden WPM 229

Create and Manage Custom User Roles 230

Changing Logo, Theme, and Text 238

Product Language Selection... 242

Security Settings 244

Monitor Changes to Domain Admin Groups.................................... 244

Change the Encryption Key Location 248

Product Upgrade.. 252

Replace Self-signed Certificate 255

Manage Product License Key 256

Getting Started

Starting the EPM Server

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

Launching Web Interface

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

https://<EPM server hostname>:5151

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

Username: admin
Password: admin

Once you configure your setup, use the appropriate credentials to access the interface.

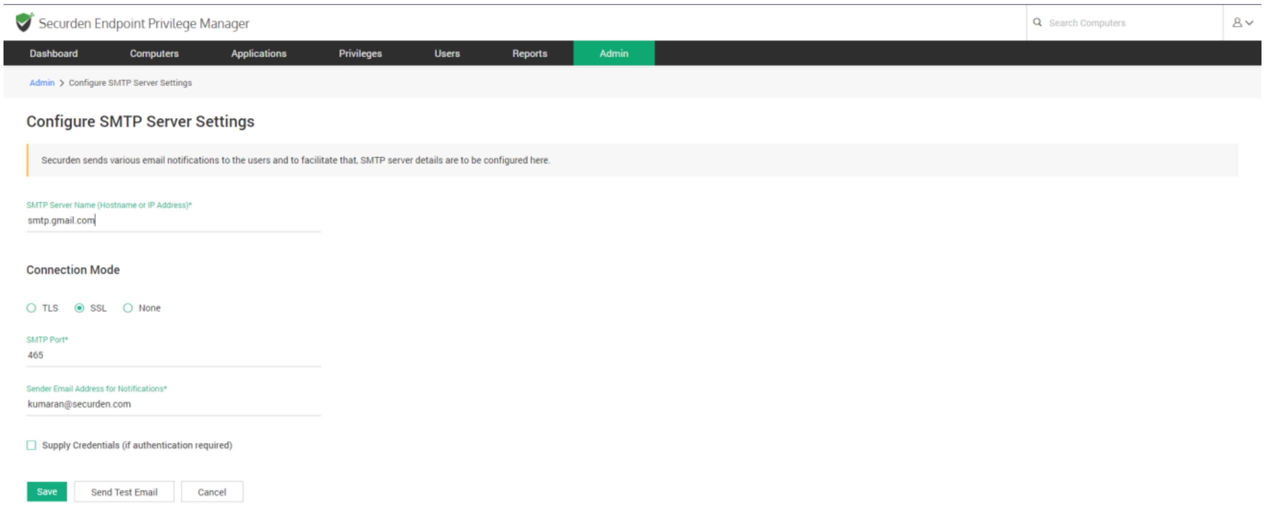
SECTION 1: General Configuration Settings

Upon deploying Securden EPM, you need to configure certain basic settings before proceeding with setting up the features. These settings are listed under the **Admin >> General** section.

The settings include configuring the mail server to enable 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 client machines and the name with which the client machines identify the Securden server host.

Configure Mail Server Settings

Securden sends various email notifications to the users and to facilitate that, SMTP server details are to be configured. To configure the SMTP server settings, navigate to **Admin >> General >> Mail Server Settings**.


Securden Endpoint Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Configure SMTP Server Settings

Configure SMTP Server Settings

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

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

Connection Mode

○ TLS ● SSL ○ None

SMTP Port*: 465

Sender Email Address for Notifications*: kumaran@securden.com

□ Supply Credentials (if authentication required)

In this GUI, enter the following details:

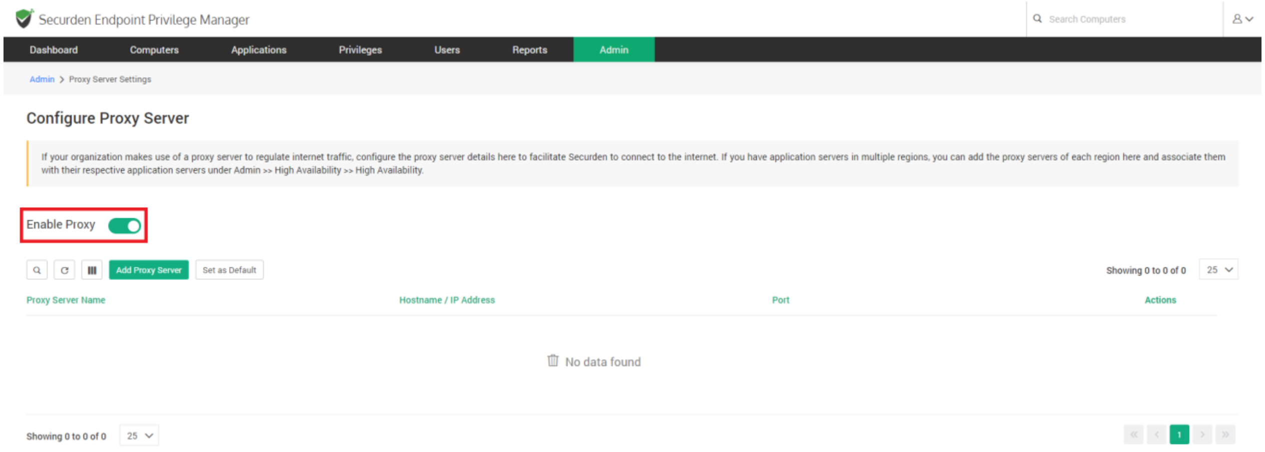
- **SMTP server name**: Enter the hostname or IP address of the machine that runs the SMTP server.
- **Connection Mode:** Select the mode in which the SMTP accepts connections. Select TLS or SSL for encrypted connections. The option **None** indicates the default SMTP connection mode (not recommended).
- **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 specified here will be used as the **From address**, when Securden triggers email notifications to users.
- **Supply Credentials:** If authentication is required to gain access to your SMTP server, you need to supply the appropriate credentials.

After providing the required details and authentication credentials, click **Save**. You may test 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** and switch the toggle **Enable Proxy** to green.



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 >> High Availability >> High Availability.

Enable Proxy ●

Showing 0 to 0 of 0 25

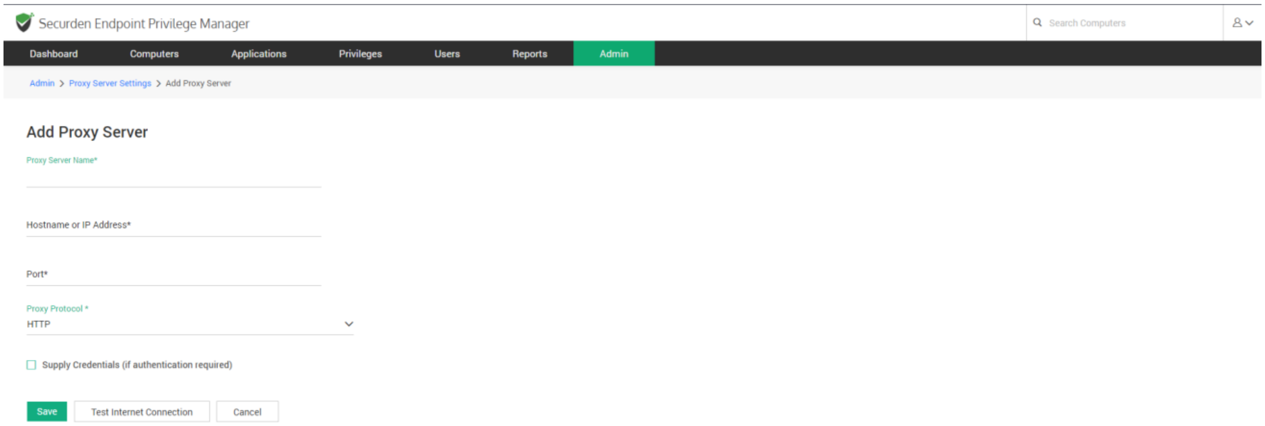
Proxy Server Name	Hostname / IP Address	Port	Actions

No data found

Showing 0 to 0 of 0 25

To add a proxy server, click on **Add Proxy Server.**

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.



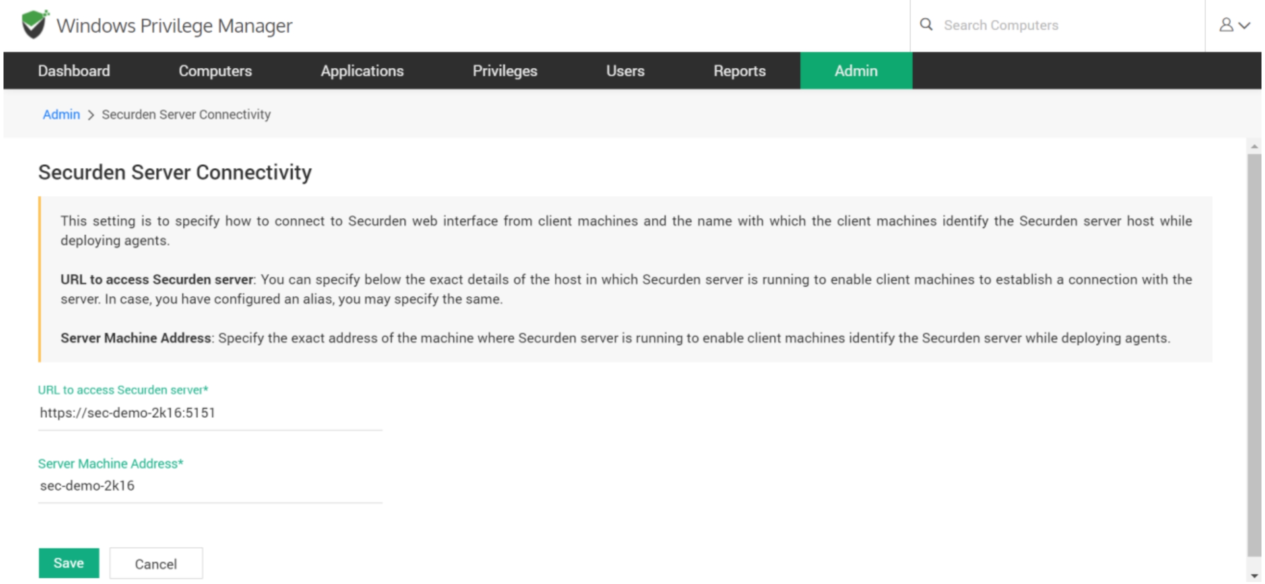
If the proxy server requires authentication, you need to enable the checkbox **Supply Credentials** and enter the credentials.

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

Securden Server Connectivity

Before your users start using Securden, you need to specify how your users can connect to the Securden web interface from endpoints and the name with which the end user machines identify the Securden server host.

To configure server settings, navigate to **Admin >> General >> Securden Server Connectivity**. In the GUI that opens, enter the following details.



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.

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.

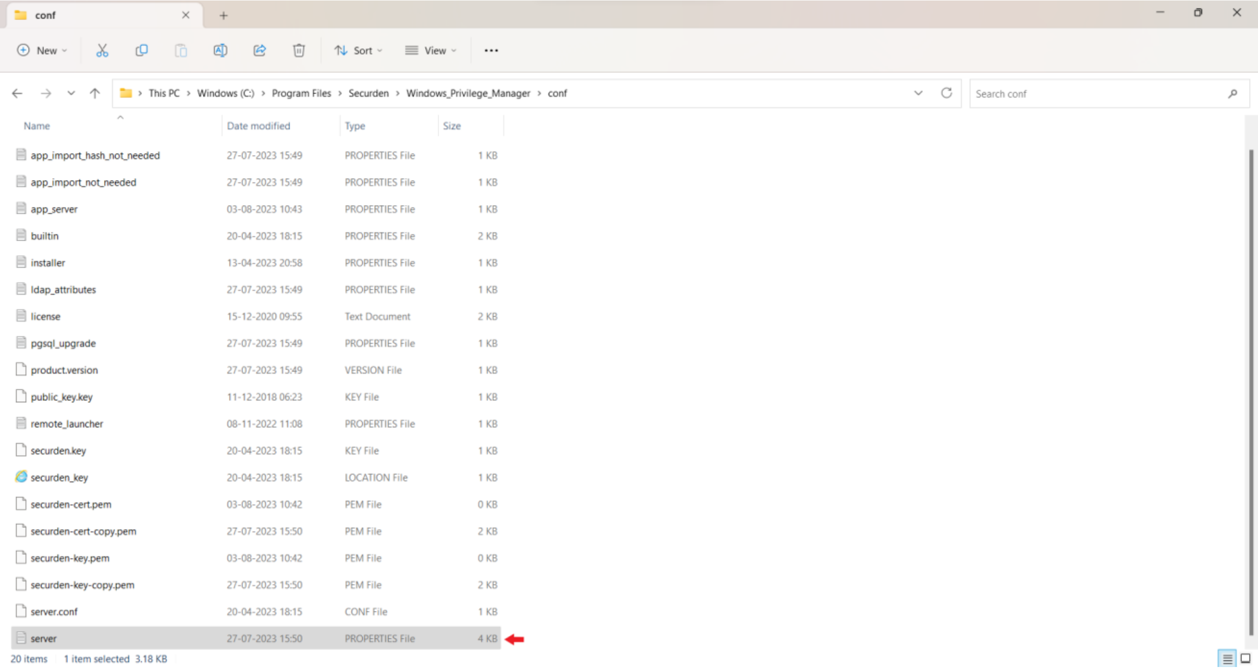
URL to access Securden server*: https://sec-demo-2k16:5151

Server Machine Address*: sec-demo-2k16

URL to access Securden server: This URL refers to the exact details of the host server on which Securden is running. These attributes 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 5151 by default. If you wish to change the Server port, follow the steps below.

To change the server port,

- Navigate to the **<securden installation folder>/conf** directory. Open the file named **server.properties** with Wordpad or notepad++.

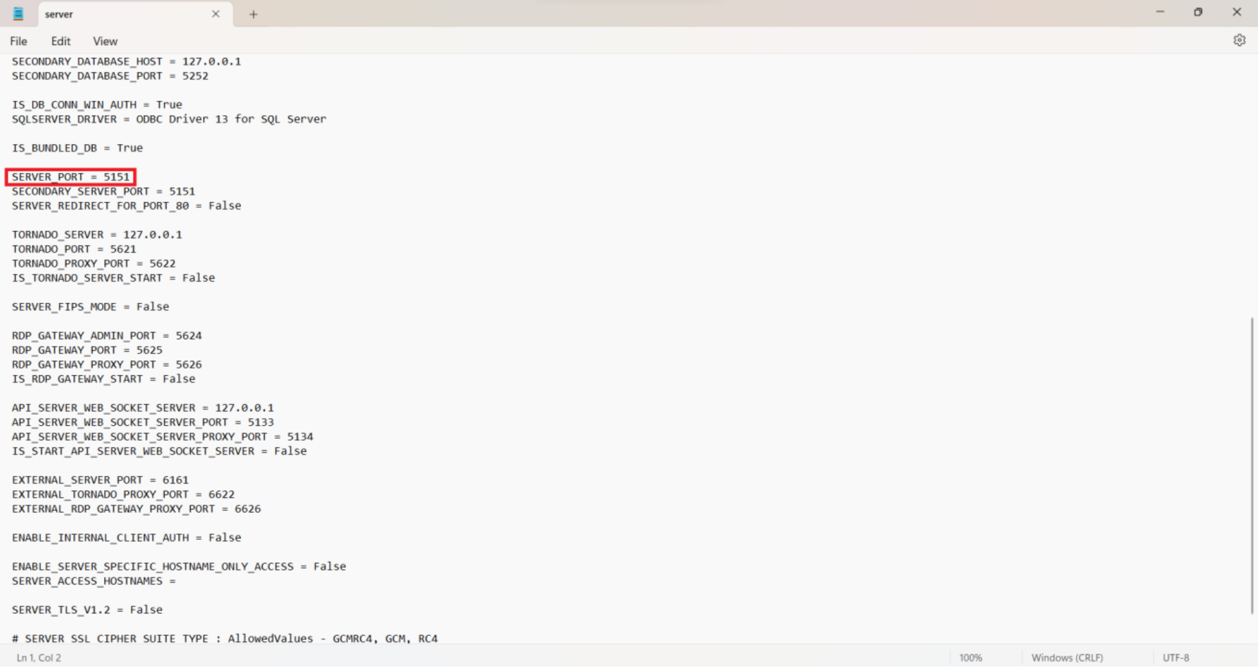


This PC > Windows (C:) > Program Files > Securden > Windows_Privilege_Manager > conf

Name	Date modified	Type	Size
app_import_hash_not_needed	27-07-2023 15:49	PROPERTIES File	1 KB
app_import_not_needed	27-07-2023 15:49	PROPERTIES File	1 KB
app_server	03-08-2023 10:43	PROPERTIES File	1 KB
builtin	20-04-2023 18:15	PROPERTIES File	2 KB
installer	13-04-2023 20:58	PROPERTIES File	1 KB
ldap_attributes	27-07-2023 15:49	PROPERTIES File	1 KB
license	15-12-2020 09:55	Text Document	2 KB
pgsql_upgrade	27-07-2023 15:49	PROPERTIES File	1 KB
product.version	27-07-2023 15:49	VERSION File	1 KB
public_key.key	11-12-2018 06:23	KEY File	1 KB
remote_launcher	08-11-2022 11:08	PROPERTIES File	1 KB
securden.key	20-04-2023 18:15	KEY File	1 KB
securden_key	20-04-2023 18:15	LOCATION File	1 KB
securden-cert.pem	03-08-2023 10:42	PEM File	0 KB
securden-cert-copy.pem	27-07-2023 15:50	PEM File	2 KB
securden-key.pem	03-08-2023 10:42	PEM File	0 KB
securden-key-copy.pem	27-07-2023 15:50	PEM File	2 KB
server.conf	20-04-2023 18:15	CONF File	1 KB
server	27-07-2023 15:50	PROPERTIES File	4 KB

20 items 1 item selected 3.18 KB

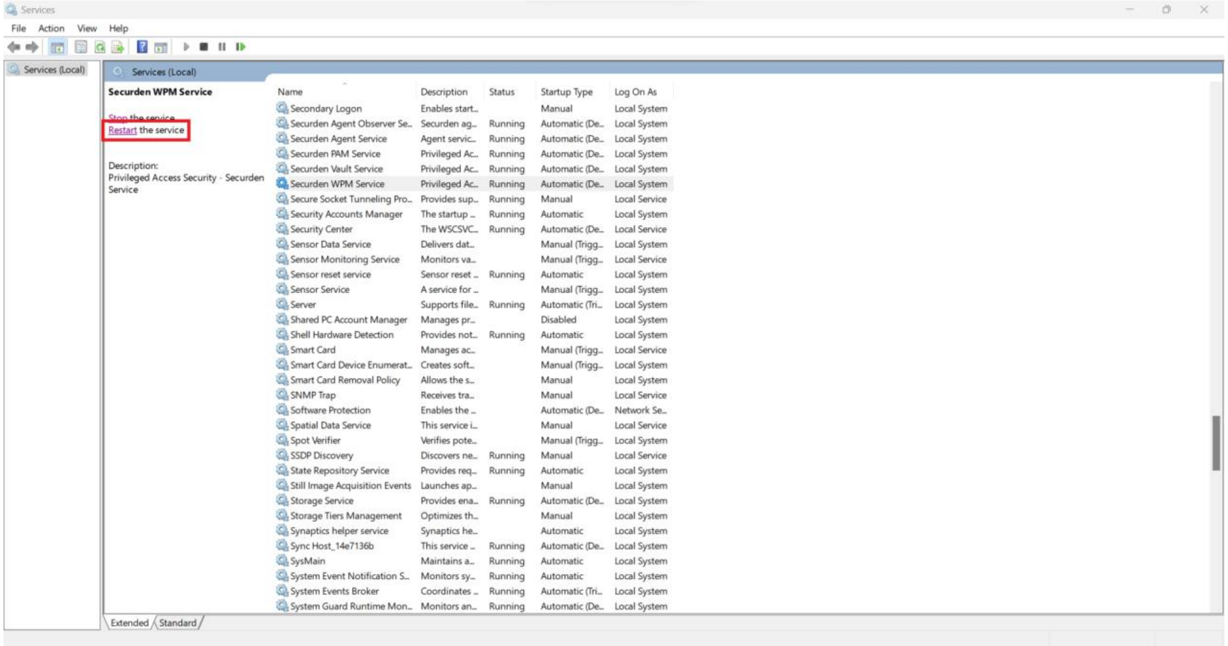
- Look for the entry **SERVER_PORT** and enter the required port number.



```
SECONDARY_DATABASE_HOST = 127.0.0.1
SECONDARY_DATABASE_PORT = 5252

IS_DB_CONN_WIN_AUTH = True
SQLSERVER_DRIVER = ODBC Driver 13 for SQL Server

IS_BUNDLED_DB = True

SERVER_PORT = 5151
SECONDARY_SERVER_PORT = 5151
SERVER_REDIRECT_FOR_PORT_80 = False

TORNADO_SERVER = 127.0.0.1
TORNADO_PORT = 5621
TORNADO_PROXY_PORT = 5622
IS_TORNADO_SERVER_START = False

SERVER_FIPS_MODE = False

RDP_GATEWAY_ADMIN_PORT = 5624
RDP_GATEWAY_PORT = 5625
RDP_GATEWAY_PROXY_PORT = 5626
IS_RDP_GATEWAY_START = False

API_SERVER_WEB_SOCKET_SERVER = 127.0.0.1
API_SERVER_WEB_SOCKET_SERVER_PORT = 5133
API_SERVER_WEB_SOCKET_SERVER_PROXY_PORT = 5134
IS_START_API_SERVER_WEB_SOCKET_SERVER = False

EXTERNAL_SERVER_PORT = 6161
EXTERNAL_TORNADO_PROXY_PORT = 6622
EXTERNAL_RDP_GATEWAY_PROXY_PORT = 6626

ENABLE_INTERNAL_CLIENT_AUTH = False

ENABLE_SERVER_SPECIFIC_HOSTNAME_ONLY_ACCESS = False
SERVER_ACCESS_HOSTNAMES =

SERVER_TLS_V1.2 = False

# SERVER SSL CIPHER SUITE TYPE : AllowedValues - GCMRC4, GCM, RC4
```

Ln 1, Col 2 100% Windows (CRLF) UTF-8

- Restart **Securden WPM Service** from services.msc.



Securden WPM Service

Stop the service
Restart the service

Description:
Privileged Access Security - Securden Service

Name	Description	Status	Startup Type	Log On As
Secondary Logon	Enables start...		Manual	Local System
Securden Agent Observer Se...	Securden ag...	Running	Automatic (De...	Local System
Securden Agent Service	Agent servic...	Running	Automatic (De...	Local System
Securden PAM Service	Privileged Ac...	Running	Automatic (De...	Local System
Securden Vault Service	Privileged Ac...	Running	Automatic (De...	Local System
Securden WPM Service	Privileged Ac...	Running	Automatic (De...	Local System
Secure Socket Tunneling Pro...	Provides sup...	Running	Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local System
Security Center	The WSCSVC...	Running	Automatic (De...	Local Service
Sensor Data Service	Delivers dat...		Manual (Trigg...	Local System
Sensor Monitoring Service	Monitors va...		Manual (Trigg...	Local Service
Sensor reset service	Sensor reset ...	Running	Automatic	Local System
Sensor Service	A service for ...		Manual (Trigg...	Local System
Server	Supports file...	Running	Automatic (Tri...	Local System
Shared PC Account Manager	Manages pr...		Disabled	Local System
Shell Hardware Detection	Provides not...	Running	Automatic	Local System
Smart Card	Manages ac...		Manual (Trigg...	Local Service
Smart Card Device Enumerat...	Creates soft...		Manual (Trigg...	Local System
Smart Card Removal Policy	Allows the s...		Manual	Local System
SNMP Trap	Receives tra...		Manual	Local Service
Software Protection	Enables the ...		Automatic (De...	Network Se...
Spatial Data Service	This service i...		Manual	Local Service
Spot Verifier	Verifies pote...		Manual (Trigg...	Local System
SSDP Discovery	Discovers ne...	Running	Manual	Local Service
State Repository Service	Provides req...	Running	Automatic	Local System
Still Image Acquisition Events	Launches ap...		Manual	Local System
Storage Service	Provides ena...	Running	Automatic (De...	Local System
Storage Tiers Management	Optimizes th...		Manual	Local System
Synaptics helper service	Synaptics he...		Automatic	Local System
Sync Host_14e7136b	This service ...	Running	Automatic (De...	Local System
SysMain	Maintains a...	Running	Automatic	Local System
System Event Notification S...	Monitors sy...	Running	Automatic	Local System
System Events Broker	Coordinates ...	Running	Automatic (Tri...	Local System
System Guard Runtime Mon...	Monitors an...	Running	Automatic (De...	Local System

If you wish to open the Securden WPM interface without entering the port number, you can use the default port number **443**.

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 the Securden server using the domain name, then you can connect using the IP address of the server on which the service is hosted.

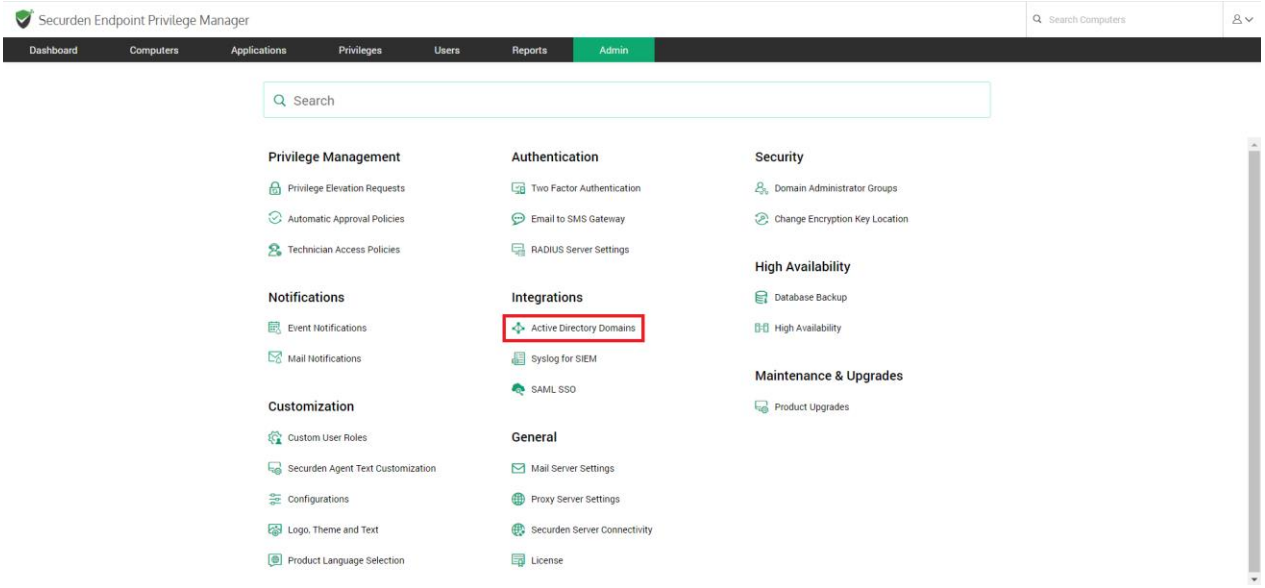
Server Machine Address: Specify the exact address of the machine where the Securden server is running to enable client machines to identify the Securden server while deploying agents.

Integrating Active Directory Domains

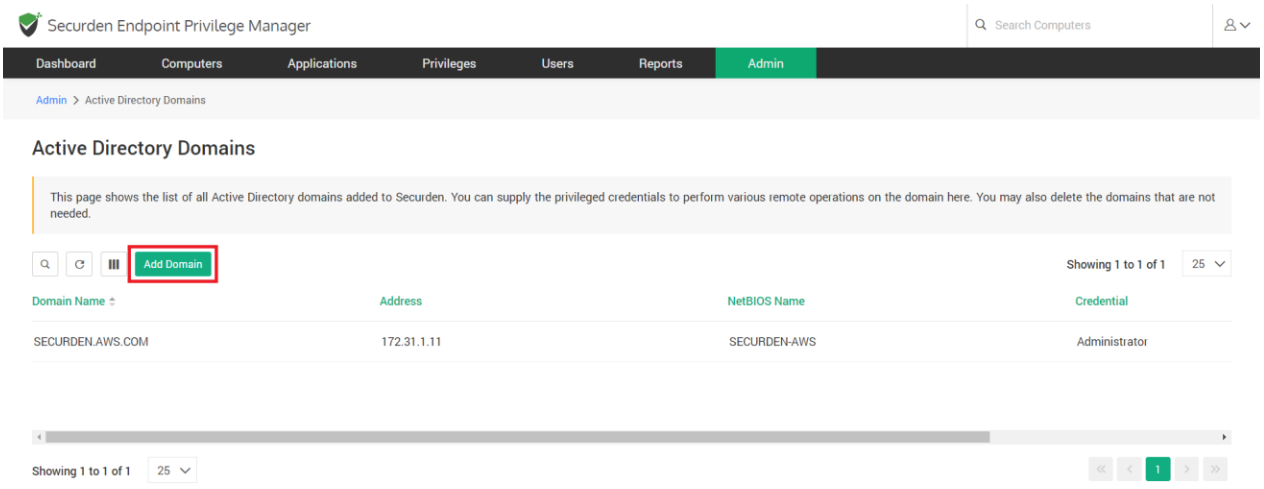
All users and endpoints in your network are linked with your domain. Domain-connected computers, users and OUs in your domain can be easily fetched by Securden WPM into its interface for management.

Securden allows you to add multiple AD domains. You can add all the domains here. Basically, you need to specify the IP address of the domain you want to add and its connectivity details.

To add a new domain, navigate to **Admin >> Integrations >> Active Directory Domains**



If you are about to add your first AD domain to Securden, you will be directly redirected to the **Add Domain** page. If you have already added a domain, it will appear in the list. To add a new domain, click on **Add Domain**.

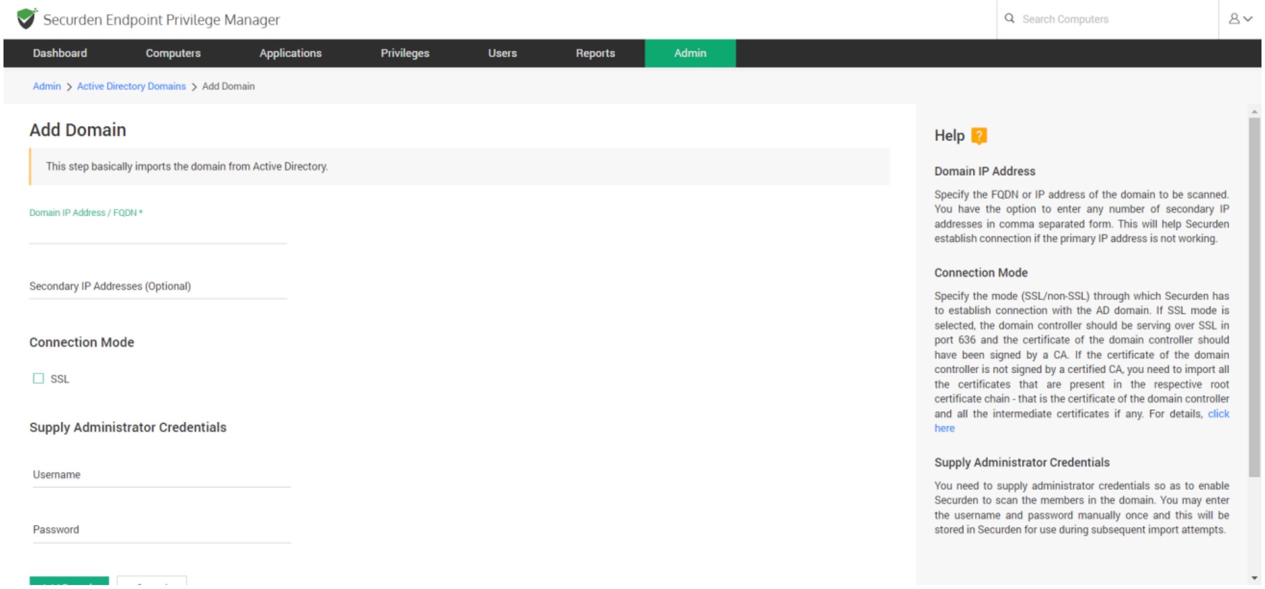


Active Directory Domains

This page shows the list of all Active Directory domains added to Securden. You can supply the privileged credentials to perform various remote operations on the domain here. You may also delete the domains that are not needed.

Domain Name	Address	NetBIOS Name	Credential
SECURDEN.AWS.COM	172.31.1.11	SECURDEN-AWS	Administrator

In the GUI that opens, enter the following details:


Securden Endpoint Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Active Directory Domains > Add Domain

Add Domain

This step basically imports the domain from Active Directory.

Domain IP Address / FQDN *

Secondary IP Addresses (Optional)

Connection Mode

☐ SSL

Supply Administrator Credentials

Username

Password

Help ?

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 stored in Securden for use during subsequent import attempts.

Domain IP Address

Specify the FQDN or IP address of the domain to be added. 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.

Secondary IP Address

Specify the Secondary IP address of the domain, this is useful in case the Primary IP is not reachable.

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.

Supply Administrator Credentials

You need to supply administrator credentials to allow 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 subsequent use.

Once all the fields have been filled, click **Add Domain**.

Once you’ve added the domain, it will be visible on the Active Directory Domains list. You may now connect to the domain and fetch computers and users into Securden easily.

Import Domain Controllers Certificate

An example is provided below highlighting the steps involved in importing 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.

SECTION 2: User Management

Onboarding Users to WPM

User management deals with onboarding the users into Securden WPM. Since application control policy creation could involve workstations/servers as well as users, this step is needed.

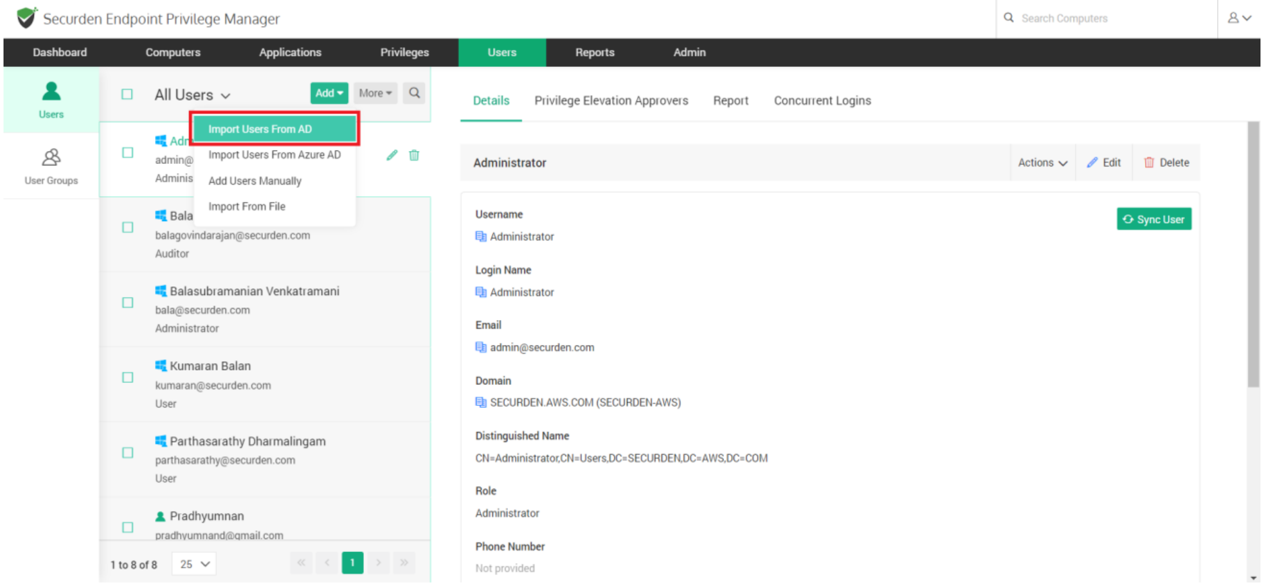
Prerequisite:

Before you proceed with onboarding the users, you should have configured the mail server settings, as the login information will be sent to the registered email address of each user.

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 search for any specific user(s) or a group of users and add them to Securden. Importing from AD is a two-step process.

Navigate to **Users >> Add >> Import Users From AD**.



Adr
admin@
Adminis

Bala
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Pradhyumnan
pradhyumnand@gmail.com

Administrator

Username
Administrator

Login Name
Administrator

Email
admin@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

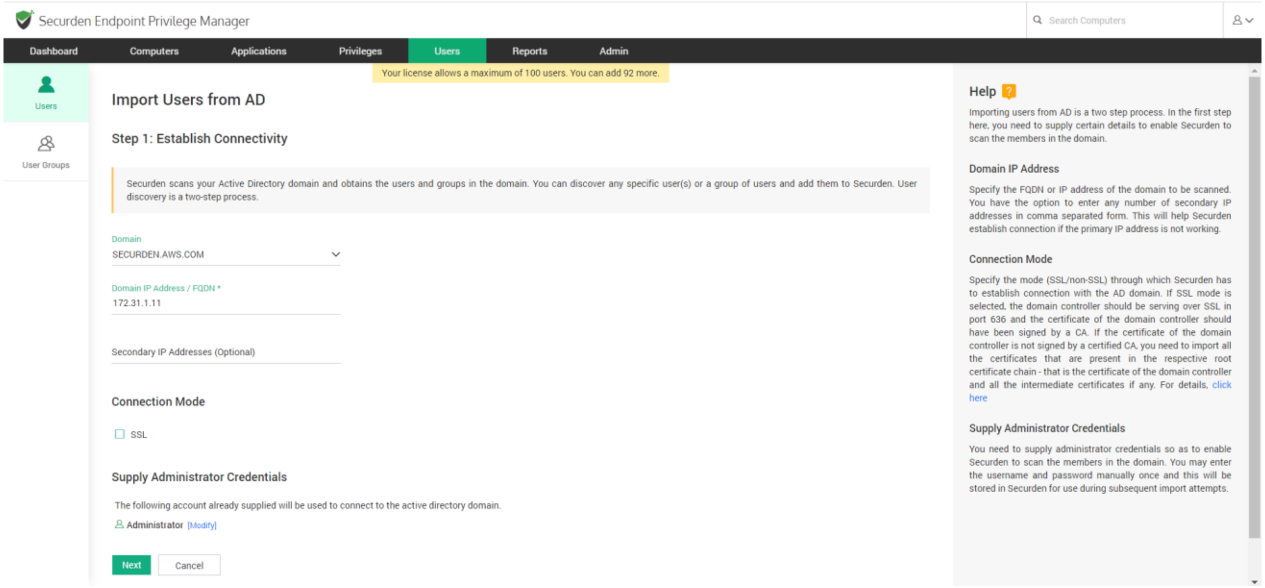
Distinguished Name
CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

Role
Administrator

Phone Number
Not provided

Step 1: Establish Connectivity

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



Your license allows a maximum of 100 users. You can add 92 more.

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
SECURDEN.AWS.COM

Domain IP Address / FQDN *
172.31.1.11

Secondary IP Addresses (Optional)

Connection Mode

□ SSL

Supply Administrator Credentials

The following account already supplied will be used to connect to the active directory domain.

Administrator [Modify]

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 stored in Securden for use during subsequent import attempts.

In the GUI that opens, enter the following details:

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 a comma-separated form. This will help Securden establish connection even if the primary IP 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.

Supply Administrator Credentials: You need to supply administrator credentials to enable Securden WPM 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 specific user(s) or a group of users and add them to Securden with these admin credentials.

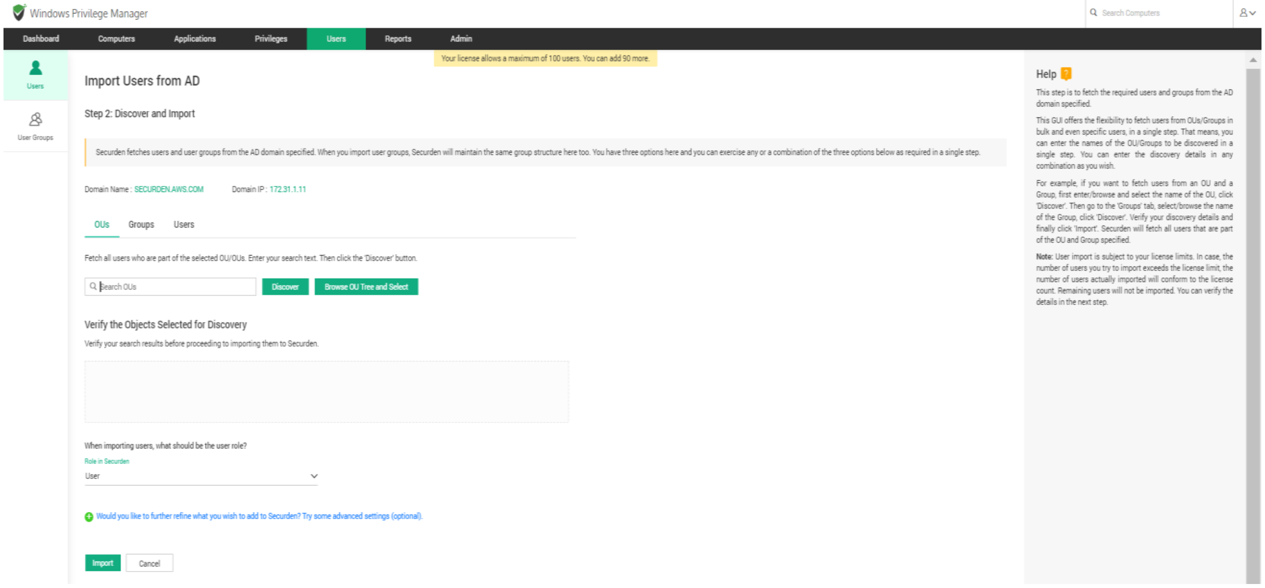
After entering all the details, click on the **Next** button.

Step 2: Import Users

This step is to select and fetch the required users and groups from the AD domain specified. The GUI offers the flexibility to fetch users from OUs/Groups in bulk and even specific users, in a single step. That means you can discover, search, and add the users, OUs, and groups to be imported in a single step.

You can enter the discovery details in any combination of OUs, groups, and users as you wish.

To import OUs, select the **OU** tab.



Your license allows a maximum of 100 users. You can add 90 more.

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

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

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

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

Help

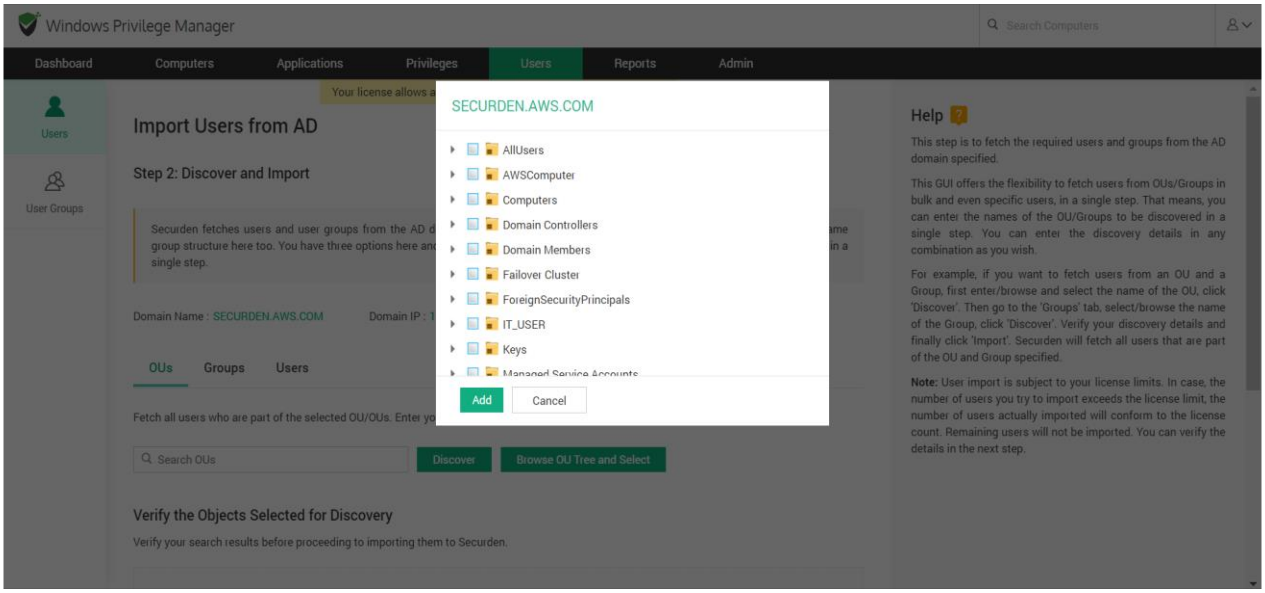
This step is to fetch the required users and groups from the AD domain specified.

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.

1. Enter the OU name in the field named **Search OU** and click **Discover.**
2. You can also browse from the OU tree by clicking on the **Browse OU Tree and Select**. You can select the required OUs from here and select **Add.**



Your license allows a

Import Users from AD

Step 2: Discover and Import

Securden fetches users and user groups from the AD d… group structure here too. You have three options here an… single step.

Domain Name : SECURDEN.AWS.COM Domain IP : 1

Fetch all users who are part of the selected OU/OUs. Enter yo

SECURDEN.AWS.COM

- AllUsers
- AWSComputer
- Computers
- Domain Controllers
- Domain Members
- Failover Cluster
- ForeignSecurityPrincipals
- IT_USER
- Keys
- Managed Service Accounts

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.

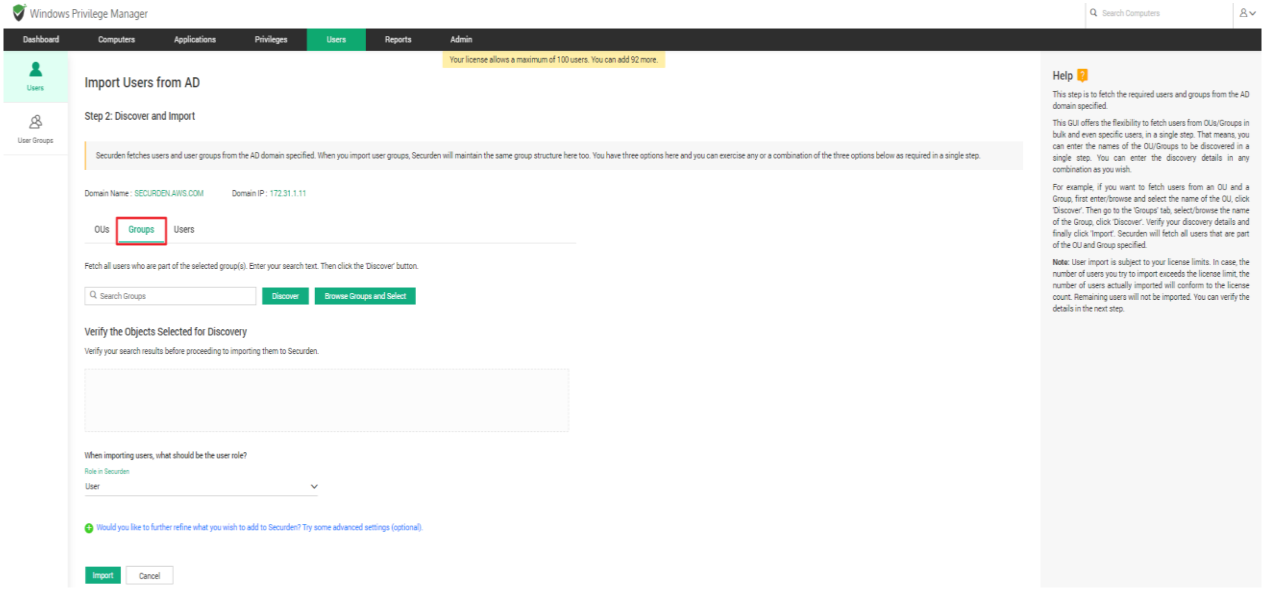
This GUI offers the flexibility to fetch users from OUs/Groups in bulk and even specific users, in a single step. That means, you can enter the names of the OU/Groups to be discovered in a single step. You can enter the discovery details in any combination as you wish.

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.

3. Once all the required OUs are selected, you can verify the selected OUs in the **Verify the Objects Selected for Discovery** section.

To import users from groups, select the **Groups** tab.



Your license allows a maximum of 100 users. You can add 92 more.

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

Fetch all users who are part of the selected group(s). Enter your search text. Then click the 'Discover' button.

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

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

Help

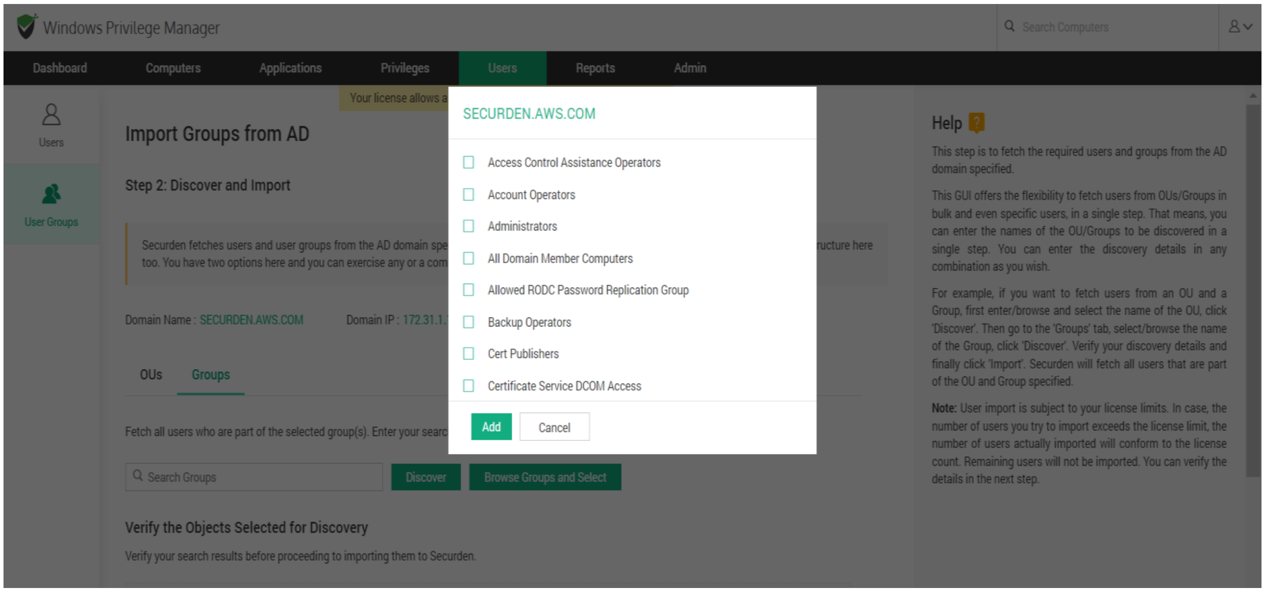
This step is to fetch the required users and groups from the AD domain specified.

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.

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 groups and select **Add.**



Import Groups from AD

Step 2: Discover and Import

Securden fetches users and user groups from the AD domain spe … ructure here too. You have two options here and you can exercise any or a com

Domain Name : SECURDEN.AWS.COM Domain IP : 172.31.1.

Fetch all users who are part of the selected group(s). Enter your searc

SECURDEN.AWS.COM

- □ Access Control Assistance Operators
- □ Account Operators
- □ Administrators
- □ All Domain Member Computers
- □ Allowed RODC Password Replication Group
- □ Backup Operators
- □ Cert Publishers
- □ Certificate Service DCOM Access

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.

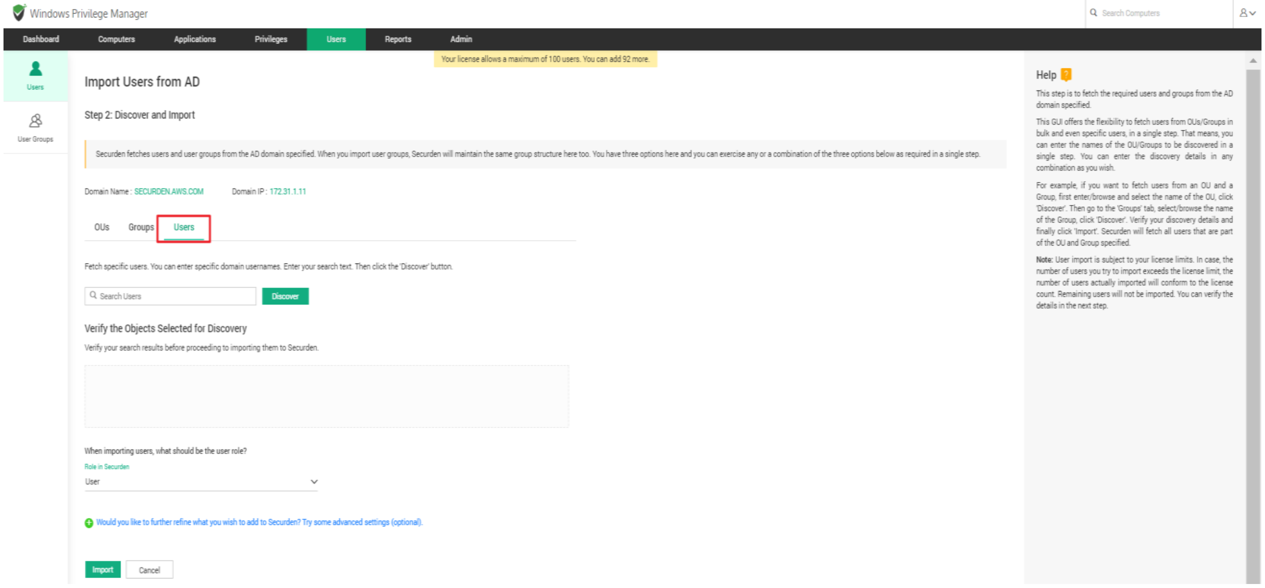
This GUI offers the flexibility to fetch users from OUs/Groups in bulk and even specific users, in a single step. That means, you can enter the names of the OU/Groups to be discovered in a single step. You can enter the discovery details in any combination as you wish.

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.

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

To import Users Individually, **Select the Users tab.**



Your license allows a maximum of 100 users. You can add 92 more.

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

Fetch specific users. You can enter specific domain usernames. Enter your search text. Then click the 'Discover' button.

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

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

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.

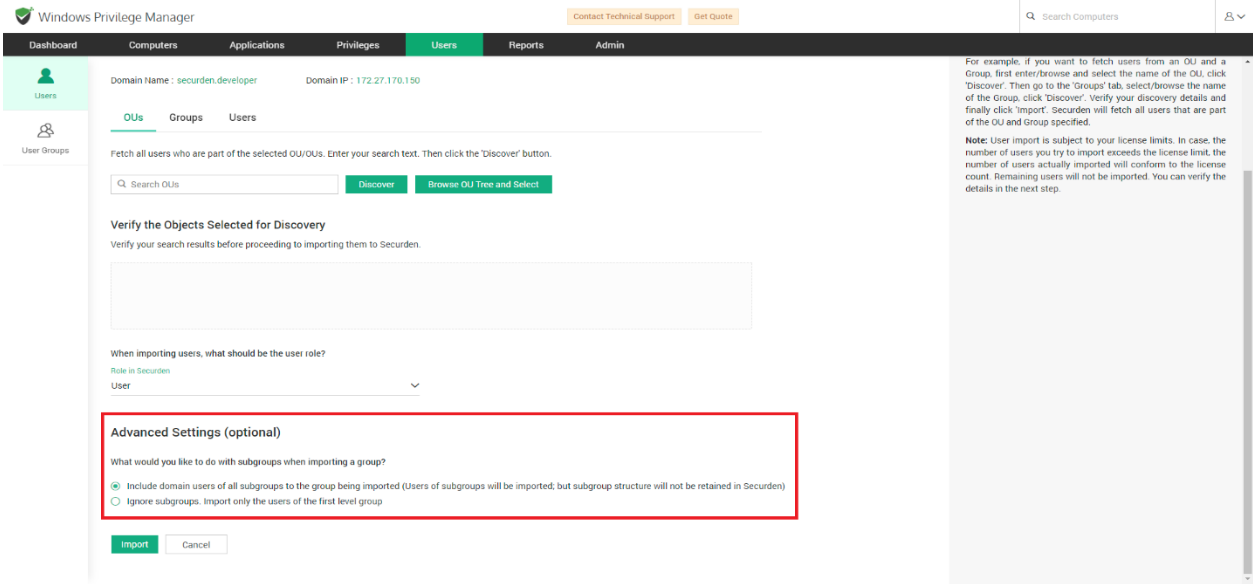
1. Enter the name of the user to be searched and select **Discover.**
2. You can then verify your selection in the **Verify the Objects Selected for Discovery** section.

Once you have selected the required OUs, groups, and users, you may assign a user role for the selected entities from the **Role in Securden** dropdown.

Before selecting import, you can look into the advanced settings which are explained below.

Advanced settings

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



Domain Name : securden.developer

Domain IP : 172.27.170.150

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

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

Advanced Settings (optional)

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

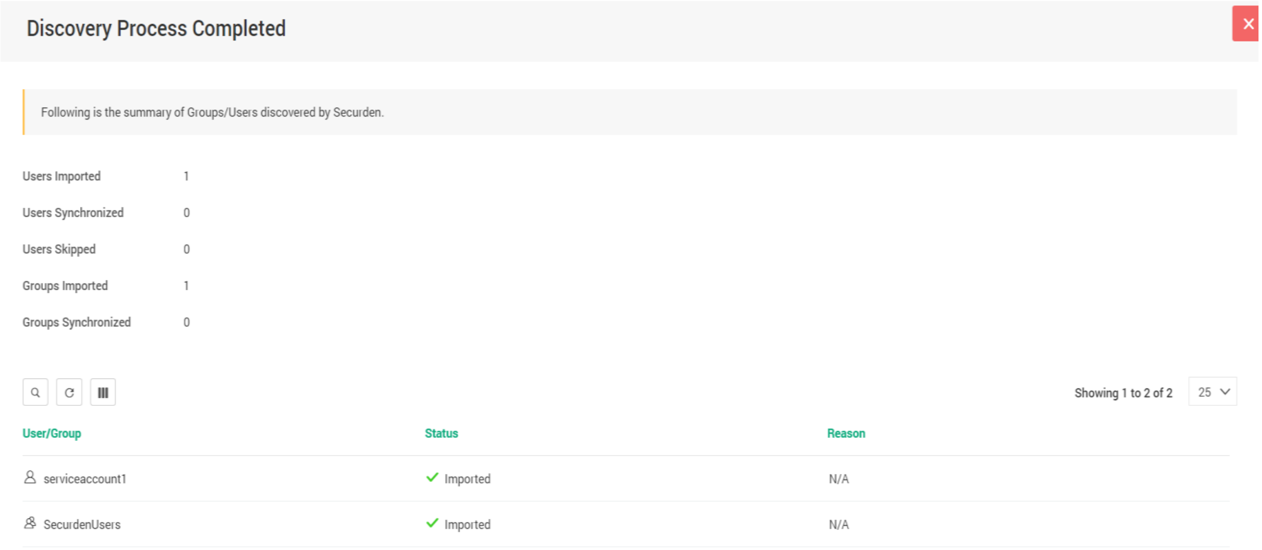
For example, if you want to fetch users from an OU and a Group, first enter/browse and select the name of the OU, click 'Discover'. Then go to the 'Groups' tab, select/browse the name of the Group, click 'Discover'. Verify your discovery details and finally click 'Import'. Securden will fetch all users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

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 may write to support@securden.com for an upgraded license.

You can verify the details in the next step. On selecting the required OUs, groups, and users, Click **Import**.

The process of discovering the OUs/Groups/Users will take a while to complete. The discovered OUs/Groups/Users will be automatically populated to Securden inventory after completion. The summary of imported Users, OUs, and Groups will be displayed as shown below.



Discovery Process Completed

Following is the summary of Groups/Users discovered by Securden.

Users Imported	1
Users Synchronized	0
Users Skipped	0
Groups Imported	1
Groups Synchronized	0

Showing 1 to 2 of 2

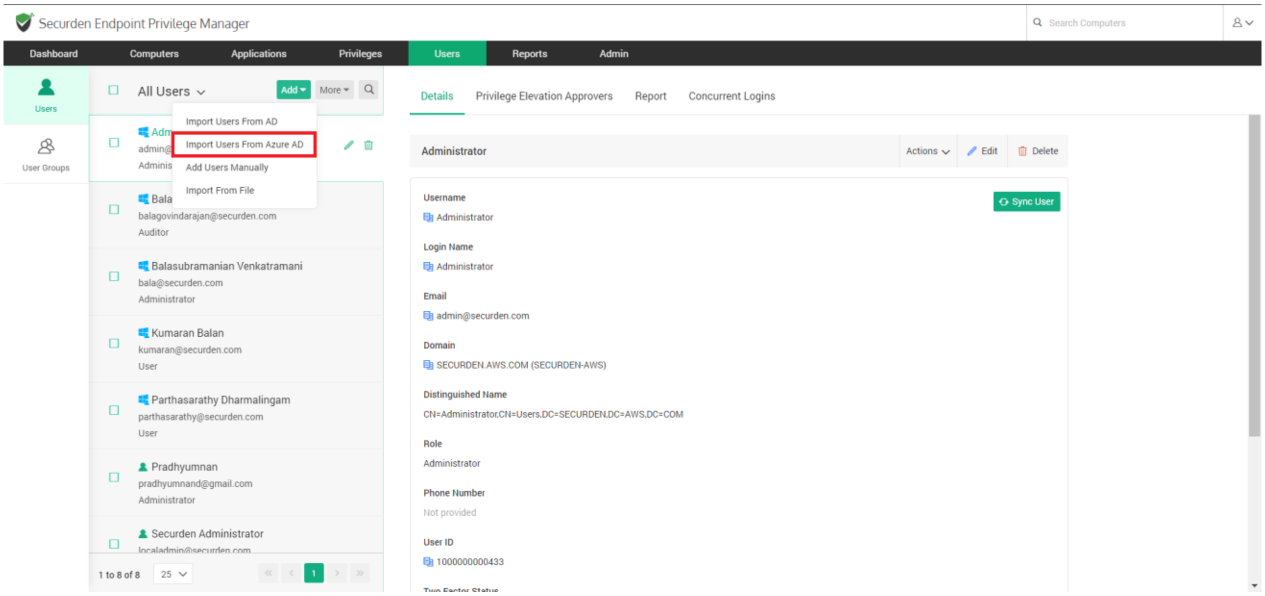
User/Group	Status	Reason
serviceaccount1	✓ Imported	N/A
SecurdenUsers	✓ Imported	N/A

Import from Azure AD

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 (from **Admin >> General >> Proxy Server Settings**).

Securden allows you to import users from Azure AD.

Navigate to **Users >> Add >> Import Users from Azure AD**



Adm
admin@
Adminis

Bala
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Pradhyumnan
pradhyumnand@gmail.com
Administrator

Securden Administrator
localadmin@securden.com

Administrator

Username
Administrator

Login Name
Administrator

Email
admin@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

Role
Administrator

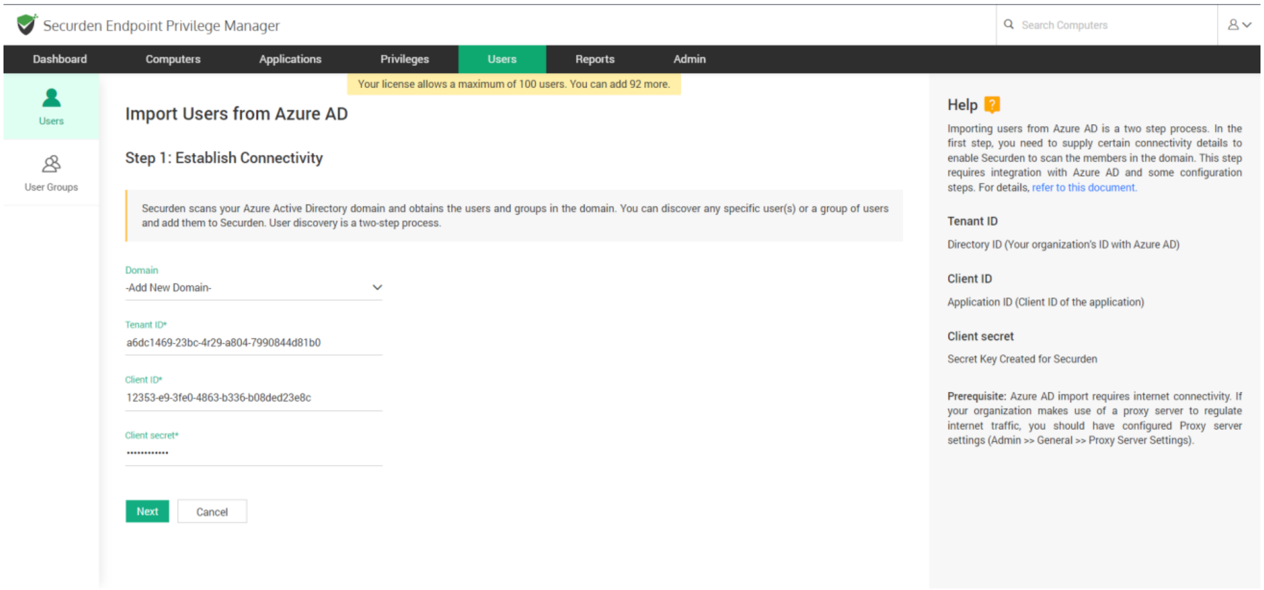
Phone Number
Not provided

User ID
1000000000433

Two Factor Status

Step 1: Establish Connectivity

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.



Your license allows a maximum of 100 users. You can add 92 more.

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.

Domain
-Add New Domain-

Tenant ID*
a6dc1469-23bc-4r29-a804-7990844d81b0

Client ID*
12353-e9-3fe0-4863-b336-b08ded23e8c

Client secret*
••••••••••••

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 that opens, you need the following fields:

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.

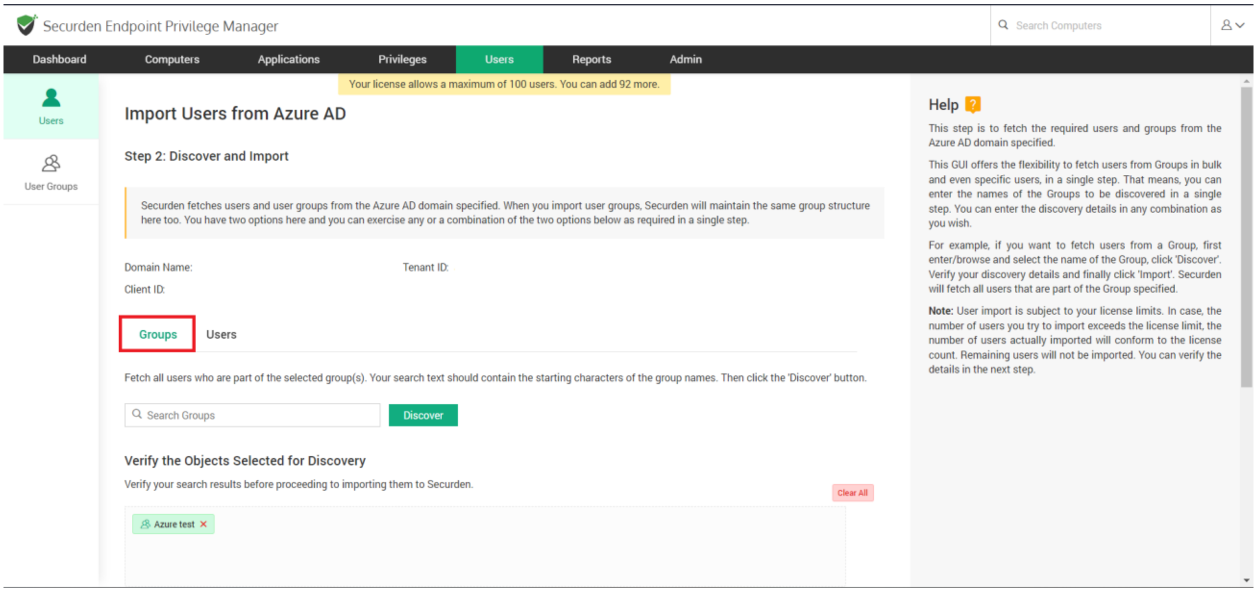
(These details are available on your Azure AD interface)

Once the required details have been filled in, click **Next**.

Step 2: Import Users

This step is to fetch the required users and groups from the Azure AD domain specified. This GUI offers the flexibility to fetch users from groups in bulk and individual users, in a single step. That means you can enter the names of the groups and users to be discovered in a single step.

To import Groups, select the Groups tab.



Your license allows a maximum of 100 users. You can add 92 more.

Import Users from Azure AD

Step 2: Discover and Import

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

Domain Name:

Tenant ID:

Client ID:

Fetch all users who are part of the selected group(s). Your search text should contain the starting characters of the group names. Then click the 'Discover' button.

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 Azure AD domain specified.

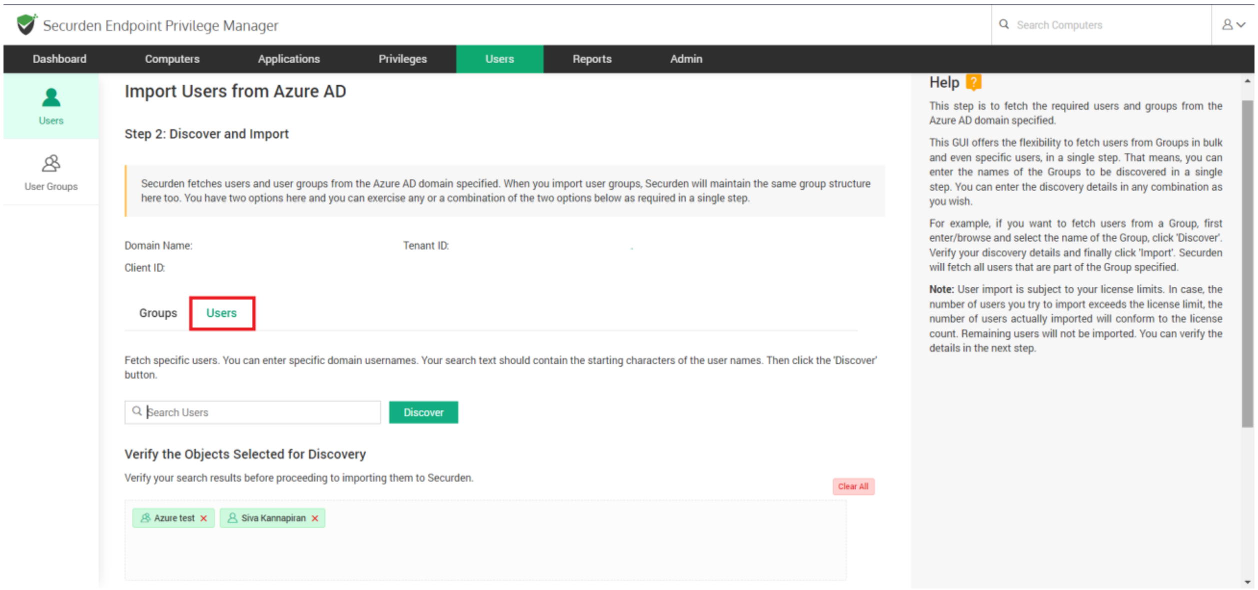
This GUI offers the flexibility to fetch users from Groups in bulk and even specific users, in a single step. That means, you can enter the names of the Groups to be discovered in a single step. You can enter the discovery details in any combination as you wish.

For example, if you want to fetch users from a Group, first enter/browse and select 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 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.

1. Enter the required group name and select **Discover.**
2. You can then verify your selection in the **Verify the Objects Selected for Discovery.**
3. You can select the role for the groups imported using the **Role in Securden** dropdown.

To import Users, Select the Users tab



Import Users from Azure AD

Step 2: Discover and Import

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

Domain Name:

Tenant ID:

Client ID:

Fetch specific users. You can enter specific domain usernames. Your search text should contain the starting characters of the user names. Then click the 'Discover' button.

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 Azure AD domain specified.

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

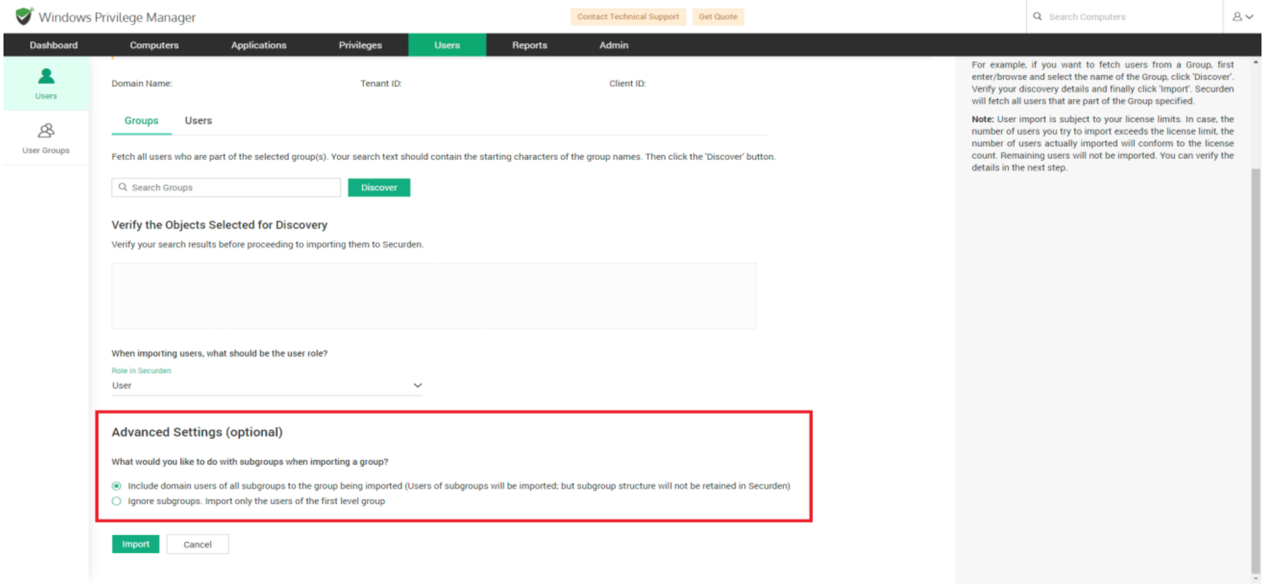
For example, if you want to fetch users from a Group, first enter/browse and select the name of the Group, click 'Discover'. Verify your discovery details and finally click 'Import'. Securden will fetch all users that are part of the Group specified.

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.

1. Enter the name of the user in the search bar and select **Discover.**
2. Verify your selection in the **Verify the Objects Selected for Discovery.**
3. You can select the role for the Users imported using the **Role in Securden** dropdown.

Advanced settings

It is common to have subgroups in AD. When importing a group, you have the option to import all the subgroups along with the users. You can choose to import the subgroup or ignore them.



Domain Name: Tenant ID: Client ID:

Fetch all users who are part of the selected group(s). Your search text should contain the starting characters of the group names. Then click the 'Discover' button.

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

Advanced Settings (optional)

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

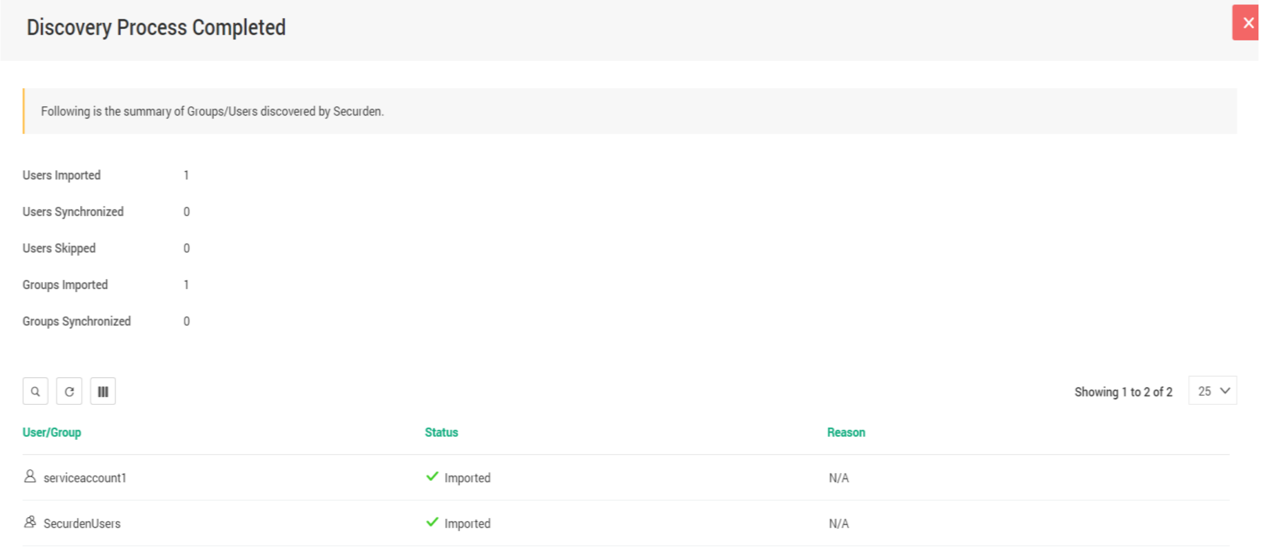
For example, if you want to fetch users from a Group, first enter/browse and select the name of the Group, click 'Discover'. Verify your discovery details and finally click 'Import'. Securden will fetch all users that are part of the Group specified.

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.

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.

On selecting the required Users, OUs and Groups, click on **Import**.

The process of discovering and importing the OUs/Groups/Users will take some time to complete. The discovered OUs/Groups/Users will be automatically populated to Securden inventory after completion. The summary of imported Users, OUs, and Groups will be displayed.



Discovery Process Completed

Following is the summary of Groups/Users discovered by Securden.

Users Imported	1
Users Synchronized	0
Users Skipped	0
Groups Imported	1
Groups Synchronized	0

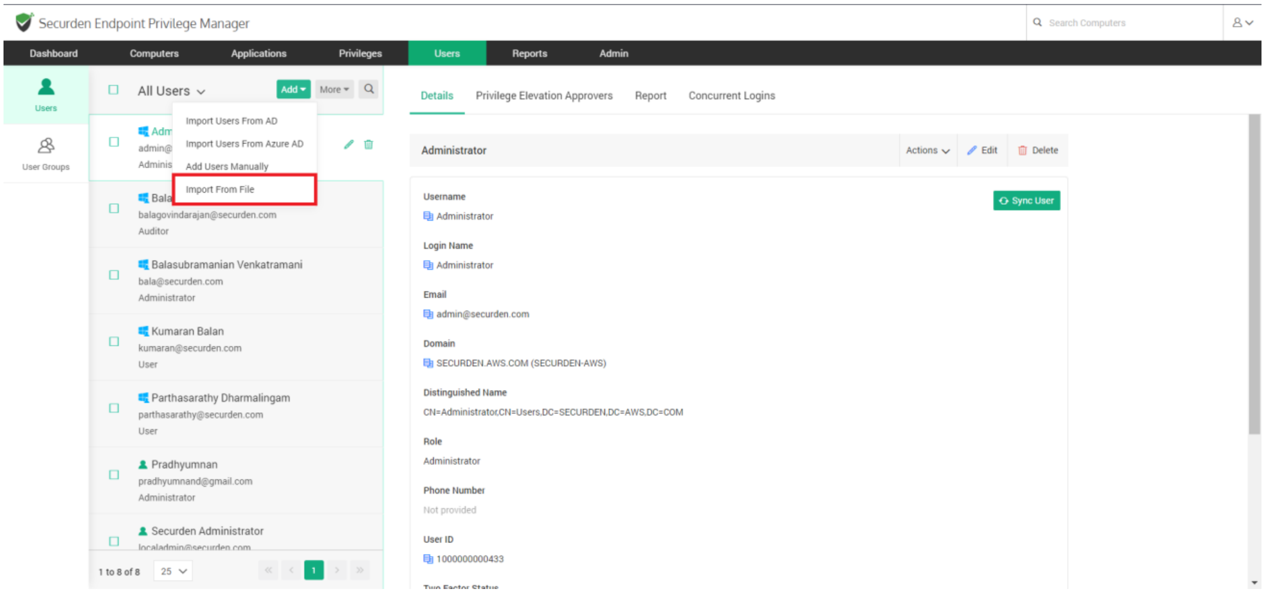
Showing 1 to 2 of 2

User/Group	Status	Reason
serviceaccount1	✓ Imported	N/A
SecurdenUsers	✓ Imported	N/A

Import from File

Importing users is very flexible in Securden. If you already have cataloged users or if you have a file exported from another password manager/repository, then you can import them using an XLSX/CSV file. As part of the import process, you may need to convert the input file format to Securden database file format using the mapping feature discussed below. Typically, each line in the input file is added as a user.

To import users, navigate to **Users >> Add >> Import From File**.



Adm
admin@
Adminis

Bala
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Pradhyumnan
pradhyumnand@gmail.com
Administrator

Securden Administrator
localadmin@securden.com

Administrator

Username
Administrator

Login Name
Administrator

Email
admin@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

Role
Administrator

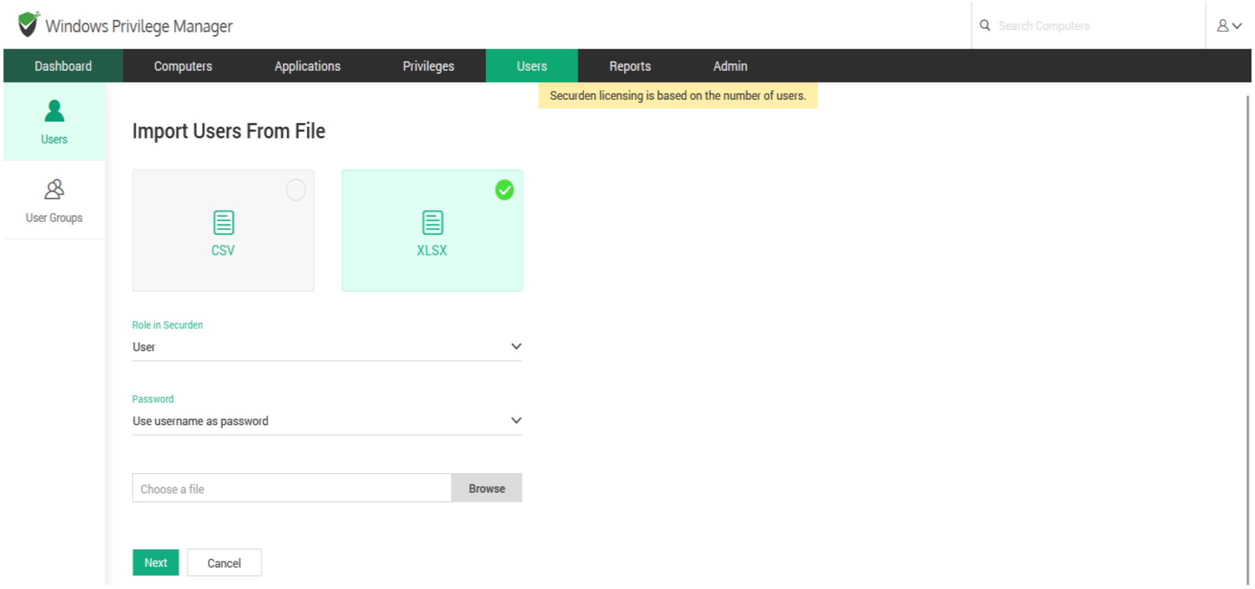
Phone Number
Not provided

User ID
1000000000433

Two Factor Status

In the GUI that opens, fill in the required details as below

File Format: Choose your input file format here. CSV will be selected by default. If you need to import using excel sheet, then simply select the XLSX option.



Securden licensing is based on the number of users.

Import Users From File

Role in Securden
User

Password
Use username as password

Choose a file

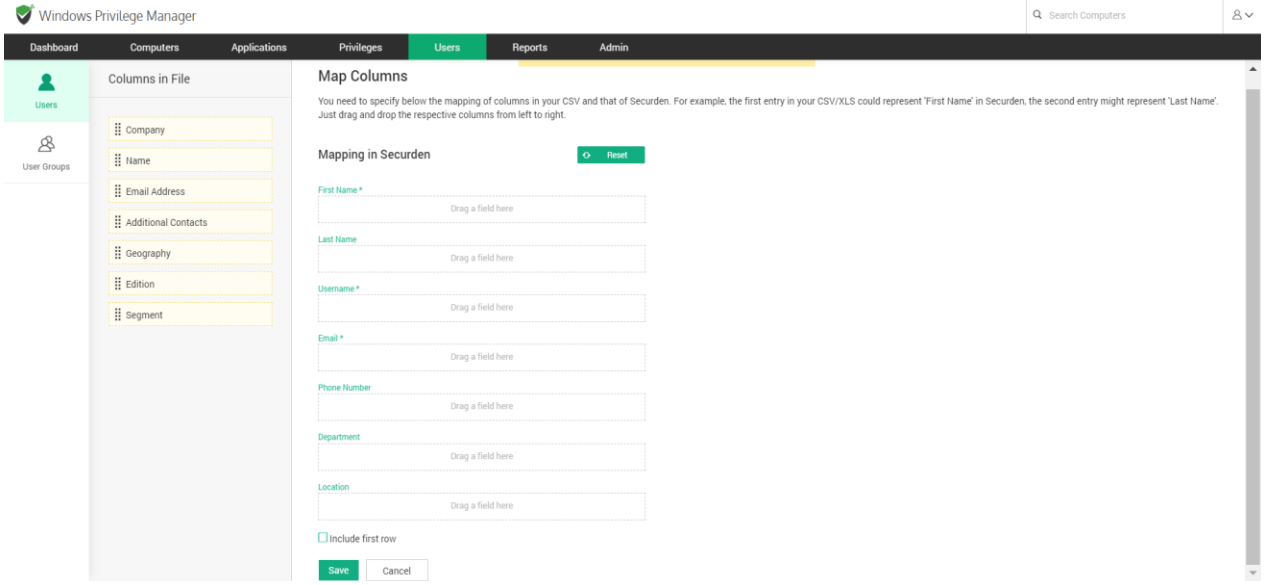
If you are importing from a CSV file, you need to specify the delimiter in the **Delimiter** field to separate the values in the file. You have comma, tab, colon, and semicolon options to choose from the drop-down. Irrespective of your file format selection, the rest of the GUI fields are the same. You should proceed further to fill in other fields as below.

- **Role in Securden:** You can select the user role of the imported user(s) from the dropdown.
- **Password:** Here you have the option to choose between sending an email with the password creation link and using the username as a password. Choose your option from the drop down.
- **Browse:** Browse the location of your input file and select it.

Once done, click **Next**.

Map Columns

Here you can map the columns in your input file to attributes in Securden WPM.



Columns in File

- Company
- Name
- Email Address
- Additional Contacts
- Geography
- Edition
- Segment

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

First Name *: Drag a field here

Last Name: Drag a field here

Username *: Drag a field here

Email *: Drag a field here

Phone Number: Drag a field here

Department: Drag a field here

Location: Drag a field here

☐ Include first row

For example, you can map (LHS) --> (RHS),

Username ---> Name,

Password --> Password,

URL --> URL,

Hostname --> Hostname (created as additional field),

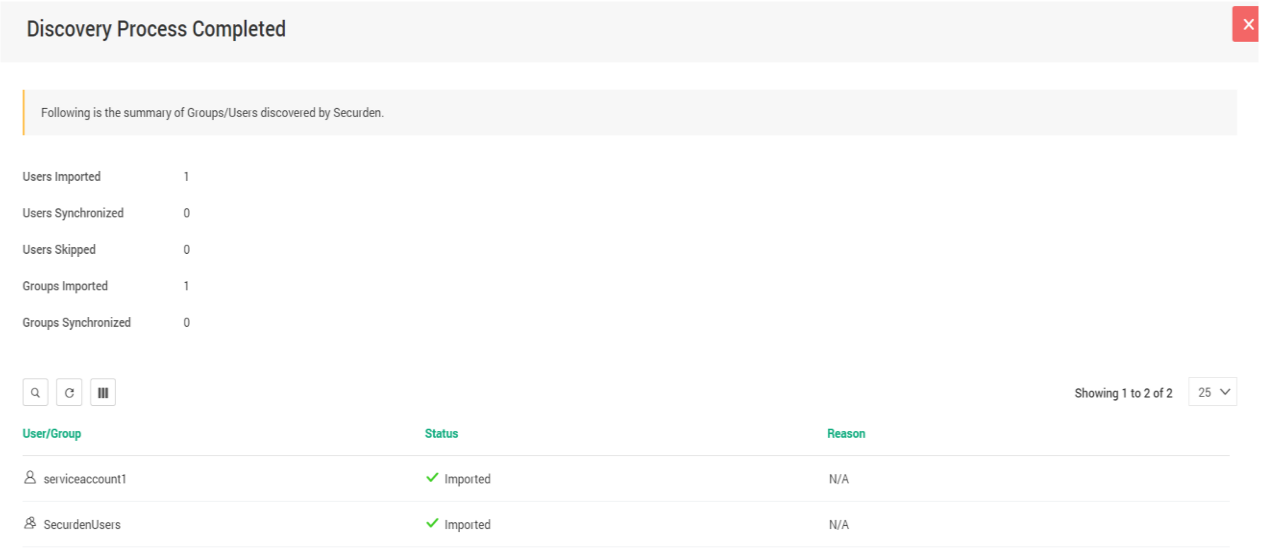
extra --> extra (created as additional field),

grouping ---> Folders.

Note: If you have used the first row of your file to define a user, you need to select the checkbox named **Include first row**.

After mapping the fields, click **Save**.

The discovery process will take few moments to import and populate all the users in Securden. Once the process is complete, a summary of users and user groups that were imported, synchronized, skipped will be displayed.



Discovery Process Completed

Following is the summary of Groups/Users discovered by Securden.

Users Imported	1
Users Synchronized	0
Users Skipped	0
Groups Imported	1
Groups Synchronized	0

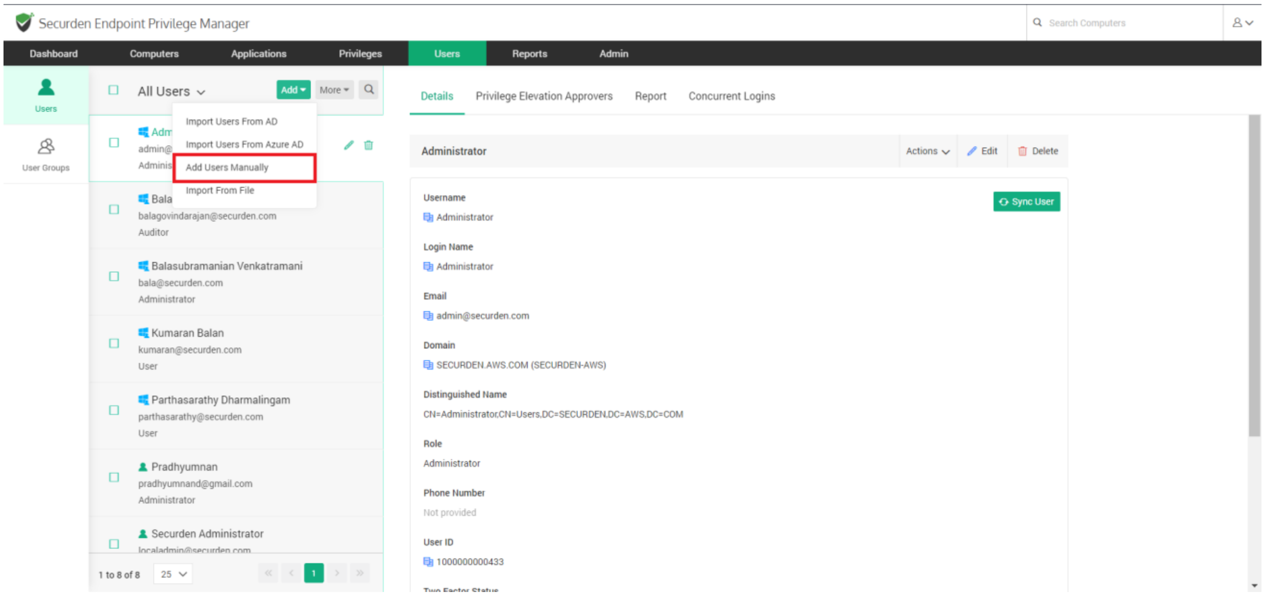
Showing 1 to 2 of 2 | 25

User/Group	Status	Reason
serviceaccount1	✓ Imported	N/A
SecurdenUsers	✓ Imported	N/A

Note: When an attempt is made to import more users than what is provisioned through the license, the number of users provisioned through the license will be imported and the rest will be skipped.

Add Users Manually

You can also create users in Securden WPM manually. Similar to importing from files, users added manually will get login credentials to access WPM. Navigate to **Users >> Add >> Add Users Manually.**



Adm
admin@
Adminis

Bala
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Pradhyumnan
pradhyumnand@gmail.com
Administrator

Securden Administrator
localadmin@securden.com

Administrator

Username
Administrator

Login Name
Administrator

Email
admin@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

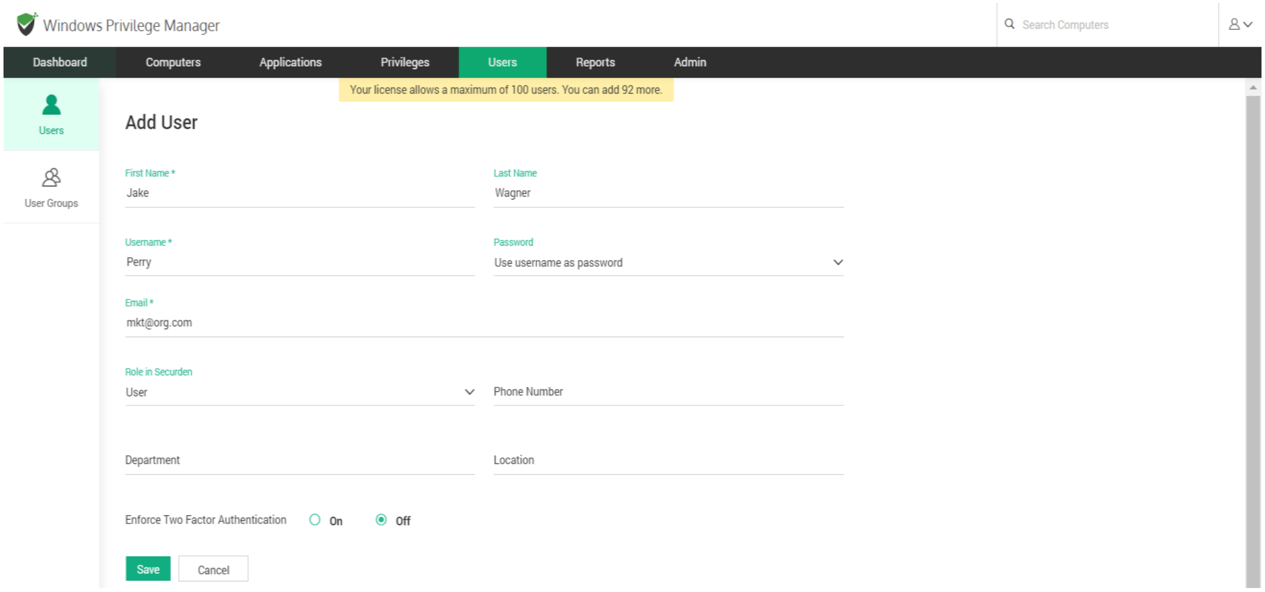
Role
Administrator

Phone Number
Not provided

User ID
1000000000433

Two Factor Status

In this GUI, you will have to provide the following information to add a user.



Your license allows a maximum of 100 users. You can add 92 more.

Add User

First Name * Jake

Last Name Wagner

Username * Perry

Password Use username as password

Email * mkt@org.com

Role in Securden User

Phone Number

Department

Location

Enforce Two Factor Authentication ○ On ● Off

Save Cancel

1. **First Name** - Enter the user's first name in the respective field.
2. **Last name** - Enter the user’s last name. This field is not mandatory.
3. **Username** - Enter a unique username with which the user can log in to Securden.
4. For the password, choose from three options:
    - **Use Username as Password** - The password will be the same as the username provided.
    - **Email Password Creation Link** - An email will be sent to the user using which they can create their own password.
5. **Password Policy** - Select a password policy from the drop-down.
6. **Role in Securden** - You can set the access level of the user by selecting the role the user will be categorized as. You can choose from five roles, Super Administrator, Administrator, Auditor, Account Manager, and User. The access levels of each role are explained later in the section **Default User Roles**.

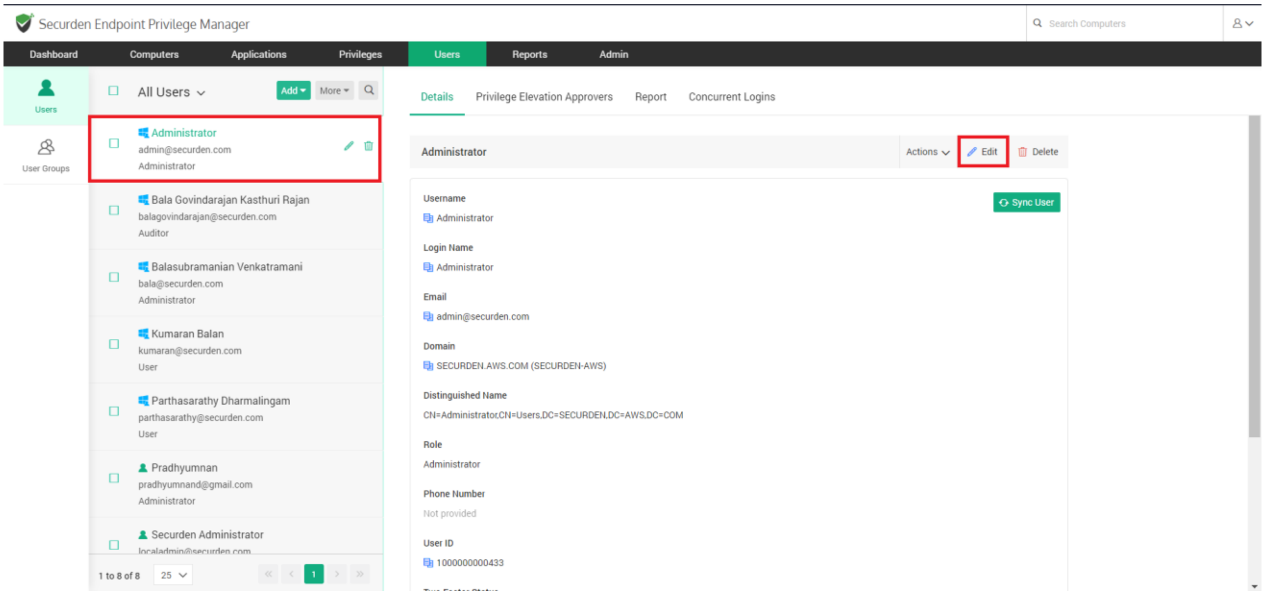
7. **Phone Number, Department & Location** - These three fields are not mandatory, but you can add them to ensure precise user information for efficient management.

You have the option to enforce two-factor authentication for the user created. You can select the checkbox named **User specific 2FA options** and enable 2FA.

Once all the details are furnished, click **Save** to create the user.

Editing Users

After importing the users into Securden, you can make modifications to the user attributes if you want. Select the required user and click **Edit**.



Administrator
admin@securden.com
Administrator

Bala Govindarajan Kasthuri Rajan
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Pradhyumnan
pradhyumnand@gmail.com
Administrator

Securden Administrator
localadmin@securden.com

Administrator

Username
Administrator

Login Name
Administrator

Email
admin@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

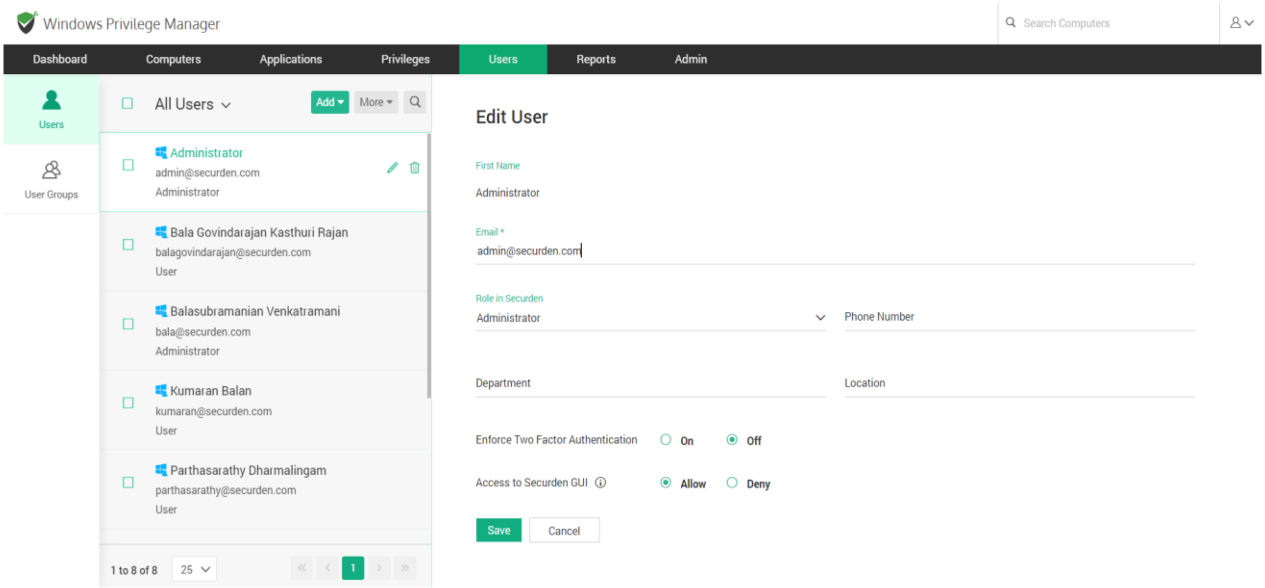
Distinguished Name
CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

Role
Administrator

Phone Number
Not provided

User ID
1000000000433

You can modify any field you want.



Administrator
admin@securden.com
Administrator

Bala Govindarajan Kasthuri Rajan
balagovindarajan@securden.com
User

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Edit User

First Name: Administrator

Email *: admin@securden.com

Role in Securden: Administrator

Phone Number

Department

Location

Enforce Two Factor Authentication ○ On ● Off

Access to Securden GUI ● Allow ○ Deny

Save Cancel

You can enable or disable two-factor authentication and temporarily deny or allow specific users to access the Securden web interface as needed.

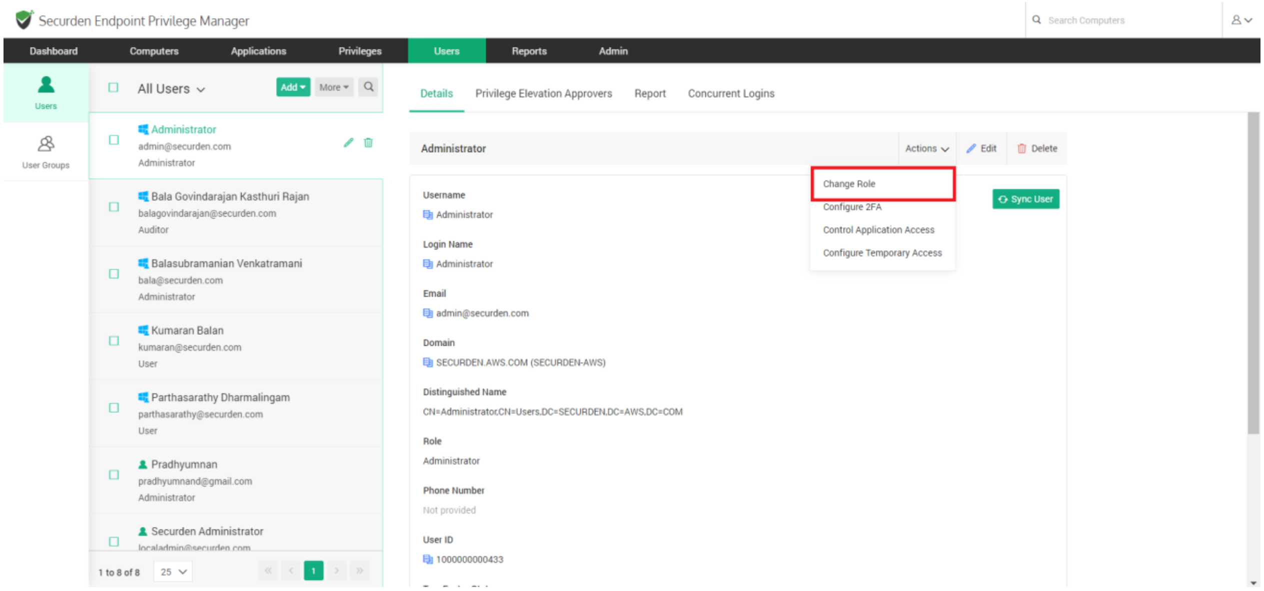
Make the required changes and click **Save.**

Assign Roles to Users

By default, the users imported from Active Directory or other means will have the role **User**. You can change and assign roles for these users individually or in groups.

To change the role of a user,

1. Navigate to the **Users** tab in the GUI, and select the required users.
2. Go to **Actions >> Change Role**.



Administrator
admin@securden.com
Administrator

Bala Govindarajan Kasthuri Rajan
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Pradhyumnan
pradhyumnand@gmail.com
Administrator

Securden Administrator
localadmin@securden.com

Administrator

Username
Administrator

Login Name
Administrator

Email
admin@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

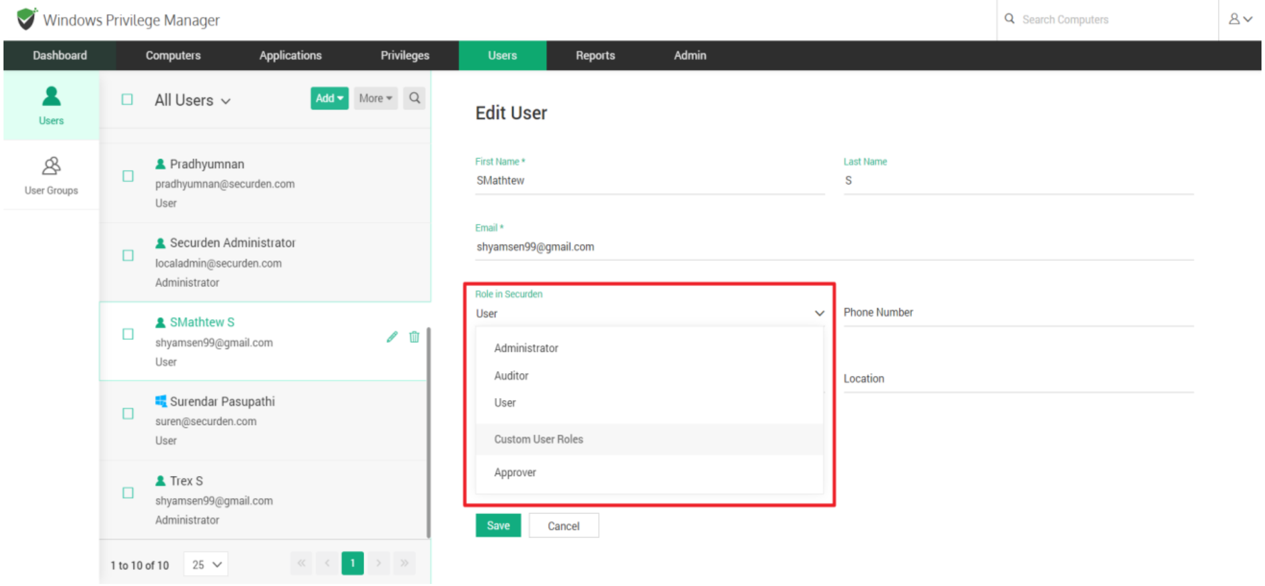
Role
Administrator

Phone Number
Not provided

User ID
1000000000433

Alternatively, you may use the **Edit** option to change the role of users.

Under the drop-down named **Role in Securden,** you will find a list of three default roles available in Securden. They are explained as below



Pradhyumnan
pradhyumnan@securden.com
User

Securden Administrator
localadmin@securden.com
Administrator

SMathtew S
shyamsen99@gmail.com
User

Surendar Pasupathi
suren@securden.com
User

Trex S
shyamsen99@gmail.com
Administrator

Edit User

First Name * SMathtew

Last Name S

Email * shyamsen99@gmail.com

Role in Securden User

Phone Number

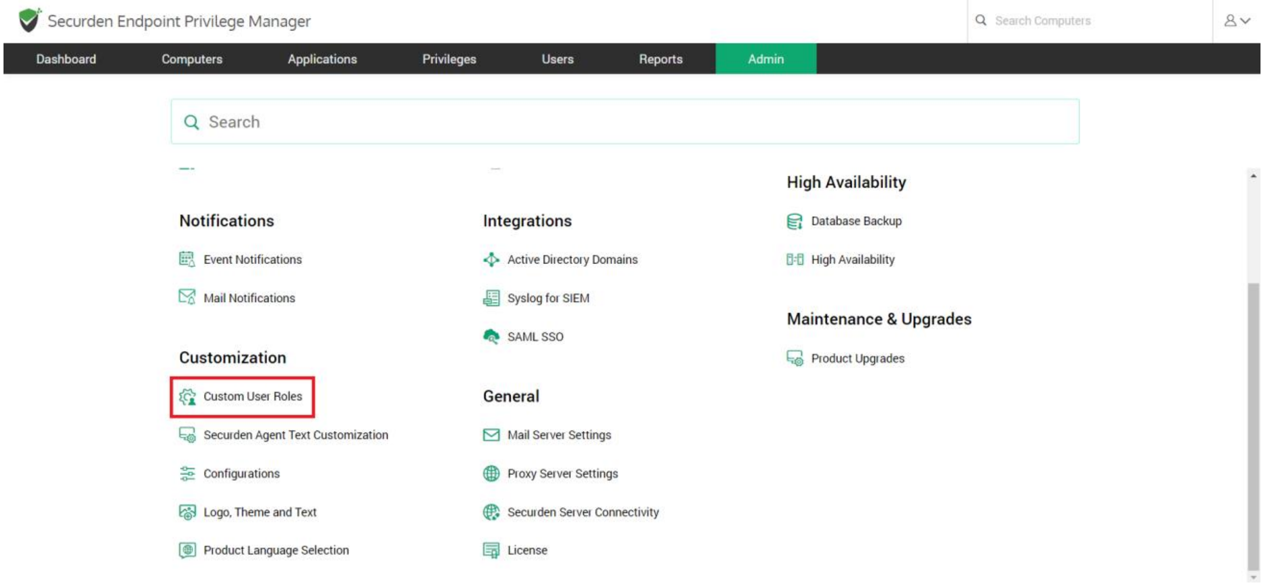
Location

- **Administrator** - They can administer the application, including user management. They will be able to manage privilege elevation requests raised by users.
- **Approver –** They can manage privilege elevation requests raised by users. They can choose to approve or reject requests once they vaildate them.
- **Auditor** - They can view the reports and audit trails generated in the application. They can manually add users.
- **User** - They will have general access to the web UI. Most of their interactions will be with the Securden agent. They can raise privilege elevation requests using the agent.

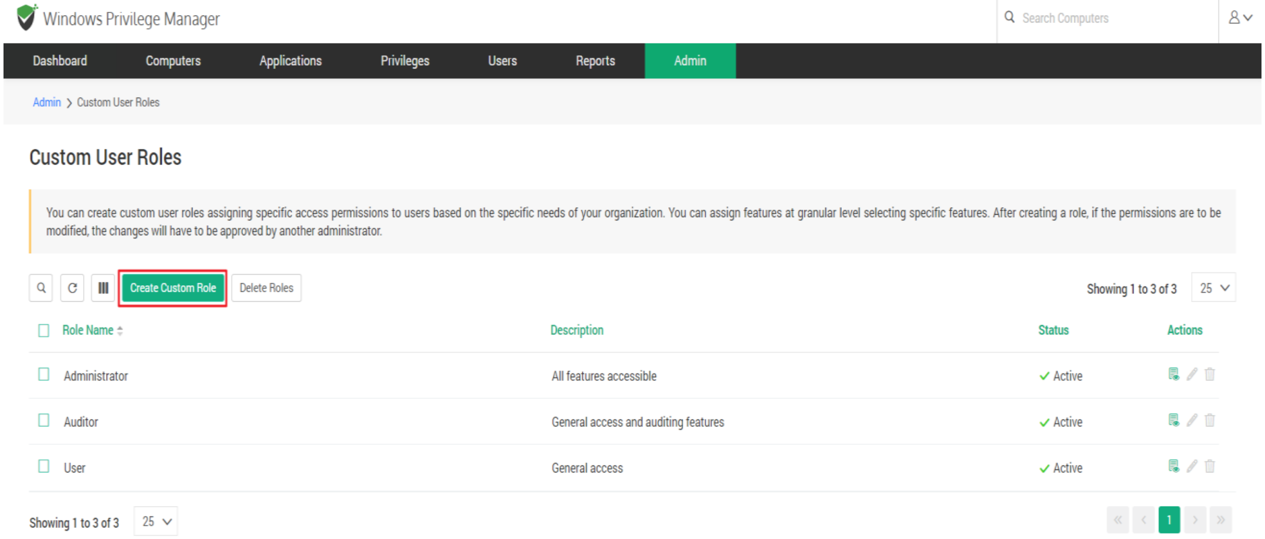
Custom User Roles

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. After creating a role, if the permissions are to be modified, the changes will have to be approved by another administrator.

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



A list containing all the existing roles and corresponding descriptions will be displayed. In addition, you have the option to create new roles or delete existing roles.



Custom User Roles

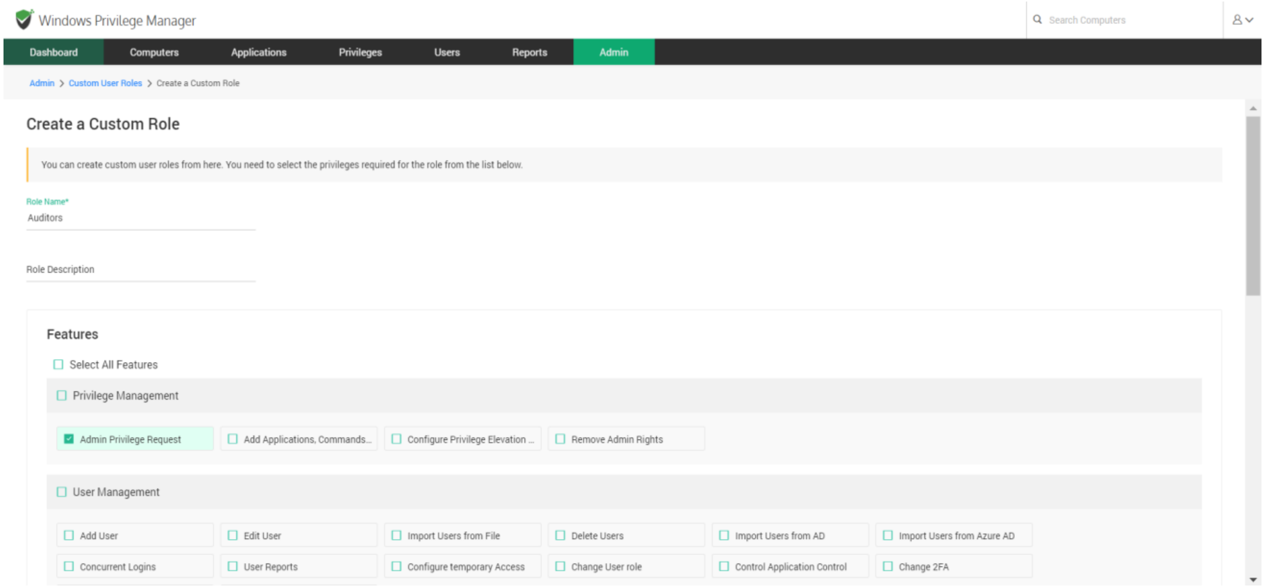
You can create custom user roles assigning specific access permissions to users based on the specific needs of your organization. You can assign features at granular level selecting specific features. After creating a role, if the permissions are to be modified, the changes will have to be approved by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

Showing 1 to 3 of 3 25

□	Role Name	Description	Status	Actions
□	Administrator	All features accessible	✓ Active	
□	Auditor	General access and auditing features	✓ Active	
□	User	General access	✓ Active	

Showing 1 to 3 of 3 25

To create a custom role, click on **Create Custom Role**. In this GUI, enter the following details:



Windows Privilege Manager

Search Computers

Dashboard | Computers | Applications | Privileges | Users | 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*
Auditors

Role Description

Features

□ Select All Features

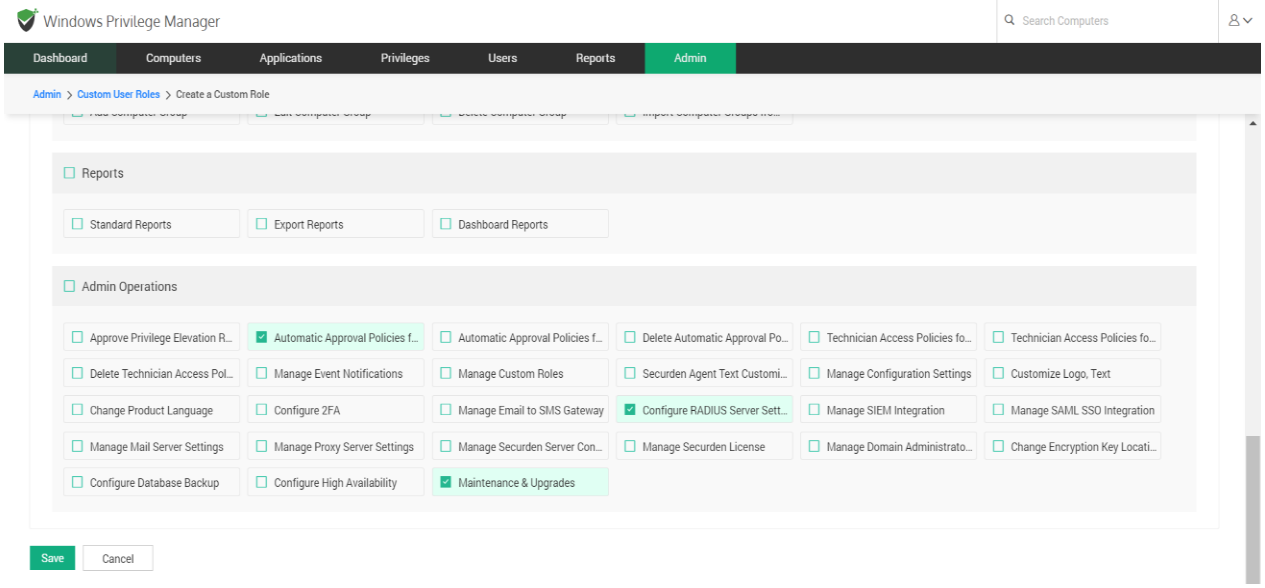
□ Privilege Management

☑ Admin Privilege Request
□ Add Applications, Commands...
□ Configure Privilege Elevation ...
□ Remove Admin Rights

□ User Management

□ Add User
□ Edit User
□ Import Users from File
□ Delete Users
□ Import Users from AD
□ Import Users from Azure AD
□ Concurrent Logins
□ User Reports
□ Configure temporary Access
□ Change User role
□ Control Application Control
□ Change 2FA

- **Role Name:** Name of the newly created role. This will be displayed in all the role-related fields and drop-down menus in the GUI.
- **Role Description:** A short brief of the role.
- **Features:** You can select the features listed in checkboxes. Any user assigned to this role will be able to access/perform these features/activities.



Windows Privilege Manager

Search Computers

Dashboard | Computers | Applications | Privileges | Users | Reports | Admin

Admin > Custom User Roles > Create a Custom Role

□ Reports

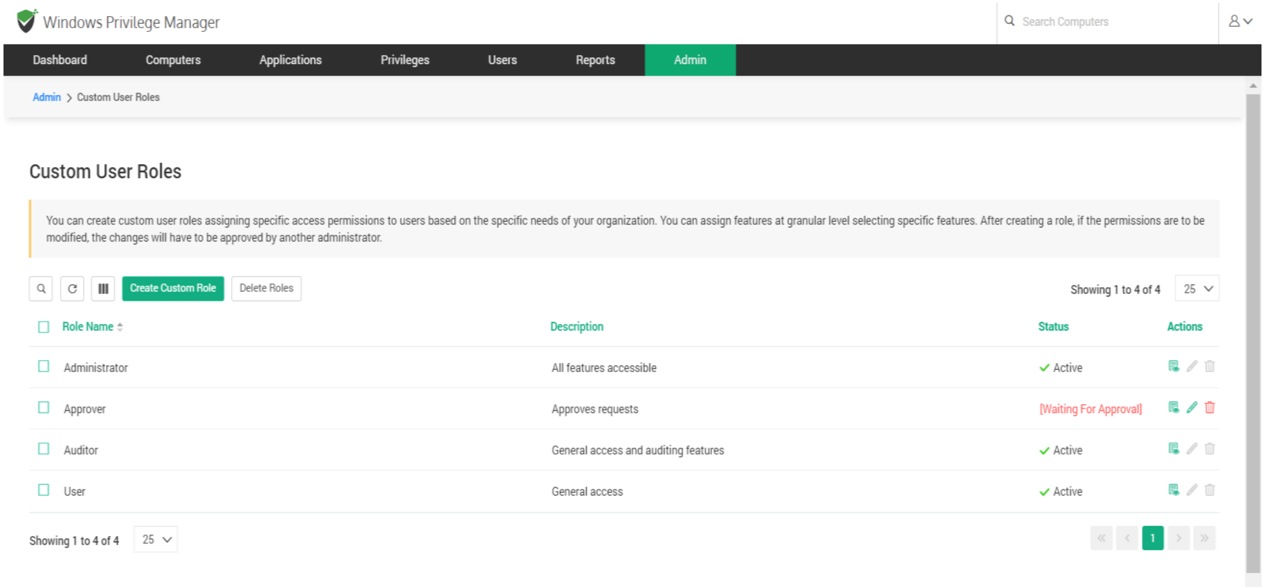
□ Standard Reports
□ Export Reports
□ Dashboard Reports

□ Admin Operations

□ Approve Privilege Elevation R...
☑ Automatic Approval Policies f...
□ Automatic Approval Policies f...
□ Delete Automatic Approval Po...
□ Technician Access Policies fo...
□ Technician Access Policies fo...
□ Delete Technician Access Pol...
□ Manage Event Notifications
□ Manage Custom Roles
□ Securden Agent Text Customi...
□ Manage Configuration Settings
□ Customize Logo, Text
□ Change Product Language
□ Configure 2FA
□ Manage Email to SMS Gateway
☑ Configure RADIUS Server Sett...
□ Manage SIEM Integration
□ Manage SAML SSO Integration
□ Manage Mail Server Settings
□ Manage Proxy Server Settings
□ Manage Securden Server Con...
□ Manage Securden License
□ Manage Domain Administrato...
□ Change Encryption Key Locati...
□ Configure Database Backup
□ Configure High Availability
☑ Maintenance & Upgrades

Save | Cancel

Once you have selected the required features. Click on the **Save** button to complete role creation. The newly created role will be visible on the custom user roles list.



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.

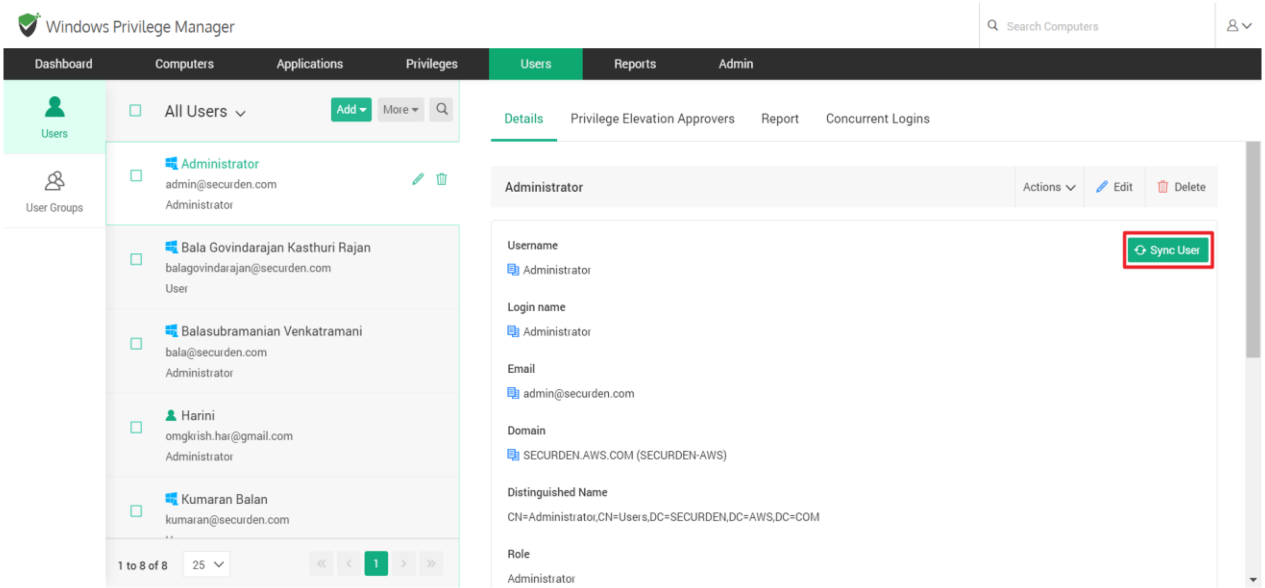
Role Name	Description	Status	Actions
Administrator	All features accessible	✓ Active	
Approver	Approves requests	[Waiting For Approval]	
Auditor	General access and auditing features	✓ Active	
User	General access	✓ Active	

Showing 1 to 4 of 4 25

Note: After creation, custom user roles have to be approved by another administrator. You can assign a custom role to users once they have been approved.

User Details

In the **Details** section, you can find the Username, Login Name, Email, and other user information. You can select the **Sync User** option to synchronize user details in WPM with corresponding user details in AD or Azure AD and keep them up to date.



Administrator	admin@securden.com	Administrator
Bala Govindarajan Kasthuri Rajan	balagovindarajan@securden.com	User
Balasubramanian Venkatramani	bala@securden.com	Administrator
Harini	omgkrish.har@gmail.com	Administrator
Kumaran Balan	kumaran@securden.com	

Administrator

Username: Administrator

Login name: Administrator

Email: admin@securden.com

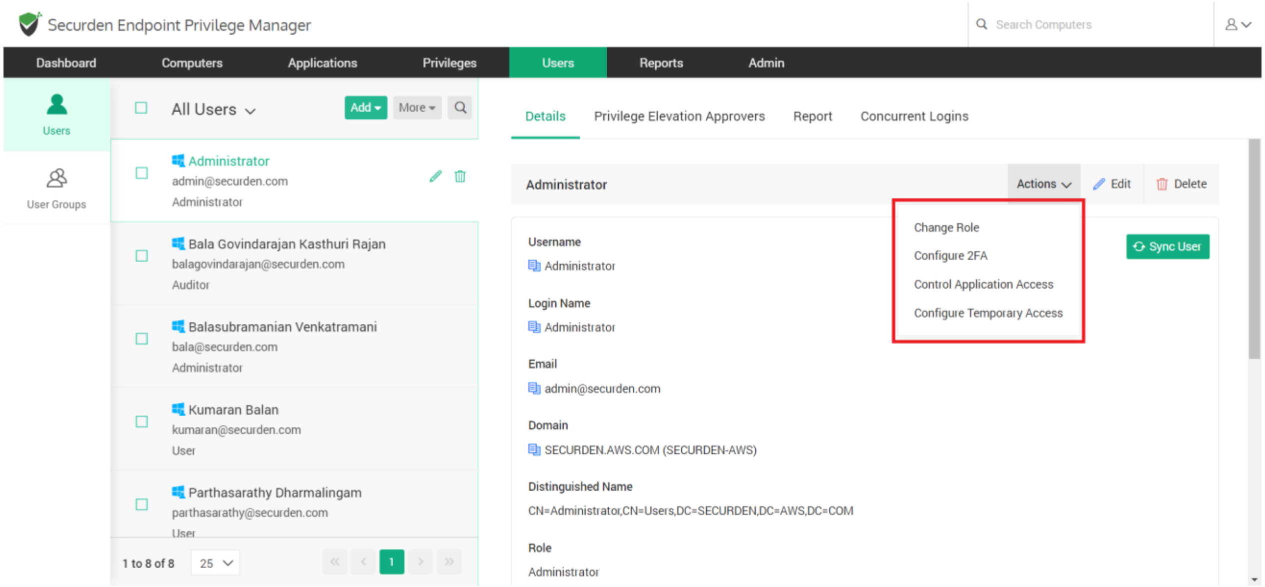
Domain: SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name: CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

Role: Administrator

Actions

Under Actions, you can find user settings such as **Change Role**, **Enable or Disable 2FA**, **Control Application Access**, and **Configure Temporary Access**. These settings are discussed in detail below.



Administrator	admin@securden.com	Administrator
Bala Govindarajan Kasthuri Rajan	balagovindarajan@securden.com	Auditor
Balasubramanian Venkatramani	bala@securden.com	Administrator
Kumaran Balan	kumaran@securden.com	User
Parthasarathy Dharmalingam	parthasarathy@securden.com	User

Administrator

Username: Administrator

Login Name: Administrator

Email: admin@securden.com

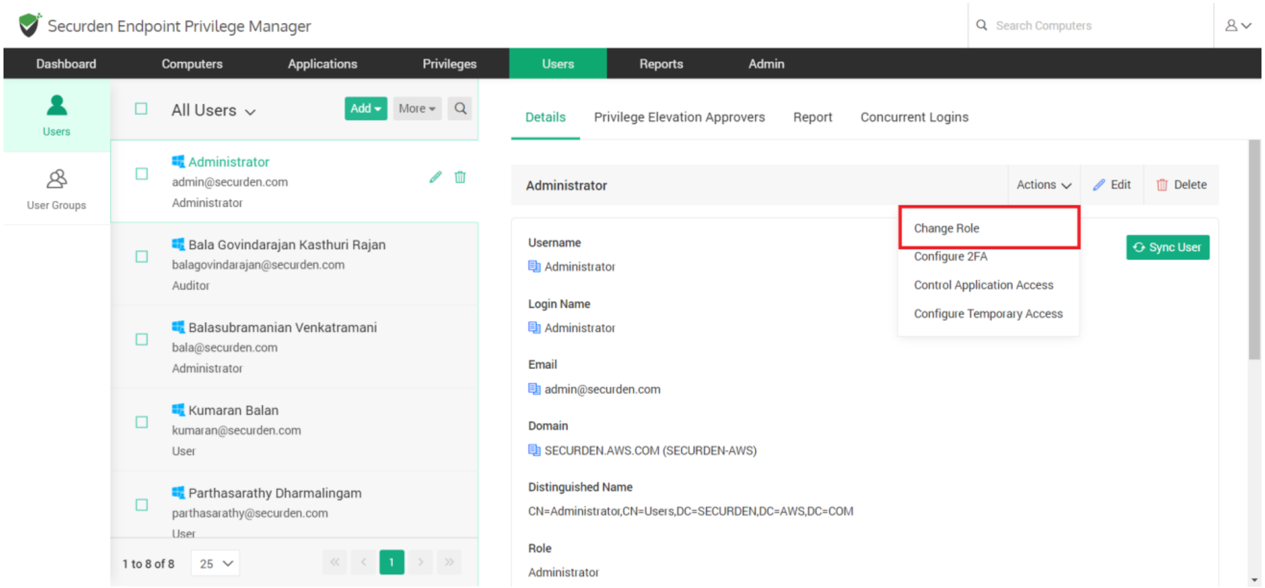
Domain: SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name: CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

Role: Administrator

Change Role

You can change the role of the selected user(s) from here.



Administrator
admin@securden.com
Administrator

Bala Govindarajan Kasthuri Rajan
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Administrator

Username
Administrator

Login Name
Administrator

Email
admin@securden.com

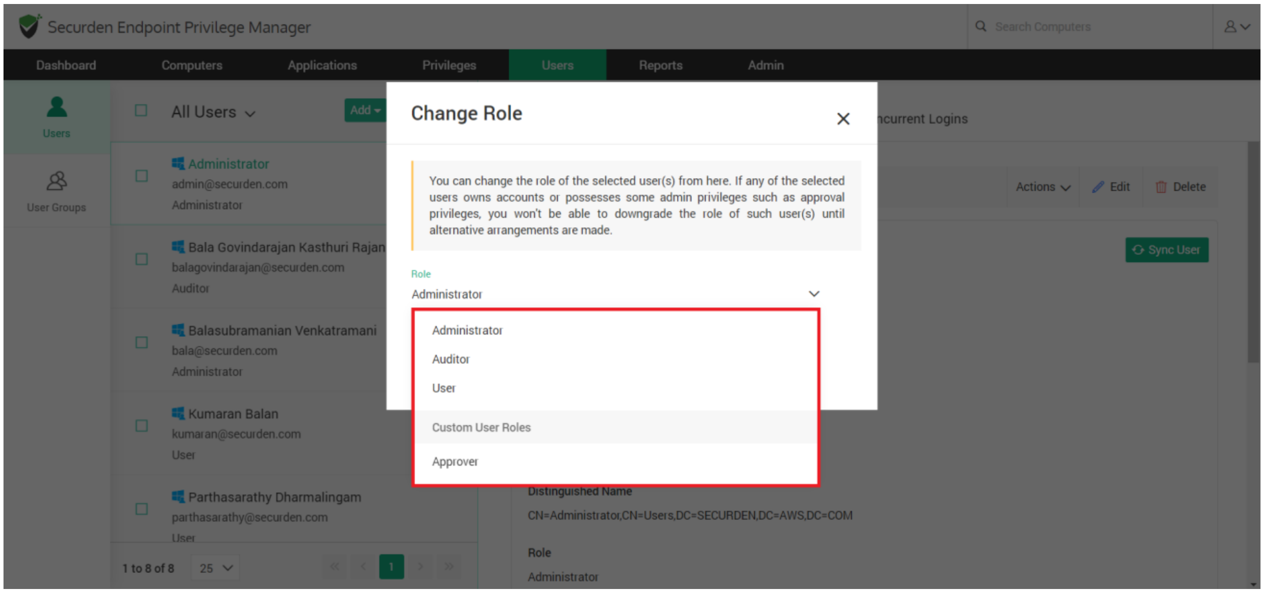
Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

Role
Administrator

If any of the selected users possess administrator level privileges such as approval privileges, you won't be able to downgrade the role of such user(s) until alternative arrangements are made.

You can choose the role from the drop-down that appears and select **Save**.



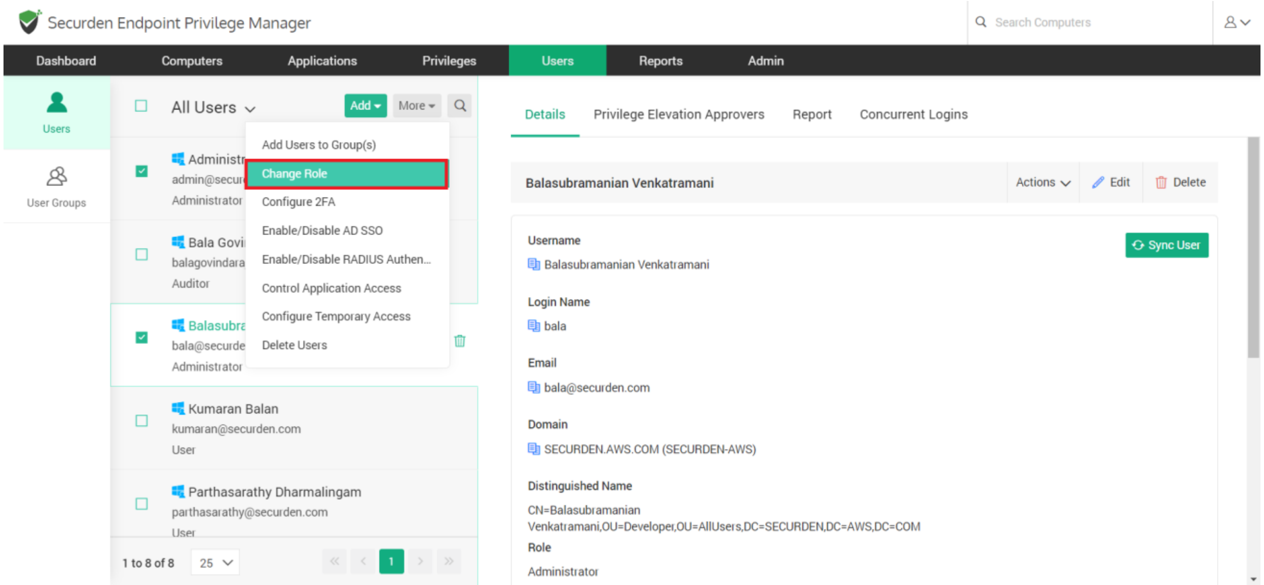
You can change the role of the selected user(s) from here. If any of the selected users owns accounts or possesses some admin privileges such as approval privileges, you won't be able to downgrade the role of such user(s) until alternative arrangements are made.

Role
Administrator

Distinguished Name
CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

Role
Administrator

To change roles of multiple users, you need to navigate to the **Users** tab, select the required users and then go to **More >> Change Role**.



Username
Balasubramanian Venkatramani

Login Name
bala

Email
bala@securden.com

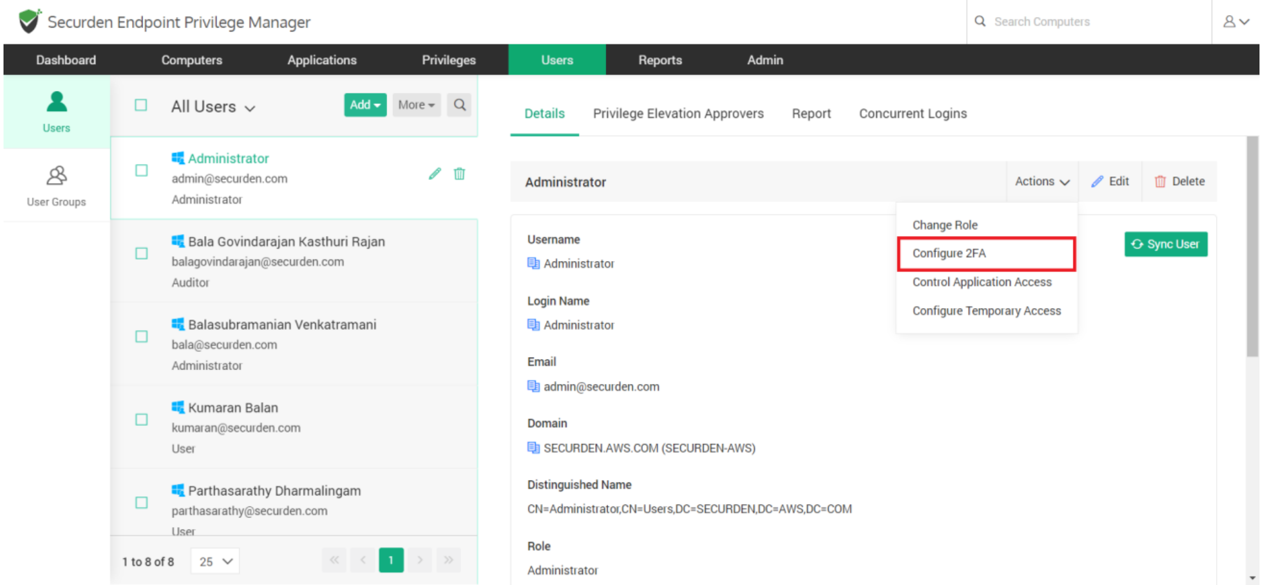
Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Balasubramanian Venkatramani,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM

Role
Administrator

Enable/Disable 2FA

Note: If you have not configured 2FA under **Admin >> Authentication >> Two Factor Authentication**, you can simply select the **Configure** button that appears and enable 2FA for the server.



Administrator
admin@securden.com
Administrator

Bala Govindarajan Kasthuri Rajan
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Administrator

Username: Administrator

Login Name: Administrator

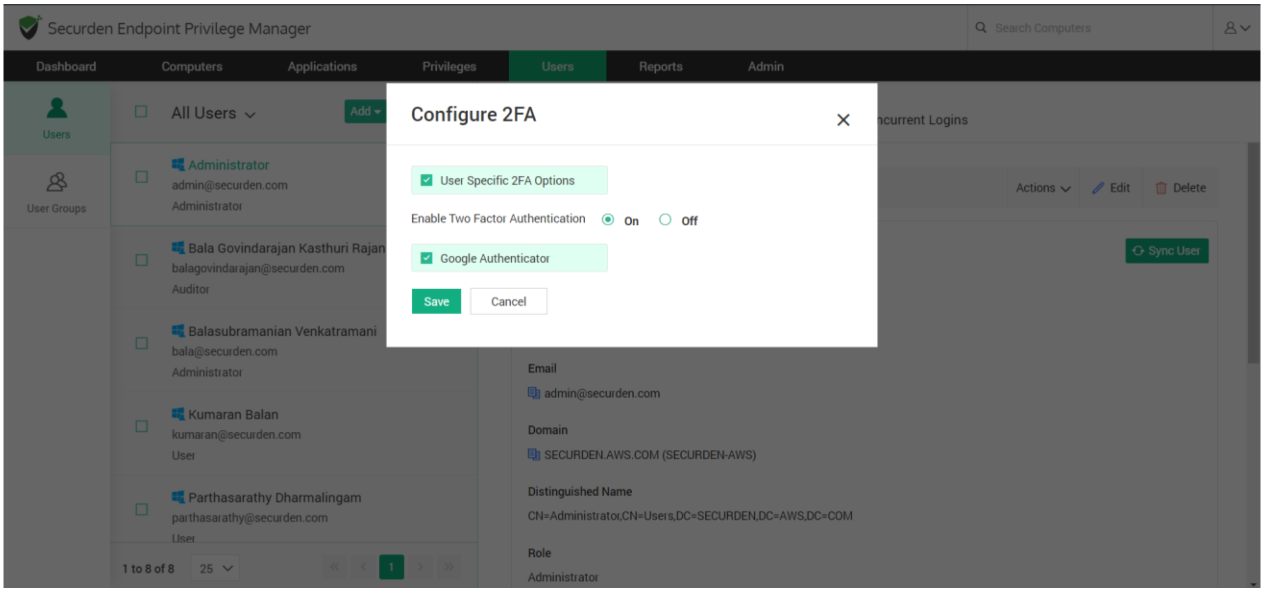
Email: admin@securden.com

Domain: SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name: CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

Role: Administrator

Navigate to **Users >> Details >> Actions >> Configure 2FA.**



Configure 2FA

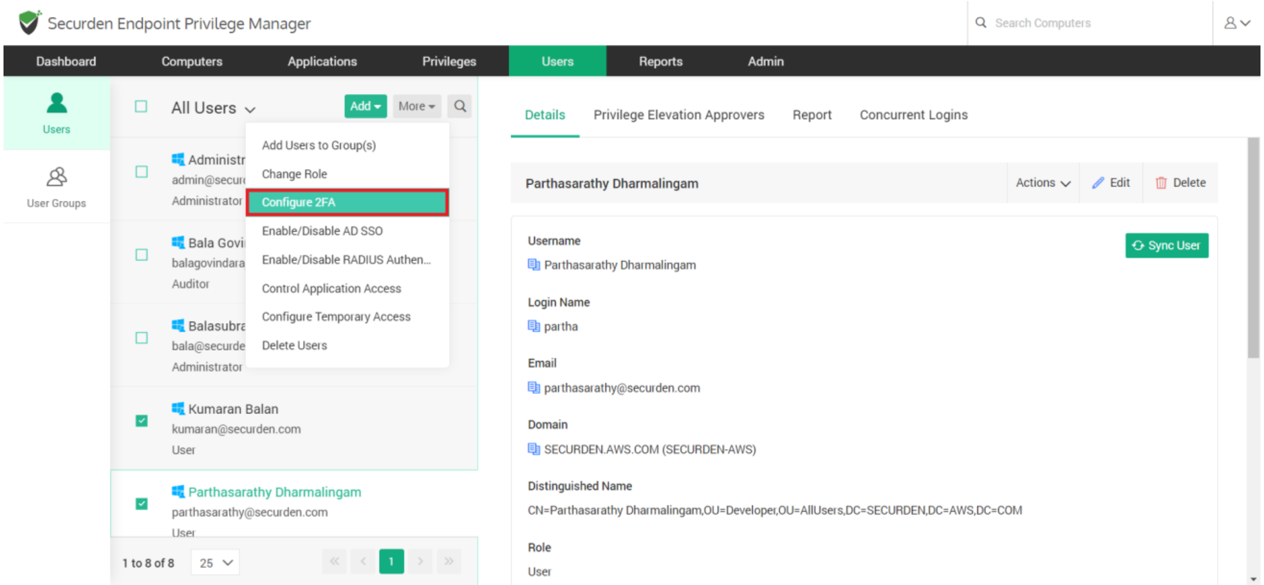
☑ User Specific 2FA Options

Enable Two Factor Authentication ● On ○ Off

☑ Google Authenticator

You need to select the checkbox named **User specific 2FA options** and then enable two factor authentication for the selected user. Then you need to select all the allowed 2FA options for this user.

If you want to enable or disable 2FA for multiple users at the same time, you can do so by selecting the required users and then navigating to **Users >> More >> Enable/Disable 2FA**. The steps are similar as above.



Username
Parthasarathy Dharmalingam

Login Name
partha

Email
parthasarathy@securden.com

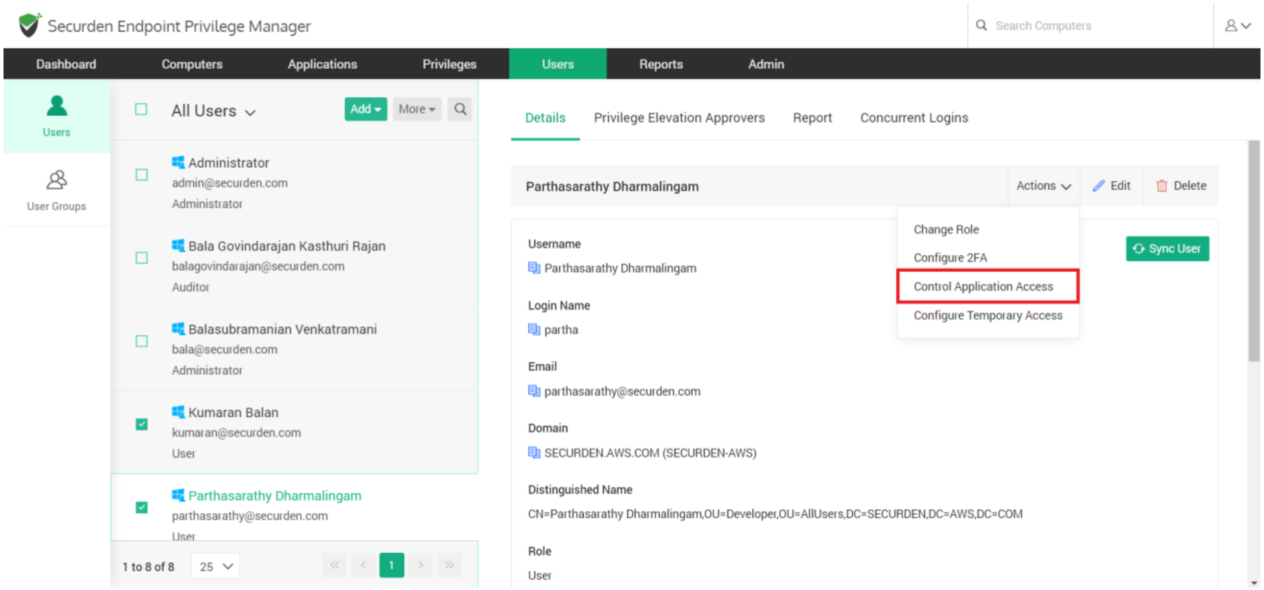
Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Parthasarathy Dharmalingam,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM

Role
User

Control Application Access

Using this feature, you can either allow or deny access to the interface for specific users.



Administrator
admin@securden.com
Administrator

Bala Govindarajan Kasthuri Rajan
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

☑ Kumaran Balan
kumaran@securden.com
User

☑ Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Parthasarathy Dharmalingam

Username
Parthasarathy Dharmalingam

Login Name
partha

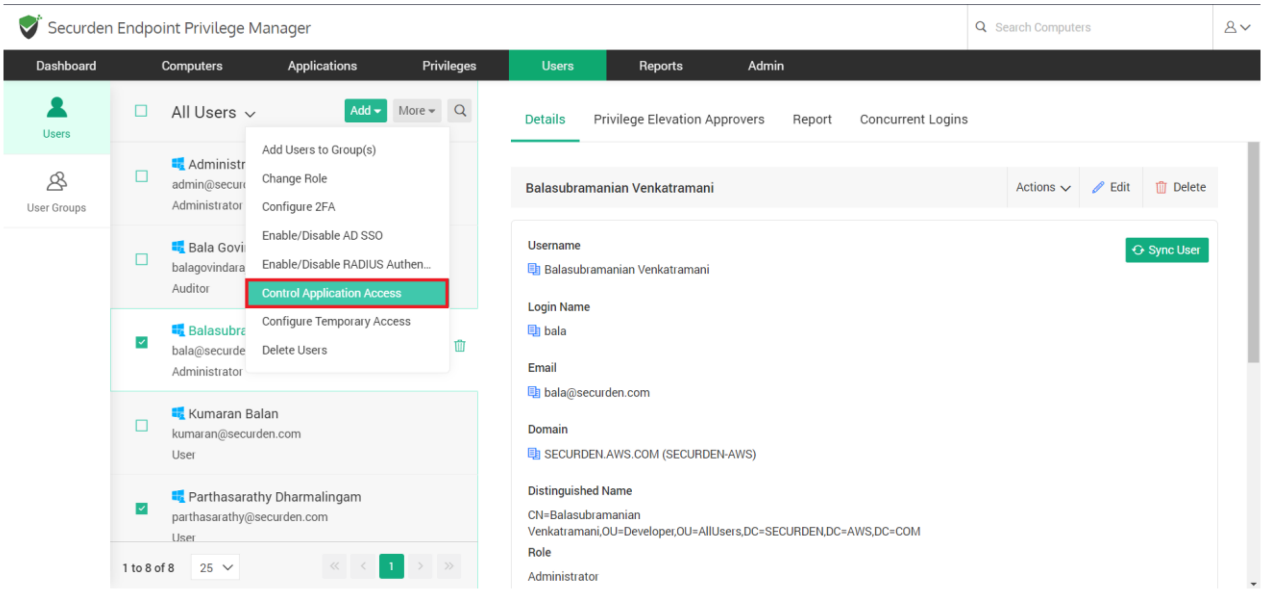
Email
parthasarathy@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Parthasarathy Dharmalingam,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM

Role
User

If you want to allow or deny access to multiple users at the same time, you can do so by selecting the required users and then navigating to **Users >> More >> Control Application Access** as shown below.



Administr
admin@secur
Administrator

Bala Govi
balagovindara
Auditor

☑ Balasubra
bala@securde
Administrator

Kumaran Balan
kumaran@securden.com
User

☑ Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Balasubramanian Venkatramani

Username
Balasubramanian Venkatramani

Login Name
bala

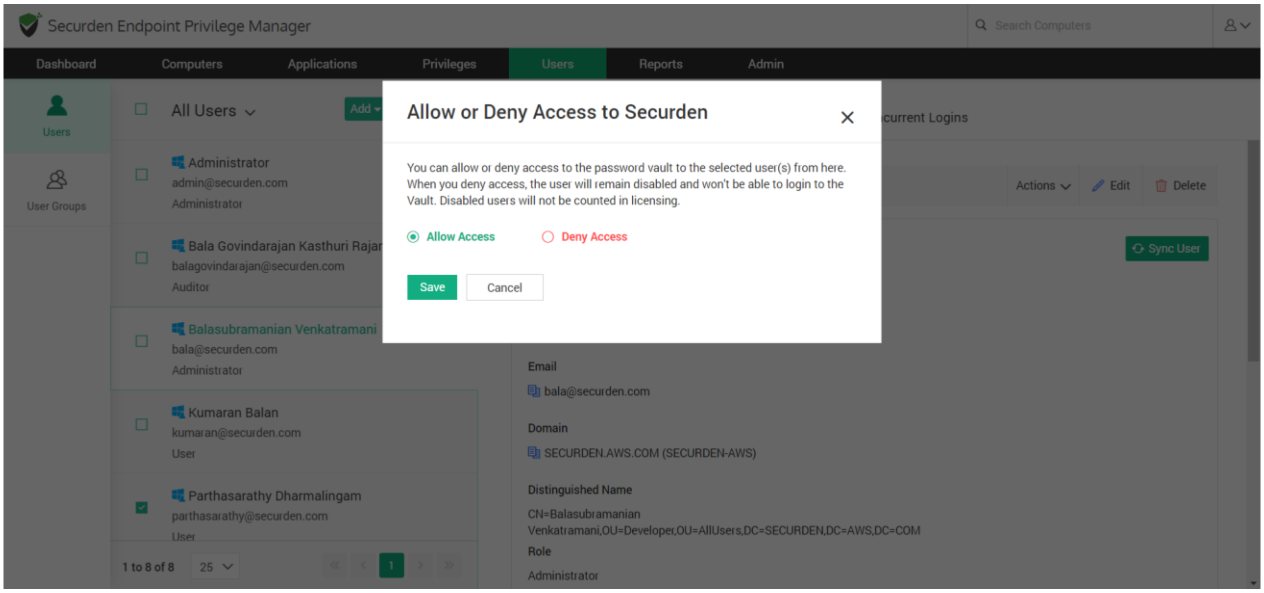
Email
bala@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Balasubramanian Venkatramani,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM

Role
Administrator

Click on **Allow Access** or **Deny Access** and then click **Save**.



Allow or Deny Access to Securden

You can allow or deny access to the password vault to the selected user(s) from here. When you deny access, the user will remain disabled and won't be able to login to the Vault. Disabled users will not be counted in licensing.

● Allow Access ○ Deny Access

Save Cancel

Administrator
admin@securden.com
Administrator

Bala Govindarajan Kasthuri Rajan
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

☑ Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Email
bala@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Balasubramanian Venkatramani,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM

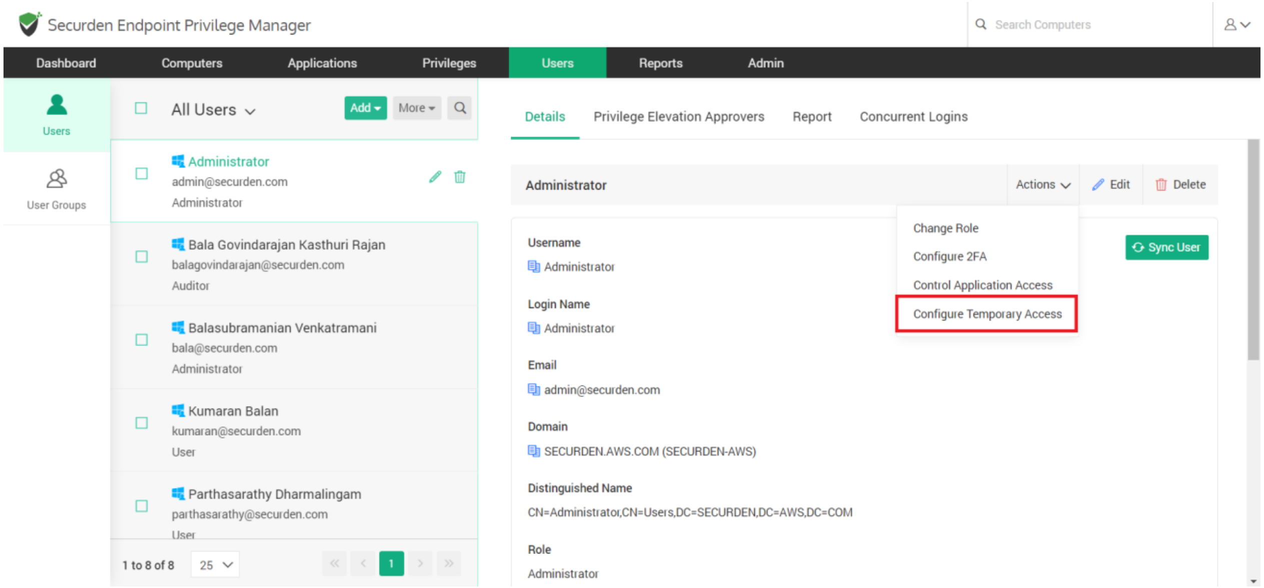
Role
Administrator

When you deny access, the user will remain disabled and won't be able to login into WPM.

Note: Disabled users will not be counted in licensing.

Configure Temporary Access

This feature allows you to grant temporary access to the users to access the Securden Web Interface. This feature comes in handy when you want to give access to third parties for a limited duration.



Administrator
admin@securden.com
Administrator

Bala Govindarajan Kasthuri Rajan
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Administrator

Username
Administrator

Login Name
Administrator

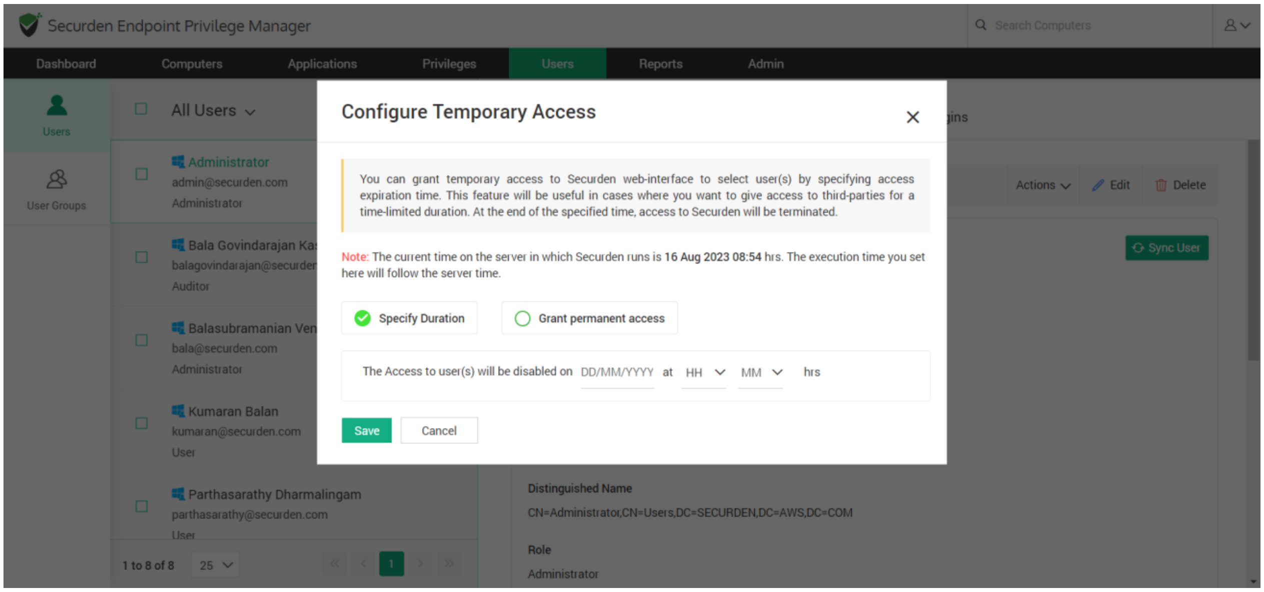
Email
admin@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

Role
Administrator

If you select **Specify Duration,** you will have to mention the date and time when the user access will be disabled.



Configure Temporary Access

You can grant temporary access to Securden web-interface to select user(s) by specifying access expiration time. This feature will be useful in cases where you want to give access to third-parties for a time-limited duration. At the end of the specified time, access to Securden will be terminated.

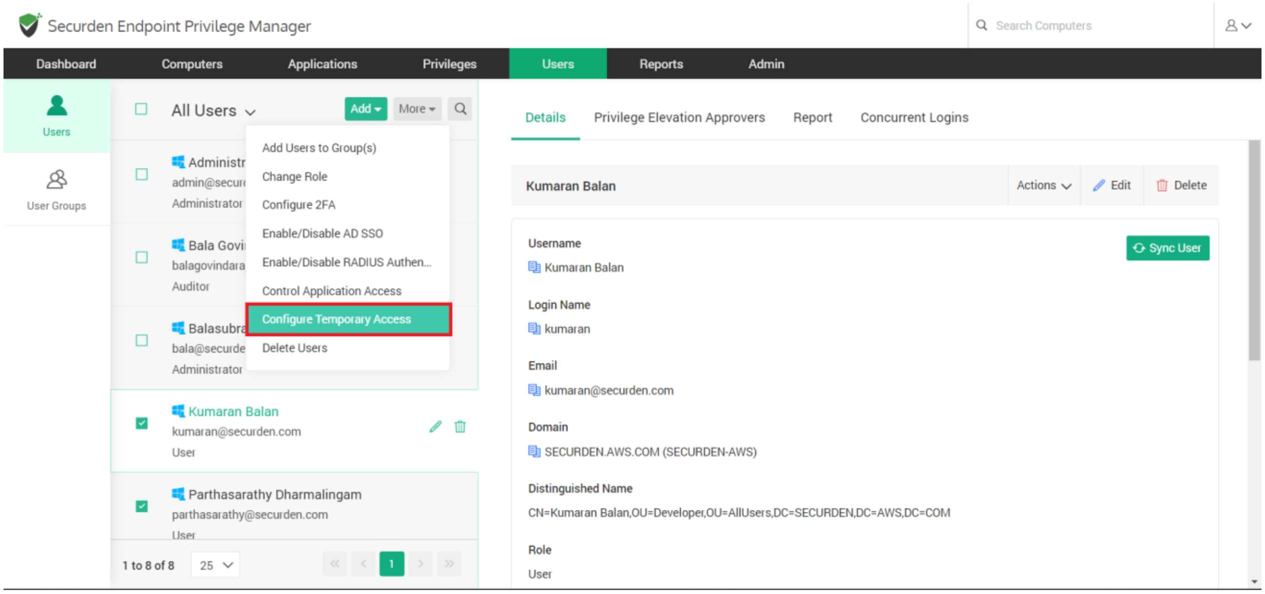
Note: The current time on the server in which Securden runs is **16 Aug 2023 08:54** hrs. The execution time you set here will follow the server time.

● Specify Duration ○ Grant permanent access

The Access to user(s) will be disabled on DD/MM/YYYY at HH MM hrs

If you select **Grant Permanent Access,** then the user will be able to access the Securden web interface anytime they want. After choosing between specific duration and permanent access, click **Save**.

You can also configure temporary access to multiple users at the same time. To do so, select the appropriate users and navigate to **Users >> More >> Configure Temporary Access**.



Administr
admin@secur
Administrator

Bala Govi
balagovindara
Auditor

Balasubra
bala@securde
Administrator

☑ Kumaran Balan
kumaran@securden.com
User

☑ Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Kumaran Balan

Username
Kumaran Balan

Login Name
kumaran

Email
kumaran@securden.com

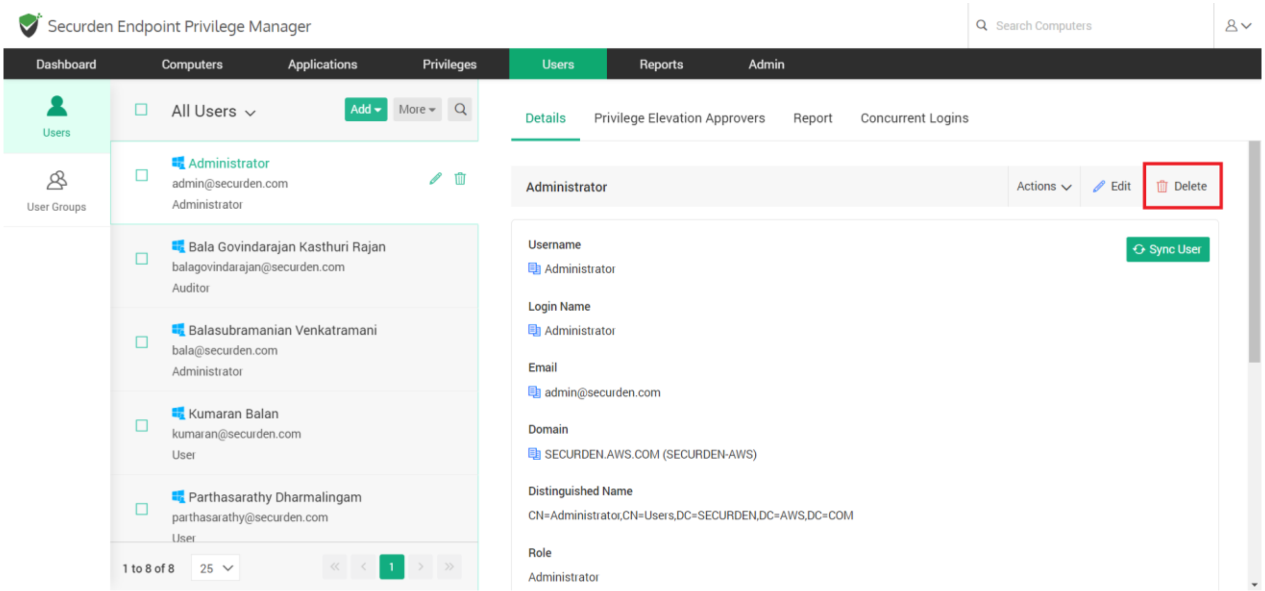
Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Kumaran Balan,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM

Role
User

Delete Users

If you need to remove a user from Securden, you can do so by selecting the **Delete** icon beside the user**.**



Administrator
admin@securden.com
Administrator

Bala Govindarajan Kasthuri Rajan
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Administrator

Username
Administrator

Login Name
Administrator

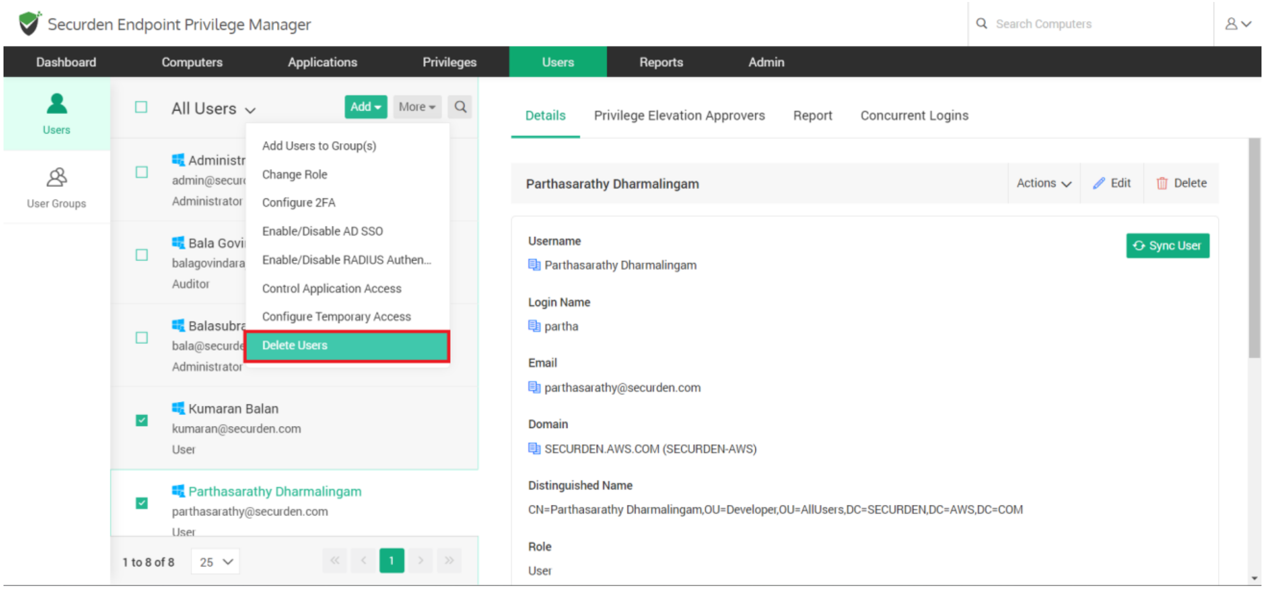
Email
admin@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

Role
Administrator

If you want to delete multiple users at the same time, you need to select the required users and navigate to **Users >> More >> Delete Users** and do so.



□ Administr
admin@secur
Administrator

□ Bala Govi
balagovindara
Auditor

□ Balasubra
bala@securd
Administrator

☑ Kumaran Balan
kumaran@securden.com
User

☑ Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Parthasarathy Dharmalingam

Username
Parthasarathy Dharmalingam

Login Name
partha

Email
parthasarathy@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

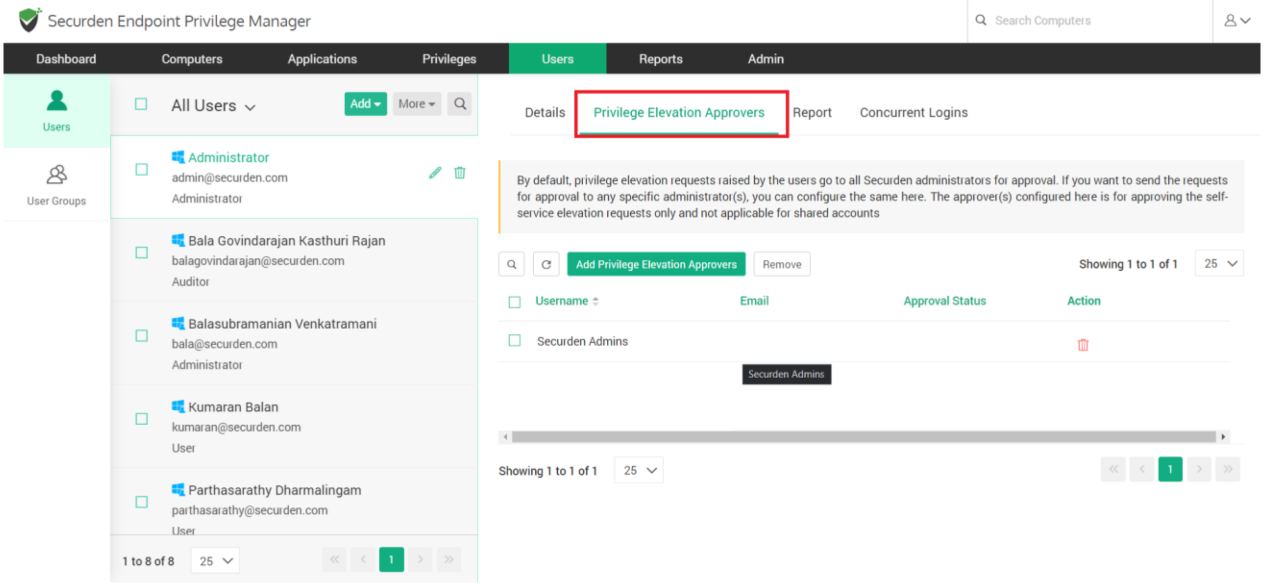
Distinguished Name
CN=Parthasarathy Dharmalingam,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM

Role
User

Privilege Elevation Approvers for Users

By default, privilege elevation requests raised by the users go to all Securden administrators for approval. If you want to send the requests for approval to any specific administrator(s), you can configure the same here.

Navigate to **Users >> Privilege Elevation Approvers** as shown below



Name	Email	Role
Administrator	admin@securden.com	Administrator
Bala Govindarajan Kasthuri Rajan	balagovindarajan@securden.com	Auditor
Balasubramanian Venkatramani	bala@securden.com	Administrator
Kumaran Balan	kumaran@securden.com	User
Parthasarathy Dharmalingam	parthasarathy@securden.com	User

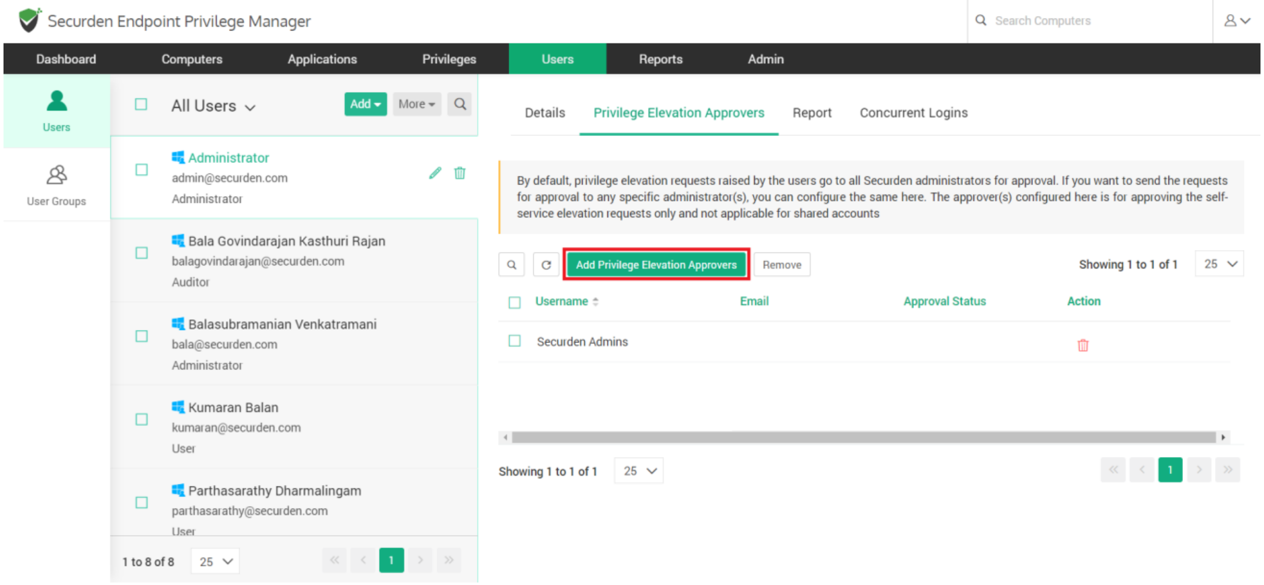
1 to 8 of 8

By default, privilege elevation requests raised by the users go to all Securden administrators for approval. If you want to send the requests for approval to any specific administrator(s), you can configure the same here. The approver(s) configured here is for approving the self-service elevation requests only and not applicable for shared accounts

Username	Email	Approval Status	Action
Securden Admins			🗑

Showing 1 to 1 of 1

To add an approver, click on **Add Privilege Elevation Approvers**. A list of all users with the ability to manage requests will be displayed.

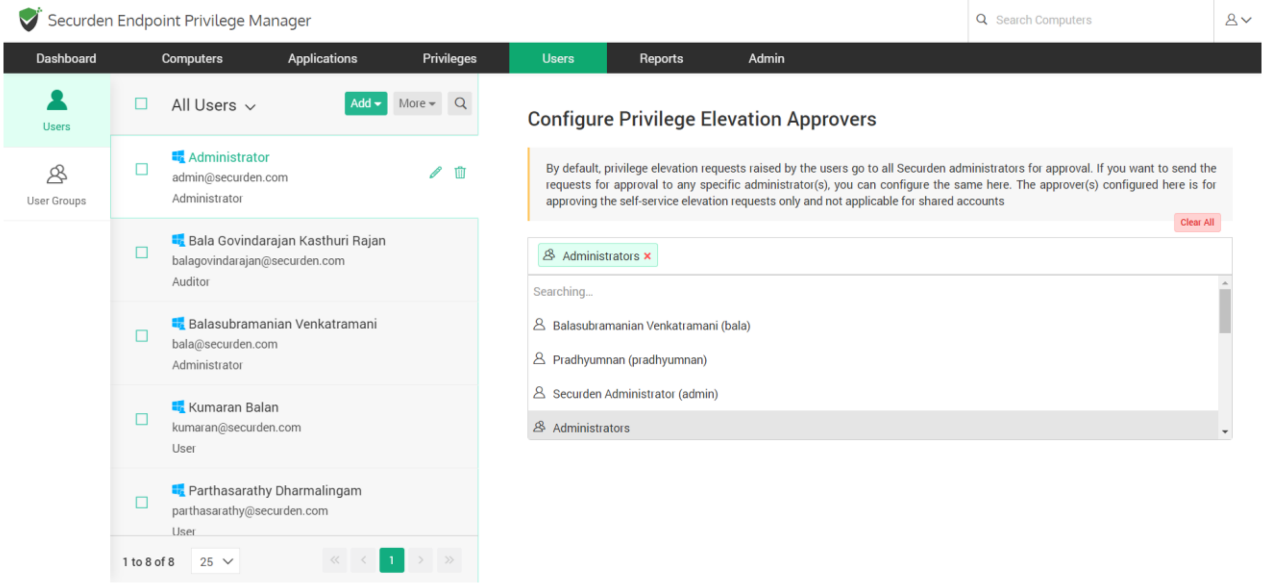


□	Name	Email	Role
□	Administrator	admin@securden.com	Administrator
□	Bala Govindarajan Kasthuri Rajan	balagovindarajan@securden.com	Auditor
□	Balasubramanian Venkatramani	bala@securden.com	Administrator
□	Kumaran Balan	kumaran@securden.com	User
□	Parthasarathy Dharmalingam	parthasarathy@securden.com	User

By default, privilege elevation requests raised by the users go to all Securden administrators for approval. If you want to send the requests for approval to any specific administrator(s), you can configure the same here. The approver(s) configured here is for approving the self-service elevation requests only and not applicable for shared accounts

□	Username	Email	Approval Status	Action
□	Securden Admins			🗑

From the drop down menu, choose the desired approver. This designated approver will be handling privilege elevation requests raised by the selected user.



□	Name	Email	Role
□	Administrator	admin@securden.com	Administrator
□	Bala Govindarajan Kasthuri Rajan	balagovindarajan@securden.com	Auditor
□	Balasubramanian Venkatramani	bala@securden.com	Administrator
□	Kumaran Balan	kumaran@securden.com	User
□	Parthasarathy Dharmalingam	parthasarathy@securden.com	User

Configure Privilege Elevation Approvers

By default, privilege elevation requests raised by the users go to all Securden administrators for approval. If you want to send the requests for approval to any specific administrator(s), you can configure the same here. The approver(s) configured here is for approving the self-service elevation requests only and not applicable for shared accounts

Administrators ×

Searching...

- Balasubramanian Venkatramani (bala)
- Pradhyumnan (pradhyumnan)
- Securden Administrator (admin)
- Administrators

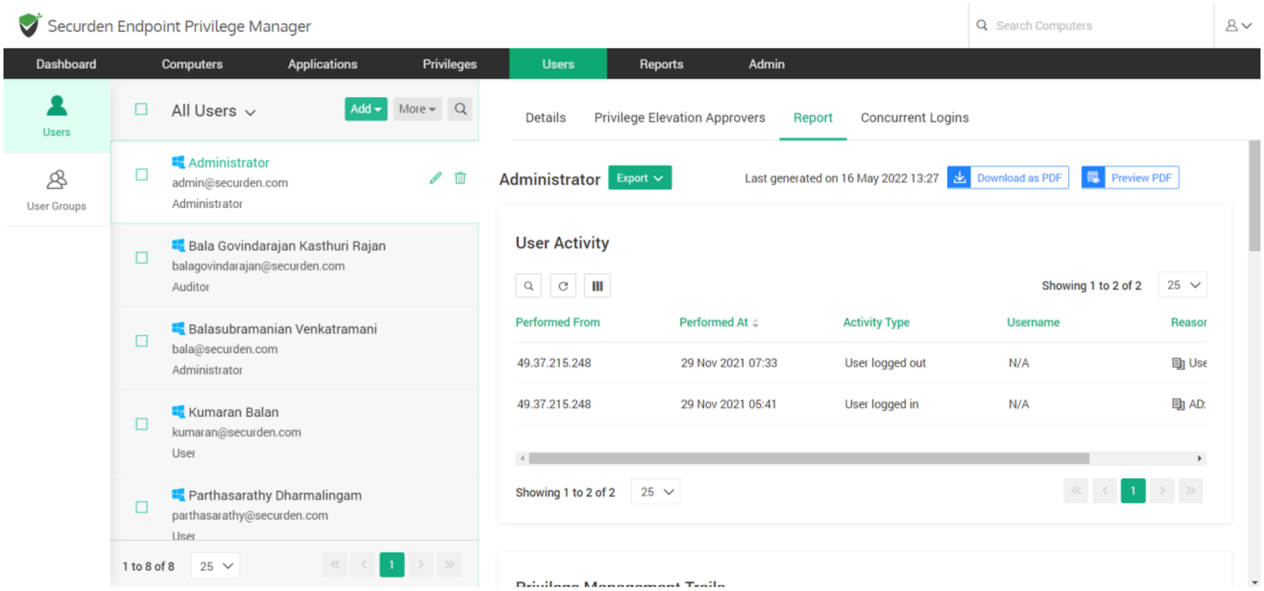
After designating the approver, click on **Save**.

Report

This tab shows reports on the activities of a specific user. This includes different types of activities such as user login, logout and so on. It also captures every privileged activity done by the user such as privilege elevation request raised, applications elevated, application control policies created, elevated applications revoked and so on. In addition, the report will also reveal if the user is part of any other groups such as domain admin, schema admin and so on.

The report can be exported in the form of PDF, CSV or XLSX formats by simply clicking the **Export** button.

You may make use of the search option based on the column headers to obtain drilled down data. You also have an option to customize the column headers as needed choosing only required columns you want to see in the report.



Administrator
admin@securden.com
Administrator

Bala Govindarajan Kasthuri Rajan
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

1 to 8 of 8 25

Administrator

Last generated on 16 May 2022 13:27

User Activity

Showing 1 to 2 of 2 25

Performed From	Performed At	Activity Type	Username	Reasor
49.37.215.248	29 Nov 2021 07:33	User logged out	N/A	Use
49.37.215.248	29 Nov 2021 05:41	User logged in	N/A	AD:

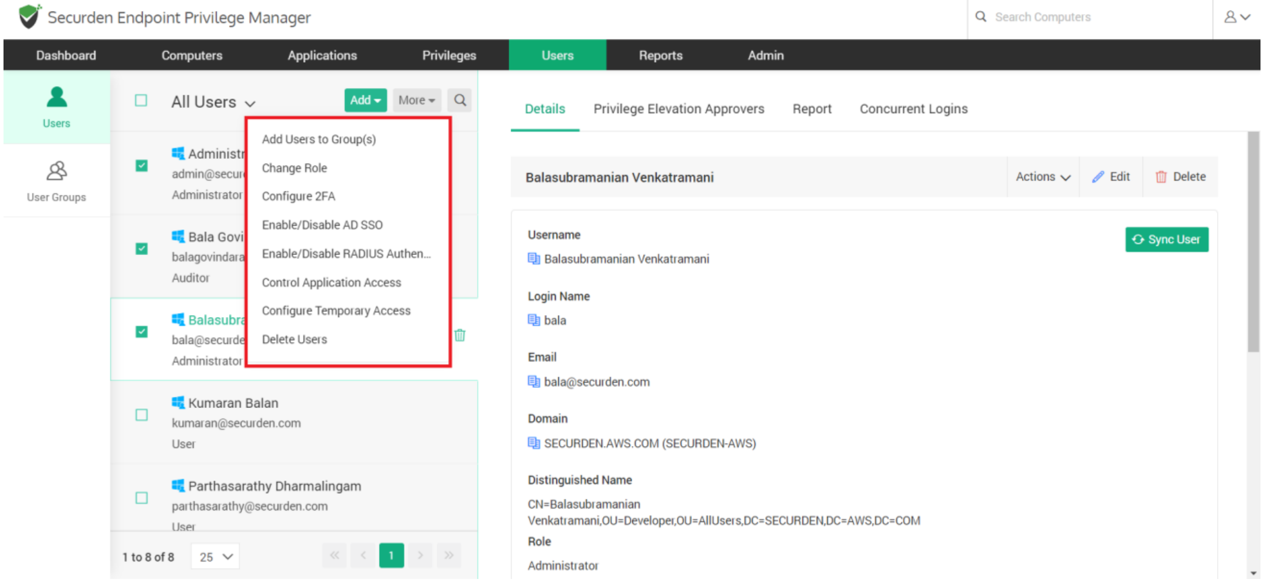
Showing 1 to 2 of 2 25

Privilege Management Trails

Additional Settings

You can exercise granular control over the users in Securden. From the **Users** tab, you can monitor the concurrent logins of each user separately. 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 logins. You can review and even terminate any or all the sessions, which will forcefully log out the user from Securden GUI.

In addition, from the **More** drop-down, you can exercise other controls such as selectively enabling/disabling 2FA, AD SSO, granting temporary access to Securden, temporarily disabling access, and even deleting users. These options are provided to help perform the above-mentioned functions for multiple users at the same time. You need to select the appropriate users and then navigate to the required section from **Users >> More**.



Username
Balasubramanian Venkatramani

Login Name
bala

Email
bala@securden.com

Domain
SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name
CN=Balasubramanian Venkatramani,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM

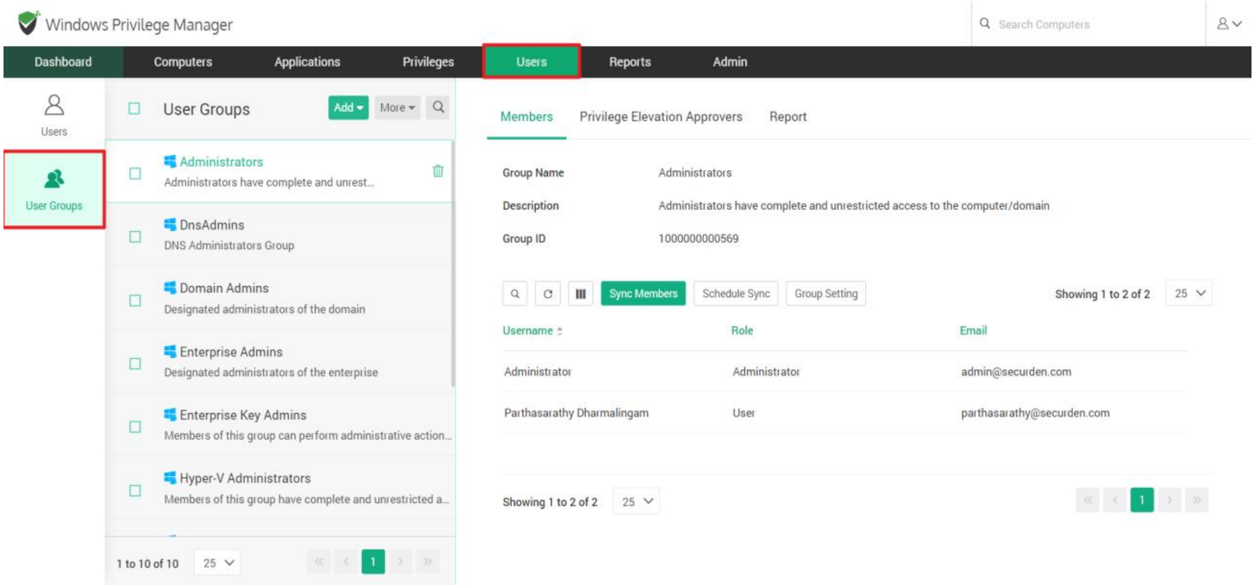
Role
Administrator

Groups

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

There are a couple of ways using which you can create user groups - you can either import groups directly from directories such as AD and Azure AD, or add them manually.

Navigate to **Users >> User Groups** in the GUI to perform this step.



Administrators
Administrators have complete and unrest...

DnsAdmins
DNS Administrators Group

Domain Admins
Designated administrators of the domain

Enterprise Admins
Designated administrators of the enterprise

Enterprise Key Admins
Members of this group can perform administrative action...

Hyper-V Administrators
Members of this group have complete and unrestricted a...

Group Name: Administrators
Description: Administrators have complete and unrestricted access to the computer/domain
Group ID: 1000000000569

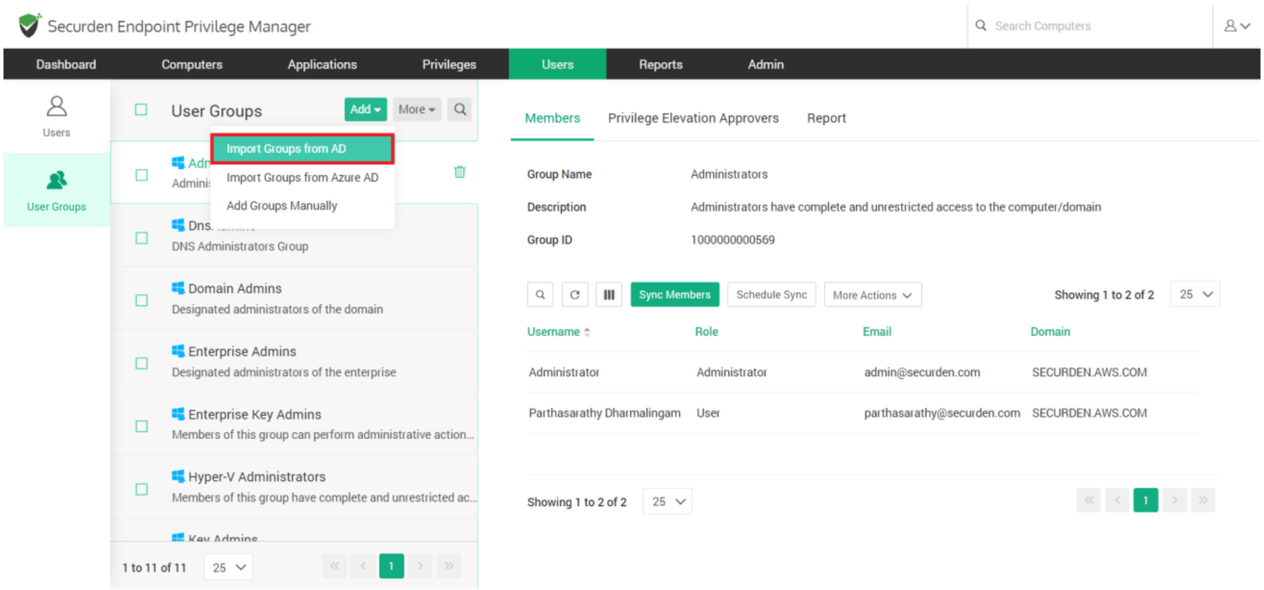
Username	Role	Email
Administrator	Administrator	admin@securden.com
Parthasarathy Dharmalingam	User	parthasarathy@securden.com

You can define various access permissions at the group level, when a new member joins the organization, by placing the member in the required group, the member can inherit the access permissions granted to that group automatically.

Import User Groups from AD

Securden scans your Active Directory domain and obtains the groups in the domain. You can discover a group of users and add them to Securden.

Navigate to **Users >> Import Groups from AD**.



Group Name Administrators

Description Administrators have complete and unrestricted access to the computer/domain

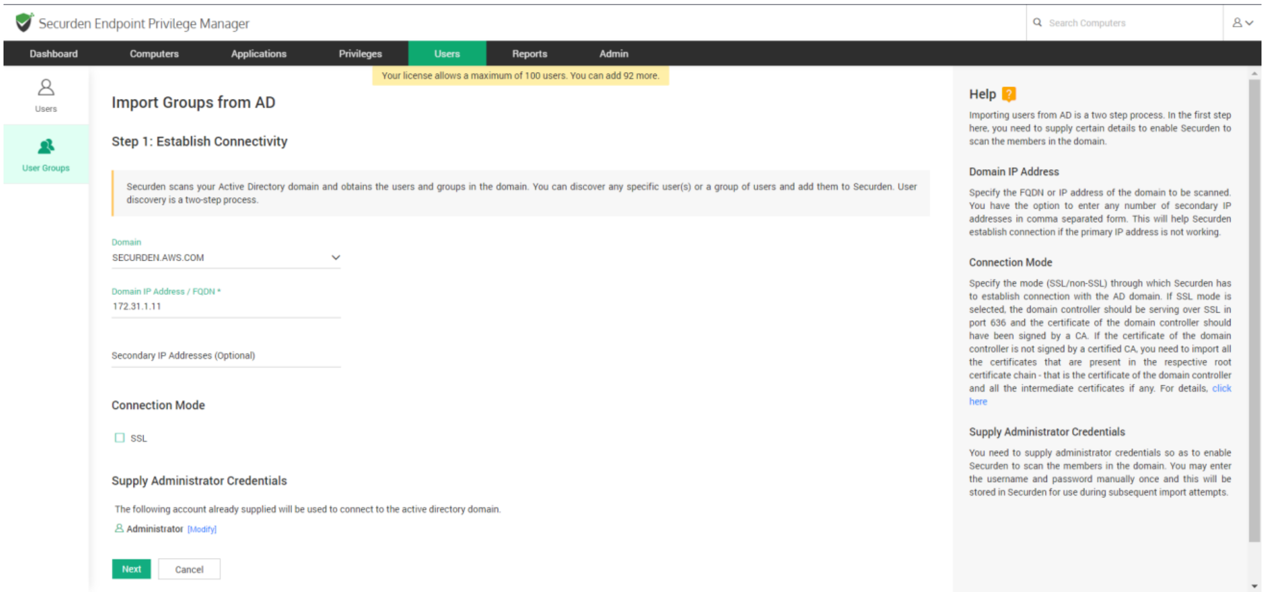
Group ID 1000000000569

Username	Role	Email	Domain
Administrator	Administrator	admin@securden.com	SECURDEN.AWS.COM
Parthasarathy Dharmalingam	User	parthasarathy@securden.com	SECURDEN.AWS.COM

User group discovery is a two-step process. The first step is to establish connection with the Active Directory domain and the second step is to scan and add the required groups into the Securden database.

Step 1: Establish Connectivity

This step requires you to provide certain details to allow securden to scan members in the AD domain.



Your license allows a maximum of 100 users. You can add 92 more.

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)

Connection Mode

□ SSL

Supply Administrator Credentials

The following account already supplied will be used to connect to the active directory domain.

Administrator [Modify]

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 stored in Securden for use during subsequent import attempts.

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 Google Chrome and navigate to **Settings >> Privacy and Security >> Manage Certificates.**
- In this GUI, click **Import**.
- Select Next and 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.

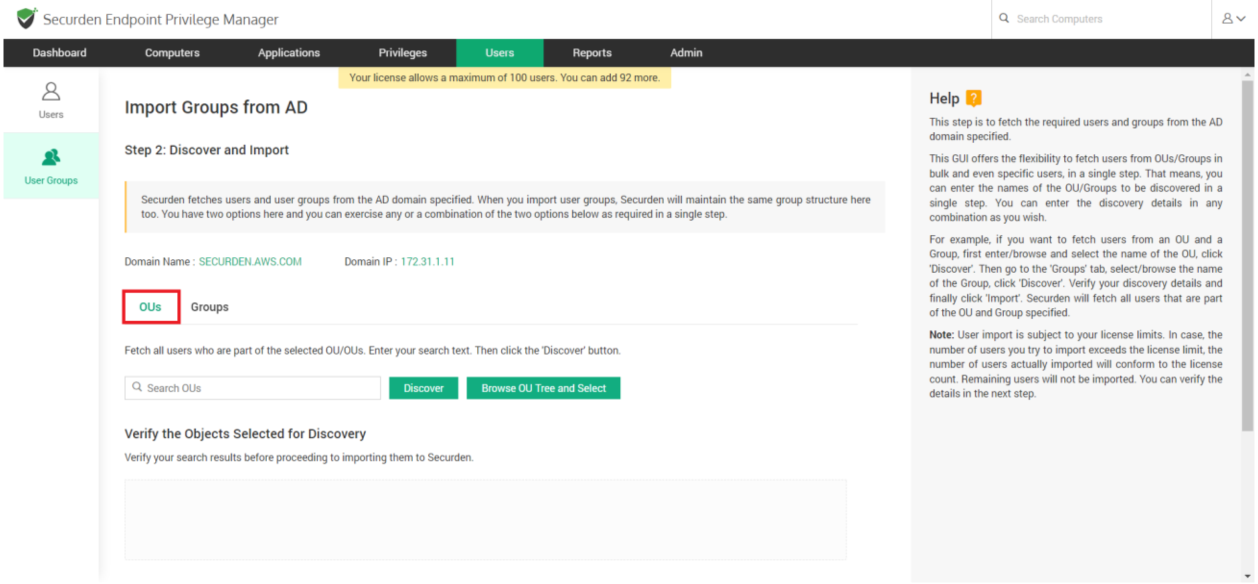
After entering all the details, click on the **Next** button.

Step 2: Import Groups

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

This GUI offers the flexibility to fetch user groups from OUs and Groups in bulk 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.

To import OUs, select the OU tab from OUs | Groups



Your license allows a maximum of 100 users. You can add 92 more.

Import Groups 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 two options here and you can exercise any or a combination of the two options below as required in a single step.

Domain Name : SECURDEN.AWS.COM

Domain IP : 172.31.1.11

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

Verify the Objects Selected for Discovery

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

Help

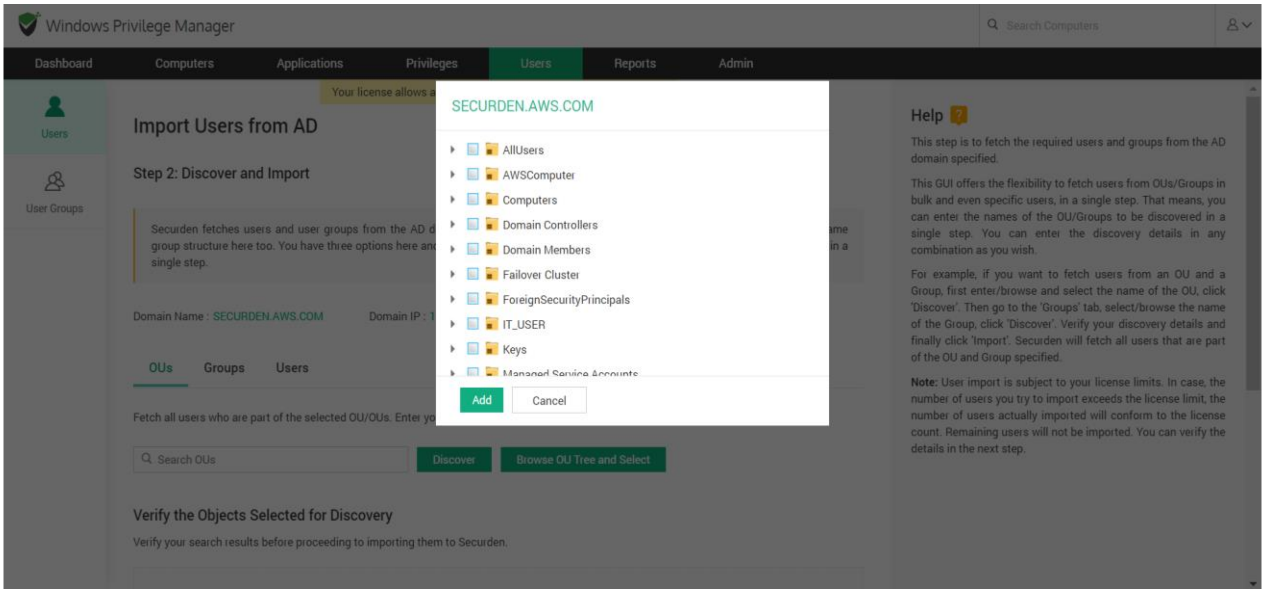
This step is to fetch the required users and groups from the AD domain specified.

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.

1. Enter the OU name in the search bar 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.**



Import Users from AD

Step 2: Discover and Import

Securden fetches users and user groups from the AD d… group structure here too. You have three options here an… single step.

Domain Name : SECURDEN.AWS.COM Domain IP : 1

Fetch all users who are part of the selected OU/OUs. Enter yo

Verify the Objects Selected for Discovery

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

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

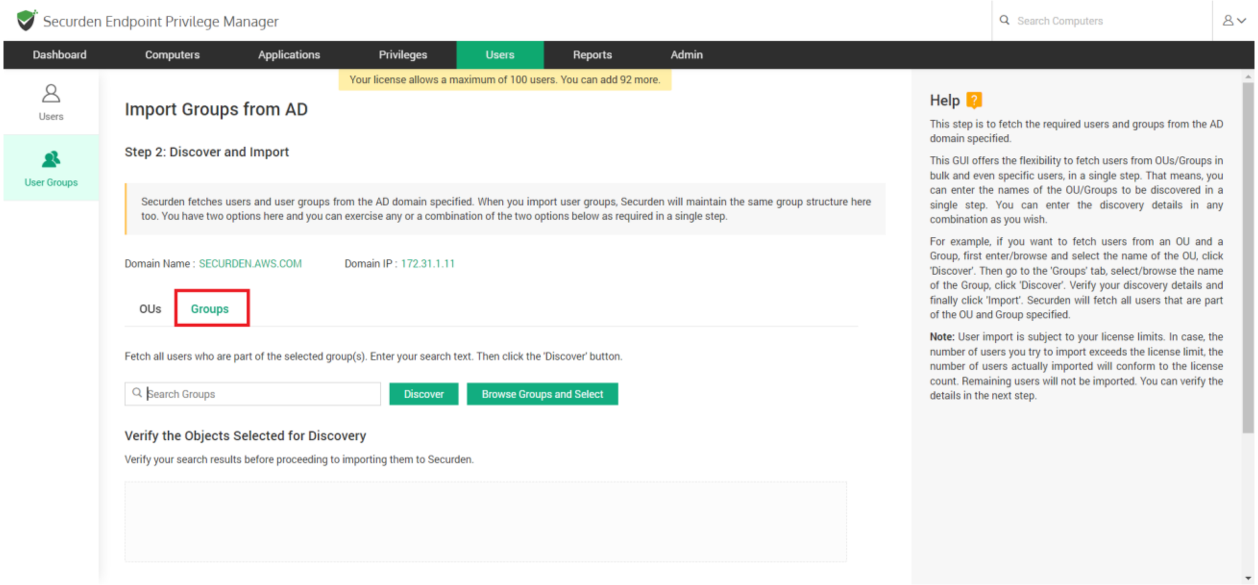
This GUI offers the flexibility to fetch users from OUs/Groups in bulk and even specific users, in a single step. That means, you can enter the names of the OU/Groups to be discovered in a single step. You can enter the discovery details in any combination as you wish.

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.

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

To import groups, select the **Groups** tab.



Your license allows a maximum of 100 users. You can add 92 more.

Import Groups 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 two options here and you can exercise any or a combination of the two options below as required in a single step.

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

Fetch all users who are part of the selected group(s). Enter your search text. Then click the 'Discover' button.

Verify the Objects Selected for Discovery

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

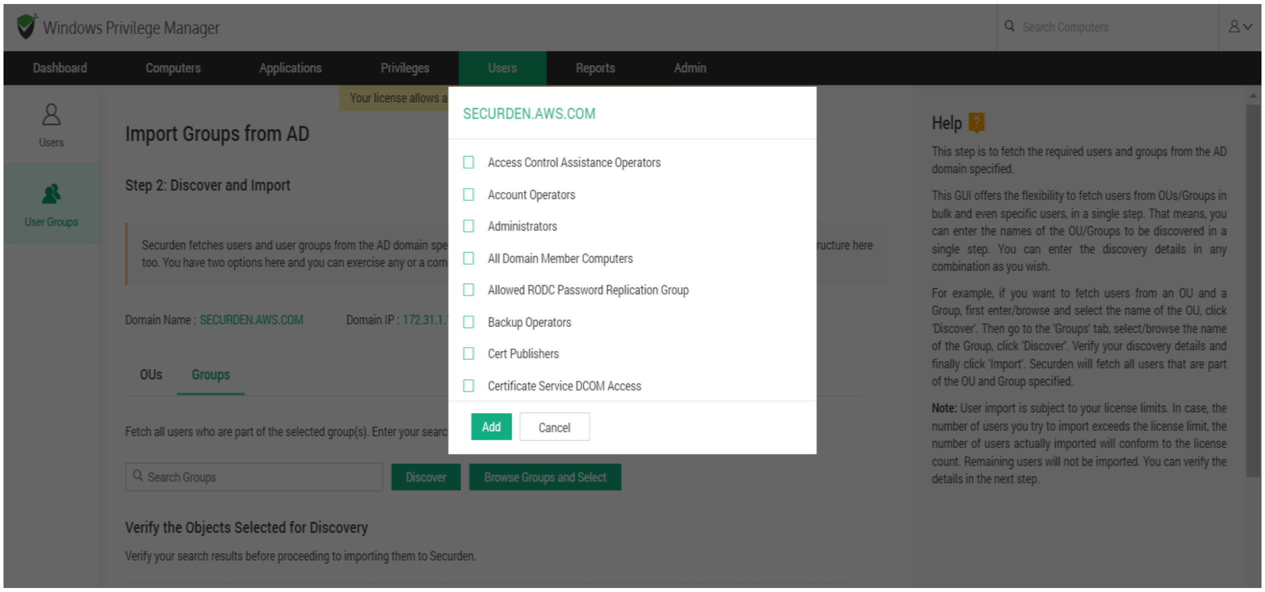
This step is to fetch the required users and groups from the AD domain specified.

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.

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



Your license allows a

Import Groups from AD

Step 2: Discover and Import

Securden fetches users and user groups from the AD domain spe ructure here too. You have two options here and you can exercise any or a com

Domain Name : SECURDEN.AWS.COM Domain IP : 172.31.1.

Fetch all users who are part of the selected group(s). Enter your searc

Verify the Objects Selected for Discovery

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

SECURDEN.AWS.COM

- □ Access Control Assistance Operators
- □ Account Operators
- □ Administrators
- □ All Domain Member Computers
- □ Allowed RODC Password Replication Group
- □ Backup Operators
- □ Cert Publishers
- □ Certificate Service DCOM Access

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.

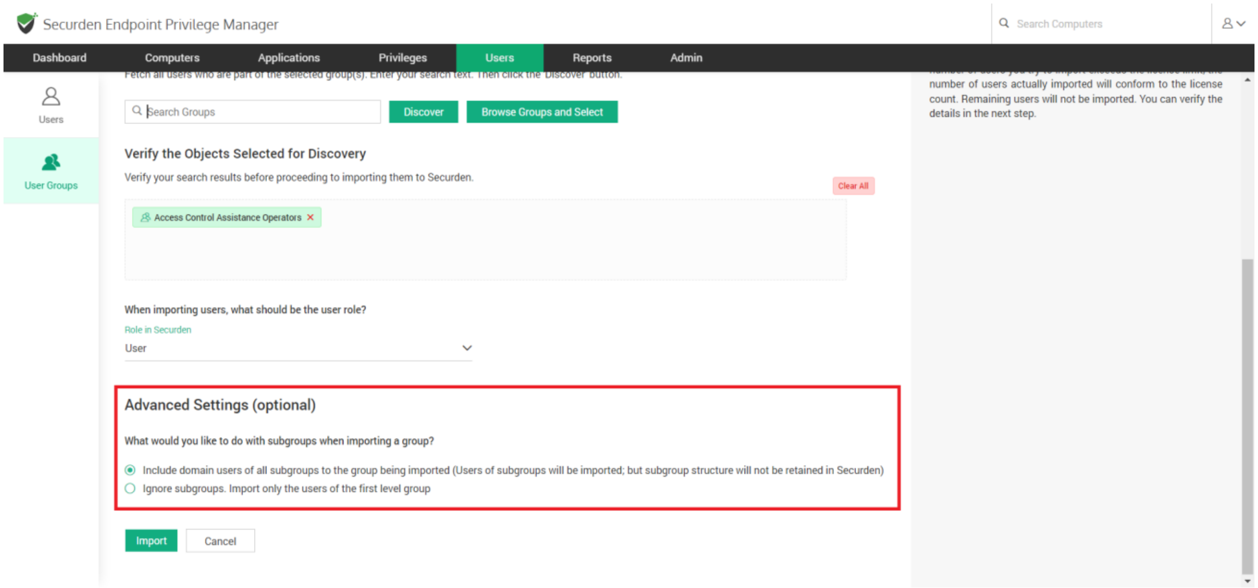
Note: User import is subject to your license limits. In case, the number of users you try to import exceeds the license limit, the number of users actually imported will conform to the license count. Remaining users will not be imported. You can verify the details in the next step.

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

You can select the role of the users in the group(s) imported using the **Role in Securden** dropdown. Before selecting import, you can look into the advanced settings which are explained below.

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.



Fetch all users who are part of the selected group(s). Enter your search text. Then click the 'Discover' button.

Verify the Objects Selected for Discovery

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

Access Control Assistance Operators ✕

When importing users, what should be the user role?

Role in Securden: User

Advanced Settings (optional)

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

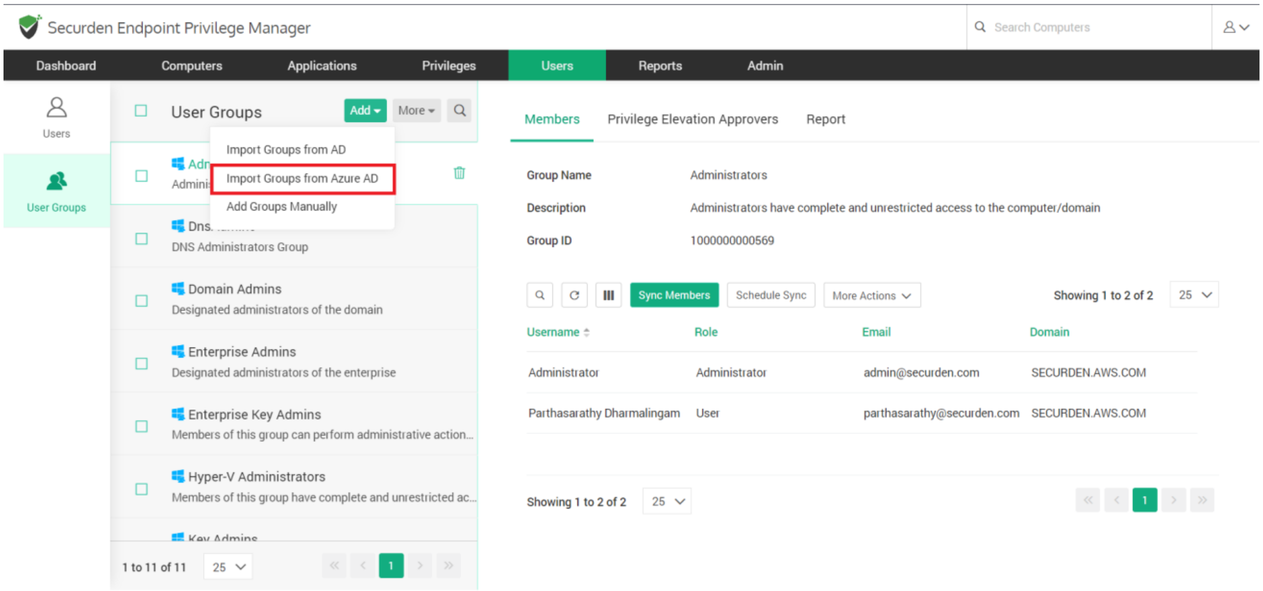
number of users actually imported will conform to the license count. Remaining users will not be imported. You can verify the details in the next step.

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 user groups actually imported will conform to the license count. The remaining user groups will not be imported. You can verify the details in the next step.

Import User Groups from Azure AD

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 (from **Admin >> General >> Proxy Server Settings**).

Securden allows you to import user groups from Azure AD. Navigate to **User Groups >> Add >> Import Groups from Azure AD**



Adr
Admini

Dns.
DNS Administrators Group

Domain Admins
Designated administrators of the domain

Enterprise Admins
Designated administrators of the enterprise

Enterprise Key Admins
Members of this group can perform administrative action...

Hyper-V Administrators
Members of this group have complete and unrestricted ac...

Key Admins

1 to 11 of 11 25

Group Name	Administrators
Description	Administrators have complete and unrestricted access to the computer/domain
Group ID	1000000000569

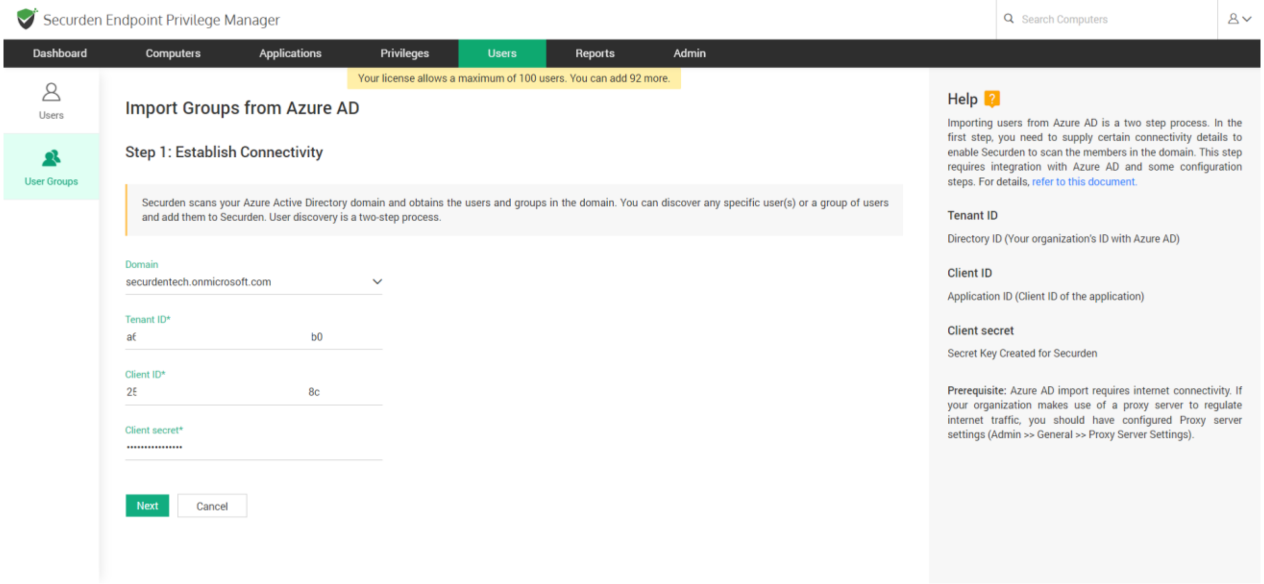
Showing 1 to 2 of 2 25

Username	Role	Email	Domain
Administrator	Administrator	admin@securden.com	SECURDEN.AWS.COM
Parthasarathy Dharmalingam	User	parthasarathy@securden.com	SECURDEN.AWS.COM

Showing 1 to 2 of 2 25

Step 1: Establish Connectivity

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. In the GUI, you need the following fields:



Your license allows a maximum of 100 users. You can add 92 more.

Import Groups 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.

Domain
securdentech.onmicrosoft.com

Tenant ID*
a6 b0

Client ID*
25 8c

Client secret*
••••••••••••••••

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).

Tenant ID: Enter the directory ID i.e., your organization's ID with Azure AD.

Client ID: Enter the Client ID of the application.

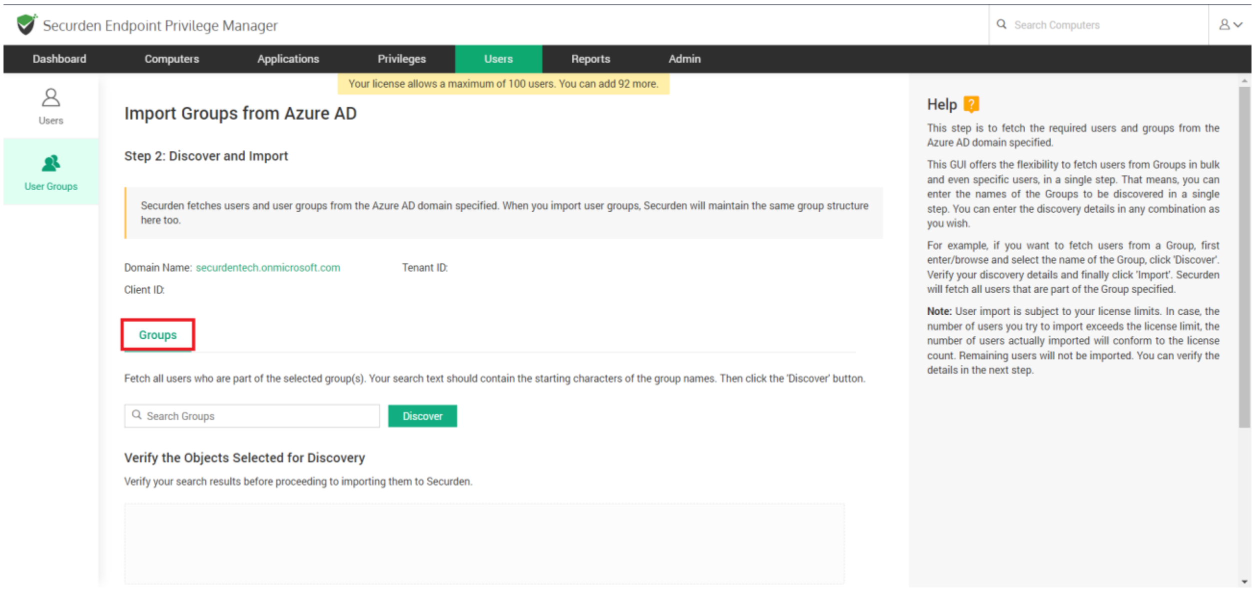
Client secret: This is the secret key created for Securden.

Once the required details have been filled in, click **Next**.

Step 2: Import User Groups

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

To import Groups, select the Groups tab



Your license allows a maximum of 100 users. You can add 92 more.

Import Groups from Azure AD

Step 2: Discover and Import

Securden fetches users and user groups from the Azure AD domain specified. When you import user groups, Securden will maintain the same group structure here too.

Domain Name: securdentech.onmicrosoft.com

Tenant ID:

Client ID:

Fetch all users who are part of the selected group(s). Your search text should contain the starting characters of the group names. Then click the 'Discover' button.

Verify the Objects Selected for Discovery

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

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

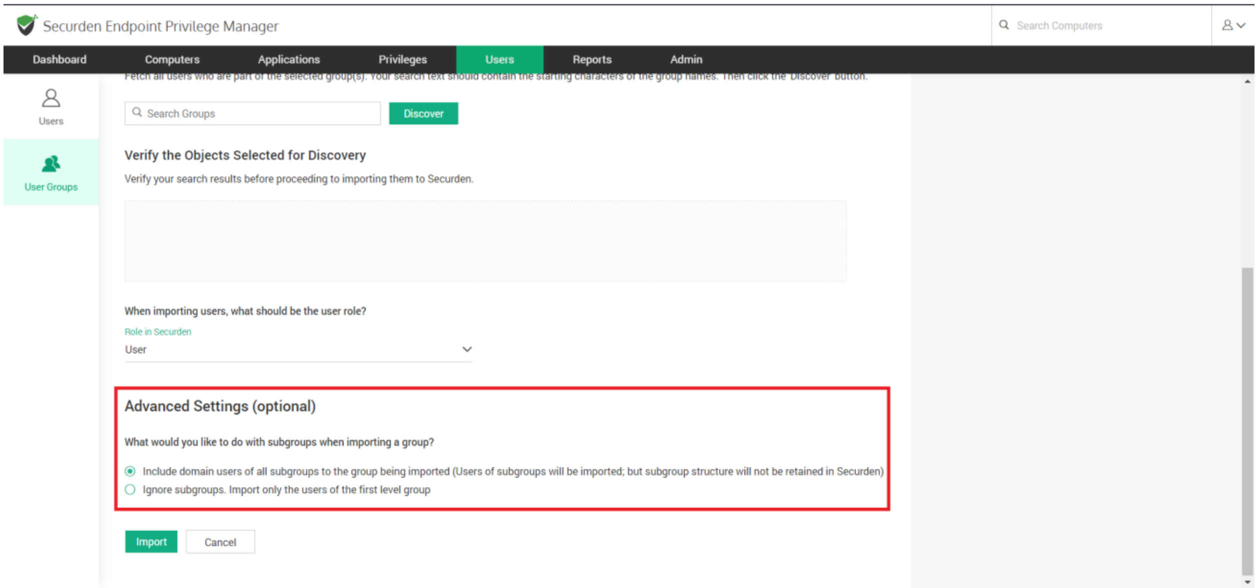
This GUI offers the flexibility to fetch users from Groups in bulk and even specific users, in a single step. That means, you can enter the names of the Groups to be discovered in a single step. You can enter the discovery details in any combination as you wish.

For example, if you want to fetch users from a Group, first enter/browse and select 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 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.

1. Enter the starting letters of your group name and click **Discover.**
2. You can then verify your selection in the **Verify the Objects Selected for Discovery.**
3. You can select the role for the groups imported using the **Role in Securden** dropdown.

Advanced settings



Fetch all users who are part of the selected group(s). Your search text should contain the starting characters of the group names. Then click the 'Discover' button.

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

Advanced Settings (optional)

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)

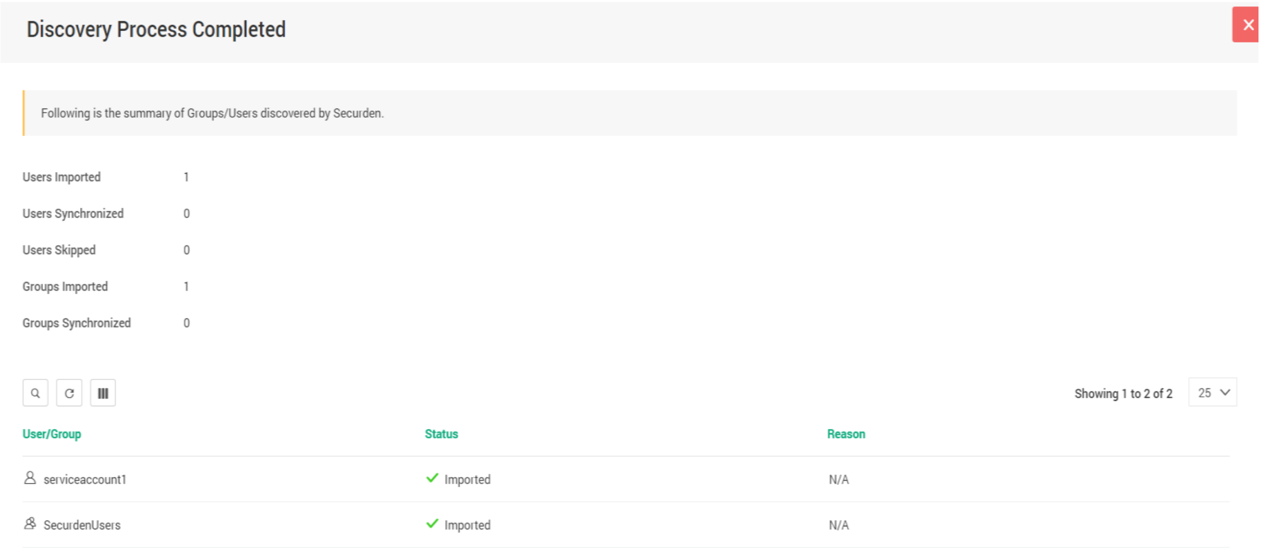
○ Ignore subgroups. Import only the users of the first level group

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 user groups actually imported will conform to the license count. The remaining user groups will not be imported. You can verify the details in the next step.

After selecting the required groups, click on **Import**.

The process of discovering the groups will take a while to complete. The discovered groups will be automatically populated to Securden inventory after completion. The summary of imported groups will be displayed.



Discovery Process Completed

Following is the summary of Groups/Users discovered by Securden.

Users Imported	1
Users Synchronized	0
Users Skipped	0
Groups Imported	1
Groups Synchronized	0

Showing 1 to 2 of 2

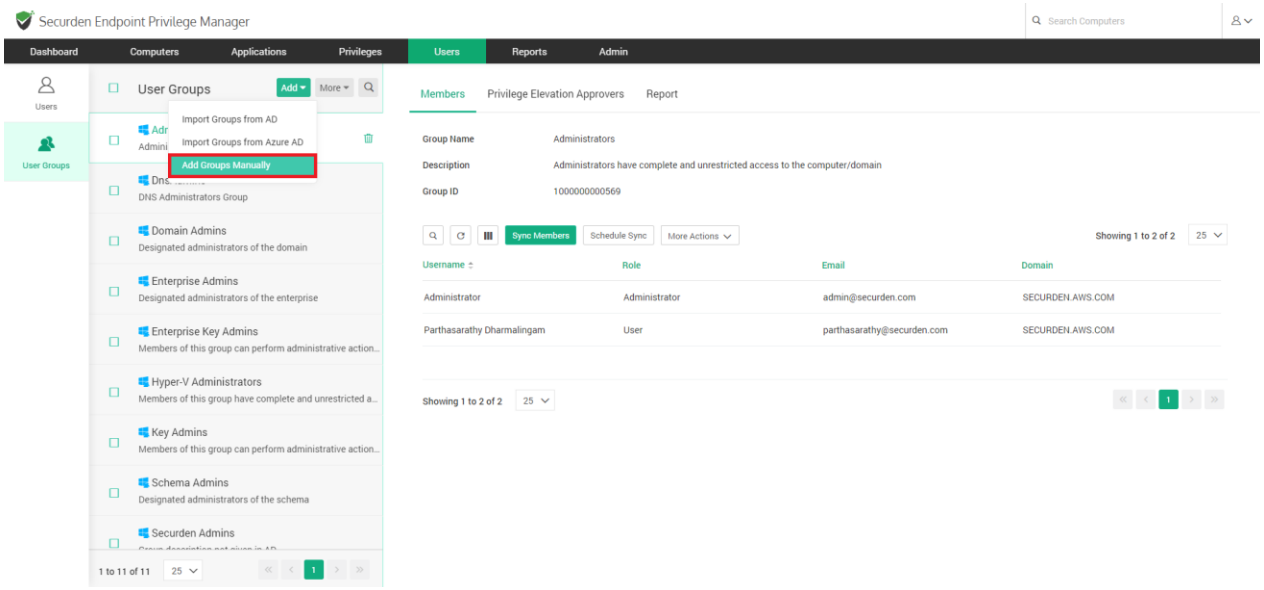
User/Group	Status	Reason
serviceaccount1	✓ Imported	N/A
SecurdenUsers	✓ Imported	N/A

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.



Adr Admini	
Dns DNS Administrators Group	
Domain Admins	Designated administrators of the domain
Enterprise Admins	Designated administrators of the enterprise
Enterprise Key Admins	Members of this group can perform administrative action...
Hyper-V Administrators	Members of this group have complete and unrestricted a...
Key Admins	Members of this group can perform administrative action...
Schema Admins	Designated administrators of the schema
Securden Admins	

Group Name Administrators

Description Administrators have complete and unrestricted access to the computer/domain

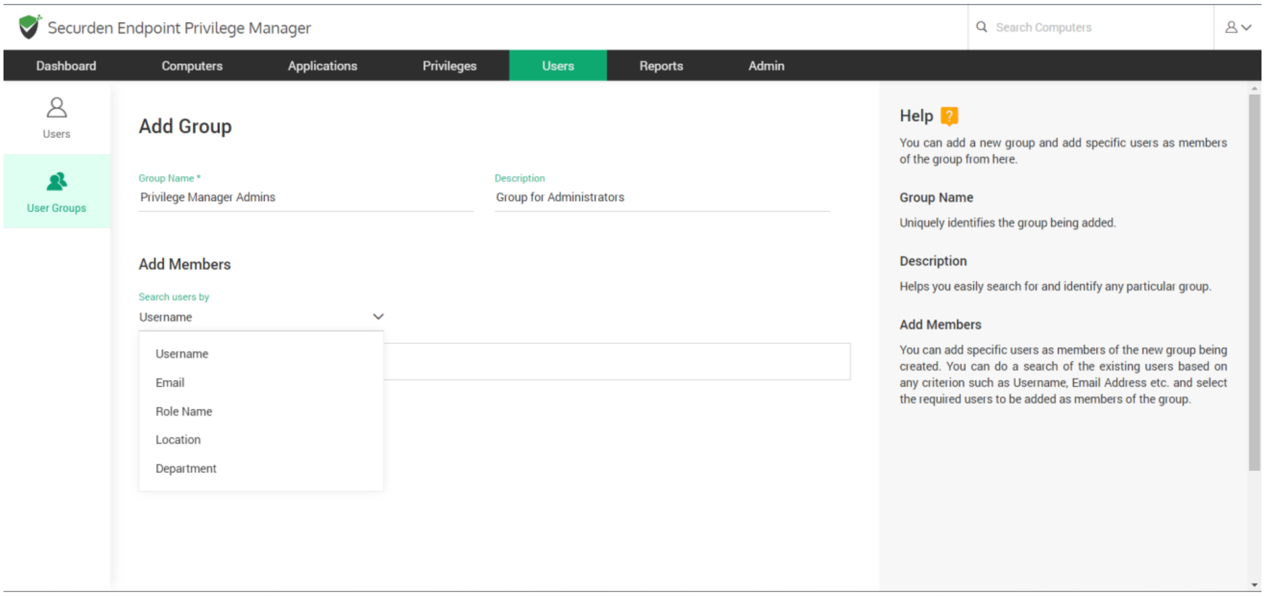
Group ID 1000000000569

Showing 1 to 2 of 2 25

Username	Role	Email	Domain
Administrator	Administrator	admin@securden.com	SECURDEN.AWS.COM
Parthasarathy Dharmalingam	User	parthasarathy@securden.com	SECURDEN.AWS.COM

Showing 1 to 2 of 2 25

In the GUI that opens, fill in the fields according to the guidelines below:



Add Group

Group Name * Privilege Manager Admins

Description Group for Administrators

Add Members

Search users by Username

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.

- **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.

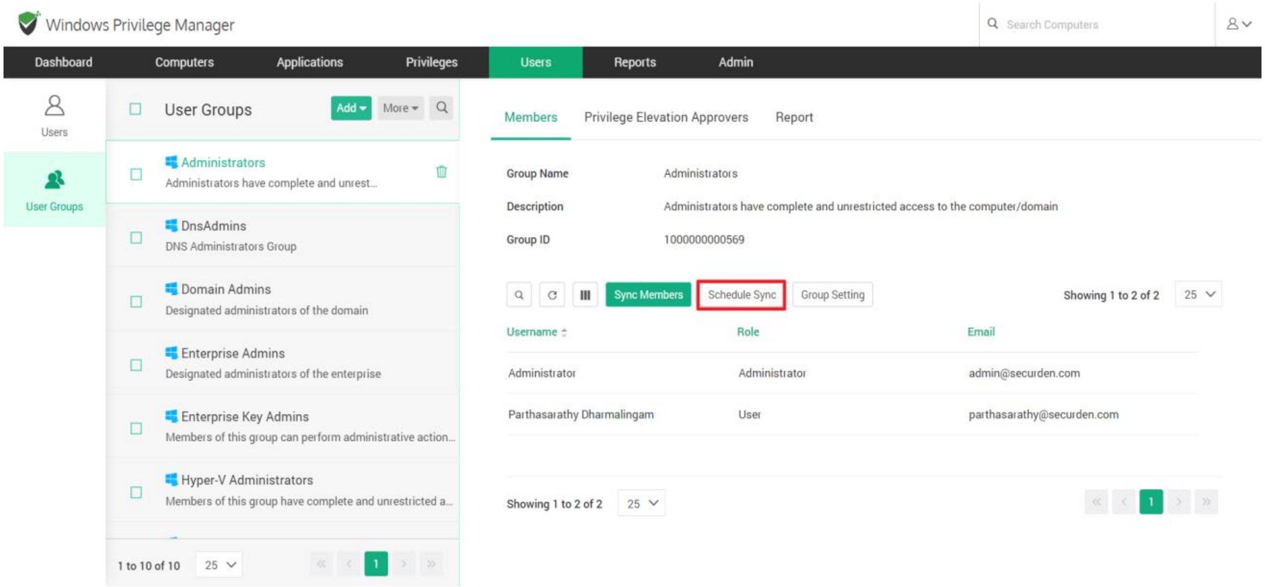
You can search the existing users based on any criteria such as username, email address, etc., and select the required users to be added as members of the group.

After providing these details, click on **Save**, and the user group will get created.

Configure Periodic Synchronization of Groups

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

To do this, navigate to **Users >> User Groups >> Members** and click on **Schedule Sync**.

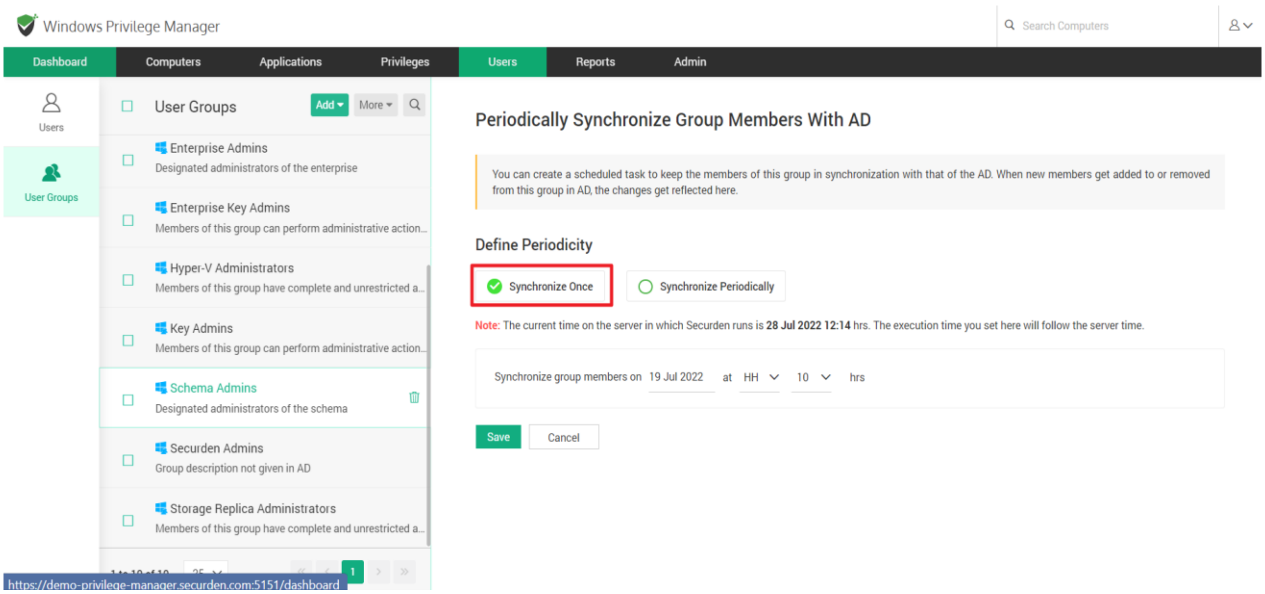


Group Name: Administrators
Description: Administrators have complete and unrestricted access to the computer/domain
Group ID: 1000000000569

Username	Role	Email
Administrator	Administrator	admin@securden.com
Parthasarathy Dharmalingam	User	parthasarathy@securden.com

In the GUI that opens, you can either schedule the synchronization activity for a one-time run or create scheduled tasks to run periodically and ensure regular synchronization.

To synchronize once with your AD, click **Synchronize Once**



User Groups

- Enterprise Admins
  Designated administrators of the enterprise
- Enterprise Key Admins
  Members of this group can perform administrative action...
- Hyper-V Administrators
  Members of this group have complete and unrestricted a...
- Key Admins
  Members of this group can perform administrative action...
- Schema Admins
  Designated administrators of the schema
- Securden Admins
  Group description not given in AD
- Storage Replica Administrators
  Members of this group have complete and unrestricted a...

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.

Define Periodicity

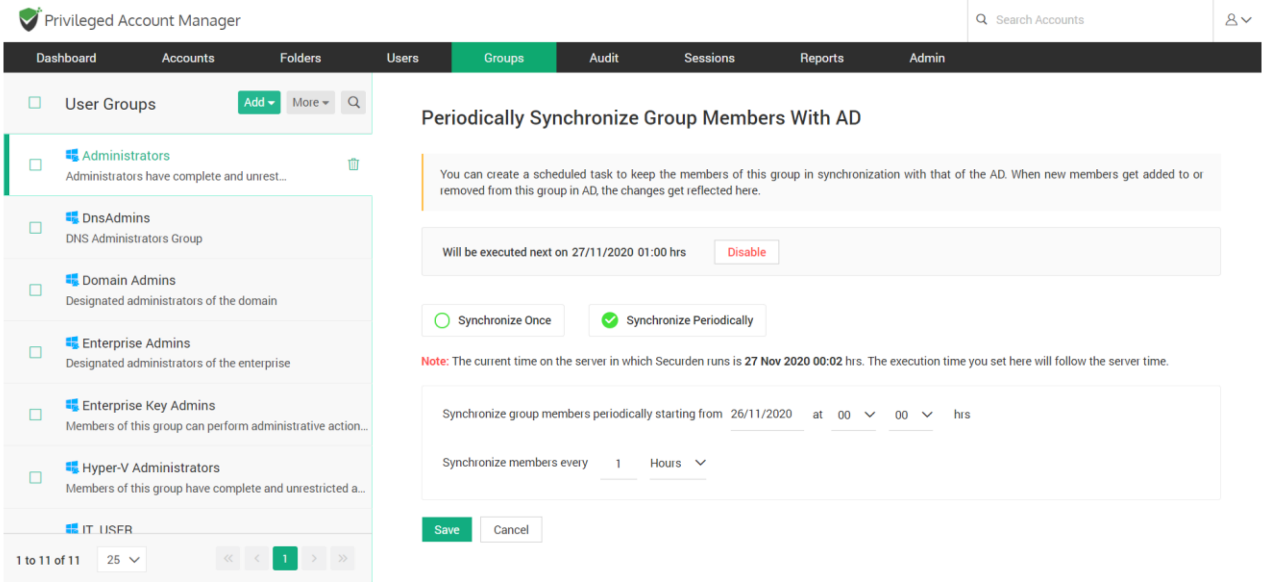
● Synchronize Once ○ Synchronize Periodically

Note: The current time on the server in which Securden runs is **28 Jul 2022 12:14** hrs. The execution time you set here will follow the server time.

Synchronize group members on 19 Jul 2022 at HH 10 hrs

Save Cancel

Select the **Date** and **Time** on which you want to synchronize. For periodic synchronization, click **Synchronize Periodically**



Administrators
Administrators have complete and unrest...
DnsAdmins
DNS Administrators Group
Domain Admins
Designated administrators of the domain
Enterprise Admins
Designated administrators of the enterprise
Enterprise Key Admins
Members of this group can perform administrative action...
Hyper-V Administrators
Members of this group have complete and unrestricted a...
IT USER
1 to 11 of 11 25

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 27/11/2020 01:00 hrs

○ Synchronize Once ● Synchronize Periodically

Note: The current time on the server in which Securden runs is **27 Nov 2020 00:02** hrs. The execution time you set here will follow the server time.

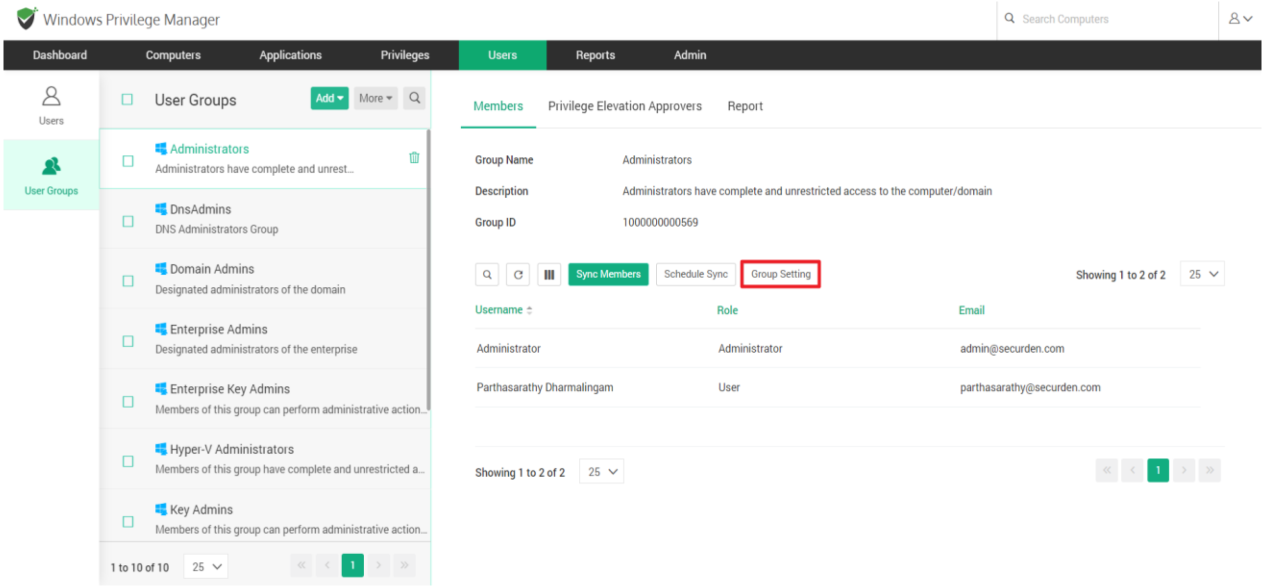
Synchronize group members periodically starting from 26/11/2020 at 00 00 hrs

Synchronize members every 1 Hours

You can choose the start time and date, and set the synchronization interval of your liking.

Modify Group Settings

The **Group Setting** option allows you to modify the role to the users in groups being imported into Securden.



User Groups

Administrators
Administrators have complete and unrest...
DnsAdmins
DNS Administrators Group
Domain Admins
Designated administrators of the domain
Enterprise Admins
Designated administrators of the enterprise
Enterprise Key Admins
Members of this group can perform administrative action...
Hyper-V Administrators
Members of this group have complete and unrestricted a...
Key Admins
Members of this group can perform administrative action...
1 to 10 of 10 25

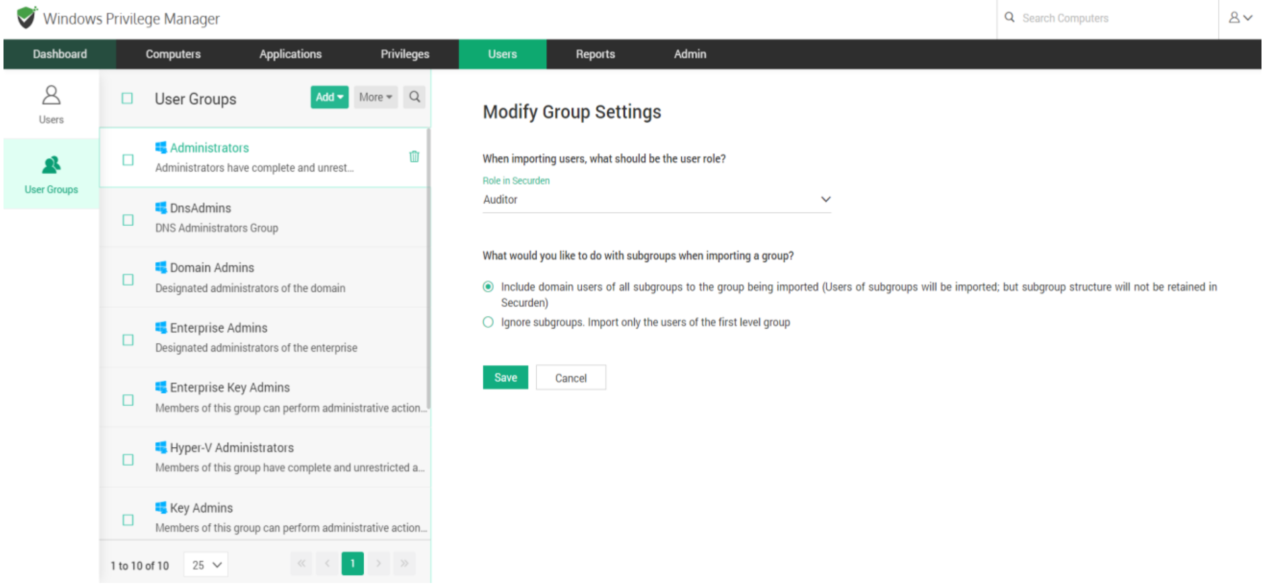
Group Name Administrators
Description Administrators have complete and unrestricted access to the computer/domain
Group ID 1000000000569

Showing 1 to 2 of 2 25

Username	Role	Email
Administrator	Administrator	admin@securden.com
Parthasarathy Dharmalingam	User	parthasarathy@securden.com

Showing 1 to 2 of 2 25

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



Administrators
Administrators have complete and unrest...

DnsAdmins
DNS Administrators Group

Domain Admins
Designated administrators of the domain

Enterprise Admins
Designated administrators of the enterprise

Enterprise Key Admins
Members of this group can perform administrative action...

Hyper-V Administrators
Members of this group have complete and unrestricted a...

Key Admins
Members of this group can perform administrative action...

1 to 10 of 10 25

Modify Group Settings

When importing users, what should be the user role?

Role in Securden: Auditor

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

On making the required changes, click **Save**.

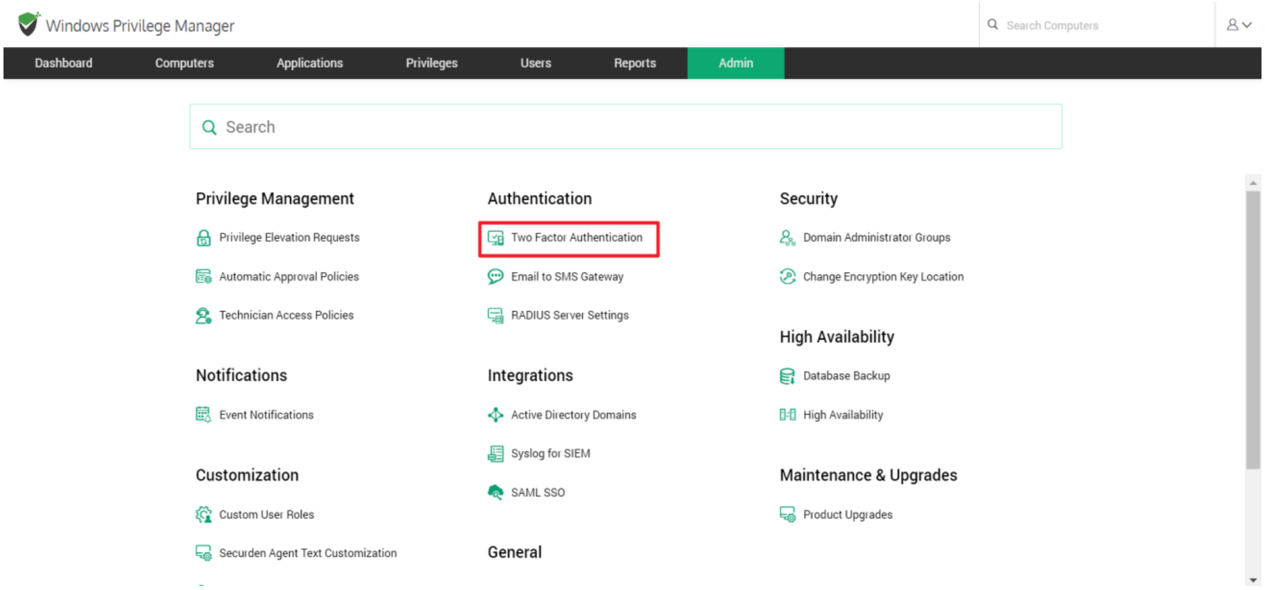
Configure Multi-Factor Authentication

For enhanced security, you can enforce the second layer of authentication for your users to access the Securden interface. Typically, end users need not have to access the interface at all. Only the administrators will need to access it to configure privilege management. Once TFA is configured and enforced, the users will have to authenticate through two successive stages. First by providing their primary credentials followed by the second level of authentication. Securden integrates with a wide range of two factor authentication (TFA) mechanisms and you may integrate with the one that suits you the best.

Configuring TFA is a three-step process:

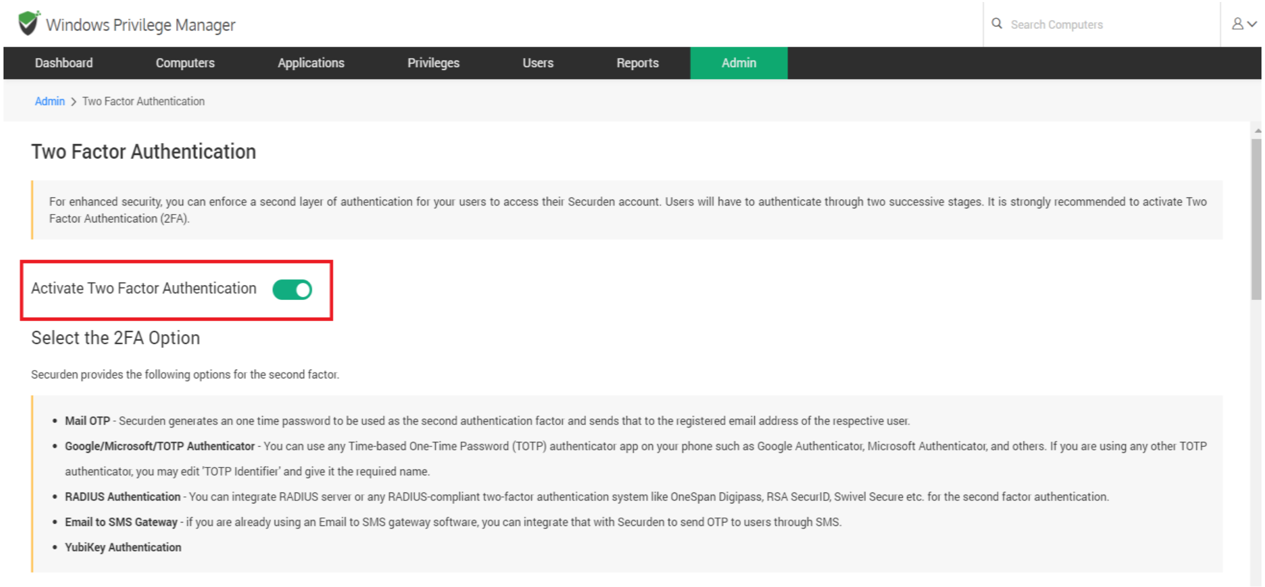
- Activate TFA
- Select the required TFA option and configure
- Configure the enforcement option

To configure two factor authentication, navigate to **Admin >> Authentication >> Two Factor Authentication**.



Activate TFA

The first step in configuring TFA is to activate the option. Toggle **Activate Two Factor Authentication** to green.



Two Factor Authentication

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

Activate Two Factor Authentication ●

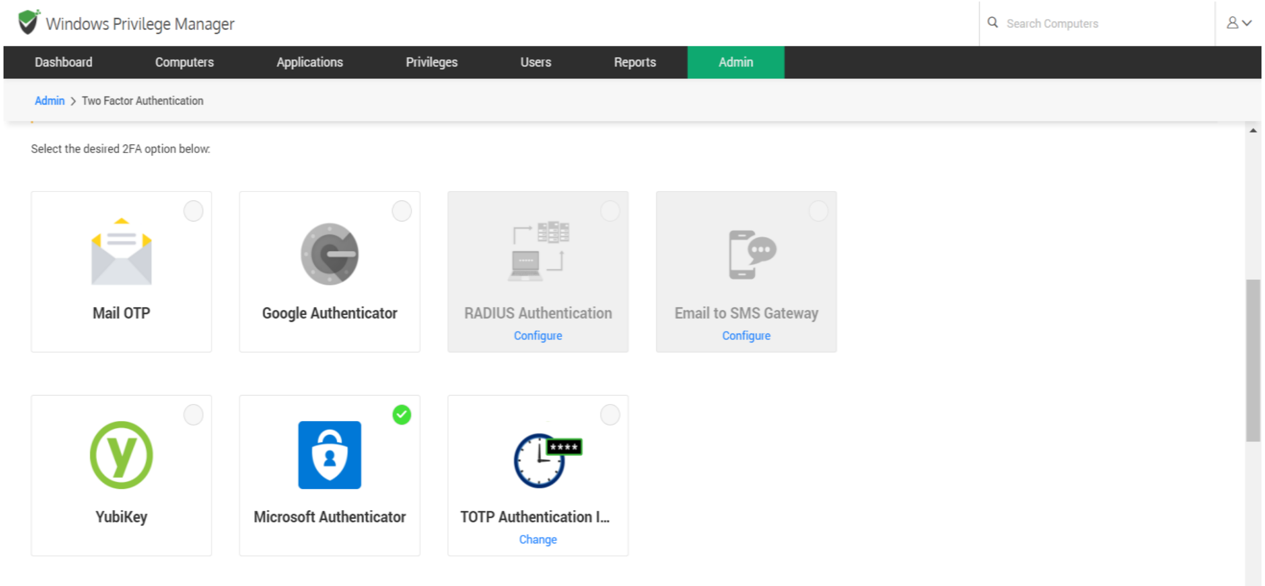
Select the 2FA Option

Securden provides the following options for the second factor.

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

Select the required TFA option

The next step is to select the required TFA option from the various supported options.



Select the desired 2FA option below.

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 TOTP authenticator. If you are using any other TOTP authenticator, you may edit the **TOTP Identifier** and give it an appropriate 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 solution, you can integrate that with Securden to send OTP to users through SMS.

- **YubiKey Authentication –** If you want to use a YubiKey hardware authentication device, you can configure that with Securden and use it.

Configuring Two-Factor Authentication - Once you select the required TFA option, you need to configure its settings. Steps involved in configuring each TFA option is discussed in detail below.

Mail OTP

Securden generates an OTP and sends it to the user who tries to log in. This option requires that the **Mail Server Setting** is configured and also an email address is associated with each user. This OTP, sent through the email will only be valid for the current session and expires when the user logs out.

To configure mail OTP for TFA:

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

   Note: OTP through email requires email addresses to be associated with users. Ensure that email addresses have been associated before enabling this 2FA option. When you change the two-step verification mechanism, the existing configuration for 2FA for the respective users in Securden will be reset. The existing 2FA mechanism will be replaced with the new 2FA mechanism chosen.

Google Authenticator/ Microsoft Authenticator/ TOTP Authenticator

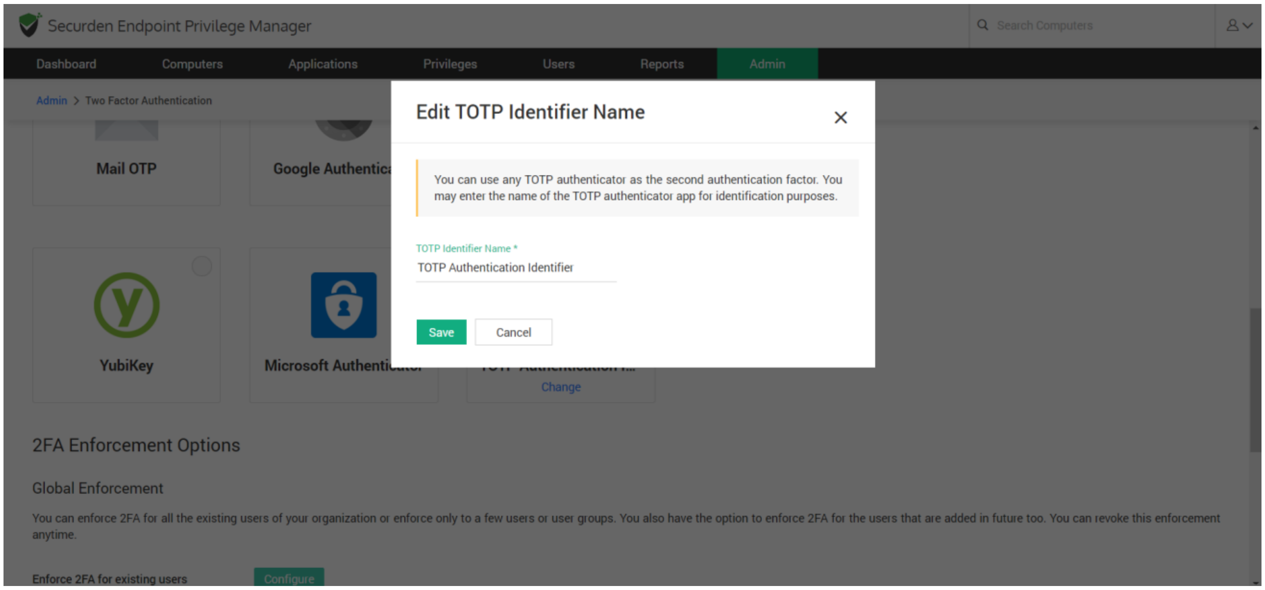
TOTP authenticators like Google Authenticator, Microsoft Authenticator, and others provide a six-digit code to authenticate the second level of access. Users just need to have the Google Authenticator/Microsoft Authenticator/TOTP Authenticator app on their mobile phones or tablet devices.

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

1. Navigate to **Admin >> Authentication >> Two-Factor Authentication**.
2. Choose any of the options **Google Authenticator/ Microsoft Authenticator / TOTP Authenticator**.

Self-support any TOTP Authenticator

If you are using any other TOTP authentication mechanism, you may self-support it by configuring the **TOTP Authentication Identifier.** If you choose to configure a TOTP authentication identifier, you will be prompted to enter an identifier name. Enter the name of your TOTP authentication mechanism and click **Save.**



Edit TOTP Identifier Name

You can use any TOTP authenticator as the second authentication factor. You may enter the name of the TOTP authenticator app for identification purposes.

TOTP Identifier Name *: TOTP Authentication Identifier

2FA Enforcement Options

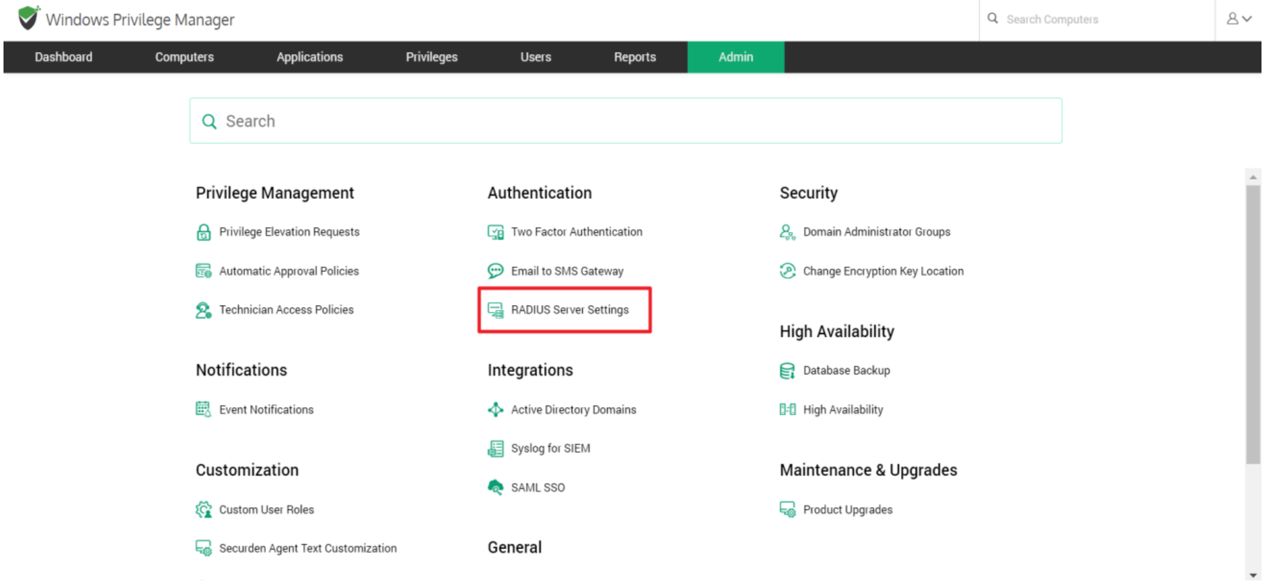
Global Enforcement

You can enforce 2FA for all the existing users of your organization or enforce only to a few users or user groups. You also have the option to enforce 2FA for the users that are added in future too. You can revoke this enforcement anytime.

Enforce 2FA for existing users

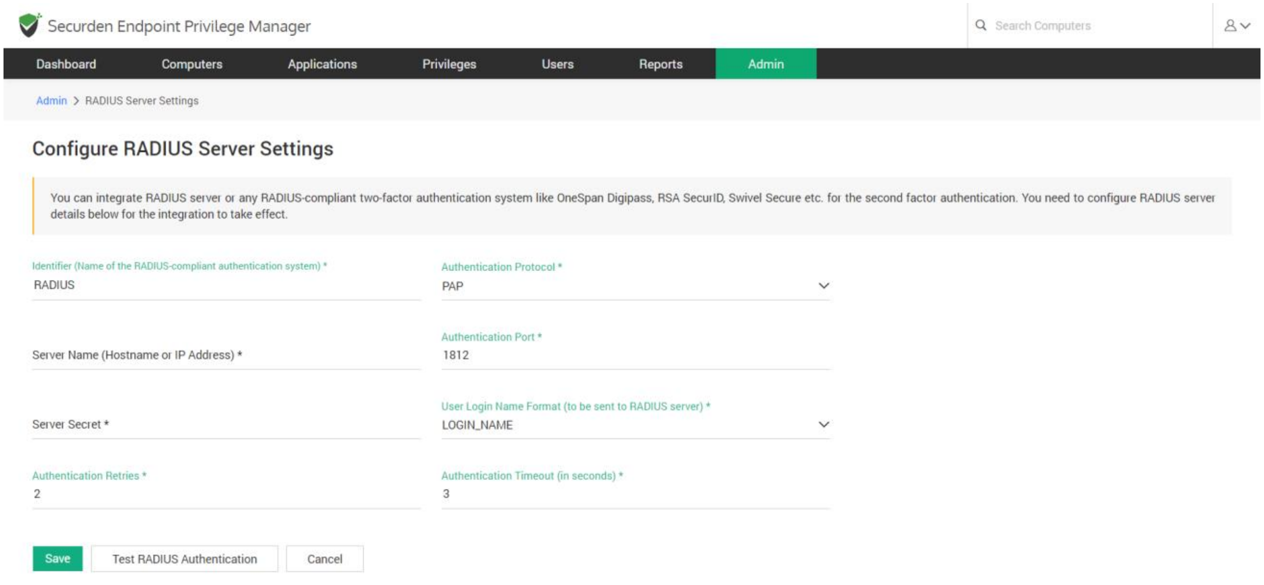
RADIUS Authentication

You can integrate a 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 for the integration to take effect.



To configure RADIUS server, navigate to **Admin >> Authentication >> Two-Factor Authentication >> RADIUS Server Settings.**

In this GUI, you need to enter the following details:


Securden Endpoint Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > RADIUS Server Settings
Save
Test RADIUS Authentication
Cancel

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) *: RADIUS

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 *: 2

Authentication Timeout (in seconds) *: 3

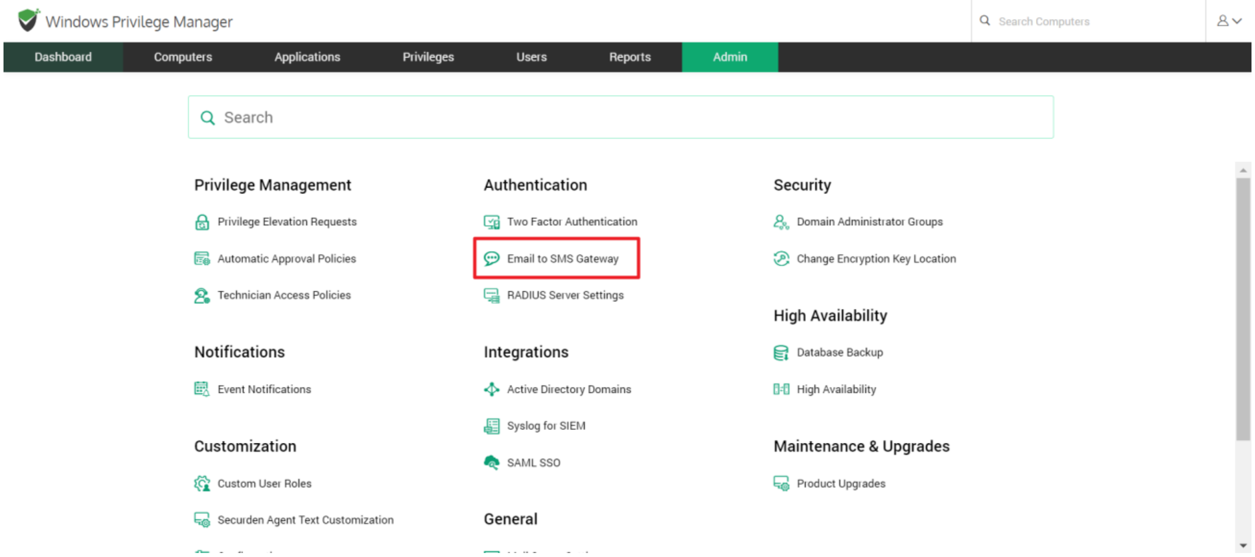
- **Identifier** - Name of the RADIUS-compliant authentication mechanism you are trying to integrate. The name you enter here will appear on the Securden login screen.
- **Servername** - The hostname or IP address of the RADIUS server
- **Server Secret** - The secret key that RADIUS clients use to access the RADIUS server
- **Authentication Retries** - The maximum number of times Securden must try to authenticate with the RADIUS server
- **Authentication Protocol -** Select the authentication method from the list of supported protocols PAP, CHAP, MS-CHAP, MS-CHAPv2
- **Authentication Port** - Enter the RADIUS server port (1812 by default)
- **User Login Format** - The specific format in which the user would enter the login name. This format will be sent to the RADIUS server for authentication. You can select one of the predefined formats or add a new one.
- **Authentication timeout** (in seconds): The maximum time after which the authentication attempt times out.

After entering the details, click **Save** and you may check RADIUS authentication once.

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 through SMS.

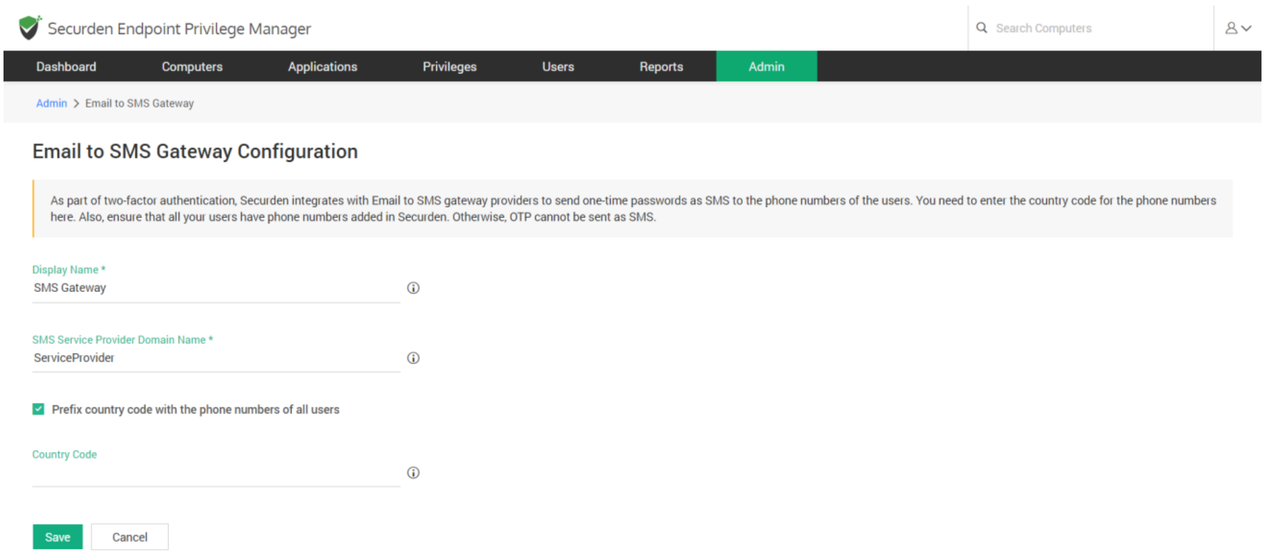
- Navigate to **Admin >> Authentication >> Email to SMS Gateway** to configure this setting.



In the GUI that opens, fill the following fields:

- **Display Name**: The name you give here appears in the list of available TFA options.

- **SMS Service Provider Domain Name**: Enter the domain name of your email service provider here.
- **Country Code**: Enter the country code that needs to be appended to the mobile number. If the country code is already associated with users you may leave this field blank.



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 Gateway

SMS Service Provider Domain Name *
ServiceProvider

☑ Prefix country code with the phone numbers of all users

Country Code

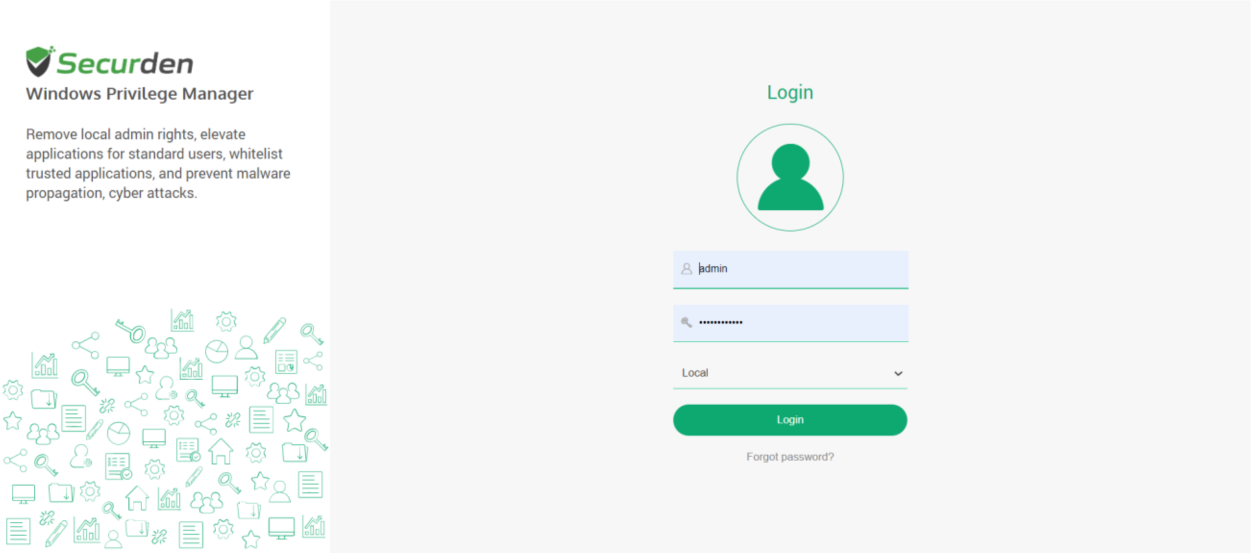
After filling all the required fields, click **Save**.

Yubikey

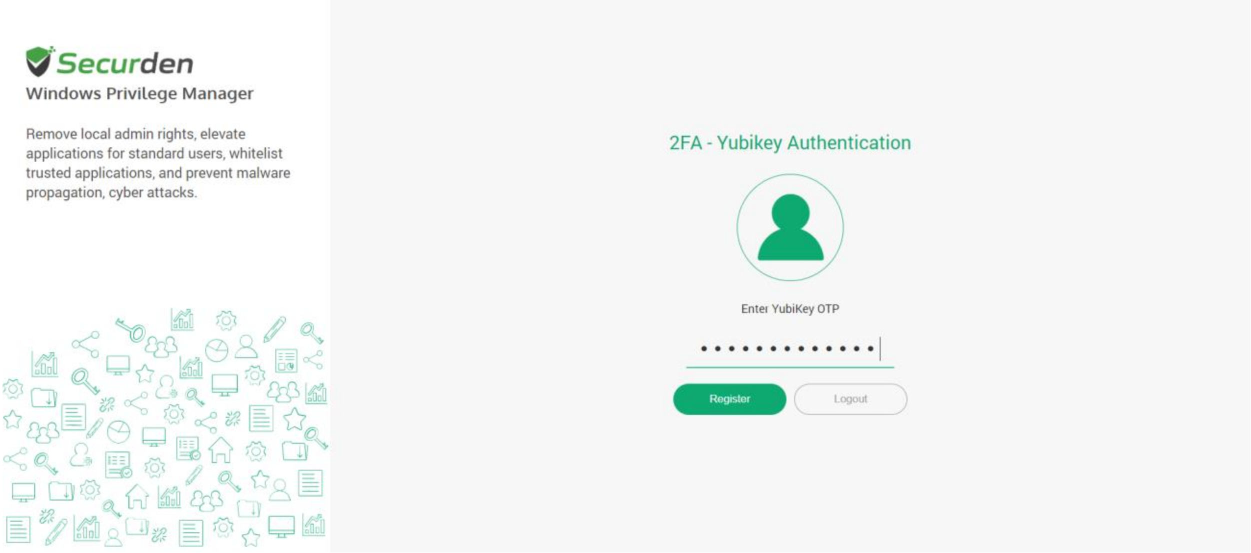
Yubikey tokens supplied by Yubico can be integrated with Securden Windows Privilege Manager for TFA. To configure your Yubikey in Securden, navigate to **Admin >> Authentication >> Two-Factor Authentication** and select **Yubikey**.

Each Yubikey has two slots, which are configured for either a mobile device or a computer/laptop.

To login to Securden WPM using Yubikey as the second factor of authentication, users need to do the following:


Securden
Windows Privilege Manager
Remove local admin rights, elevate applications for standard users, whitelist trusted applications, and prevent malware propagation, cyber attacks.
Login
admin
••••••••••••
Local
Login
Forgot password?

- Enter their Securden credentials and complete the first level of authentication. Once it succeeds, you will be asked to enter the Yubikey OTP.


Securden
Windows Privilege Manager
Remove local admin rights, elevate applications for standard users, whitelist trusted applications, and prevent malware propagation, cyber attacks.
2FA - Yubikey Authentication
Enter YubiKey OTP
••••••••••••••
Register
Logout

Before generating a one-time password using the Yubikey, you need to decide which of the two slots, slot 1 or slot 2, you intend to use for authenticating with Securden.

In the USB port of your Computer/Mobile, insert the Yubikey and generate a 12-character key.

- Securden associates the 12-character key against your account in the database. This key will be used to verify your identity during subsequent login attempts.

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.

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

- cccjgdwkdjkwjdkjwikjdkhhfgrtnnlgedjlftrbdeut
- cccjgjubuebduhubnjkedjkehijeiocjbnublfnrev
- cccjgjgkcbejnvchfkfhiiuunbtnvgihdfiktncvlhck

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.

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.

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

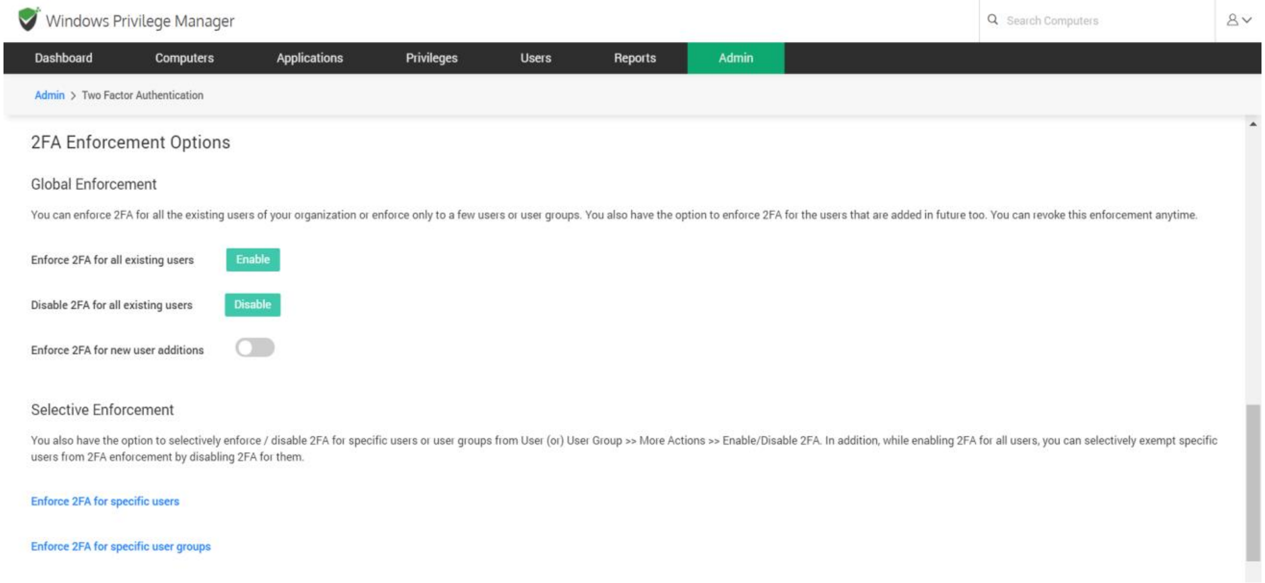
Note: For users logging in for the first time, the users will be prompted to reset their login password after they register their YubiKey.

Enforcement Options

After the TFA option has been configured, the next step is to choose enforcement options. You can choose which users will be required to access WPM using 2FA.

From the **Global Enforcement** option at the bottom of the TFA configuration page, you can do the following:

- Enable 2FA for all existing users
- Disable 2FA for all existing users
- Enable 2FA only for new user additions



2FA Enforcement Options

Global Enforcement

You can enforce 2FA for all the existing users of your organization or enforce only to a few users or user groups. You also have the option to enforce 2FA for the users that are added in future too. You can revoke this enforcement anytime.

Enforce 2FA for all existing users — Enable

Disable 2FA for all existing users — Disable

Enforce 2FA for new user additions

Selective 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.

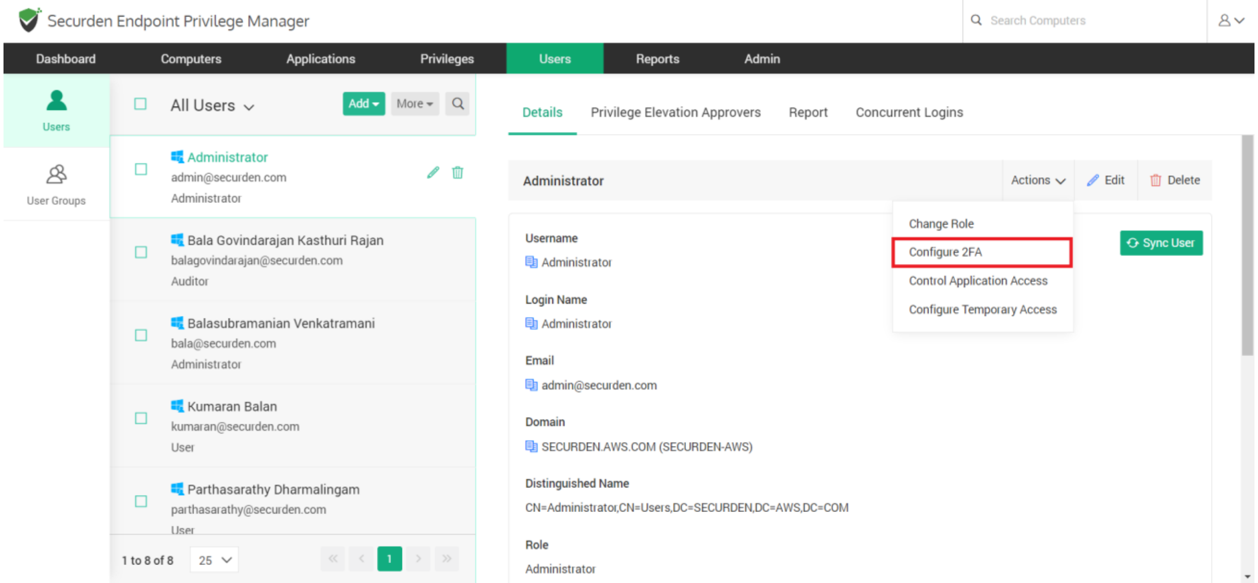
Enforce 2FA for specific users

Enforce 2FA for specific user groups

Selective MFA Enforcement

For Users

You have the option to selectively enforce/disable 2FA for specific users. On clicking **Enforce 2FA for specific users**, you will be redirected to the **Users** tab. Click on the required user and navigate to **User >> Actions >> Configure 2FA** as per the below screenshot.



Administrator
admin@securden.com
Administrator

Bala Govindarajan Kasthuri Rajan
balagovindarajan@securden.com
Auditor

Balasubramanian Venkatramani
bala@securden.com
Administrator

Kumaran Balan
kumaran@securden.com
User

Parthasarathy Dharmalingam
parthasarathy@securden.com
User

Administrator

Username: Administrator

Login Name: Administrator

Email: admin@securden.com

Domain: SECURDEN.AWS.COM (SECURDEN-AWS)

Distinguished Name: CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

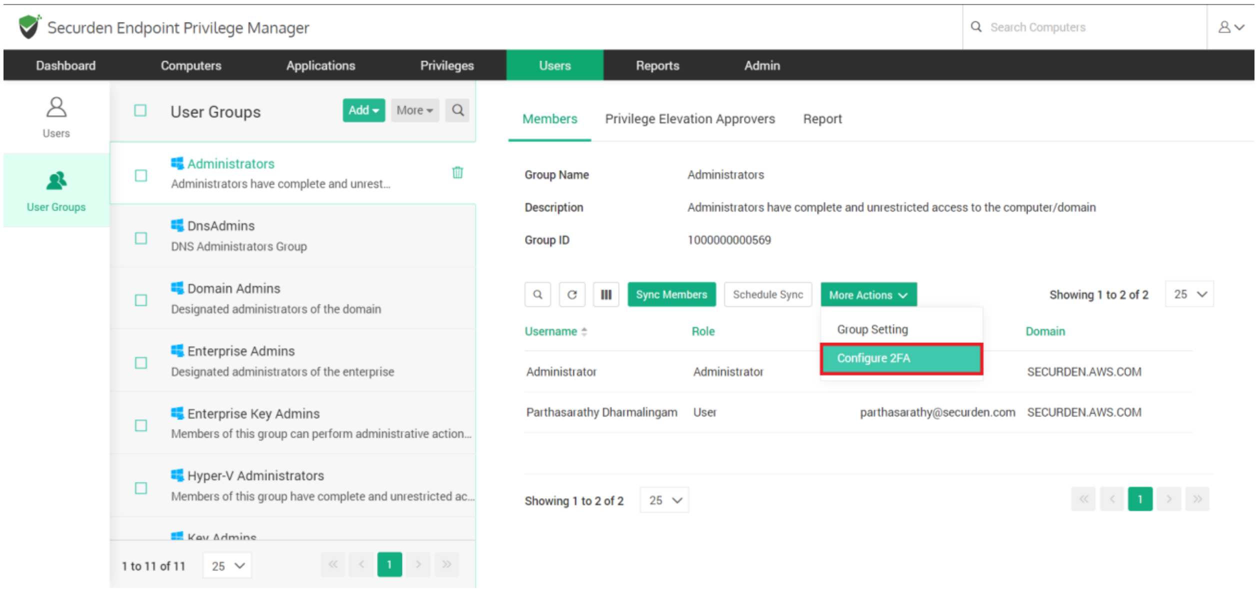
Role: Administrator

In the popup, you need to enable 2FA for the selected groups and choose all the applicable 2FA options from the list of checkboxes. Any 2FA option configured from **Admin >> Authentication >> Two-factor Authentication** will be displayed here.

You can also configure 2FA for multiple users at the same time. You need to select all the required users and go to **Users >> More >> Configure 2FA**.

For User Groups

On clicking Enforce 2FA for specific user groups, you will be redirected to the user groups section. All you have to do is to select the required user group and then navigate to **More Actions >> Configure 2FA** as per the below screenshot.



- Administrators: Administrators have complete and unrest...
- DnsAdmins: DNS Administrators Group
- Domain Admins: Designated administrators of the domain
- Enterprise Admins: Designated administrators of the enterprise
- Enterprise Key Admins: Members of this group can perform administrative action...
- Hyper-V Administrators: Members of this group have complete and unrestricted ac...
- Key Admins

Group Name: Administrators
Description: Administrators have complete and unrestricted access to the computer/domain
Group ID: 1000000000569

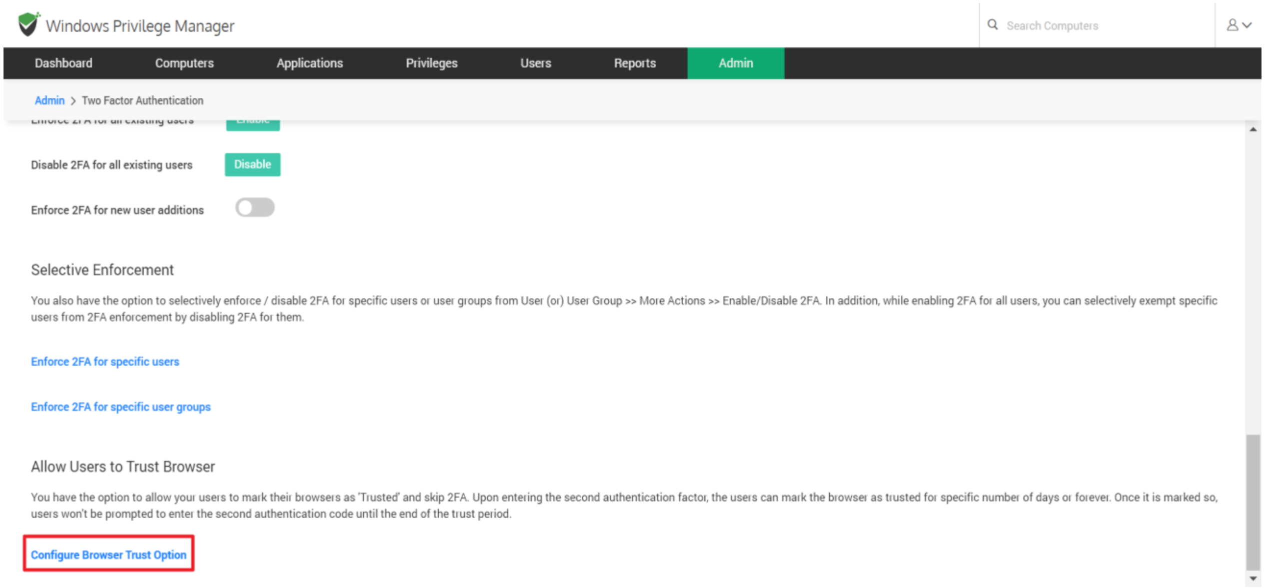
Username	Role		Domain
Administrator	Administrator		SECURDEN.AWS.COM
Parthasarathy Dharmalingam	User	parthasarathy@securden.com	SECURDEN.AWS.COM

In the popup, you need to enable 2FA for the selected groups and choose all the applicable 2FA options from the list of checkboxes. Any 2FA option configured from **Admin >> Authentication >> Two-factor Authentication** will be displayed here.

You can also configure 2FA for multiple user groups at the same time. You need to select all the required user groups and go to **Users >> User Groups >> More >> Configure 2FA**.

Allow Users to Trust Browser

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


Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Two Factor Authentication
Disable 2FA for all existing users
Disable
Enforce 2FA for new user additions
Enforce 2FA for specific users
Enforce 2FA for specific user groups
Configure Browser Trust Option

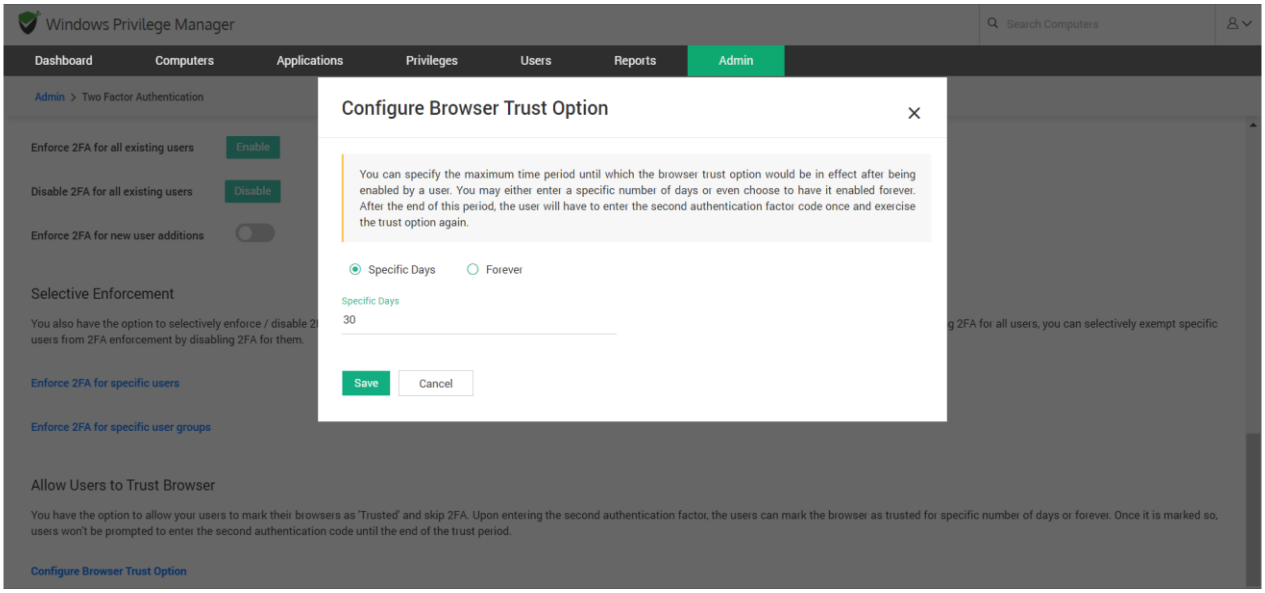
Selective Enforcement

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 specific number of days or forever. Once it is marked so, users won't be prompted to enter the second authentication code until the end of the trust period.

To enable this feature, click the **Configure Browser Trust Option** link, and a pop-up box will appear. Here, you can specify the maximum period until which the browser trust option would be in effect. 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.


Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Two Factor Authentication
Enable
Disable
Save
Cancel
Enforce 2FA for specific users
Enforce 2FA for specific user groups
Configure Browser Trust Option

Enforce 2FA for all existing users

Disable 2FA for all existing users

Enforce 2FA for new user additions

Selective Enforcement

You also have the option to selectively enforce / disable 2 g 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 specific number of days or forever. Once it is marked so, users won't be prompted to enter the second authentication code until the end of the trust period.

Configure Browser Trust Option

You can specify the maximum time 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.

● Specific Days ○ Forever

Specific Days: 30

Configure SAML-based SSO

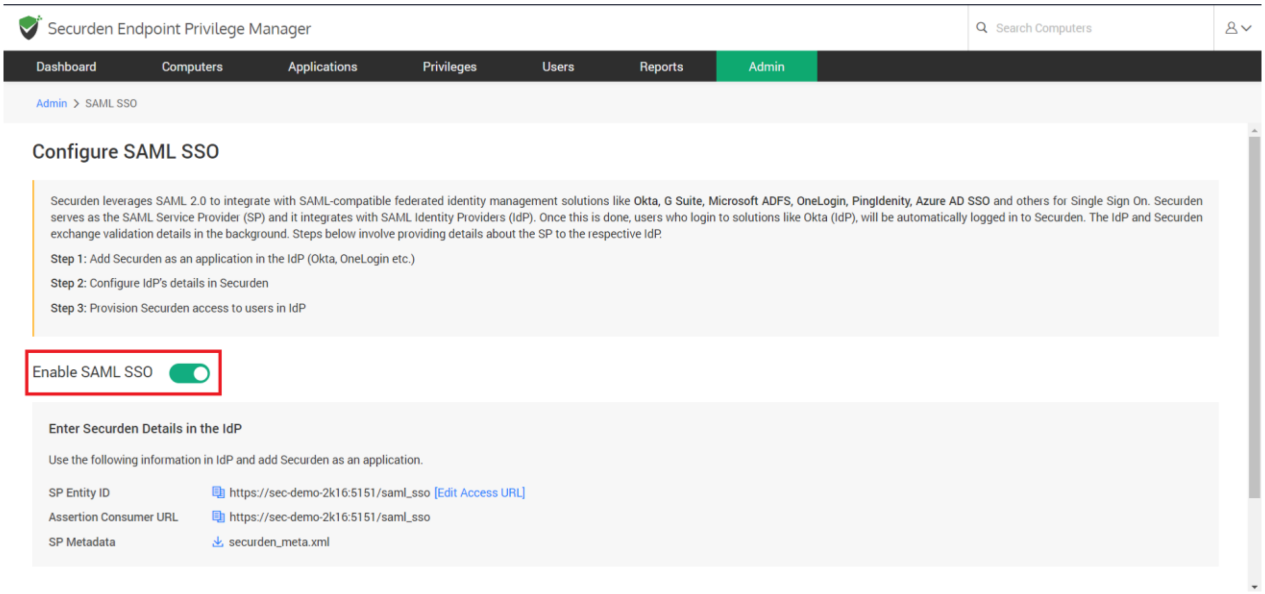
Securden leverages SAML 2.0 to seamlessly integrate with SAML-compatible federated identity management solutions like Okta, G Suite, Microsoft ADFS, OneLogin, PingIdentity, Azure AD SSO, and others for single sign-on. Securden serves as the SAML service provider (SP) and it integrates with SAML identity providers (IdP). Once the configuration is done, you can provide your users the single sign on experience to access Securden GUI.

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

- **Step 1:** Add Securden WPM 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:

Navigate to **Admin >> Integration >> Configure SAML SSO**. In the GUI that opens, toggle the **Enable SAML SSO** button to green.



Configure SAML SSO

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

Step 1: Add Securden as an application in the IdP (Okta, OneLogin etc.)

Step 2: Configure IdP's details in Securden

Step 3: Provision Securden access to users in IdP

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://sec-demo-2k16:5151/saml_sso [Edit Access URL]
Assertion Consumer URL	https://sec-demo-2k16:5151/saml_sso
SP Metadata	securden_meta.xml

Step 1: Add Securden as an application in your IdP

For adding Securden (The service provider) as an application in your IdP, you would typically require the following details:

SP Entity ID - https://sec-demo-2k16:5151/saml_sso
Assertion Consumer URL - https://sec-demo-2k16:5151/saml_sso
SP Metadata - securden_meta.xml

Enter the details mentioned above in the interface of your IdP portal, and then proceed with the next step.

(Note: The .xml file is available for download from the above GUI on clicking the ⤓ icon)

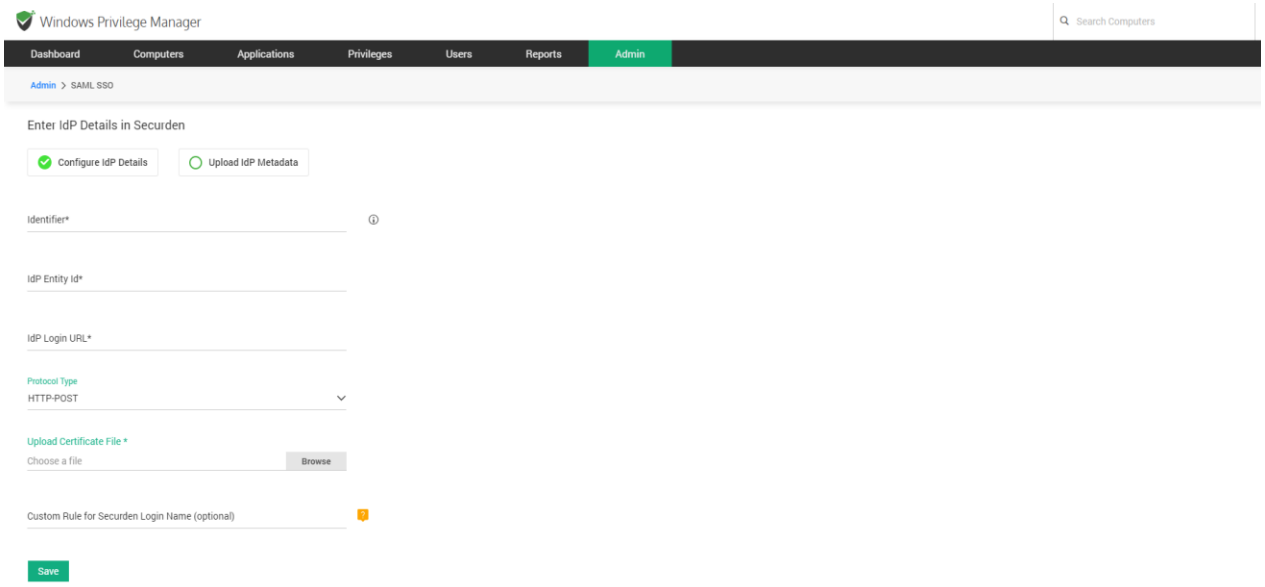
Step 2: Configure IdP's details in Securden

Once you have completed step 1 and added Securden as an application in your IdP portal, you would have certain details obtained from the IdP like IdP entity ID, IdP login URL, and protocol type. You need to supply those details on the **Enter IdP Details** page on the Securden interface.

You have two options here -

- Configure IdP Details
- Upload IdP’s Metadata

Configure IdP Details



Enter IdP Details in Securden

● Configure IdP Details ○ Upload IdP Metadata

Protocol Type
HTTP-POST

Fill in the following details:

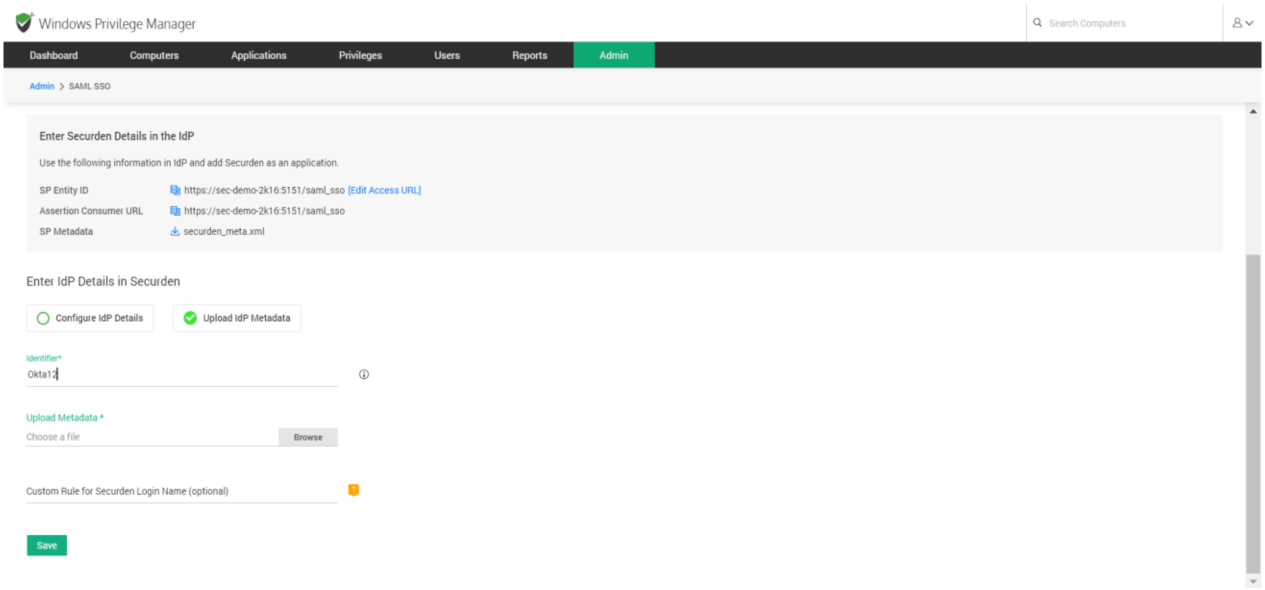
- **Identifier** - This will appear on the Securden WPM login page and enable users to identify the SAML identity provider.
- **IdP Entity Id -** A globally unique name for the identity provider
- **Login URL** - The URL to login into the IdP
  (IdP entity Id and login URL details should be fetched from your IdP interface)
- **Protocol type** - This can either be an HTTP POST or an HTTP redirect protocol.
- **Certificate File** - The digital certificate of the IdP browsed from your system and added here.
- **Custom Rule for Securden Login Name** - This is an optional field. 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, **str** denotes the name returned by the identity provider.

Function	Input Parameters	Example	Output
stringAppend	(String str, String suffix)	stringAppend('This is', ' a test')	This is a test
toUpperCase	(String str)	toUpperCase('This is a test')	THIS IS A TEST
toLowerCase	(String str)	toLowerCase('This is a test')	this is a test
substringBefore	(String str, String searchString)	substringBefore('abc@securden.com', '@')	abc
substringAfter	(String str, String searchString)	substringAfter('abc@securden.com', '@')	securden.com

On filling in the details, click **Save**.

Upload IdP's Metadata



Enter Securden Details in the IdP

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

SP Entity ID	https://sec-demo-2k16:5151/saml_sso [Edit Access URL]
Assertion Consumer URL	https://sec-demo-2k16:5151/saml_sso
SP Metadata	securden_meta.xml

Enter IdP Details in Securden

○ Configure IdP Details ● Upload IdP Metadata

Identifier*: Okta12

Upload Metadata *: Choose a file Browse

Custom Rule for Securden Login Name (optional)

On clicking Upload IdP Meta, fill in the following details:

- **Identifier** - This will appear on the Securden WPM login page and enable users to identify the SAML identity provider.
- **Metadata** - Data in a .xml format that provides the details of the IdP, including the IdP entity data, login URL, protocol type, and digital certificate.
- **Custom rule for Securden Login Name** - This field is optional. 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**.

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, **str** denotes the name returned by the identity provider.

Function	Input Parameters	Example	Output
stringAppend	(String str, String suffix)	stringAppend('This is', ' a test')	This is a test
toUpperCase	(String str)	toUpperCase('This is a test')	THIS IS A TEST
toLowerCase	(String str)	toLowerCase('This is a test')	this is a test
substringBefore	(String str, String searchString)	substringBefore('abc@securden.com' , '@')	abc
substringAfter	(String str, String searchString)	substringAfter('abc@securden.com', '@')	securden.com

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

After completing the integration, remember to provision access to Securden WPM for your users in the IdP. Without provisioning access, users will not be able to access Securden WPM by leveraging SSO capabilities.

Troubleshooting Tips

After integration, if you get **invalid user response**, following are the typical reasons:

The username format could be the cause of this issue. For authentication, Securden validates the value against the **Username** in Securden.

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 username alone).

So, in the SSO configuration page, if you change the **Custom rule for Securden login** as below, the issue might be resolved:

*stringAppend('**DOMAINNAME**', loginname)*

Example: stringAppend('**SECURDENDEV**', loginname)

In addition, there might be an email mismatch with username.

If an email is received from SSO, the domain name has to be trimmed from the value:

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

For extracting username from email:

substringBefore(loginname, '@')

The above steps typically apply for integrating any SAML-based SSO solution. If you need any assistance in integrating with any specific IdP, write to support@securden.com .

SECTION 3: Privilege Management Configurations

Configuring privilege management in Securden is a simple four step process.

- **Step 1:** The first step is to deploy the Securden agent on the required workstations/servers. Once the agent is installed, it will populate all the endpoints it is deployed on. Then, it starts discovering the applications and processes (that require admin rights) that are present in the endpoints.
- **Step 2:** In addition to automatic application discovery, you can also manually add applications.
- **Step 3:** The third step is to create control policies.
- **Step 4:** The final step is to remove local admin rights.

Prior to deploying the agent, **optionally**, you can do a discovery of the workstations and deploy the agent from the GUI on the discovered computers too.

Step 1: Deploy Securden Agent on Computers

To elevate applications and processes for standard users, you need to deploy the Securden agent on workstations and servers. The agent takes care of elevating the whitelisted applications and processes for standard users.

Securden agent can be deployed in three ways:

1. Installing manually on workstations and servers

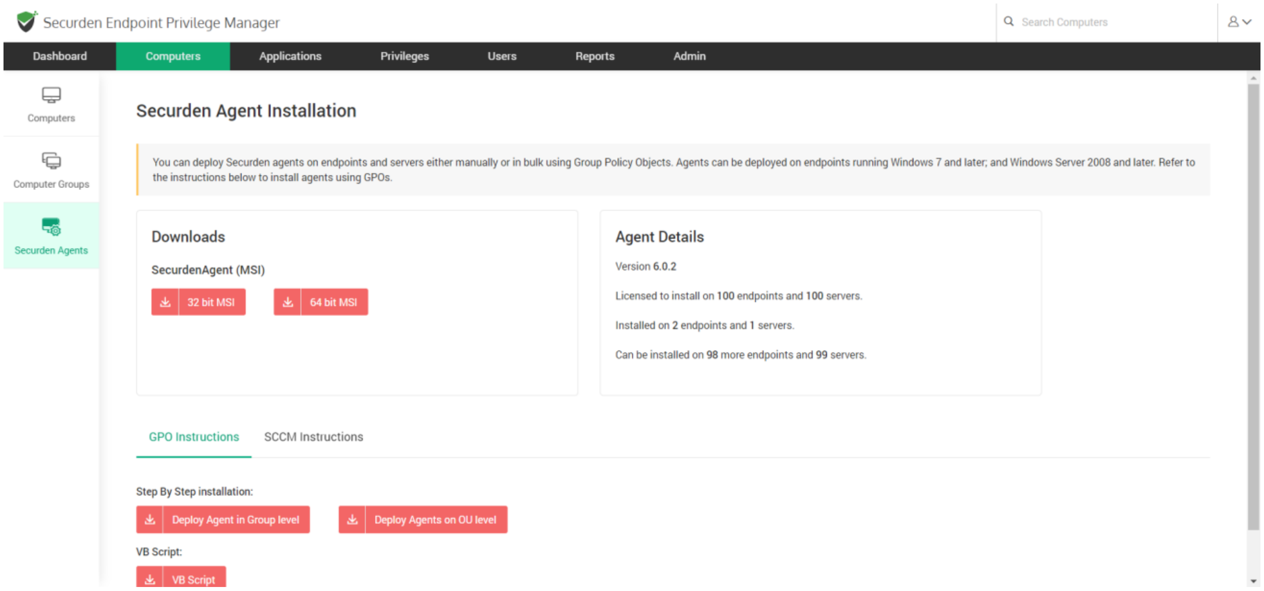
2. Install in bulk using group policy objects (GPO) or by using your SCCM solution
3. You can also push the agent on the required workstations from the product interface

Manual Installation

Navigate to **Computers >> Securden Agents** to download and install the agent manually on the required workstations and servers.

Agent Installation Using GPO

Navigate to **Computers >> Securden Agents** and scroll down to **GPO Instructions**



Securden Agent Installation

You can deploy Securden agents on endpoints and servers either manually or in bulk using Group Policy Objects. Agents can be deployed on endpoints running Windows 7 and later; and Windows Server 2008 and later. Refer to the instructions below to install agents using GPOs.

Downloads

SecurdenAgent (MSI)

Agent Details

Version 6.0.2

Licensed to install on 100 endpoints and 100 servers.

Installed on 2 endpoints and 1 servers.

Can be installed on 98 more endpoints and 99 servers.

Step By Step installation:

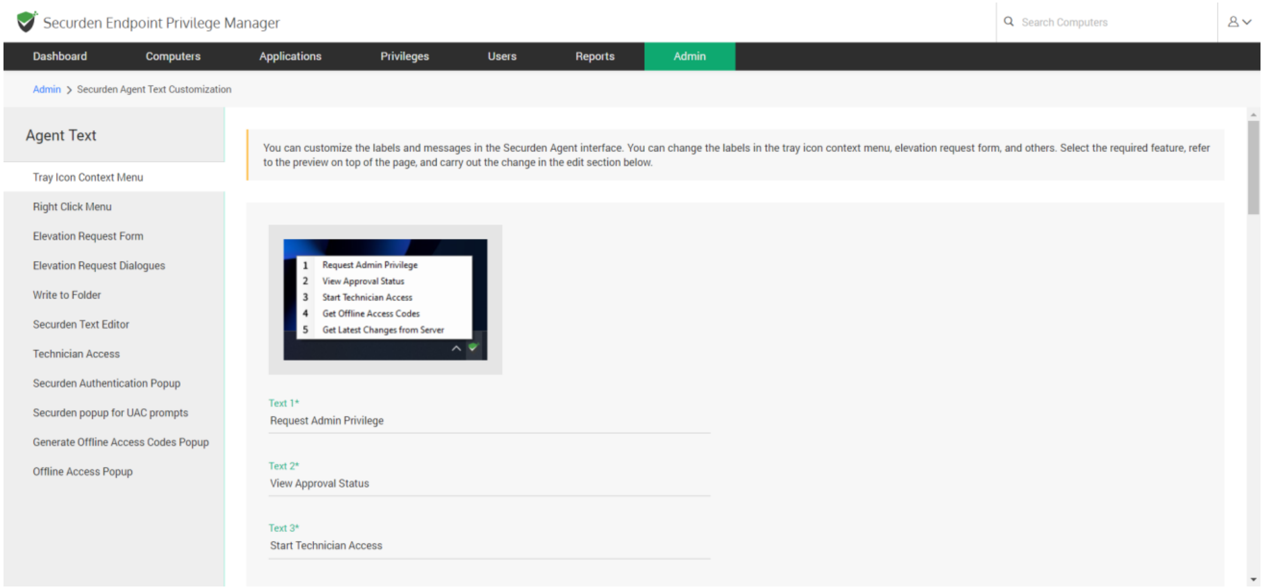
VB Script:

You can push Securden agents to multiple computers at once by using a group policy object. You can either push the agent to all computers belonging to an OU or push the agent to computers belonging to specific groups. You can find step-by-step instructions to configure a GPO using the gpmc.msc service as a downloadable PDF in the Securden user interface for both deployment options.

Securden Agent Text Customization

The Securden agent displays various labels, context menus, and forms. You can customize the message text and labels in such a way that your end users will be able to understand the options without any training. 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** and select the required option.


Securden Endpoint Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Securden Agent Text Customization
Agent Text
Tray Icon Context Menu
Right Click Menu
Elevation Request Form
Elevation Request Dialogues
Write to Folder
Securden Text Editor
Technician Access
Securden Authentication Popup
Securden popup for UAC prompts
Generate Offline Access Codes Popup
Offline Access Popup
1 Request Admin Privilege
2 View Approval Status
3 Start Technician Access
4 Get Offline Access Codes
5 Get Latest Changes from Server

You can customize the labels and messages in the Securden Agent interface. You can change the labels in the tray icon context menu, elevation request form, and others. Select the required feature, refer to the preview on top of the page, and carry out the change in the edit section below.

Text 1*
Request Admin Privilege

Text 2*
View Approval Status

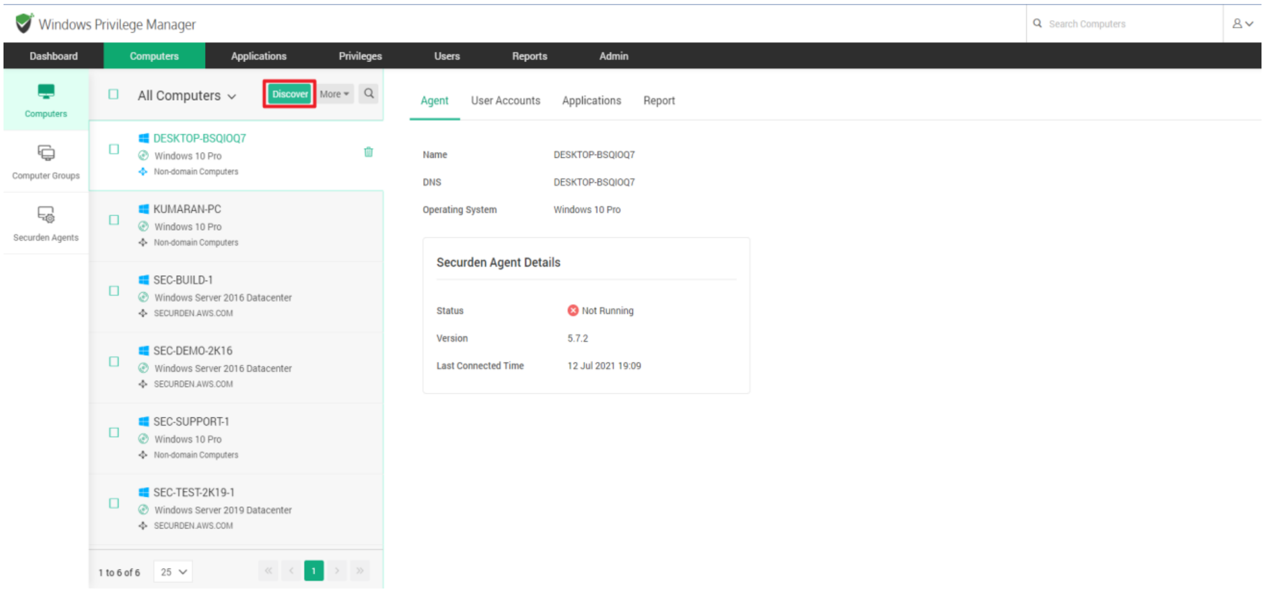
Text 3*
Start Technician Access

The menu located at the left hand side lists the different types of messages related to the Securden agent. You will see the related screenshots in each section. In the text fields below the respective screenshots, you have the option to customize the text. Once the agent text changes are done, click **Save** to save your changes

Discover Workstations (Optional)

As explained earlier, you can push agents to workstations directly from Securden GUI. If you want to do this, you need to discover the required computers.

To discover computers, navigate to **Computers** tab and click **Discover**



DESKTOP-BSQIOQ7 Windows 10 Pro Non-domain Computers	
KUMARAN-PC Windows 10 Pro Non-domain Computers	
SEC-BUILD-1 Windows Server 2016 Datacenter SECURDEN.AWS.COM	
SEC-DEMO-2K16 Windows Server 2016 Datacenter SECURDEN.AWS.COM	
SEC-SUPPORT-1 Windows 10 Pro Non-domain Computers	
SEC-TEST-2K19-1 Windows Server 2019 Datacenter SECURDEN.AWS.COM	

Name DESKTOP-BSQIOQ7
DNS DESKTOP-BSQIOQ7
Operating System Windows 10 Pro

Securden Agent Details

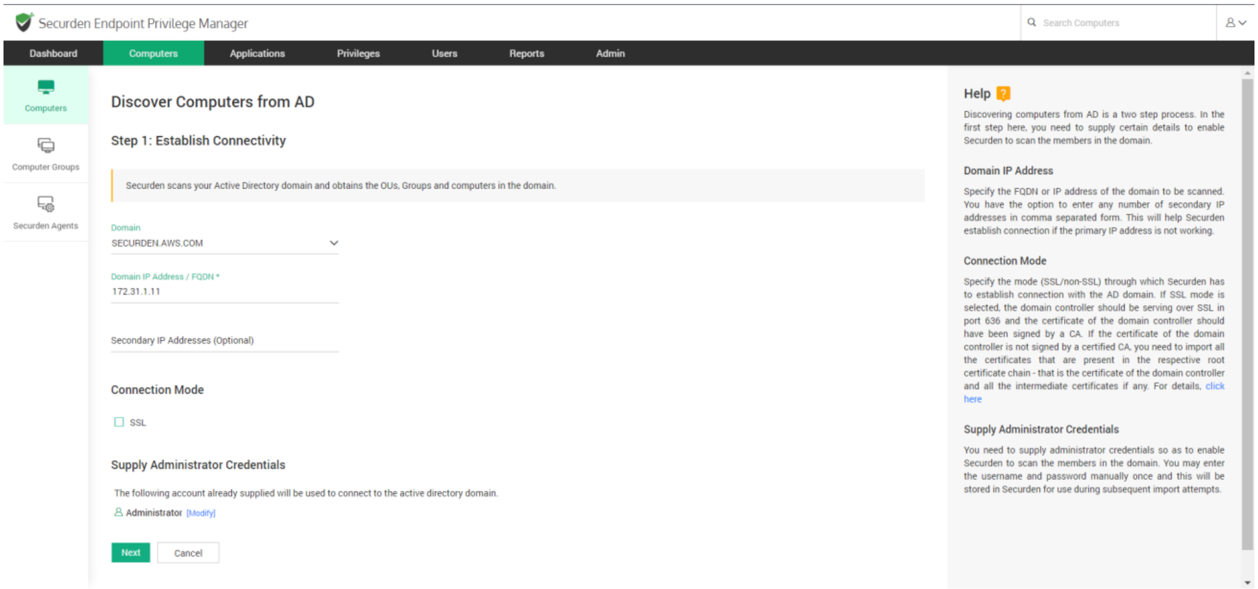
Status Not Running
Version 5.7.2
Last Connected Time 12 Jul 2021 19:09

Discovery is a two-step process:

First, you need to establish connectivity to the domain. To connect with the domain, certain details such as **domain IP address** and **administrator credentials** are required.

Additionally, you need to specify the connection 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 a certified CA does not sign the certificate of the domain controller, 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.

Based on the details furnished, Securden will connect with the AD Domain and fetch the computers and computer groups available.



Discover Computers from AD

Step 1: Establish Connectivity

Securden scans your Active Directory domain and obtains the OUs, Groups and computers in the domain.

Domain: SECURDEN.AWS.COM

Domain IP Address / FQDN *: 172.31.1.11

Secondary IP Addresses (Optional)

Connection Mode

□ SSL

Supply Administrator Credentials

The following account already supplied will be used to connect to the active directory domain.

Administrator [Modify]

Help

Discovering computers 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.

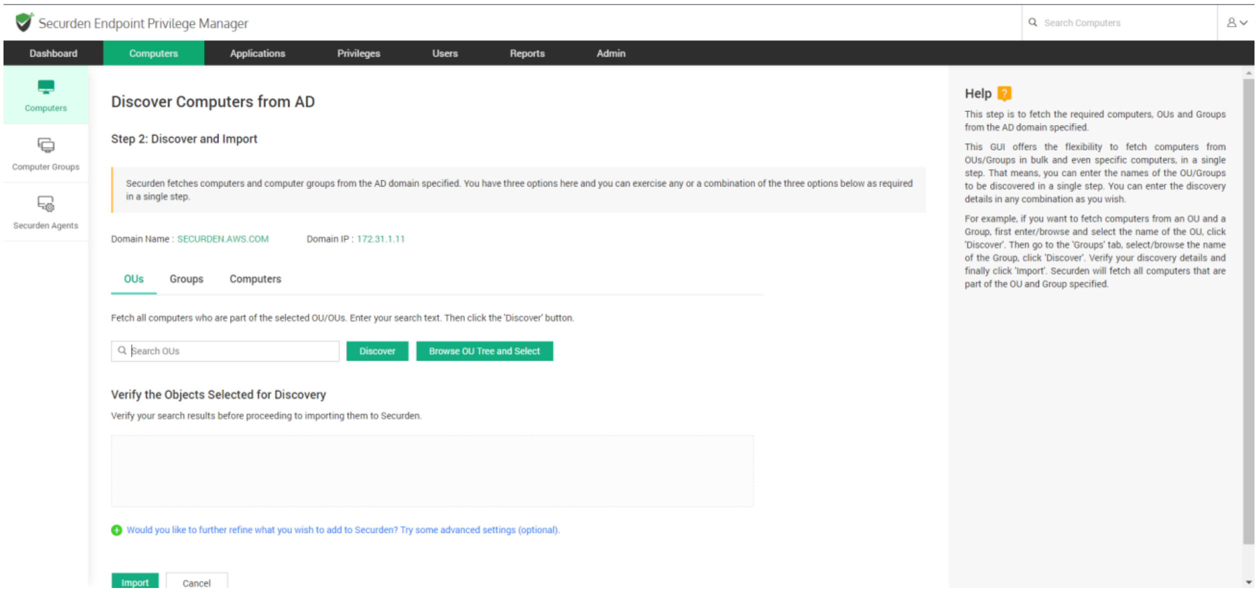
Connection Mode

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 stored in Securden for use during subsequent import attempts.

Once Securden connects with the AD domain, it discovers computers and computer groups in the AD. You have three options here (OUs, Groups, Computers) to select the computers to be onboarded. You can exercise any or a combination of the three options as required in a single step to import computers from the AD domain.



Discover Computers from AD

Step 2: Discover and Import

Securden fetches computers and computer groups from the AD domain specified. 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

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

Verify the Objects Selected for Discovery

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

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

Help

This step is to fetch the required computers, OUs and Groups from the AD domain specified.

This GUI offers the flexibility to fetch computers from OUs/Groups in bulk and even specific computers, 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 computers 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 computers that are part of the OU and Group specified.

For example, if you want to fetch computers 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 computers that are part of the OU and group specified.

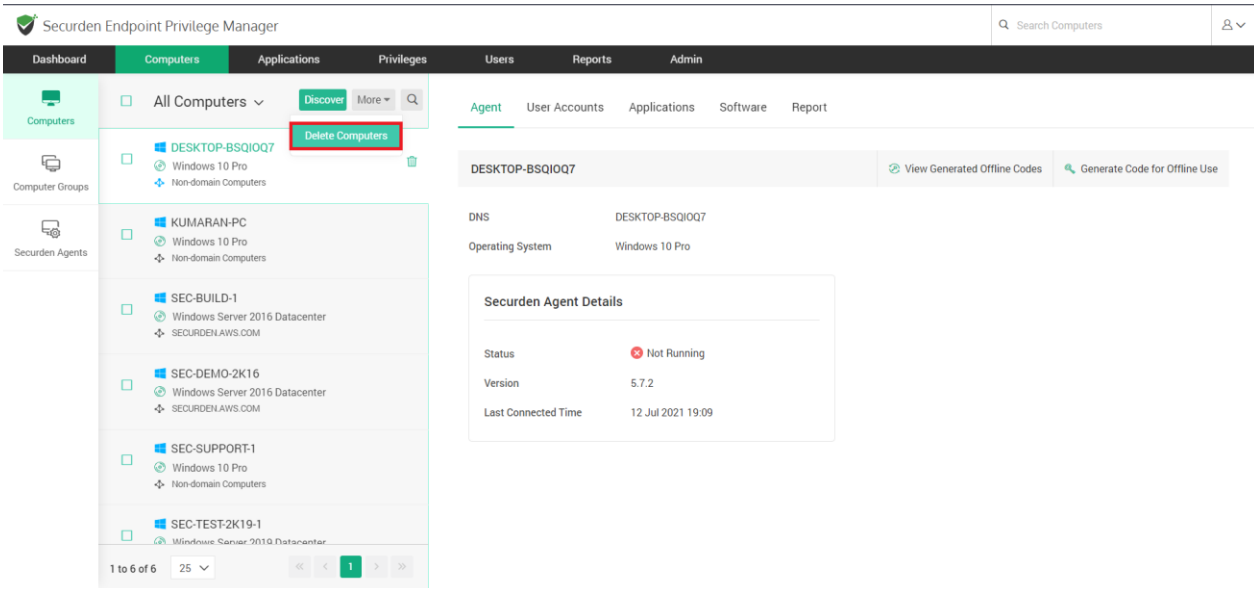
In the advanced settings, you can choose whether to ignore subgroups while importing computer groups. If you choose to ignore subgroups, Securden will still import computers in the subgroup since all computers are a part of the parent group. However, the imported computers will not follow the subgroup structure in Securden.

Once the required computers are onboarded to Securden, you can view them from the **Computers** tab. For computers that don't have an agent installed, the steps to directly push the agent from the Securden UI will be displayed. You need to follow these steps and to install the agent on the device.

Deleting Computers

You can delete computers from Securden by navigating to **Computers** and selecting the computer(s) to be deleted.

To delete the selected computers, click on **More >> Delete**.



DESKTOP-BSQIOQ7
Windows 10 Pro
Non-domain Computers

KUMARAN-PC
Windows 10 Pro
Non-domain Computers

SEC-BUILD-1
Windows Server 2016 Datacenter
SECURDEN.AWS.COM

SEC-DEMO-2K16
Windows Server 2016 Datacenter
SECURDEN.AWS.COM

SEC-SUPPORT-1
Windows 10 Pro
Non-domain Computers

SEC-TEST-2K19-1
Windows Server 2019 Datacenter

DESKTOP-BSQIOQ7

DNS	DESKTOP-BSQIOQ7
Operating System	Windows 10 Pro

Securden Agent Details

Status	Not Running
Version	5.7.2
Last Connected Time	12 Jul 2021 19:09

Computer Groups

Computer Groups are used to place similar computers and organize them with a defined structure and hierarchy. These groups can be used to enforce group control policies in Securden for effective privilege management.

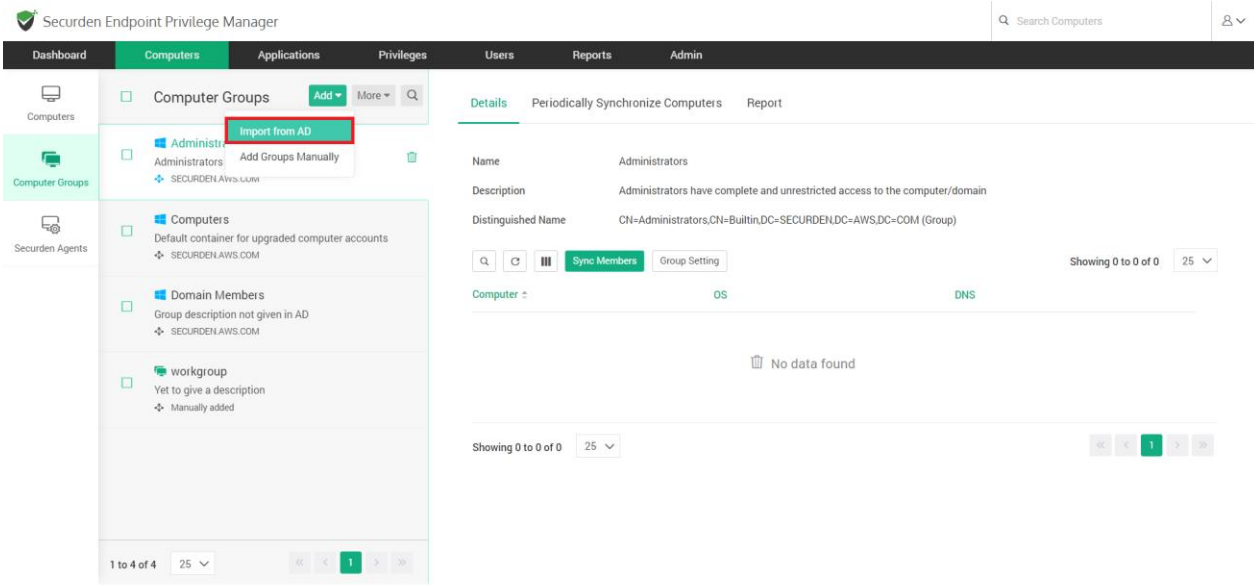
Adding a Computer Group

You can add any number of computer groups in Securden. Adding a computer group can be done in two ways. You can either

1. Import from AD directly (or)
2. Add groups manually.

Importing groups from AD

To import computer groups from AD, navigate to **Computers >> Computer Groups** (In the left side pane) **>> Add >> Import from AD**.



Administra
Administrators
SECURDEN.AWS.COM

Computers
Default container for upgraded computer accounts
SECURDEN.AWS.COM

Domain Members
Group description not given in AD
SECURDEN.AWS.COM

workgroup
Yet to give a description
Manually added

Name	Administrators
Description	Administrators have complete and unrestricted access to the computer/domain
Distinguished Name	CN=Administrators,CN=Builtin,DC=SECURDEN,DC=AWS,DC=COM (Group)

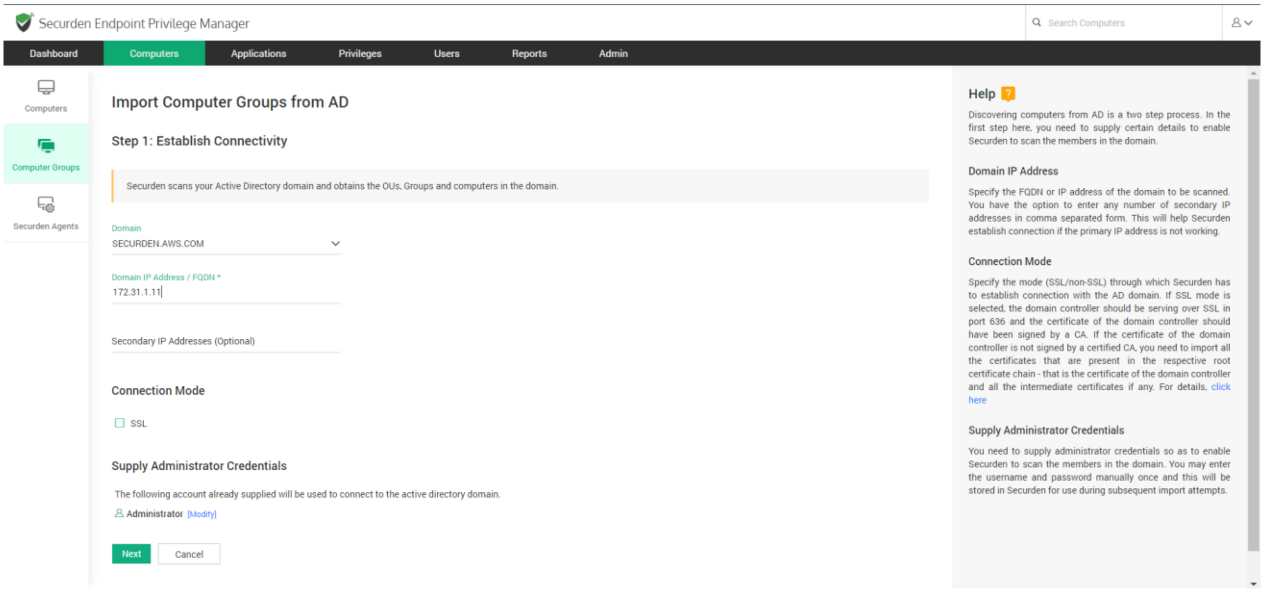
Computer	OS	DNS

No data found

Note: You can add groups to Securden along with computers during the discovery process as well.

In this two-step process, you need to furnish certain details related to the AD so that Securden can establish a connection. After this step is completed, Securden will search for computer groups within the AD and fetch everything discovered. You can then select the computer groups needed and import them to Securden.

Step 1: Establishing AD Connectivity



Import Computer Groups from AD

Step 1: Establish Connectivity

Securden scans your Active Directory domain and obtains the OUs, Groups and computers in the domain.

Domain: SECURDEN.AWS.COM

Domain IP Address / FQDN *: 172.31.1.11

Secondary IP Addresses (Optional)

Connection Mode

□ SSL

Supply Administrator Credentials

The following account already supplied will be used to connect to the active directory domain.

Administrator [Modify]

Help

Discovering computers 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 stored in Securden for use during subsequent import attempts.

You need to specify the domain, domain IP address (or) FQDN, and add secondary IP addresses if needed. Further, you need to specify the connection mode (SSL/non-SSL) through which Securden establishes the connection with the AD domain.

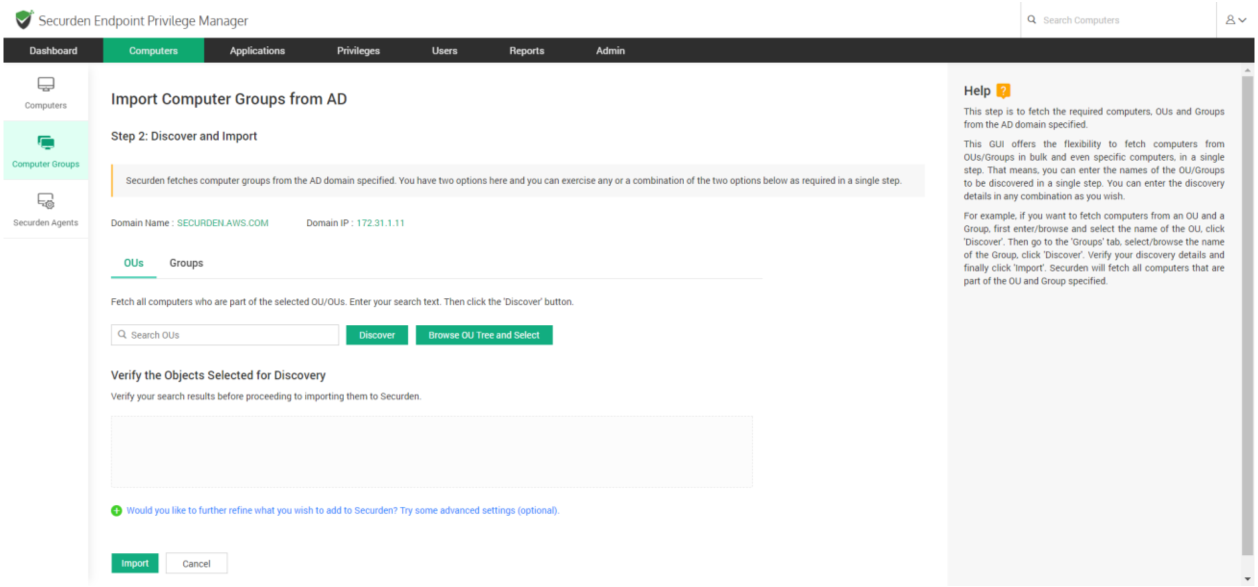
If SSL mode is selected, the domain controller should be serving over SSL in port 636 and the certificate of the domain controller should have been signed by a CA. If a certified CA does not sign the certificate of the domain controller, you need to import all the certificates that are present in the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

You need to supply the administrator credentials to Securden which will be used to authenticate the connection between Securden and the AD domain.

Finally, click **Next**.

Step 2: Select and Import Computer Groups

In the next step, Securden will display all the computer groups and OUs discovered from the AD domain.



Import Computer Groups from AD

Step 2: Discover and Import

Securden fetches computer groups from the AD domain specified. You have two options here and you can exercise any or a combination of the two options below as required in a single step.

Domain Name : SECURDEN.AWS.COM

Domain IP : 172.31.1.11

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

Verify the Objects Selected for Discovery

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

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

Help

This step is to fetch the required computers, OUs and Groups from the AD domain specified.

This GUI offers the flexibility to fetch computers from OUs/Groups in bulk and even specific computers, 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 computers 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 computers that are part of the OU and Group specified.

In this GUI, you have the flexibility to fetch computers from OUs/Groups in bulk in a single step. That means you can enter the names of the OU/Groups to be discovered in any combination as you wish. Once the discovery process is over, you can browse the groups and OU tree and select the required groups.

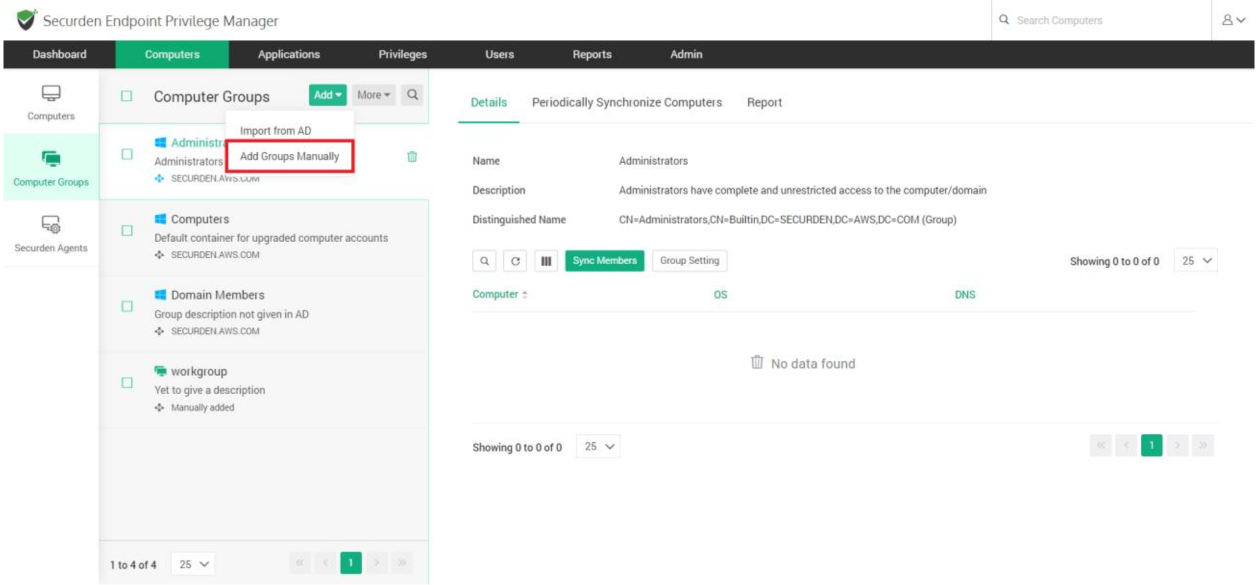
For example, if you want to fetch computers from an OU and a group, first enter/browse and select the name of the OU, click **Discover**. Then go to the **Groups** tab, select/browse the name of the group, and click **Discover**. Verify the selected entities and finally click **Import**. Securden will fetch all computers that are part of the OU and group specified.

In the advanced settings, you can choose whether to ignore subgroups while importing computer groups. If you choose to ignore subgroups, Securden will still import computers in the subgroup and place them inside the first-level group.

Manually Adding Computer Groups

You can create a new computer group in Securden and add specific computers as members to the newly created group. When you need to manage endpoints that are not a part of the domain, you need to onboard the computers and group them as workgroup computers to effectively manage all the endpoints available in your organization.

To manually create a computer group, navigate to **Computers >> Computer Group >> Add >> Add Groups Manually**.



Administrators
Administrators
SECURDEN.AWS.COM

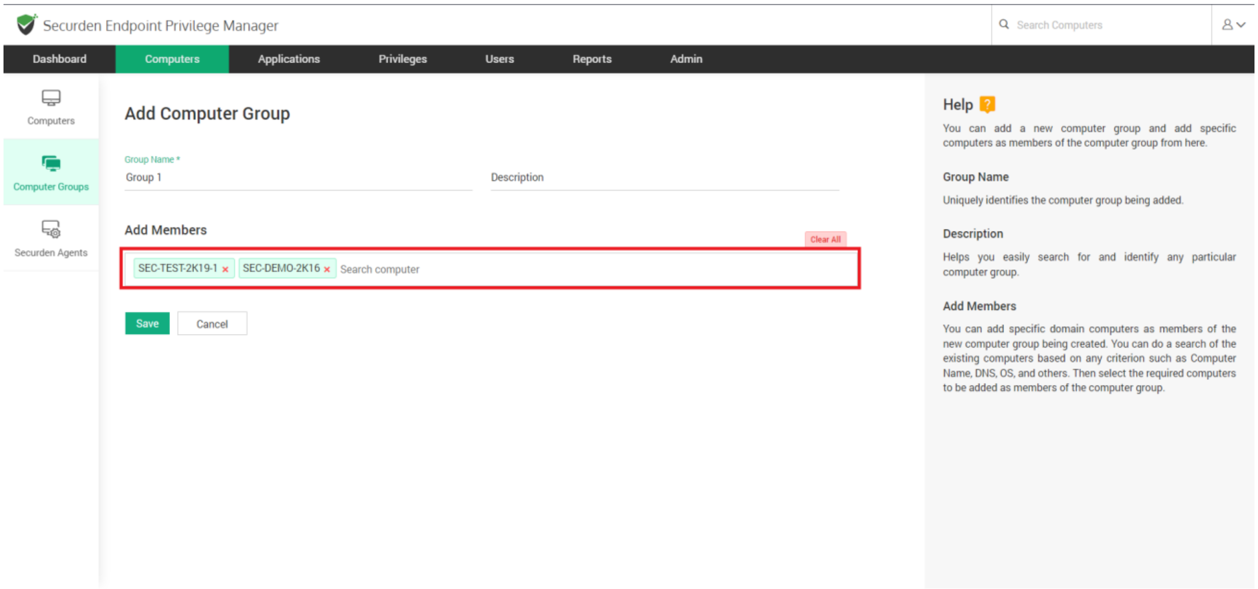
Computers
Default container for upgraded computer accounts
SECURDEN.AWS.COM

Domain Members
Group description not given in AD
SECURDEN.AWS.COM

workgroup
Yet to give a description
Manually added

Name: Administrators
Description: Administrators have complete and unrestricted access to the computer/domain
Distinguished Name: CN=Administrators,CN=Builtin,DC=SECURDEN,DC=AWS,DC=COM (Group)

In the GUI that opens, enter the following details:



Add Computer Group

Group Name *
Group 1

Description

Add Members

SEC-TEST-2K19-1 × SEC-DEMO-2K16 × Search computer

Help

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

Group Name

Uniquely identifies the computer group being added.

Description

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

Add Members

You can add specific domain computers as members of the new computer group being created. You can do a search of the existing computers based on any criterion such as Computer Name, DNS, OS, and others. Then select the required computers to be added as members of the computer group.

You need to provide a suitable group identifier for identification purposes. You can also add a group description to help you easily search and identify particular computer groups.

Add Members

You can add specific domain computers as members of the new computer group being created. You can search the existing computers based on any criteria such as Computer Name, DNS, OS, and others. Then select the required computers to be added as members of the computer group.

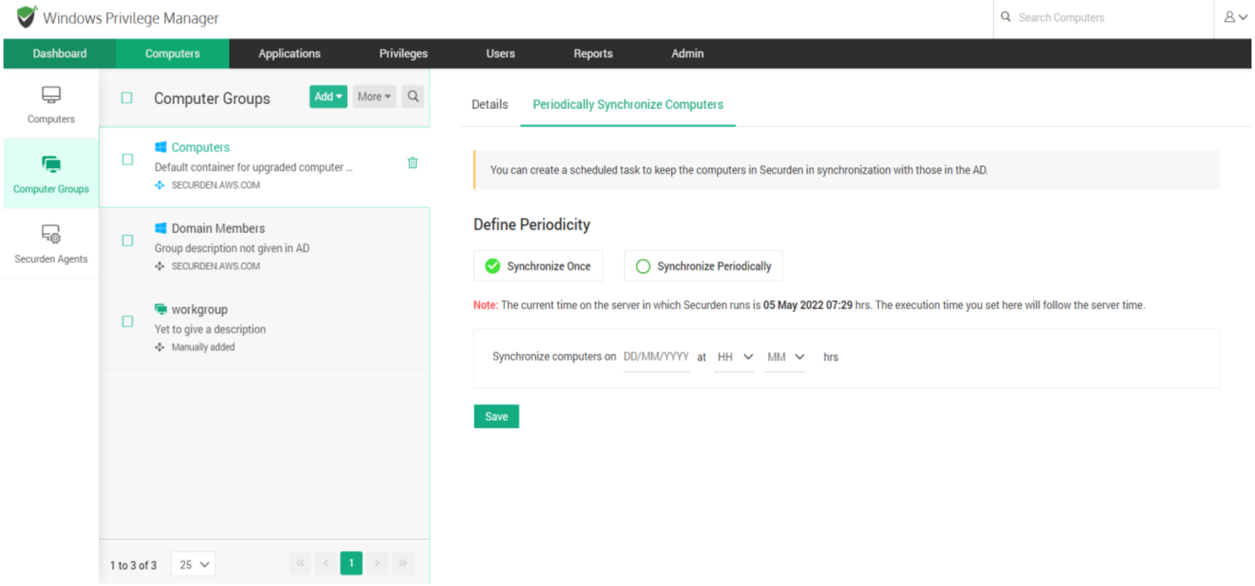
Synchronizing with AD

When a new computer group is created or new changes are made in an existing group, you can update the same in Securden by clicking on **Sync Members** in the **Computer Groups** section. Securden will then run the discovery process again and check for any changes that need to be reflected in Securden.

Additionally, you can schedule tasks in Securden for periodic synchronization with the AD domain. You can either choose to **Synchronize Once** or **Synchronize Periodically**.

The first option is used to schedule the synchronization on a specific date. This is often useful when you are expecting a change to be made in the AD domain soon.

To schedule member synchronization, you need to specify the date and time in the UI.



Computers
Default container for upgraded computer ...
SECURDEN.AWS.COM

Domain Members
Group description not given in AD
SECURDEN.AWS.COM

workgroup
Yet to give a description
Manually added

You can create a scheduled task to keep the computers in Securden in synchronization with those in the AD.

Define Periodicity

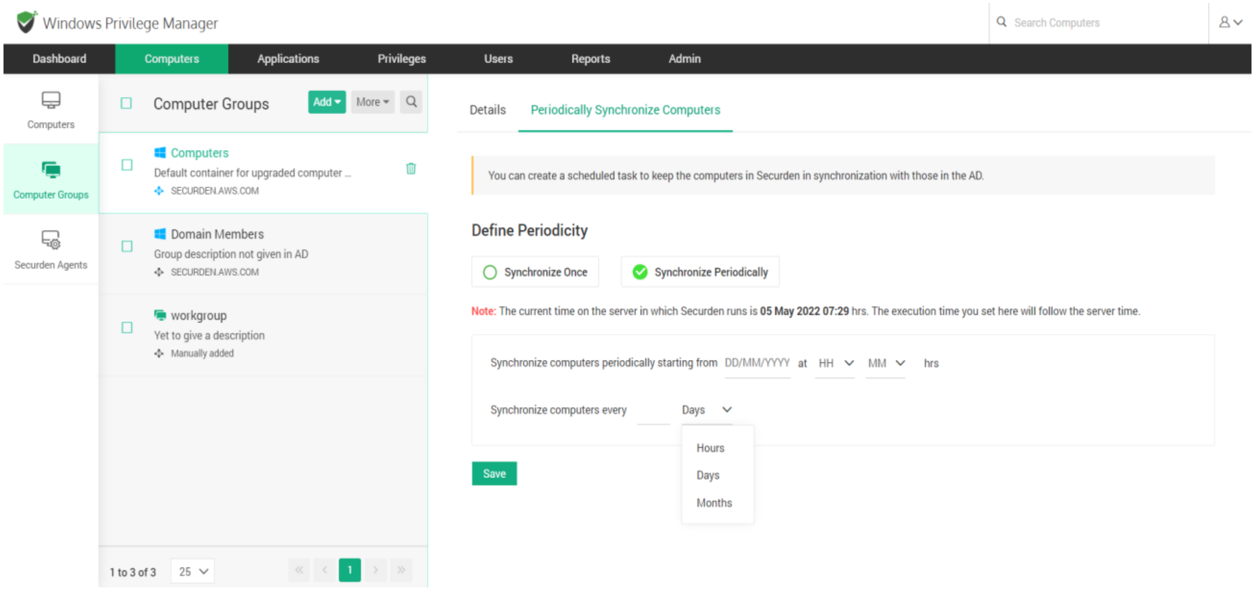
● Synchronize Once ○ Synchronize Periodically

Note: The current time on the server in which Securden runs is **05 May 2022 07:29** hrs. The execution time you set here will follow the server time.

Synchronize computers on DD/MM/YYYY at HH MM hrs

You can also choose to run this synchronization process every few days to ensure that Securden is up-to-date with the changes made in the AD domain.

You need to specify the date and time at which the first synchronization needs to be performed. You should also specify the interval at which subsequent synchronization needs to be executed.



Computers
Default container for upgraded computer ...
SECURDEN.AWS.COM

Domain Members
Group description not given in AD
SECURDEN.AWS.COM

workgroup
Yet to give a description
Manually added

You can create a scheduled task to keep the computers in Securden in synchronization with those in the AD.

Define Periodicity

○ Synchronize Once ● Synchronize Periodically

Note: The current time on the server in which Securden runs is **05 May 2022 07:29** hrs. The execution time you set here will follow the server time.

Synchronize computers periodically starting from DD/MM/YYYY at HH MM hrs

Synchronize computers every Days

Note: The scheduled task will be executed at the specified date and time with respect to the time on the server in which Securden is running. This is displayed in the UI and can be seen while scheduling the task.

Step 2: Discover and Add Applications

The essential aspect of privilege management is elevating the privileges for applications and allowing users to run them whenever required. You can **whitelist** the trusted applications that can be installed/run by standard users with elevated privileges. The term **application** refers to any Windows process/executable. You need to consolidate all your applications prior to creating whitelists and policies.

When you install the Securden agent on Windows workstations and servers, the applications that normally require admin privileges are discovered and added to Securden. You can also manually add applications. You can review the consolidated list and add any other application that needs to be controlled.

Automatic Discovery of Applications

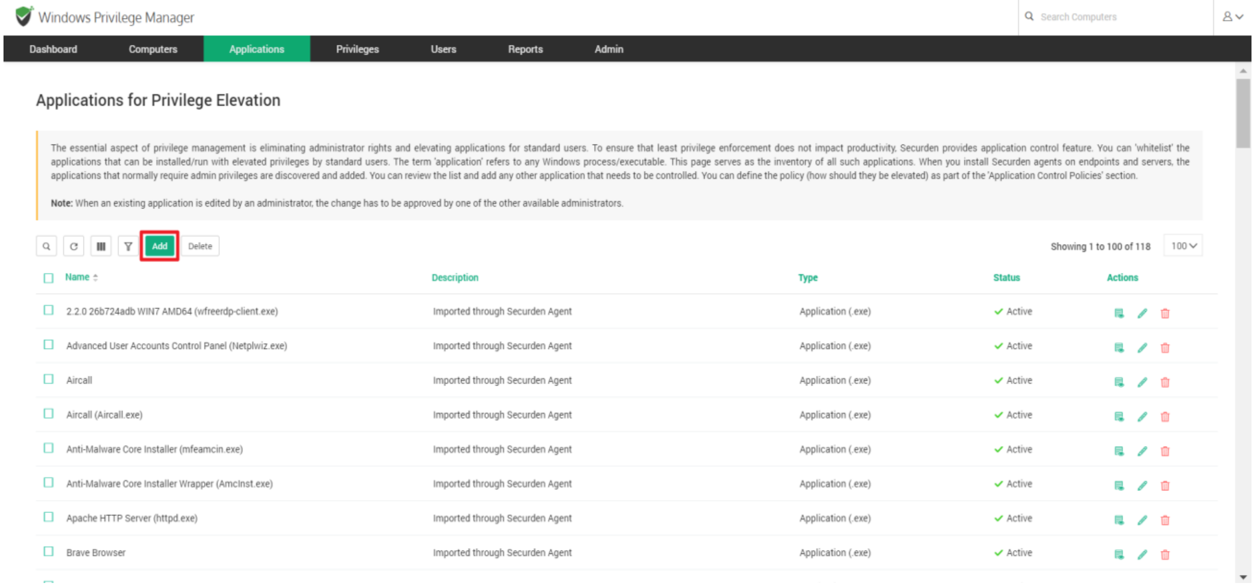
Once you install the Securden agent on the workstations and servers, the agent starts discovering the applications and adds them to the applications inventory.

The discovery process initially would run in learning mode and it takes about a couple of weeks to complete the initial discovery 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 **Applications** section.

Adding Applications Manually

While the automatic discovery takes time, if you want to add applications instantly, you need to manually add them. To add applications, navigate to the **Applications** section in the GUI and click the button **Add**.



Applications for Privilege Elevation

The essential aspect of privilege management is eliminating administrator rights and elevating applications for standard users. To ensure that least privilege enforcement does not impact productivity, Securden provides application control feature. You can 'whitelist' the applications that can be installed/run with elevated privileges by standard users. The term 'application' refers to any Windows process/executable. This page serves as the inventory of all such applications. When you install Securden agents on endpoints and servers, the applications that normally require admin privileges are discovered and added. You can review the list and add any other application that needs to be controlled. You can define the policy (how should they be elevated) as part of the 'Application Control Policies' section.

Note: When an existing application is edited by an administrator, the change has to be approved by one of the other available administrators.

Showing 1 to 100 of 118

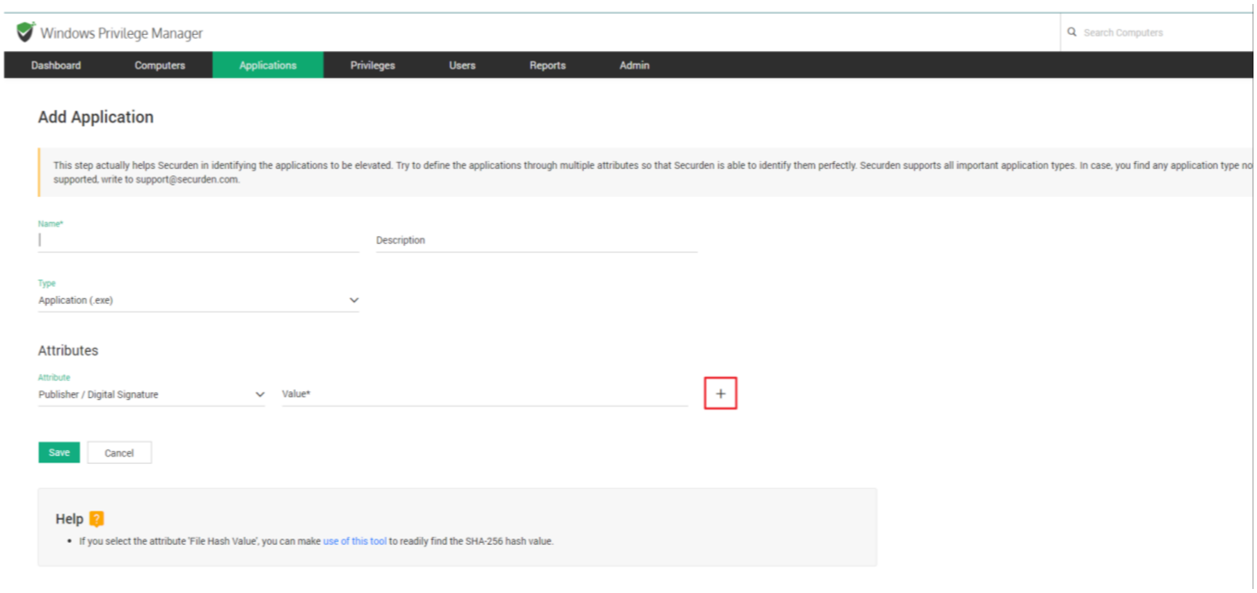
□	Name	Description	Type	Status	Actions
□	2.2.0 26b724adb WIN7 AMD64 (wfreerdp-client.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Advanced User Accounts Control Panel (Netplwiz.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Aircall	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Aircall (Aircall.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Anti-Malware Core Installer (mfeamcin.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Anti-Malware Core Installer Wrapper (Amclnst.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Apache HTTP Server (httpd.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Brave Browser	Imported through Securden Agent	Application (.exe)	✓ Active	

In the GUI that opens, you need to specify the type of application (exe/msi/msc, etc.) and the attributes that would help Securden identify the application.

The application types are as follows:

- **Application (.exe)**
- **Windows Installer (.msi)**
- **Management Console (.msc)**
- **PowerShell Script (.ps1)**
- **VB Script (.vbs)**
- **Batch File (.bat)**
- **Securden Text Editor -** To allow editing of text using Securden's text editor
- **Control Panel file (.cpl)**
- **Write to Folder:** To restrict users from accessing (or) modifying the contents of a specific folder. Some folders might hold configuration files and other sensitive information.

After selecting the application type, you need to specify the attributes that would help the Securden agent to identify the applications properly. The attributes could be digital signatures, actual file path, original file name, and the hash value of files. You may provide any number of attributes as desired by using the option shown below.



Add Application

This step actually helps Securden in identifying the applications to be elevated. Try to define the applications through multiple attributes so that Securden is able to identify them perfectly. Securden supports all important application types. In case, you find any application type no supported, write to support@securden.com.

Name*

Description

Type: Application (.exe)

Attributes

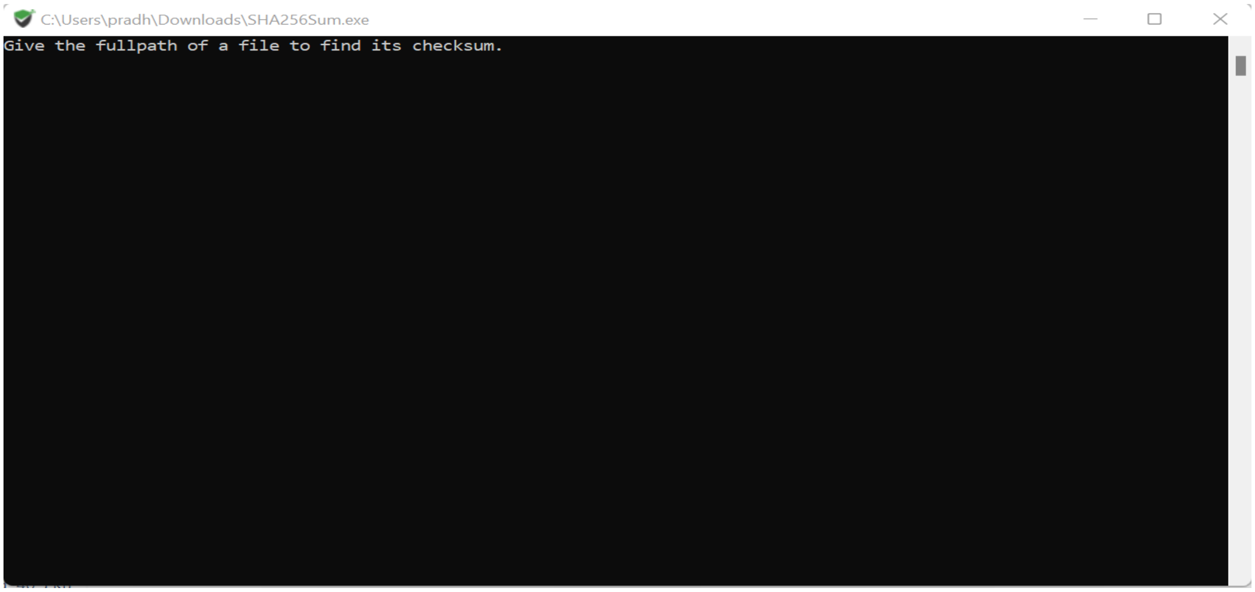
Attribute: Publisher / Digital Signature

Value*

Help

- If you select the attribute 'File Hash Value', you can make use of this tool to readily find the SHA-256 hash value.

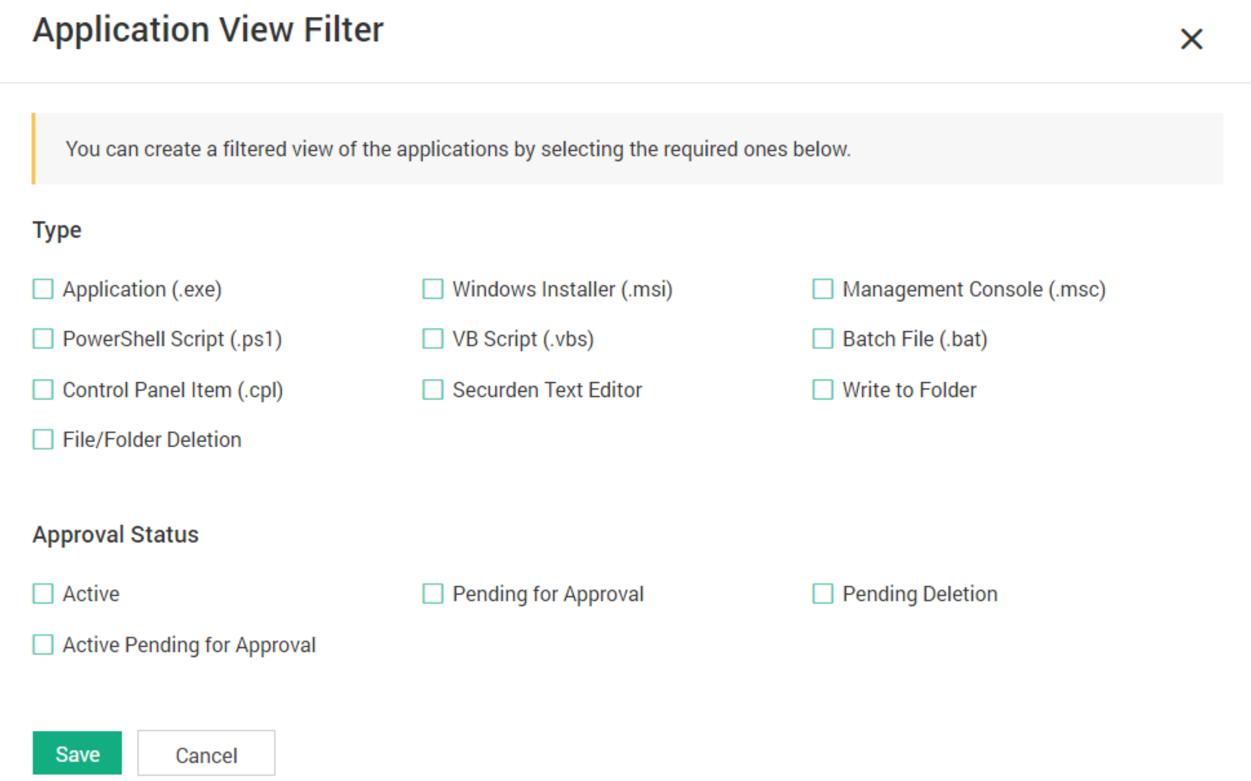
Note: If you choose the attribute **File Hash Value**, you can make use of the application provided in the UI to readily find the SHA-256 value for the application. To find the file hash value, you need to specify the exact file location of the application.



```
Give the fullpath of a file to find its checksum.
```

Searching Applications

You can use the filter and choose the type of applications you want to look at. **Column chooser** helps you search for specific information in each column while the **Filter** helps in displaying applications with specific attributes. You can select any number of attributes when using the filter to effectively search for the required application.



Application View Filter

You can create a filtered view of the applications by selecting the required ones below.

Type

□ Application (.exe)
□ Windows Installer (.msi)
□ Management Console (.msc)
□ PowerShell Script (.ps1)
□ VB Script (.vbs)
□ Batch File (.bat)
□ Control Panel Item (.cpl)
□ Securden Text Editor
□ Write to Folder
□ File/Folder Deletion

Approval Status

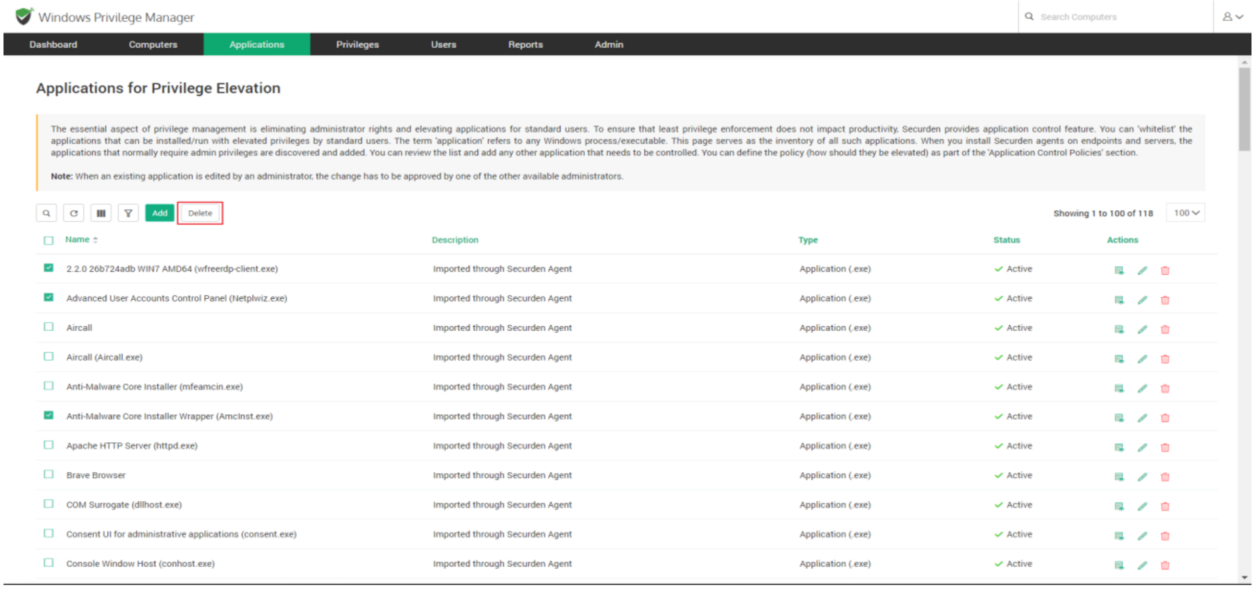
□ Active
□ Pending for Approval
□ Pending Deletion
□ Active Pending for Approval

Editing and Deleting Applications

Attributes of applications previously added to Securden can be modified whenever required. However, any changes made to the applications need to be reviewed and approved by other administrators.

You can remove applications from the list at any time. Once you remove an application from the list, Securden will not automatically rediscover the same application. If you need to add the application back to the list, you have to manually do it.

To remove applications, select the required applications and click **Delete**.



Applications for Privilege Elevation

The essential aspect of privilege management is eliminating administrator rights and elevating applications for standard users. To ensure that least privilege enforcement does not impact productivity, Securden provides application control feature. You can 'whitelist' the applications that can be installed/run with elevated privileges by standard users. The term 'application' refers to any Windows process/executable. This page serves as the inventory of all such applications. When you install Securden agents on endpoints and servers, the applications that normally require admin privileges are discovered and added. You can review the list and add any other application that needs to be controlled. You can define the policy (how should they be elevated) as part of the 'Application Control Policies' section.

Note: When an existing application is edited by an administrator, the change has to be approved by one of the other available administrators.

Showing 1 to 100 of 118 100

□	Name	Description	Type	Status	Actions
☑	2.2.0 26b724adb WIN7 AMD64 (wfreerdp-client.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
☑	Advanced User Accounts Control Panel (Netplwiz.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Aircall	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Aircall (Aircall.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Anti-Malware Core Installer (mfeamcin.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
☑	Anti-Malware Core Installer Wrapper (Amcinst.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Apache HTTP Server (httpd.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Brave Browser	Imported through Securden Agent	Application (.exe)	✓ Active	
□	COM Surrogate (dllhost.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Consent UI for administrative applications (consent.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	
□	Console Window Host (conhost.exe)	Imported through Securden Agent	Application (.exe)	✓ Active	

For example, in the image displayed above, the three selected applications will be deleted once you click **Delete**.

Step 3: Define Application Control Policies (Whitelist/Blacklist Applications)

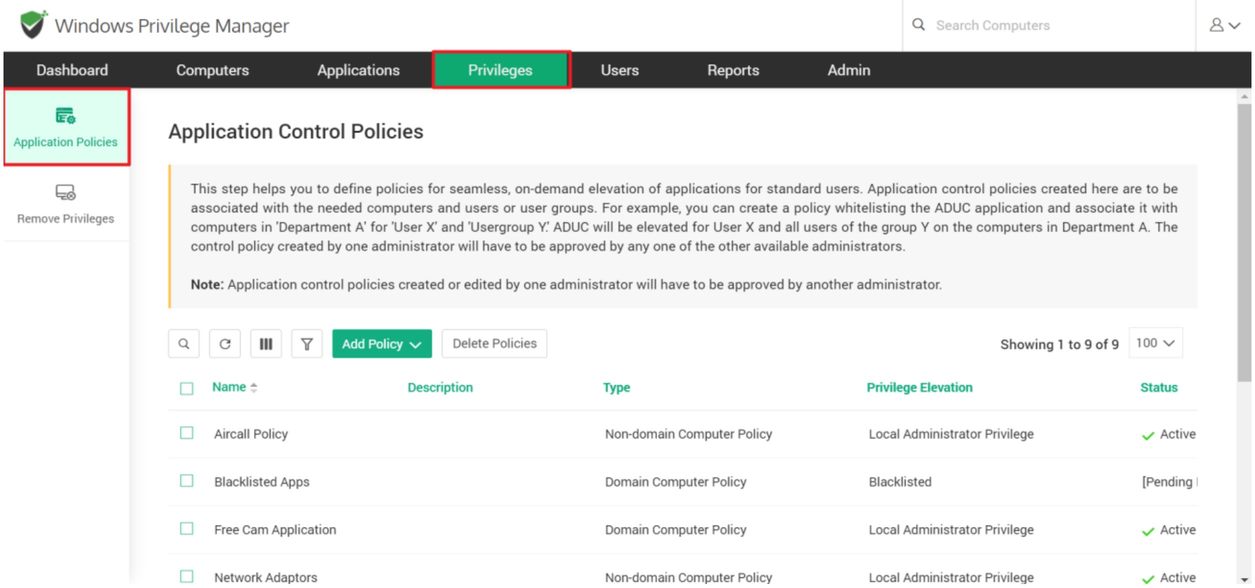
This step helps you to define policies for the seamless, on-demand elevation of applications for standard users. Control policies created here are to be associated with the required computers and users or user groups. For example, you can create a policy whitelisting the ADUC application and associate 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 any one of the other available administrators.

Configure an application control policy

Prerequisite: Deploy agents on all the required endpoints to discover and populate the endpoints in Securden. Let the agents discover applications that require administrator privileges on endpoints and list them in Securden.

Navigate to **Privileges>>Application Control Policies**



Application Control Policies

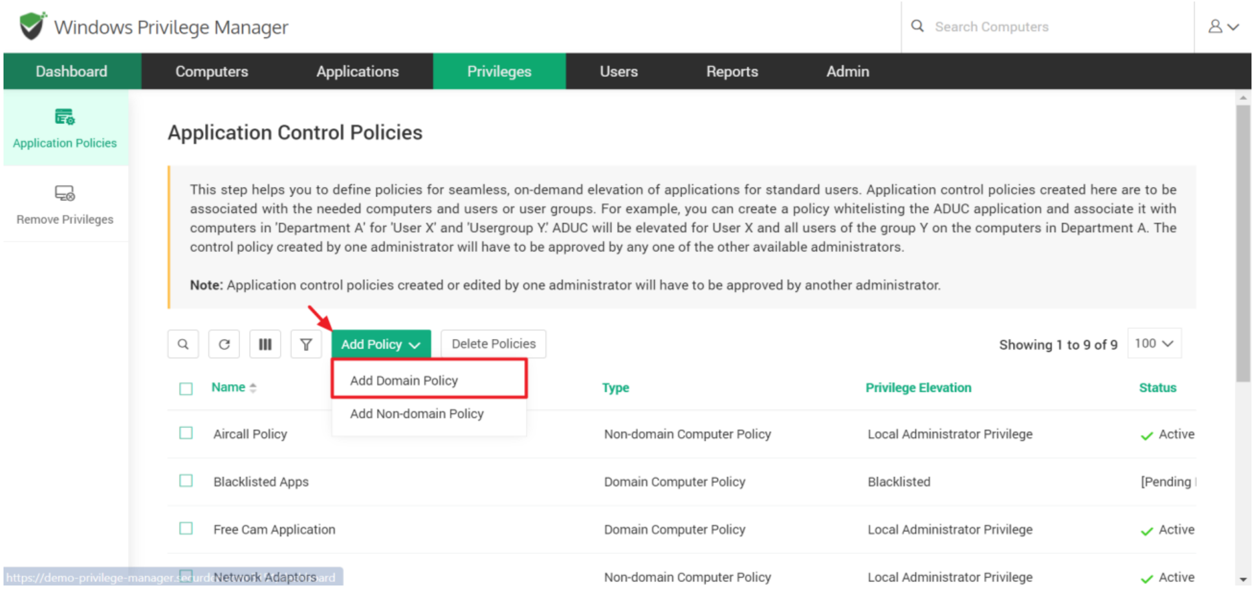
This step helps you to define policies for seamless, on-demand elevation of applications for standard users. Application control policies created here are to be associated with the needed computers and users or user groups. For example, you can create a policy whitelisting the ADUC application and associate 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 any one of the other available administrators.

Note: Application control policies created or edited by one administrator will have to be approved by another administrator.

□	Name	Description	Type	Privilege Elevation	Status
□	Aircall Policy		Non-domain Computer Policy	Local Administrator Privilege	✓ Active
□	Blacklisted Apps		Domain Computer Policy	Blacklisted	[Pending
□	Free Cam Application		Domain Computer Policy	Local Administrator Privilege	✓ Active
□	Network Adaptors		Non-domain Computer Policy	Local Administrator Privilege	✓ Active

Adding a Domain-policy

You can create and use domain policies to control application usage on domain joined computers. While creating domain policies, you can associate the policy with domain joined computers and domain users. To create a domain policy, navigate to **Privileges >> Application Policies**, click on **Add Policy** and select **Add Domain Policy**.



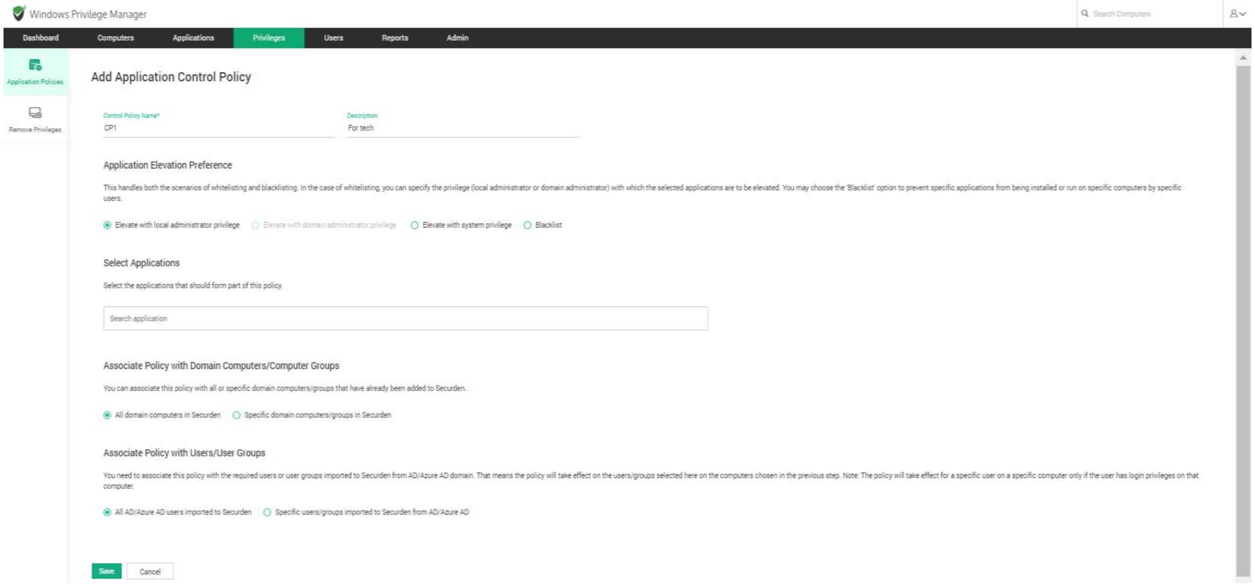
Application Control Policies

This step helps you to define policies for seamless, on-demand elevation of applications for standard users. Application 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 any one of the other available administrators.

Note: Application control policies created or edited by one administrator will have to be approved by another administrator.

Name	Type	Privilege Elevation	Status
Aircall Policy	Non-domain Computer Policy	Local Administrator Privilege	✓ Active
Blacklisted Apps	Domain Computer Policy	Blacklisted	[Pending
Free Cam Application	Domain Computer Policy	Local Administrator Privilege	✓ Active
Network Adaptors	Non-domain Computer Policy	Local Administrator Privilege	✓ Active

Enter the following details in this GUI.



Add Application Control Policy

Control Policy Name*: CP1

Description: For tech

Application Elevation Preference

This handles both the scenarios of whitelisting and blacklisting. In the case of whitelisting, you can specify the privilege (local administrator or domain administrator) with which the selected applications are to be elevated. You may choose the 'Blacklist' option to prevent specific applications from being installed or run on specific computers by specific users.

● 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.

Associate Policy with Domain Computers/Computer Groups

You can associate this policy with all or specific domain computers/groups that have already been added to Securden.

● All domain computers in Securden ○ Specific domain computers/groups in Securden

Associate Policy with Users/User Groups

You need to associate this policy with the required users or user groups imported to Securden from AD/Azure AD domain. That means the policy will take effect on the users/groups selected here on the computers chosen in the previous step. Note: The policy will take effect for a specific user on a specific computer only if the user has login privileges on that computer.

● All AD/Azure AD users imported to Securden ○ Specific users/groups imported to Securden from AD/Azure AD

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: A brief explaining the purpose of the application control policy.

Application Elevation Preference

- **Elevate with local admin privilege:** You can run the application with local admin rights, this means the app elevated can make use of admin rights to configure system settings
- **Elevate with domain admin privilege:** Domain administrators are a part of local administrator group of all domain joined devices. This privilege can be used to allow the user to run domain apps such as domain tree etc.
- **Elevate with system privilege:** You can run processes and scheduled tasks without the user intervention by elevating with system administrator privilege.
- **Blacklist:** Blacklist works purely to stop certain applications from running. This is done in case your policy requires you to block specific applications.

Select Applications

Your policy allows you to choose the applications that will run under the selected elevated privileges. If you have chosen blacklist then these applications will be prohibited from running.

You can use the **Search application** field to select the application from the list, or enter the application name and select it. Now that the applications for the policy are selected, you can associate them with the required users, and computers.

Associate Policy with Domain Computers/Computer Groups

You can choose to have all domain computers follow this policy, or choose a specific set of computers to adhere to it. To associate selective computers with the policy, you can enable the **Specific domain computers/groups** option and choose the computers from the drop down which will be running with this policy.

Associate policy with Users/User Groups

This step lets you granularly select specific domain users and user groups and associate this application control policy with the selected users.

- To associate the policy with all domain users enable **All users**.
- To select individual users or groups, use the **Include specific user/groups** and choose from the list of users/groups.
- To associate this policy with all users except a select few, you can select **Exclude specific user/groups** and choose from the list of users/groups.

Once the preferences are selected, click **Save**.

On completing this step, the control policy will be created and sent to review. It will take effect after it is reviewed and approved by a fellow administrator. Once it is in effect, it will be listed on the control policies page.

Add a non-domain policy

To add a non-domain policy, you can follow the same steps as given above for the domain policy, the only difference here is that non-domain policy cannot be associated with AD domain users. However, you may associate a non-domain policy with Azure AD users and local users on endpoints.

Once you select the required elevation preference, and the applications, you need to associate the policy with the required computers and users.

You have two options when associating with computers. You can either choose to associate the policy with all non-domain computers in the inventory or choose specific non-domain endpoints.

Similarly, you can choose to associate the policy with all local users and Azure AD users or specify individual users and groups.

Once all the required preferences have been selected, you may click on **Save**.

Step 4: Remove Local Admin Rights

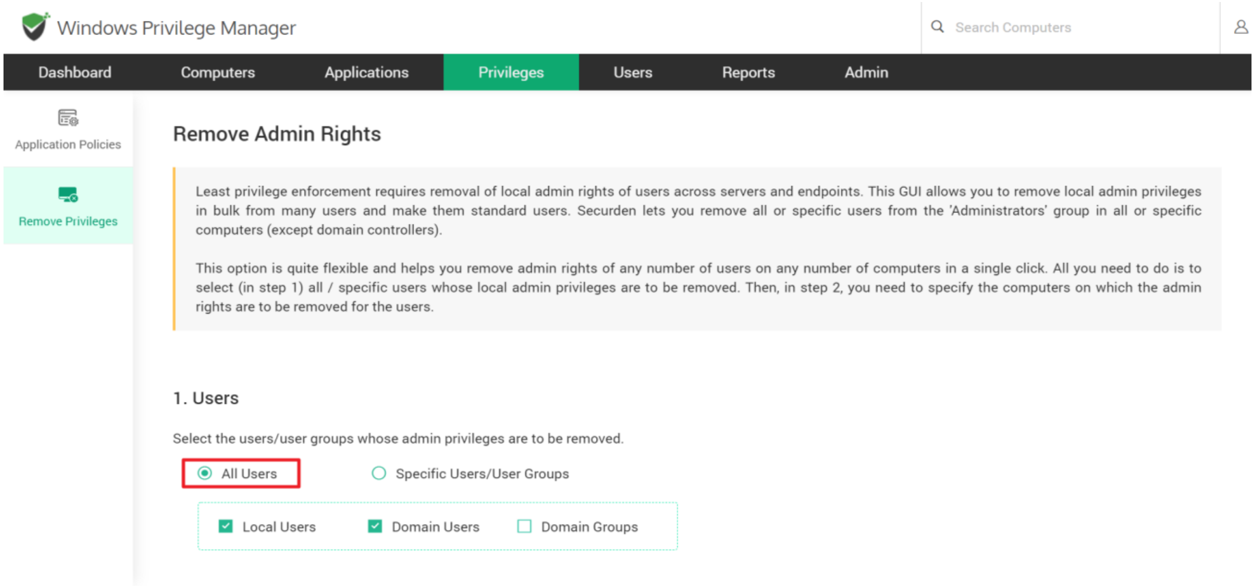
Along with the device discovery, the Securden agent captures the list of local administrator accounts on each computer. This GUI allows you to remove local admin privileges in bulk from many users and make them standard users. Securden lets you remove all or specific users from the **Administrators** group in all or specific computers (except domain controllers). 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.

To remove the local admin accounts, navigate to **Privileges >> Remove Privileges** in the GUI.

- **Step 1:** Select all the specific users/user groups whose local admin privileges are to be removed.
- **Step 2:** Specify the computers on which the admin rights are to be removed for users selected in step 1.

Select The users/user groups

On clicking **All Users**, you have the option to select **Local Users**, **Domain Users**, or **Users in Domain Groups**. You can select all three of them to include every user.



Remove Admin Rights

Least privilege enforcement requires removal of local admin rights 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. Securden lets you remove all or specific users from the 'Administrators' group in all or specific computers (except domain controllers).

This option is quite flexible and helps you remove admin rights of any number of users on any number of computers in a single click. All you need to do is to select (in step 1) all / specific users whose local admin privileges are to be removed. Then, in step 2, you need to specify the computers on which the admin rights are to be removed for the users.

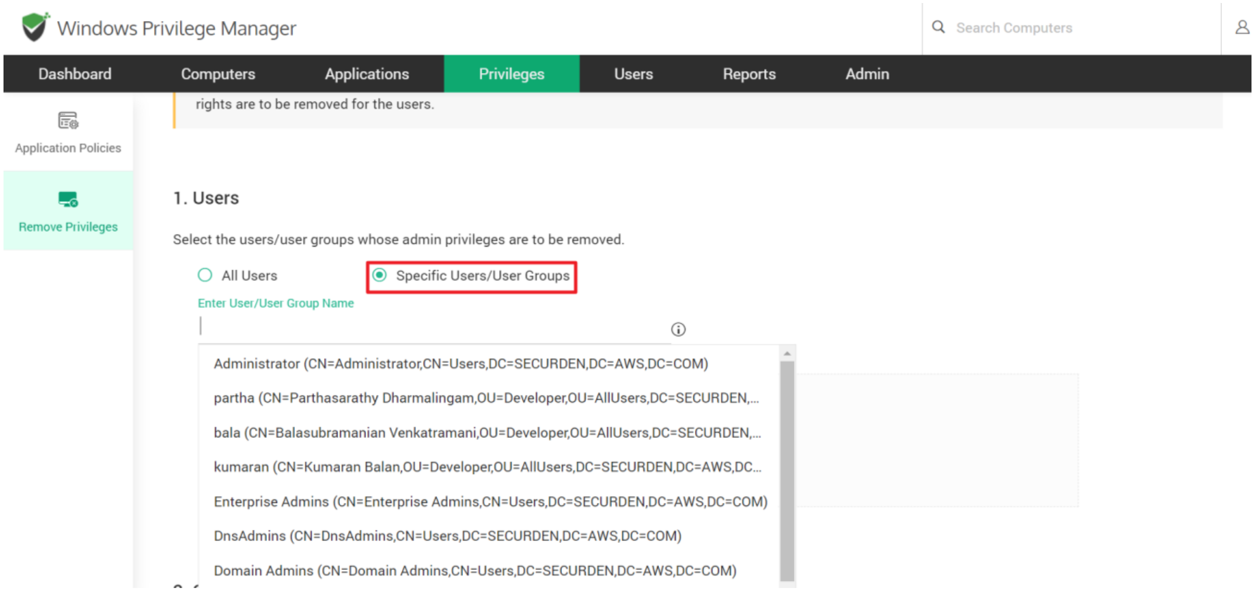
1. Users

Select the users/user groups whose admin privileges are to be removed.

● All Users ○ Specific Users/User Groups

☑ Local Users ☑ Domain Users □ Domain Groups

On clicking **Specific Users/User Groups**, you have the option to select individual users or user groups from the drop-down.



rights are to be removed for the users.

1. Users

Select the users/user groups whose admin privileges are to be removed.

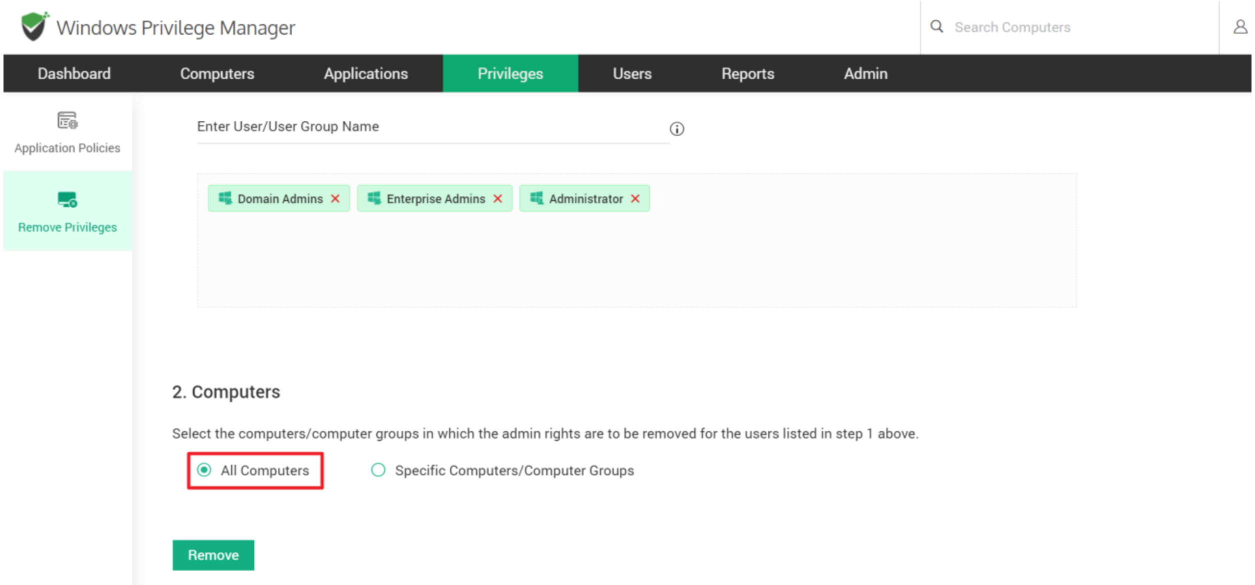
○ All Users ● Specific Users/User Groups

Enter User/User Group Name

Administrator (CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM)
partha (CN=Parthasarathy Dharmalingam,OU=Developer,OU=AllUsers,DC=SECURDEN,...
bala (CN=Balasubramanian Venkatramani,OU=Developer,OU=AllUsers,DC=SECURDEN,...
kumaran (CN=Kumaran Balan,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC...
Enterprise Admins (CN=Enterprise Admins,CN=Users,DC=SECURDEN,DC=AWS,DC=COM)
DnsAdmins (CN=DnsAdmins,CN=Users,DC=SECURDEN,DC=AWS,DC=COM)
Domain Admins (CN=Domain Admins,CN=Users,DC=SECURDEN,DC=AWS,DC=COM)

Select Computers/Computer groups

To include every computer, click **All Computers**.



Enter User/User Group Name

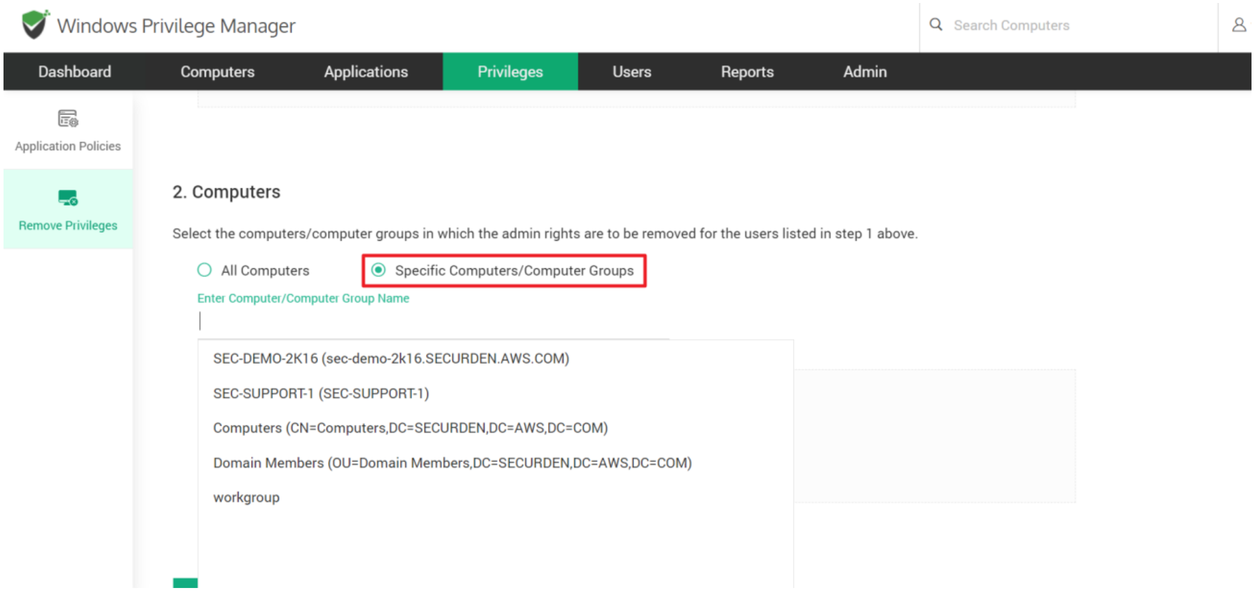
Domain Admins ✕ Enterprise Admins ✕ Administrator ✕

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

On clicking **Specific Computers/Computer Groups**, you have the option to select individual computers or computer groups from the drop-down.



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

SEC-DEMO-2K16 (sec-demo-2k16.SECURDEN.AWS.COM)

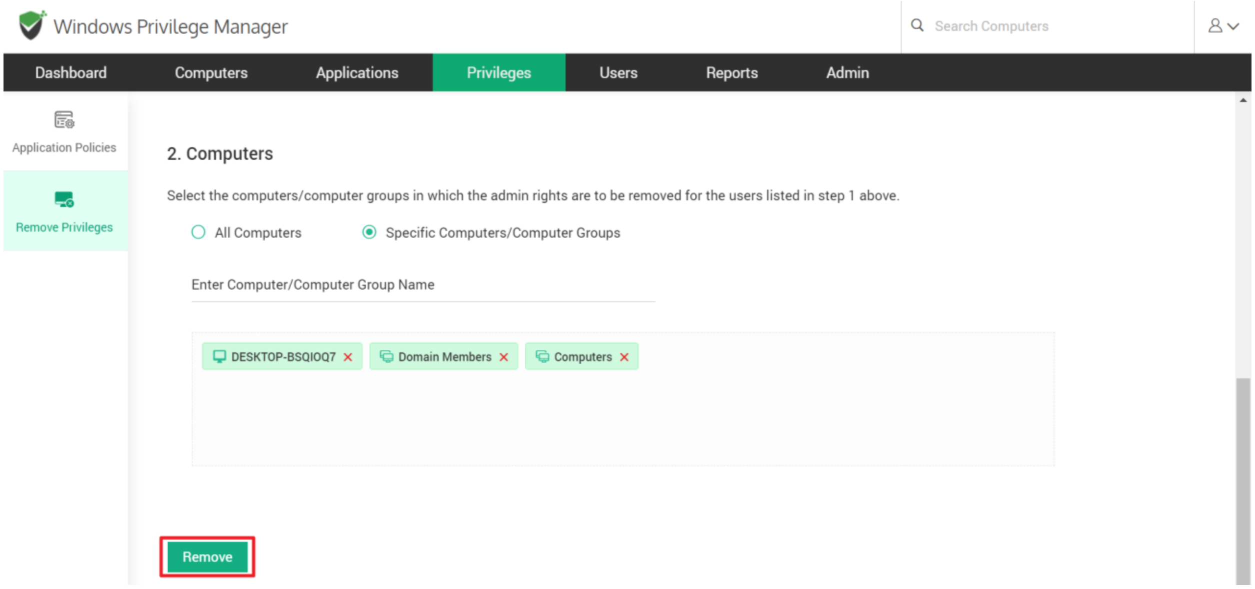
SEC-SUPPORT-1 (SEC-SUPPORT-1)

Computers (CN=Computers,DC=SECURDEN,DC=AWS,DC=COM)

Domain Members (OU=Domain Members,DC=SECURDEN,DC=AWS,DC=COM)

workgroup

On selecting the required users and computers, click on **Proceed**.



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

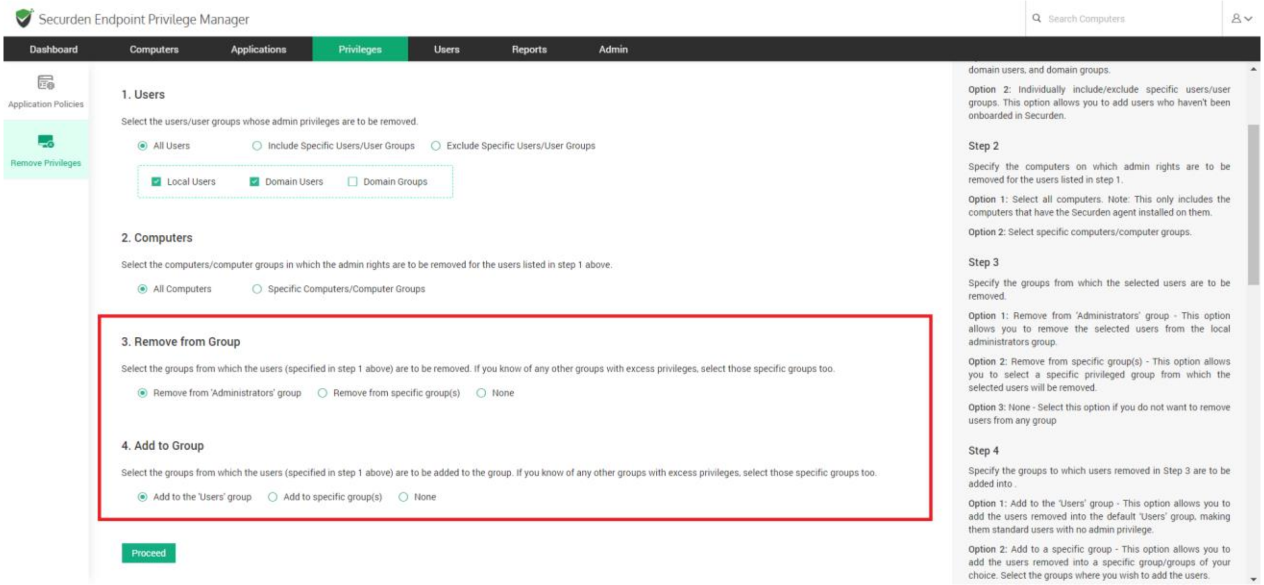
DESKTOP-BSQIOQ7 ✕ Domain Members ✕ Computers ✕

On clicking **Proceed**, all the computers/computer groups selected will be accessible without administrative rights for the users/user groups selected.

Move Users from One Group to Another

In addition to removing users from the administrator groups, Securden allows you to move an user from any one group to another. To explore this option, click on **Would you like to remove users from one group and add them to a different group? Explore the advanced settings (Optional).**

Once you click this, you will be able to see the options displayed below.



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

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

4. Add to Group

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.

● Add to the 'Users' group ○ Add to specific group(s) ○ None

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 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.

You need to select the group from which the user(s) needs to be removed and the group to which they need to be added.

Once you have selected your preferences, click **Proceed**.

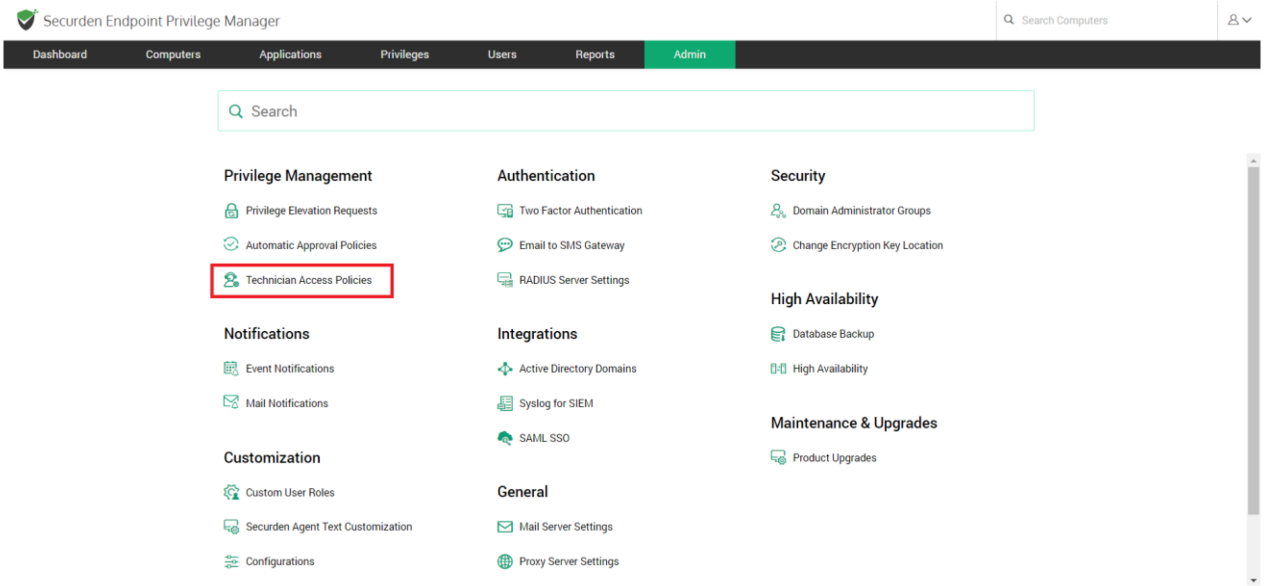
Technician Access Policies

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.

Creating technician access policies

To create a technician access policy, navigate to **Admin>> Privilege Management >> Technician Access Policies**



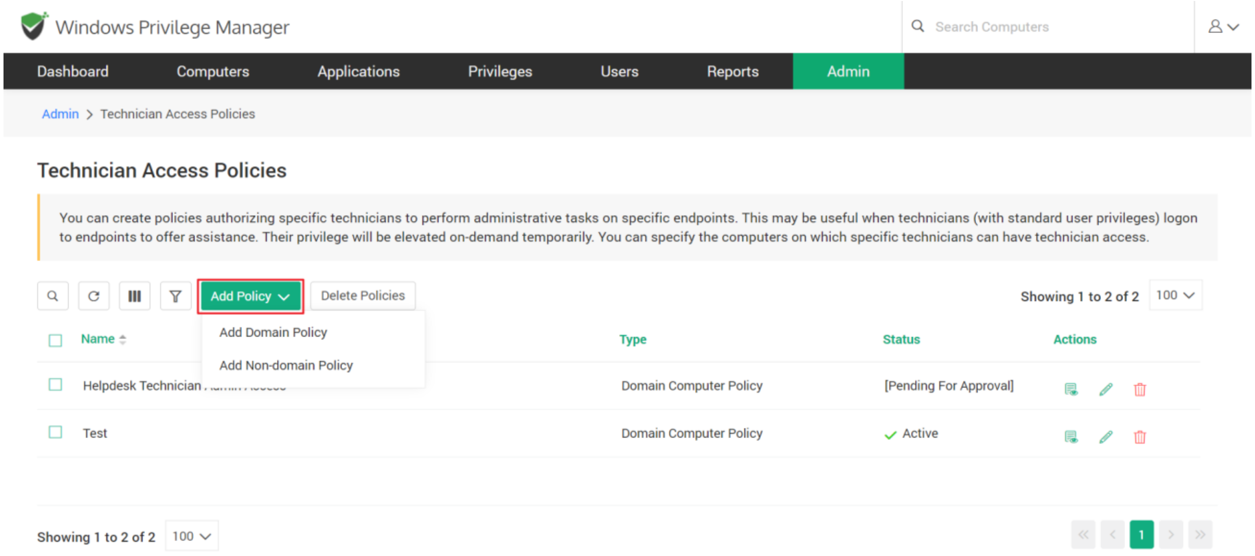
You need to create policies for domain-joined computers and non-domain computers separately. When creating the policy, you need to select **Domain Policy** or **Non-domain Policy** as required.

Steps to create a technician access 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 **Add Non-domain Policy** as needed.

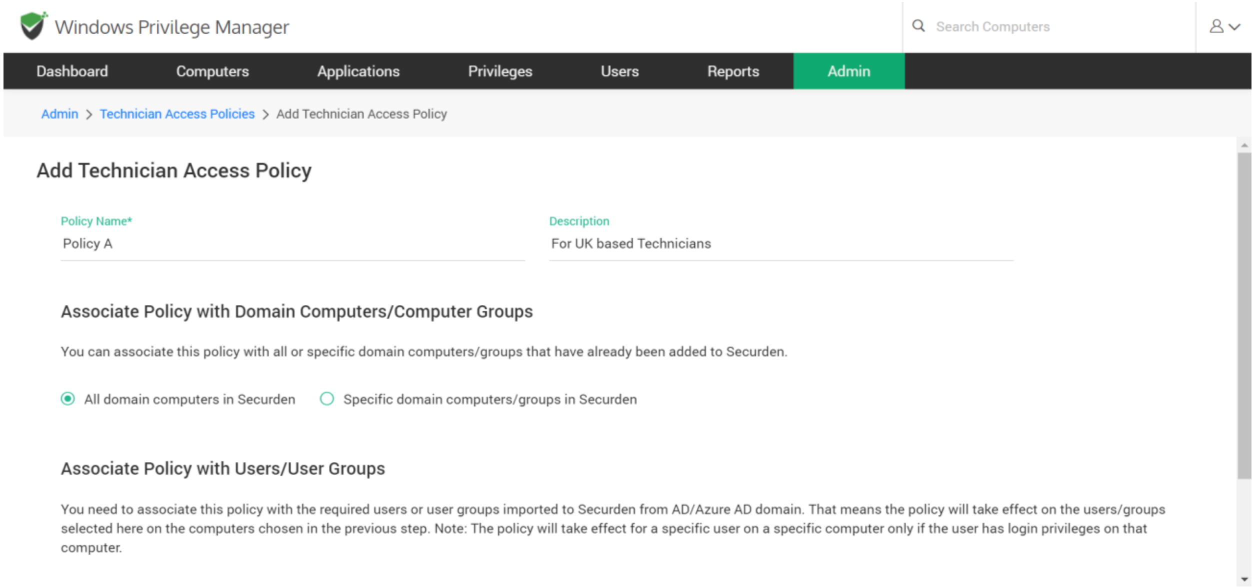


Technician Access Policies

You can create policies authorizing specific technicians to perform administrative tasks on specific endpoints. This may be useful when technicians (with standard user privileges) logon to endpoints to offer assistance. Their privilege will be elevated on-demand temporarily. You can specify the computers on which specific technicians can have technician access.

	Name	Type	Status	Actions
□	Helpdesk Technician Admin Access	Domain Computer Policy	[Pending For Approval]	
□	Test	Domain Computer Policy	✓ Active	

In the GUI that opens, enter the following information:


Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Technician Access Policies > Add Technician Access Policy

Add Technician Access Policy

Policy Name*: Policy A

Description: For UK based Technicians

Associate Policy with Domain Computers/Computer Groups

You can associate this policy with all or specific domain computers/groups that have already been added to Securden.

● All domain computers in Securden ○ Specific domain computers/groups in Securden

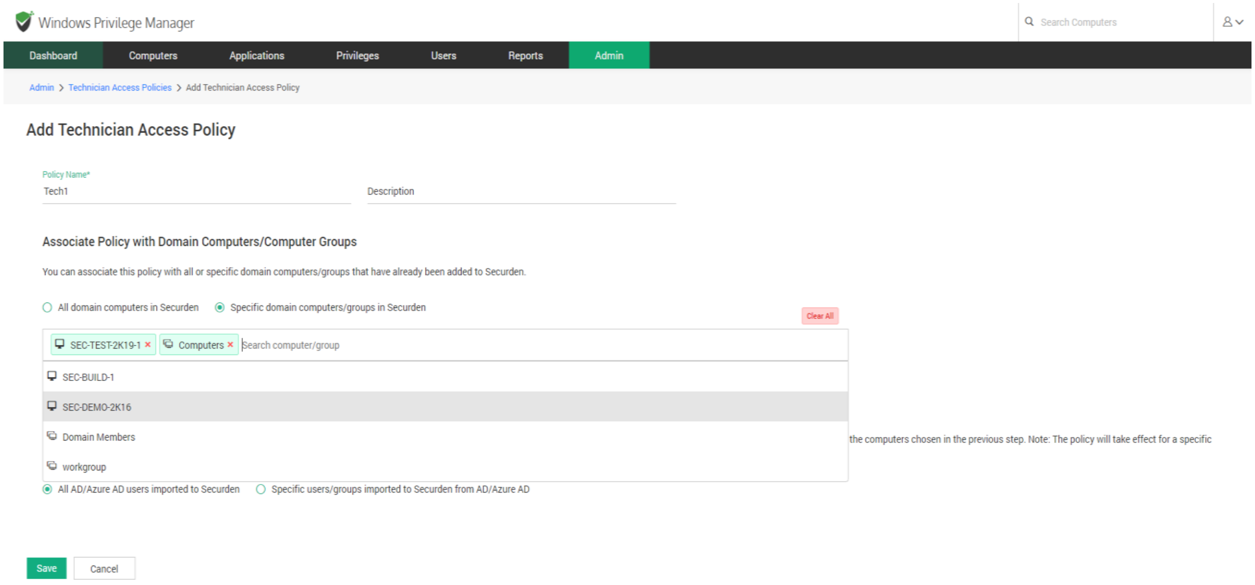
Associate Policy with Users/User Groups

You need to associate this policy with the required users or user groups imported to Securden from AD/Azure AD domain. That means the policy will take effect on the users/groups selected here on the computers chosen in the previous step. Note: The policy will take effect for a specific user on a specific computer only if the user has login privileges on that computer.

- **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

The next step would be to associate the policy with all computers or specific computers in the domain. The computers associated with this policy will allow technicians to access them with ease.

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.


Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Technician Access Policies > Add Technician Access Policy

Add Technician Access Policy

Policy Name*: Tech1

Description

Associate Policy with Domain Computers/Computer Groups

You can associate this policy with all or specific domain computers/groups that have already been added to Securden.

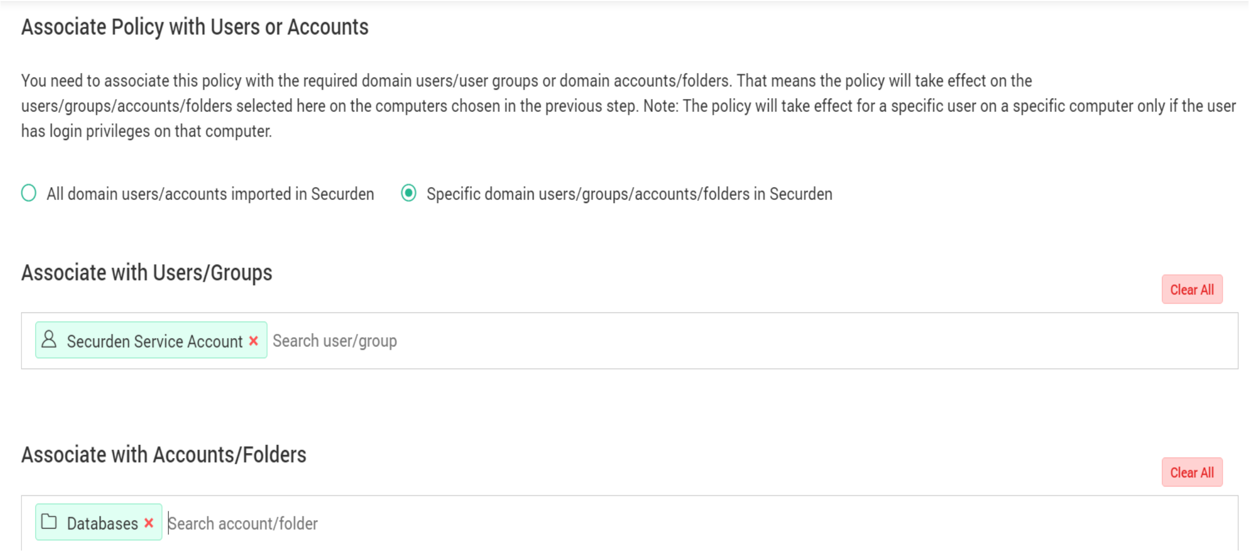
○ All domain computers in Securden ● Specific domain computers/groups in Securden

the computers chosen in the previous step. Note: The policy will take effect for a specific

● All AD/Azure AD users imported to Securden ○ Specific users/groups imported to Securden from AD/Azure AD

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 in Securden to access the computers selected in the previous step.



Associate Policy with Users or Accounts

You need to associate this policy with the required domain users/user groups or domain accounts/folders. That means the policy will take effect on the users/groups/accounts/folders selected here on the computers chosen in the previous step. Note: The policy will take effect for a specific user on a specific computer only if the user has login privileges on that computer.

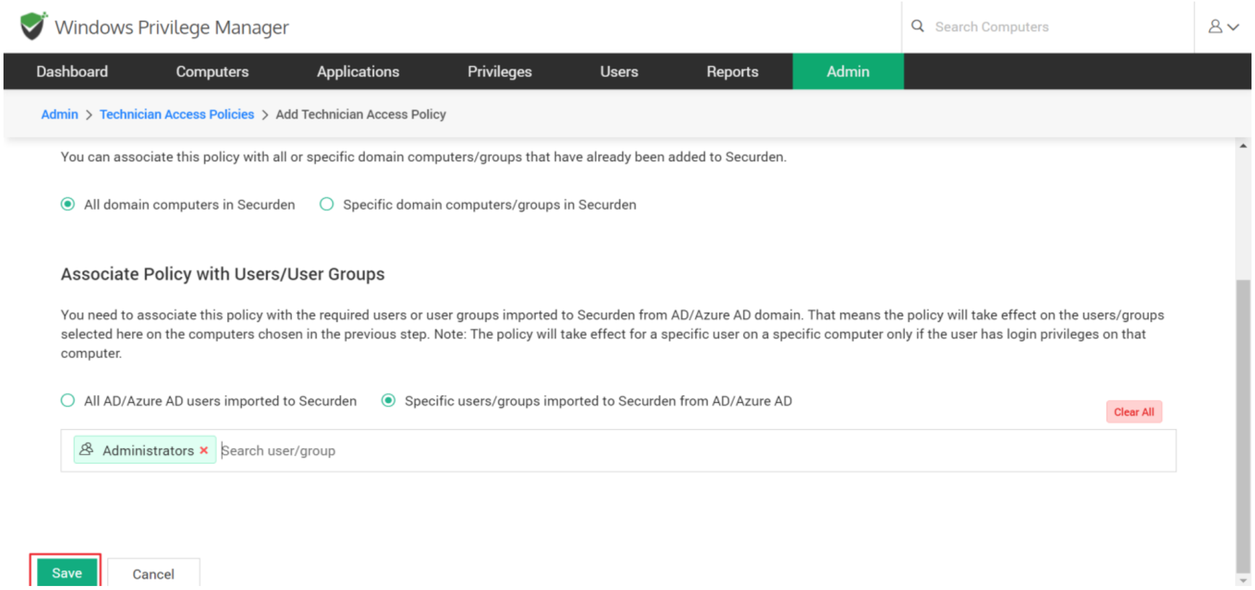
○ All domain users/accounts imported in Securden ● Specific domain users/groups/accounts/folders in Securden

Associate with Users/Groups

Associate with Accounts/Folders

- To associate the policy with all domain users/groups, enable **All domain users/groups imported in Securden**

- To select individual users or groups, use the **Search user/group** and choose from the list of users/groups.


Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Technician Access Policies > Add Technician Access Policy

You can associate this policy with all or specific domain computers/groups that have already been added to Securden.

● All domain computers in Securden ○ Specific domain computers/groups in Securden

Associate Policy with Users/User Groups

You need to associate this policy with the required users or user groups imported to Securden from AD/Azure AD domain. That means the policy will take effect on the users/groups selected here on the computers chosen in the previous step. Note: The policy will take effect for a specific user on a specific computer only if the user has login privileges on that computer.

○ All AD/Azure AD users imported to Securden ● Specific users/groups imported to Securden from AD/Azure AD

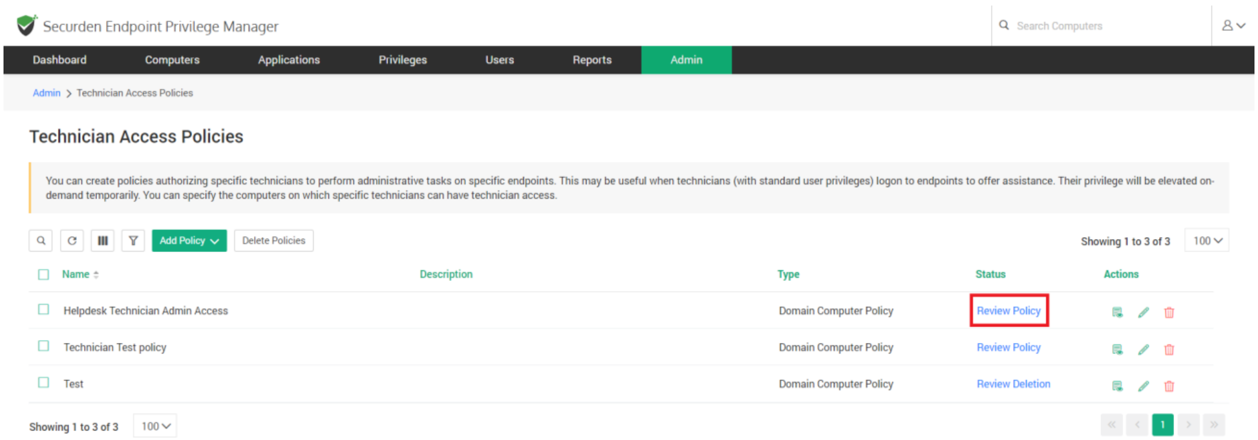
Finally, click **Save**.

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 Management>> Technician Access Policies**. Administrators will receive email notifications when a policy is created and awaits approval.



Technician Access Policies

You can create policies authorizing specific technicians to perform administrative tasks on specific endpoints. This may be useful when technicians (with standard user privileges) logon to endpoints to offer assistance. Their privilege will be elevated on-demand temporarily. You can specify the computers on which specific technicians can have technician access.

Showing 1 to 3 of 3 100

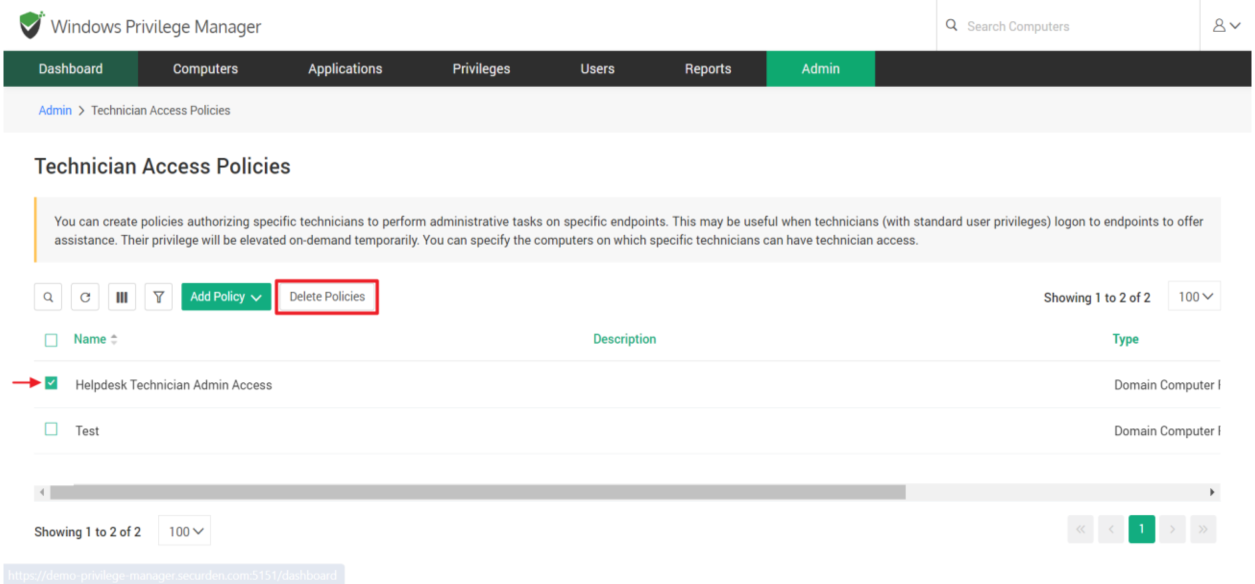
□	Name	Description	Type	Status	Actions
□	Helpdesk Technician Admin Access		Domain Computer Policy	Review Policy	
□	Technician Test policy		Domain Computer Policy	Review Policy	
□	Test		Domain Computer Policy	Review Deletion	

Showing 1 to 3 of 3 100

The administrator who has to approve the policy will click on **Review Policy**, in the GUI that opens policy details will be displayed and the administrator can decide whether to approve the policy for the specified computers and users. On clicking **Approve**, the policy will become **Active**.

Delete an existing policy

To delete a policy that has been previously created for a Technician, select the Policy Name from the list and click on **Delete Policies**.



Technician Access Policies

You can create policies authorizing specific technicians to perform administrative tasks on specific endpoints. This may be useful when technicians (with standard user privileges) logon to endpoints to offer assistance. Their privilege will be elevated on-demand temporarily. You can specify the computers on which specific technicians can have technician access.

Showing 1 to 2 of 2 100

	Name	Description	Type
☑	Helpdesk Technician Admin Access		Domain Computer I
□	Test		Domain Computer I

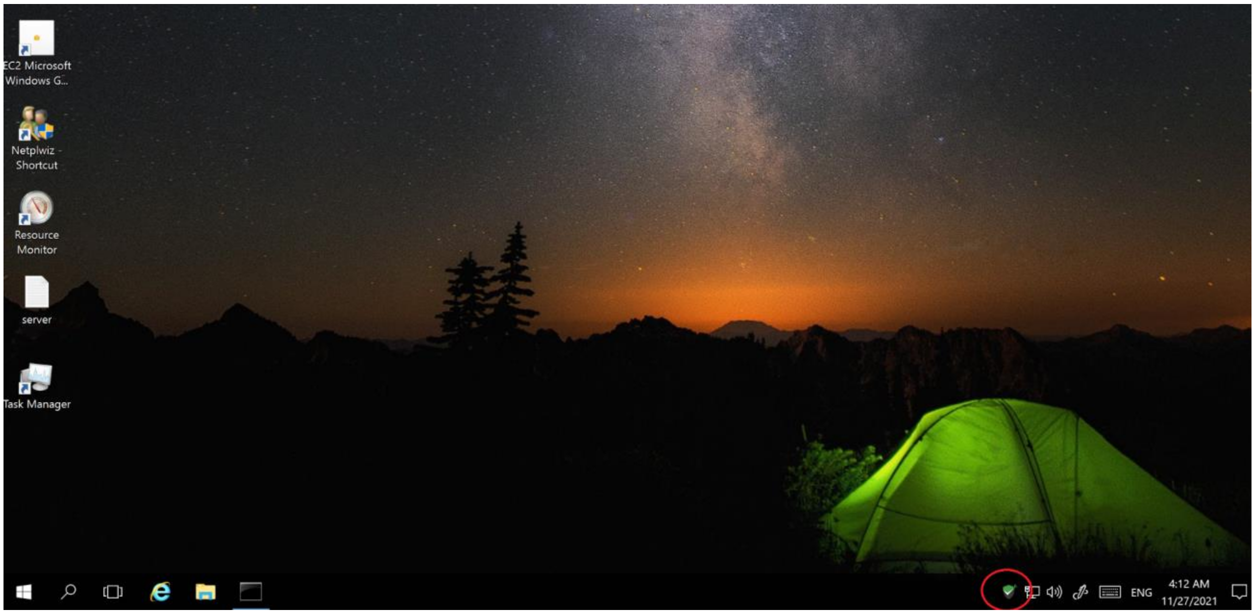
Showing 1 to 2 of 2 100

https://demo-privilege-manager.securden.com:5151/dashboard

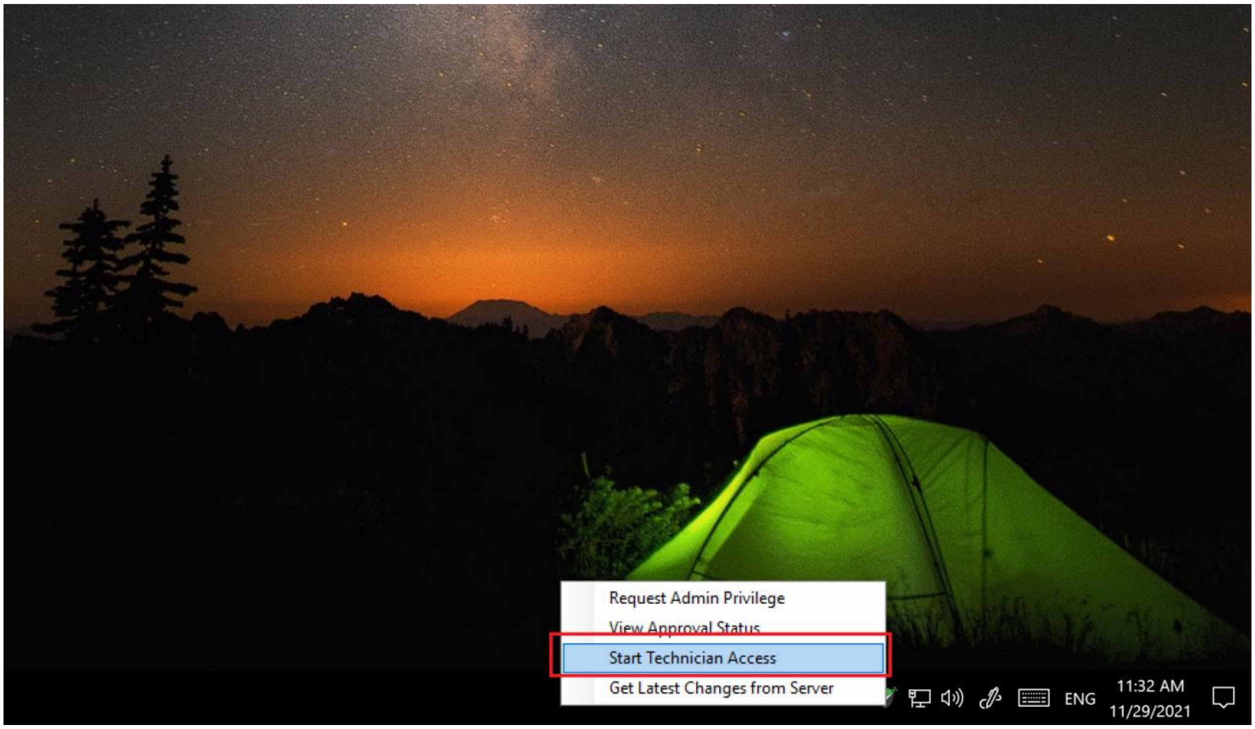
Workflow for Technicians

How do technicians commence access?

When a technician wants to access an endpoint, the technician has to access the Securden tray icon present in the required machine. (See the icon shown inside the red circle in the image below).



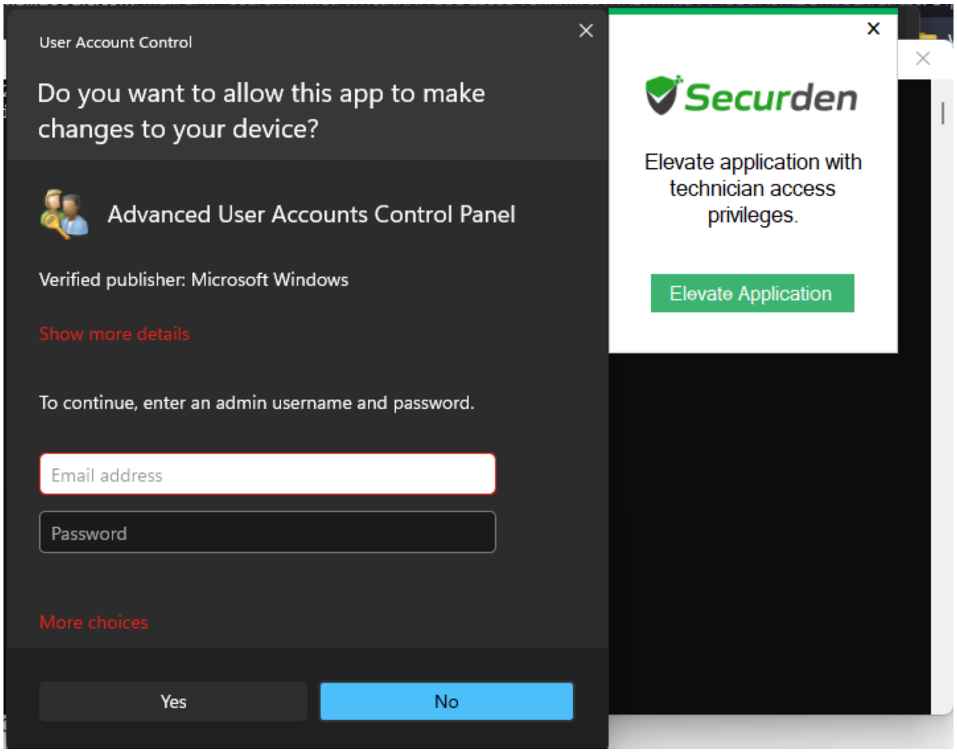
Upon clicking the tray icon, the technician will see a menu in which **Start Technician Access** will be one of the options.



When that option is clicked, the technicians will be prompted to enter their credentials for authentication. Technicians have to enter their domain account credentials to authenticate. Upon successful authentication, technician access will commence.

To use an application the technician should right-click the application and select **Run as Administrator**.

When doing so, the technician will see the UAC (User Account Control) prompt, but along with that Securden screen will also overlay as shown in the screenshot below.



User Account Control

Do you want to allow this app to make changes to your device?

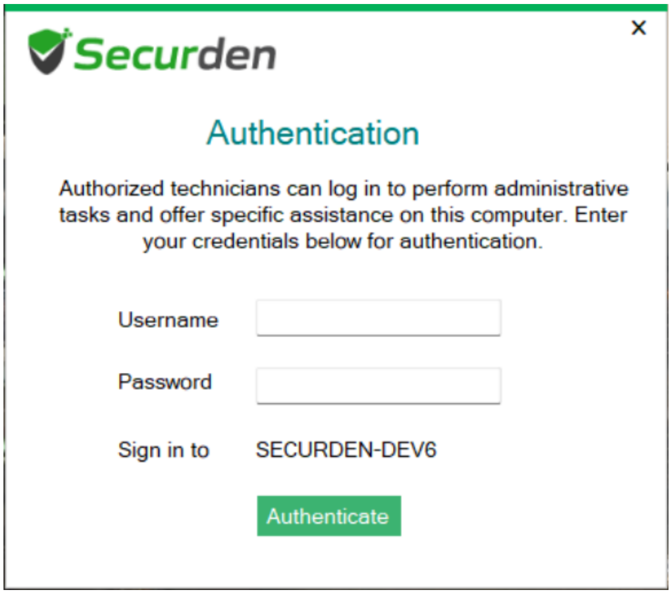
Advanced User Accounts Control Panel

Verified publisher: Microsoft Windows

To continue, enter an admin username and password.

Elevate application with technician access privileges.

On clicking **Elevate Application**, technicians will be able to log in with their user credentials and click **Authenticate.** On authentication, the application will be run.



Authentication

Authorized technicians can log in to perform administrative tasks and offer specific assistance on this computer. Enter your credentials below for authentication.

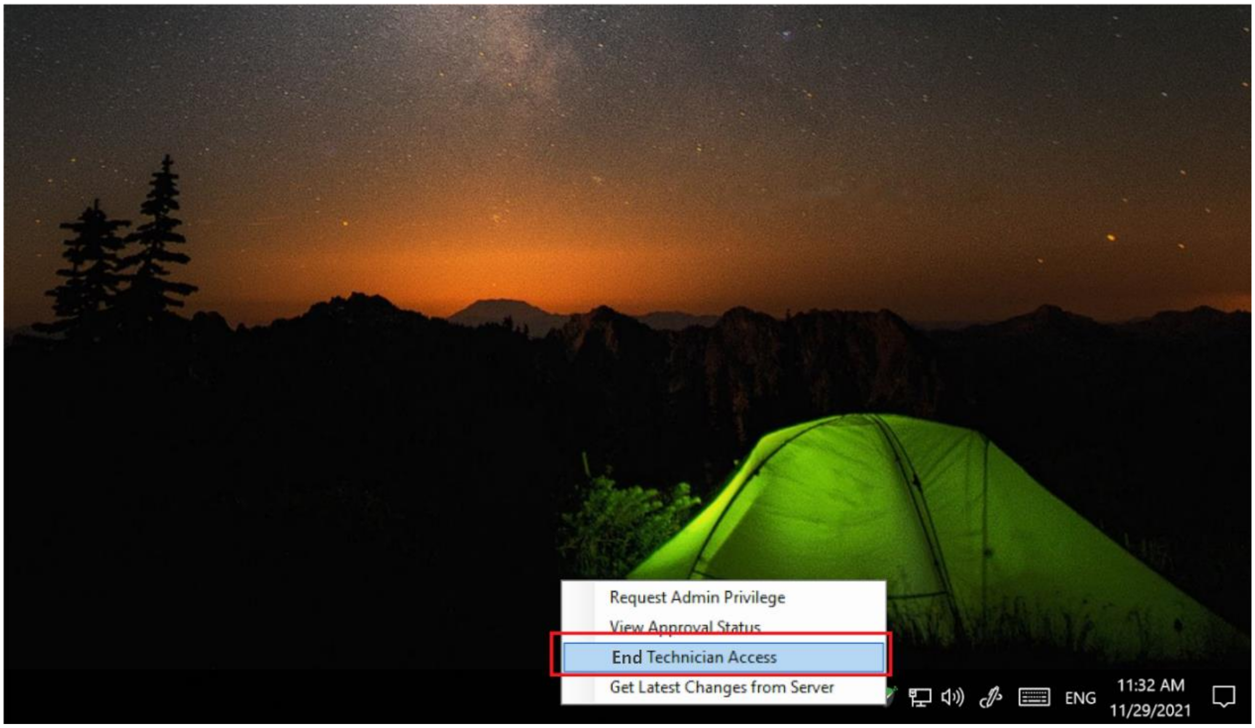
Username

Password

Sign in to SECURDEN-DEV6

How do technicians end access?

Finally, the technician has to click the **End Technician Access** option which is available in the tray icon menu.



SECTION 4: Privilege Elevation

Privilege Elevation Scenarios (for Users)

There are primarily three scenarios related to privilege elevation for standard users:

1. Elevating privileges for whitelisted applications
2. Requesting privilege elevation for new applications
3. Requesting time-limited, temporary admin access

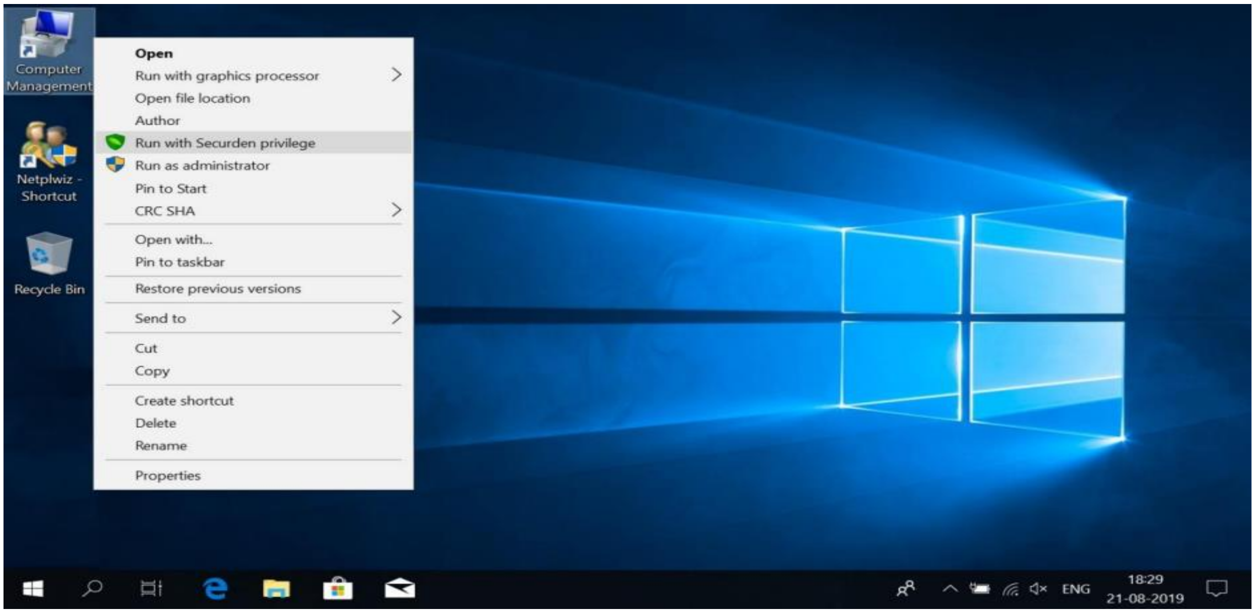
Scenario 1: Elevating Privileges for Whitelisted Applications

Standard users running applications that would normally require administrator rights.

You can run applications with admin privilege in three ways:

1. Context Menu (Right-click the application)
2. Using Run Command (Command Prompt)
3. Double-clicking the Application

Option 1: Elevating by Right-clicking (Context Menu)



Standard users can run/use an application that would normally require administrator rights anytime on-demand by right-clicking the respective application.

The context menu of all executables (.exe files) / applications will have an option named **Run With Securden Privilege**. You need to click that to get elevated privileges. However, *Start Menu* executables will not have this Option.

Alternatively, users can simply use the **Run as Administrator** option that is available by default.

Security Verification (one-time activity per session)

For security reasons, in order to ensure that it is exactly the authorized user is trying to access, Securden enforces users to go through a verification process as explained below. This is a one-time activity per session.

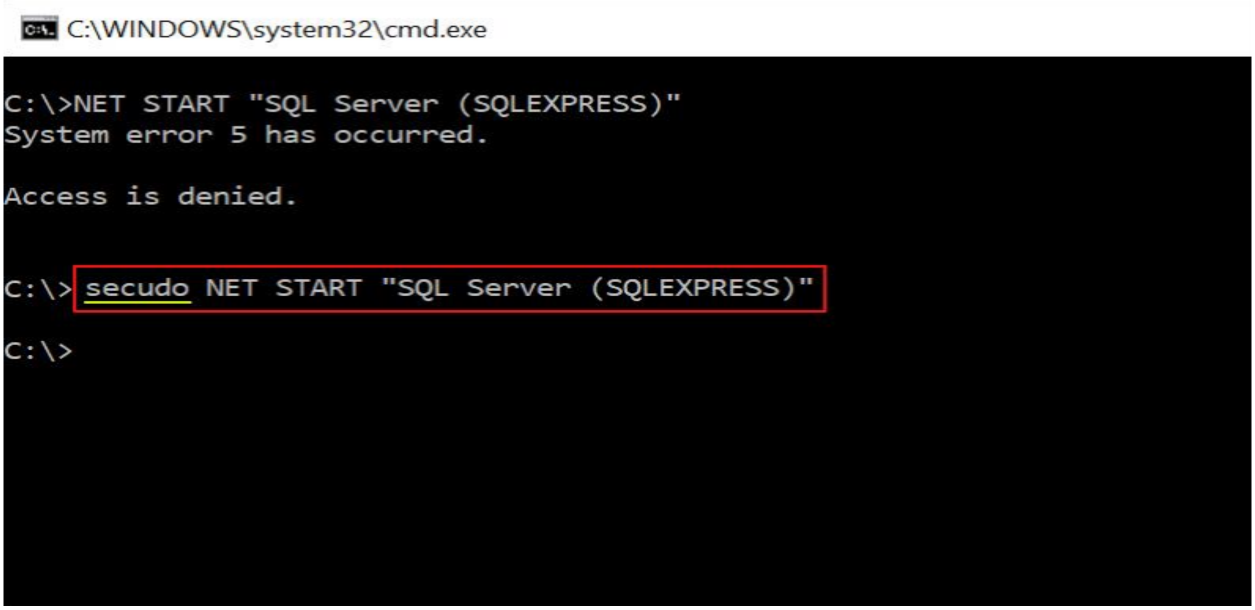
Immediately after clicking the menu **Run with Securden privilege** or **Run as Administrator**, users will be prompted to enter the following:

- A verification code sent by Securden to the email address of the user who raised the elevation request.
- **User's login credentials** (the credentials used by the user to access the endpoint and **NOT** administrator credentials. If you are trying elevation as a standard user, you need to enter your login credentials).

Option 2: Using Run Command (or) Command Prompt

You can make use of the **run command** prefixing **secudo** with the exact command.

Example: **secudo Powershell**



C:\WINDOWS\system32\cmd.exe

```
C:\>NET START "SQL Server (SQLEXPRESS)"
System error 5 has occurred.

Access is denied.


C:\>secudo NET START "SQL Server (SQLEXPRESS)"

C:\>
```

Security Verification (one-time activity per session)

For security reasons, in order to ensure that it is exactly the authorized user is trying to access, Securden enforces users to go through a verification process as explained below. This is a one-time activity per session.

Immediately after running the command, users will be prompted to enter the following:

- A verification code sent by Securden to the email address of the user who raised the elevation request.
- **User's login credentials** (the credentials used by the user to access the endpoint and **NOT** administrator credentials. If you are trying elevation as a standard user, you need to enter your login credentials).

Note: Every time during the first time login to the endpoint, the users will have to authenticate once by entering their login credentials (the credentials used by them to access the endpoint).

Option 3: By Double-clicking the Application (A different agent installation and additional configuration required)

This is perhaps the straightforward option for end users. However, using the option requires the installation of a different agent on endpoints. In addition, you need to create an **antivirus exclusion** for the Securden installation folder. If you are ready to add this exclusion, contact Securden Support (support@securden.com) for information on downloading the agent required for this purpose.

Scenarios 2 & 3 : Requesting Elevated Access

Scenario 2: Requesting privilege elevation for new applications (that are not whitelisted already)

Scenario 3: Requesting time-limited, temporary administrator access
When users need access to the applications that are not whitelisted already, they can raise a request for accessing that specific application alone. Sometimes, users might require administrator access for a temporary time period. In the case of granting temporary administrator access also, only applications are elevated for standard users. However, the main difference is that there will not be any restrictions on the applications that are to be run.

These two scenarios are handled through a well-defined workflow. Users will have to raise a request and go through an approval workflow to get elevation privileges. Administrators will review the request and grant privilege elevation. There are provisions for granting auto approvals to smoothen the workflow.

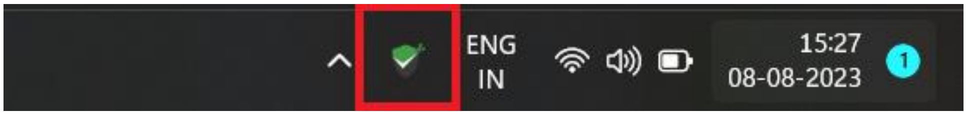
Raising Elevation Requests

Requests to access a specific application or to get time-limited, temporary administrator access can be raised in two ways:

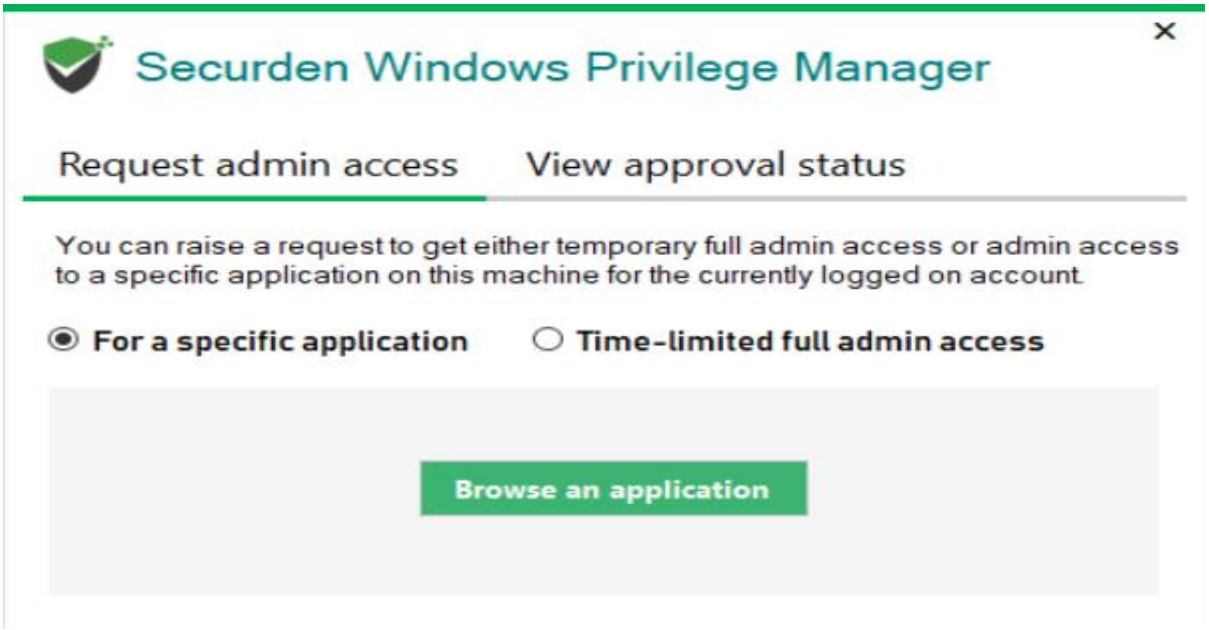
- Using Securden tray icon
- Using Securden web-interface (Full admin access only)

Option 1: Using Securden Tray Icon

Once you install Securden agents on endpoints, the Securden tray icon would be visible on all endpoints and servers.



When you click the tray icon, three options will be displayed. The option **Request Admin Access** pertains to raising a request to access a specific application or to get time-limited administrator access. When you click that, you will see the following popup:

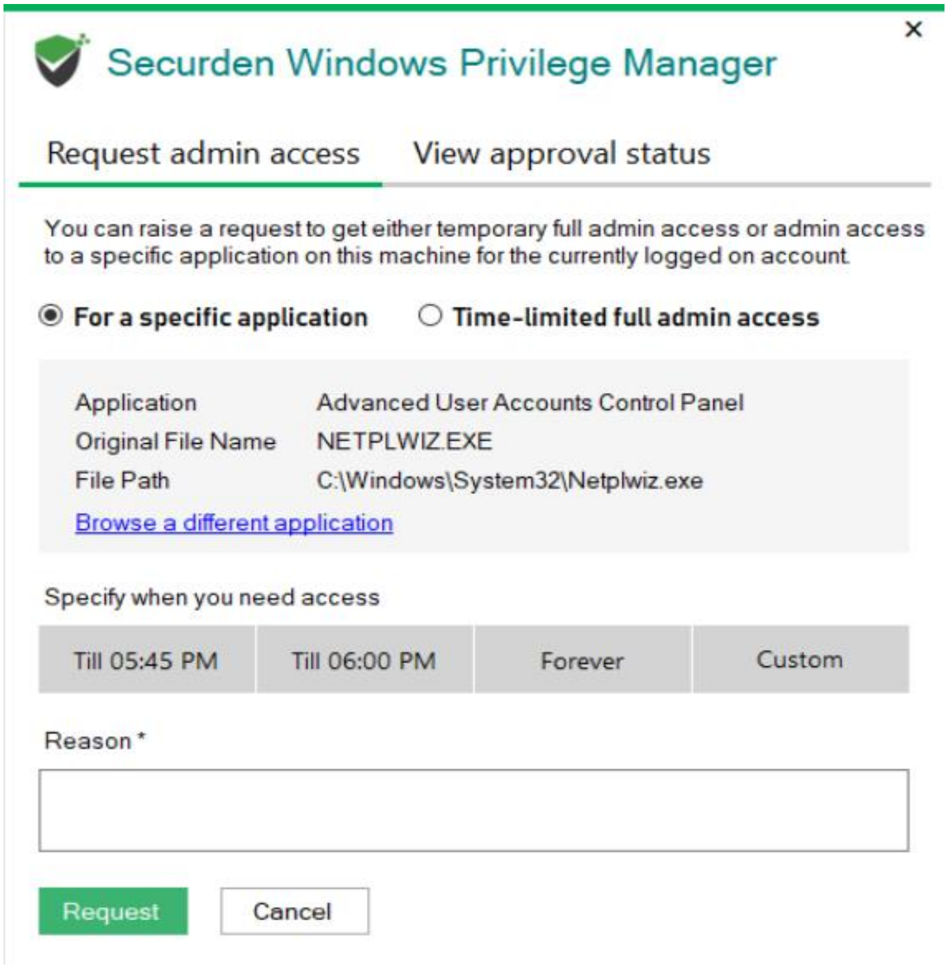


You can raise a request to get either temporary full admin access or admin access to a specific application on this machine for the currently logged on account

● For a specific application ○ Time-limited full admin access

You will see two options:

- **Raise a request for admin access to a specific application alone:** In this case, you need to browse and select the application to be run with admin privilege. Once you submit, your administrator will review the request and approve it.

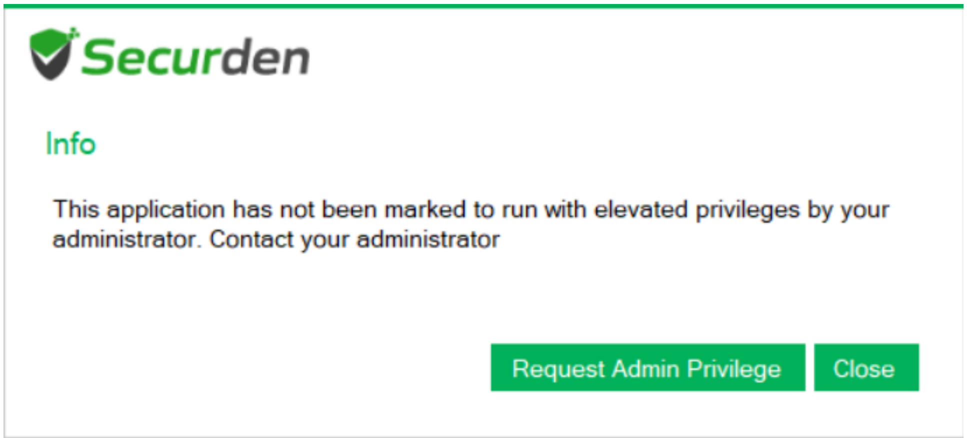


You can raise a request to get either temporary full admin access or admin access to a specific application on this machine for the currently logged on account.

● For a specific application ○ Time-limited full admin access

Application	Advanced User Accounts Control Panel
Original File Name	NETPLWIZ.EXE
File Path	C:\Windows\System32\Netplwiz.exe

Alternatively, users can simply try to elevate and run apps that are not whitelisted yet. The following window will be displayed.

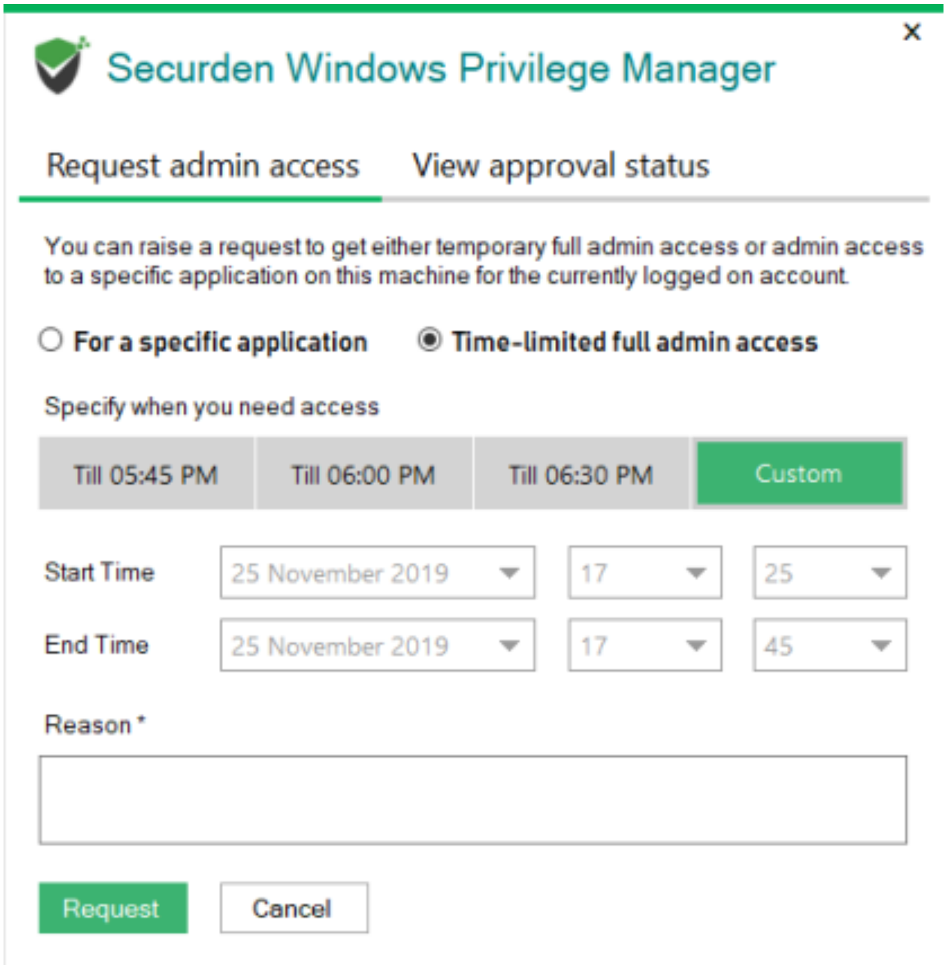


Info

This application has not been marked to run with elevated privileges by your administrator. Contact your administrator

Users can click on **Request Admin Privilege** and arrive at the same window discussed in the previous step.

- **Raise a request for time-limited administrator access:** In this case, you need to specify when you require access. Once you submit, your administrator will review the request and approve it.



You can raise a request to get either temporary full admin access or admin access to a specific application on this machine for the currently logged on account.

○ For a specific application ● Time-limited full admin access

Specify when you need access

Start Time 25 November 2019 17 25

End Time 25 November 2019 17 45

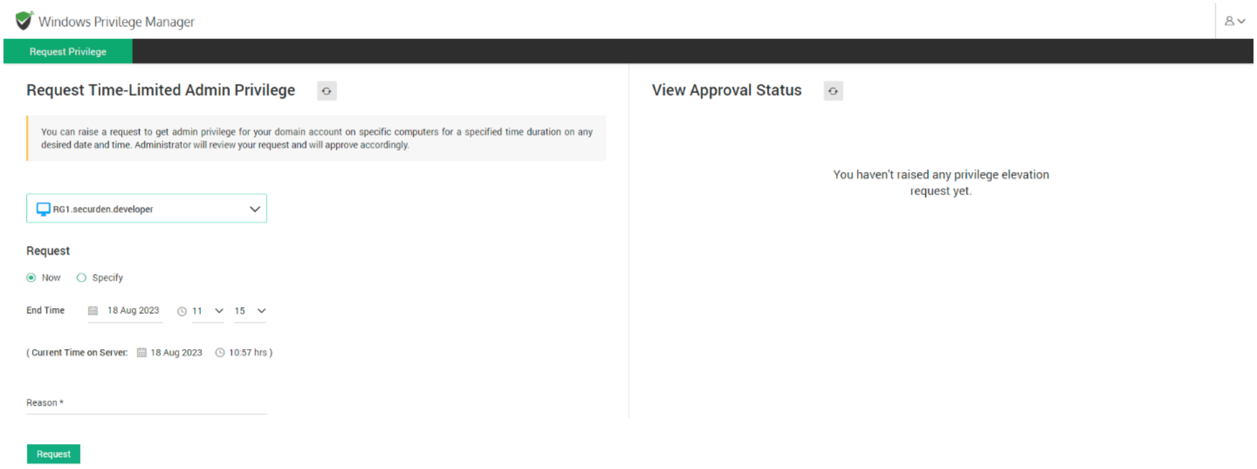
Reason *

You can check the approval status of your request by clicking the option **View approval status**.

Option 2: Through Self-Service Portal

The second option is to log in to the web interface and raise the request. To do this, navigate to **Privileges >> Request Privilege**. Domain users will directly see the self-service request portal upon logging in to the product.

This option will come in handy for domain users to get temporary administrator access.



Request Time-Limited Admin Privilege

You can raise a request to get admin privilege for your domain account on specific computers for a specified time duration on any desired date and time. Administrator will review your request and will approve accordingly.

RG1.securden.developer

Request

● Now ○ Specify

End Time 18 Aug 2023 11 15

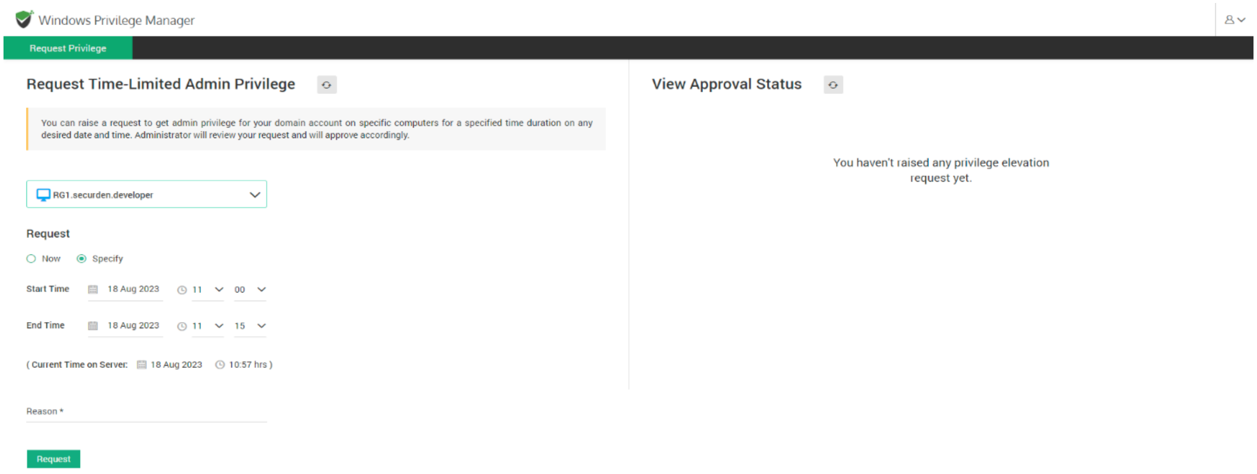
(Current Time on Server: 18 Aug 2023 10:57 hrs)

Reason *

View Approval Status

You haven't raised any privilege elevation request yet.

Domain users have the option to request for temporary administrator access for a later time or right away.



Request Time-Limited Admin Privilege

You can raise a request to get admin privilege for your domain account on specific computers for a specified time duration on any desired date and time. Administrator will review your request and will approve accordingly.

RG1.securden.developer

Request

○ Now ● Specify

Start Time 18 Aug 2023 11 00

End Time 18 Aug 2023 11 15

(Current Time on Server: 18 Aug 2023 10:57 hrs)

Reason *

View Approval Status

You haven't raised any privilege elevation request yet.

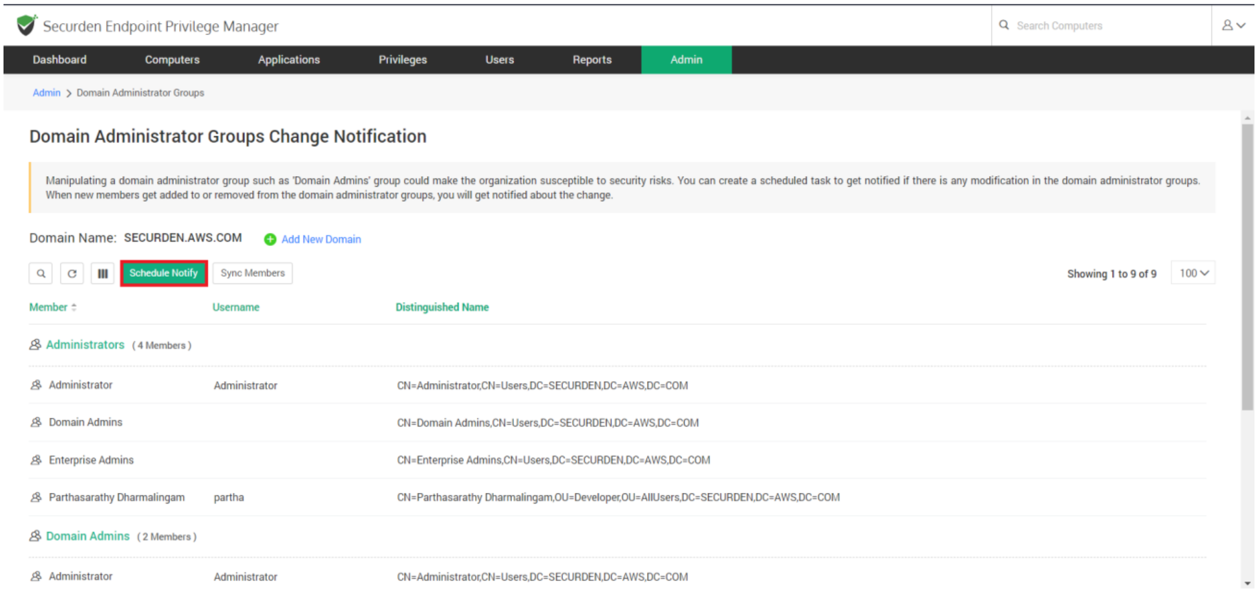
Gaining Privilege Elevation

The process to run applications with elevated privileges is the same as the one explained for Scenario 1 above.

Monitor Changes to Domain Admin Group

Manipulating a domain administrator group 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.

Navigate to **Admin >> Security >> Domain Administrator Groups >> Schedule Notify** to perform this action.



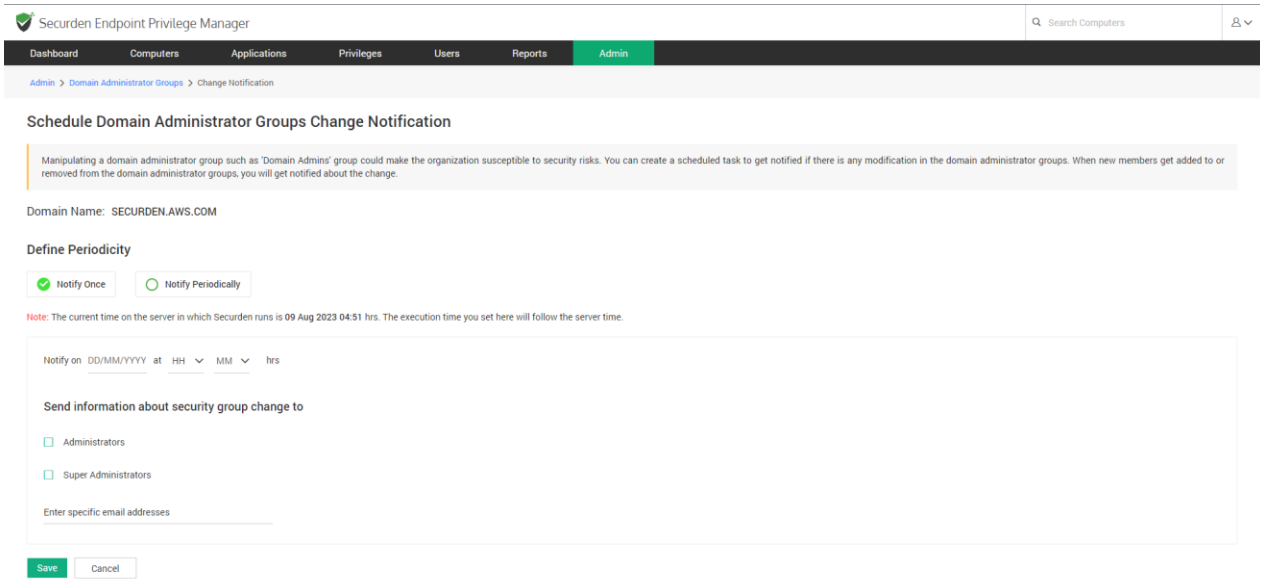
Domain Administrator Groups Change Notification

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.

Domain Name: SECURDEN.AWS.COM

Member	Username	Distinguished Name
Administrators (4 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
Enterprise Admins		CN=Enterprise 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
Domain Admins (2 Members)		
Administrator	Administrator	CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

You need to schedule these notifications by specifying the date, time, and the recipients. You have the option to schedule notifications once and periodically.


Securden Endpoint Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Domain Administrator Groups > Change Notification
Save
Cancel

Schedule Domain Administrator Groups Change Notification

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.

Domain Name: SECURDEN.AWS.COM

Define Periodicity

● Notify Once ○ Notify Periodically

Note: The current time on the server in which Securden runs is 09 Aug 2023 04:51 hrs. The execution time you set here will follow the server time.

Notify on DD/MM/YYYY at HH MM hrs

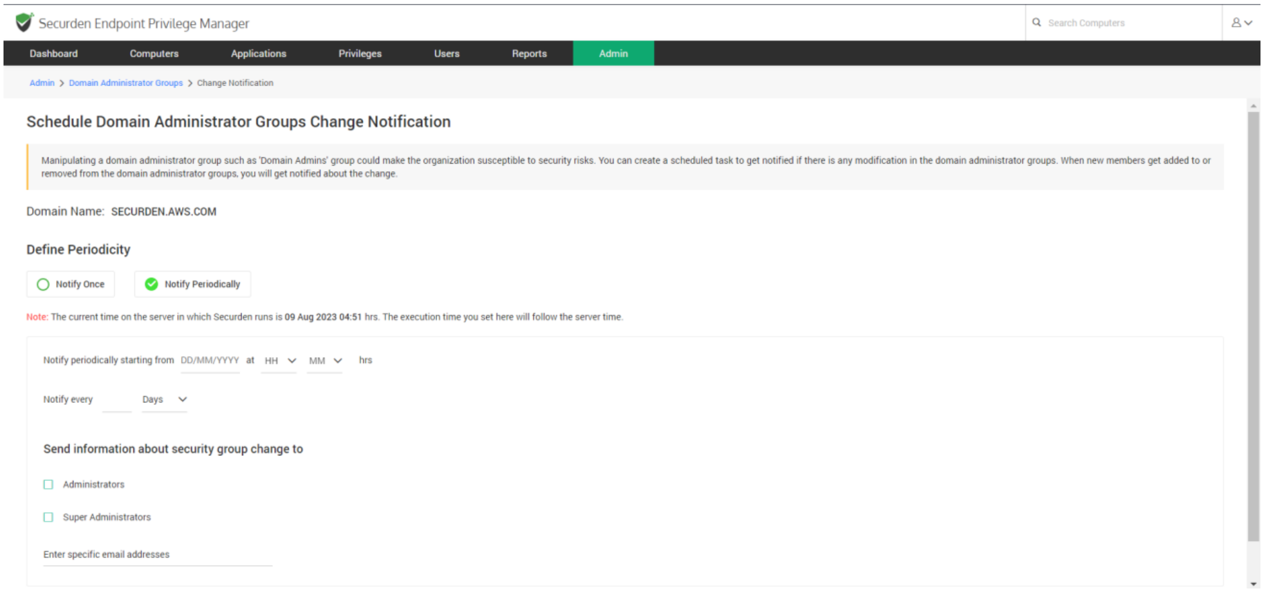
Send information about security group change to

□ Administrators

□ Super Administrators

Enter specific email addresses

If you choose to schedule notifications periodically, you need to specify the periodicity with which the notifications need to be sent.


Securden Endpoint Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Domain Administrator Groups > Change Notification

Schedule Domain Administrator Groups Change Notification

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.

Domain Name: SECURDEN.AWS.COM

Define Periodicity

○ Notify Once ● Notify Periodically

Note: The current time on the server in which Securden runs is 09 Aug 2023 04:51 hrs. The execution time you set here will follow the server time.

Notify periodically starting from DD/MM/YYYY at HH MM hrs

Notify every Days

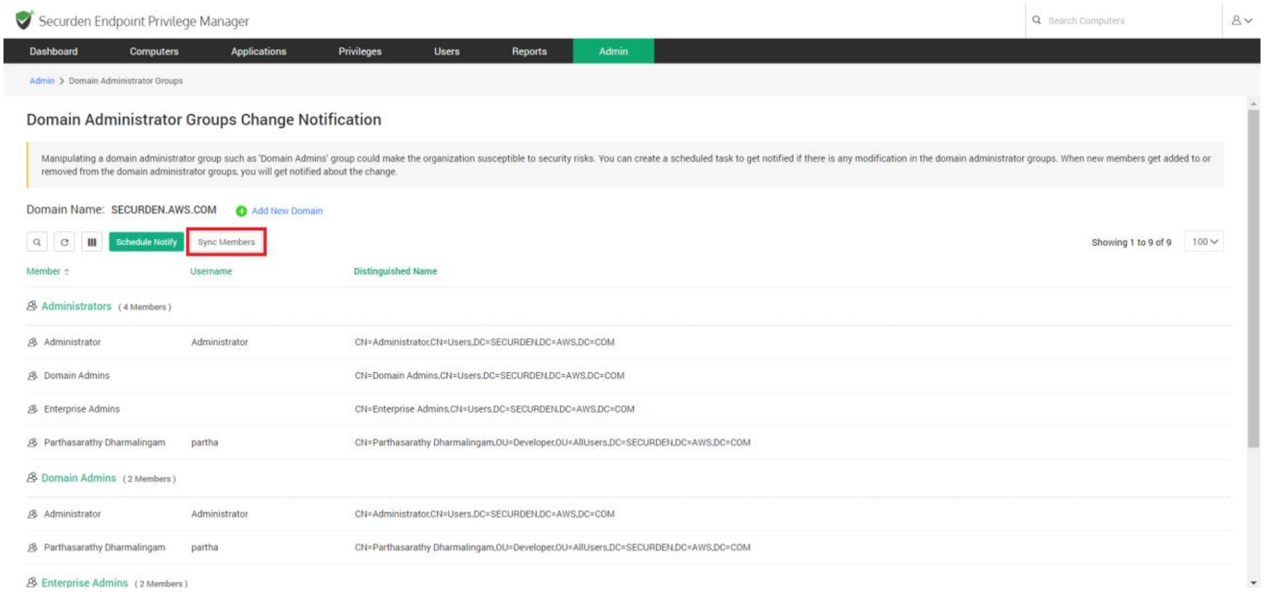
Send information about security group change to

□ Administrators

□ Super Administrators

Enter specific email addresses

Additionally, you can synchronize Securden with your domain administrator group by clicking on **Sync Members**.



Domain Administrator Groups Change Notification

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.

Domain Name: SECURDEN.AWS.COM

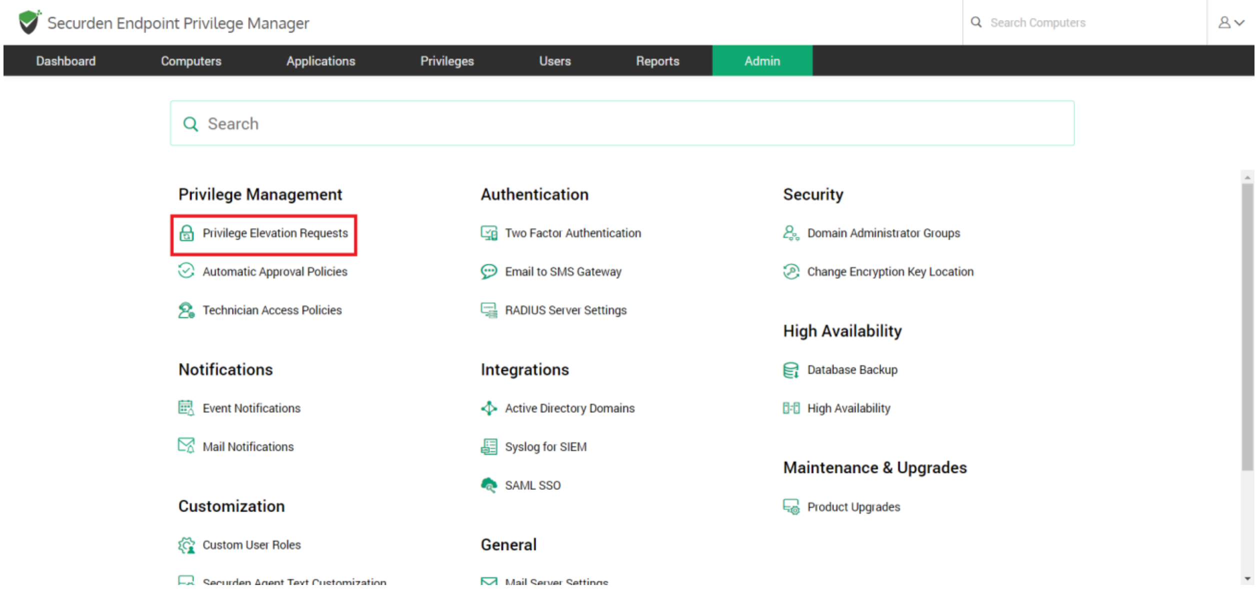
Showing 1 to 9 of 9 | 100

Member	Username	Distinguished Name
Administrators (4 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
Enterprise Admins		CN=Enterprise 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
Domain Admins (2 Members)		
Administrator	Administrator	CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM
Parthasarathy Dharmalingam	partha	CN=Parthasarathy Dharmalingam,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM
Enterprise Admins (2 Members)		

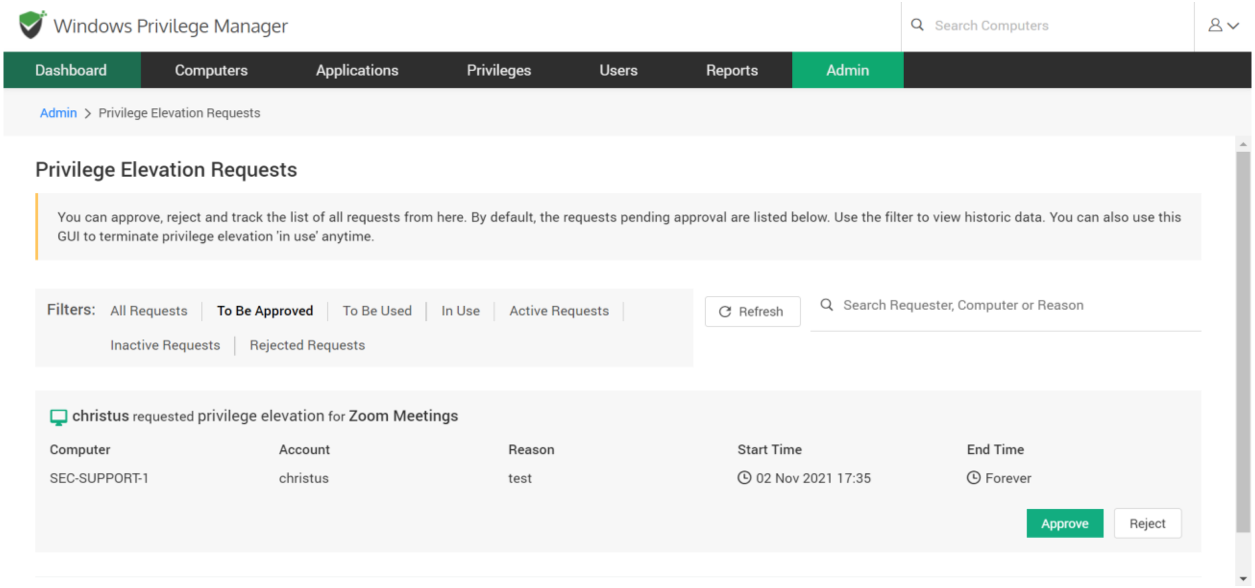
Once you click **Sync Members**, the process status will be displayed.

Privilege Elevation Requests

Privilege elevation requests are made by standard users, or users without the required privileges to access certain applications with admin rights when the need arises. These requests are managed by the administrator or authorized users. On approval, the standard user will be able to run applications with admin rights on their local system. Elevated access can be requested for a defined time duration.



As an administrator or an authorized user, to track and/or approve/reject elevation requests you can navigate to **Admin >> Privilege Management >> Privilege Elevation Requests.**


Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Privilege Elevation Requests

Privilege Elevation Requests

You can approve, reject and track the list of all requests from here. By default, the requests pending approval are listed below. Use the filter to view historic data. You can also use this GUI to terminate privilege elevation 'in use' anytime.

Filters: All Requests | To Be Approved | To Be Used | In Use | Active Requests | Inactive Requests | Rejected Requests
Refresh
Search Requester, Computer or Reason

christus requested privilege elevation for Zoom Meetings

Computer	Account	Reason	Start Time	End Time
SEC-SUPPORT-1	christus	test	02 Nov 2021 17:35	Forever

In this GUI, you will see the requests pending approval by default. However to track all historical data you can use one of the following filters:

All Requests: Displays all requests, including past requests.

To be Used: Displays approved requests which are to be used by the user.

In Use: Displays approved requests which are in use by the user.

Active Requests: Displays active requests.

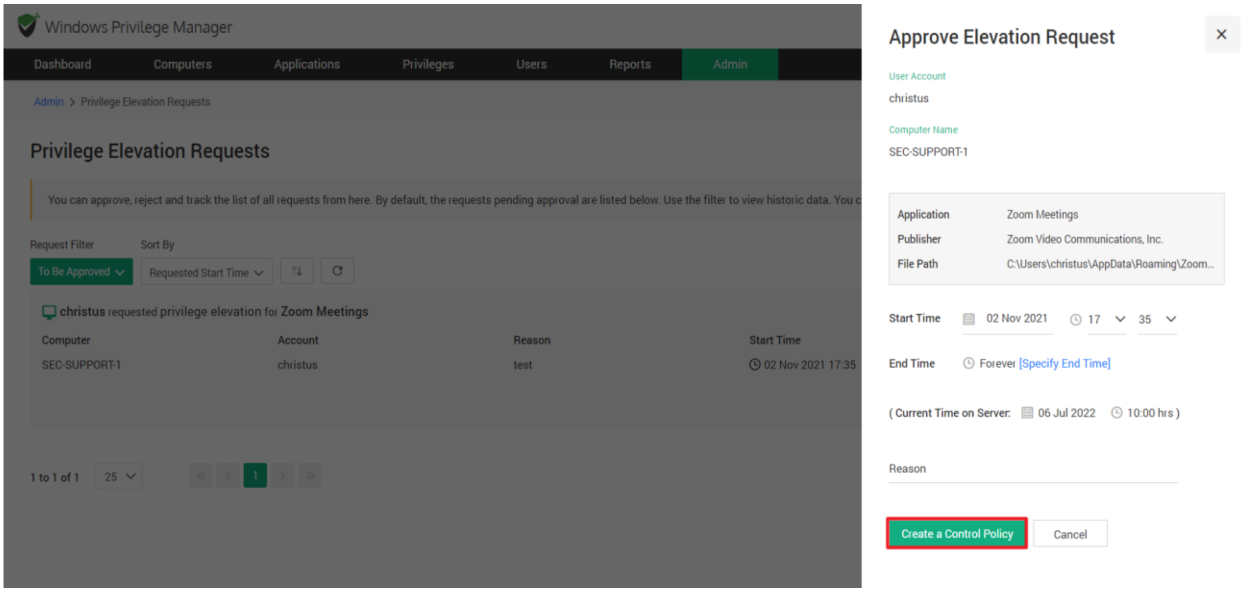
Inactive requests: Displays requests which have timed out.

Rejected requests: Displays all the rejected requests.

Approving requests

As an administrator or an authorized user, you have the ability to approve a raised request, to do so, skim over the request and then click on **Approve**.

In doing so you will be shown a GUI on the side which provides a quick overview of the request.


Windows Privilege Manager
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Privilege Elevation Requests

Privilege Elevation Requests

You can approve, reject and track the list of all requests from here. By default, the requests pending approval are listed below. Use the filter to view historic data. You c

Request Filter: To Be Approved

Sort By: Requested Start Time

christus requested privilege elevation for Zoom Meetings

Computer	Account	Reason	Start Time
SEC-SUPPORT-1	christus	test	02 Nov 2021 17:35

1 to 1 of 1 25

Approve Elevation Request

User Account: christus

Computer Name: SEC-SUPPORT-1

Application	Zoom Meetings
Publisher	Zoom Video Communications, Inc.
File Path	C:\Users\christus\AppData\Roaming\Zoom...

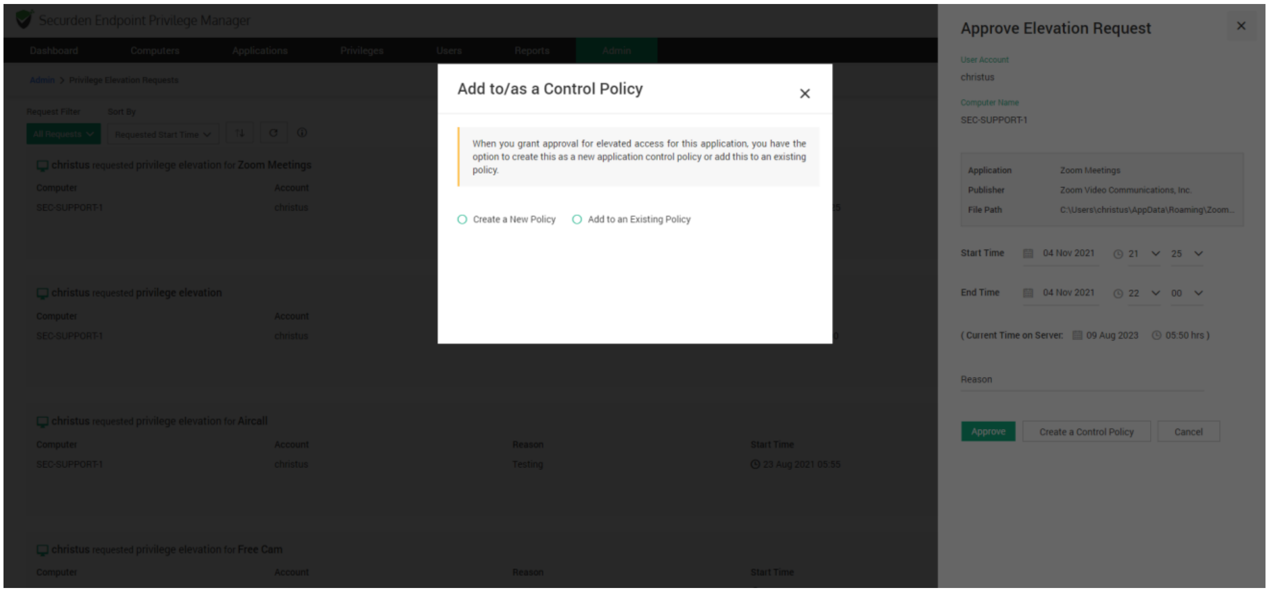
Start Time: 02 Nov 2021 17 35

End Time: Forever [Specify End Time]

(Current Time on Server: 06 Jul 2022 10:00 hrs)

Reason

When you grant approval for elevated access for this application, you have the option to create this as a new application control policy or add this to an existing policy.



christus requested privilege elevation for Zoom Meetings

Computer	Account
SEC-SUPPORT-1	christus

christus requested privilege elevation

Computer	Account
SEC-SUPPORT-1	christus

christus requested privilege elevation for Aircall

Computer	Account	Reason	Start Time
SEC-SUPPORT-1	christus	Testing	23 Aug 2021 05:55

christus requested privilege elevation for Free Cam

Add to/as a Control Policy

When you grant approval for elevated access for this application, you have the option to create this as a new application control policy or add this to an existing policy.

○ Create a New Policy ○ Add to an Existing Policy

Approve Elevation Request

User Account
christus

Computer Name
SEC-SUPPORT-1

Application	Zoom Meetings
Publisher	Zoom Video Communications, Inc.
File Path	C:\Users\christus\AppData\Roaming\Zoom...

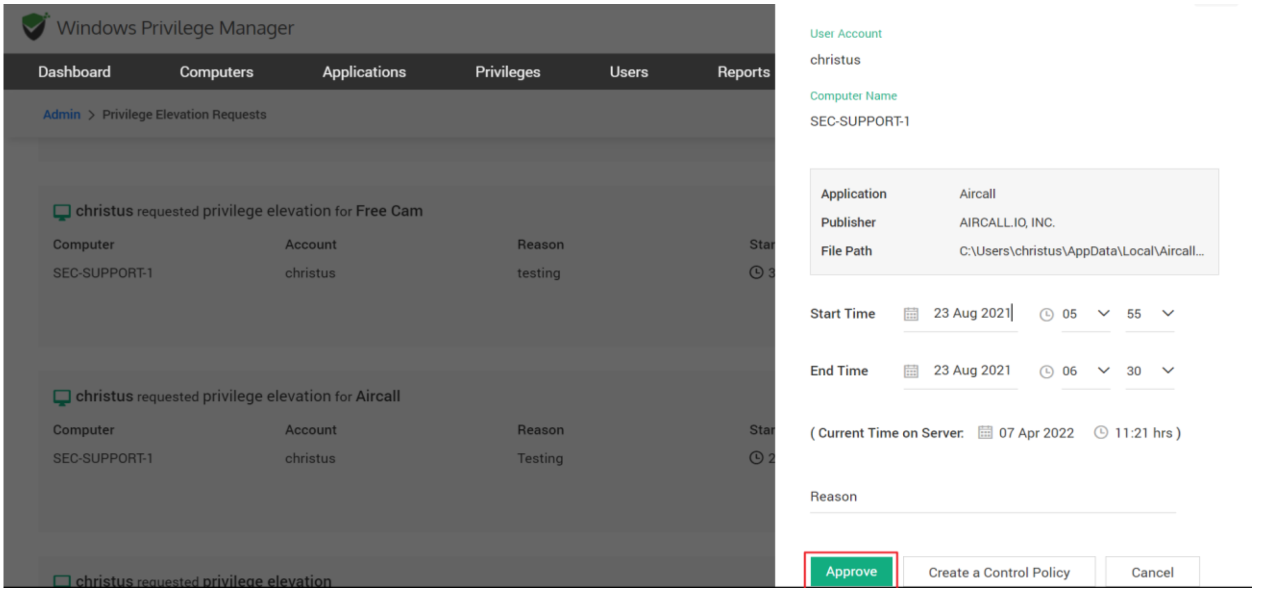
Start Time 04 Nov 2021 21 25

End Time 04 Nov 2021 22 00

(Current Time on Server: 09 Aug 2023 05:50 hrs)

Reason

If you don't have the need to create a control policy, you can simply approve the request by clicking **Approve**.


Windows Privilege Manager
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin > Privilege Elevation Requests

christus requested privilege elevation for Free Cam

Computer	Account	Reason
SEC-SUPPORT-1	christus	testing

christus requested privilege elevation for Aircall

Computer	Account	Reason
SEC-SUPPORT-1	christus	Testing

christus requested privilege elevation

User Account
christus

Computer Name
SEC-SUPPORT-1

Application	Aircall
Publisher	AIRCALL.IO, INC.
File Path	C:\Users\christus\AppData\Local\Aircall...

Start Time 23 Aug 2021 05 55

End Time 23 Aug 2021 06 30

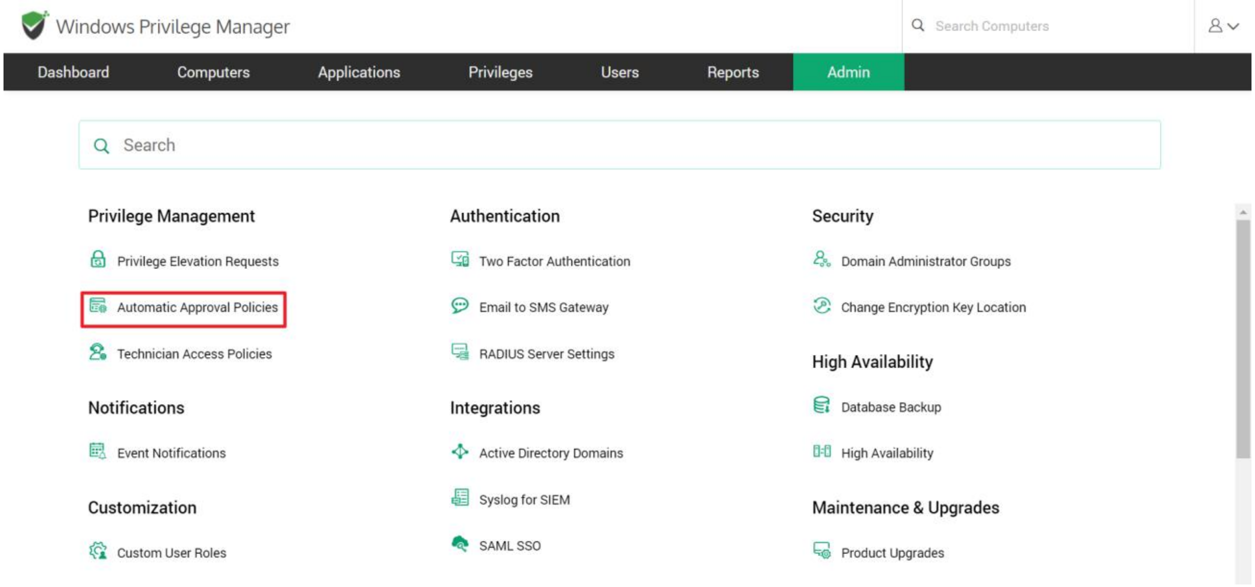
(Current Time on Server: 07 Apr 2022 11:21 hrs)

Reason

Automatic Approval Policies

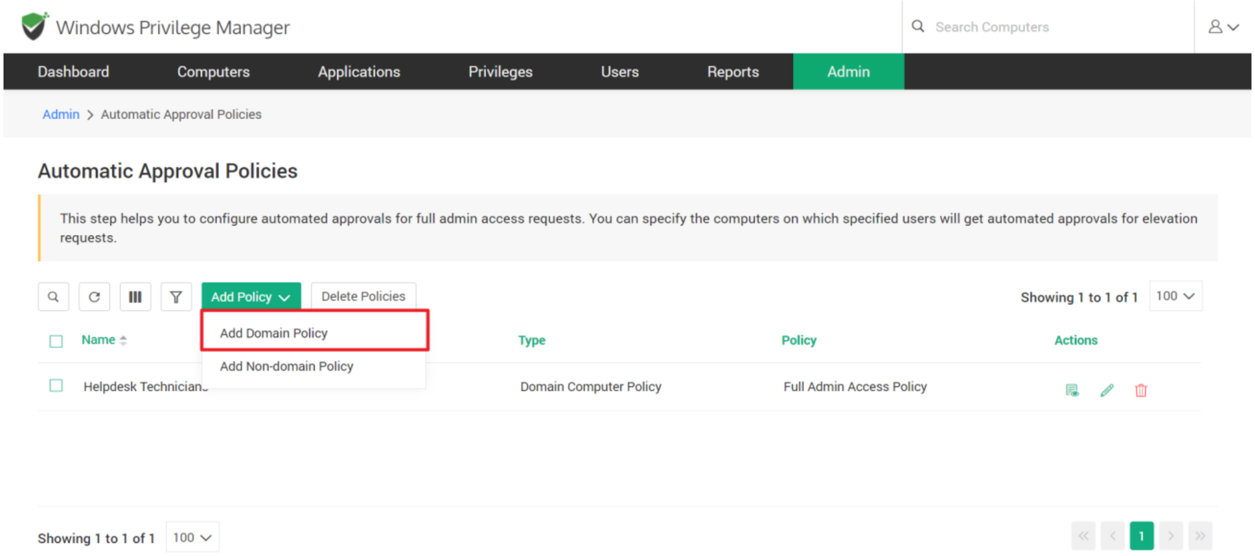
You can configure Securden to automatically approve admin access requests raised by specific users who may require privileged access to perform certain administrative tasks. You may add a domain policy for AD users and a non-domain approval policy to automate the approval process.

You can navigate to **Admin >> Privilege Management >> Automatic Approval Policies** to set up the policy.



Adding a domain approval policy

To add a domain policy click on **Add Policy** and select **Add Domain Policy**.

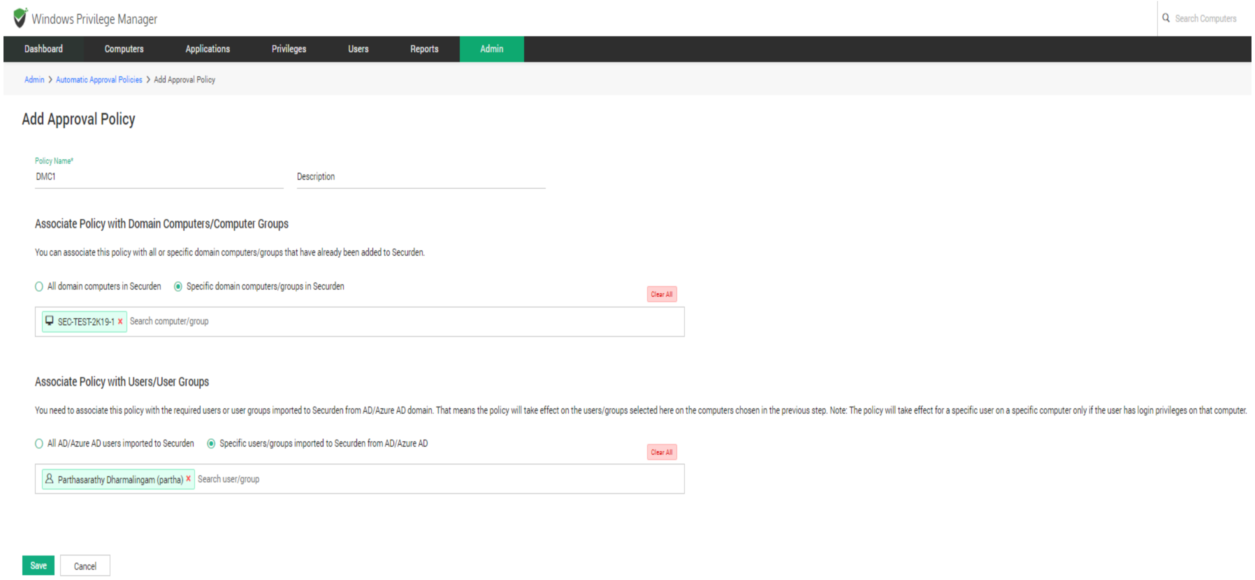


Automatic Approval Policies

This step helps you to configure automated approvals for full admin access requests. You can specify the computers on which specified users will get automated approvals for elevation requests.

Name	Type	Policy	Actions
Helpdesk Technician	Domain Computer Policy	Full Admin Access Policy	

In this GUI, enter the following details:


Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Automatic Approval Policies > Add Approval Policy

Add Approval Policy

Policy Name*: DMC1

Description

Associate Policy with Domain Computers/Computer Groups

You can associate this policy with all or specific domain computers/groups that have already been added to Securden.

○ All domain computers in Securden ● Specific domain computers/groups in Securden

Clear All

SEC-TEST-2K19-1 × Search computer/group

Associate Policy with Users/User Groups

You need to associate this policy with the required users or user groups imported to Securden from AD/Azure AD domain. That means the policy will take effect on the users/groups selected here on the computers chosen in the previous step. Note: The policy will take effect for a specific user on a specific computer only if the user has login privileges on that computer.

○ All AD/Azure AD users imported to Securden ● Specific users/groups imported to Securden from AD/Azure AD

Clear All

Parthasarathy Dharmalingam (partha) × Search user/group

Save Cancel

- **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

You need to associate this policy with the required computer/computer groups. As a prerequisite, all the devices/computers should have been added to Securden.

To select All domain computers in Securden, you can click on **All domain computers/groups in Securden**.

To select specific domain computers in Securden, you can click on **Specific domain computers/groups in Securden** and then use the search to choose a computer and/or a group.

You need to associate this policy with the required users or user groups imported to Securden from AD/Azure AD domain. That means the policy will take effect on the users/groups selected here and on the computers chosen in the previous step.

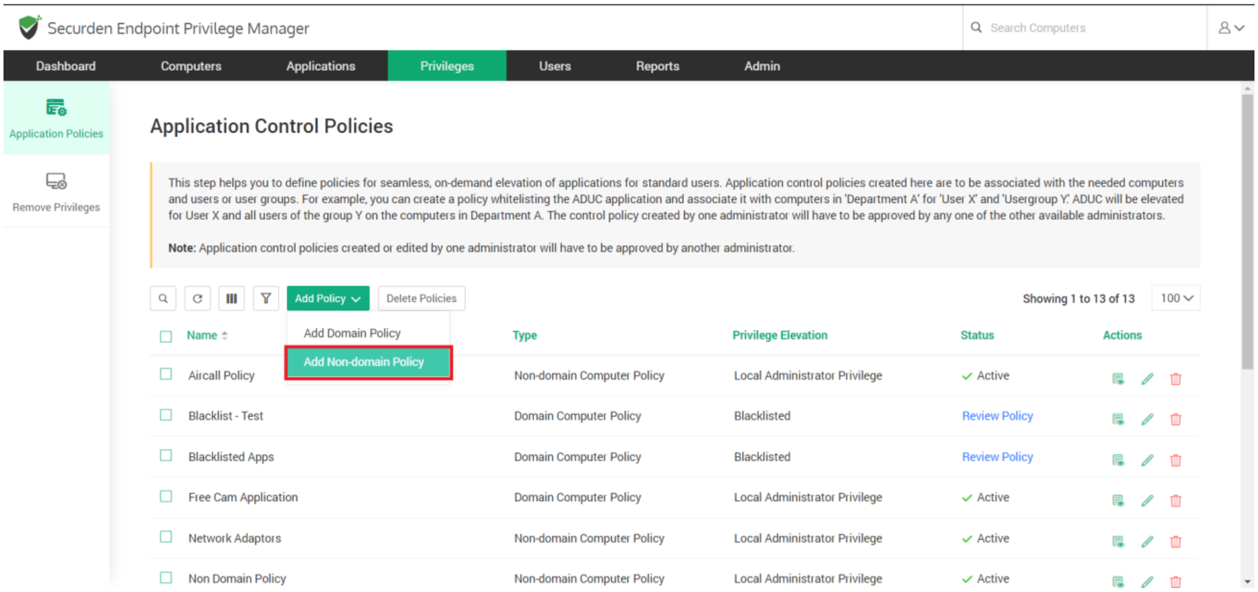
You can use the **Search user/group** bar to select the users and groups who will adopt this policy.

Once you have selected all the computer/groups and user/groups you may save the changes by clicking on **Save**.

Note: The policy will take effect for a specific user on a specific computer only if the user has login privileges on that computer.

Adding a non-domain approval policy

You can add automatic approval policies for non-domain computers/groups and the local, Azure AD users of the respective non-domain computers. To add a non-domain policy click on **Add Policy** and select **Add Non-Domain Policy**.



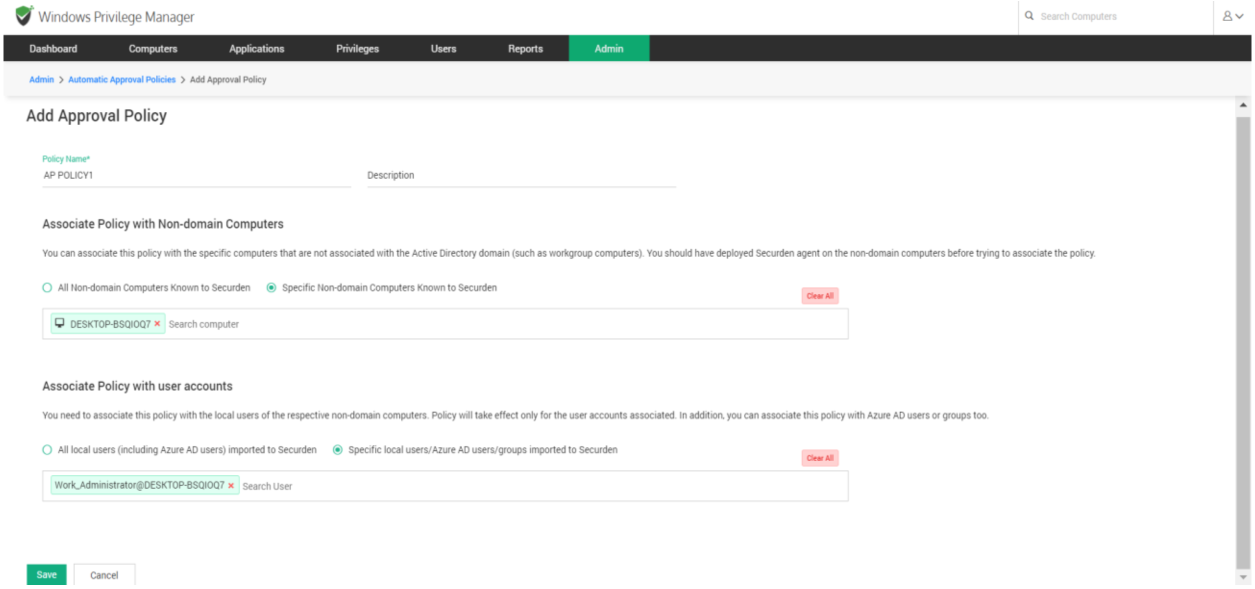
Application Control Policies

This step helps you to define policies for seamless, on-demand elevation of applications for standard users. Application 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 any one of the other available administrators.

Note: Application control policies created or edited by one administrator will have to be approved by another administrator.

☐	Name	Type	Privilege Elevation	Status	Actions
☐	Aircall Policy	Non-domain Computer Policy	Local Administrator Privilege	✓ Active	
☐	Blacklist - Test	Domain Computer Policy	Blacklisted	Review Policy	
☐	Blacklisted Apps	Domain Computer Policy	Blacklisted	Review Policy	
☐	Free Cam Application	Domain Computer Policy	Local Administrator Privilege	✓ Active	
☐	Network Adaptors	Non-domain Computer Policy	Local Administrator Privilege	✓ Active	
☐	Non Domain Policy	Non-domain Computer Policy	Local Administrator Privilege	✓ Active	

In this GUI, enter the following details:



Add Approval Policy

Policy Name* AP POLICY1

Description

Associate Policy with Non-domain Computers

You can associate this policy with the specific computers that are not associated with the Active Directory domain (such as workgroup computers). You should have deployed Securden agent on the non-domain computers before trying to associate the policy.

○ All Non-domain Computers Known to Securden ● Specific Non-domain Computers Known to Securden

DESKTOP-BSQIOQ7 × Search computer

Associate Policy with user accounts

You need to associate this policy with the local users of the respective non-domain computers. Policy will take effect only for the user accounts associated. In addition, you can associate this policy with Azure AD users or groups too.

○ All local users (including Azure AD users) imported to Securden ● Specific local users/Azure AD users/groups imported to Securden

Work_Administrator@DESKTOP-BSQIOQ7 × Search User

- **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

The next step is to associate this policy with the required non-domain computer/computer groups.

To select all domain computers click on **All non–domain computers in Securden**.

To select specific non-domain computers, you can click on **Specific non-domain computers/groups in Securden** and then use the search to choose a computer and/or a group.

After selecting the computers, you then need to associate this policy with the required local and Azure AD users and user groups in Securden. You have the option to associate this policy with all non-domain users or select specific users.

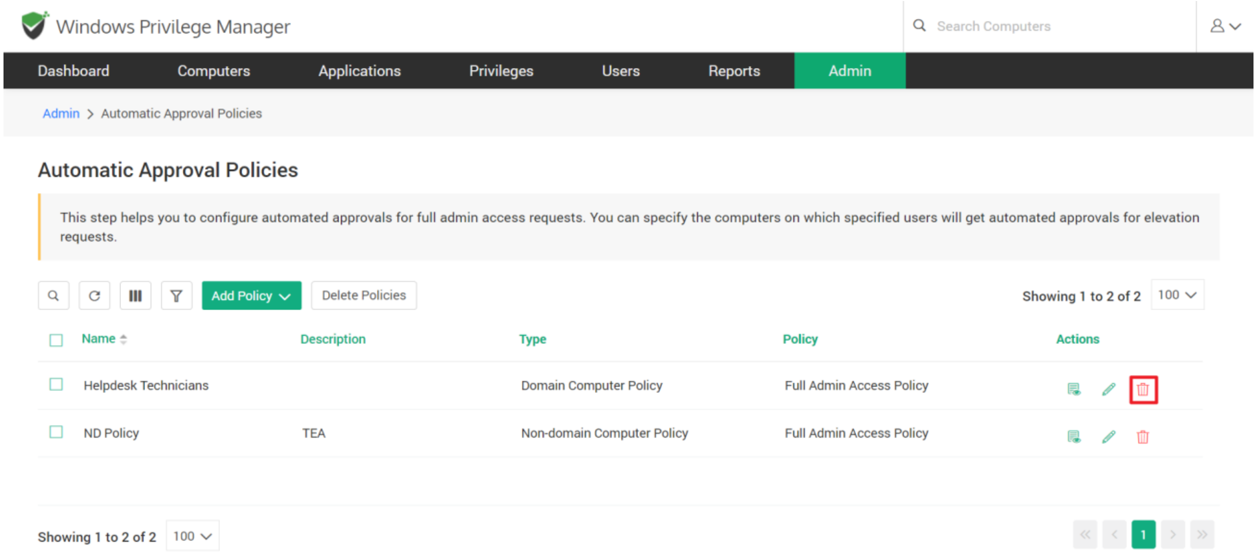
You can use the **Search user/group** bar to select the users and groups who will adopt this policy.

Once you have selected all the computer/groups and user/groups you may save the changes by clicking on **Save**.

Note: The policy will take effect for a specific user on a specific computer only if the user has login privileges on that computer.

Delete automatic approval policies

To delete policies individually, you may click on the **Delete** icon beside the policy.



Automatic Approval Policies

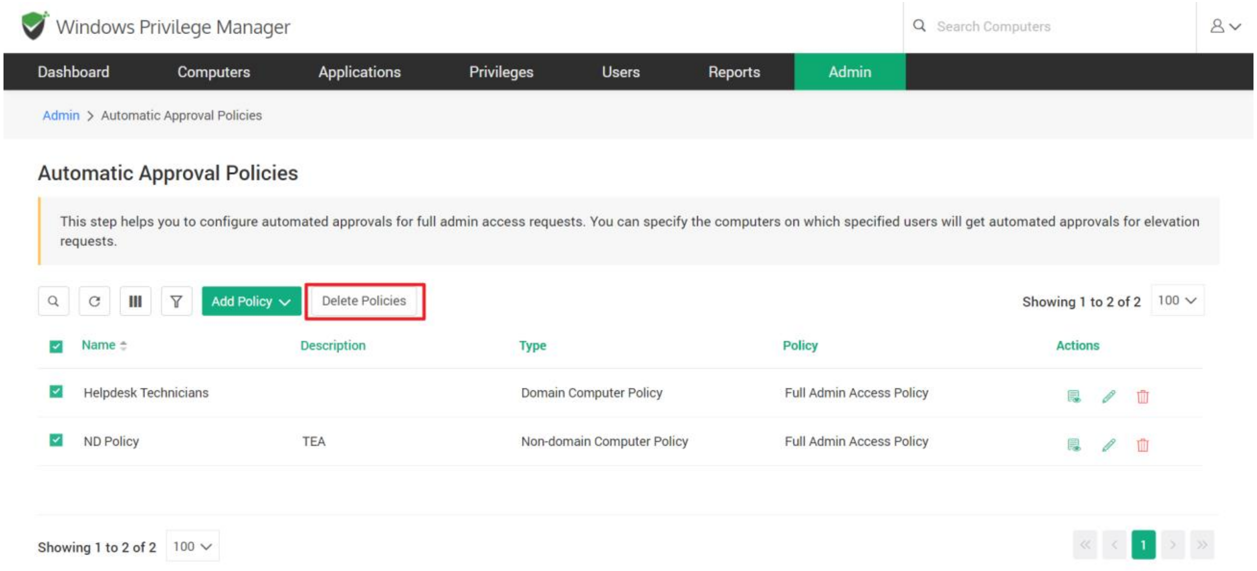
This step helps you to configure automated approvals for full admin access requests. You can specify the computers on which specified users will get automated approvals for elevation requests.

Showing 1 to 2 of 2

Name	Description	Type	Policy	Actions
Helpdesk Technicians		Domain Computer Policy	Full Admin Access Policy	
ND Policy	TEA	Non-domain Computer Policy	Full Admin Access Policy	

Showing 1 to 2 of 2

To delete policies together, you can select them and then click on **Delete Policies**.



Automatic Approval Policies

This step helps you to configure automated approvals for full admin access requests. You can specify the computers on which specified users will get automated approvals for elevation requests.

☑	Name	Description	Type	Policy	Actions
☑	Helpdesk Technicians		Domain Computer Policy	Full Admin Access Policy	
☑	ND Policy	TEA	Non-domain Computer Policy	Full Admin Access Policy	

You will receive a popup asking you to confirm the deletion. On clicking **OK** the selected policies will be deleted.

Privilege Elevation in Offline Scenarios

It is common to have employees in the field who need elevated access to applications. You have the option to allow users to generate privilege elevation codes and use them when they are offline.

Configuring Offline Codes for Privilege Elevation

In situations where the agent cannot establish connectivity with the server, users can elevate applications and gain temporary admin privileges by using **Offline Codes**.

Note: Users can utilize **Offline Codes** to elevate privileges - only when the administrator explicitly allows them to do so. The **Offline Codes** can be utilized in two ways:

- Allow users to generate codes themselves.
- The administrator can generate offline codes and share them with the user(s)when they require offline access.

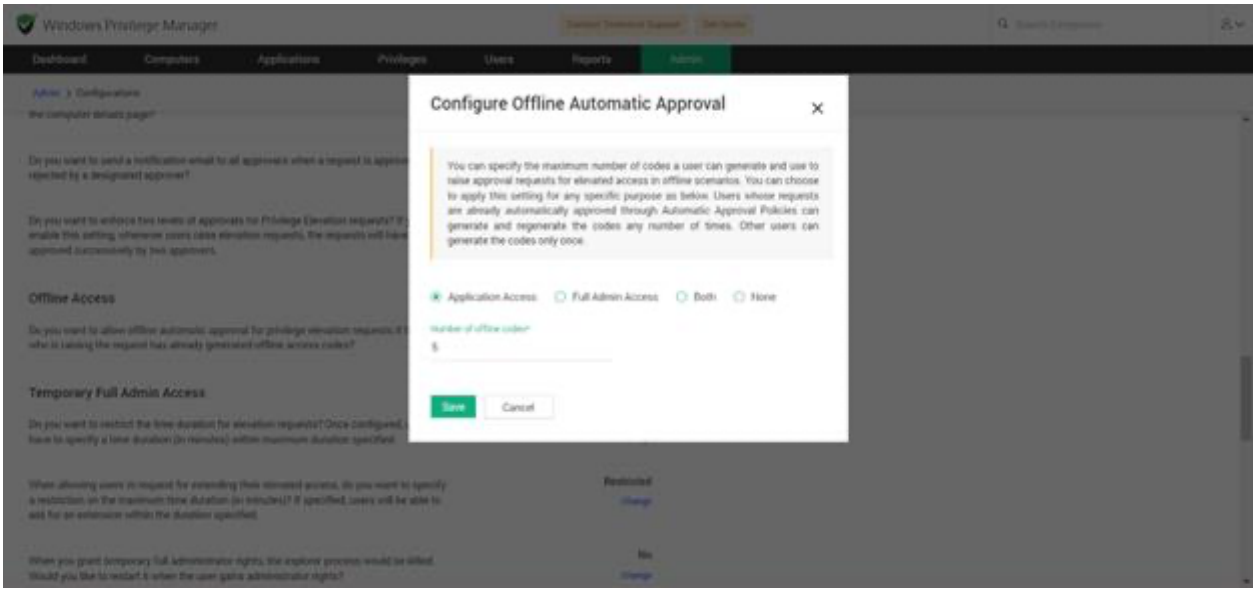
Configuration - For Codes to be Generated by Users

To enable this option, navigate to **Admin >> Configurations >> Offline Access.**

Locate **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?** and set the value for this as **Yes**.

Once you select **Yes**, a dialog box will pop up. In this dialog box, you have the option to allow **Application Access**, and **Full Admin Access** either separately or Both at the same time.

You can specify the number of codes that can be generated at once, per user (maximum **99**).



Configure Offline Automatic Approval

You can specify the maximum number of codes a user can generate and use to raise approval requests for elevated access in offline scenarios. You can choose to apply this setting for any specific purpose as below. Users whose requests are already automatically approved through Automatic Approval Policies can generate and regenerate the codes any number of times. Other users can generate the codes only once.

● Application Access ○ Full Admin Access ○ Both ○ None

Number of offline codes* 5

Save Cancel

Once enabled, the user can generate these offline codes using the agent's tray icon and store them for future use. (The user can only generate codes when the agent is connected to the Securden WPM server)

When the user attempts to run an application using administrator privilege, the user will be prompted to use the offline codes. **This can be done only if:**

- **The agent cannot establish connectivity with the WPM server.**

&

- **The permission to auto-elevate the application is not already facilitated through any application control policy.**

Note: The agent automatically synchronizes with the server every 60 minutes. If the application control policy was pushed into effect and synchronization hasn't taken place, the user will be prompted to use the offline codes.

Users can also manually synchronize the agent with the server by right-clicking the agent try icon and selecting **Get Latest Changes from the Server**.

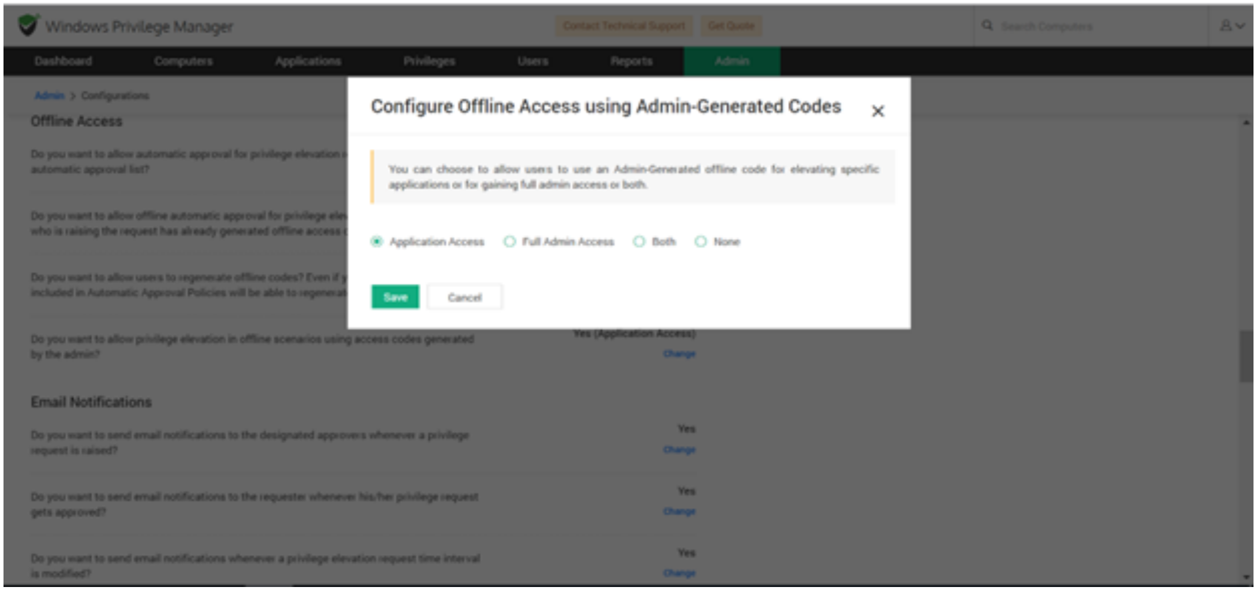
Note: Each offline code generated by a user can only be used once. After it is used, the code becomes inactive. The activities done during this time will be captured by the Securden agent and will be populated in the **Audit** section once connectivity is re-established.

Configuration - For Codes to be Generated by Administrators

To enable this option, navigate to **Admin >> Configurations >> Offline Access**

Locate **Do you want to allow privilege elevation in offline scenarios using access codes generated by the admin?** and set the value as **Yes**.

Once you select **Yes**, a dialog box will pop up. In this dialog box, you have the option to allow application access and full admin access separately, or both at the same time.



Configure Offline Access using Admin-Generated Codes ×

You can choose to allow users to use an Admin-Generated offline code for elevating specific applications or for gaining full admin access or both.

● Application Access ○ Full Admin Access ○ Both ○ None

Save Cancel

Do you want to allow privilege elevation in offline scenarios using access codes generated by the admin? Yes (Application Access)

Do you want to send email notifications to the designated approvers whenever a privilege request is raised? Yes

Do you want to send email notifications to the requester whenever his/her privilege request gets approved? Yes

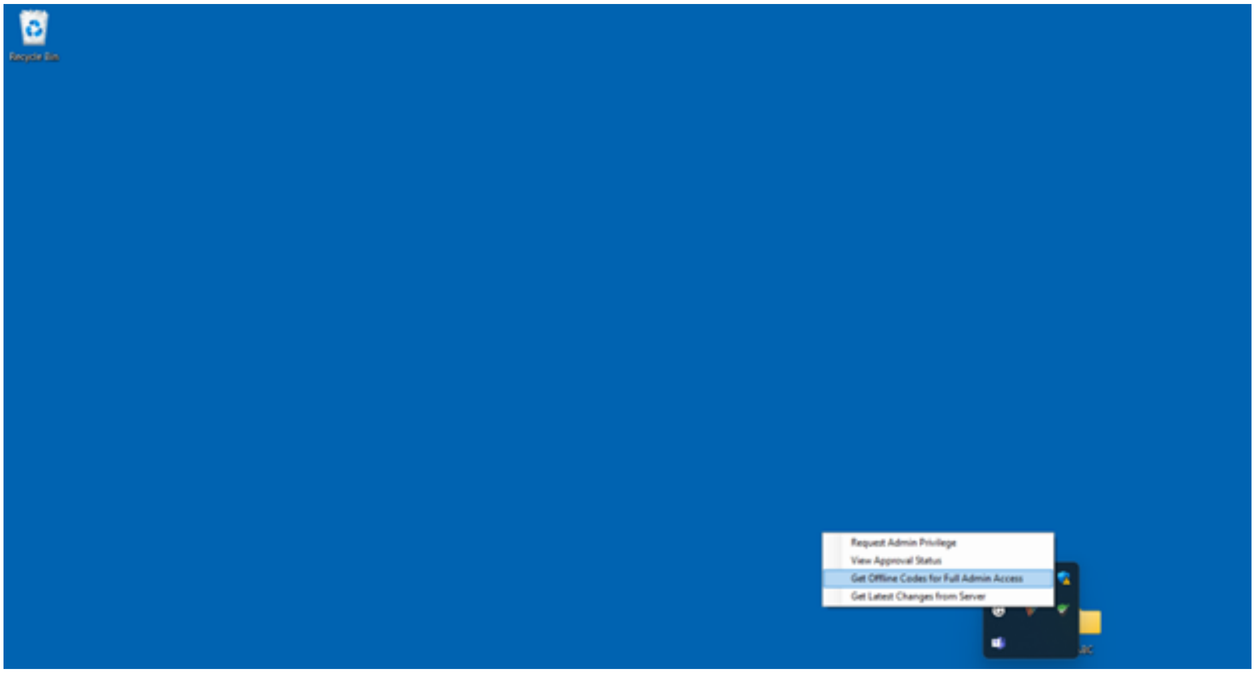
Do you want to send email notifications whenever a privilege elevation request time interval is modified? Yes

Once enabled, the administrator can generate offline codes from the WPM interface and share them with the user. When the user attempts to run an application using Securden privilege, the user will be prompted to use the admin offline code.

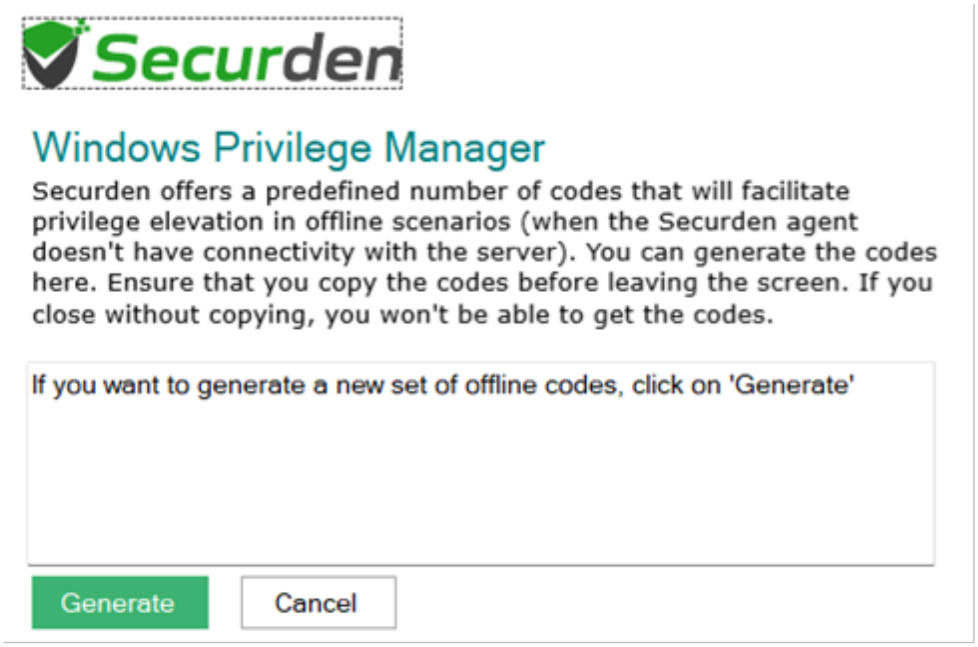
Generating Offline Access Codes for Yourself

To elevate applications using offline codes, users need to generate the codes while connectivity is established between the agent and the WPM server. When the connectivity is lost and they are offline, they can utilize these codes.

1) To generate codes, users can click on the Securden Agent tray icon and click **Get Offline Codes for Privilege Elevation**.


Recycle Bin
Request Admin Privilege
View Approval Status
Get Offline Codes for Full Admin Access
Get Latest Changes from Server

In the window that opens, they would click **Generate**.

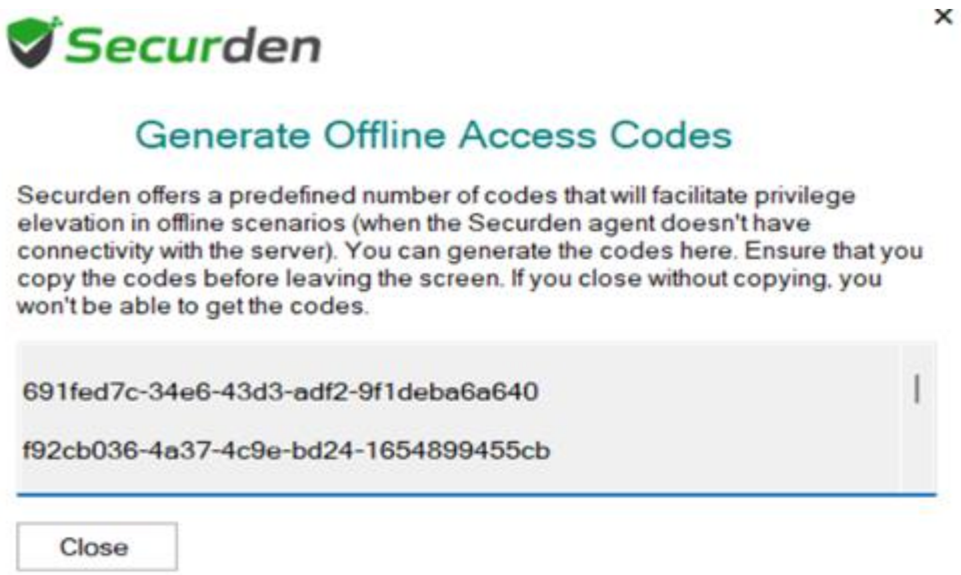


Windows Privilege Manager

Securden offers a predefined number of codes that will facilitate privilege elevation in offline scenarios (when the Securden agent doesn't have connectivity with the server). You can generate the codes here. Ensure that you copy the codes before leaving the screen. If you close without copying, you won't be able to get the codes.

If you want to generate a new set of offline codes, click on 'Generate'

After the codes are generated, a pop-up window will appear from which users can copy the generated codes and store them for future use.



Generate Offline Access Codes

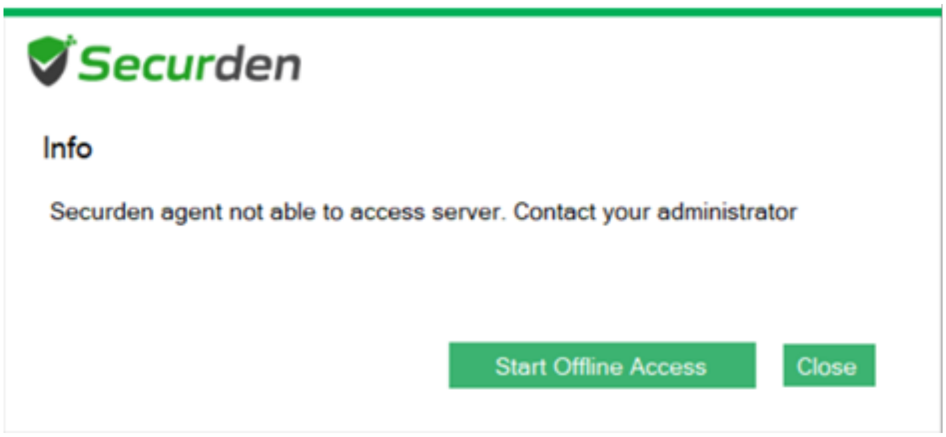
Securden offers a predefined number of codes that will facilitate privilege elevation in offline scenarios (when the Securden agent doesn't have connectivity with the server). You can generate the codes here. Ensure that you copy the codes before leaving the screen. If you close without copying, you won't be able to get the codes.

691fed7c-34e6-43d3-adf2-9f1deba6a640

f92cb036-4a37-4c9e-bd24-1654899455cb

Elevating an Application Using User-Generated Offline Codes

1) When the Securden Agent cannot establish connectivity with the WPM server, a pop-up window appears when users try to run an application with administrator privilege.



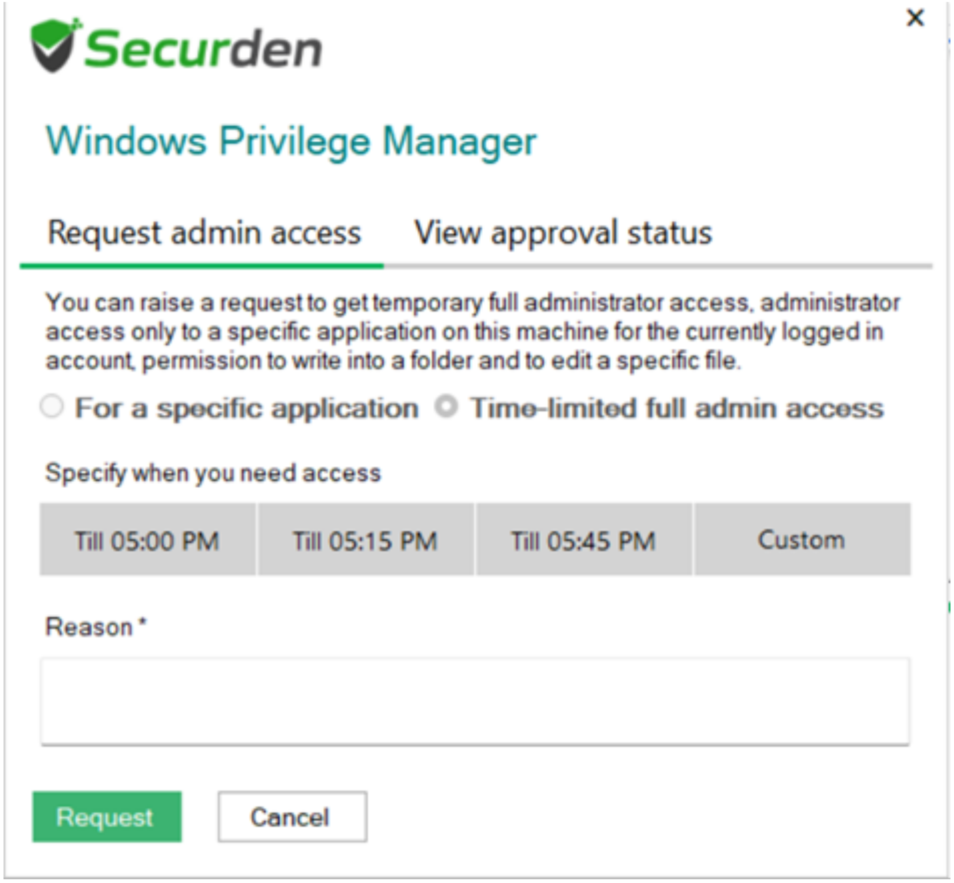
Info

Securden agent not able to access server. Contact your administrator

In the GUI that opens, click on **Start Offline Access**.

In the window that opens, select **For a specific application** (or) **Time-limited full admin access** based on the requirement.

Users have to specify the time until when they might need access and the reason why they need to elevate the application. After furnishing the required details, they may click **Request**.

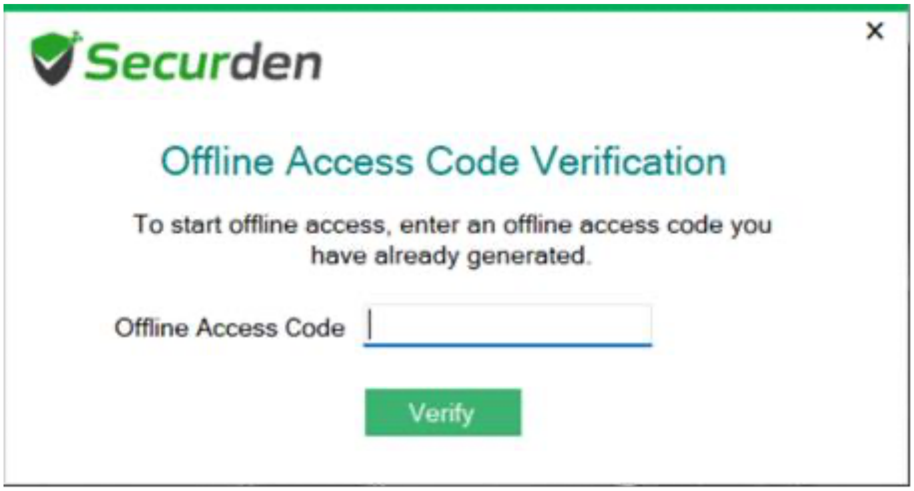


You can raise a request to get temporary full administrator access, administrator access only to a specific application on this machine for the currently logged in account, permission to write into a folder and to edit a specific file.

○ For a specific application ○ Time-limited full admin access

Specify when you need access

When the agent cannot establish connectivity with the server, the window shown below pops up. Users need to paste one of the active offline codes in the field and click **Verify**.



To start offline access, enter an offline access code you have already generated.

Offline Access Code

Once the code is verified, access will be granted and users can start using the application.

Note: Access will be revoked just as soon as the duration expires and all activities performed within this time will be recorded locally by the agent. These recorded activities will be populated in the **Audit** section of WPM once connectivity is re-established.

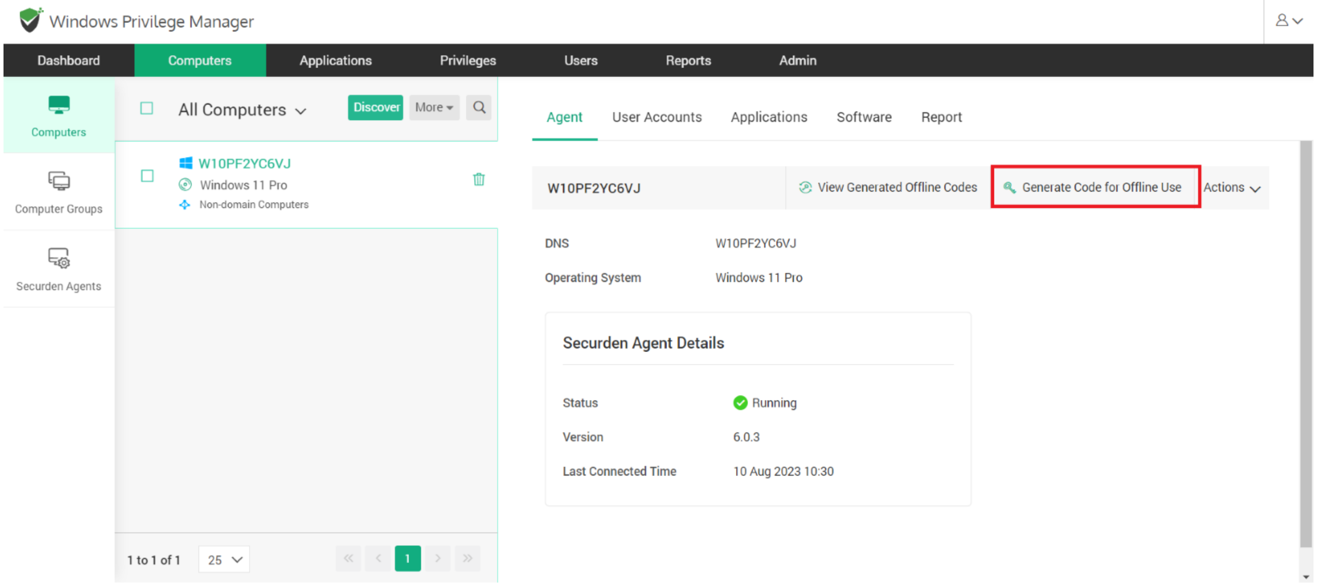
Note: Once a specific code is used, it becomes inactive and cannot be used again.

In case, the users fail to generate offline codes themselves, they may request an administrator to generate a code for them.

Administrators Generating Codes for Users

To elevate applications using offline codes for users, administrators may generate the offline code. This can be done in the absence of agent-server connectivity, in the case a user goes offline without generating offline codes.

To generate a code, administrators may navigate to **Computers >> Select a computer** and click on **Generate an offline code**.



W10PF2YC6VJ

DNS W10PF2YC6VJ

Operating System Windows 11 Pro

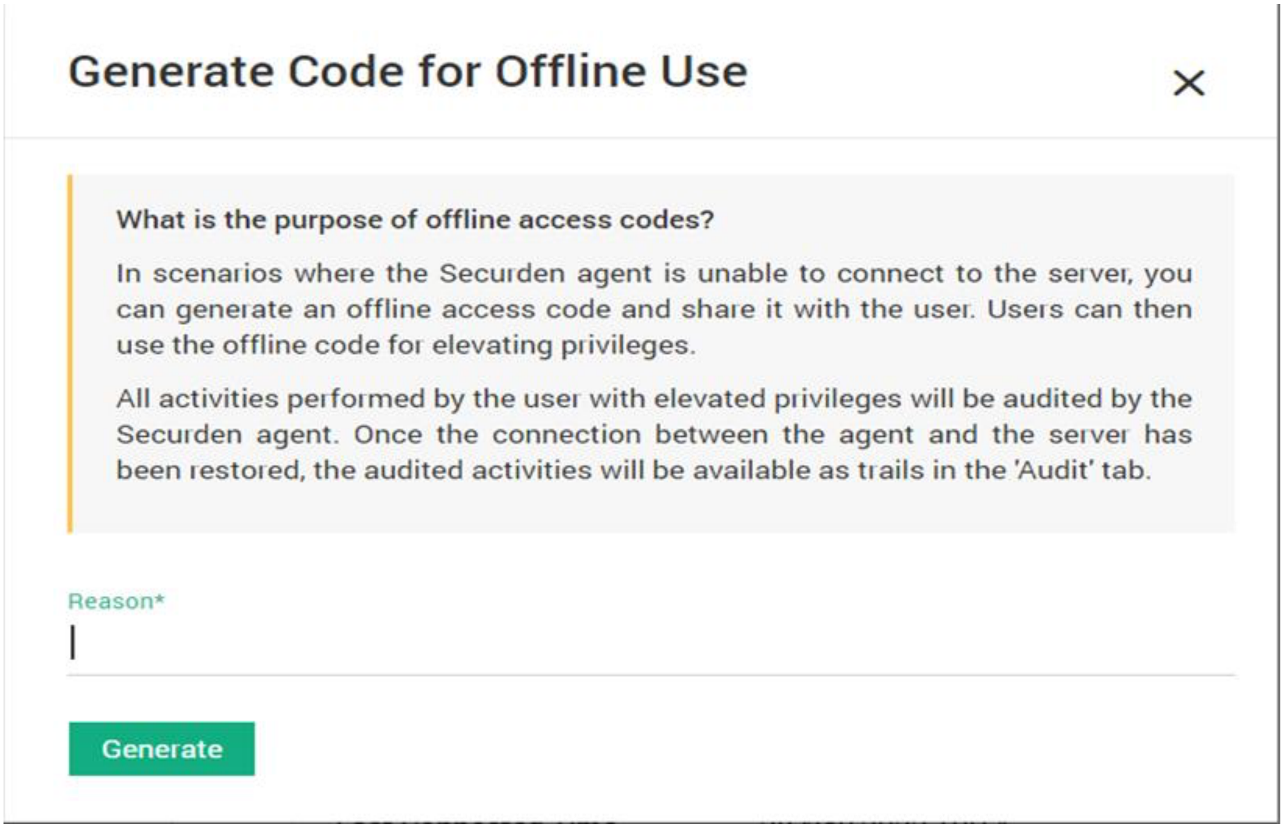
Securden Agent Details

Status ✓ Running

Version 6.0.3

Last Connected Time 10 Aug 2023 10:30

The administrator has to provide a reason for generating offline access code in this GUI. After providing the reason, click **Generate**.



Generate Code for Offline Use ×

What is the purpose of offline access codes?

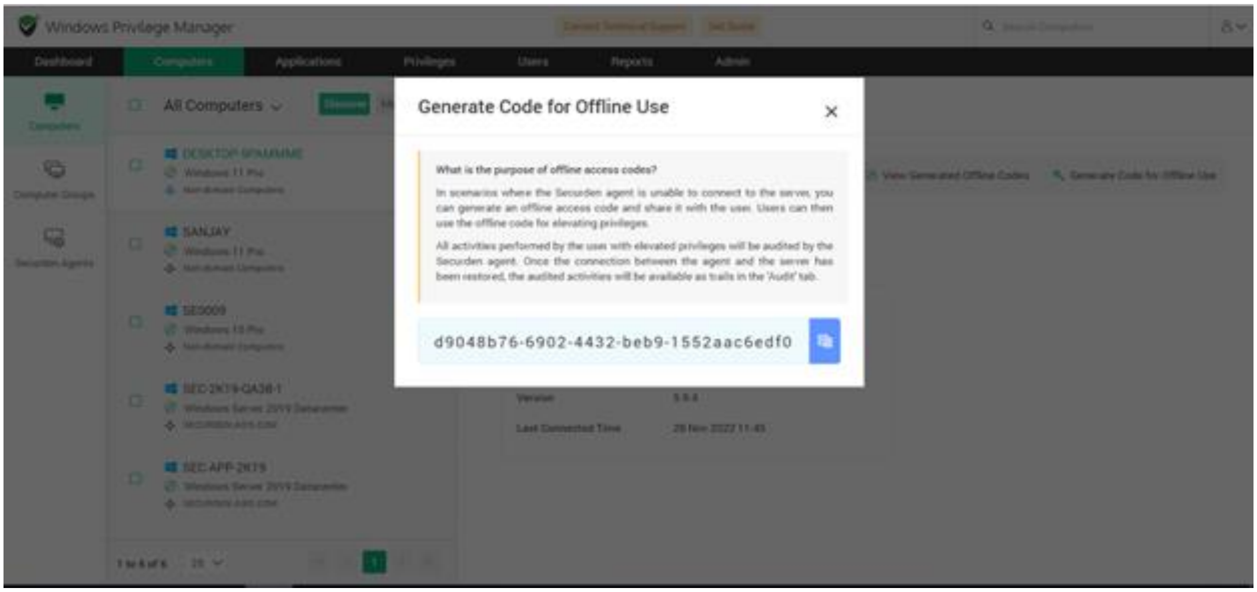
In scenarios where the Securden agent is unable to connect to the server, you can generate an offline access code and share it with the user. Users can then use the offline code for elevating privileges.

All activities performed by the user with elevated privileges will be audited by the Securden agent. Once the connection between the agent and the server has been restored, the audited activities will be available as trails in the 'Audit' tab.

Reason*

Generate

On generating the code, the administrator may copy the offline code(s) and share it with the user by any means.



Generate Code for Offline Use

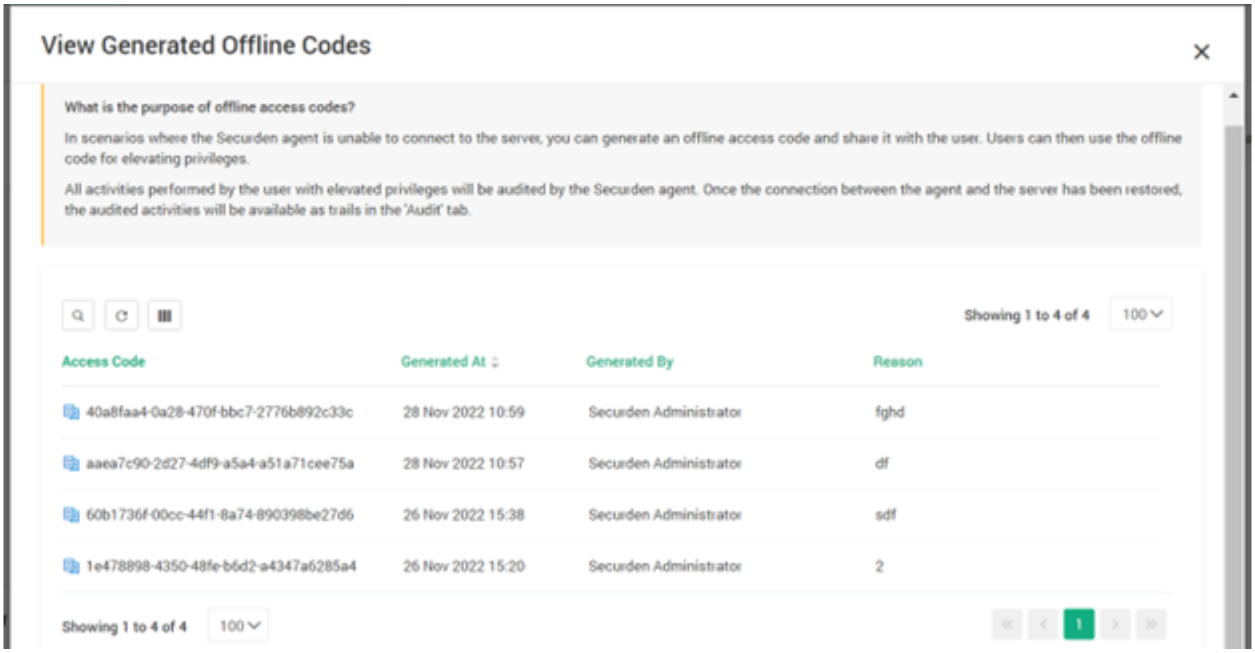
What is the purpose of offline access codes?

In scenarios where the Securden agent is unable to connect to the server, you can generate an offline access code and share it with the user. Users can then use the offline code for elevating privileges.

All activities performed by the user with elevated privileges will be audited by the Securden agent. Once the connection between the agent and the server has been restored, the audited activities will be available as trails in the 'Audit' tab.

d9048b76-6902-4432-beb9-1552aac6edf0

Previously generated codes are also accessible to administrators from **View Generated Offline Codes**.



View Generated Offline Codes

What is the purpose of offline access codes?

In scenarios where the Securden agent is unable to connect to the server, you can generate an offline access code and share it with the user. Users can then use the offline code for elevating privileges.

All activities performed by the user with elevated privileges will be audited by the Securden agent. Once the connection between the agent and the server has been restored, the audited activities will be available as trails in the 'Audit' tab.

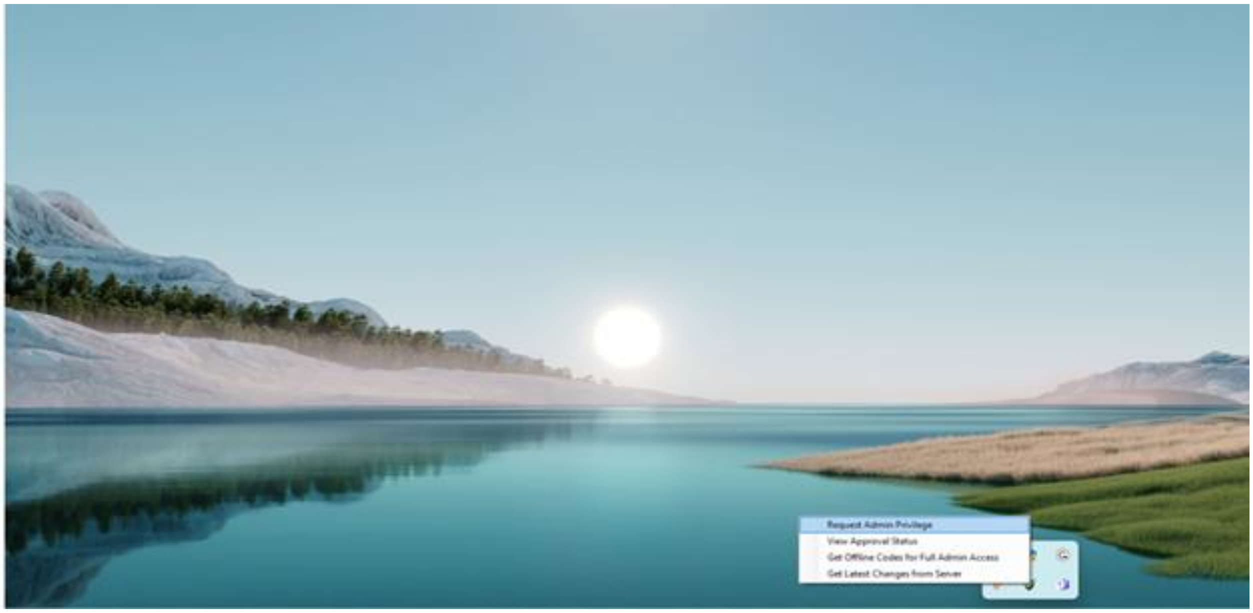
Showing 1 to 4 of 4 100

Access Code	Generated At	Generated By	Reason
40a8faa4-0a28-470f-bbc7-2776b892c33c	28 Nov 2022 10:59	Securden Administrator	fghd
aaea7c90-2d27-4df9-a5a4-a51a71cee75a	28 Nov 2022 10:57	Securden Administrator	df
60b1736f-00cc-44f1-8a74-890398be27d6	26 Nov 2022 15:38	Securden Administrator	sdf
1e478898-4350-48fe-b6d2-a4347a6285a4	26 Nov 2022 15:20	Securden Administrator	2

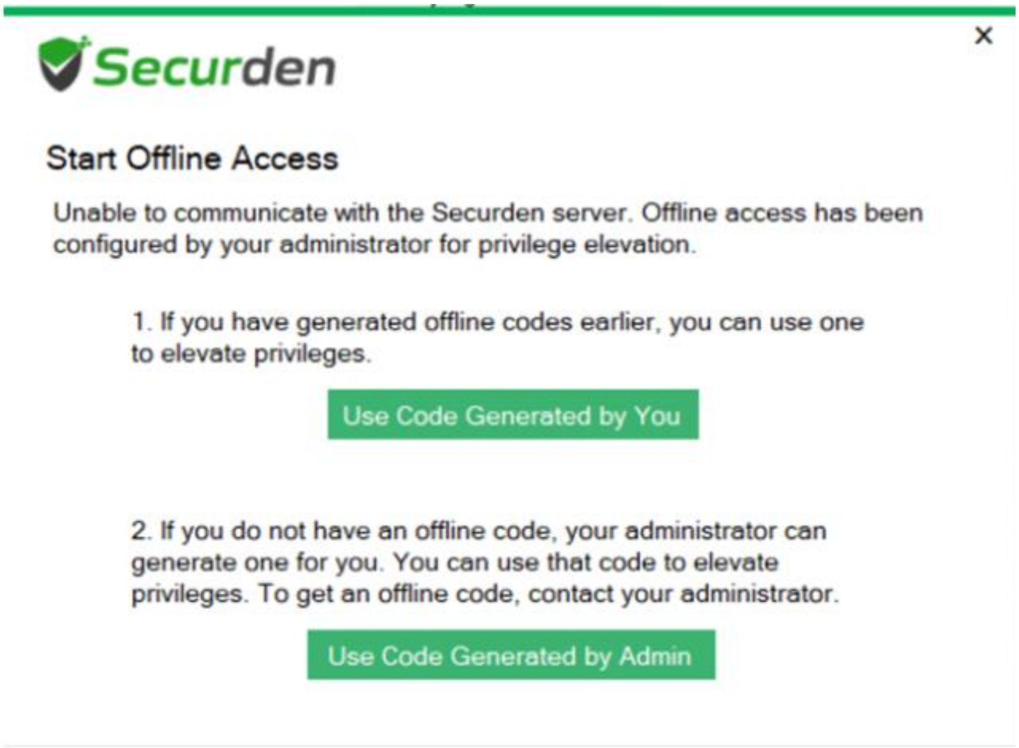
Showing 1 to 4 of 4 100

Elevating an Application Using Admin-Generated Offline Codes

When the Securden Agent cannot establish connectivity with the WPM server, a pop-up window appears when you try to run an application with Securden Privilege. (Either by clicking **Request Admin Privilege** or by running an application with administrator privilege)


Request Admin Privilege
View Approval Status
Get Offline Codes for Full Admin Access
Get Latest Changes from Server

In the pop-up window that appears, users may click on **Use Code Generated by Admin**.



Securden

Start Offline Access

Unable to communicate with the Securden server. Offline access has been configured by your administrator for privilege elevation.

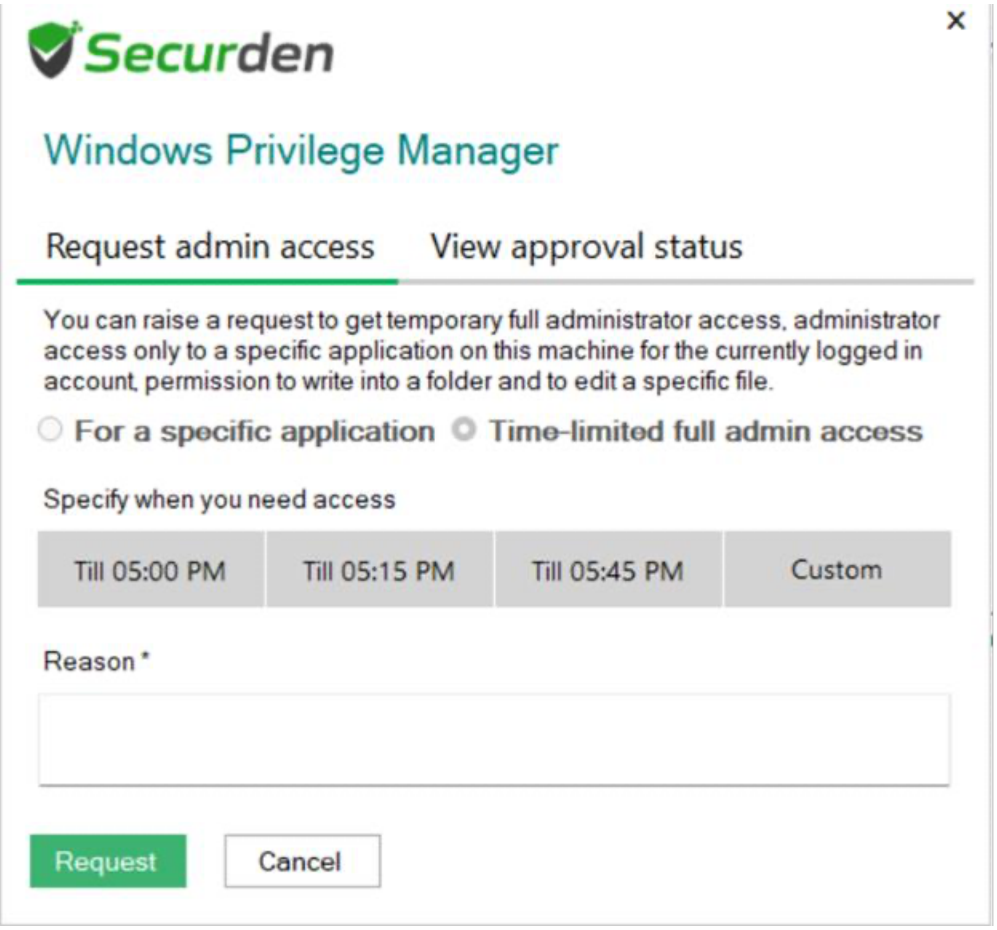
1. If you have generated offline codes earlier, you can use one to elevate privileges.

2. If you do not have an offline code, your administrator can generate one for you. You can use that code to elevate privileges. To get an offline code, contact your administrator.

In the window that opens, they may select **For a specific application** (or) **Time-limited full admin access** based on the requirement.

Users have to specify the time until when they might need access, and the reason to why they need to elevate the application.

After furnishing the required details, they click **Request**.



Securden

Windows Privilege Manager

Request admin access | View approval status

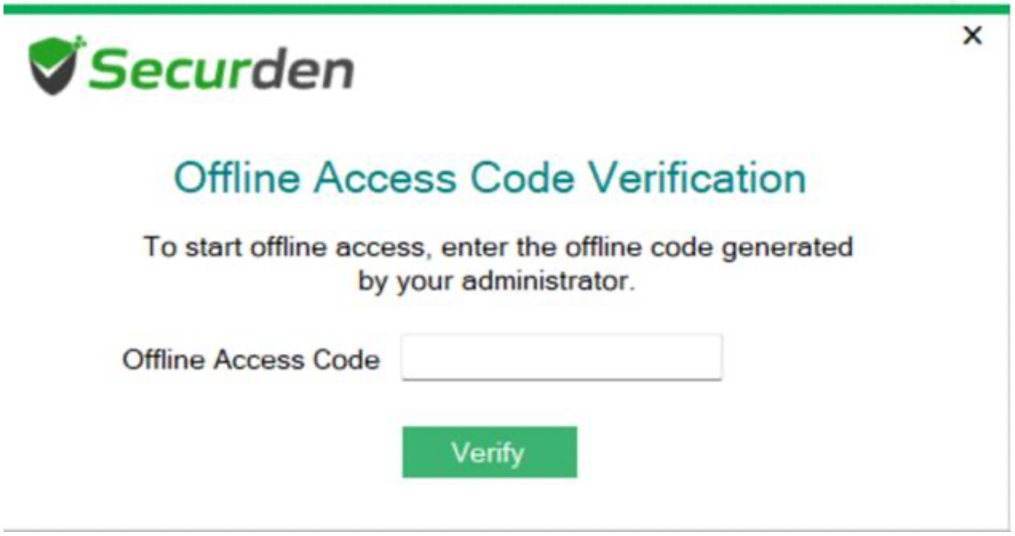
You can raise a request to get temporary full administrator access, administrator access only to a specific application on this machine for the currently logged in account, permission to write into a folder and to edit a specific file.

○ For a specific application ● Time-limited full admin access

Specify when you need access

Reason *

When the agent cannot establish connectivity with the server, the window shown below pops up. You need to paste one of the active offline codes in the field and click **Verify**.



Securden

Offline Access Code Verification

To start offline access, enter the offline code generated by your administrator.

Offline Access Code

Once the code is verified, access will be granted and the user can start using the application.

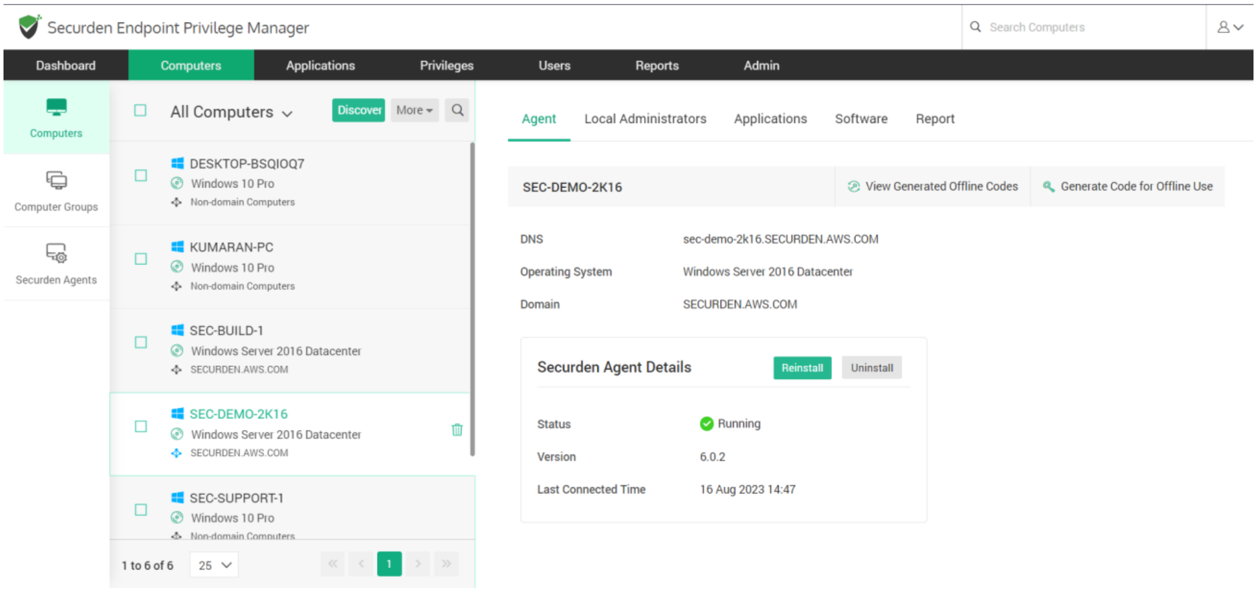
Note: Access will be revoked just as soon as the duration expires and all activities performed within this time will be recorded locally by the agent. These recorded activities will be populated in the Audit section of WPM once connectivity is re-established.

Once a specific offline code is used, it becomes inactive and cannot be used again.

Management Operations from Computers Tab

Monitor the Securden Agent

You can check the attributes of agents present on each computer in the **Computer >> Agent** section. Computer details such as name, DNS, and operating system version along with the Agent details such as version, status, and time when the agent last connected with Securden can be viewed in this section.



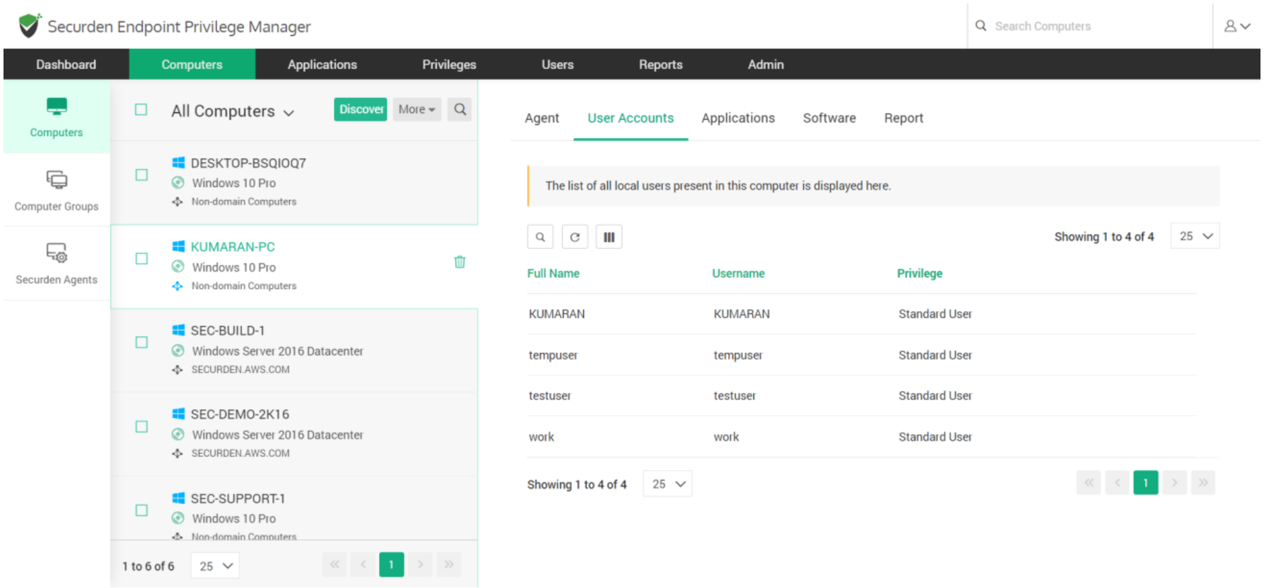
SEC-DEMO-2K16

DNS	sec-demo-2k16.SECURDEN.AWS.COM
Operating System	Windows Server 2016 Datacenter
Domain	SECURDEN.AWS.COM

Securden Agent Details

Status	✓ Running
Version	6.0.2
Last Connected Time	16 Aug 2023 14:47

A list containing all local users or administrators present on each computer can be viewed in **Computers >> User Accounts / Local Administrators** (as shown below). You can use the column chooser to filter the list and search for users.



The list of all local users present in this computer is displayed here.

Full Name	Username	Privilege
KUMARAN	KUMARAN	Standard User
tempuser	tempuser	Standard User
testuser	testuser	Standard User
work	work	Standard User

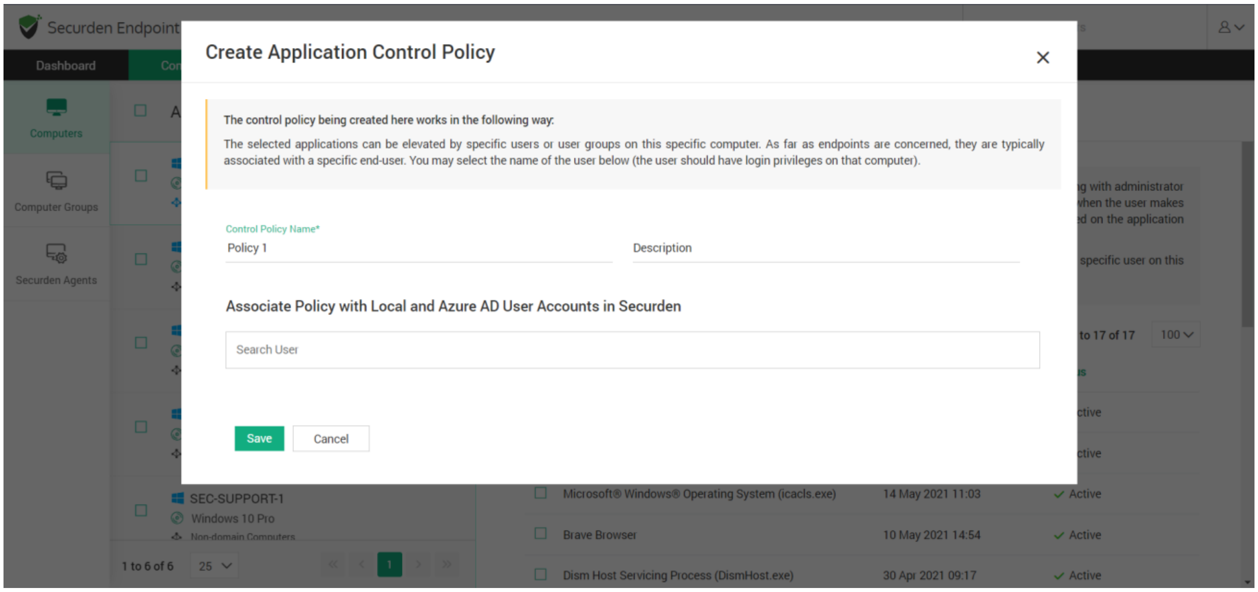
Application Policies for Specific Computers

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.

Once applications are discovered and added to the list, you can whitelist these applications from the **Computers >> Application** section. You can either create new control policies for selected applications or add selected applications to existing control policies by navigating to **Computers >> Applications**.

Note: The policies created from this GUI will be associated with this computer alone. It will not be enforced on any other endpoint in the repository.

You can create a new control policy for specific users using this computer from the **Computers >> Applications** section. Once the policy is enforced, the selected application will be elevated on this computer for the specified user automatically.



Create Application Control Policy

The control policy being created here works in the following way:

The selected applications can be elevated by specific users or user groups on this specific computer. As far as endpoints are concerned, they are typically associated with a specific end-user. You may select the name of the user below (the user should have login privileges on that computer).

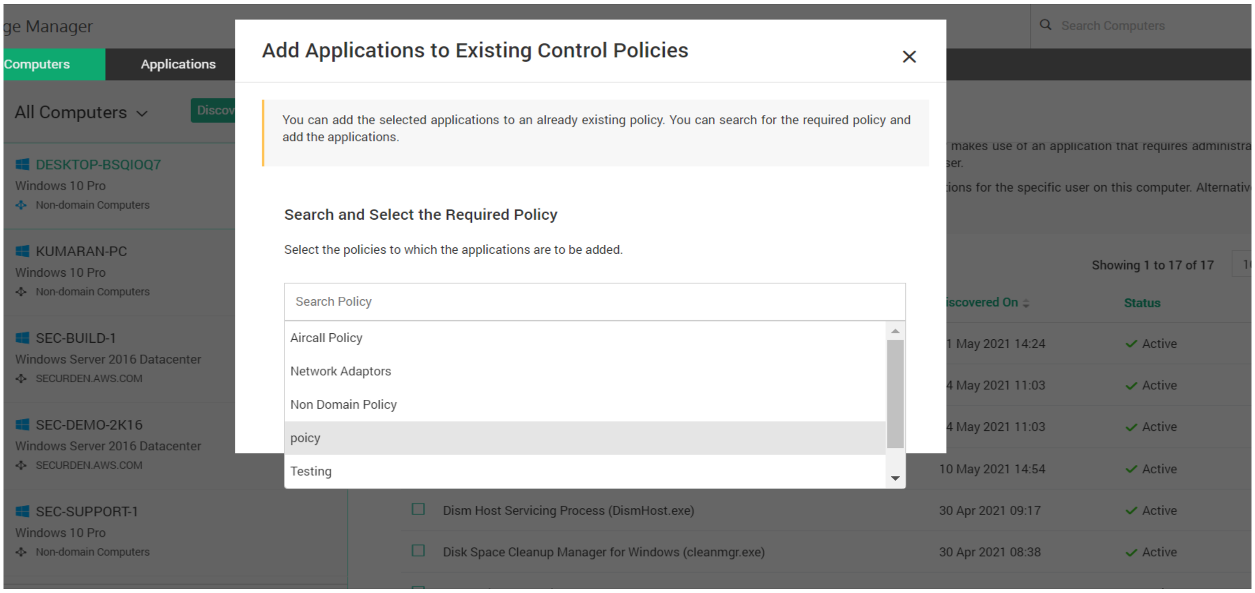
Control Policy Name*: Policy 1

Description

Associate Policy with Local and Azure AD User Accounts in Securden

Search User

To add applications to an existing policy, select the applications and click **Add to Existing Policies**. You can search the existing policies from the drop-down and select the required policy. This application will be added to the selected application control policy and will be elevated in accordance with the policy specifications.



Add Applications to Existing Control Policies

You can add the selected applications to an already existing policy. You can search for the required policy and add the applications.

Search and Select the Required Policy

Select the policies to which the applications are to be added.

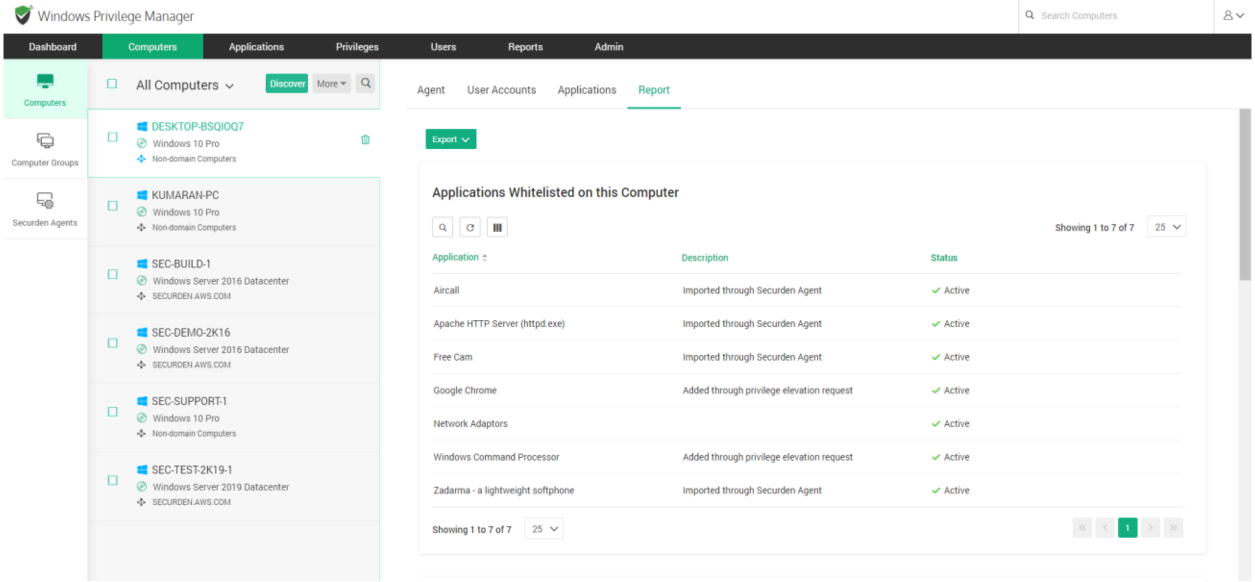
Search Policy

- Aircall Policy
- Network Adaptors
- Non Domain Policy
- poicy
- Testing

Dism Host Servicing Process (DismHost.exe)	30 Apr 2021 09:17	✓ Active
Disk Space Cleanup Manager for Windows (cleanmgr.exe)	30 Apr 2021 08:38	✓ Active

Computer Specific Reports

In this section, you can view analytical reports on applications that are whitelisted and blacklisted on the selected computer along with the list of elevated applications and processes.



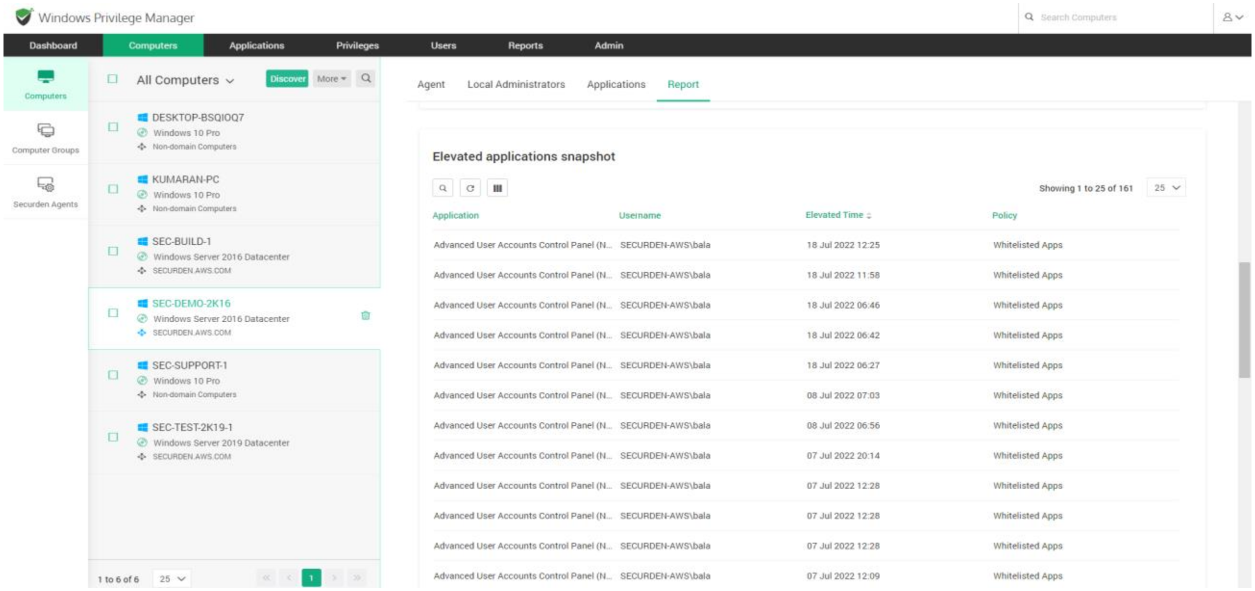
Applications Whitelisted on this Computer

Showing 1 to 7 of 7

Application	Description	Status
Aircall	Imported through Securden Agent	✓ Active
Apache HTTP Server (httpd.exe)	Imported through Securden Agent	✓ Active
Free Cam	Imported through Securden Agent	✓ Active
Google Chrome	Added through privilege elevation request	✓ Active
Network Adaptors		✓ Active
Windows Command Processor	Added through privilege elevation request	✓ Active
Zadarma - a lightweight softphone	Imported through Securden Agent	✓ Active

Showing 1 to 7 of 7

The whitelisted and blacklisted applications are displayed along with their application status.



Elevated applications snapshot

Showing 1 to 25 of 161 25

Application	Username	Elevated Time	Policy
Advanced User Accounts Control Panel (N...	SECURDEN-AWS\bala	18 Jul 2022 12:25	Whitelisted Apps
Advanced User Accounts Control Panel (N...	SECURDEN-AWS\bala	18 Jul 2022 11:58	Whitelisted Apps
Advanced User Accounts Control Panel (N...	SECURDEN-AWS\bala	18 Jul 2022 06:46	Whitelisted Apps
Advanced User Accounts Control Panel (N...	SECURDEN-AWS\bala	18 Jul 2022 06:42	Whitelisted Apps
Advanced User Accounts Control Panel (N...	SECURDEN-AWS\bala	18 Jul 2022 06:27	Whitelisted Apps
Advanced User Accounts Control Panel (N...	SECURDEN-AWS\bala	08 Jul 2022 07:03	Whitelisted Apps
Advanced User Accounts Control Panel (N...	SECURDEN-AWS\bala	08 Jul 2022 06:56	Whitelisted Apps
Advanced User Accounts Control Panel (N...	SECURDEN-AWS\bala	07 Jul 2022 20:14	Whitelisted Apps
Advanced User Accounts Control Panel (N...	SECURDEN-AWS\bala	07 Jul 2022 12:28	Whitelisted Apps
Advanced User Accounts Control Panel (N...	SECURDEN-AWS\bala	07 Jul 2022 12:28	Whitelisted Apps
Advanced User Accounts Control Panel (N...	SECURDEN-AWS\bala	07 Jul 2022 12:28	Whitelisted Apps
Advanced User Accounts Control Panel (N...	SECURDEN-AWS\bala	07 Jul 2022 12:09	Whitelisted Apps

You will also be able to view the list of all applications elevated on the selected endpoint and the policy using which the application was elevated.

SECTION 5: High Availability

Configure High Availability

Securden comes with high availability architecture to ensure an uninterrupted and reliable supply of credentials.

Configuring High Availability (with PostgreSQL database as the backend)

To configure high availability in Securden WPM, two or more servers have to be deployed.

1. Primary server with bundled PostgreSQL database.
2. One secondary standby server with a 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 a 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 (5252) 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 WPM 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 Server
Step 3	Downloading and Transferring download package
Step 4	Configuring the Secondary Server
Step 5	Verifying the High Availability Setup

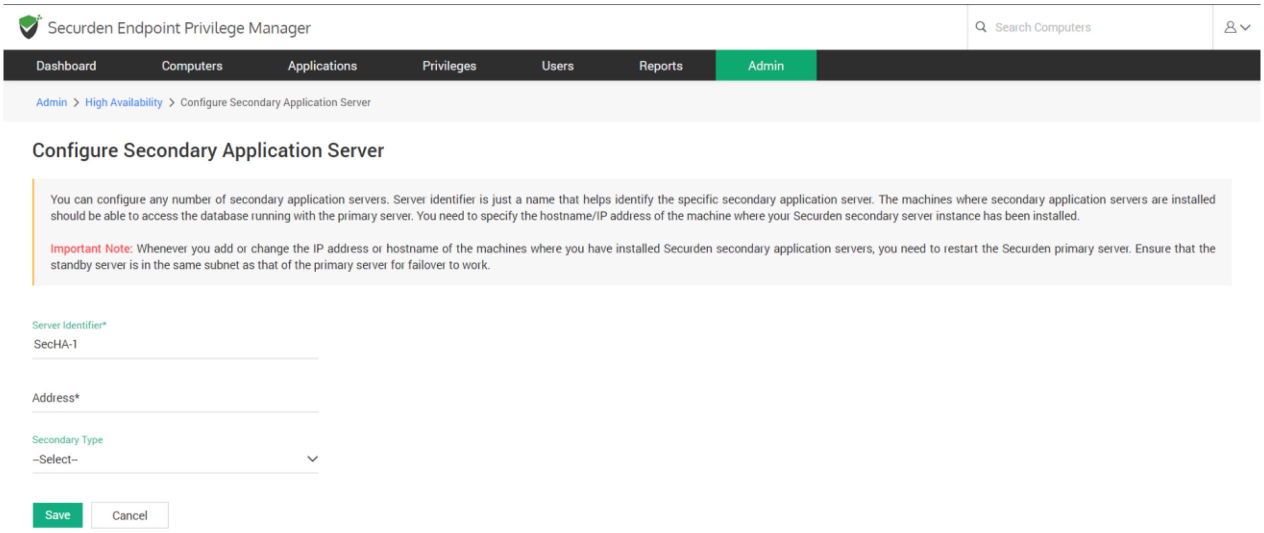
Step 1: Setting up a Secondary Server

1. Identify a machine that would act as a secondary server. Consider the current Securden WPM installation as the primary server.
2. Install Securden WPM 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 WPM. 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 WPM in the primary server.


Securden Endpoint Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > High Availability > Configure Secondary Application Server
Save
Cancel

Configure Secondary Application Server

You can configure any number of secondary application servers. Server identifier is just a name that helps identify the specific secondary application server. The machines where secondary application servers are installed should be able to access the database running with the primary server. You need to specify the hostname/IP address of the machine where your Securden secondary server instance has been installed.

Important Note: Whenever you add or change the IP address or hostname of the machines where you have installed Securden secondary 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.

Server Identifier* SecHA-1

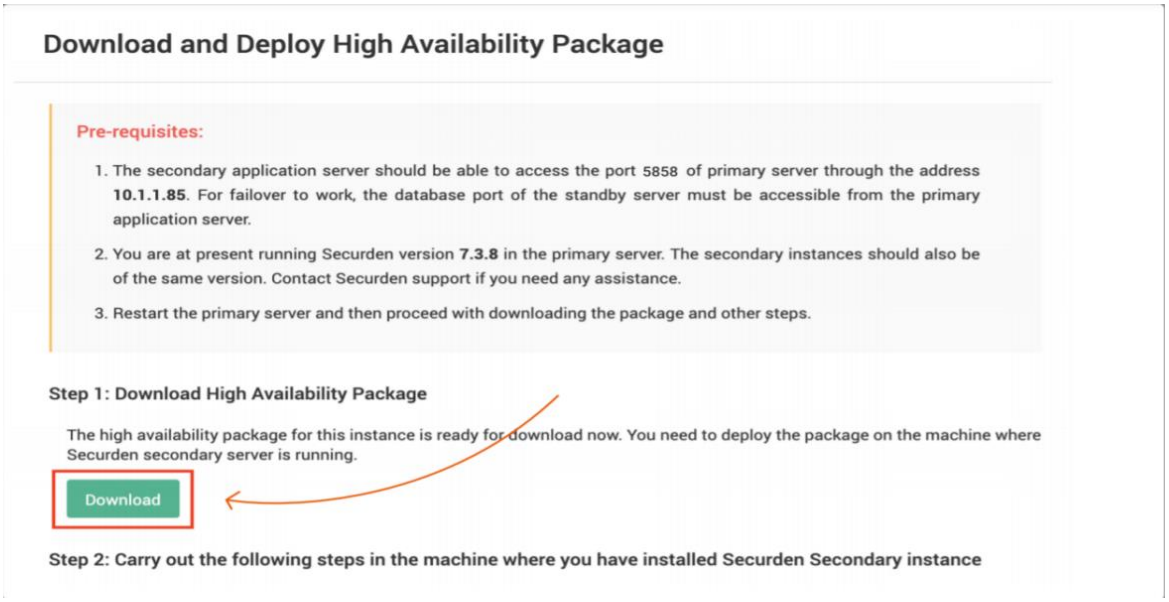
Address*

Secondary Type --Select--

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.
   c. **Secondary Type** - Two types of secondary servers can be deployed: An application server without a 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.

   Download and Deploy High Availability Package

   Pre-requisites:

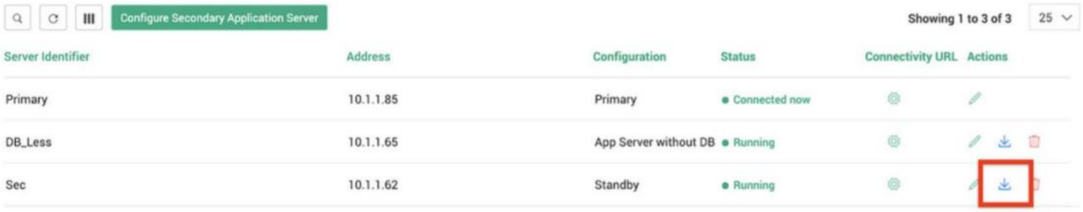
   1. The secondary application server should be able to access the port 5858 of primary server through the address **10.1.1.85**. For failover to work, the database port of the standby server must be accessible from the primary application server.
   2. You are at present running Securden version **7.3.8** in the primary server. The secondary instances should also be of the same version. Contact Securden support if you need any assistance.
   3. Restart the primary server and then proceed with downloading the package and other steps.

   Step 1: Download High Availability Package

   The high availability package for this instance is ready for download now. You need to deploy the package on the machine where Securden secondary server is running.

   Step 2: Carry out the following steps in the machine where you have installed Securden Secondary instance

   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.

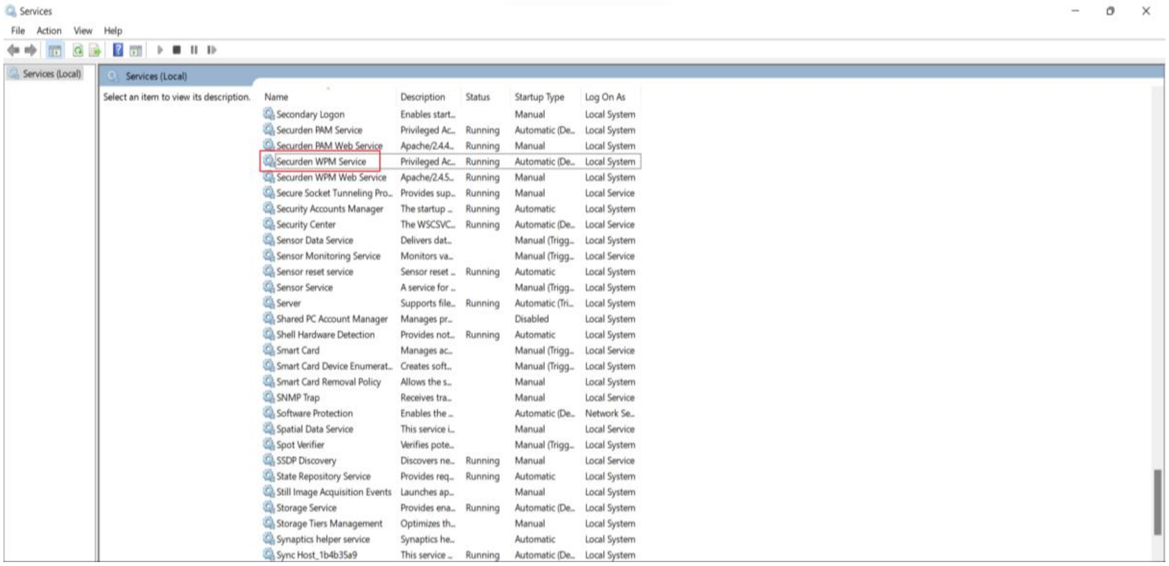
   

Server Identifier	Address	Configuration	Status	Connectivity URL	Actions
Primary	10.1.1.85	Primary	● Connected now		
DB_Less	10.1.1.65	App Server without DB	● Running		
Sec	10.1.1.62	Standby	● Running		

2. Transfer the downloaded zip file to the secondary server.

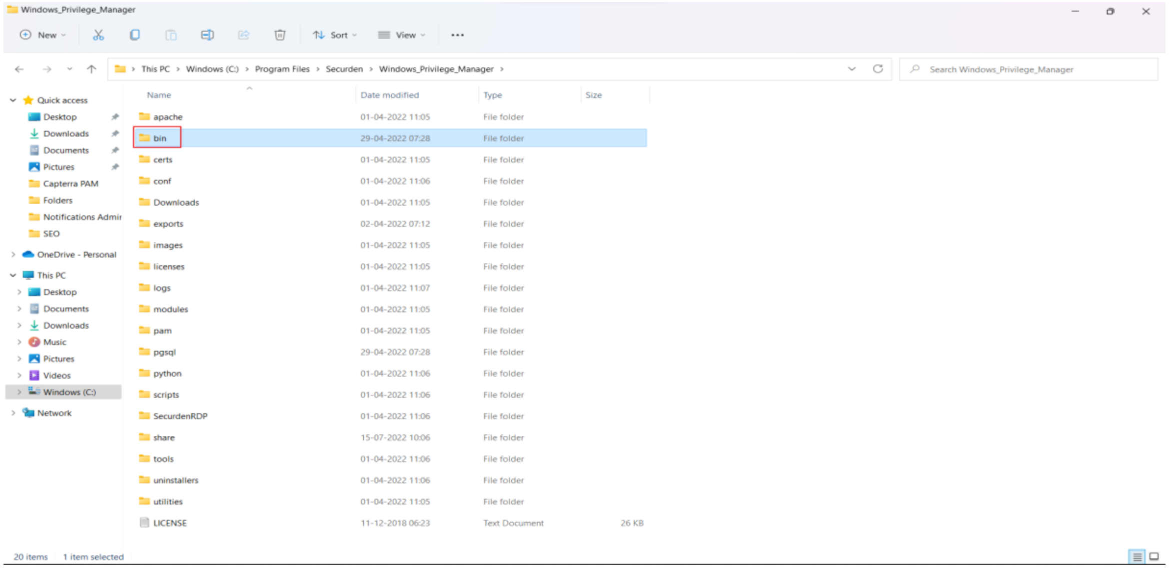
Step 4: Configuring the secondary server

1. Stop the server if it is running. Open windows service manager (run **services.msc**) and stop Securden WPM Service.



Name	Description	Status	Startup Type	Log On As
Secondary Logon	Enables start...		Manual	Local System
Securden PAM Service	Privileged Ac...	Running	Automatic (De...	Local System
Securden PAM Web Service	Apache/2.4.4...	Running	Manual	Local System
Securden WPM Service	Privileged Ac...	Running	Automatic (De...	Local System
Securden WPM Web Service	Apache/2.4.5...	Running	Manual	Local System
Secure Socket Tunneling Pro...	Provides sup...	Running	Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local System
Security Center	The WSCSVC...	Running	Automatic (De...	Local Service
Sensor Data Service	Delivers dat...		Manual (Trigg...	Local System
Sensor Monitoring Service	Monitors va...		Manual (Trigg...	Local Service
Sensor reset service	Sensor reset ...	Running	Automatic	Local System
Sensor Service	A service for ...		Manual (Trigg...	Local System
Server	Supports file...	Running	Automatic (Tri...	Local System
Shared PC Account Manager	Manages pr...		Disabled	Local System
Shell Hardware Detection	Provides not...	Running	Automatic	Local System
Smart Card	Manages ac...		Manual (Trigg...	Local Service
Smart Card Device Enumerat...	Creates soft...		Manual (Trigg...	Local System
Smart Card Removal Policy	Allows the s...		Manual	Local System
SNMP Trap	Receives tra...		Manual	Local Service
Software Protection	Enables the ...		Automatic (De...	Network Se...
Spatial Data Service	This service i...		Manual	Local Service
Spot Verifier	Verifies pote...		Manual (Trigg...	Local System
SSDP Discovery	Discovers ne...	Running	Manual	Local Service
State Repository Service	Provides req...	Running	Automatic	Local System
Still Image Acquisition Events	Launches ap...		Manual	Local System
Storage Service	Provides ena...	Running	Automatic (De...	Local System
Storage Tiers Management	Optimizes th...		Manual	Local System
Synaptics helper service	Synaptics he...		Automatic	Local System
Sync Host_1b4b35a9	This service ...	Running	Automatic (De...	Local System

2. Put the high availability package under the **/bin** directory in the installation folder on the **Secondary Server**.



Name	Date modified	Type	Size
apache	01-04-2022 11:05	File folder	
bin	29-04-2022 07:28	File folder	
certs	01-04-2022 11:05	File folder	
conf	01-04-2022 11:06	File folder	
Downloads	01-04-2022 11:05	File folder	
exports	02-04-2022 07:12	File folder	
images	01-04-2022 11:05	File folder	
licenses	01-04-2022 11:05	File folder	
logs	01-04-2022 11:07	File folder	
modules	01-04-2022 11:05	File folder	
pam	01-04-2022 11:05	File folder	
pgsql	29-04-2022 07:28	File folder	
python	01-04-2022 11:06	File folder	
scripts	01-04-2022 11:06	File folder	
SecurdenRDP	01-04-2022 11:06	File folder	
share	15-07-2022 10:06	File folder	
tools	01-04-2022 11:06	File folder	
uninstallers	01-04-2022 11:06	File folder	
utilities	01-04-2022 11:05	File folder	
LICENSE	11-12-2018 06:23	Text Document	26 KB

20 items 1 item selected

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 **/conf/securden_key.location** is accessible from the secondary server. (You can open securden_key.location using 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 WPM 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 and working properly.

Deploying additional secondary application servers without DB (Optional)

You can deploy any number of secondary application servers without a 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 a database, follow Step 1 through Step 5 again, and except for **Standby** as a secondary type in Step 2, select **App server without DB**.

Troubleshooting Tips

Issue: 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 (5151) 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 5151
In primary server: Telnet 5151

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,5151
5.	Action: Allow the connection
6.	Profile: Domain, Private, Public
7.	Name(Example): TCP5151
8.	Click **Finish**

Configuring High availability with MS SQL Server as the Backend Database

To configure High availability in Securden WPM, you will need two or more application servers and a database server with an 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 Always On high availability groups.

Prerequisites: A primary server with Securden WPM 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 SQLserver** 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

3. Identify a machine that would act as a secondary server. Consider the current Securden WPM installation as the primary server.
4. Install Securden WPM 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 WPM. Navigate to **User Details** (On the top right corner) **>> About >> Version** to check for the current product version. Contact Securden support for any assistance.

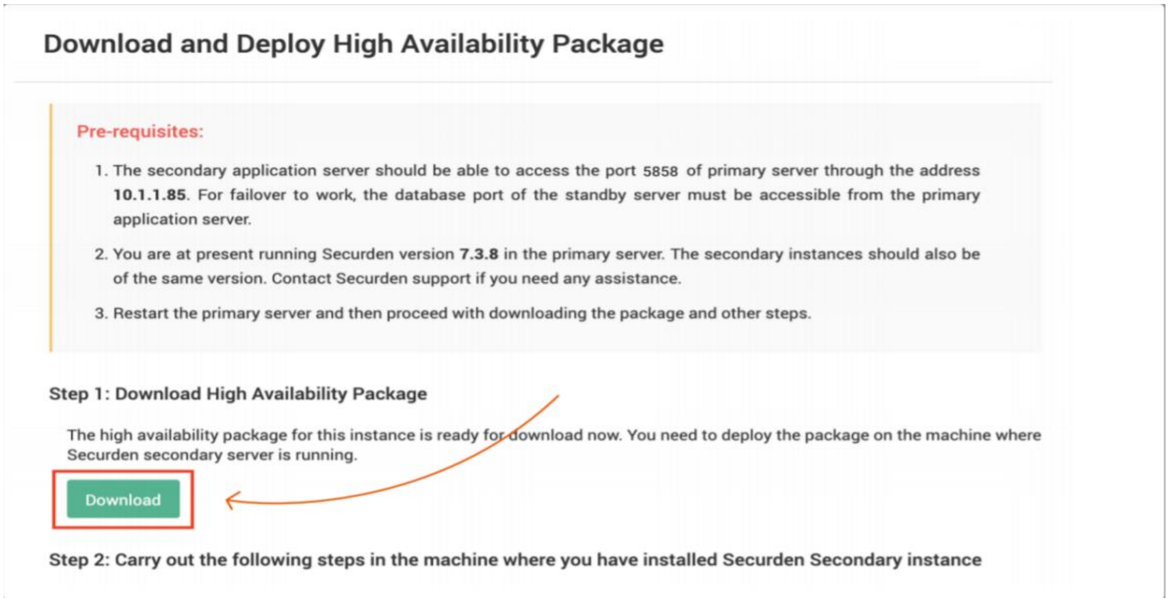
Step 2: Configuring HA in the primary server

1. Navigate to **Admin>> High Availability** in the GUI of Securden WPM 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 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



Download and Deploy High Availability Package

Pre-requisites:

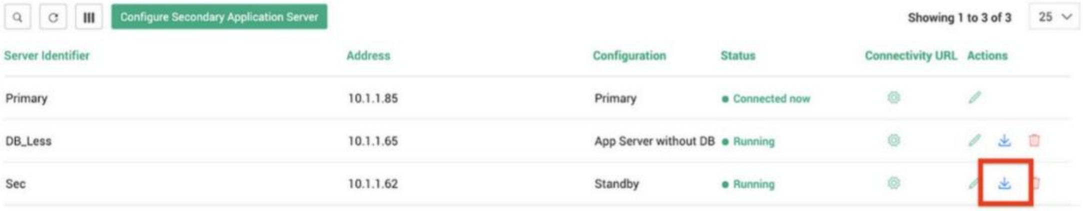
1. The secondary application server should be able to access the port 5858 of primary server through the address **10.1.1.85**. For failover to work, the database port of the standby server must be accessible from the primary application server.
2. You are at present running Securden version **7.3.8** in the primary server. The secondary instances should also be of the same version. Contact Securden support if you need any assistance.
3. Restart the primary server and then proceed with downloading the package and other steps.

Step 1: Download High Availability Package

The high availability package for this instance is ready for download now. You need to deploy the package on the machine where Securden secondary server is running.

Step 2: Carry out the following steps in the machine where you have installed Securden Secondary instance

2. 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.



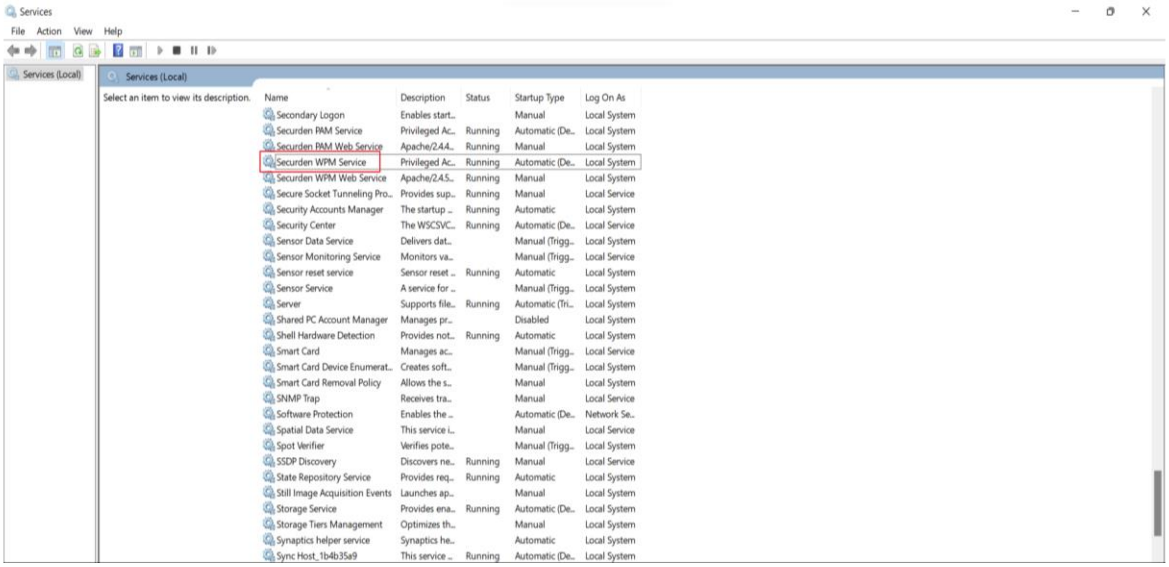
Showing 1 to 3 of 3 | 25

Server Identifier	Address	Configuration	Status	Connectivity URL	Actions
Primary	10.1.1.85	Primary	● Connected now	⚙	✎
DB_Less	10.1.1.65	App Server without DB	● Running	⚙	✎ ⤓ 🗑
Sec	10.1.1.62	Standby	● Running	⚙	✎ ⤓ 🗑

3. Transfer the downloaded zip file to the secondary server.

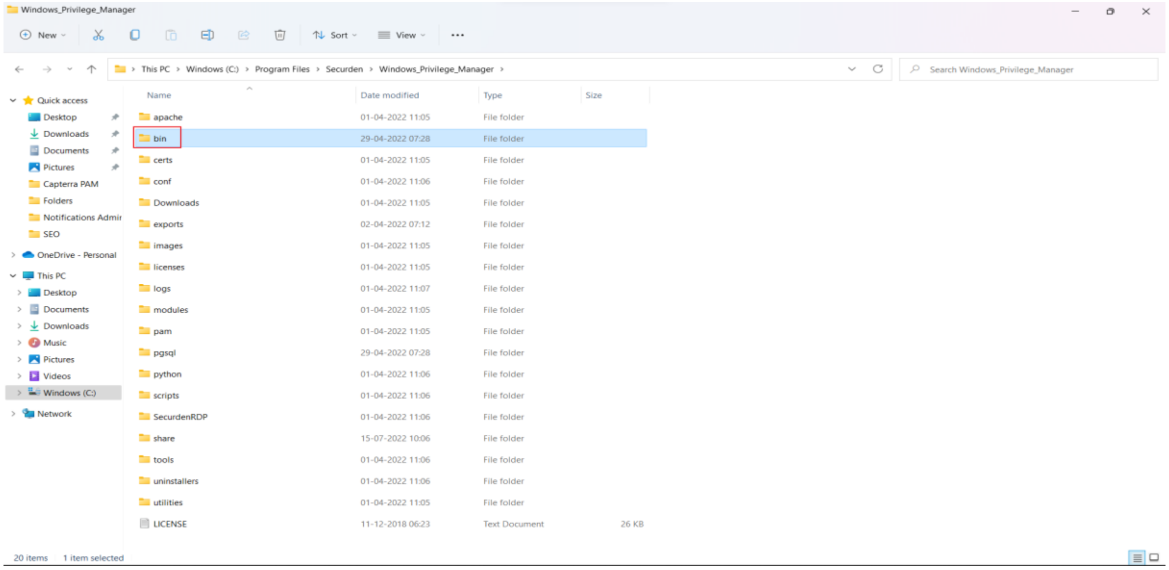
Step 4: Configuring the secondary server

1. Stop the server if it is running. Open windows service manager (run **services.msc**) and stop Securden WPM service.



Name	Description	Status	Startup Type	Log On As
Secondary Logon	Enables start...		Manual	Local System
Securden PAM Service	Privileged Ac...	Running	Automatic (De...	Local System
Securden PAM Web Service	Apache/2.4.4...	Running	Manual	Local System
Securden WPM Service	Privileged Ac...	Running	Automatic (De...	Local System
Securden WPM Web Service	Apache/2.4.5...	Running	Manual	Local System
Secure Socket Tunneling Pro...	Provides sup...	Running	Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local System
Security Center	The WSCSVC...	Running	Automatic (De...	Local Service
Sensor Data Service	Delivers dat...		Manual (Trigg...	Local System
Sensor Monitoring Service	Monitors va...		Manual (Trigg...	Local Service
Sensor reset service	Sensor reset ...	Running	Automatic	Local System
Sensor Service	A service for ...		Manual (Trigg...	Local System
Server	Supports file...	Running	Automatic (Tri...	Local System
Shared PC Account Manager	Manages pr...		Disabled	Local System
Shell Hardware Detection	Provides not...	Running	Automatic	Local System
Smart Card	Manages ac...		Manual (Trigg...	Local Service
Smart Card Device Enumerat...	Creates soft...		Manual (Trigg...	Local System
Smart Card Removal Policy	Allows the s...		Manual	Local System
SNMP Trap	Receives tra...		Manual	Local Service
Software Protection	Enables the ...		Automatic (De...	Network Se...
Spatial Data Service	This service i...		Manual	Local Service
Spot Verifier	Verifies pote...		Manual (Trigg...	Local System
SSDP Discovery	Discovers ne...	Running	Manual	Local Service
State Repository Service	Provides req...	Running	Automatic	Local System
Still Image Acquisition Events	Launches ap...		Manual	Local System
Storage Service	Provides ena...	Running	Automatic (De...	Local System
Storage Tiers Management	Optimizes th...		Manual	Local System
Synaptics helper service	Synaptics he...		Automatic	Local System
Sync Host_1b4b35a9	This service ...	Running	Automatic (De...	Local System

2. Put the high availability package under the **/bin** directory in the installation folder on the **Secondary Server**.



Name	Date modified	Type	Size
apache	01-04-2022 11:05	File folder	
bin	29-04-2022 07:28	File folder	
certs	01-04-2022 11:05	File folder	
conf	01-04-2022 11:06	File folder	
Downloads	01-04-2022 11:05	File folder	
exports	02-04-2022 07:12	File folder	
images	01-04-2022 11:05	File folder	
licenses	01-04-2022 11:05	File folder	
logs	01-04-2022 11:07	File folder	
modules	01-04-2022 11:05	File folder	
pam	01-04-2022 11:05	File folder	
pgsql	29-04-2022 07:28	File folder	
python	01-04-2022 11:06	File folder	
scripts	01-04-2022 11:06	File folder	
SecurdenRDP	01-04-2022 11:06	File folder	
share	15-07-2022 10:06	File folder	
tools	01-04-2022 11:06	File folder	
uninstallers	01-04-2022 11:06	File folder	
utilities	01-04-2022 11:05	File folder	
LICENSE	11-12-2018 06:23	Text Document	26 KB

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 **/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 WPM service.

Securden High availability setup is now ready.

Step 5: Verifying High Availability

3. Navigate to **Admin>>High availability** in the GUI of the primary server.
4. 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 **/conf/securden_key.location** is accessible from the secondary server. (You can open securden_key.location with any text editor)

Solution 3: Database port (by default 1433) of MS SQL and web server port (5151) should be accessible from the secondary server.
Run the following telnet commands in your secondary server to verify the connections:

```
Telnet <database server address> <Port Number>
Telnet <primary server address> 5151
```

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): TCP5151
8.	Click **Finish**

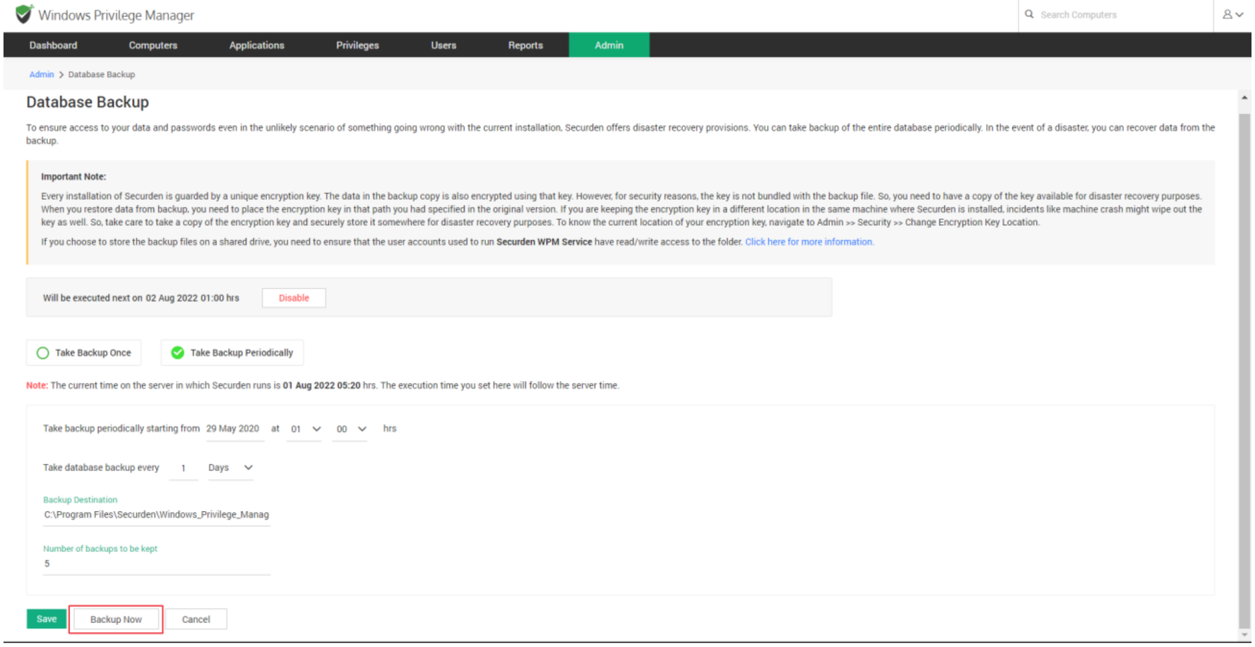
Database Backup

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**.



Database Backup

To ensure access to your data and passwords even in the unlikely scenario of something going wrong with the current installation, Securden offers disaster recovery provisions. You can take backup of the entire database periodically. In the event of a disaster, you can recover data from the backup.

Important Note:

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

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

Will be executed next on 02 Aug 2022 01:00 hrs Disable

○ Take Backup Once ● Take Backup Periodically

Note: The current time on the server in which Securden runs is **01 Aug 2022 05:20** hrs. The execution time you set here will follow the server time.

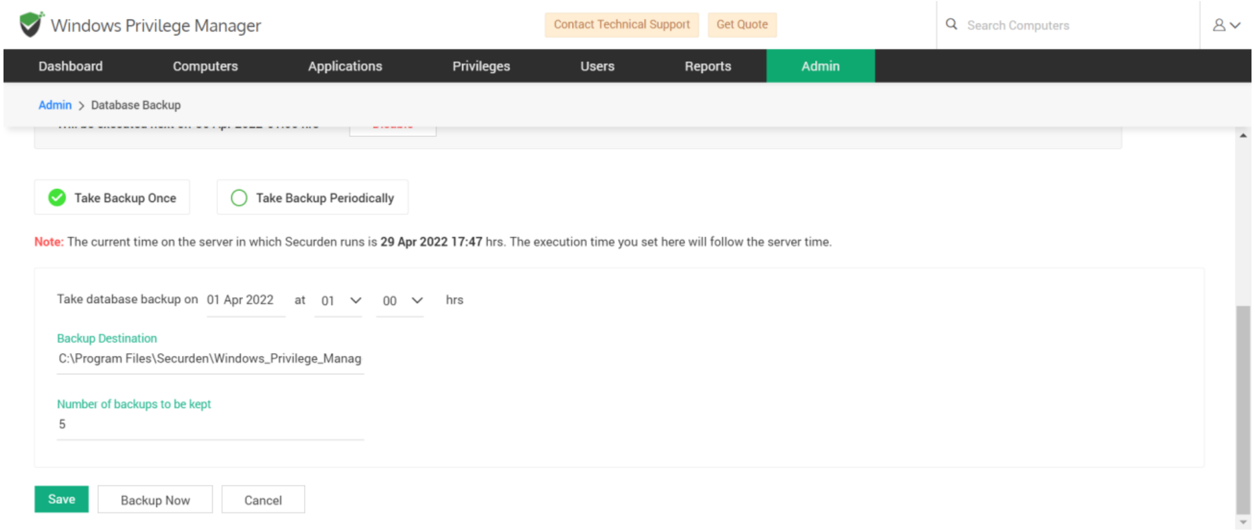
Take backup periodically starting from 29 May 2020 at 01 00 hrs

Take database backup every 1 Days

Backup Destination
C:\Program Files\Securden\Windows_Privilege_Manag

Number of backups to be kept
5

If you choose **Take Backup Once**, follow the steps below:



Note: The current time on the server in which Securden runs is **29 Apr 2022 17:47** hrs. The execution time you set here will follow the server time.

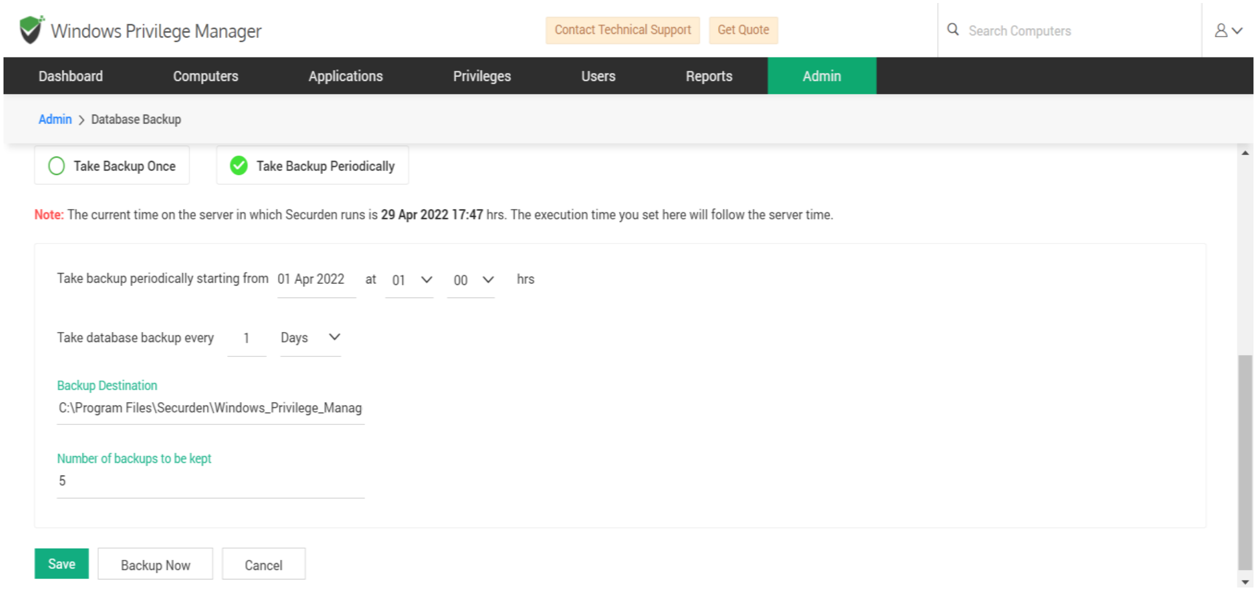
Take database backup on 01 Apr 2022 at 01 00 hrs

Backup Destination
C:\Program Files\Securden\Windows_Privilege_Manag

Number of backups to be kept
5

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 five, only the most recent five backup copies will be retained.
4. Click **Save**.

If you choose **Take Backup Periodically**, follow the steps below to create a scheduled task:



○ Take Backup Once ● Take Backup Periodically

Note: The current time on the server in which Securden runs is **29 Apr 2022 17:47** hrs. The execution time you set here will follow the server time.

Take backup periodically starting from 01 Apr 2022 at 01 00 hrs

Take database backup every 1 Days

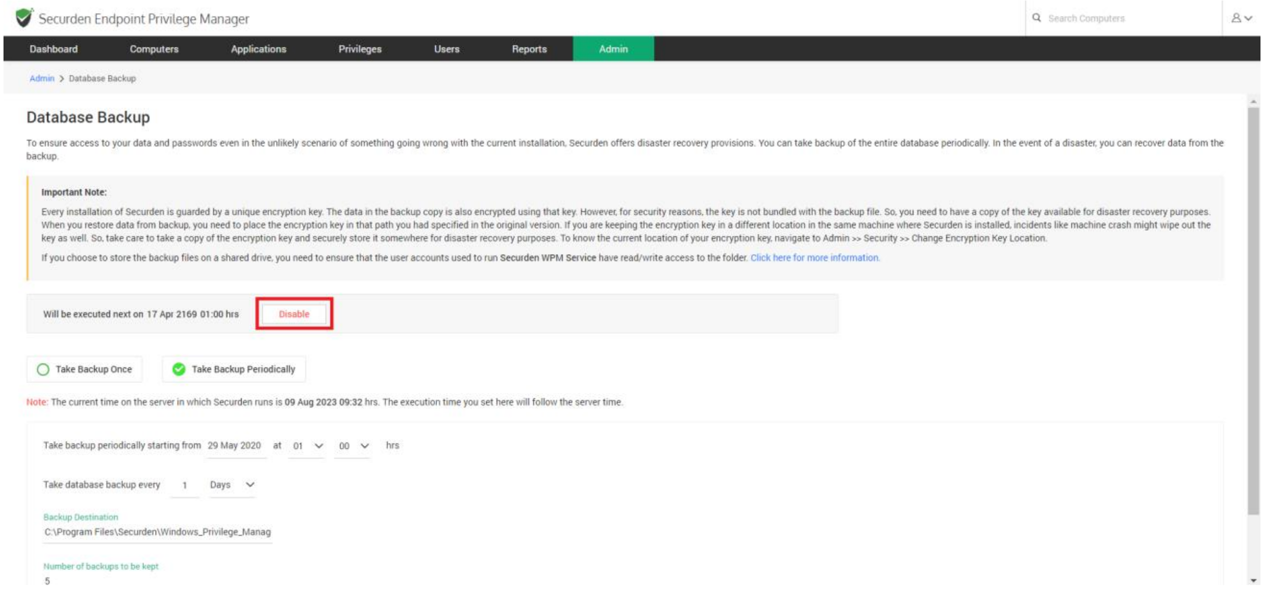
Backup Destination
C:\Program Files\Securden\Windows_Privilege_Manag

Number of backups to be kept
5

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 five, only the most recent five 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.



Database Backup

To ensure access to your data and passwords even in the unlikely scenario of something going wrong with the current installation, Securden offers disaster recovery provisions. You can take backup of the entire database periodically. In the event of a disaster, you can recover data from the backup.

Important Note:

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

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

Will be executed next on 17 Apr 2169 01:00 hrs Disable

○ Take Backup Once ✓ Take Backup Periodically

Note: The current time on the server in which Securden runs is **09 Aug 2023 09:32** hrs. The execution time you set here will follow the server time.

Take backup periodically starting from 29 May 2020 at 01 00 hrs

Take database backup every 1 Days

Backup Destination
C:\Program Files\Securden\Windows_Privilege_Manag

Number of backups to be kept
5

Important Note:

1. If you choose to store the backup files on a shared drive, you need to ensure that the user accounts used to run Securden WPM service have read/write access to the folder.
2. 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 **/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.

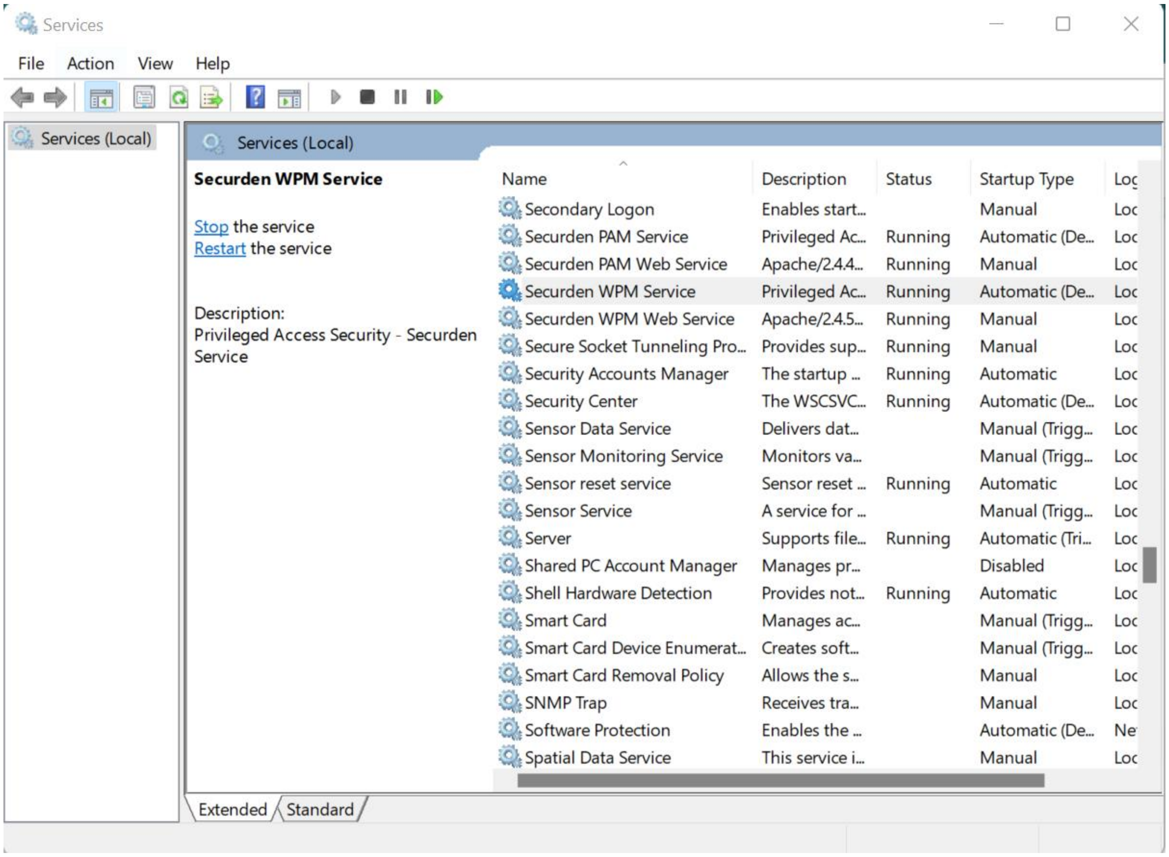
Ensure the key is available at the location specified in the current (new) installation of Securden. By default, the encryption key is located at **/conf/securden.key**.
You can also identify the current location of the encryption key by navigating to **Admin>>Security>> Change encryption key location**, 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

/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 and Navigate to Securden WPM Service.

- **Stop** the service.



Securden WPM Service

Stop the service
Restart the service

Description:
Privileged Access Security - Securden Service

Name	Description	Status	Startup Type	Loc
Secondary Logon	Enables start...		Manual	Loc
Securden PAM Service	Privileged Ac...	Running	Automatic (De...	Loc
Securden PAM Web Service	Apache/2.4.4...	Running	Manual	Loc
Securden WPM Service	Privileged Ac...	Running	Automatic (De...	Loc
Securden WPM Web Service	Apache/2.4.5...	Running	Manual	Loc
Secure Socket Tunneling Pro...	Provides sup...	Running	Manual	Loc
Security Accounts Manager	The startup ...	Running	Automatic	Loc
Security Center	The WSCSVC...	Running	Automatic (De...	Loc
Sensor Data Service	Delivers dat...		Manual (Trigg...	Loc
Sensor Monitoring Service	Monitors va...		Manual (Trigg...	Loc
Sensor reset service	Sensor reset ...	Running	Automatic	Loc
Sensor Service	A service for ...		Manual (Trigg...	Loc
Server	Supports file...	Running	Automatic (Tri...	Loc
Shared PC Account Manager	Manages pr...		Disabled	Loc
Shell Hardware Detection	Provides not...	Running	Automatic	Loc
Smart Card	Manages ac...		Manual (Trigg...	Loc
Smart Card Device Enumerat...	Creates soft...		Manual (Trigg...	Loc
Smart Card Removal Policy	Allows the s...		Manual	Loc
SNMP Trap	Receives tra...		Manual	Loc
Software Protection	Enables the ...		Automatic (De...	Ne
Spatial Data Service	This service i...		Manual	Loc

- Open Command Prompt by clicking on **Run as Administrator**.
- Navigate to **/bin**.
- In the cmd window, use the following command. *RestoreDatabase.exe C:\Program Files\**(backup file location)***
- Start Securden WPM service from services.msc. (You can safely ignore the other service named Securden Web Service, which is automatically taken care of).

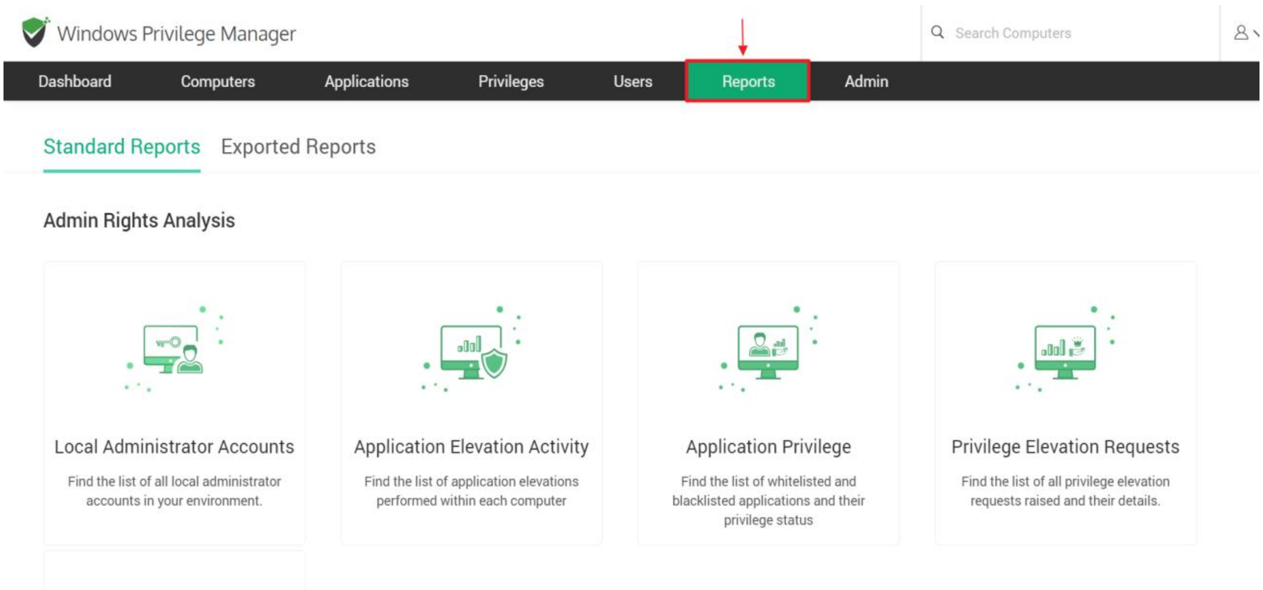
SECTION 6: Audit, Compliance & Reports

Securden Windows Privilege Manager lets you generate detailed reports of all privileged activity across your organization.   This allows you to get clear visibility to always stay in control of your IT security as well as fulfilling compliance requirements.

Who can view reports?

Reports generated in WPM, are visible to the default roles of **Administrator** and **Auditor**. Although you can configure custom user roles to to granularly view, access and download generated reports.

Reports in WPM are accessible from the **Reports** Tab, shown in the screenshot below.



Admin Rights Analysis

Local Administrator Accounts
Find the list of all local administrator accounts in your environment.

Application Elevation Activity
Find the list of application elevations performed within each computer

Application Privilege
Find the list of whitelisted and blacklisted applications and their privilege status

Privilege Elevation Requests
Find the list of all privilege elevation requests raised and their details.

Standard Reports: These are a set of reports built to give you a complete visibility of all the privileged activities happening in an organization. You may find reports that provide detailed insights about the list of elevated applications, inventory of local admin accounts, list of privileged elevation requests raised and so on. In addition to this, there are reports about the user activity, application privileges, inventory of processes and software included under this category.

Exported Reports:You can view the reports that were already exported in various formats. In case you need, there is also an option to download them from here.

Standard Reports

There are different reports that are classified under standard reports. They are explained in brief below.

Activity Reports

All user activity and privileged activity are captured under these reports. Activity reports also come in handy when auditors wish to track specific tasks performed by specific users. There are two reports under this category as below.

- **Privilege Management Trails:** All privilege management related activities performed in the application are captured here as audit trails.
- **User activities:** All activities performed by the users in Securden are captured here as audit trails.

Admin Rights Analysis

Admin rights reports give an insight into all application privilege requests granted and revoked, these reports also capture users who have local administrator rights and a report of all whitelisted and blacklisted applications. Admin rights analysis reports consists of five reports listed as below

- **Local Administrator Accounts:** List of all local administrators in your organization.
- **Application Elevation Activity:** List of application elevations performed within each computer.
- **Application Privilege:** Whitelisted and blacklisted applications and their approval status.
- **Privilege Elevation Requests:** List of all privilege requests raised and their status
- **Automatic Approval Policy:** List of computers configured under Automatic Approval Policies.

Processes and Software Reports

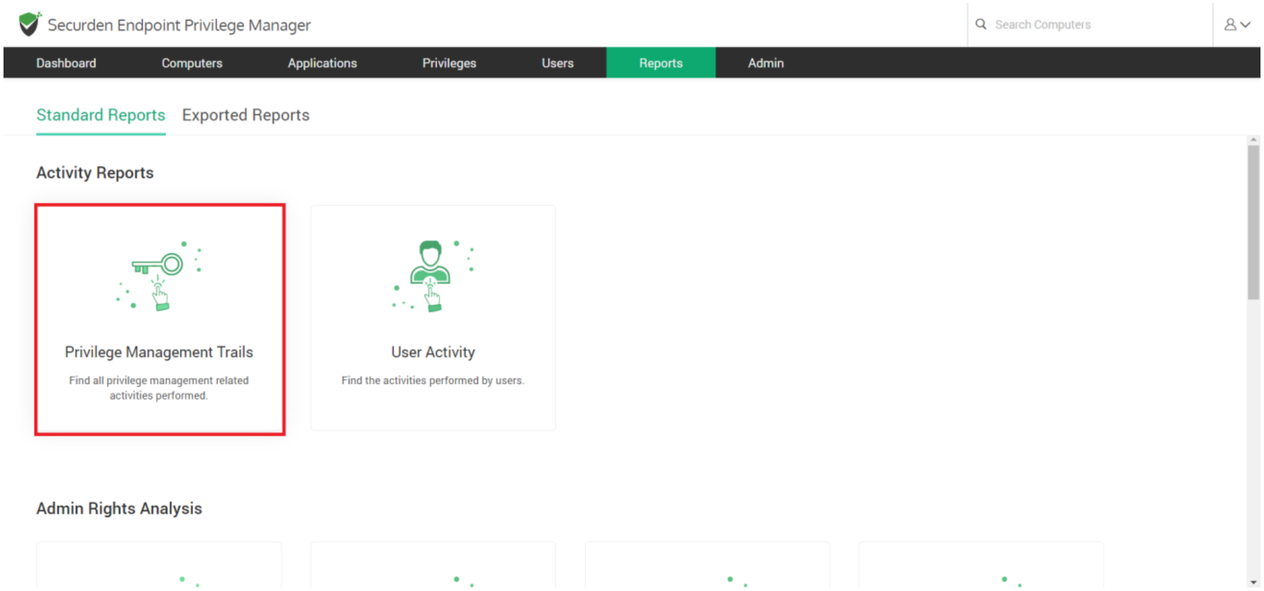
Users can view a list of all processes and software running on endpoints using these reports. They also include information on the Securden Agent installed on systems and the version they run with. **Processes and Software reports** consists of the following four parts.

- **Processes and Software Inventory**: List of processes and software installed on each computer.
- **Process Inventory**: List of processes across all computers
- **Software Inventory**: List of software installed across all computers

- **Securden Agents on Computers**: Version of Securden Agents installed on computers.

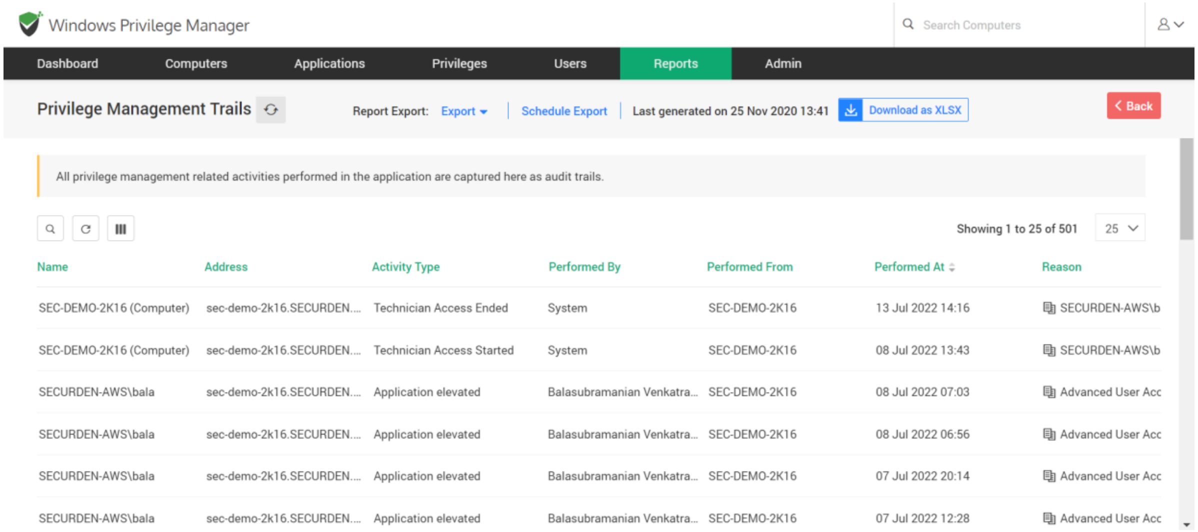
Privilege Management Trails Report

The Privileged activity report can be accessed from **Reports >> Standard Reports >> Activity Reports >> Privilege Management Trials**. All privilege management related activities performed in WPM are captured here as audit trails.


Securden Endpoint Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Standard Reports
Exported Reports
Activity Reports
Privilege Management Trails
Find all privilege management related activities performed.
User Activity
Find the activities performed by users.
Admin Rights Analysis

The privilege management report includes the fields:

- **Name** -The name of the account performing the activity
- **Address** - The device address associated with the privilege activity
- **Activity Type** - Description of the activity
- **Performed by** - The name of the user/device performing the activity
- **Performed from** - The device from which the activity was performed
- **Performed at** - The time and date at which the activity was performed
- **Reason** - A short brief of why the activity was performed (Supplied by the user performing the privileged activity)



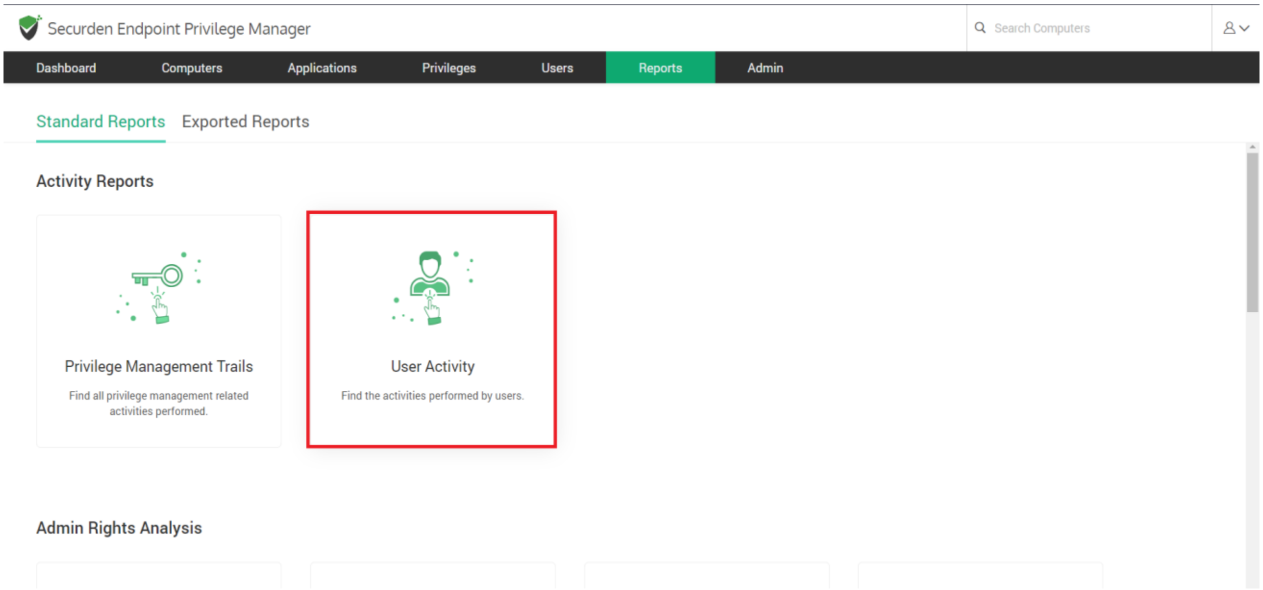
Last generated on 25 Nov 2020 13:41

All privilege management related activities performed in the application are captured here as audit trails.

Name	Address	Activity Type	Performed By	Performed From	Performed At	Reason
SEC-DEMO-2K16 (Computer)	sec-demo-2k16.SECURDEN....	Technician Access Ended	System	SEC-DEMO-2K16	13 Jul 2022 14:16	SECURDEN-AWS\b
SEC-DEMO-2K16 (Computer)	sec-demo-2k16.SECURDEN....	Technician Access Started	System	SEC-DEMO-2K16	08 Jul 2022 13:43	SECURDEN-AWS\b
SECURDEN-AWS\bala	sec-demo-2k16.SECURDEN....	Application elevated	Balasubramanian Venkatra...	SEC-DEMO-2K16	08 Jul 2022 07:03	Advanced User Acc
SECURDEN-AWS\bala	sec-demo-2k16.SECURDEN....	Application elevated	Balasubramanian Venkatra...	SEC-DEMO-2K16	08 Jul 2022 06:56	Advanced User Acc
SECURDEN-AWS\bala	sec-demo-2k16.SECURDEN....	Application elevated	Balasubramanian Venkatra...	SEC-DEMO-2K16	07 Jul 2022 20:14	Advanced User Acc
SECURDEN-AWS\bala	sec-demo-2k16.SECURDEN....	Application elevated	Balasubramanian Venkatra...	SEC-DEMO-2K16	07 Jul 2022 12:28	Advanced User Acc

User Activities Report

The user activity report can be accessed from **Reports >> Standard Reports >> Activity Reports >> User Activities**. All user activities performed in WPM are captured here as audit trails.

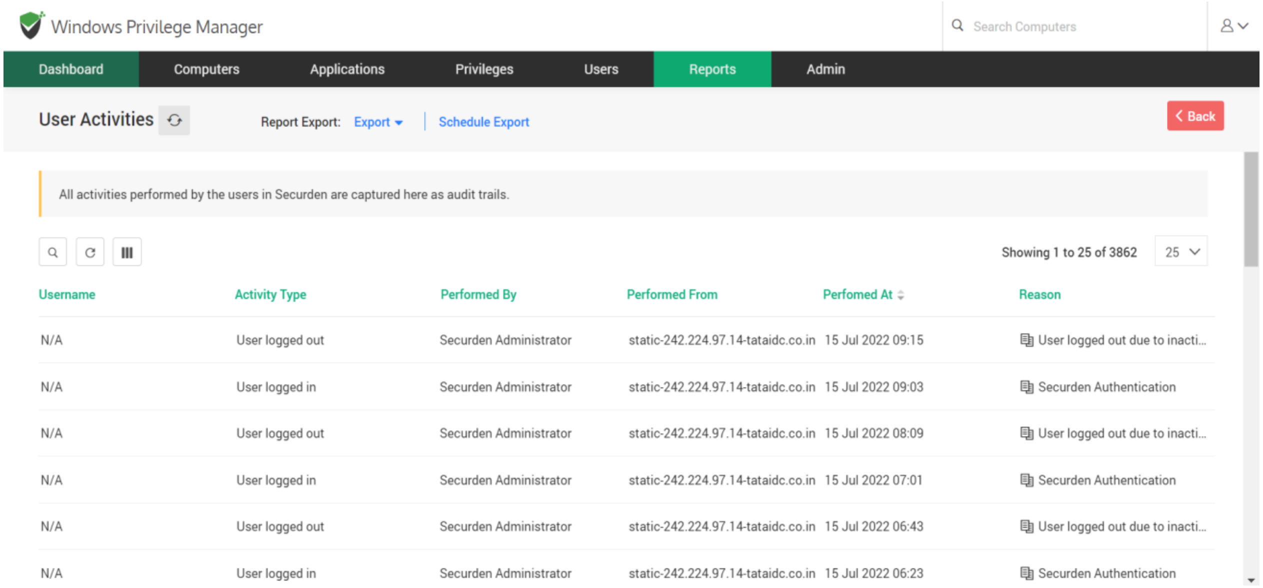


Find all privilege management related activities performed.

Find the activities performed by users.

The user activity report includes the fields:

- **Username** - The name of the user performing the activity
- **Activity Type** - Description of the activity
- **Performed by** - The name of the system user/device performing the activity
- **Performed from** - The device from which the activity was performed
- **Performed at** - The time and date at which the activity was performed
- **Reason** - A short brief of why the activity was performed (Supplied by the user/device performing the privileged activity)

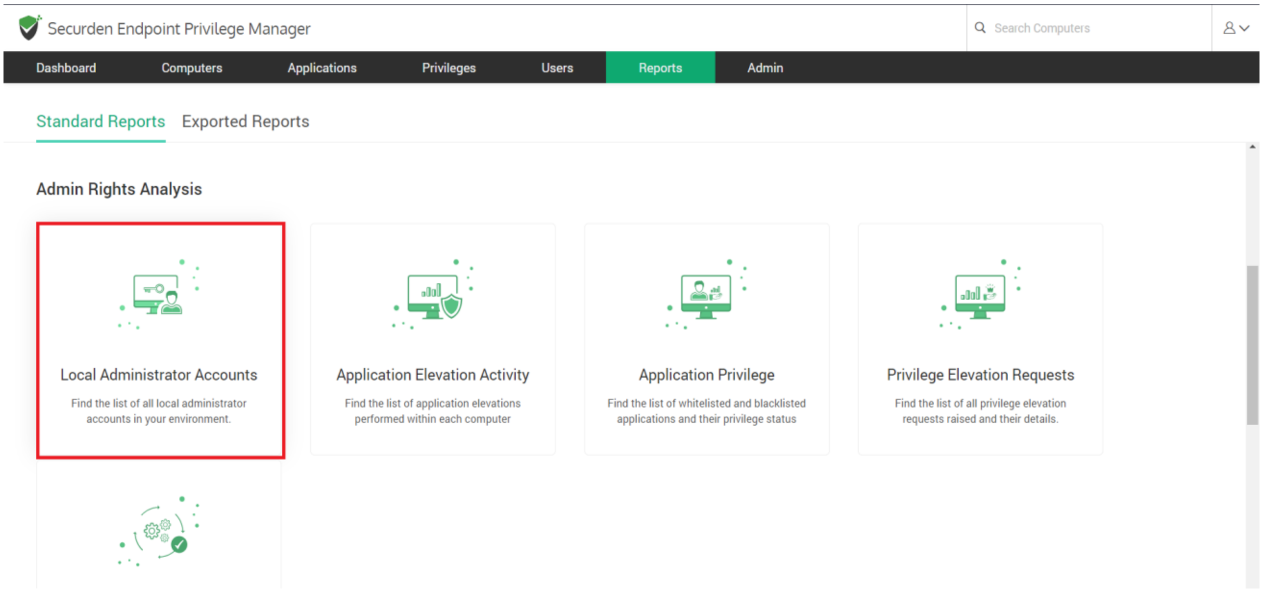


All activities performed by the users in Securden are captured here as audit trails.

Username	Activity Type	Performed By	Performed From	Perfomed At	Reason
N/A	User logged out	Securden Administrator	static-242.224.97.14-tataidc.co.in	15 Jul 2022 09:15	User logged out due to inacti...
N/A	User logged in	Securden Administrator	static-242.224.97.14-tataidc.co.in	15 Jul 2022 09:03	Securden Authentication
N/A	User logged out	Securden Administrator	static-242.224.97.14-tataidc.co.in	15 Jul 2022 08:09	User logged out due to inacti...
N/A	User logged in	Securden Administrator	static-242.224.97.14-tataidc.co.in	15 Jul 2022 07:01	Securden Authentication
N/A	User logged out	Securden Administrator	static-242.224.97.14-tataidc.co.in	15 Jul 2022 06:43	User logged out due to inacti...
N/A	User logged in	Securden Administrator	static-242.224.97.14-tataidc.co.in	15 Jul 2022 06:23	Securden Authentication

Local Administrator Accounts Report

This report can be accessed from **Reports >> Standard Reports >> Admin Rights Analysis >> Local Administrator Accounts**.



Admin Rights Analysis

Local Administrator Accounts

Find the list of all local administrator accounts in your environment.

Application Elevation Activity

Find the list of application elevations performed within each computer

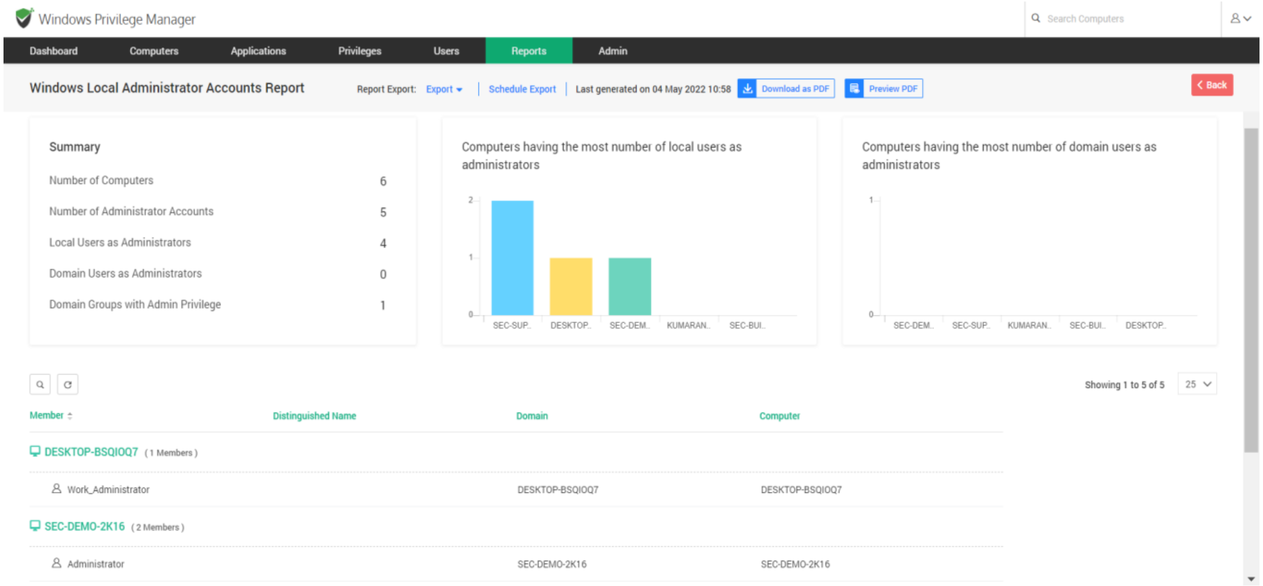
Application Privilege

Find the list of whitelisted and blacklisted applications and their privilege status

Privilege Elevation Requests

Find the list of all privilege elevation requests raised and their details.

All local administrator accounts present in your environment are listed here. You can drill down and view the list of local administrator accounts in each computer in your network. This report helps you to gain complete visibility on the presence of local administrator accounts.



Windows Local Administrator Accounts Report

Last generated on 04 May 2022 10:58

Summary

Number of Computers	6
Number of Administrator Accounts	5
Local Users as Administrators	4
Domain Users as Administrators	0
Domain Groups with Admin Privilege	1

Computers having the most number of local users as administrators

Computers having the most number of domain users as administrators

Member	Distinguished Name	Domain	Computer
DESKTOP-BSQIOQ7 (1 Members)			
Work_Administrator		DESKTOP-BSQIOQ7	DESKTOP-BSQIOQ7
SEC-DEMO-2K16 (2 Members)			
Administrator		SEC-DEMO-2K16	SEC-DEMO-2K16

The report includes a dashboard with a summary

Summary: Count of all computers, admins, users and other information compiled as a quick count list.

Computers with most local users as administrators: This bar graph shows the devices with most local administrators and helps you revoke rights from them and effectively reduce risks.

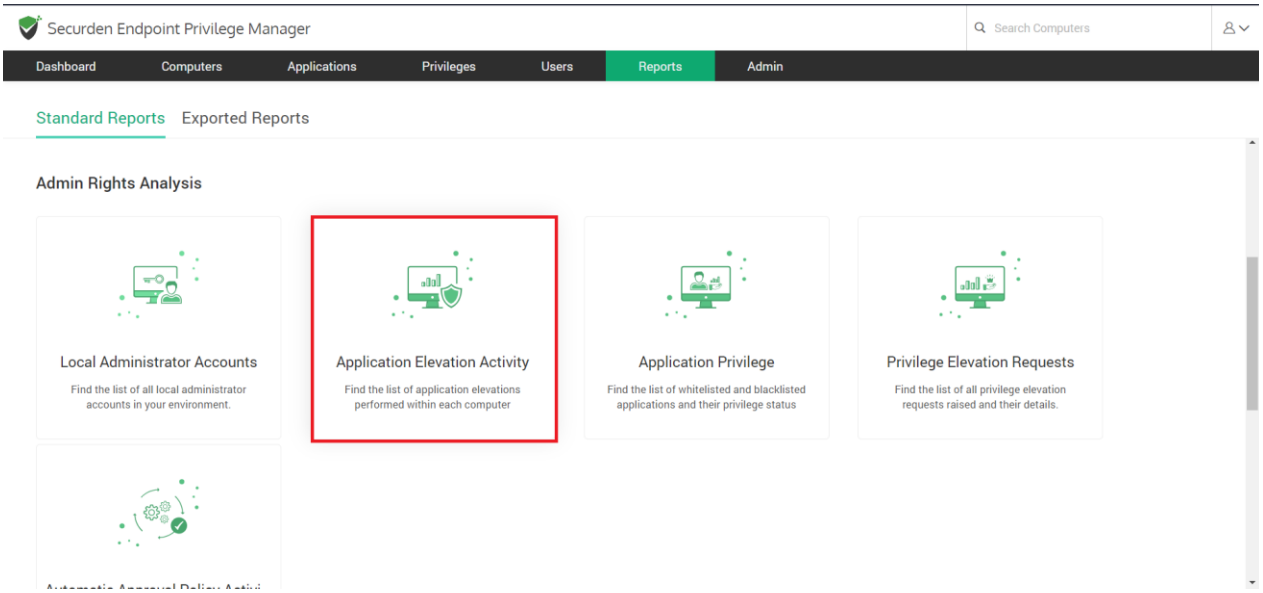
Computers with most domain users as administrators: This bar graph shows the devices with most domain administrators and helps you revoke rights from them and effectively reduce risks.

The attributes included in the report are:

- **Member**- The members on each device having local administrator rights.
- **Distinguished name**- If the member was given a distinguished name this is displayed here.
- **Domain**- The name of the system user/device performing the activity.
- **Computer -** The computer that has local administrator rights.

Application Elevation Activity Report

The user activity report can be accessed from **Reports >> Standard Reports >> Admin Rights Analysis >> Application Elevation Activity**.



Securden Endpoint Privilege Manager

Admin Rights Analysis

Local Administrator Accounts
Find the list of all local administrator accounts in your environment.

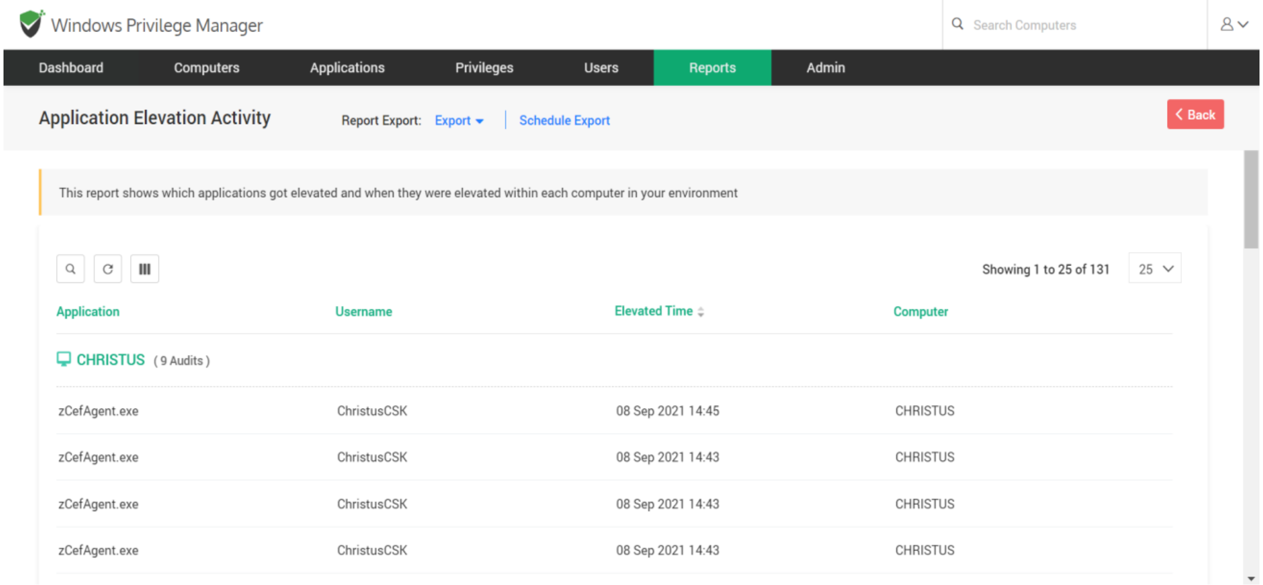
Application Elevation Activity
Find the list of application elevations performed within each computer

Application Privilege
Find the list of whitelisted and blacklisted applications and their privilege status

Privilege Elevation Requests
Find the list of all privilege elevation requests raised and their details.

Automatic Approval Policy Activi

This report shows which applications were elevated and when they were elevated within each computer in your environment.



Windows Privilege Manager

Application Elevation Activity

This report shows which applications got elevated and when they were elevated within each computer in your environment

Showing 1 to 25 of 131 25

Application	Username	Elevated Time	Computer
CHRISTUS (9 Audits)			
zCefAgent.exe	ChristusCSK	08 Sep 2021 14:45	CHRISTUS
zCefAgent.exe	ChristusCSK	08 Sep 2021 14:43	CHRISTUS
zCefAgent.exe	ChristusCSK	08 Sep 2021 14:43	CHRISTUS
zCefAgent.exe	ChristusCSK	08 Sep 2021 14:43	CHRISTUS

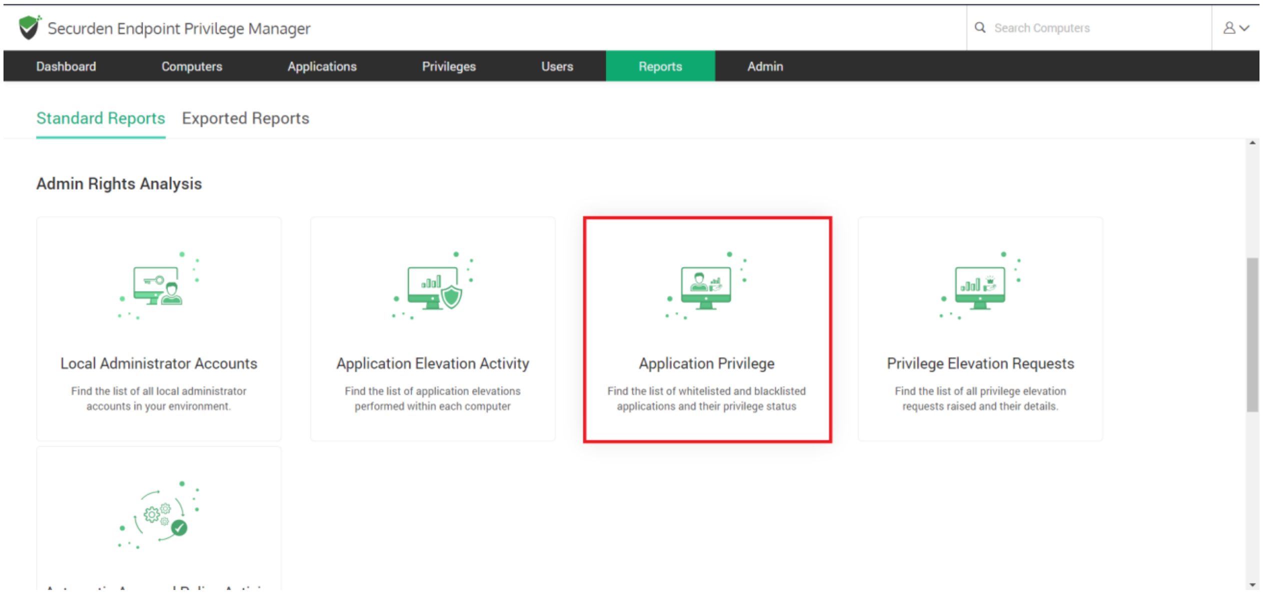
The application elevation activity report includes the fields:

- **Application** -The name of the application being elevated.
- **Username** - The name of the user elevating the application.

- **Elevated Time** - The date, and the time in minutes for which an application was elevated.
- **Computer** - The computer on which application was elevated.

Application Privilege Report

The user activity report can be accessed from **Reports >> Standard Reports >> Admin Rights Analysis >> Application Privilege**



Local Administrator Accounts

Find the list of all local administrator accounts in your environment.

Application Elevation Activity

Find the list of application elevations performed within each computer

Application Privilege

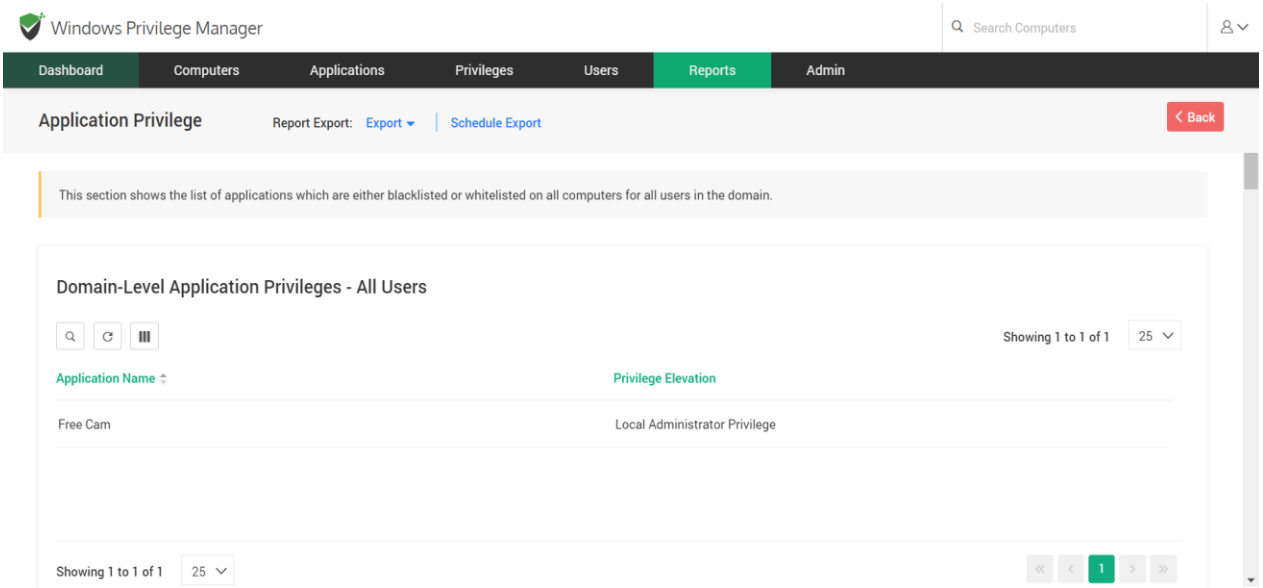
Find the list of whitelisted and blacklisted applications and their privilege status

Privilege Elevation Requests

Find the list of all privilege elevation requests raised and their details.

Domain Level Application Privileges - All users

This report shows the list of applications which are either blacklisted or whitelisted on all computers for all users in the domain.



This section shows the list of applications which are either blacklisted or whitelisted on all computers for all users in the domain.

Domain-Level Application Privileges - All Users

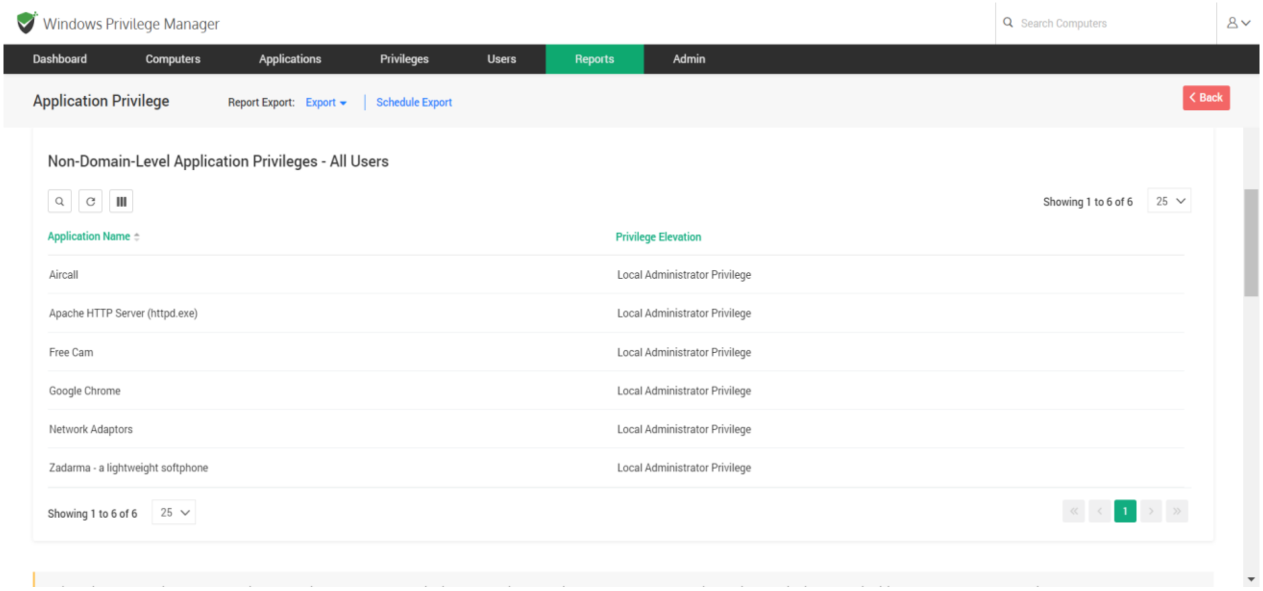
Showing 1 to 1 of 1 25

Application Name	Privilege Elevation
Free Cam	Local Administrator Privilege

Showing 1 to 1 of 1 25

Non-Domain Level Application Privileges - All users

This section shows the list of applications which are either blacklisted or whitelisted on all non-domain computers for all users.



Non-Domain-Level Application Privileges - All Users

Showing 1 to 6 of 6 25

Application Name	Privilege Elevation
Aircall	Local Administrator Privilege
Apache HTTP Server (httpd.exe)	Local Administrator Privilege
Free Cam	Local Administrator Privilege
Google Chrome	Local Administrator Privilege
Network Adaptors	Local Administrator Privilege
Zadarma - a lightweight softphone	Local Administrator Privilege

Showing 1 to 6 of 6 25

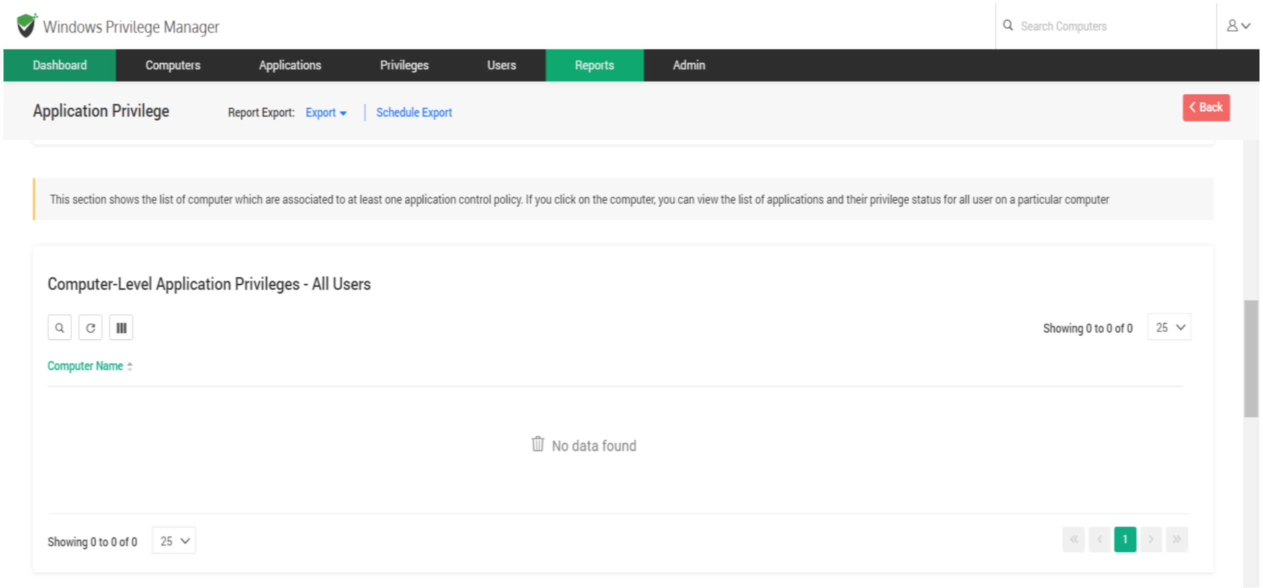
These application privilege reports include the fields:

- **Application Name** -The name of the application being elevated

- **Privilege Elevation** - The level of elevation for this application

Computer-Level Application Privileges - All users

This section shows the list of computers which are associated with at least one application control policy. If you click on the computer, you can view the list of applications and their privilege status for all user on a particular computer



This section shows the list of computer which are associated to at least one application control policy. If you click on the computer, you can view the list of applications and their privilege status for all user on a particular computer

Computer-Level Application Privileges - All Users

Showing 0 to 0 of 0 | 25

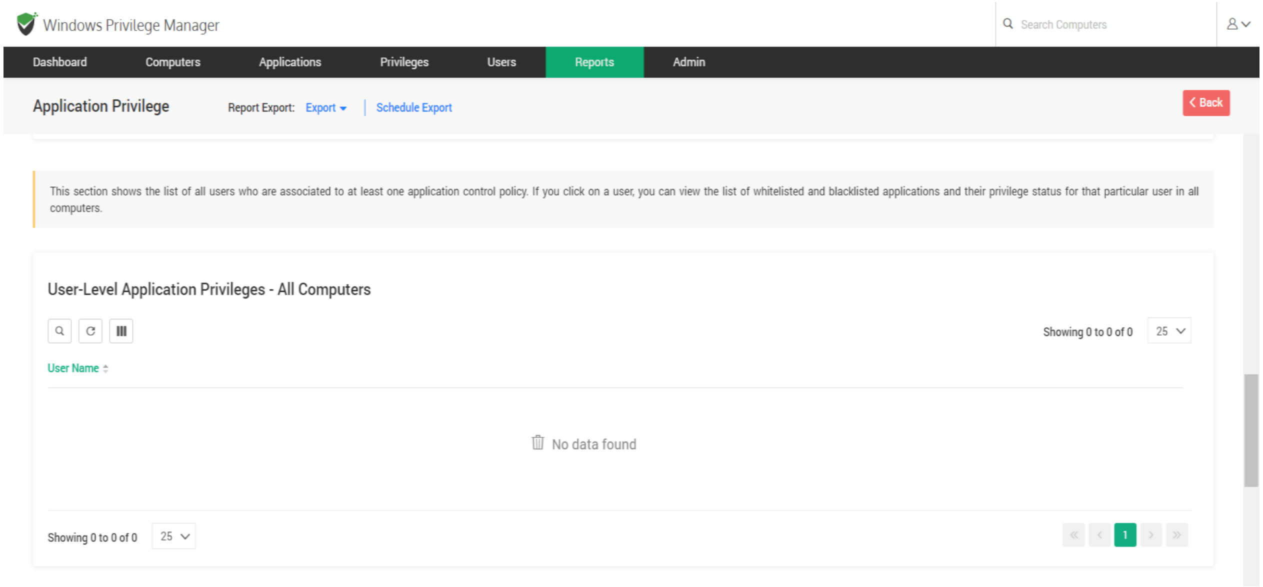
Computer Name

No data found

Showing 0 to 0 of 0 | 25

User-Level Application Privileges - All computers

This section shows the list of all users who are associated with at least one application control policy applicable on all computers. If you click on a user, you can view the list of whitelisted and blacklisted applications and their privilege status for that particular user in all computers.



This section shows the list of all users who are associated to at least one application control policy. If you click on a user, you can view the list of whitelisted and blacklisted applications and their privilege status for that particular user in all computers.

User-Level Application Privileges - All Computers

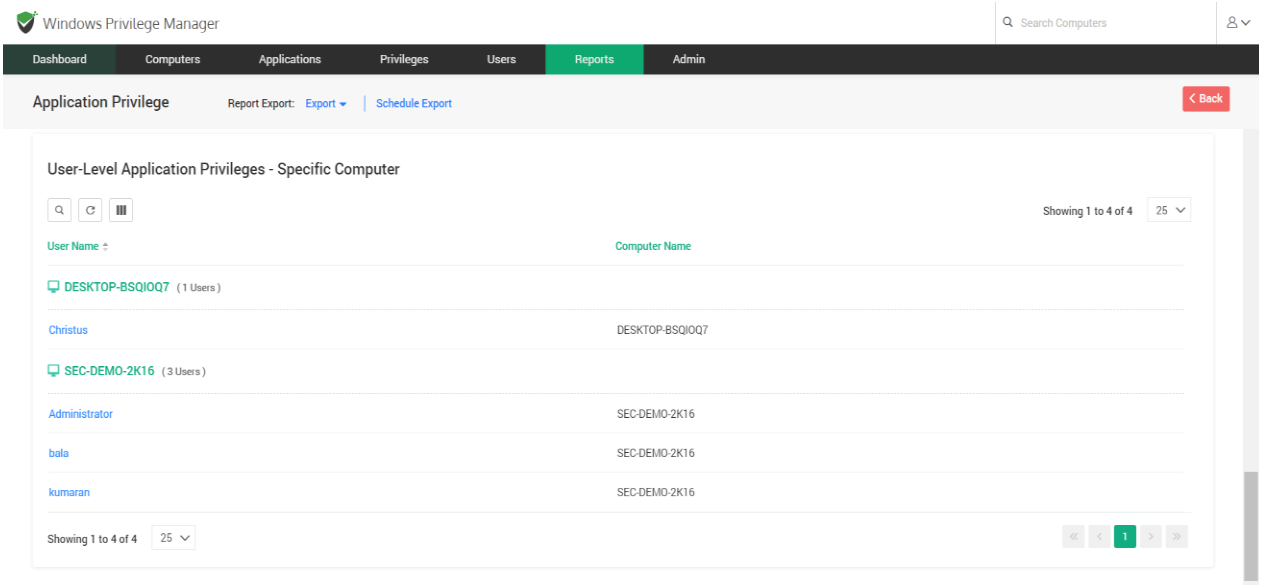
Showing 0 to 0 of 0 25

User Name
No data found

Showing 0 to 0 of 0 25

User-Level Application Privileges - Specific computer

This section shows the list of users on each computer who are associated with at least one application control policy. If you click on a user, you can view the list of whitelisted and blacklisted applications and their privilege status for that particular user on a specific computer.



User-Level Application Privileges - Specific Computer

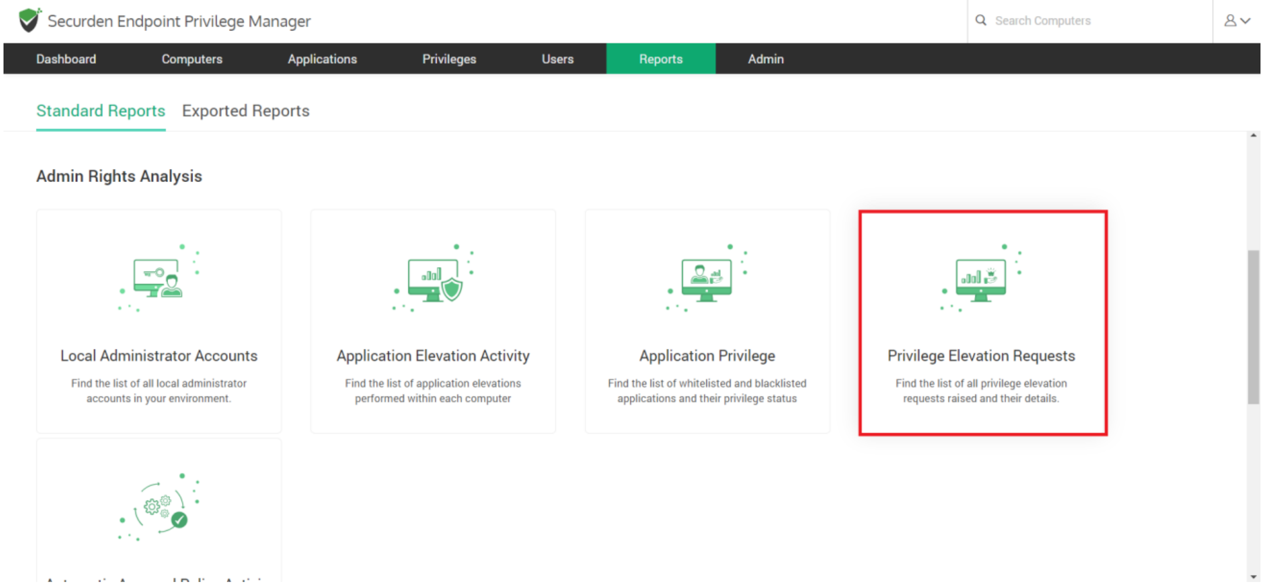
Showing 1 to 4 of 4 25

User Name	Computer Name
DESKTOP-BSQIOQ7 (1 Users)	
Christus	DESKTOP-BSQIOQ7
SEC-DEMO-2K16 (3 Users)	
Administrator	SEC-DEMO-2K16
bala	SEC-DEMO-2K16
kumaran	SEC-DEMO-2K16

Showing 1 to 4 of 4 25

Privilege Elevation Requests Report

The privilege elevation requests report can be accessed from **Reports >> Standard Reports >> Admin Rights Analysis >> Privilege Elevation Requests**



Local Administrator Accounts

Find the list of all local administrator accounts in your environment.

Application Elevation Activity

Find the list of application elevations performed within each computer

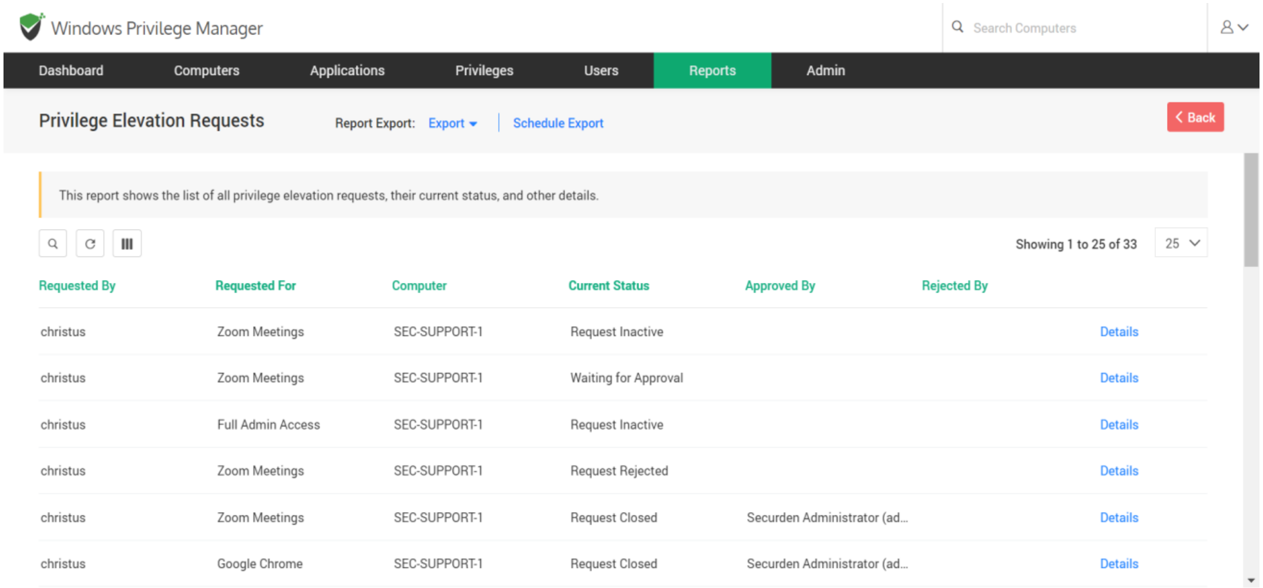
Application Privilege

Find the list of whitelisted and blacklisted applications and their privilege status

Privilege Elevation Requests

Find the list of all privilege elevation requests raised and their details.

This report shows the list of all privilege elevation requests, their current status, and other details.



This report shows the list of all privilege elevation requests, their current status, and other details.

Showing 1 to 25 of 33

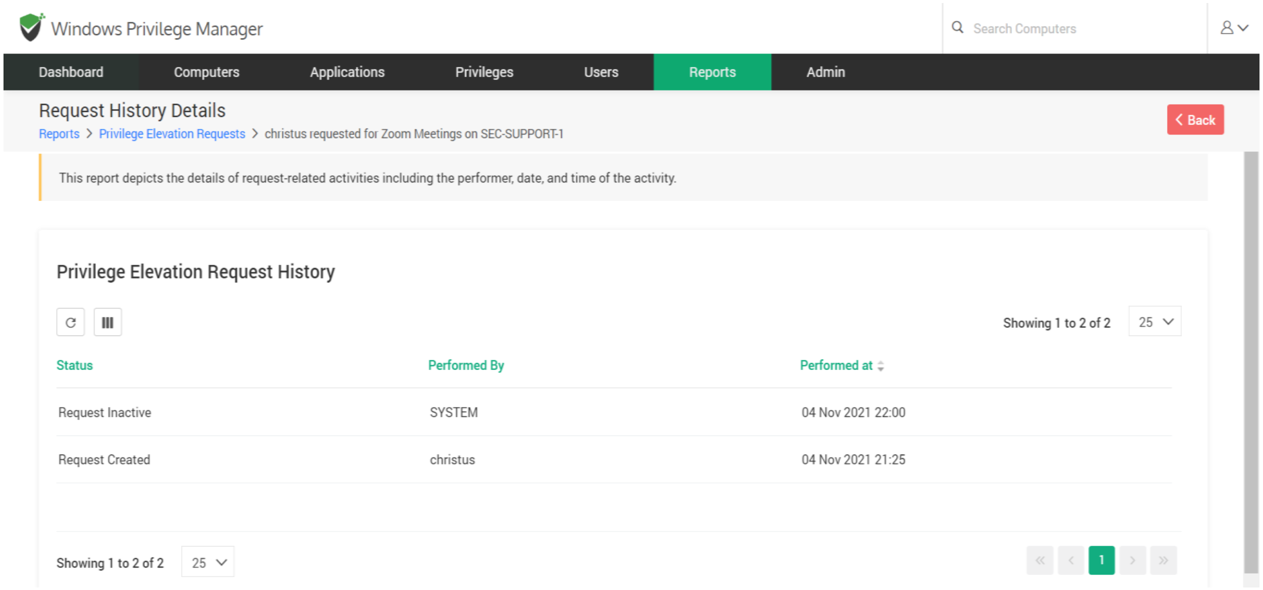
Requested By	Requested For	Computer	Current Status	Approved By	Rejected By	
christus	Zoom Meetings	SEC-SUPPORT-1	Request Inactive			Details
christus	Zoom Meetings	SEC-SUPPORT-1	Waiting for Approval			Details
christus	Full Admin Access	SEC-SUPPORT-1	Request Inactive			Details
christus	Zoom Meetings	SEC-SUPPORT-1	Request Rejected			Details
christus	Zoom Meetings	SEC-SUPPORT-1	Request Closed	Securden Administrator (ad…		Details
christus	Google Chrome	SEC-SUPPORT-1	Request Closed	Securden Administrator (ad…		Details

The privilege elevation requests report includes the fields:

- **Requested by**-The name of the user who has requested elevated privileges
- **Requested for**- The application for which elevation has been requested
- **Computer** - The computer on which the application has to be elevated
- **Current Status** - Shows if the request was approved, rejected, in use or inactive
- **Approved by -** Name of the administrator who had approved the request
- **Rejected by** - Name of the administrator who had rejected the request

Clicking on **Details** will take you to the Privilege Elevation Request History revealing the below details.

- **Status -** The status of the request (Active/Inactive etc.)
- **Performed By -** The user/device which obtained elevated privileges
- **Performed At -** The date and time at which the privilege elevation was performed


Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Back
Reports > Privilege Elevation Requests > christus requested for Zoom Meetings on SEC-SUPPORT-1
25
« ‹ 1 › »

Request History Details

This report depicts the details of request-related activities including the performer, date, and time of the activity.

Privilege Elevation Request History

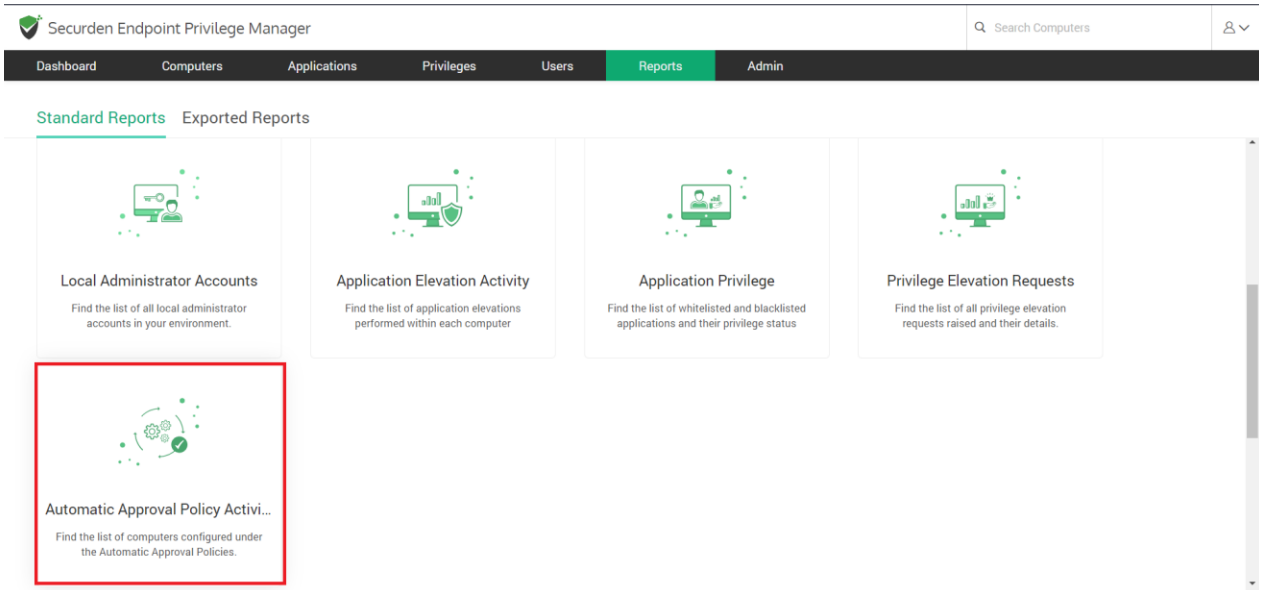
Showing 1 to 2 of 2

Status	Performed By	Performed at
Request Inactive	SYSTEM	04 Nov 2021 22:00
Request Created	christus	04 Nov 2021 21:25

Showing 1 to 2 of 2

Automatic Approval Policy Report

The admin rights analysis report can be accessed from **Reports >> Standard Reports >> Admin Rights Analysis >> Automatic Approval Policy Activities.**



Local Administrator Accounts

Find the list of all local administrator accounts in your environment.

Application Elevation Activity

Find the list of application elevations performed within each computer

Application Privilege

Find the list of whitelisted and blacklisted applications and their privilege status

Privilege Elevation Requests

Find the list of all privilege elevation requests raised and their details.

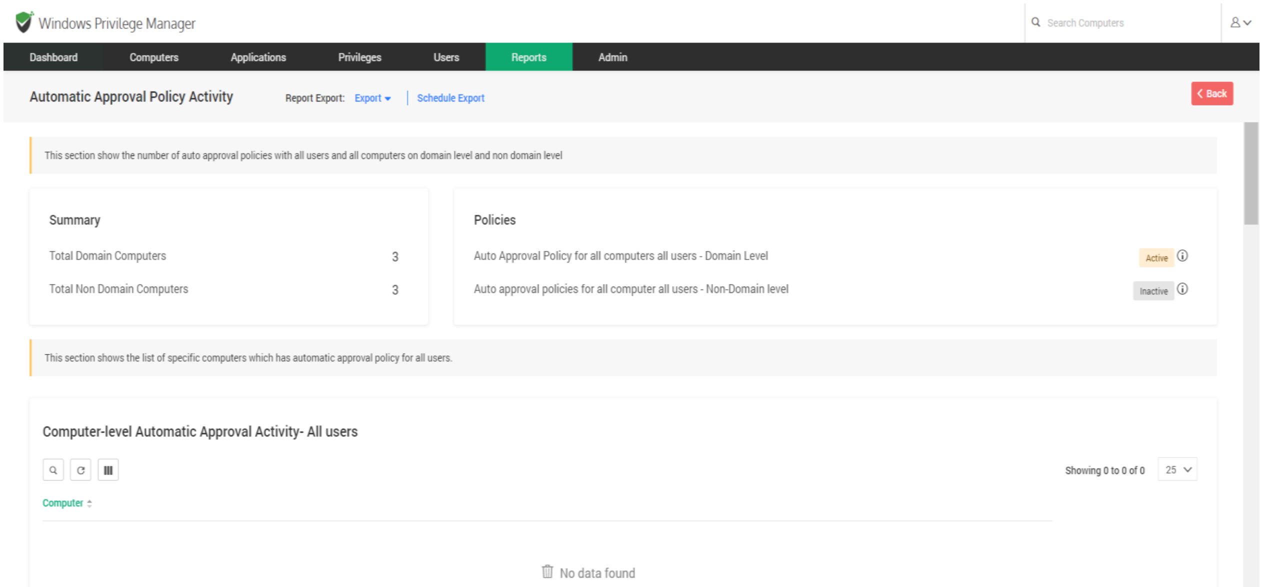
Automatic Approval Policy Activi...

Find the list of computers configured under the Automatic Approval Policies.

This report contains two sections, the first one shows a dashboard of automated approval policies created for all users and computers.

Computer Level Automatic Approval Activity - All Users

This section shows the list of specific computers which have automatic approval policy activity for all users.



Automatic Approval Policy Activity

This section show the number of auto approval policies with all users and all computers on domain level and non domain level

Summary

Total Domain Computers	3
Total Non Domain Computers	3

Policies

Auto Approval Policy for all computers all users - Domain Level	Active
Auto approval policies for all computer all users - Non-Domain level	Inactive

This section shows the list of specific computers which has automatic approval policy for all users.

Computer-level Automatic Approval Activity- All users

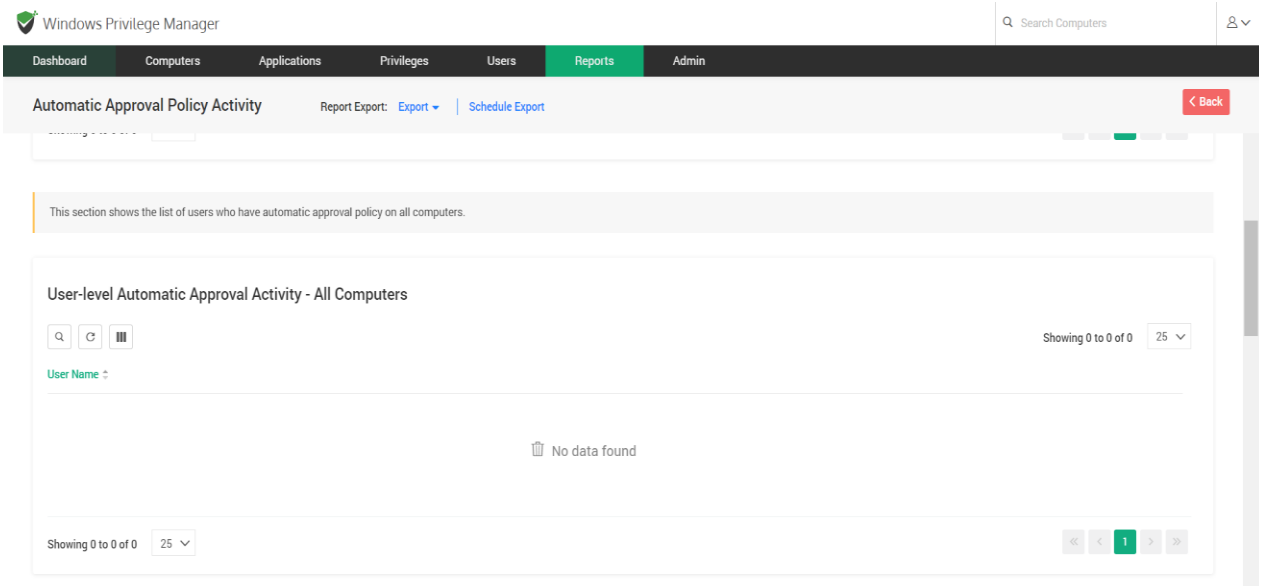
Showing 0 to 0 of 0 25

Computer

No data found

User Level Automatic Approval Activity - All Computers

This section shows the list of users who have automatic approval policy on all computers.



This section shows the list of users who have automatic approval policy on all computers.

User-level Automatic Approval Activity - All Computers

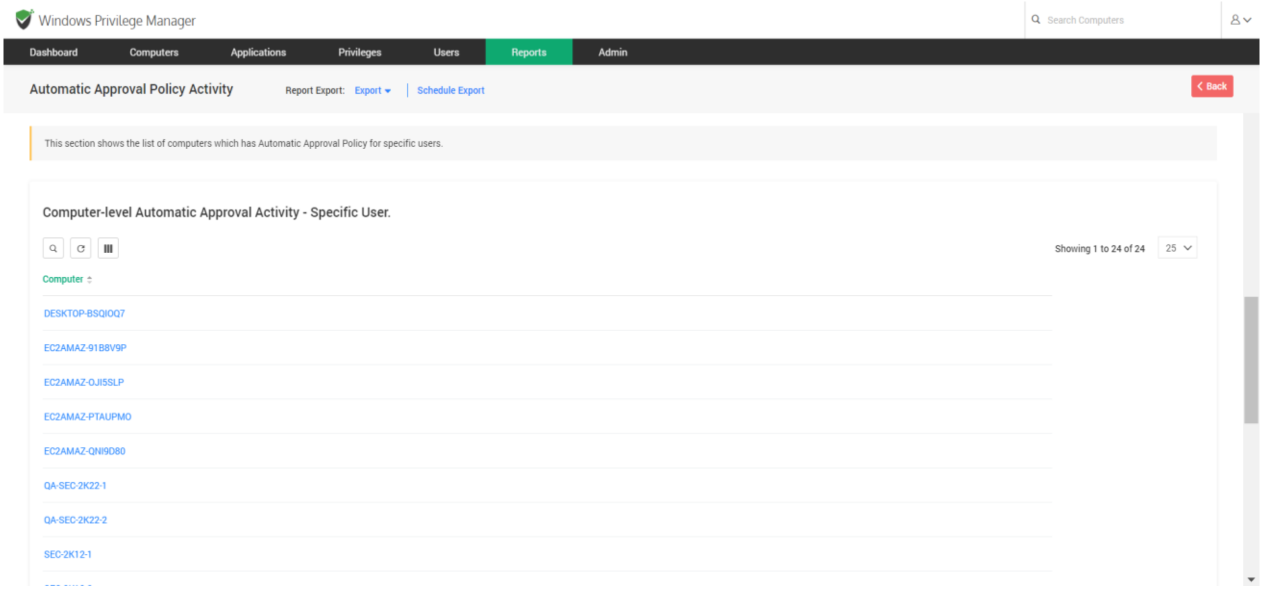
Showing 0 to 0 of 0 25

User Name
No data found

Showing 0 to 0 of 0 25

Computer-Level Automatic Approval Activity - Specific User

This section shows the list of computers which have Automatic Approval activity for specific users.



This section shows the list of computers which has Automatic Approval Policy for specific users.

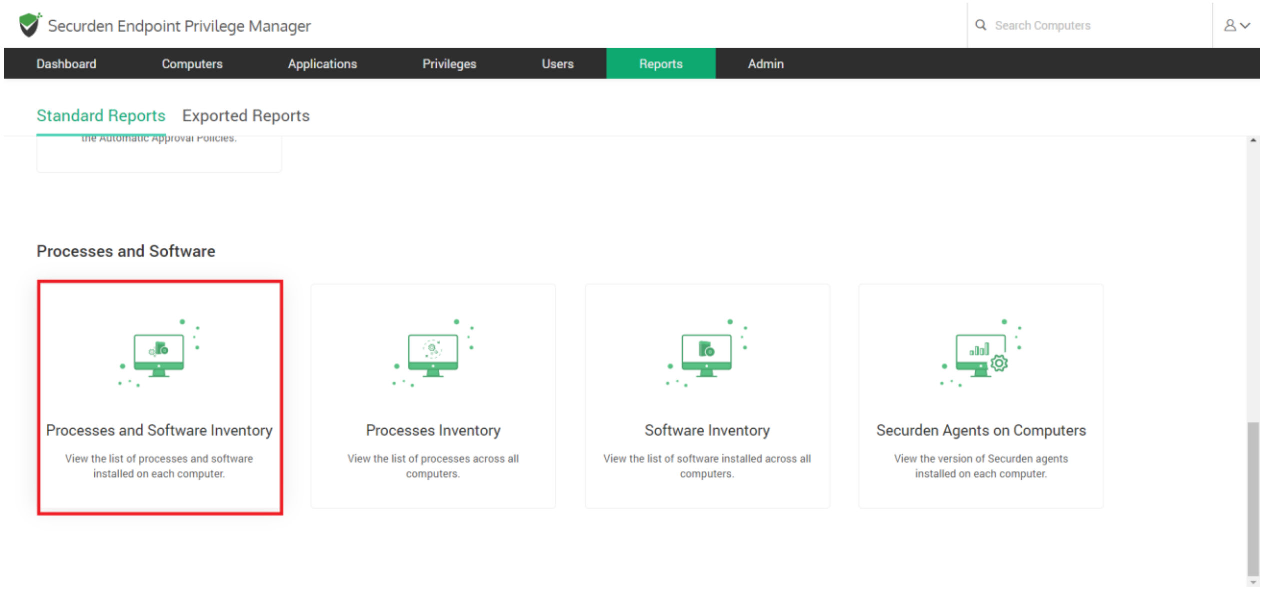
Computer-level Automatic Approval Activity - Specific User.

Showing 1 to 24 of 24 25

Computer
DESKTOP-BSQIOQ7
EC2AMAZ-91B8V9P
EC2AMAZ-OJI5SLP
EC2AMAZ-PTAUPMO
EC2AMAZ-QNI9D80
QA-SEC-2K22-1
QA-SEC-2K22-2
SEC-2K12-1

Processes and Software Inventory Report

The processes and software report can be accessed from **Reports >> Standard Reports >> Processes and Software >> Processes and Software Inventory**



Processes and Software Inventory
View the list of processes and software installed on each computer.

Processes Inventory
View the list of processes across all computers.

Software Inventory
View the list of software installed across all computers.

Securden Agents on Computers
View the version of Securden agents installed on each computer.

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.

This report includes the following fields:

Processes Table

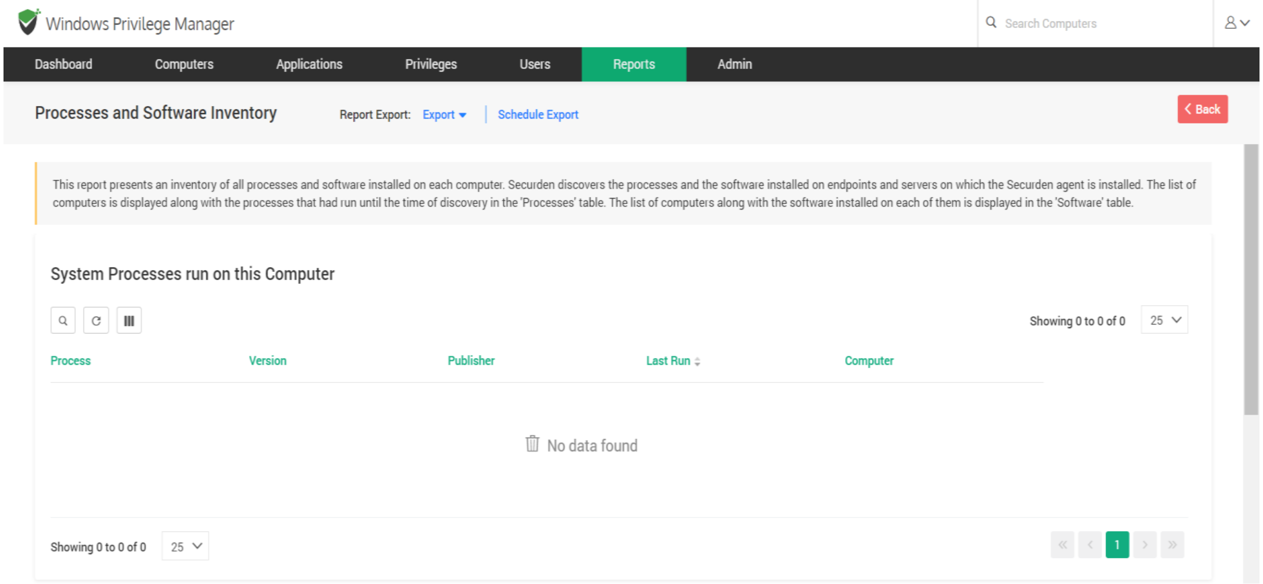
Process - Name of the process run on the computer.

Version - Version of the Securden Agent installed on that computer.

Publisher - Verified publisher of the process.

Last Run - Time and date the process was run last.

Computer - The computer on which the process was run.



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 0 to 0 of 0 25

Process	Version	Publisher	Last Run	Computer

No data found

Showing 0 to 0 of 0 25

Software table

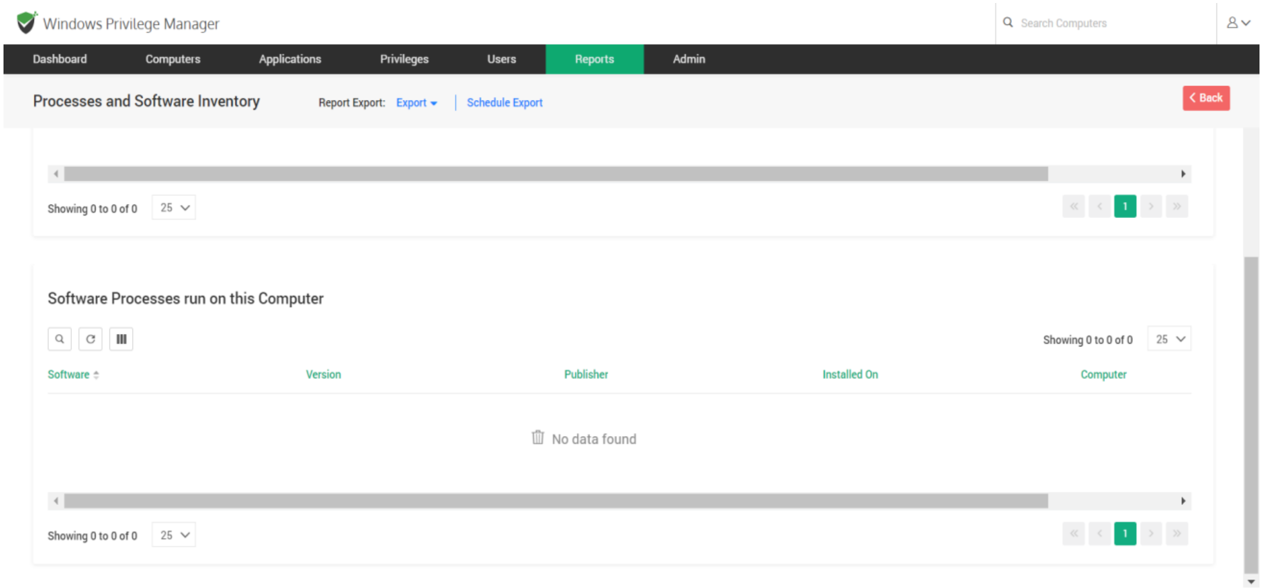
Software - Name of the software installed on the computer.

Version - Version of the Securden Agent installed on that computer.

Publisher - Verified publisher of the software.

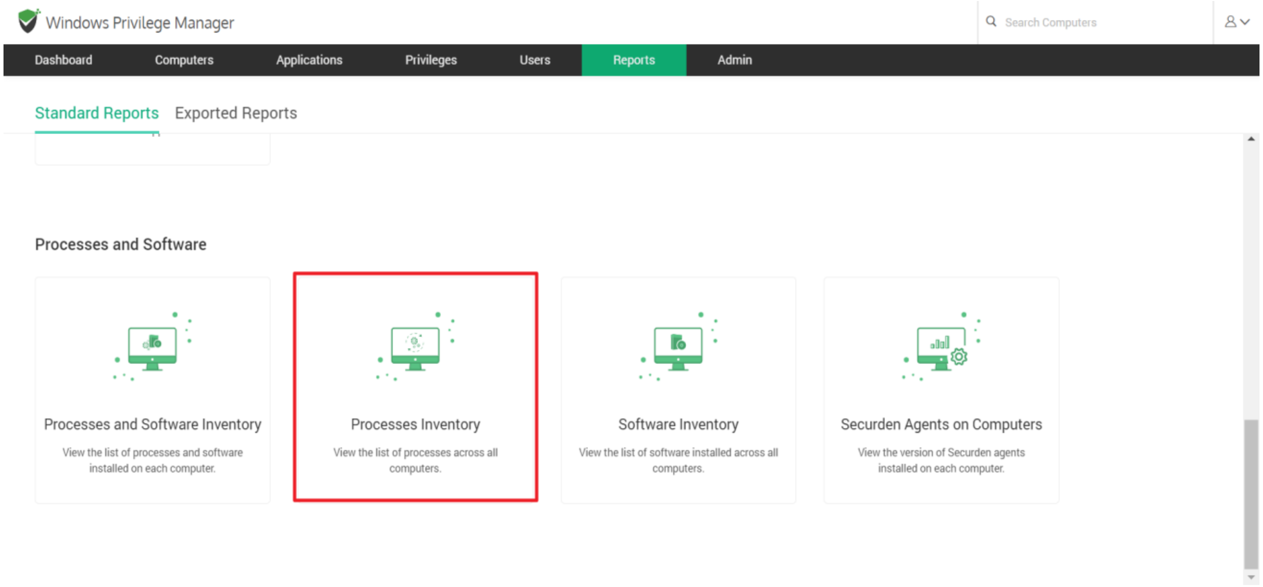
Installed on - Time and date the software was installed.

Computer - The computer on which the software was installed.



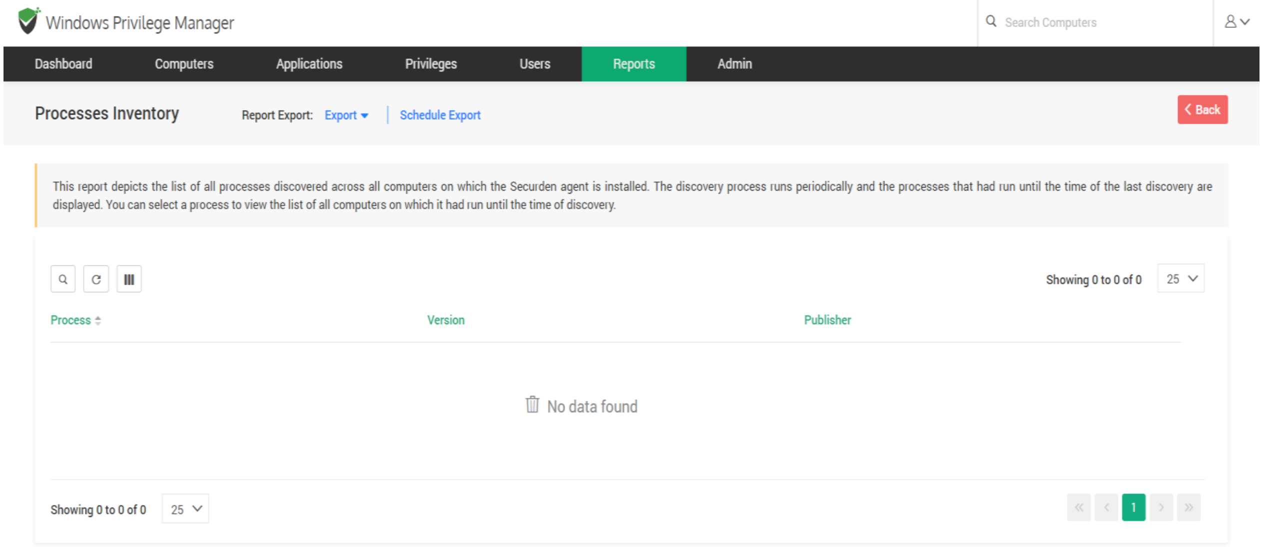
Processes Inventory Report

The processes report can be accessed from **Reports >> Standard Reports >> Processes and Software >> Processes Inventory**.


Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Standard Reports
Exported Reports
Processes and Software
Processes and Software Inventory
View the list of processes and software installed on each computer.
Processes Inventory
View the list of processes across all computers.
Software Inventory
View the list of software installed across all computers.
Securden Agents on Computers
View the version of Securden agents installed on each computer.

This report presents an inventory of all processes running on each computer. Securden discovers the processes 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.



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.

Process	Version	Publisher

No data found

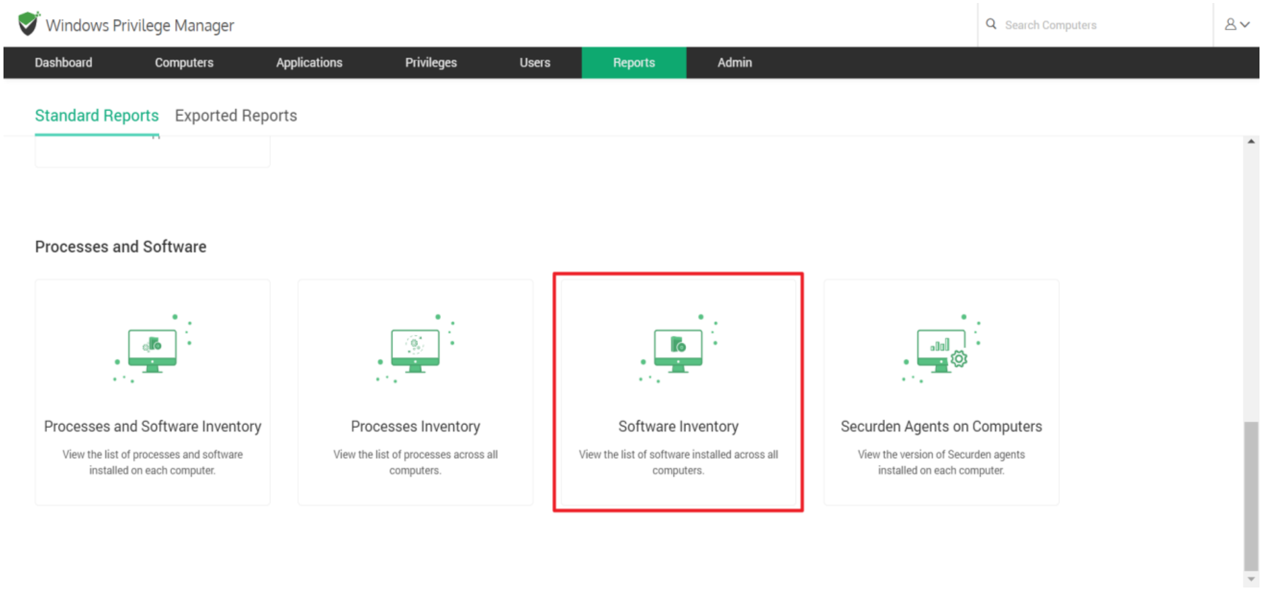
Showing 0 to 0 of 0 25

This report includes the following fields:

Process - Name of the process run on the computer.
Version - Version of the Securden Agent installed on that computer.
Publisher - Verified publisher of the process.

Software Inventory Report

The software report can be accessed from **Reports >> Standard Reports >> Processes and Software >> Software Inventory**.



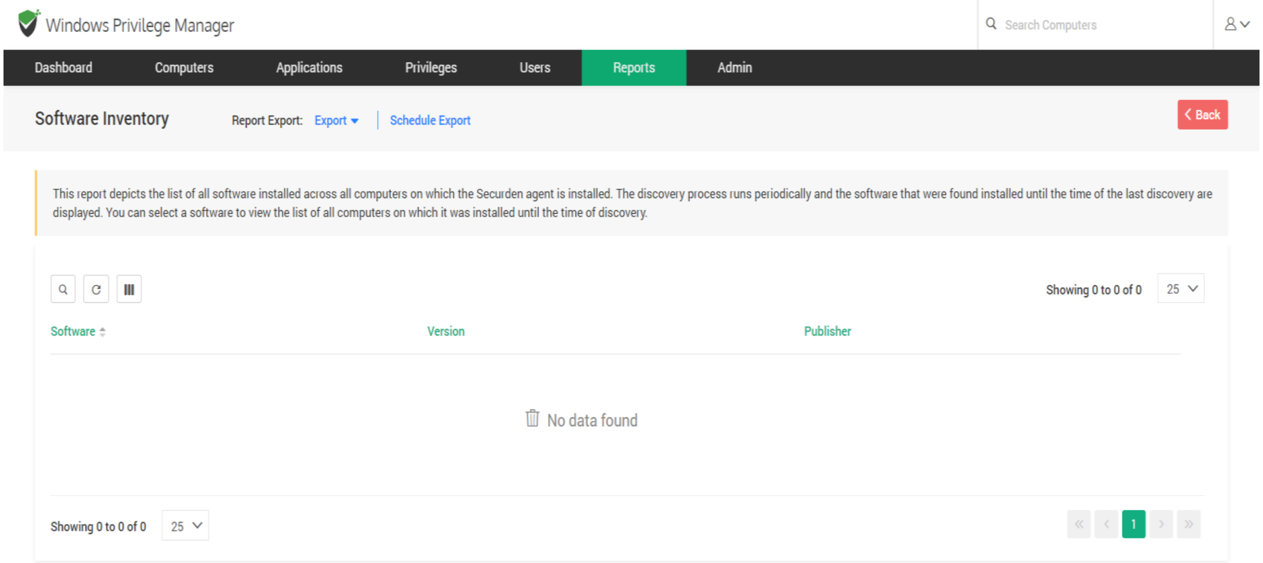
View the list of processes and software installed on each computer.

View the list of processes across all computers.

View the list of software installed across all computers.

View the version of Securden agents installed on each computer.

This report presents an inventory of all software installed on each computer. Securden discovers the software installed on endpoints and servers on which the Securden agent is installed. The list of computers along with the software installed on each of them is displayed in the table.



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.

This report includes the following fields:

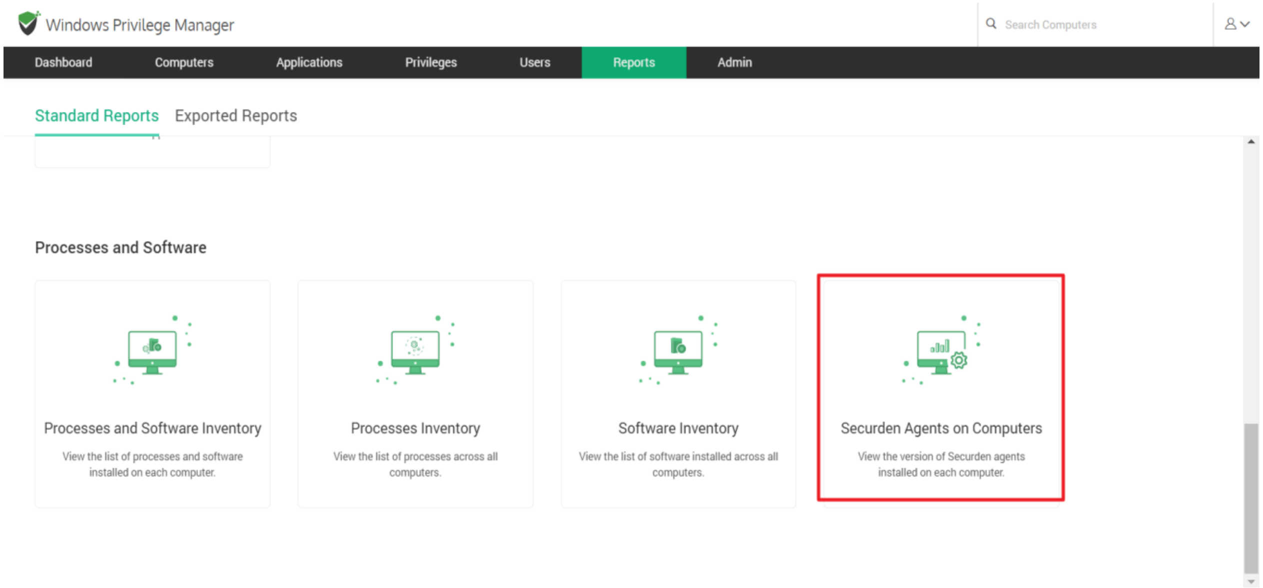
Software- Name of the software run on the computer.

Version - Version of the Securden Agent installed on that computer.

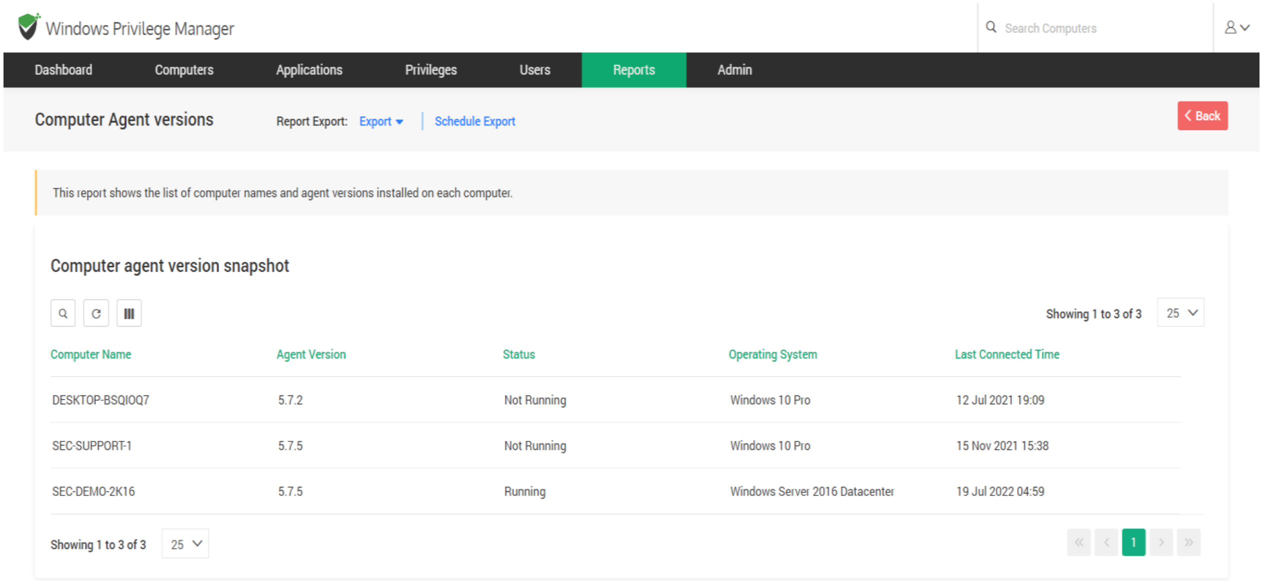
Publisher - Verified publisher of the process.

Securden Agent Report

The processes and software report can be accessed from **Reports >> Standard Reports >> Processes and Software >> Securden Agents on Computers**.


Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Standard Reports
Exported Reports
Processes and Software
Processes and Software Inventory
View the list of processes and software installed on each computer.
Processes Inventory
View the list of processes across all computers.
Software Inventory
View the list of software installed across all computers.
Securden Agents on Computers
View the version of Securden agents installed on each computer.

This report shows the list of computer names and agent versions installed on each computer.



Computer Agent versions

This report shows the list of computer names and agent versions installed on each computer.

Computer agent version snapshot

Computer Name	Agent Version	Status	Operating System	Last Connected Time
DESKTOP-BSQIOQ7	5.7.2	Not Running	Windows 10 Pro	12 Jul 2021 19:09
SEC-SUPPORT-1	5.7.5	Not Running	Windows 10 Pro	15 Nov 2021 15:38
SEC-DEMO-2K16	5.7.5	Running	Windows Server 2016 Datacenter	19 Jul 2022 04:59

This report table has the following fields:

Computer - The computer on which Securden Agent has been installed.

Agent Version - The version of the Agent installed on this computer.

Status - The running status of the Agent installed.

Operating System - The operating system of the computer.

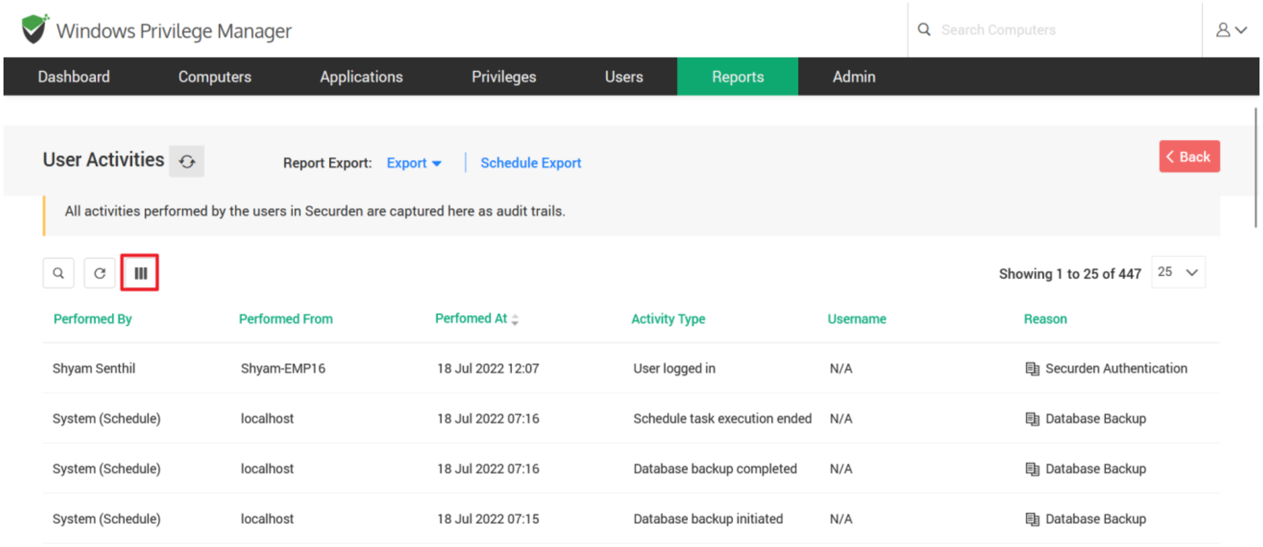
Last Connected Time - The date and time the agent was last connected.

Exporting and Scheduling Exports for Reports

All reports generated in WPM can be exported from the interface in a similar manner. First navigate to the report you would like to export. On the relevant GUI you have a few options to customize your report.

Column chooser

The column chooser lets you determine which fields/attributes of the report will be displayed in the interface. Click on the icon as shown below.



User Activities

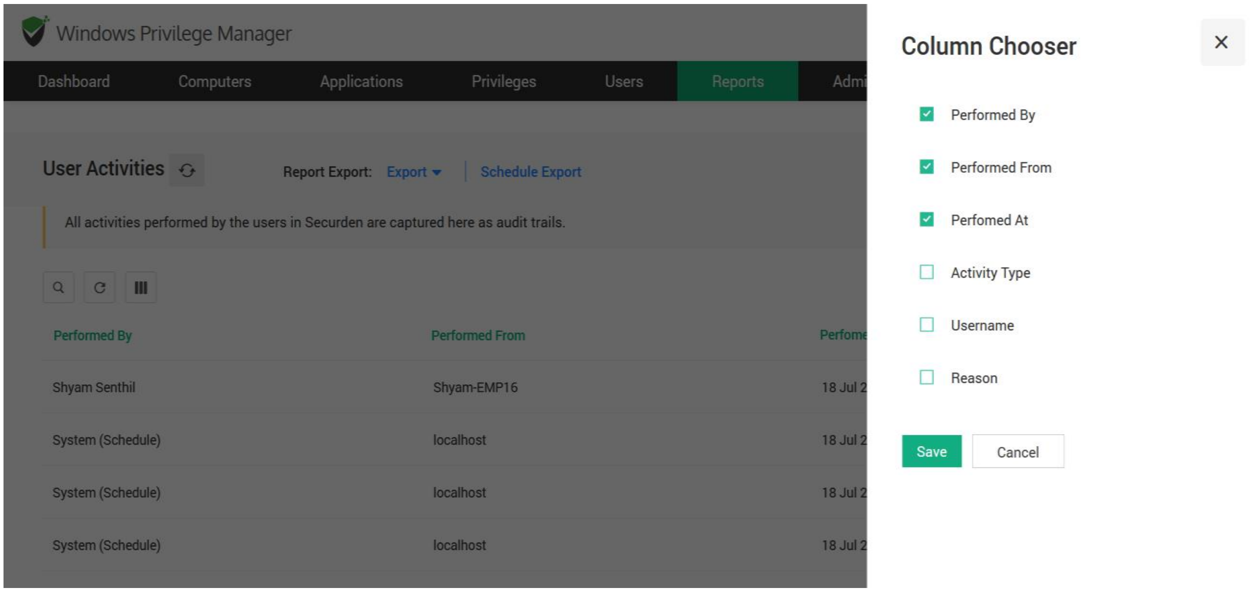
Report Export: Export ▾ | Schedule Export

All activities performed by the users in Securden are captured here as audit trails.

Showing 1 to 25 of 447 25

Performed By	Performed From	Perfomed At	Activity Type	Username	Reason
Shyam Senthil	Shyam-EMP16	18 Jul 2022 12:07	User logged in	N/A	Securden Authentication
System (Schedule)	localhost	18 Jul 2022 07:16	Schedule task execution ended	N/A	Database Backup
System (Schedule)	localhost	18 Jul 2022 07:16	Database backup completed	N/A	Database Backup
System (Schedule)	localhost	18 Jul 2022 07:15	Database backup initiated	N/A	Database Backup

Select the attribute that you want to display and click **Save**.



Column Chooser

☑ Performed By

☑ Performed From

☑ Perfomed At

☐ Activity Type

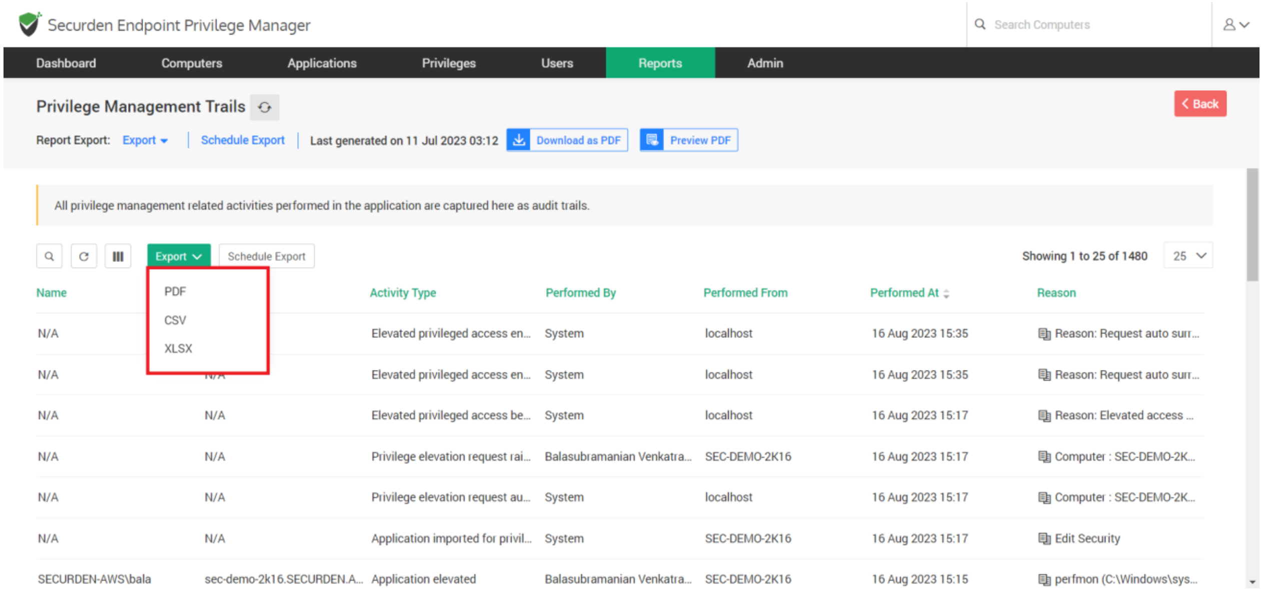
☐ Username

☐ Reason

Save Cancel

Export reports

Reports in WPM can be exported as a PDF, CSV or an XLSX file. Click on **Export** as highlighted below and select the format in which you would like to export the report.



Privilege Management Trails

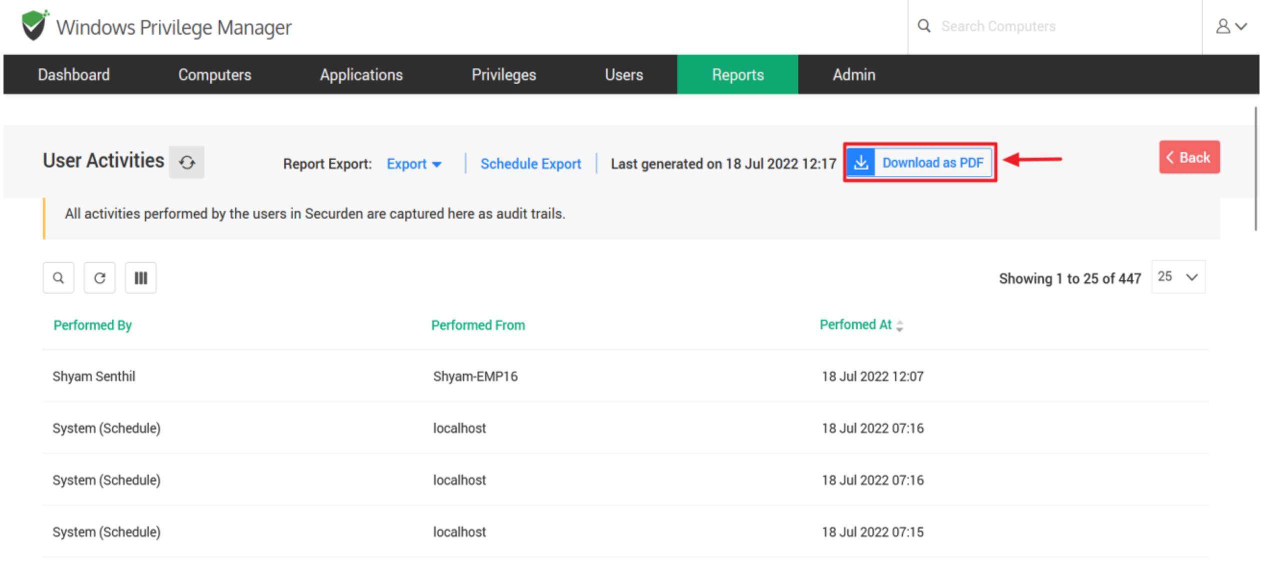
Report Export: Export | Schedule Export | Last generated on 11 Jul 2023 03:12

All privilege management related activities performed in the application are captured here as audit trails.

Showing 1 to 25 of 1480

Name		Activity Type	Performed By	Performed From	Performed At	Reason
N/A		Elevated privileged access en...	System	localhost	16 Aug 2023 15:35	Reason: Request auto surr...
N/A	N/A	Elevated privileged access en...	System	localhost	16 Aug 2023 15:35	Reason: Request auto surr...
N/A	N/A	Elevated privileged access be...	System	localhost	16 Aug 2023 15:17	Reason: Elevated access ...
N/A	N/A	Privilege elevation request rai...	Balasubramanian Venkatra...	SEC-DEMO-2K16	16 Aug 2023 15:17	Computer : SEC-DEMO-2K...
N/A	N/A	Privilege elevation request au...	System	localhost	16 Aug 2023 15:17	Computer : SEC-DEMO-2K...
N/A	N/A	Application imported for privil...	System	SEC-DEMO-2K16	16 Aug 2023 15:17	Edit Security
SECURDEN-AWS\bala	sec-demo-2k16.SECURDEN.A...	Application elevated	Balasubramanian Venkatra...	SEC-DEMO-2K16	16 Aug 2023 15:15	perfmon (C:\Windows\sys...

On clicking the format, a file with the specified format will be generated and be ready for download. Refer to the screenshot below. On clicking **Download**, you will be able to save a copy of the report.



User Activities

Report Export: Export | Schedule Export | Last generated on 18 Jul 2022 12:17 Download as PDF

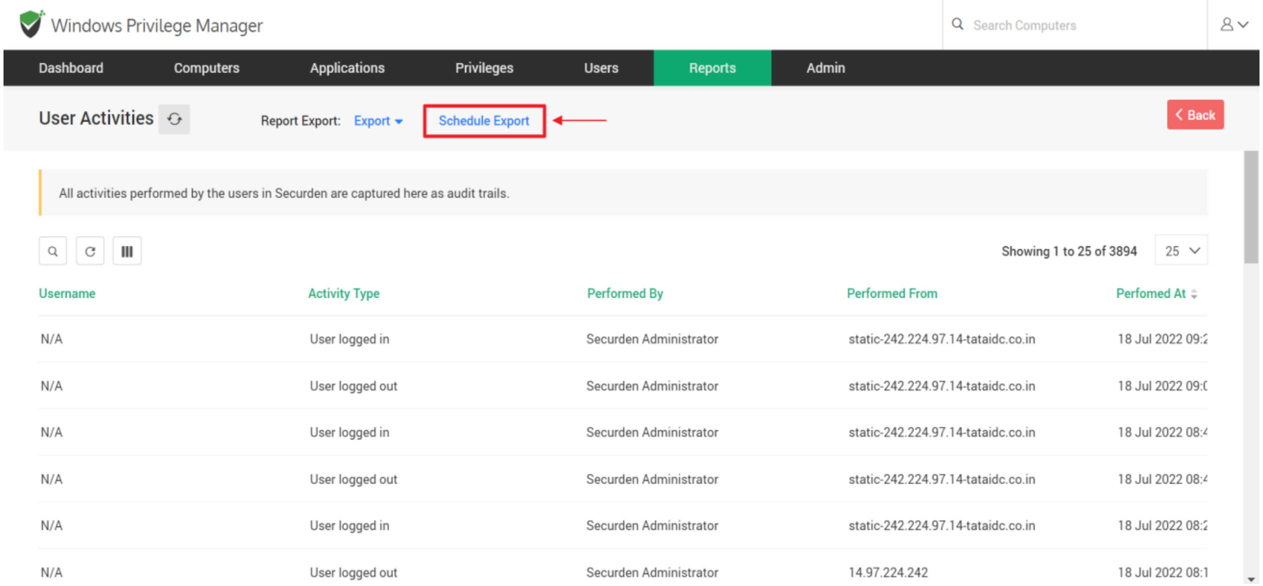
All activities performed by the users in Securden are captured here as audit trails.

Showing 1 to 25 of 447 25

Performed By	Performed From	Perfomed At
Shyam Senthil	Shyam-EMP16	18 Jul 2022 12:07
System (Schedule)	localhost	18 Jul 2022 07:16
System (Schedule)	localhost	18 Jul 2022 07:16
System (Schedule)	localhost	18 Jul 2022 07:15

Schedule exports

WPM allows you to schedule individual reports to be exported once, or periodically. All reports can be scheduled for export in a similar manner. Click on **Schedule Export** to configure.



User Activities

Report Export: Export Schedule Export

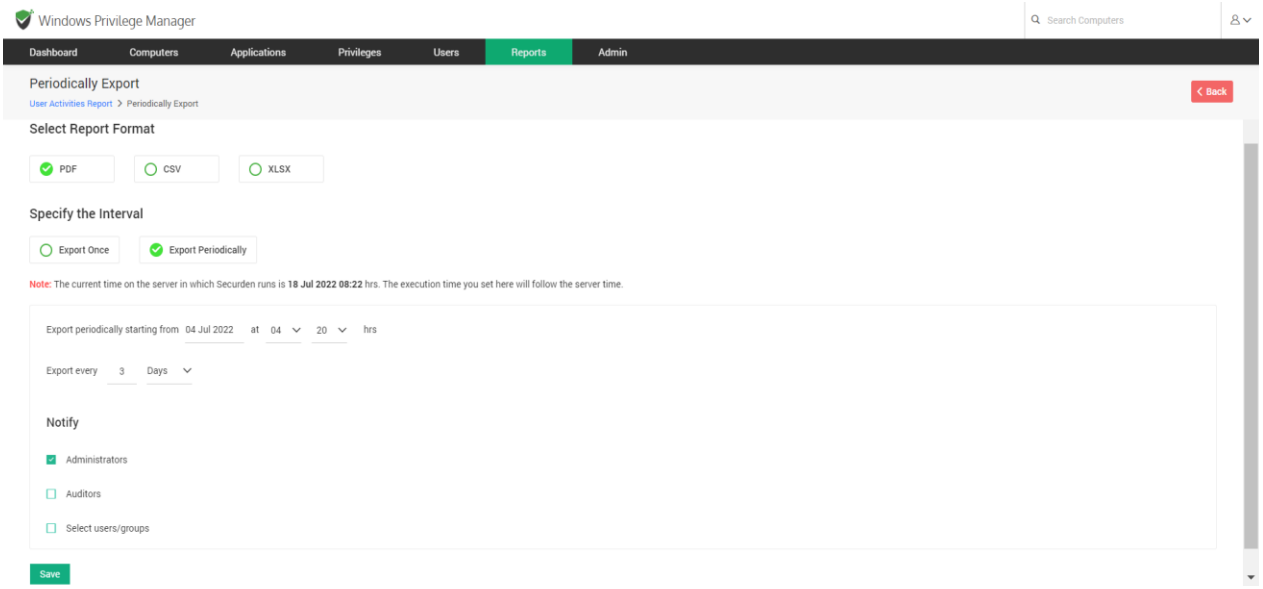
All activities performed by the users in Securden are captured here as audit trails.

Showing 1 to 25 of 3894 25

Username	Activity Type	Performed By	Performed From	Perfomed At
N/A	User logged in	Securden Administrator	static-242.224.97.14-tataidc.co.in	18 Jul 2022 09:2
N/A	User logged out	Securden Administrator	static-242.224.97.14-tataidc.co.in	18 Jul 2022 09:0
N/A	User logged in	Securden Administrator	static-242.224.97.14-tataidc.co.in	18 Jul 2022 08:4
N/A	User logged out	Securden Administrator	static-242.224.97.14-tataidc.co.in	18 Jul 2022 08:4
N/A	User logged in	Securden Administrator	static-242.224.97.14-tataidc.co.in	18 Jul 2022 08:2
N/A	User logged out	Securden Administrator	14.97.224.242	18 Jul 2022 08:1

To schedule an export you need to select/fill the following fields:

- **Report format** - You can choose the format in which reports will be exported - PDF, CSV or XLSX.
- **Interval** - You can choose to export the report once, or at a specific time interval
- **Notifications** - You can select users based on their roles and specify individual users in WPM who will be notified that a report has been exported as per the schedule.



Periodically Export

User Activities Report > Periodically Export

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 **18 Jul 2022 08:22** hrs. The execution time you set here will follow the server time.

Export periodically starting from 04 Jul 2022 at 04 20 hrs

Export every 3 Days

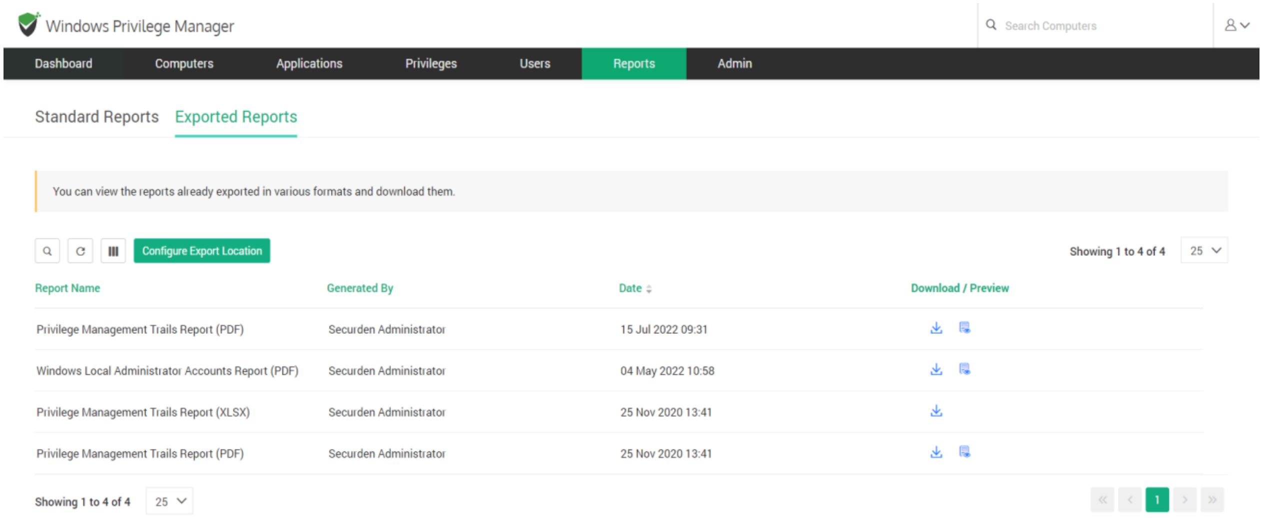
Notify

☑ Administrators

□ Auditors

□ Select users/groups

Exported reports



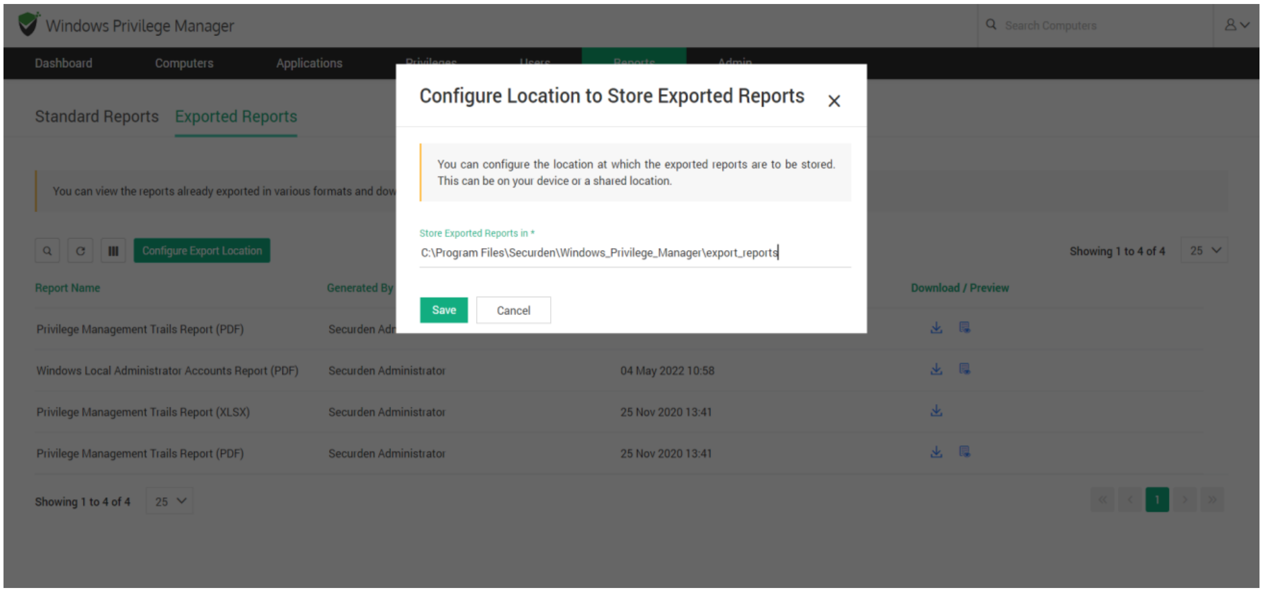
You can view the reports already exported in various formats and download them.

Showing 1 to 4 of 4

Report Name	Generated By	Date	Download / Preview
Privilege Management Trails Report (PDF)	Securden Administrator	15 Jul 2022 09:31	
Windows Local Administrator Accounts Report (PDF)	Securden Administrator	04 May 2022 10:58	
Privilege Management Trails Report (XLSX)	Securden Administrator	25 Nov 2020 13:41	
Privilege Management Trails Report (PDF)	Securden Administrator	25 Nov 2020 13:41	

Showing 1 to 4 of 4

You can configure the location at which exported reports are to be stored. This can be on your device or a shared location. To modify the download location, click **Configure Export Location**. In the GUI that opens, select the path of the location and click **Save**.



Configure Location to Store Exported Reports

You can configure the location at which the exported reports are to be stored. This can be on your device or a shared location.

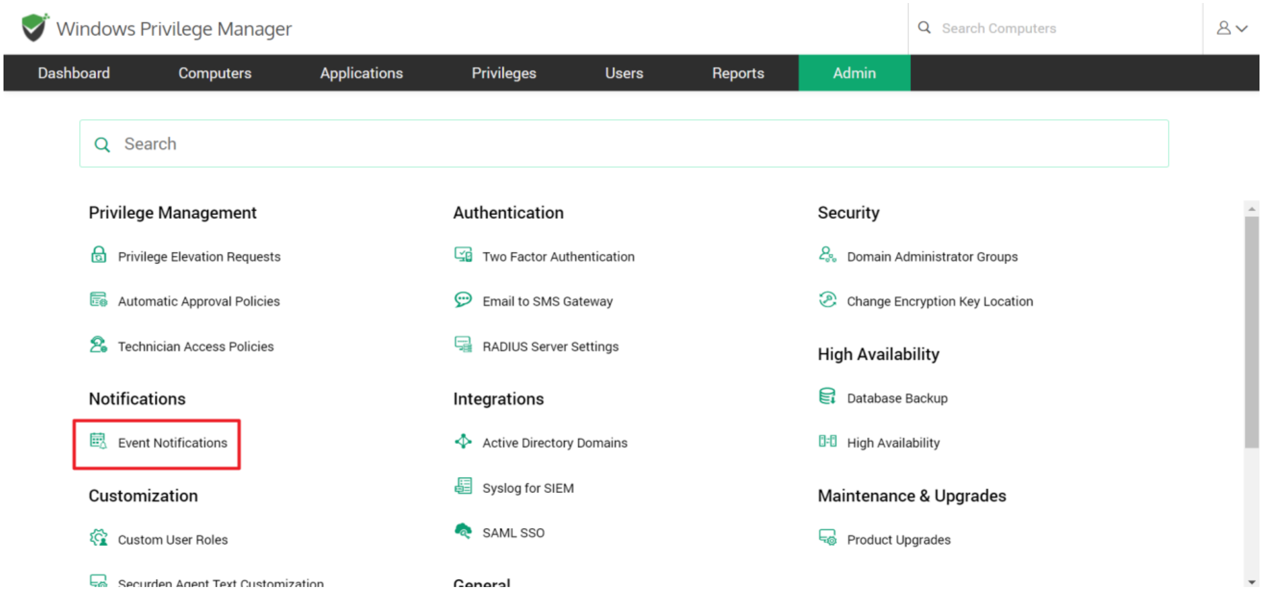
Store Exported Reports in *
C:\Program Files\Securden\Windows_Privilege_Manager\export_reports

Event Notifications

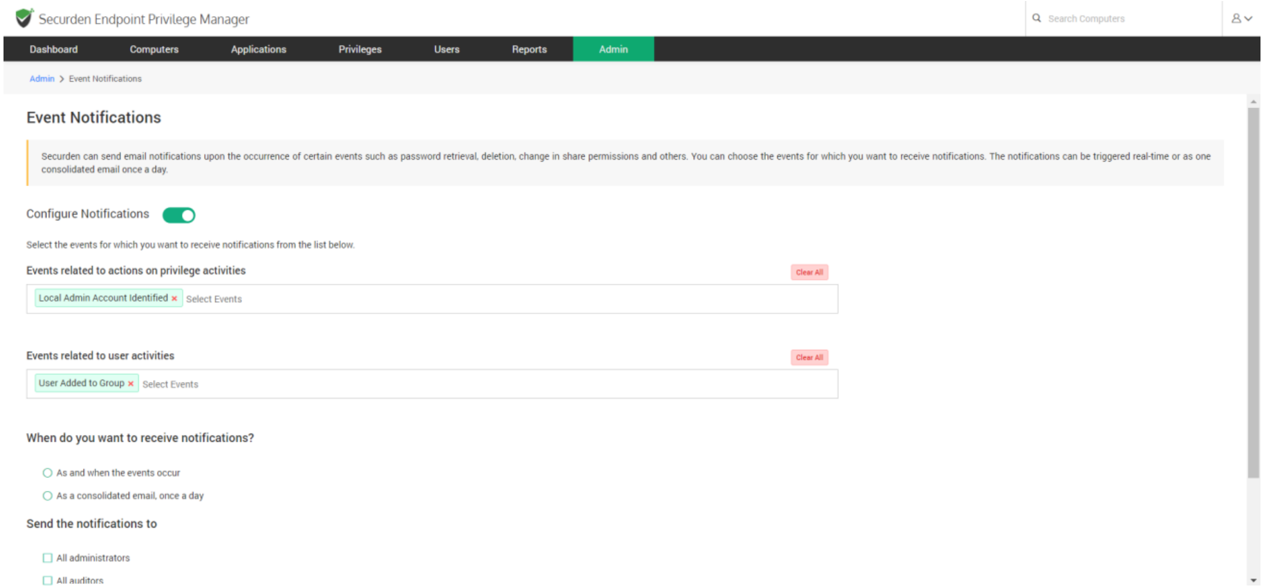
You can choose to send or receive email alerts upon the occurrence of any specific event like password retrieval, addition, deletion, and other modification activities. You can choose which events are to be notified of. The notifications can be sent out in real-time as and when the event occurs or as a consolidated email once a day.

Configure Event Notifications

Prerequisite: Before configuring event notifications, you should have configured the Mail Server Settings that enable Securden to send email notifications. You can configure this from **Admin >> General >> Mail Server Settings**.



To configure event notifications, navigate to **Admin >> Notifications >> Event Notifications** and move the toggle **Configure Notifications** to green.



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 privilege activities — Clear All

Local Admin Account Identified × Select Events

Events related to user activities — Clear All

User Added to Group × Select Events

When do you want to receive notifications?

○ As and when the events occur

○ As a consolidated email, once a day

Send the notifications to

□ All administrators

□ All auditors

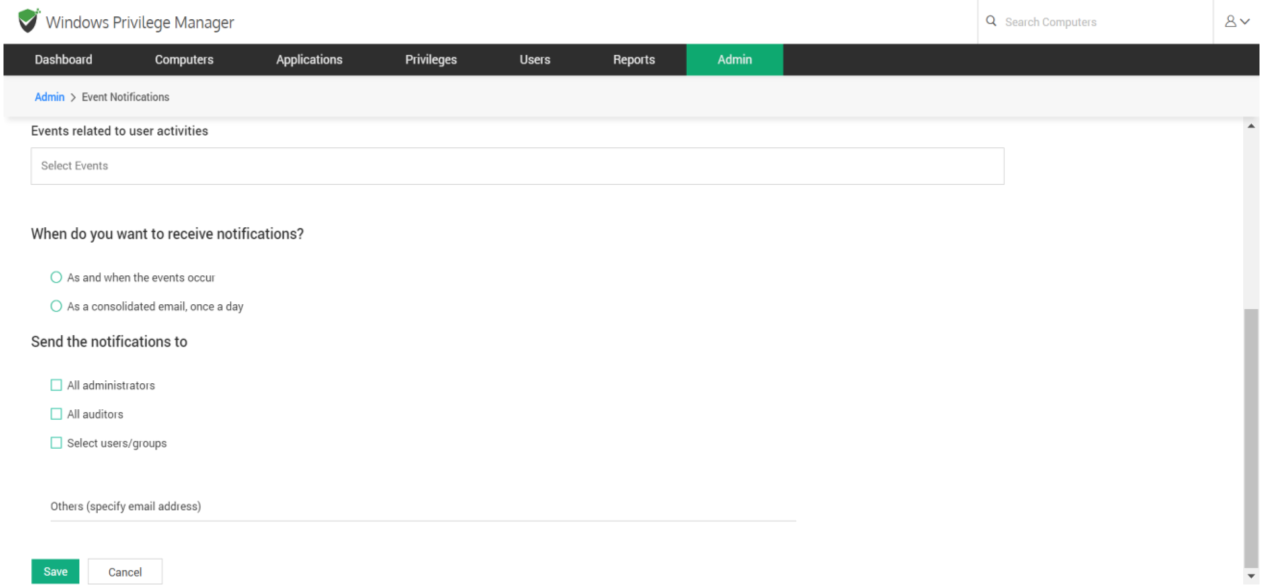
Step 1 - Select the events

After enabling notifications, you need to select the events for which the notifications are to be triggered. These can be selected from a range of user activity notifications or privileged activity notifications.

- You will see two fields named **Events related to actions on privileged activities** and **Events related to user activities**. Search these two fields for the required activities and add them.

- 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.

Step 2 - Configure notifications



Events related to user activities

Select Events

When do you want to receive notifications?

○ As and when the events occur

○ As a consolidated email, once a day

Send the notifications to

□ All administrators

□ All auditors

□ Select users/groups

Others (specify email address)

Choose when you want to receive notifications

Choose the option **As and when the events occur** if you want to get notifications in real-time. Instead, if a consolidated report once a day would be sufficient, select the option **As a consolidated email, once a day**.

Send notifications

You can trigger the notification upon the occurrence of the selected events to any specific user(s) or user group(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 field named **Others (specify email address)**.

Finally, click **Save**.

Note: You may also modify the notification settings anytime as desired.

In addition to this, you may enable and disable mail notifications for privilege elevation activities by navigating to **Admin >> Notifications >> Mail Notifications**.

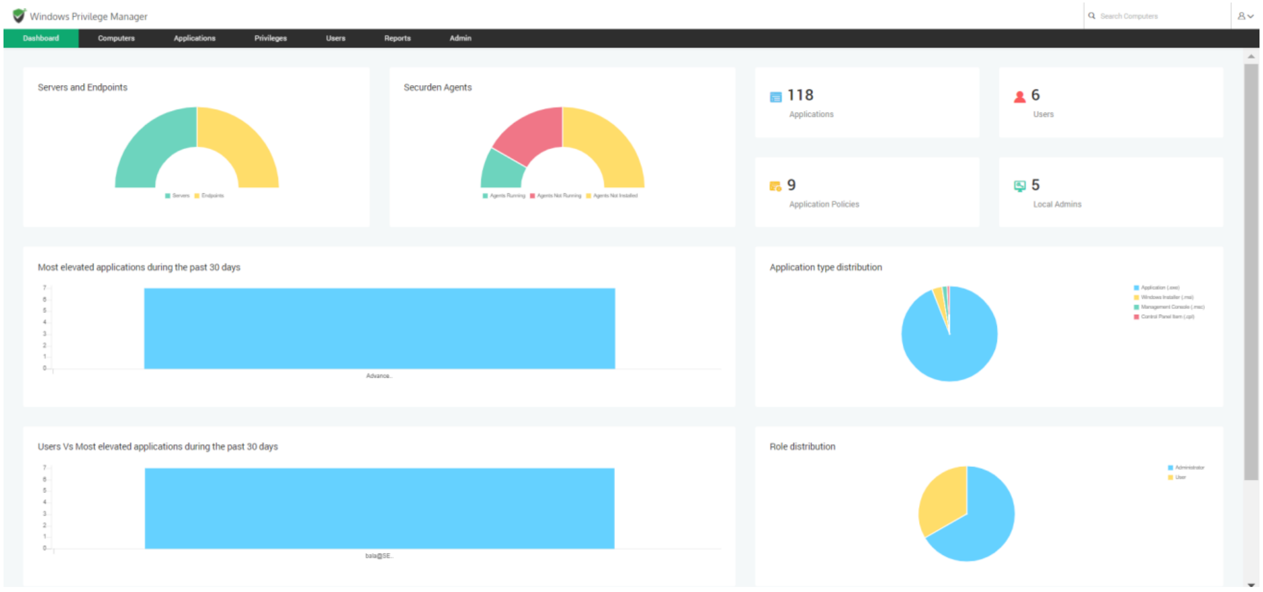
SECTION 7: Miscellaneous

Admin Dashboard

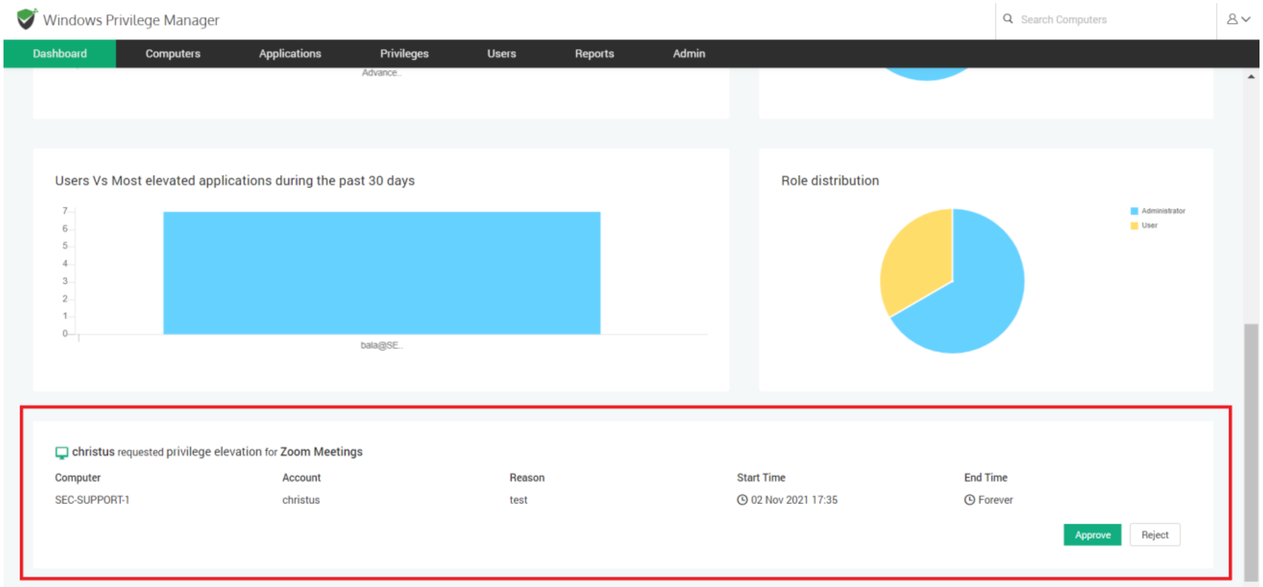
The Dashboard gives a snapshot of everything that is happening inside Securden. You will get a bird's eye view of details regarding users, endpoints, servers and also some valuable insights on application usage.

In addition to this, the dashboard also provides a consolidated count of the privileged applications installed and discovered, number of users, number of local administrator accounts, and the total number of application policies in place.

The Securden agents graph provides insights on how many agents are installed and running, how many are installed but not running, and how many endpoints are running without an agent deployed.



The Dashboard also provides insights on the most used application and the user who has used the most number of applications in Securden.



christus requested privilege elevation for Zoom Meetings

Computer	Account	Reason	Start Time	End Time
SEC-SUPPORT-1	christus	test	02 Nov 2021 17:35	Forever

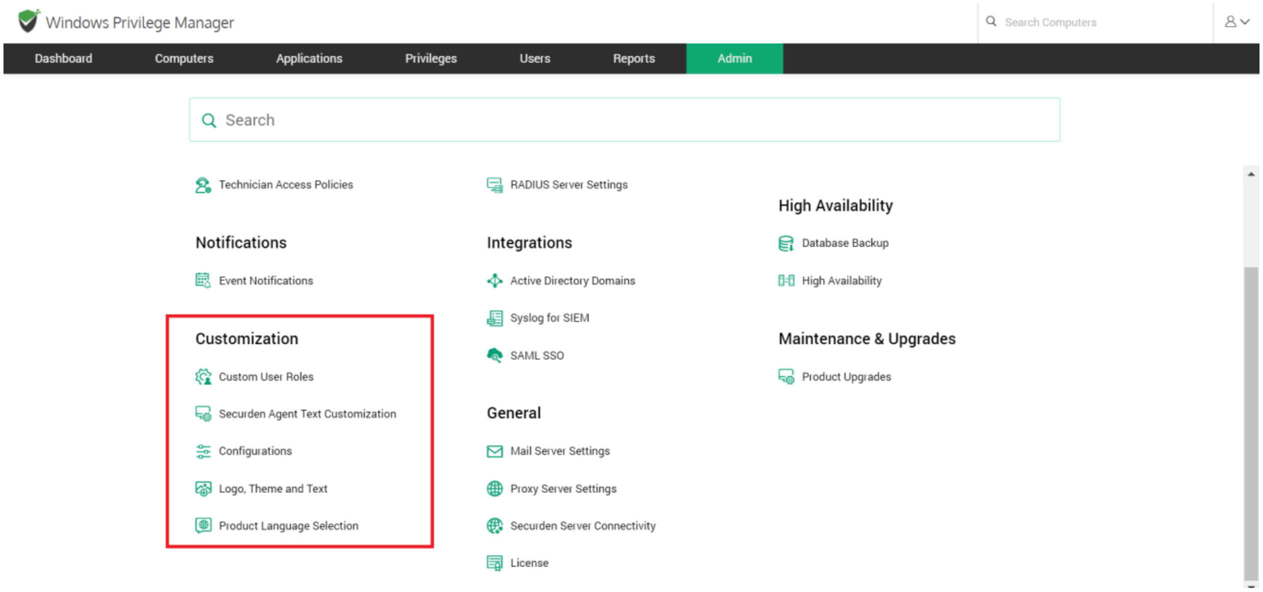
Active elevation requests, if any, can also be viewed in the **Dashboard**. You can approve or reject the raised requests from here without navigating to the **Privilege Elevation Requests** section.

While the dashboard helps with an overview of what is happening across your organization, clicking on the individual sections in the dashboard will redirect you to the respective reports section where you can derive further insights. See the reports section of this guide for further details.

Customize Securden WPM

You can customize Securden WPM to suit your organization’s unique needs. Securden WPM 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 the product interface, and so on.

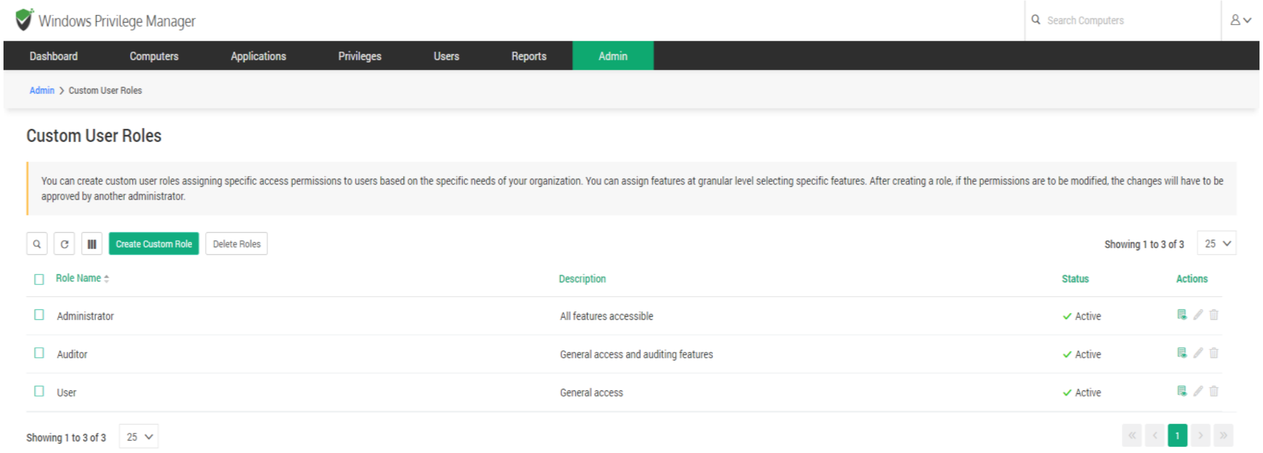
Navigate to **Admin >> Customization** section to check the various customization options.



Create and Manage Custom User Roles

The user roles help control access to platform resources. Securden WPM offers three predefined user roles carrying various access privileges. These include User, Auditor, and Administrator. Additionally, a custom role named **Approver** is also comes as a built-in role out-of-the-box.

Navigate to **Admin >> Customisations>> Custom User Roles** to manage 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.

Showing 1 to 3 of 3

□	Role Name	Description	Status	Actions
□	Administrator	All features accessible	✓ Active	
□	Auditor	General access and auditing features	✓ Active	
□	User	General access	✓ Active	

Showing 1 to 3 of 3

User: Users with this role will be granted general access to the web interface. This default role has minimal privileges and represents a standard user.

Auditor: Users with this role will be able to access audit records in addition to the basic privileges similar to a standard user.

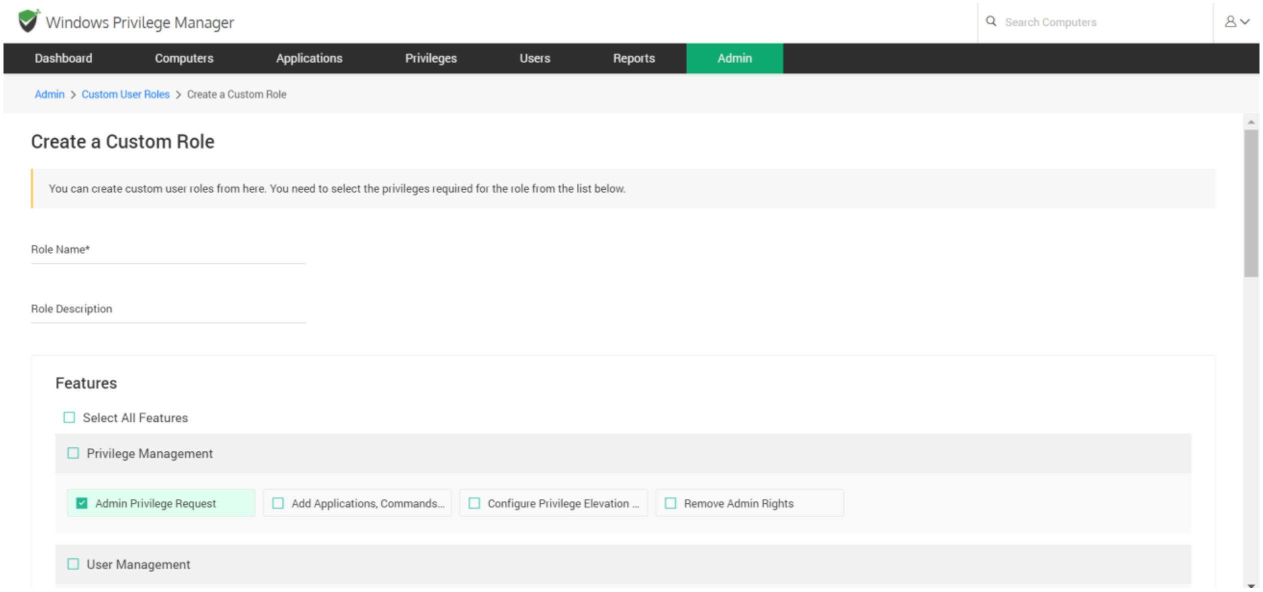
Administrator: This default user role carries the highest level of privileges inside the web interface. Users with administrator roles will be able to control application access, customize the interface, control all aspects of the web-interface. It is recommended to limit the number of administrators to two or three as a security best practice.

Additionally, you can create custom user roles assigning specific access permissions to users based on the specific needs of your organization.

You can assign privileges at a granular level by selecting the required actions. As an additional security measure, dual controls are enforced for custom role creation and modification. The custom role created or modified by one administrator will have to be approved by another administrator.

Create a Custom User Role

Navigate to **Admin >> Customisations>> Custom User Roles >> Create Custom Role** to create a new custom user role.


Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
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*

Role Description

Features

□ Select All Features

□ Privilege Management

☑ Admin Privilege Request □ Add Applications, Commands... □ Configure Privilege Elevation ... □ Remove Admin Rights

□ User Management

Specify a name and description for the new role and then select the privileges required for that specific role from the list. Various actions and operations in Securden are listed as checkboxes. You can granularly select any or all actions within each category.

These features are categorized under privilege management, user management, user group management, computer management, computer group management, reports, and admin operations.

- The features listed under privilege management are related to aspects of managing application privileges, removing admin rights, managing elevation requests, creating policies and so on.

- User and group management section contains features that help onboard and offboard users individually and in bulk, managing 2FA, creating and managing user groups, configuring temporary access, manage authentication methods, manage concurrent logins and so on.

- Computer and Computer group management contains features that let a user add, delete and modify computers individually and in bulk respectively.

- Reports section contains features that lets an user to access and export different types of reports.

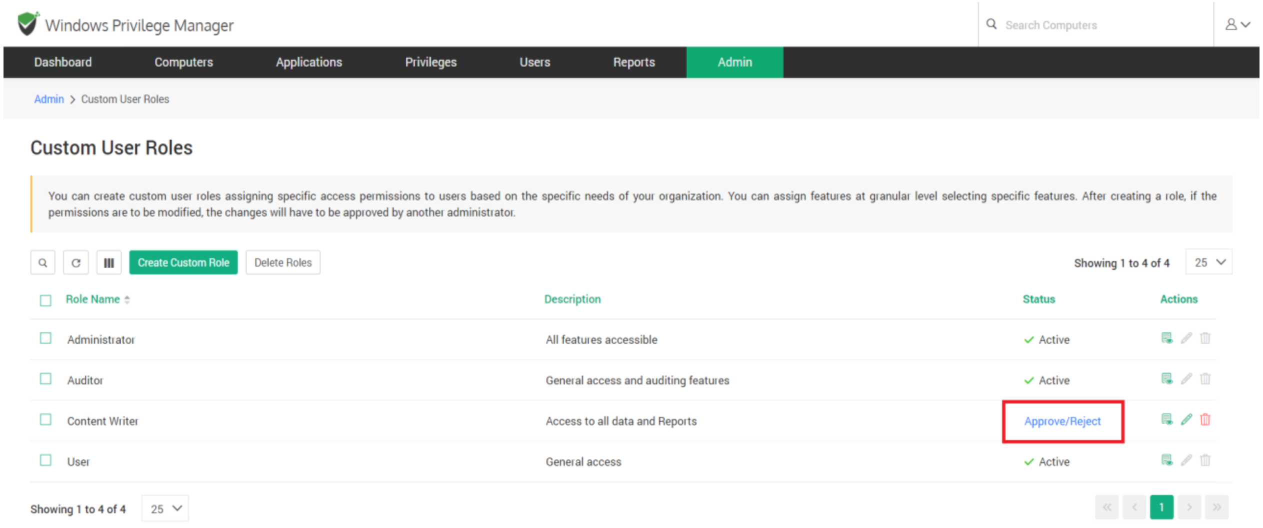
- Admin management section contains features that help manage the Securden WPM user interface and lets the user configure and manage security features such as 2FA, automated privilege elevation requests, etc.

After selecting the required features, click **Save**.

Approval for the new role

The newly created role will have to be approved by another administrator for it to become active.

When another administrator logs in and navigates to the Custom Roles page, the link to approve or reject the new role will appear as shown below.



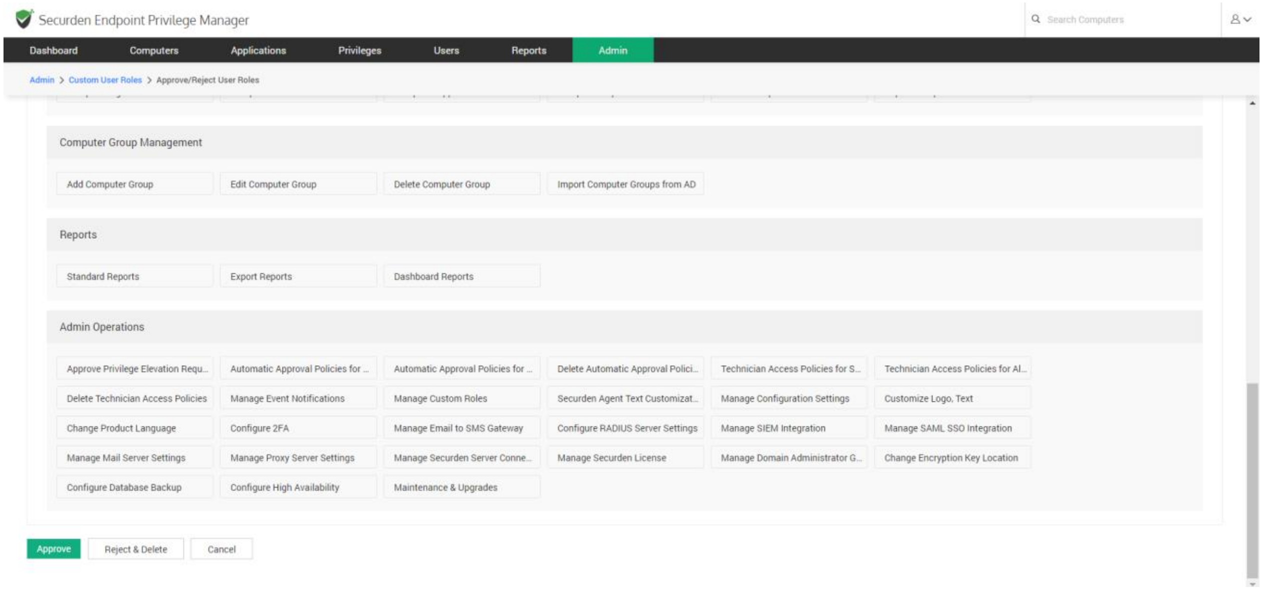
Custom User Roles

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.

□	Role Name	Description	Status	Actions
□	Administrator	All features accessible	✓ Active	
□	Auditor	General access and auditing features	✓ Active	
□	Content Writer	Access to all data and Reports	Approve/Reject	
□	User	General access	✓ Active	

Showing 1 to 4 of 4 25

On clicking Approve/Reject, you will be able to see the privileges that are associated with the user role.



Computer Group Management

Add Computer Group | Edit Computer Group | Delete Computer Group | Import Computer Groups from AD

Reports

Standard Reports | Export Reports | Dashboard Reports

Admin Operations

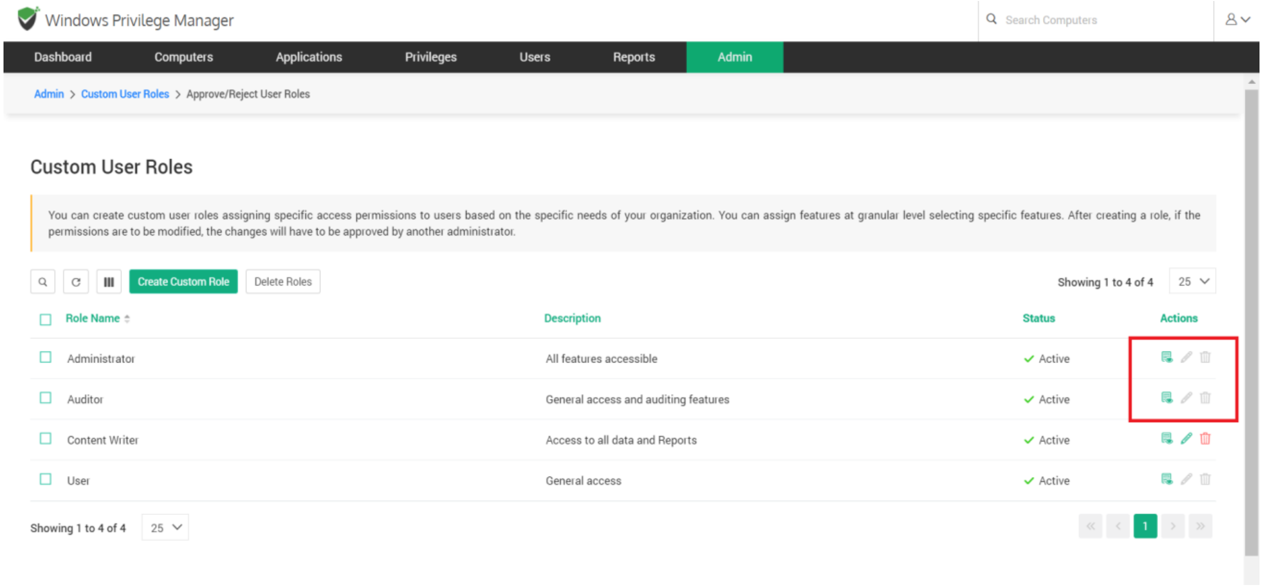
Approve Privilege Elevation Requ... | Automatic Approval Policies for ... | Automatic Approval Policies for ... | Delete Automatic Approval Polici... | Technician Access Policies for S... | Technician Access Policies for Al...
Delete Technician Access Policies | Manage Event Notifications | Manage Custom Roles | Securden Agent Text Customizat... | Manage Configuration Settings | Customize Logo, Text
Change Product Language | Configure 2FA | Manage Email to SMS Gateway | Configure RADIUS Server Settings | Manage SIEM Integration | Manage SAML SSO Integration
Manage Mail Server Settings | Manage Proxy Server Settings | Manage Securden Server Conne... | Manage Securden License | Manage Domain Administrator G... | Change Encryption Key Location
Configure Database Backup | Configure High Availability | Maintenance & Upgrades

You may choose to **Approve** or **Reject and Delete** the user role.

Managing Custom Roles

The **Admin >> Customization>> Custom User Roles** page displays the list of all user roles that are already present. The **Role name, Description,**

Status, and Actions are displayed in a tabular format. The status shows whether that user role is in an **Active** status or awaiting approval.



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.

Showing 1 to 4 of 4 25

□	Role Name	Description	Status	Actions
□	Administrator	All features accessible	✓ Active	
□	Auditor	General access and auditing features	✓ Active	
□	Content Writer	Access to all data and Reports	✓ Active	
□	User	General access	✓ Active	

Showing 1 to 4 of 4 25

Actions

Under Actions, you can **View Role Entitlements, Edit, and Delete user roles**. The **system-defined roles** cannot be **edited or deleted.**

View Role Entitlements

This page shows you the list of all permissions granted to the selected custom role.

Edit Custom Role

You can edit the permissions granted for any custom role. When you do so, the changes will have to be approved by another administrator.

Delete Custom Roles

You can delete a custom role anytime. If the role has any associated users, you won't be able to delete the role. You will have to assign a different role for the associated users before deleting the role.

Configurations

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

The customization options have been classified into different categories.
The categories include Default Selection, Privilege Management, Temporary Full Admin access, Elevation using MFA, Technician Access using MFA, and General configurations.

Each option under Default Selection helps configure Securden WPM to establish default options for different aspects such as logging in to the interface, importing a new user and so on.

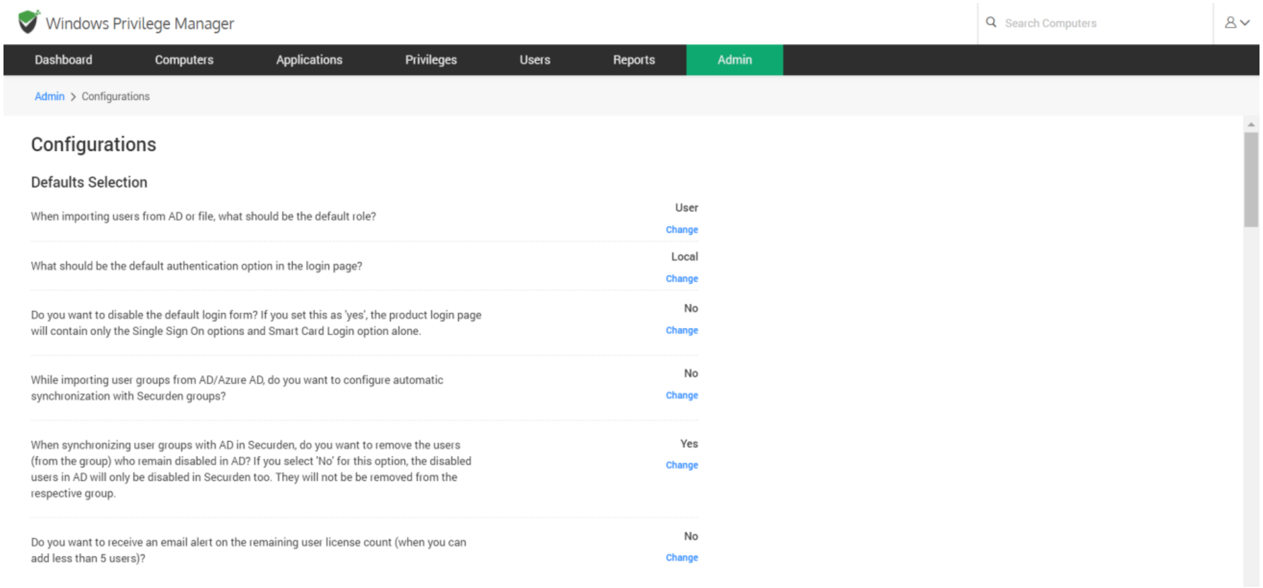
Options under privilege management are involved in managing privilege requests and helps automate helpdesk tasks upto a certain level.

You can also configure certain parameters concerned with granting temporary admin rights to users. This includes limiting the maximum duration of elevated privileges, allowing users to request additional time duration for administrative access and so on.

You can setup mandatory MFA for users and technicians while elevating privileges from the **Elevation Using MFA** and the **Technician Access using MFA** sections respectively

General section has options that help configure the basic preferences inside the Securden WPM user interface. The options include setting up the default date and time format, session timeout, enabling and disabling local authentication, allowing users to reset passwords using the forgot password option.

The exact configuration options are quite simple. You can set the options as required.



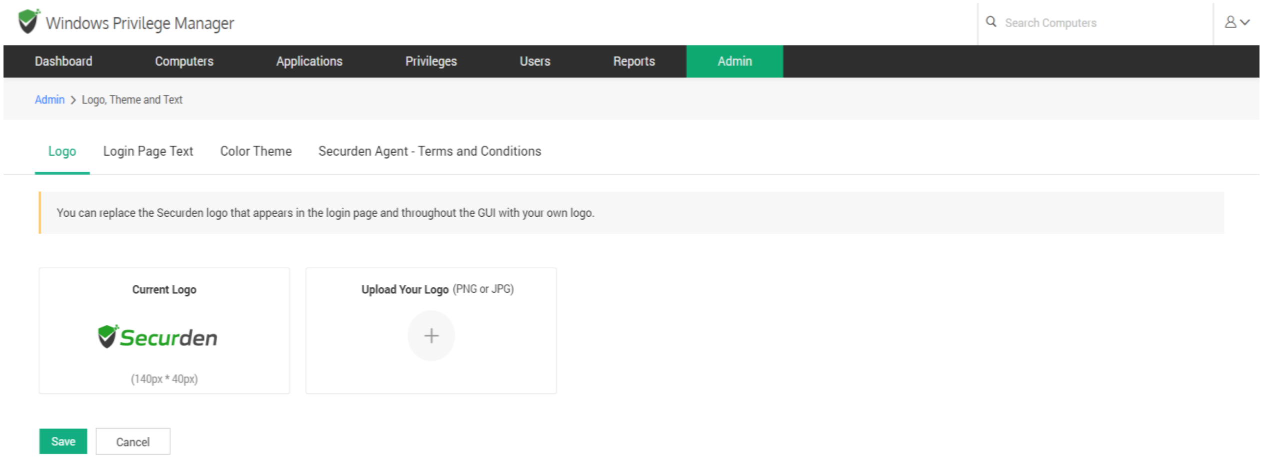
Configurations

Defaults Selection

When importing users from AD or file, what should be the default role?	User Change
What should be the default authentication option in the login page?	Local Change
Do you want to disable the default login form? If you set this as 'yes', the product login page will contain only the Single Sign On options and Smart Card Login option alone.	No Change
While importing user groups from AD/Azure AD, do you want to configure automatic synchronization with Securden groups?	No Change
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 be removed from the respective group.	Yes Change
Do you want to receive an email alert on the remaining user license count (when you can add less than 5 users)?	No Change

Changing Logo, Theme, and Text

You can replace the Securden logo that appears on the login page and on the browser extension GUI with your own logo. Navigate to **Admin >> Customization >> Logo, Theme and Text.**

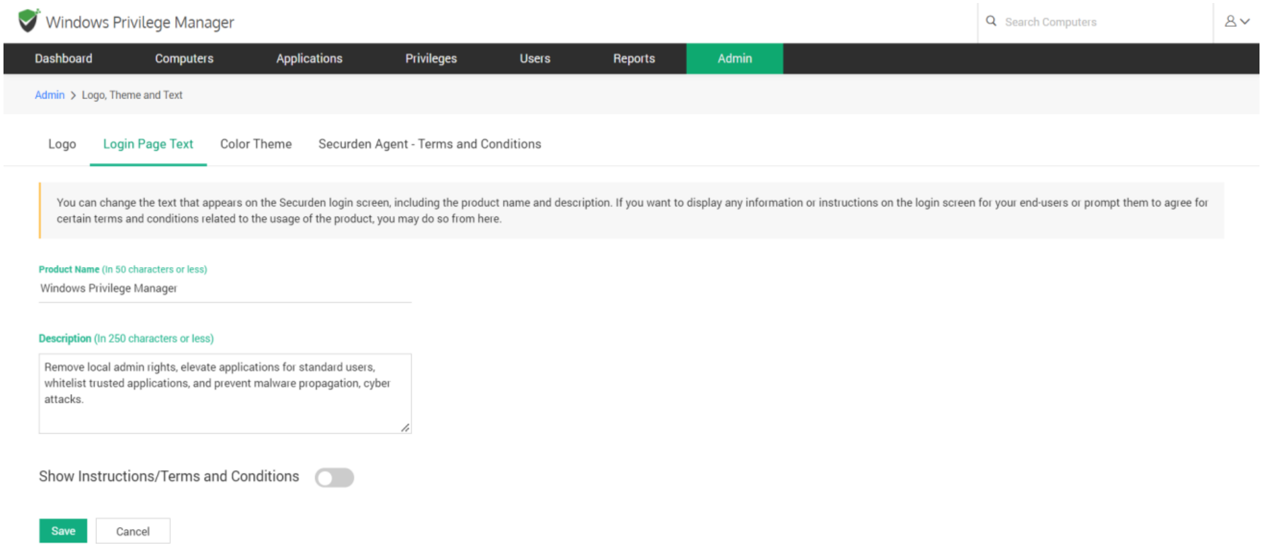


You can replace the Securden logo that appears in the login page and throughout the GUI with your own logo.

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 PNG or JPG format and the selected file should not exceed 1 MB in size.

Once uploaded, Click **Save**.

Login Page Text



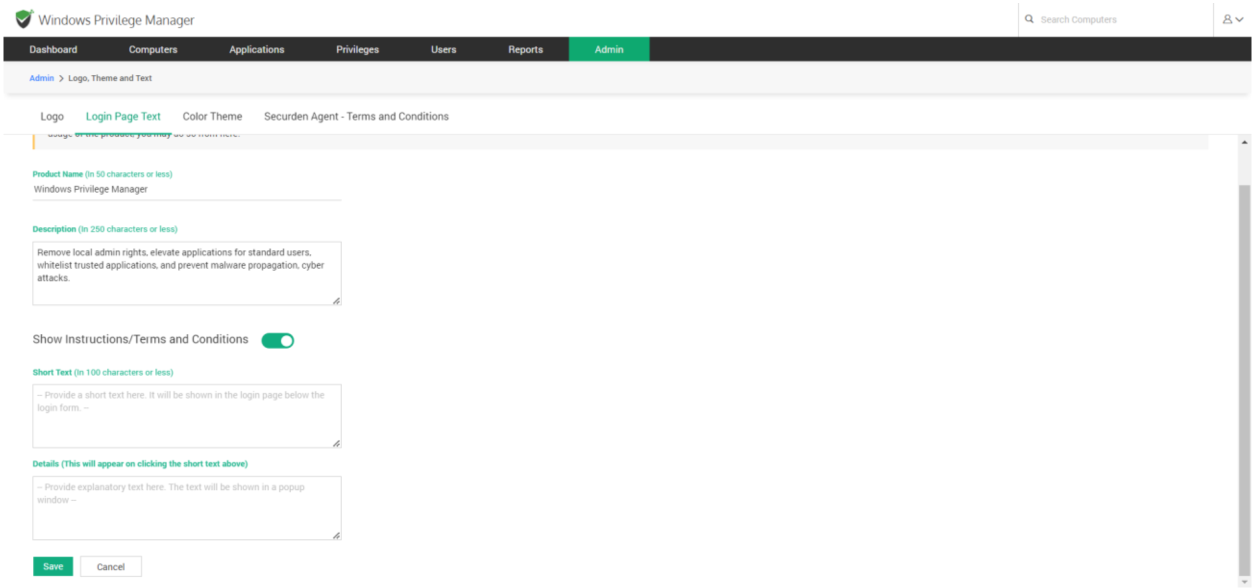
You can change the text that appears on the Securden login screen, including the product name and description. If you want to display any information or instructions on the login screen for your end-users or prompt them to agree for certain terms and conditions related to the usage of the product, you may do so from here.

Product Name (In 50 characters or less)
Windows Privilege Manager

Description (In 250 characters or less)
Remove local admin rights, elevate applications for standard users, whitelist trusted applications, and prevent malware propagation, cyber attacks.

Show Instructions/Terms and Conditions ○

You can change the text that appears on the Securden login screen, including the product name and description. If you want to display any additional 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 by switching the toggle ON in this page. Click the **Admin >> Customization >> Logo, Theme and Text >> Login Page Text.**



usage of the product, you may do so from here.

Product Name (In 50 characters or less)

Windows Privilege Manager

Description (In 250 characters or less)

Remove local admin rights, elevate applications for standard users, whitelist trusted applications, and prevent malware propagation, cyber attacks.

Show Instructions/Terms and Conditions ●

Short Text (In 100 characters or less)

-- Provide a short text here. It will be shown in the login page below the login form. --

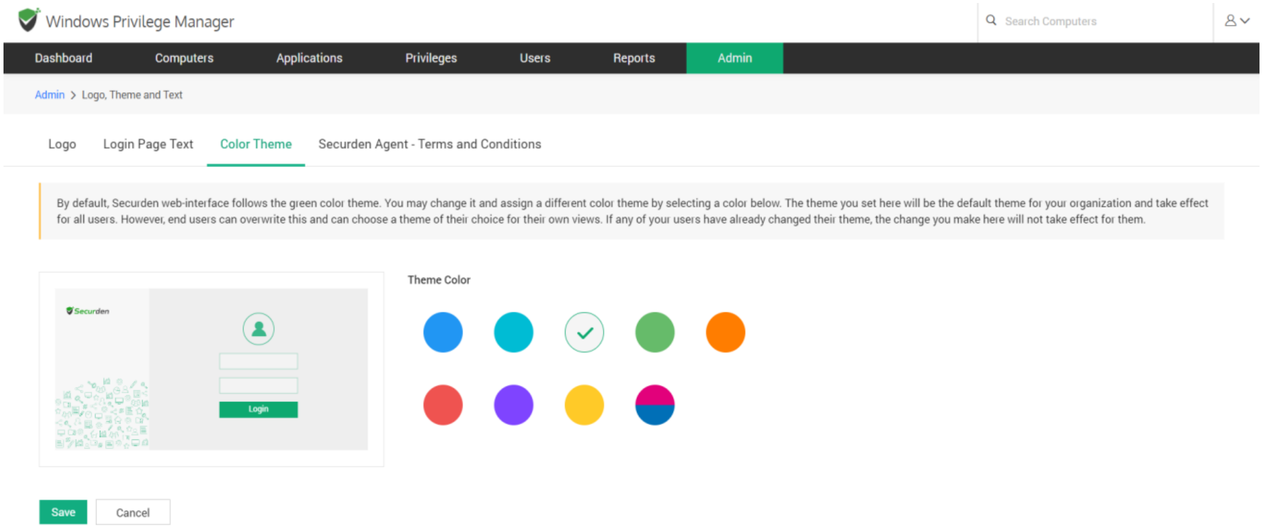
Details (This will appear on clicking the short text above)

-- Provide explanatory text here. The text will be shown in a popup window --

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.**

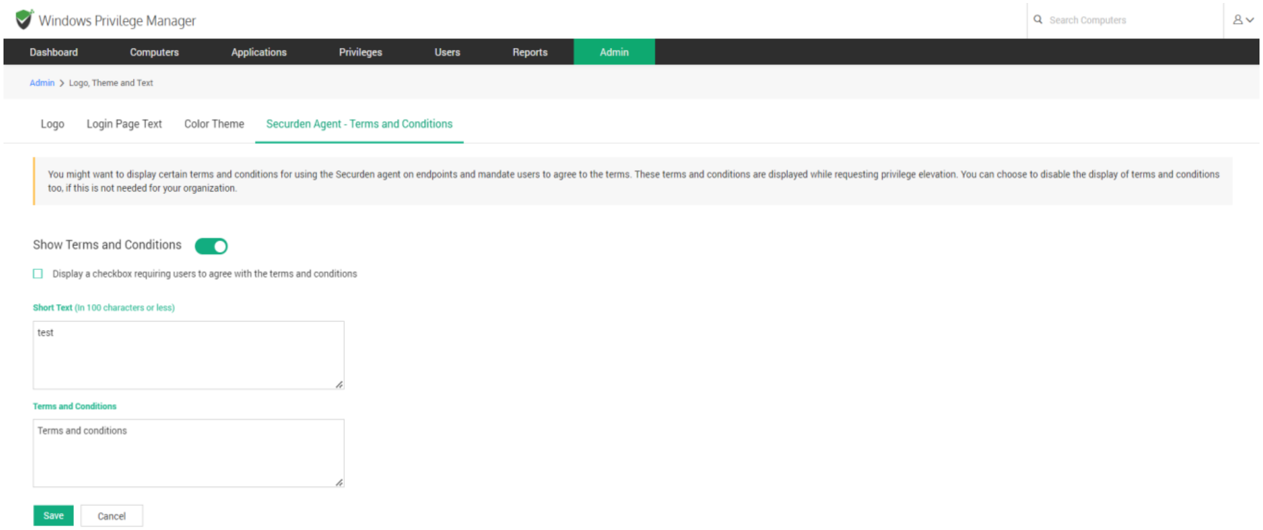


By default, Securden web-interface follows the green color theme. You may change it and assign a different color theme by selecting a color below. The theme you set here will be the default theme for your organization and take effect for all users. However, end users can overwrite this and can choose 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.

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 Agents - Terms and Conditions

If you want to display any Terms and Conditions the users need to agree to upon using the Securden Agent, you may do so from this section. To display the terms and conditions, enable the feature by toggling the button and provide the text to be displayed in the appropriate fields. There is an option to display a checkbox using which users can express their consent to the terms and conditions displayed while requesting privilege elevation.



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.

Show Terms and Conditions

□ Display a checkbox requiring users to agree with the terms and conditions

Short Text (In 100 characters or less)

test

Terms and Conditions

Terms and conditions

Product Language Selection

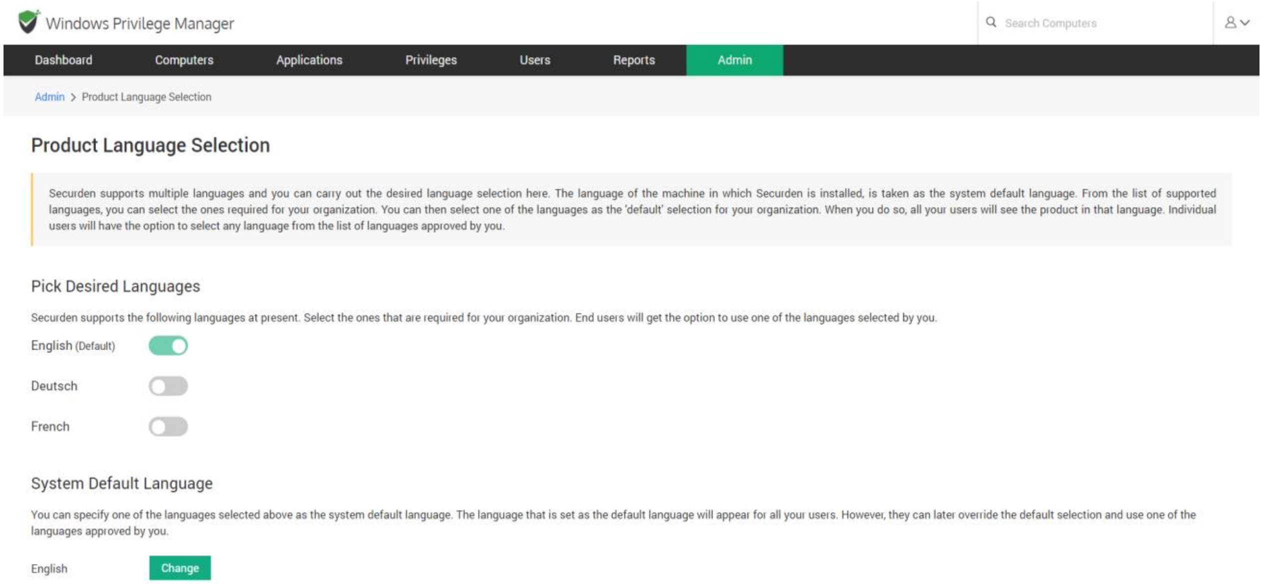
Securden WPM supports multiple languages and you can select the desired language here. The language of the machine in which Securden WPM is installed, is taken as the system default language. From the list of supported languages, you can select the ones required for your organization. You can then select 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>> Customisations >> Product Language Selection.** 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 currently available and supported by Securden at present are:

- English
- French
- Deutsch



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) ●
Deutsch ○
French ○

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

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.

Security Settings

You can carry out certain security settings to protect the Securden installation and control access to the interface.

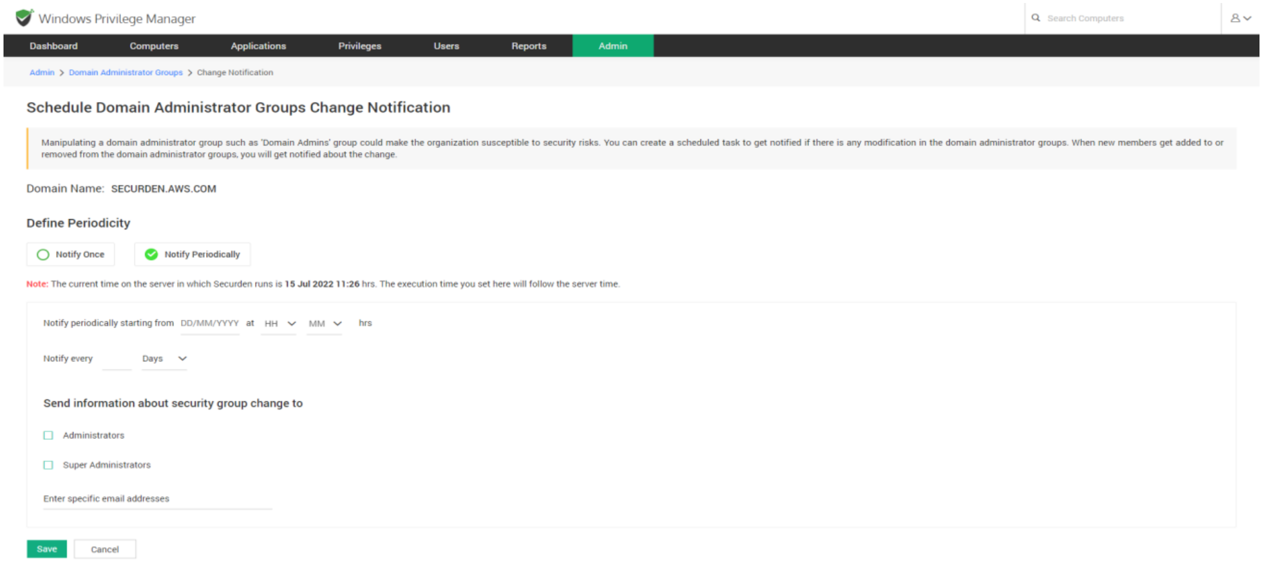
Monitor Changes to Domain Admin Groups

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** section. In the GUI that opens, click the button **Schedule Notify**.



Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Domain Administrator Groups > Change Notification

Schedule Domain Administrator Groups Change Notification

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.

Domain Name: SECURDEN.AWS.COM

Define Periodicity

○ Notify Once ● Notify Periodically

Note: The current time on the server in which Securden runs is **15 Jul 2022 11:26** hrs. The execution time you set here will follow the server time.

Notify periodically starting from DD/MM/YYYY at HH MM hrs

Notify every Days

Send information about security group change to

□ Administrators

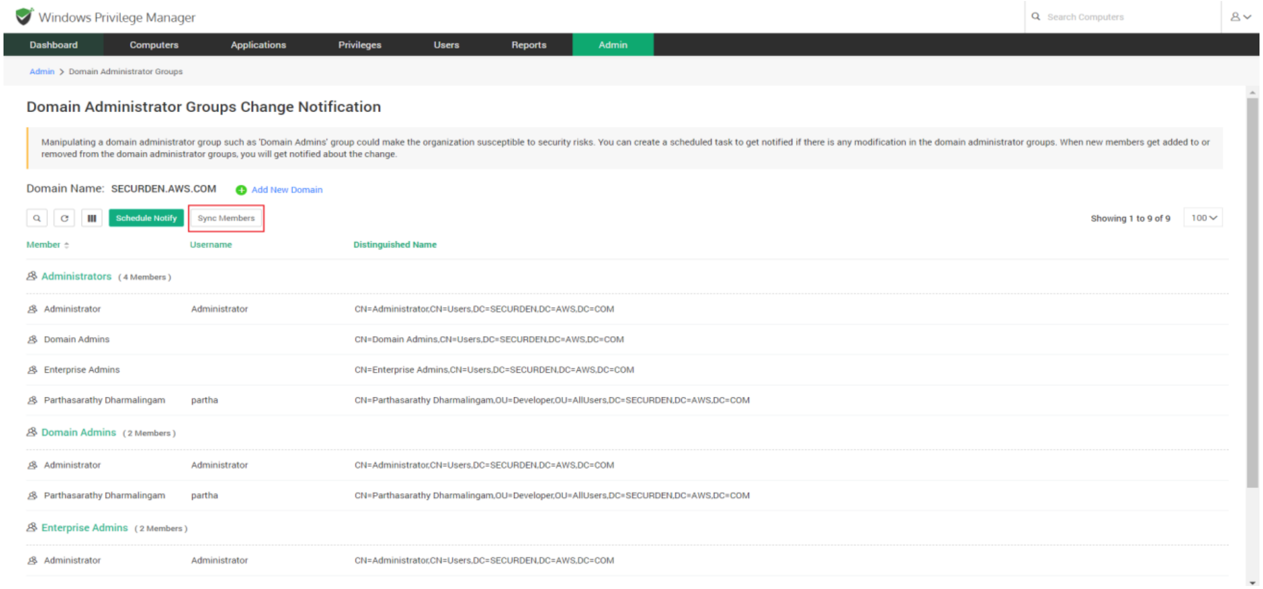
□ Super Administrators

Enter specific email addresses

You have two options here - carry out the check once (**Notify Once**) at the required time slot and trigger notification (or) carry out the check at periodic intervals (**Notify Periodically**). Select the required option in the 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 a 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.



Domain Administrator Groups Change Notification

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.

Domain Name: SECURDEN.AWS.COM

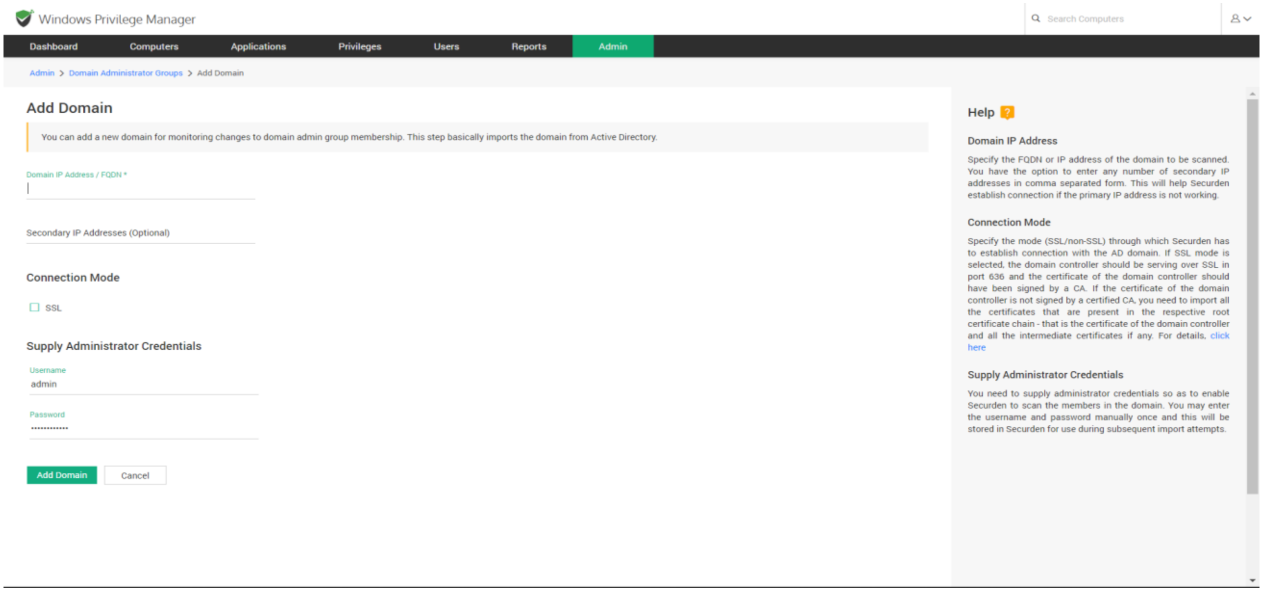
Member	Username	Distinguished Name
Administrators (4 Members)		
Administrator	Administrator	CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM
Domain Admins		CN=Domain Admins,CN=Users,DC=SECURDEN,DC=AWS,DC=COM
Enterprise Admins		CN=Enterprise Admins,CN=Users,DC=SECURDEN,DC=AWS,DC=COM
Parthasarathy Dharmalingam	partha	CN=Parthasarathy Dharmalingam,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM
Domain Admins (2 Members)		
Administrator	Administrator	CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM
Parthasarathy Dharmalingam	partha	CN=Parthasarathy Dharmalingam,OU=Developer,OU=AllUsers,DC=SECURDEN,DC=AWS,DC=COM
Enterprise Admins (2 Members)		
Administrator	Administrator	CN=Administrator,CN=Users,DC=SECURDEN,DC=AWS,DC=COM

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**.

Follow the steps below to add a new domain.

Click on **Add New Domain** in the Domain administrator groups interface. In the GUI that opens, enter the following details:


Windows Privilege Manager
Search Computers
Dashboard
Computers
Applications
Privileges
Users
Reports
Admin
Admin > Domain Administrator Groups > Add Domain

Add Domain

You can add a new domain for monitoring changes to domain admin group membership. This step basically imports the domain from Active Directory.

Domain IP Address / FQDN *

Secondary IP Addresses (Optional)

Connection Mode

□ SSL

Supply Administrator Credentials

Username: admin

Password: ••••••••••••

Help

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 stored in Securden for use during subsequent import attempts.

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 a comma-separated form. This will help Securden establish a connection if the primary IP address is not working.

Secondary IP Address

Specify the secondary IP address of the domain, this is useful in case the primary IP is not reachable.

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.

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.

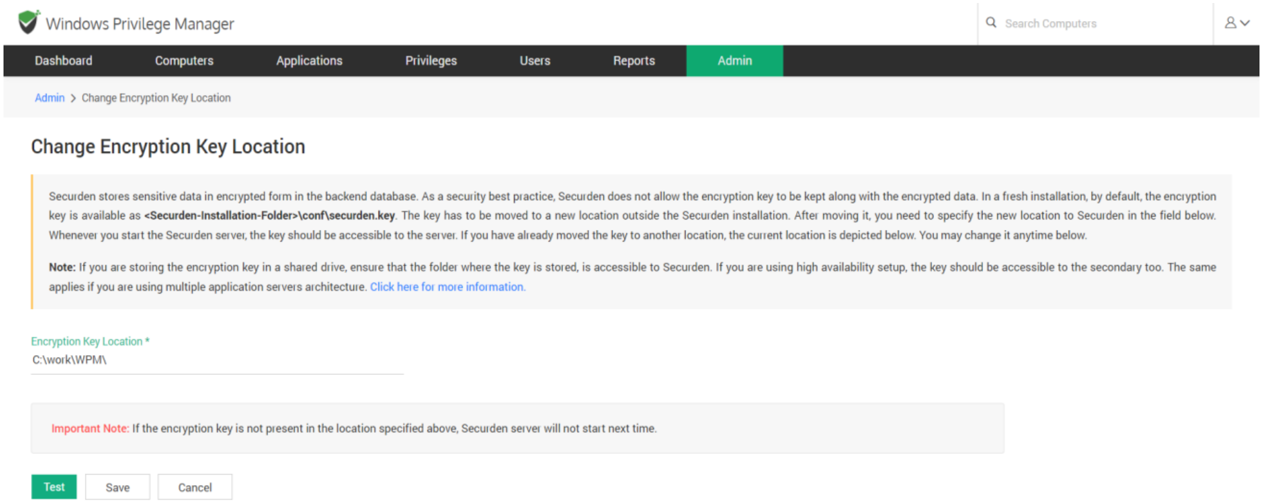
Once you are done filling up the form, you can click **Add Domain** to complete the process.

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.

When deploying the product to production, Securden enforces moving the key out of the installation folder.



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.

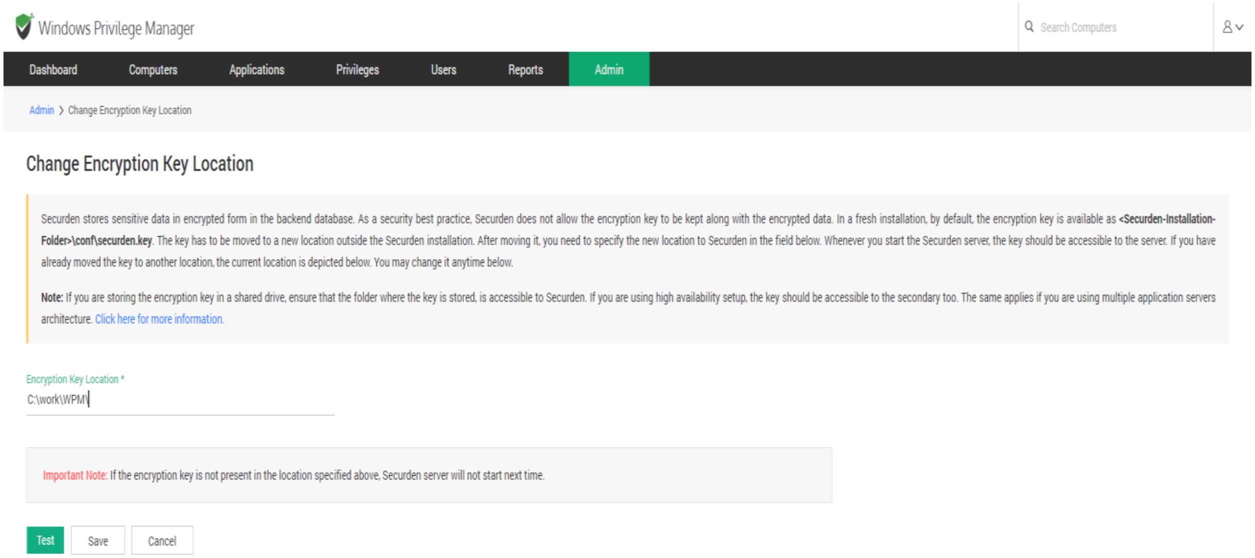
Note: If you are storing the encryption key in a shared drive, ensure that the folder where the key is stored, is accessible to Securden. If you are using high availability setup, the key should be accessible to the secondary too. The same applies if you are using multiple application servers architecture.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

Encryption Key Location *
C:\work\WPM\

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

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, Navigate to **Admin >> Security >> Change 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.

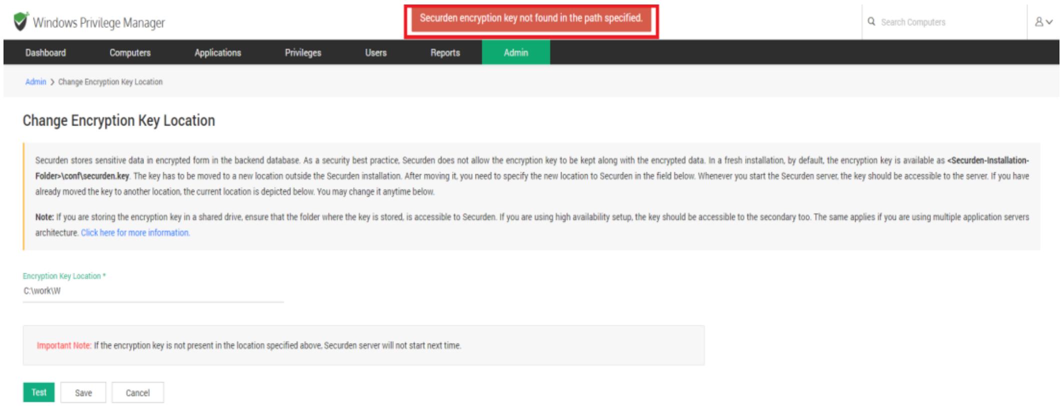
Encryption Key Location *
C:\work\WPM\

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

Specify the location.

Click **Test** to check whether the key is found in the specified location.

a. If the floating screen states **Securden encryption key not found in the path specified**, the specified file path is incorrect. Try again with the correct file path.



Securden encryption key not found in the path specified.

Change Encryption Key Location

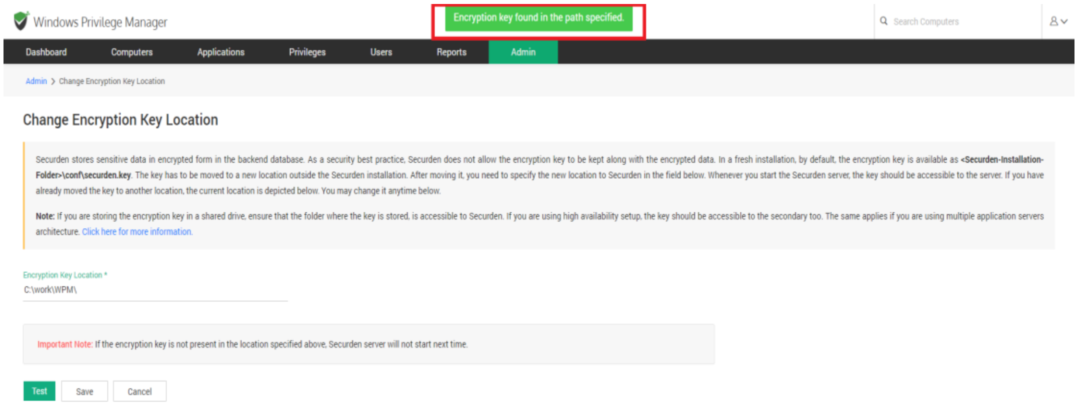
Securden stores sensitive data in encrypted form in the backend database. As a security best practice, Securden does not allow the encryption key to be kept along with the encrypted data. In a fresh installation, by default, the encryption key is available as **<Securden-Installation-Folder>\conf\securden.key**. 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\W

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

b. 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**.


Windows Privilege Manager
Encryption key found in the path specified.
Search Computers
Dashboard
Computers
Applications
Privileges
Users
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\WPM\

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

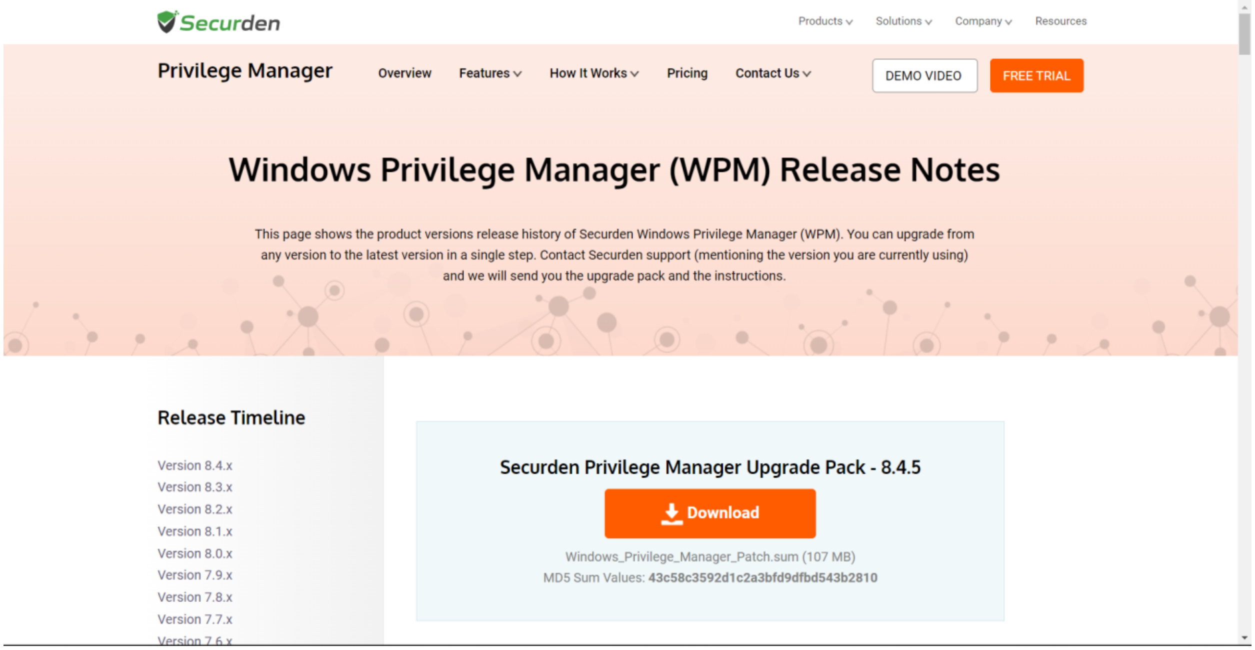
Once the location is verified, click on **Save**.

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.

Product Upgrade

Securden products are upgraded to keep security measures always proactive which in turn enables you to stand a step ahead of the looming threats. To upgrade Securden WPM, navigate to **Admin >> Maintenance and Upgrades >> Product Upgrade**.

Check for the latest updates to Windows Privilege Manager here. https://www.securden.com/windows-privilege-manager/release-notes.html



Windows Privilege Manager (WPM) Release Notes

This page shows the product versions release history of Securden Windows Privilege Manager (WPM). You can upgrade from any version to the latest version in a single step. Contact Securden support (mentioning the version you are currently using) and we will send you the upgrade pack and the instructions.

Release Timeline

Version 8.4.x
Version 8.3.x
Version 8.2.x
Version 8.1.x
Version 8.0.x
Version 7.9.x
Version 7.8.x
Version 7.7.x
Version 7.6.x

Securden Privilege Manager Upgrade Pack - 8.4.5

Windows_Privilege_Manager_Patch.sum (107 MB)
MD5 Sum Values: **43c58c3592d1c2a3bfd9dfbd543b2810**

Steps to upgrade:

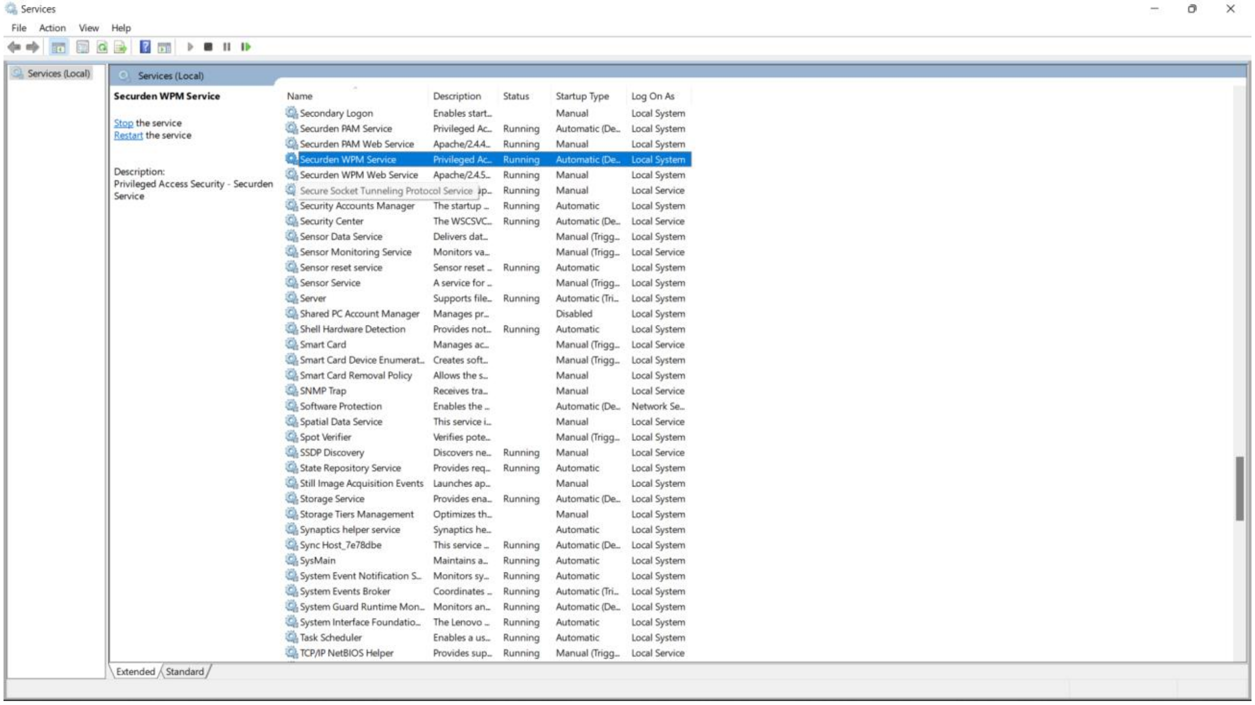
Step 1: How to download the upgrade pack?

Download the upgrade pack from the link below.

https://www.securden.com/windows-privilege-manager/release-notes.html#upgrade-pack

Step 2: How to stop Securden WPM service?

- Open Run on the primary server by pressing **Win+R**.
- Open **services.msc**.
- Search and locate **Securden WPM Service** from the list of all available services.



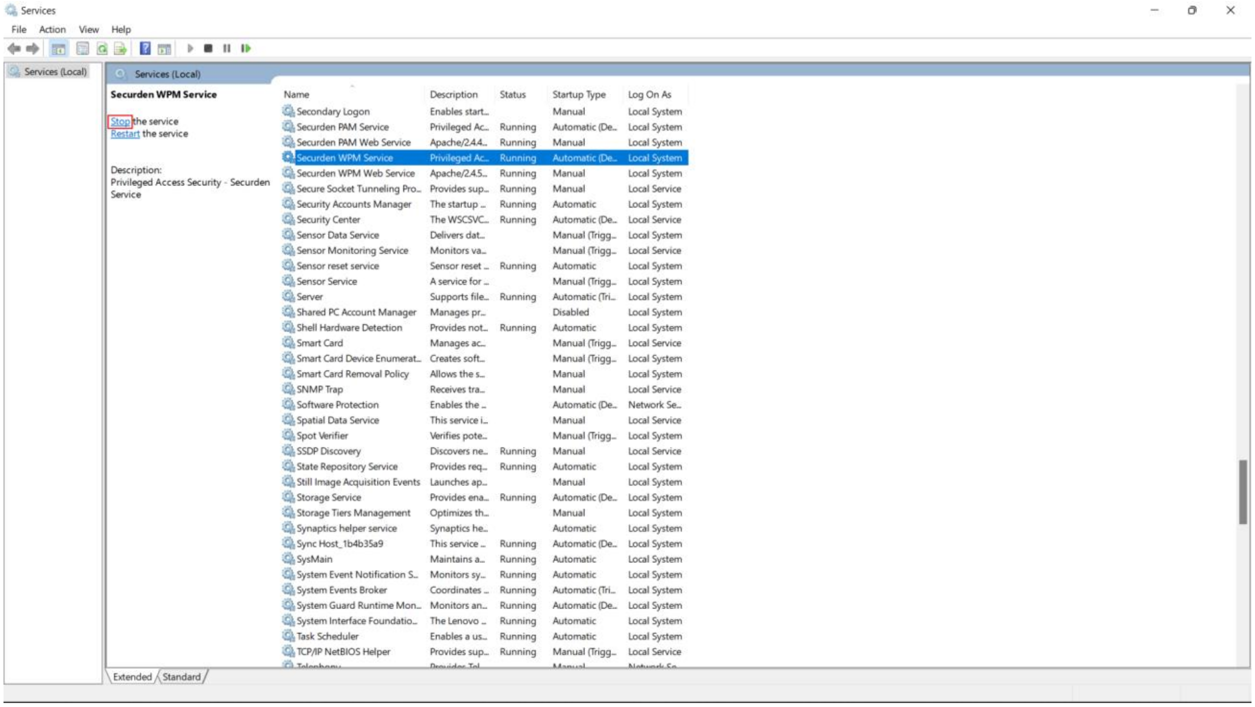
Securden WPM Service

Stop the service
Restart the service

Description:
Privileged Access Security - Securden Service

Name	Description	Status	Startup Type	Log On As
Secondary Logon	Enables start…		Manual	Local System
Securden PAM Service	Privileged Ac…	Running	Automatic (De…	Local System
Securden PAM Web Service	Apache/2.4.4…	Running	Manual	Local System
Securden WPM Service	Privileged Ac…	Running	Automatic (De…	Local System
Securden WPM Web Service	Apache/2.4.5…	Running	Manual	Local System
Secure Socket Tunneling Protocol Service	ıp…	Running	Manual	Local Service
Security Accounts Manager	The startup …	Running	Automatic	Local System
Security Center	The WSCSVC…	Running	Automatic (De…	Local Service
Sensor Data Service	Delivers dat…		Manual (Trigg…	Local System
Sensor Monitoring Service	Monitors va…		Manual (Trigg…	Local Service
Sensor reset service	Sensor reset …	Running	Automatic	Local System
Sensor Service	A service for …		Manual (Trigg…	Local System
Server	Supports file…	Running	Automatic (Tri…	Local System
Shared PC Account Manager	Manages pr…		Disabled	Local System
Shell Hardware Detection	Provides not…	Running	Automatic	Local System
Smart Card	Manages ac…		Manual (Trigg…	Local Service
Smart Card Device Enumerat…	Creates soft…		Manual (Trigg…	Local System
Smart Card Removal Policy	Allows the s…		Manual	Local System
SNMP Trap	Receives tra…		Manual	Local Service
Software Protection	Enables the …		Automatic (De…	Network Se…
Spatial Data Service	This service i…		Manual	Local Service
Spot Verifier	Verifies pote…		Manual (Trigg…	Local System
SSDP Discovery	Discovers ne…	Running	Manual	Local Service
State Repository Service	Provides req…	Running	Automatic	Local System
Still Image Acquisition Events	Launches ap…		Manual	Local System
Storage Service	Provides ena…	Running	Automatic (De…	Local System
Storage Tiers Management	Optimizes th…		Manual	Local System
Synaptics helper service	Synaptics he…		Automatic	Local System
Sync Host_7e78dbe	This service …	Running	Automatic (De…	Local System
SysMain	Maintains a…	Running	Automatic	Local System
System Event Notification S…	Monitors sy…	Running	Automatic	Local System
System Events Broker	Coordinates …	Running	Automatic (Tri…	Local System
System Guard Runtime Mon…	Monitors an…	Running	Automatic (De…	Local System
System Interface Foundatio…	The Lenovo …	Running	Automatic	Local System
Task Scheduler	Enables a us…	Running	Automatic	Local System
TCP/IP NetBIOS Helper	Provides sup…	Running	Manual (Trigg…	Local Service

- Stop **Securden WPM Service** from services.msc.



Securden WPM Service

Stop the service
Restart the service

Description:
Privileged Access Security - Securden Service

Name	Description	Status	Startup Type	Log On As
Secondary Logon	Enables start...		Manual	Local System
Securden PAM Service	Privileged Ac...	Running	Automatic (De...	Local System
Securden PAM Web Service	Apache/2.4.4...	Running	Manual	Local System
Securden WPM Service	Privileged Ac...	Running	Automatic (De...	Local System
Securden WPM Web Service	Apache/2.4.5...	Running	Manual	Local System
Secure Socket Tunneling Pro...	Provides sup...	Running	Manual	Local Service
Security Accounts Manager	The startup ...	Running	Automatic	Local System
Security Center	The WSCSVC...	Running	Automatic (De...	Local Service
Sensor Data Service	Delivers dat...		Manual (Trigg...	Local System
Sensor Monitoring Service	Monitors va...		Manual (Trigg...	Local Service
Sensor reset service	Sensor reset ...	Running	Automatic	Local System
Sensor Service	A service for ...		Manual (Trigg...	Local System
Server	Supports file...	Running	Automatic (Tri...	Local System
Shared PC Account Manager	Manages pr...		Disabled	Local System
Shell Hardware Detection	Provides not...	Running	Automatic	Local System
Smart Card	Manages ac...		Manual (Trigg...	Local Service
Smart Card Device Enumerat...	Creates soft...		Manual (Trigg...	Local System
Smart Card Removal Policy	Allows the s...		Manual	Local System
SNMP Trap	Receives tra...		Manual	Local Service
Software Protection	Enables the ...		Automatic (De...	Network Se...
Spatial Data Service	This service i...		Manual	Local Service
Spot Verifier	Verifies pote...		Manual (Trigg...	Local System
SSDP Discovery	Discovers ne...	Running	Manual	Local Service
State Repository Service	Provides req...	Running	Automatic	Local System
Still Image Acquisition Events	Launches ap...		Manual	Local System
Storage Service	Provides ena...	Running	Automatic (De...	Local System
Storage Tiers Management	Optimizes th...		Manual	Local System
Synaptics helper service	Synaptics he...		Automatic	Local System
Sync Host_1b4b35a9	This service ...	Running	Automatic (De...	Local System
SysMain	Maintains a...	Running	Automatic	Local System
System Event Notification S...	Monitors sy...	Running	Automatic	Local System
System Events Broker	Coordinates ...	Running	Automatic (Tri...	Local System
System Guard Runtime Mon...	Monitors an...	Running	Automatic (De...	Local System
System Interface Foundatio...	The Lenovo ...	Running	Automatic	Local System
Task Scheduler	Enables a us...	Running	Automatic	Local System
TCP/IP NetBIOS Helper	Provides sup...	Running	Manual (Trigg...	Local Service

Note: You do not have to stop **Securden WPM Web Service** explicitly. It is automatically taken care of.

Step 3: How to upgrade the primary server?

Important: Copy the entire Securden installation folder from C:\Program Files\Securden\Windows_Privilege_Manager and keep that as a backup copy. This has to be done on the primary server.

- Ensure that you have taken a copy of the Securden installation folder from C:\Program Files\Securden\Windows_Privilege_Manager
- Ensure that the **Securden WPM Service** is stopped
- Navigate to C:\Program Files\Securden\Windows_Privilege_Manager\bin folder and execute **SecurdenUpgradeManager.exe** and in the upgrade manager GUI, select the downloaded upgrade pack file and click Apply Upgrade Pack button. The upgrade process will be completed in a few minutes.

- Now, start the **Securden WPM Service** from services.msc. You may ignore Securden WPM Web Service, which is automatically taken care of.
- Connect to the web interface **https://localhost:5151** (or) **https://DESKTOP-VP5DD0P:5151**
- Make sure to clear the browser cache.

Your Windows Privilege Manager instance is now up to date and running.

Replace Self-signed Certificate

By default, Securden comes bundled with a self-signed certificate. You can add your own authorized 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.**

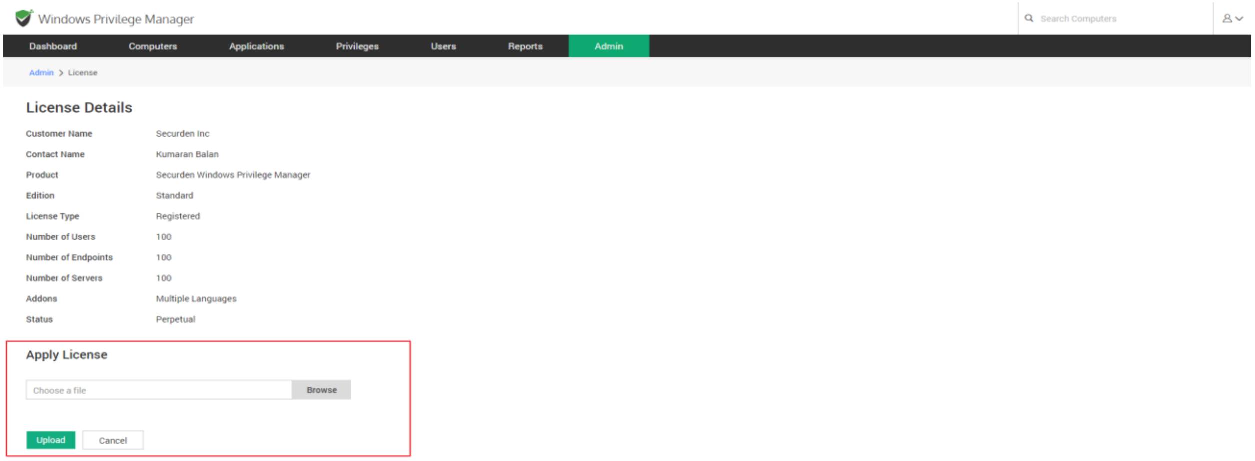
```
openssl pkcs12 -in certificate.pfx -nokeys -out securden-cert.pem
```

Once you execute the above steps, you will get a 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 WPM Service.**

Manage Product License Key

You can apply the Securden license key and get information about the existing license from **Admin >> General >> License** section. The following details are displayed:



License Details

Customer Name	Securden Inc
Contact Name	Kumaran Balan
Product	Securden Windows Privilege Manager
Edition	Standard
License Type	Registered
Number of Users	100
Number of Endpoints	100
Number of Servers	100
Addons	Multiple Languages
Status	Perpetual

To apply a license key, browse and upload the required license file.