



EPM Tutorial

All about local admin rights management



Introduction

This document explains how you can go about discovering, enumerating, and then carrying out our local administrator rights removal for your users. It also covers the pre-requisites necessary for each operation and troubleshooting tips for any issues you may face.

Management of Local Admin Rights

Gaining visibility of admin accounts across the organization helps with compliance as well as enforcing least privilege by eliminating unwanted administrative accounts.

To remove the administrative user accounts on computers you would first need to discover all the local administrator accounts on all the endpoints and servers.

Once discovered, the details of these accounts are populated in EPM. You can view these accounts and then carry out admin privilege removal through multiple available options.

This document is divided into three sections:

A) Discovering local accounts across endpoints

B) Viewing the list of local admin accounts

C) Removing local administrator accounts

A) Discovering local accounts across endpoints

Discovering the local administrator rights across systems in your organization can be done in a couple of ways in Securden EPM. You can implement one or both options based on your requirements.

1) Through the Securden Agent – Primary method for both domain and non-domain computers

You can discover accounts directly through the Securden Agent. You can configure the agent to discover all the accounts present in the endpoint periodically and populate its details in Securden EPM.

2) Through AD - For domain computers only

This can be done by discovering computers through AD and then populating the accounts in them. This requires establishing WMI connectivity with endpoints.

Discover local admin accounts through EPM Agents

To discover devices, capture the list of local administrator accounts on each computer, elevate and delegate privileges, you need to deploy Securden agents on servers and endpoints. The agent takes care of elevating the pre-approved applications and processes for standard users. The agent also allows users to request temporary access to applications/ temporary full admin access.

Pre-requisites:

- You need to enable the following configuration: “What are the entities you would like to enumerate and populate from the Local Admin Group upon installing the Securden agent?” from **Admin >> Customization >> Configurations** and choose to enumerate the entities you require.

Securden Endpoint Privilege Manager

Search Computers

DashboardComputersApplicationsPrivilegesUsersReportsAdmin

Admin > Configurations

policies, and technician access policies will take effect only after approval by another administrator unless there is only one administrator in the system.

Would you like to allow applications to be elevated with domain admin privilege?	Yes Change
Would you like to allow users to raise requests for temporary admin privilege on other endpoints in the network? If you mark 'No' for this, users can raise requests for temporary admin privilege on their machines alone.	Yes Change
Would you like to allow users to raise requests for temporary admin privilege on other servers in the network? If you mark 'No' for this, users can raise requests for temporary admin privilege on their machines alone.	Yes Change
What are the entities you would like to enumerate and populate from the Local Admin Group upon installing the Securden agent?	Users, Groups, and Group Members Change
On clicking the Securden agent tray icon on endpoints, what options would you like to show?	Both Change
Securden agent can fetch the latest changes from the server periodically at a specified interval. Would you like to set that time interval (in minutes) here?	60 Change
Securden agent requires the availability of certain services such as Application Information (Appinfo), Secondary Log-on (seclogon). Would you like to permit Securden agent to enable these services if they remain disabled?	No Change
Do you want to allow users to edit username on the authentication screen shown by Securden agent?	No Change

You need to set a time interval for the Agent to fetch changes from **Admin >> Customization >> Configurations**

“Securden agent can fetch the latest changes from the server periodically at a specified interval. Would you like to set that time interval (in minutes) here?”

Securden Endpoint Privilege Manager

Search Computers

DashboardComputersApplicationsPrivilegesUsersReportsAdmin

Admin > Configurations

Would you like to allow users to raise requests for temporary admin privilege on other endpoints in the network? If you mark 'No' for this, users can raise requests for temporary admin privilege on their machines alone.

Would you like to allow users to raise requests for temporary admin privilege on other servers in the network? If you mark 'No' for this, users can raise requests for temporary admin privilege on their machines alone.

What are the entities you would like to enumerate and populate from the Local Admin Group upon installing the Securden agent?

On clicking the Securden agent tray icon on endpoints, what options would you like to show?

Securden agent can fetch the latest changes from the server periodically at a specified interval. Would you like to set that time interval (in minutes) here?

Securden agent requires the availability of certain services such as Application Information (Appinfo), Secondary Log-on (seclogon). Would you like to permit Securden agent to enable these services if they remain disabled?

Do you want to allow users to edit username on the authentication screen shown by Securden agent?

Do you want to display the option to reinstall/upgrade and uninstall the Securden agent on the computer details page?

Do you want to send a notification email to all approvers when a request is approved or rejected by a designated approver?

The Securden agent will fetch changes from the server based on the time interval mentioned here.

For example: If you have set it to 30 minutes, the agent will query the server every 30 minutes and carry out its tasks accordingly.

Deploy the Securden Agent

Securden agent can be deployed in two ways:

You can deploy Securden agents on endpoints and servers either **manually** or **in bulk using Group Policy Objects**.

Agent for Windows Machines

Navigate to Computers >> Windows Agent to download the agents for 32-bit, 64-bit MSI and install them manually in the remote machine.

The screenshot displays the Securden Endpoint Privilege Manager web interface. The top navigation bar includes 'Dashboard', 'Computers' (selected), 'Applications', 'Privileges', 'Users', 'Reports', and 'Admin'. A search bar for 'Search Computers' and a user profile icon are on the right. The left sidebar shows 'Computers', 'Computer Groups', 'Windows Agent' (highlighted), and 'Linux Agent'. The main content area is titled 'Securden Agent Installation'. It contains a descriptive paragraph about deployment methods, a 'Downloads' section with links for 'SecurdenAgent (MSI)' in 32-bit and 64-bit MSI formats, and an 'Agent Details' section listing version 6.1.7, license limits (100 endpoints/servers), current installation counts (2 endpoints, 1 server), and remaining capacity (98 endpoints, 99 servers). Below this are tabs for 'GPO Instructions' and 'SCCM Instructions'. The 'GPO Instructions' tab is active, showing 'Step By Step installation' with links for 'Deploy Agent in Group level' and 'Deploy Agents on OU level', and a 'VB Script' section with a 'VB Script' link. The URL at the bottom is <https://demo-privilege-manager.securden.com:5151/computer/computer-agent>.

Agent Installation Using GPO

1. Connect to the domain group policy editor (gpmc.msc from Domain Controller)
2. Select all the OUs/Groups that contain the computers (endpoints and servers) in which agents must be installed.
3. Create a GPO for the selected OUs/Groups
4. Add InstallAgent.vbs as a startup script in the GPO with the following parameters:

MSIPATH = Location of the MSI file (accessible to all the endpoints and servers)

SERVER = Name of the host (FQDN / DNS) where Securden server is running

PORT = Securden server port

Example

```
/MSIPATH:"\\SECURDEN-SERVER\\Executable\\SecurdenAgent.msi"  
/SERVER:"SECURDEN-SERVER" /PORT:"5151"
```

5. Securden Agent will be deployed on the computers (endpoints and servers) during the next restart.

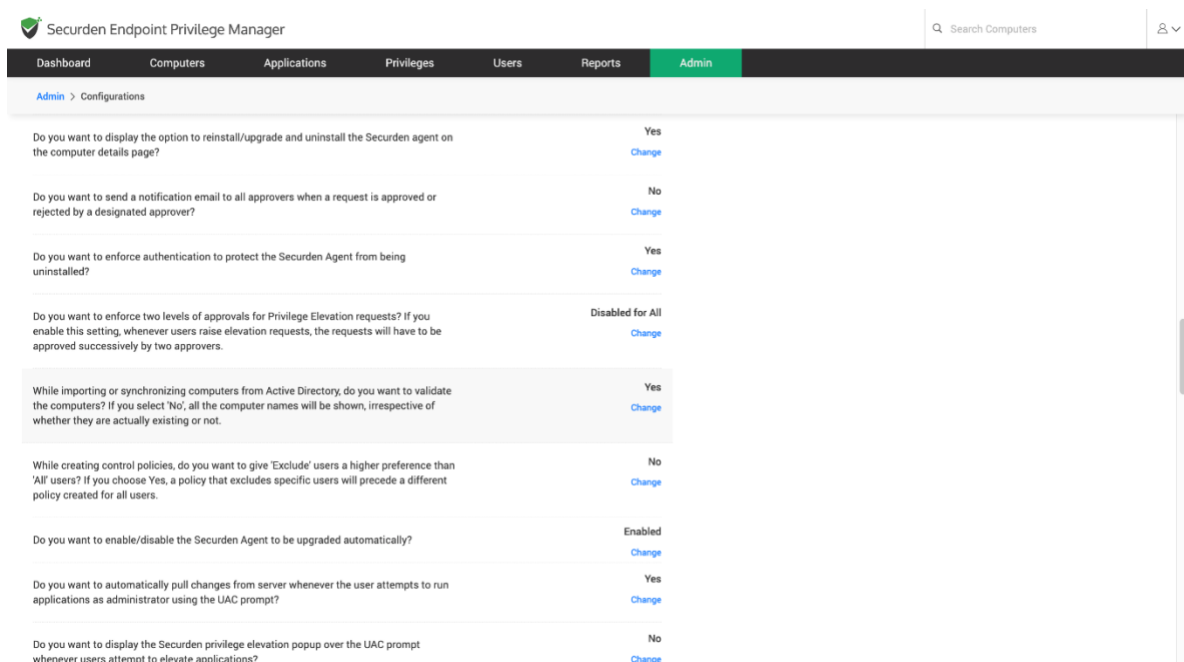
Discover local admin accounts from AD (Active Directory)

You can connect with your active directory, to discover and import all the computers in your domain and the accounts present in them.

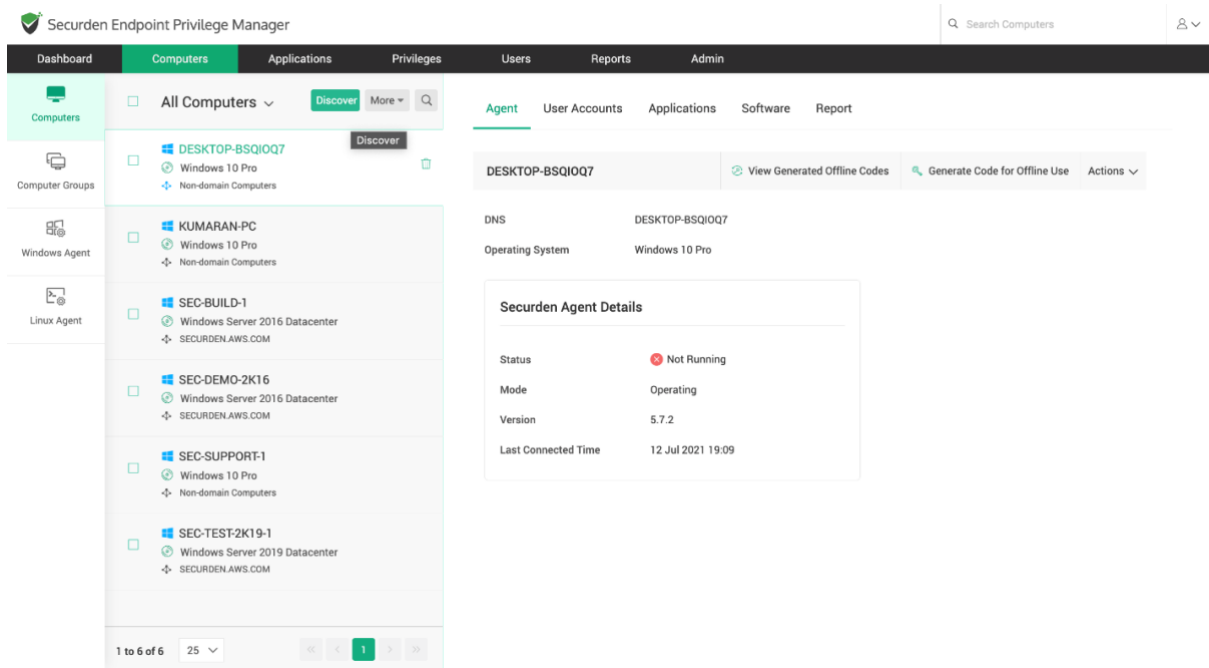
Pre-requisites:

- AD Reachability – The active directory must remain connected to Securden.
- If the users are restricted from logging in from multiple computers, login permission should be allowed from the Securden server.

- WMI Access must be enabled on all machines. You can refer to 'WMI Access Document' to learn how this must be set up.
- You need to keep the following configuration enabled under **Admin >> Customization >> Configurations** - *While importing or synchronizing computers from Active Directory, do you want to validate the computers? If you select 'No', all the computer names will be shown, irrespective of whether they are actually existing or not.*



Once you satisfy the prerequisites, you can continue with the discovery process. To run discovery, navigate to **Accounts >> Computers >> Discover Accounts**.



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

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

Step 1: Establish Connectivity with Active Directory

To establish connectivity, you need to furnish details of the Active Directory domain.

Securden Endpoint Privilege Manager

Search Computers

Dashboard Computers Applications Privileges Users Reports Admin

Computers

Computer Groups

Windows Agent

Linux Agent

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](#)

Next Cancel

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.

Remote Connector

If you want to discover computers from an AD domain in a private remote network, you need to use a Remote Connector on the target network. You can select one from the drop-down or create a new connector.

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.

FQDN/IP Address

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

Connection Mode

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

Supply Administrator Credentials

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

Step 2: Select the required computers and Import.

The screenshot shows the 'Securdent Endpoint Privilege Manager' interface. The left sidebar contains navigation options: Computers, Computer Groups, Windows Agent, and Linux Agent. The main panel is titled 'Discover Computers from AD' and 'Step 2: Discover and Import'. It provides instructions on how to fetch computers and groups from an AD domain. The 'Domain Name' is set to 'SECURDEN.AWS.COM' and the 'Domain IP' is '172.31.1.11'. There are tabs for 'OUs', 'Groups', and 'Computers'. A search bar for 'Search OUs' is present, along with 'Discover' and 'Browse OU Tree and Select' buttons. Below this, there's a section 'Verify the Objects Selected for Discovery' with a 'Clear All' button. A summary box shows 'Computers' with a count of 3. At the bottom, there's an 'Import' button and a 'Cancel' button. A help sidebar on the right explains the step and provides an example of how to use the GUI.

Securdent Endpoint Privilege Manager

Search Computers

Dashboard Computers Applications Privileges Users Reports Admin

Discover Computers from AD

Step 2: Discover and Import

Securdent 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

OUs Groups Computers

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

Search OUs Discover Browse OU Tree and Select

Verify the Objects Selected for Discovery

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

Clear All

Computers x

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

Import Cancel

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'. Securdent will fetch all computers that are part of the OU and Group specified.

Once you click Import, the discovery will run for some time and the summary of accounts/computers imported will be displayed.

The screenshot shows the 'Privileged Account Manager' interface. The left sidebar contains navigation options: Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin. The main panel is titled 'Discovery Process Completed'. It provides a summary of the discovery process, including the number of accounts imported, accounts synchronized, and computers imported. Below this, there's a table showing the details of the discovered accounts. The table has columns for Computer, Account, Status, and Reason. The first row shows a computer named 'SEC-2K16-1' with an account of 'N/A', status of 'Synced', and reason of 'N/A'. A pagination bar at the bottom indicates 'Showing 1 to 21 of 21' and '25'.

Privileged Account Manager

Search Accounts

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Discovery Process Completed

Following is the summary of Accounts discovered by Securdent. The process of fetching dependencies is running in the background. It will take a while to complete and will be automatically populated after completion.

Accounts Imported 16

Accounts Synchronized 1

Computers Imported 0

Showing 1 to 21 of 21 25

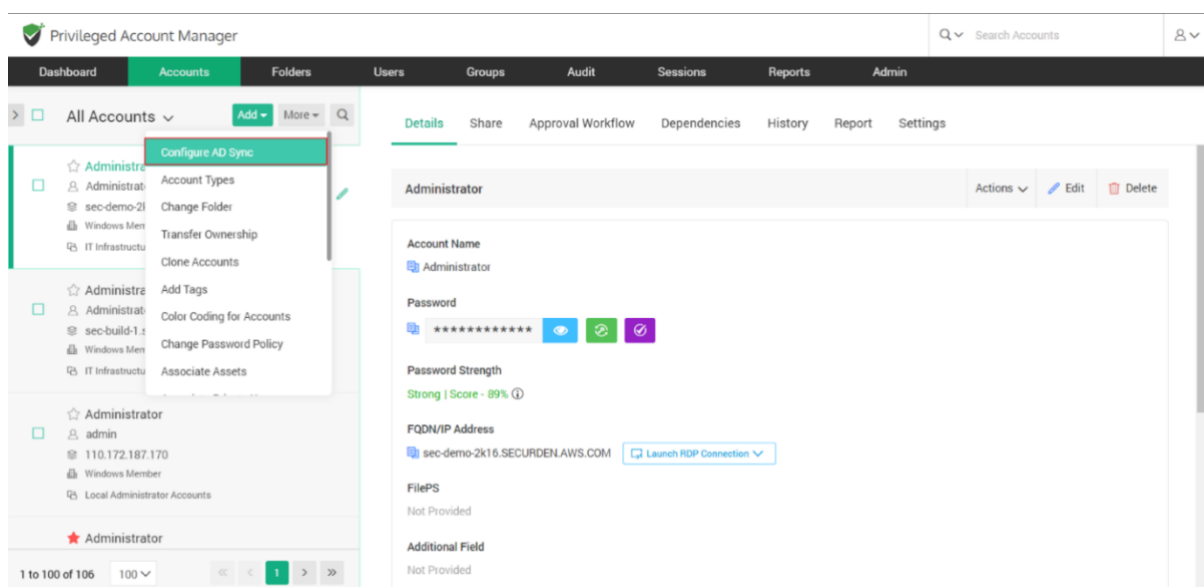
Computer	Account	Status	Reason
SEC-2K16-1	N/A	Synced	N/A

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

Configure Periodic Synchronization of Accounts, Endpoints, and Servers

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

Navigate to **Accounts >> More Actions >> Configure AD Sync** section to perform this step.



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

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Account Groups **Imp...** More

Account Operators
Members can administer domain user an...
SECURDEN.AWS.COM

All Domain Member Computers
Group description not given in AD
SECURDEN.AWS.COM

AllUsers
Group description not given in AD
SECURDEN.AWS.COM

AWSComputer
Group description not given in AD
SECURDEN.AWS.COM

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

1 to 18 of 18 25 < 1 >

Details **Periodically Synchronize Accounts**

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

Define Periodicity

☒ Synchronize Once ☐ Synchronize Periodically

Note: The current time on the server in which Securden runs is 18 Apr 2023 11:42 hrs. The execution time you set here will follow the server time.

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

Save

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

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Account Groups **Imp...** More

Account Operators
Members can administer domain user an...
SECURDEN.AWS.COM

All Domain Member Computers
Group description not given in AD
SECURDEN.AWS.COM

AllUsers
Group description not given in AD
SECURDEN.AWS.COM

AWSComputer
Group description not given in AD
SECURDEN.AWS.COM

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

1 to 18 of 18 25 < 1 >

Details **Periodically Synchronize Accounts**

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

Define Periodicity

☐ Synchronize Once ☒ Synchronize Periodically

Note: The current time on the server in which Securden runs is 18 Apr 2023 11:42 hrs. The execution time you set here will follow the server time.

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

Synchronize accounts every Days

Save

Troubleshooting Tips

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

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

Troubleshooting:

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

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

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

Troubleshooting:

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

Issue: Username or Password Incorrect

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

Troubleshooting Tip:

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

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

B) Viewing the admin accounts discovered

You can view the admin accounts on computers through multiple options in the interface. The Securden Agent and AD synchronization contribute to populating the details of this report.

1) View the administrator accounts report

You can view the list of administrators from the analysis report. Navigate to **Reports >> Standard Reports >> Admin Rights Analysis >> Local Administrator Accounts** to access this report.

The screenshot displays the Securden Endpoint Privilege Manager web interface. The top navigation bar includes 'Dashboard', 'Computers', 'Applications', 'Privileges', 'Users', 'Reports' (highlighted), and 'Admin'. A search bar labeled 'Search Computers' is on the right. Below the navigation bar, there are tabs for 'Standard Reports', 'Concise Reports', and 'Exported Reports'. The 'Standard Reports' tab is active, showing a grid of report cards. The 'Admin Rights Analysis' section is expanded, revealing five report cards: '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 applications elevated or restricted with a control policy and their corresponding privilege status), 'Privilege Elevation Requests' (Find the list of all privilege elevation requests raised and their details), and 'Automatic Approval Policy Activi...' (Find the list of computers configured under...). The 'Local Administrator Accounts' report card is highlighted with a blue border. At the bottom, a URL is visible: <https://demo-privilege-manager.securden.com:5151/report/account-gr...>

You can get the complete list of administrators from this report.

Windows Local Administrator Accounts Report

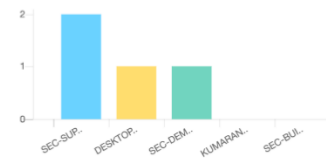
< Back

Report Export: Export Schedule Export Last generated on 04 May 2022 10:58 Download as PDF Preview PDF

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



Search Filter

Showing 1 to 5 of 5 25

Member

Distinguished Name

Domain

Computer

DESKTOP-BSQIQ7 (1 Members)

Work_Administrator

DESKTOP-BSQIQ7

DESKTOP-BSQIQ7

SEC-DEMO-2K16 (2 Members)

Administrator

SEC-DEMO-2K16

SEC-DEMO-2K16

Domain Admins

CN=Domain Admins,CN=Users,DC=SEC-DEMO-2K16,DC=AWS

SEC-DEMO-2K16

SEC-DEMO-2K16

2) View the admin accounts on domain computers from the Computers tab

For domain computers, you can view the admin accounts in them from **Computers >> Select a domain computer >> Local Administrators**.

Computers

All Computers Discover More

Computer Groups

Windows Agent

Linux Agent

DESKTOP-BSQIQ7

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

1 to 6 of 6 25

Agent

Local Administrators

Applications

Software

Report

The list of all users/groups present in the local administrator group of this computer is displayed here. You can even remove them from this GUI itself.

Search Filter

Sync Members

Showing 1 to 2 of 2 25

Member

Distinguished Name

Domain

Administrator

SEC-DEMO-2K16

Remove

Domain Admins

CN=Domain Admins,CN=Users,DC=SECURDEN.AWS.COM

Remove

Showing 1 to 2 of 2 25

1 25

3) View the admin accounts on non-domain computers from the **Computers** tab

For non-domain computers, you can view the admin accounts in them from **Computers >> Select a non-domain computer >> User Accounts**

The screenshot displays the Securden Endpoint Privilege Manager interface. The top navigation bar includes 'Dashboard', 'Computers' (selected), 'Applications', 'Privileges', 'Users', 'Reports', and 'Admin'. A search bar for 'Search Computers' is on the right. The left sidebar shows 'Computers' (selected), 'Computer Groups', 'Windows Agent', and 'Linux Agent'. The main content area is divided into two panes. The left pane shows a list of computers under 'All Computers'. The right pane shows the 'User Accounts' view for a selected computer.

Computers List:

Computer Name	Operating System	Domain
DESKTOP-BSQIQ7	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

User Accounts View:

The list of all local users present in this computer is displayed here.

Full Name	Username	Privilege
Work_Administrator	Work_Administrator	Administrator

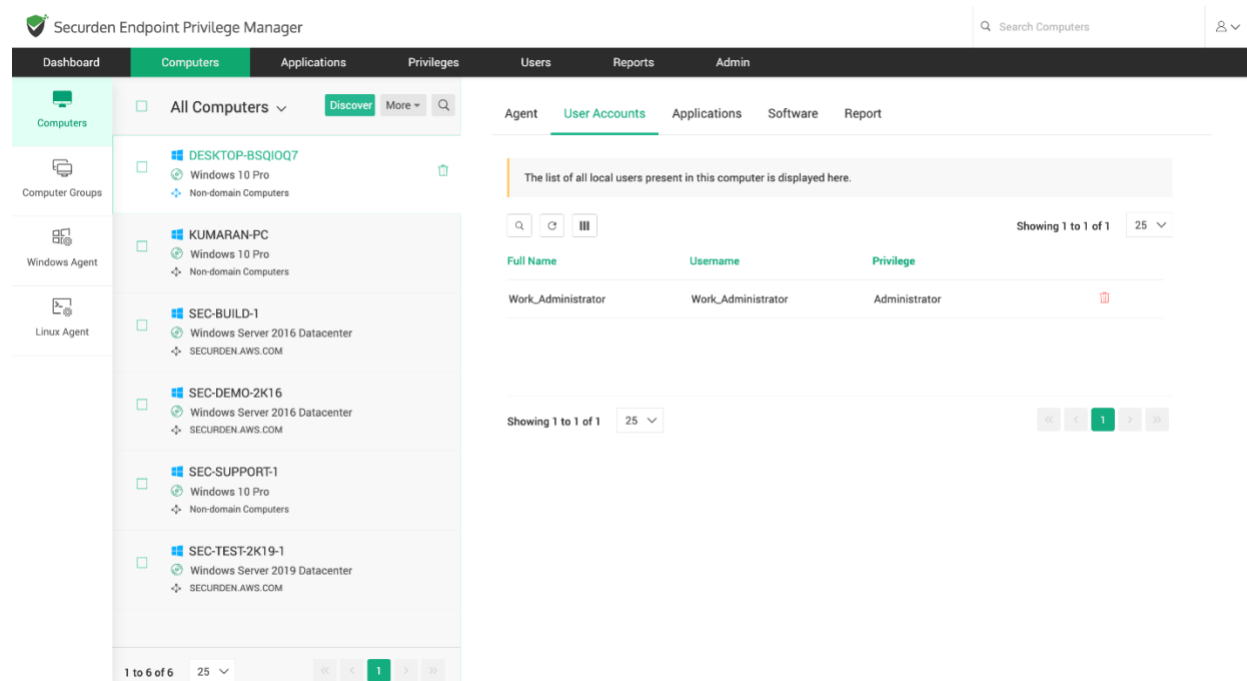
C) Removing the local admin accounts

This can be done in two ways:

- 1) Remove admin privileges on individual computers
- 1) Granularly remove admin privileges

1) Remove admin privileges on individual computers

To remove the administrators from computers individually, you can do it from the **Computers** tab, for both domain and non-domain computers.



The screenshot displays the Securden Endpoint Privilege Manager web interface. The top navigation bar includes 'Dashboard', 'Computers' (selected), 'Applications', 'Privileges', 'Users', 'Reports', and 'Admin'. A search bar for 'Search Computers' is on the right. The left sidebar shows 'Computers' as the active section, with sub-options for 'Computer Groups', 'Windows Agent', and 'Linux Agent'. The main content area is divided into two panes. The left pane lists several computers, including 'DESKTOP-BSQIQQ7', 'KUMARAN-PC', 'SEC-BUILD-1', 'SEC-DEMO-2K16', 'SEC-SUPPORT-1', and 'SEC-TEST-2K19-1'. The right pane shows the 'User Accounts' sub-tab for a selected computer, displaying a message: 'The list of all local users present in this computer is displayed here.' Below this is a table with columns 'Full Name', 'Username', and 'Privilege'. The table contains one entry: 'Work_Administrator' with 'Work_Administrator' as the username and 'Administrator' as the privilege. The interface also includes pagination controls showing 'Showing 1 to 1 of 1' and a dropdown for '25' items per page.

2) Granularly remove admin privileges

You have the option to remove admin privileges granularly. This option is very flexible and can be used to remove admin rights in bulk.

Navigate to **Privileges >> Remove Privileges**

Securden Endpoint Privilege Manager

Dashboard Computers Applications Privileges Users Reports Admin

Application Policies

Remove Privileges

Remove Admin Privilege

Least privilege enforcement requires the removal of local admin privileges of users across servers and endpoints. This GUI allows you to remove local admin privileges in bulk from many users and make them standard users. Additionally, Securden lets you remove all or specific users from a specific group and optionally move them to another group. You can select all or specific computers (except domain controllers) to remove users.

Note: Removing users from the 'Administrators' group revokes their local admin privileges.

1. Users

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

☒ All Users ☐ Include Specific Users/User Groups ☐ Exclude Specific Users/User Groups

☒ Local Users ☒ Domain Users ☐ Domain Groups

2. Computers

Select the computers/computer groups in which the admin rights are to be removed for the users listed in step 1 above.

☒ All Computers ☐ Specific Computers/Computer Groups

☒ Would you like to remove users from a specific group and add them to a different group? Explore the advanced settings (Optional).

Proceed

<https://demo-privilege-manager.securden.com:5151/privilege>

Help

This option is quite flexible and helps you remove the admin rights of any number of users on any number of computers in a single click.

Step 1

Specify users whose local administrator privileges are to be removed.

Option 1: Select All users - and filter between local users, domain users, and domain groups.

Option 2: Individually include/exclude specific users/user groups. This option allows you to add users who haven't been onboarded in Securden.

Step 2

Specify the computers on which admin rights are to be removed for the users listed in step 1.

Option 1: Select all computers. Note: This only includes the computers that have the Securden agent installed on them.

Option 2: Select specific computers/computer groups.

Step 3

Specify the groups from which the selected users are to be removed.

Option 1: Remove from 'Administrators' group - This option allows you to remove the selected users from the local administrators group.

Option 2: Remove from specific group(s) - This option allows you to select a specific privileged group from which the selected users will be removed.

Option 3: None - Select this option if you do not want to remove users from any group.

In addition to removing local admin privileges, this GUI allows you to remove users from any group on devices and add them to a different group.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Remove Admin Privilege

Least privilege enforcement requires the removal of local admin privileges of users across servers and endpoints. This GUI allows you to remove local admin privileges in bulk from many users and make them standard users. Additionally, Securden lets you remove all or specific users from a specific group and optionally move them to another group. You can select all or specific computers (except domain controllers) to remove users.

Note: Removing users from the 'Administrators' group revokes their local admin privileges.

1. Users

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

☒ All Users ☐ Include Specific Users/User Groups ☐ Exclude Specific Users/User Groups

☒ Local Users ☒ Domain Users ☐ Domain Groups

2. Computers

Select the computers/computer groups in which the admin rights are to be removed for the users listed in step 1 above.

☒ All Computers ☐ Specific Computers/Computer Groups

☒ Would you like to remove users from a specific group and add them to a different group? Explore the advanced settings (Optional).

Proceed

Help

This option is quite flexible and helps you remove the admin rights of any number of users on any number of computers in a single click.

Step 1

Specify users whose local administrator privileges are to be removed.

Option 1: Select All users - and filter between local users, domain users, and domain groups.

Option 2: Individually include/exclude specific users/user groups. This option allows you to add users who haven't been onboarded in Securden.

Step 2

Specify the computers on which admin rights are to be removed for the users listed in step 1.

Option 1: Select all computers. Note: This only includes the computers that have the Securden agent installed on them.

Option 2: Select specific computers/computer groups.

Step 3

Specify the groups from which the selected users are to be removed.

Option 1: Remove from 'Administrators' group - This option allows you to remove the selected users from the local administrators group.

Option 2: Remove from specific group(s) - This option allows you to select a specific privileged group from which the selected users will be removed.

Option 3: None - Select this option if you do not want to remove users from any group.

This option is quite flexible and helps you manage the admin rights of any number of users on any number of computers with a single click.

Step 1: Selecting Target Users

You need to specify the users for whom you want to manage privileges. You have two options going forward.

Option 1: Select All users - and filter between local users, domain users, and domain groups.

Option 2: Individually include/exclude specific users/user groups. This option allows you to add users who haven't been onboarded in Securden.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Admin > Remove Admin Rights

Remove Admin Privilege

Least privilege enforcement requires the removal of local admin privileges of users across servers and endpoints. This GUI allows you to remove local admin privileges in bulk from many users and make them standard users. Additionally, Securden lets you remove all or specific users from a specific group and optionally move them to another group. You can select all or specific computers (except domain controllers) to remove users.

Note: Removing users from the 'Administrators' group revokes their local admin privileges.

1. Users

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

☐ All Users ☐ Include Specific Users/User Groups ☒ Exclude Specific Users/User Groups

Enter User/User Group Name

jake matthew Admin Group

2. Computers

Help

This option is quite flexible and helps you remove the admin rights of any number of users on any number of computers in a single click.

Step 1

Specify users whose local administrator privileges are to be removed.

Option 1: Select All users - and filter between local users, domain users, and domain groups.

Option 2: Individually include/exclude specific users/user groups. This option allows you to add users who haven't been onboarded in Securden.

Step 2

Specify the computers on which admin rights are to be removed for the users listed in step 1.

Option 1: Select all computers. Note: This only includes the computers that have the Securden agent installed on them.

Option 2: Select specific computers/computer groups.

Step 3

Specify the groups from which the selected users are to be removed.

Option 1: Remove from 'Administrators' group - This option allows you to remove the selected users from the local administrators group.

Option 2: Remove from specific group(s) - This option allows

Step 2: Selecting Target Devices

Specify the computers on which rights are to be managed for the users selected in step 1. You have two options going forward.

Option 1: Select all computers. Note: This only includes the computers that have the Securden agent installed on them.

Option 2: Select specific computers/computer groups.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Q Search Accounts

Jake X matthew X Admin Group X

2. Computers

Select the computers/computer groups in which the admin rights are to be removed for the users listed in step 1 above.

☐ All Computers ☒ Specific Computers/Computer Groups

Enter Computer/Computer Group Name

W10PF2VASSP X

3. Remove from Group

Select the groups from which the users (specified in step 1 above) are to be removed. If you know of any other groups with excess privileges, select those specific groups too.

☒ Remove from 'Administrators' group ☐ Remove from specific group(s) ☐ None

Option 1: Select the computers from which the Secured agent is 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.
Option 3: None - Select this option if you do not want to add the users removed from group(s) specified in Step 3 to any other group(s).

Step 3: Specify Source Groups

Selected users might be a part of groups with admin privileges in the selected devices. Specify the groups from which the selected users are to be removed. You have three options going forward.

Option 1: Remove from 'Administrators' group - This option allows you to remove the selected users from the local administrators group.

Option 2: Remove from specific group(s) - This option allows you to select a specific privileged group from which the selected users will be removed.

Option 3: None - Select this option if you do not want to remove users from any group.

Privileged Account Manager

Dashboard Accounts Folders Users Groups Audit Sessions Reports Admin

Q Search Accounts

☐ All Computers ☒ Specific Computers/Computer Groups

Enter Computer/Computer Group Name

W10PF2VASSP X

3. Remove from Group

Select the groups from which the users (specified in step 1 above) are to be removed. If you know of any other groups with excess privileges, select those specific groups too.

☐ Remove from 'Administrators' group ☒ Remove from specific group(s) ☐ None

Enter Group Name ☒ Default Group ☐ Custom Group

Administrators X

Option 3: None - Select this option if you do not want to remove users from any group

Step 4
Specify the groups to which users removed in Step 3 are to be added into .
Option 1: Add to the 'Users' group - This option allows you to add the users removed into the default 'Users' group, making them standard users with no admin privilege.
Option 2: Add to a specific group - This option allows you to add the users removed into a specific group/groups of your choice. Select the groups where you wish to add the users.
Option 3: None - Select this option if you do not want to add the users removed from group(s) specified in Step 3 to any other group(s).

4. Add to Group

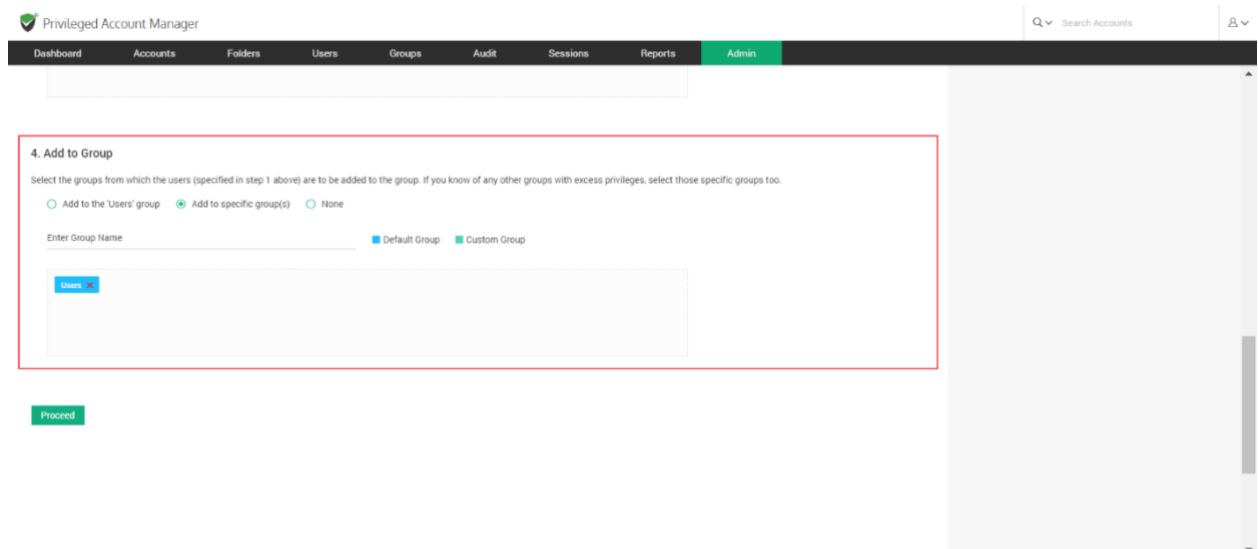
Step 4: Specify Destination Group

Specify the groups to which users removed in Step 3 are to be added into. You have three options going forward.

Option 1: Add to the 'Users' group - This option allows you to add the users removed into the default 'Users' group, making them standard users with no admin privilege.

Option 2: Add to a specific group - This option allows you to add the users removed into a specific group/groups of your choice. Select the groups where you wish to add the users.

Option 3: None - Select this option if you do not want to add the users removed from group(s) specified in Step 3 to any other group(s).



The screenshot displays the 'Privileged Account Manager' web interface. The top navigation bar includes links for Dashboard, Accounts, Folders, Users, Groups, Audit, Sessions, Reports, and Admin (which is currently selected). A search bar for 'Search Accounts' is located on the right. The main content area is titled '4. Add to Group' and contains the following text: 'Select the groups from which the users (specified in step 1 above) are to be added to the group. If you know of any other groups with excess privileges, select those specific groups too.' Below this text are three radio button options: 'Add to the Users' group' (selected), 'Add to specific group(s)', and 'None'. Under the 'Add to specific group(s)' option, there is a section for 'Enter Group Name' with two sub-options: 'Default Group' (selected) and 'Custom Group'. A text input field below these options contains the word 'Users'. At the bottom of the configuration area, there is a green 'Proceed' button.

Once you've selected and specified all the required options, click on **Proceed**.

The selected users will be added/removed for specific/all devices based on your configurations.

Post-Configuration Process

Once the admin privilege removal is configured from the web-interface, the task of carrying out the changes is assigned to the Securden Agent.

The Agent processes the changes and removes the admin accounts as per the configuration.

You have the option to check the status of admin right removal under **Privilege Management Trails** from the **Reports** tab.

Securden Endpoint Privilege Manager


Search Computers

Avatar

DashboardComputersApplicationsPrivilegesUsersReportsAdmin


Standard ReportsConcise ReportsExported Reports

Activity Reports



Privilege Management Trails


Find all privilege management related activities performed.




User Activity

Find the activities performed by users.


Admin Rights Analysis



Local Administrator Accounts




Application Elevation Activity



Application Privilege

Find the list of applications elevated or restricted with a control policy and their



Privilege Elevation Requests

Find the list of all privilege elevation requests raised and their details

<https://demo-privilege-manager.securden.com:5151/report/privilege-activity>