



Multi-Site Deployment Guide

EPP V 8.3

www.seqrite.com

Copyright Information

Copyright © 2008–2024 Quick Heal Technologies Ltd. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Quick Heal Technologies Limited, Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India.

Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies Ltd. is liable to legal prosecution.

Trademarks

Seqrite and DNAScan are registered trademarks of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

License Terms

Installation and usage of Seqrite Endpoint Protection is subject to user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit <http://www.seqrite.com/eula> and check the End-User License Control Centrement for your product.

Contents

- 1. Overview 2
- 2. Audience 2
- 3. System Requirements 2
- 4. Glossary 3
- 5. Introduction to Multi-Site Deployment 4
 - Benefits of Multi-Site Deployment 4
 - Control Center Architecture 4
- 6. Control Center 5
 - Control Center Installation Steps 5
- 7. Site Server 14
 - SSR Installation Steps 14
- 8. Site Server Onboarding from the SSR Console 19
 - Onboarding Steps after Configuring SSR 20
- 9. Site Server Approval/Rejection Steps from the Control Center Console 22
- 10. EPP Control Center Console 26
 - Dashboard 26
 - User 30
 - Site Server 35
 - Deployment 37
 - Policies 38
 - Configurations 40
 - Reports 42
 - Admin 43
- 11. Support 47
- 12. Troubleshoot 48
 - Missing Requirements 48
 - Uninstall Components 49
 - Incorrect Initial Actions 49

Overview

This document serves as a guide for deploying EPP servers across multiple organizational sites, enabling centralized endpoint management via a Central Console/GUI. Subsequent sections detail the installation procedures for both the Endpoint Protection Control Center (Control Center) and site servers. Furthermore, it provides comprehensive insights into the options and functionalities accessible within the console dashboard.

Audience

This guide is useful for the Secrite support or customer/partner system administrators who would be carrying out the deployment.

System Requirements

Multi-Site deployment is possible only for **On Prem** environment. Here are the prerequisites:

Control Center Deployment Prerequisites:

- OS: Ubuntu 22.04
- RAM: Min 6 GB, Recommended 8 GB
- Separate installer for the Aggregator and Site servers

Note that installation process will not proceed if any additional components, such as Java, Nginx, WildFly, Kafka, MongoDB, Redis, or Curl are installed on the server machine.

Site Server Deployment Prerequisites:

- OS: Ubuntu 22.04 (supported on server as well as desktop image)
- Available Disk Space: 60 GBs or above
- Available RAM: 8 GBs or above
- Processor: 4 Core (x86-64), 2.60GHz or above
- Separate installer each for Aggregator and Site servers

Glossary

Term	Description
EPP	Endpoint Protection
Endpoint	A client agent system
Control Center	Control Center
SSR	Site Server
DLP	Data Loss Prevention
AD	Active Directory

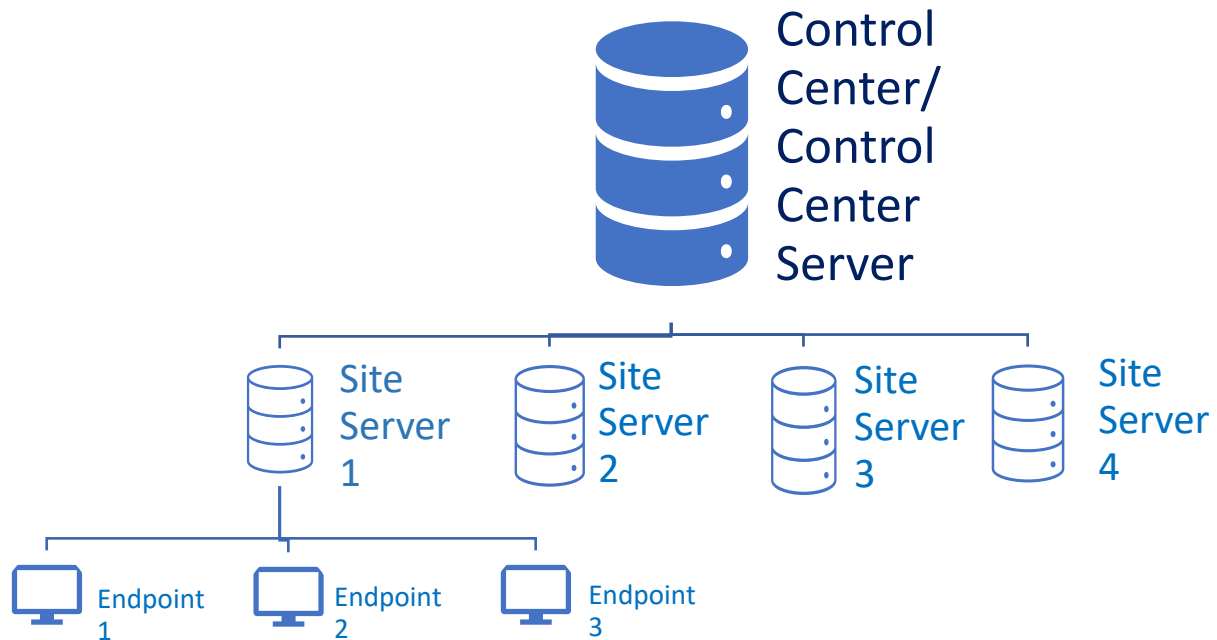
Introduction to Multi-Site Deployment

Multi-site deployment enables organizations to strategically position servers across various geographic locations while maintaining centralized management capabilities through a unified control console.

Benefits of Multi-Site Deployment

Utilizing Site Servers facilitates efficient management of a considerable quantity of endpoints. Particularly beneficial for distributed networks spanning various geographic regions, each location can host a dedicated Site Server responsible for overseeing all endpoints within its domain. The collective network of Site Servers is centrally managed by an Control Center.

Control Center Architecture



Control Center

The Control Center, acting as the EPP server, serves as the centralized hub capable of overseeing all Site Servers. Each Site Server, in turn, is responsible for managing local clients (endpoints) deployed across diverse geographical locations.

Control Center Installation Steps

Important to Note:

- The Control Center exclusively deploys server-specific components. The Aggregator installer does not include the client build, and therefore, it does not install any endpoint.
- It is recommended to install AV first on any system where Control Center will be installed. If you install the Control Center before installing AV, ensure AV is installed afterward to avoid receiving an alert.

To begin the installation of Seqrite Endpoint Protection Control Center, follow these steps:

1. Download the Control Center build.
2. Open the terminal on your Ubuntu endpoint and log in as a root user.

```
qhuser@qhuser-virtual-machine:~/Downloads$ su root
Password:
root@qhuser-virtual-machine:/home/qhuser/Downloads#
```

3. Execute the installer by typing the following command from the location where build is downloaded:

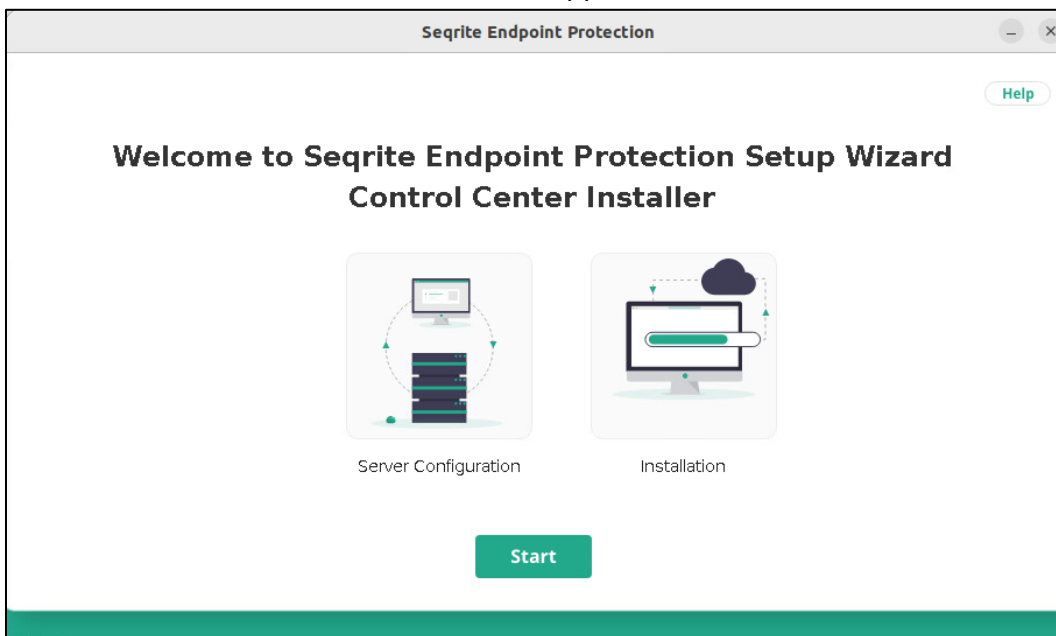
bash Seqrite_EndPoint_Security_8_3.sh

```
qhuser@qhuser-virtual-machine:~/Downloads$ su root
Password:
root@qhuser-virtual-machine:/home/qhuser/Downloads# bash Seqrite_EndPoint_Security_8_3.sh
Unpacking JRE ...
Starting Installer ...
```

It prepares for the setup wizard to start.

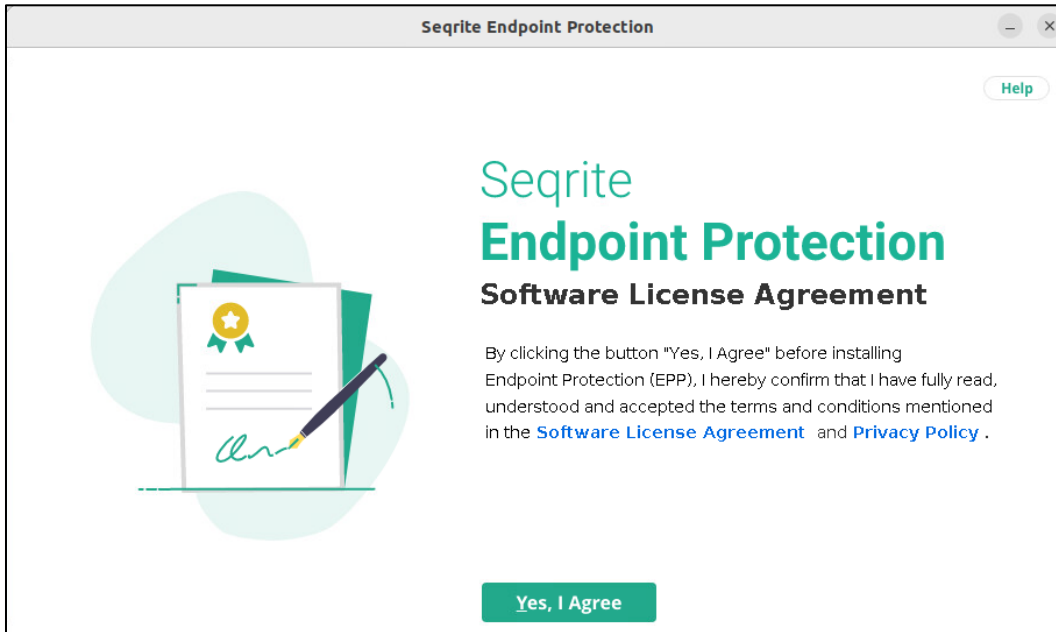


4. The Control Center Installer Wizard screen appears. Click **Start**.



5. The license Control Centereement appears. Read the License Control Centereement carefully. Installation and usage of Seqrite Endpoint Protection is subject to your formal acceptance of the Seqrite Endpoint Protection end-user license terms and conditions.

Press the **R** key to read more. Click **Yes, I Control Centree** on the Seqrite Endpoint Protection license Control Centerement screen.



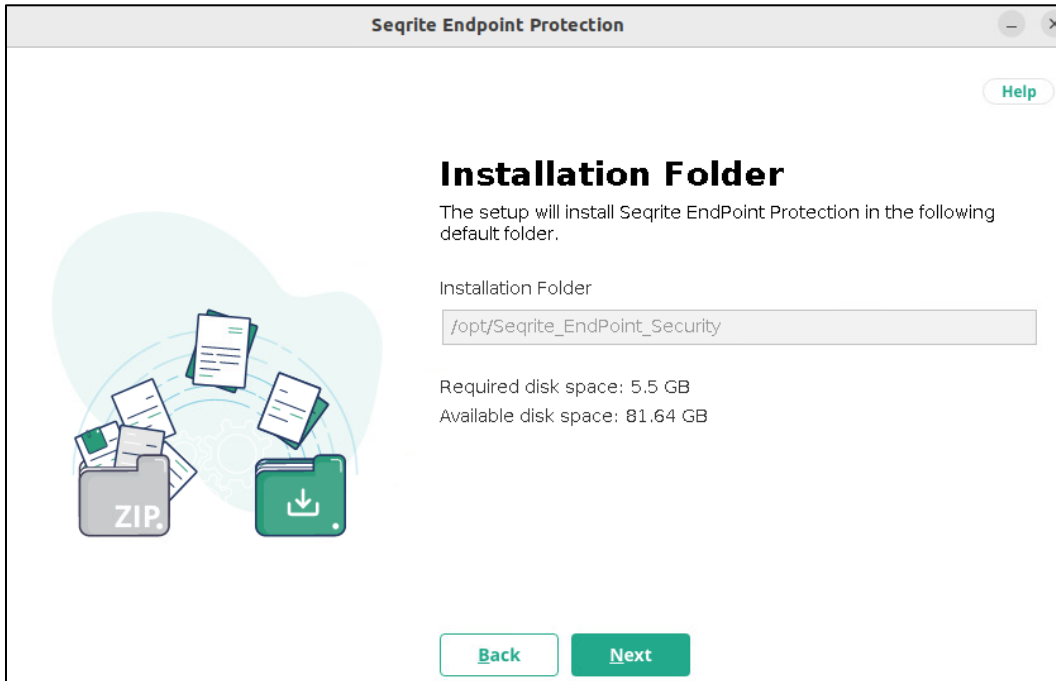
6. The **Customer Information** screen appears. Ensure that all the mandatory fields are populated with relevant information. Click **Next**.

The screenshot shows a window titled "Seqrite Endpoint Protection" with a "Help" button in the top right. The main content is titled "Customer Information" and includes the instruction: "Enter the following information. This information is used for Activation." The form contains the following fields:

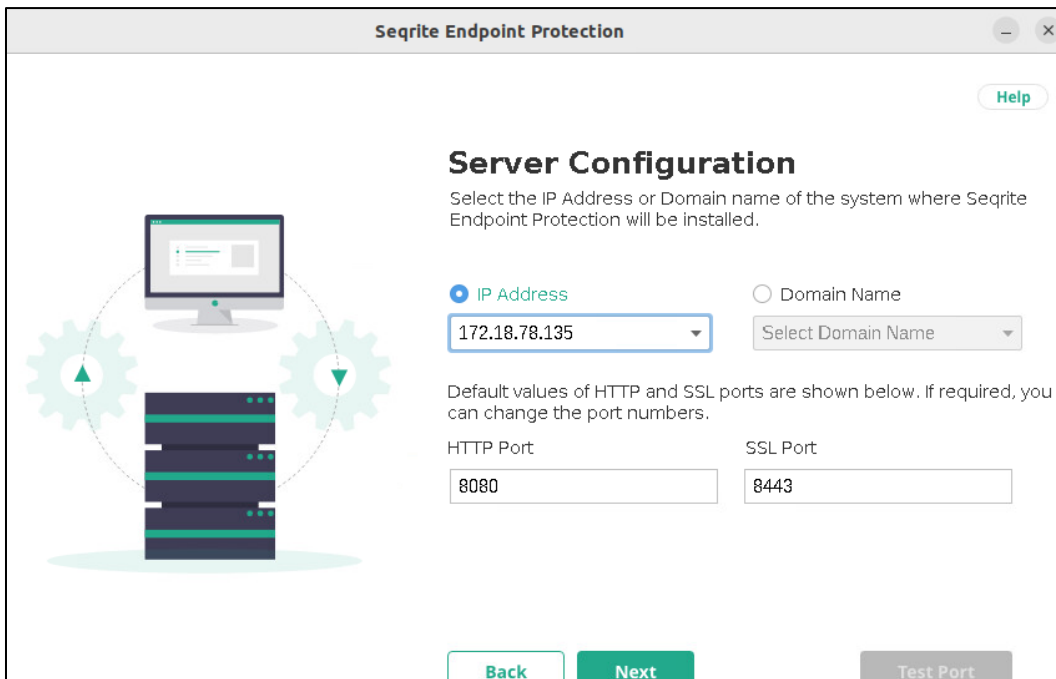
First Name	Last Name	Company Name	
<input type="text" value="AGR"/>	<input type="text" value="Server"/>	<input type="text" value="ABC"/>	
Administrator Email Address	Mobile Number	Phone Number (Optional)	
<input type="text" value="AGR@yopmail.com"/>	+91 In... <input type="text" value="8767817391"/>	<input type="text" value="Enter phone number"/>	
Address (Optional)	Country	State (Optional)	City (Optional)
<input type="text" value="Enter full address"/>	India	Maharashtra	Select

At the bottom, there are two buttons: "Back" and "Next".

7. The **Installation Folder** screen displays where the installation location is shown. Click **Next**.



8. Enter the **IP Address** of the machine on which you are installing the Control Center. OR enter the **Domain Name** if you intend to execute the installation using a specific domain name.



9. If you need, you can provide the proxy server details for additional security. This is an optional step.

10. The **Authentication** screen appears. Provide the details here. Make a note of these details as you need the same credentials to log in to the console. Click **Next** to proceed.

Seqrite Endpoint Protection

Help

Authentication

Prevent unauthorized access to Seqrite Endpoint Protection

Provide Administrator credentials here. To access EPP console, use these credentials after installation.

Administrator Email Address

AGR@yopmail.com

Password

Confirm Password

Back Next

11. Verify the details on the **Summary** screen.

Seqrite Endpoint Protection

Help

Summary

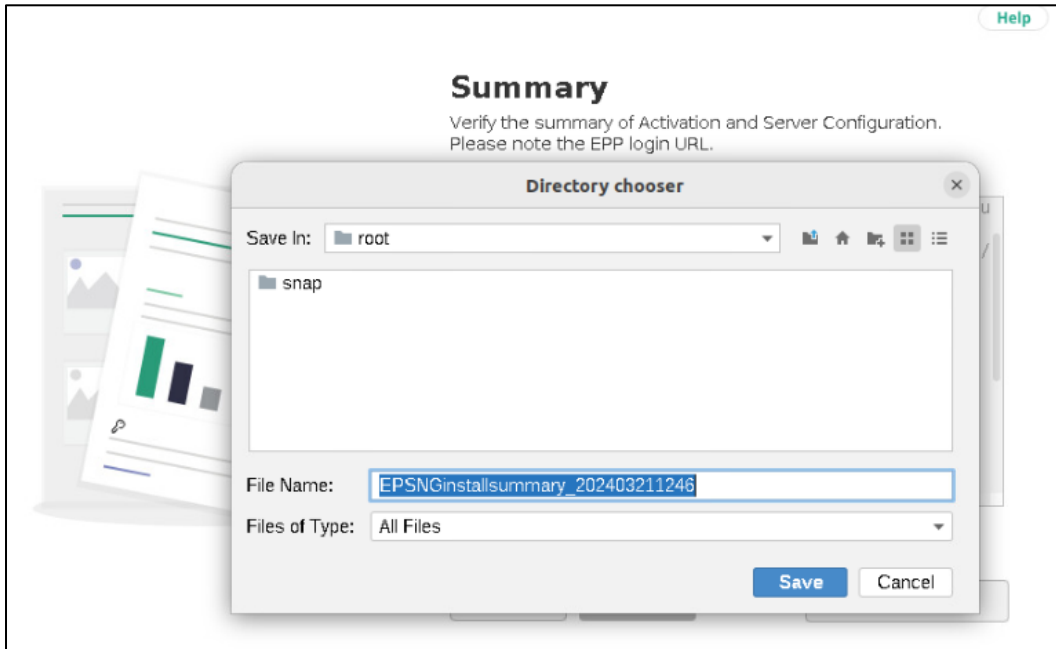
Verify the summary of Activation and Server Configuration. Please note the EPP login URL.

Installation Path	:/opt/Seqrite_EndPoint_Secu
Login URL	:https://172.18.78.135/eps/
Customer First Name	:AGR
Customer Last Name	:Server
Customer Company Name	:ABC
Customer Mobile Number	:+91-8767817391
Country	:India

Back Next Save Summary

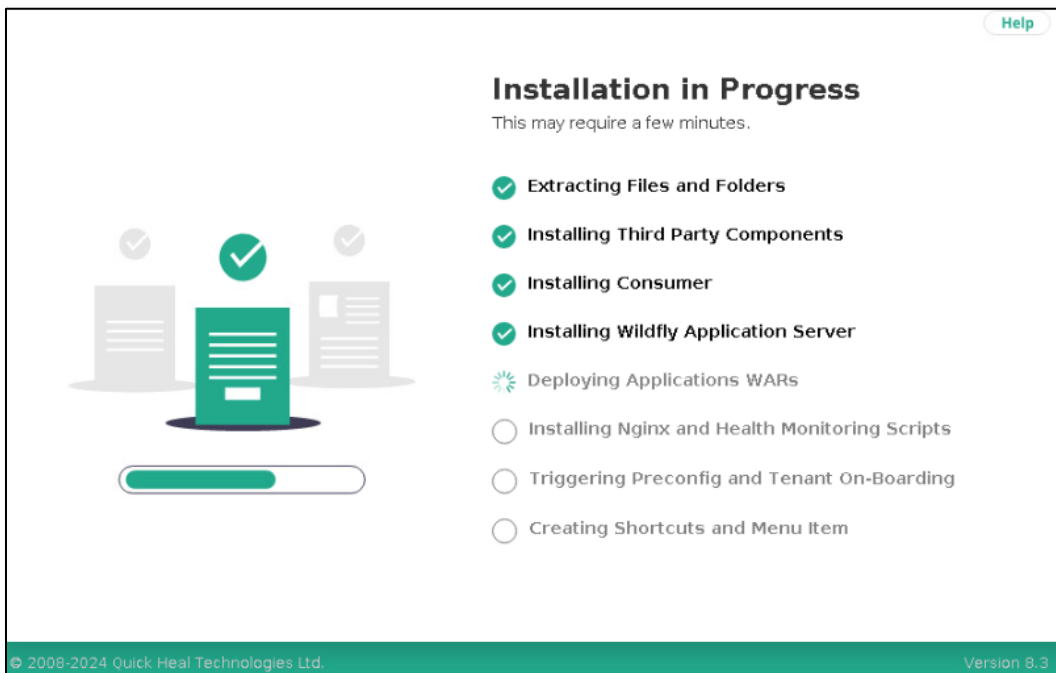
© 2008-2024 Quick Heal Technologies Ltd. Version 8.3

You can save the details as a text file by clicking **Save Summary**. Click **Save**. The .txt file gets saved.

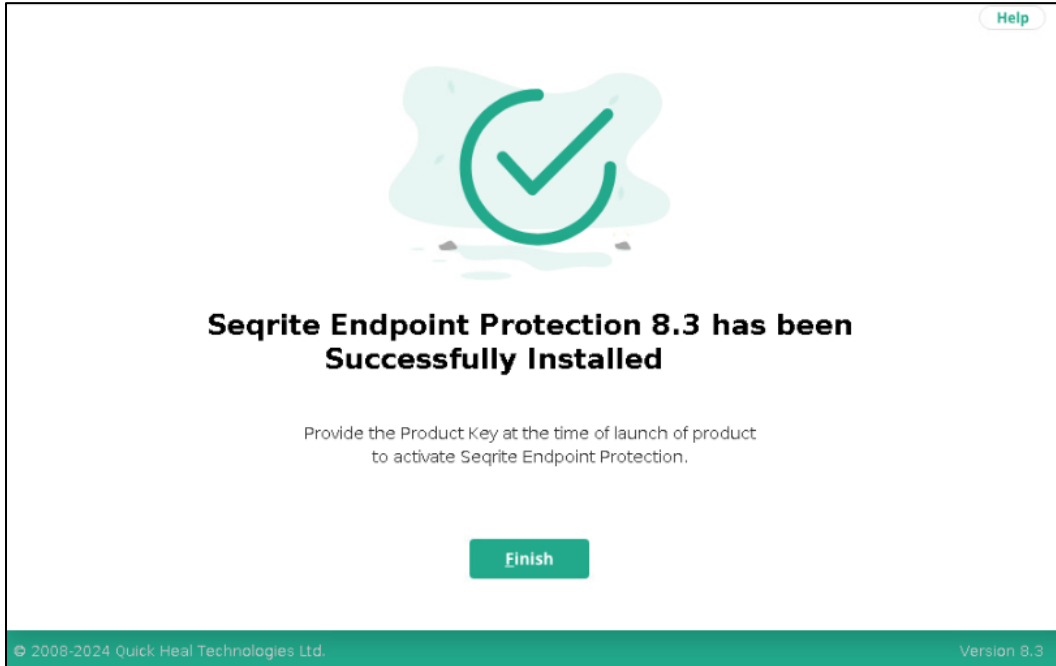


12. Click **Next**. The installation process starts.

It might take a few minutes to complete the installation.



13. Once all the components are ticked, the completion screen appears. Click **Finish**.



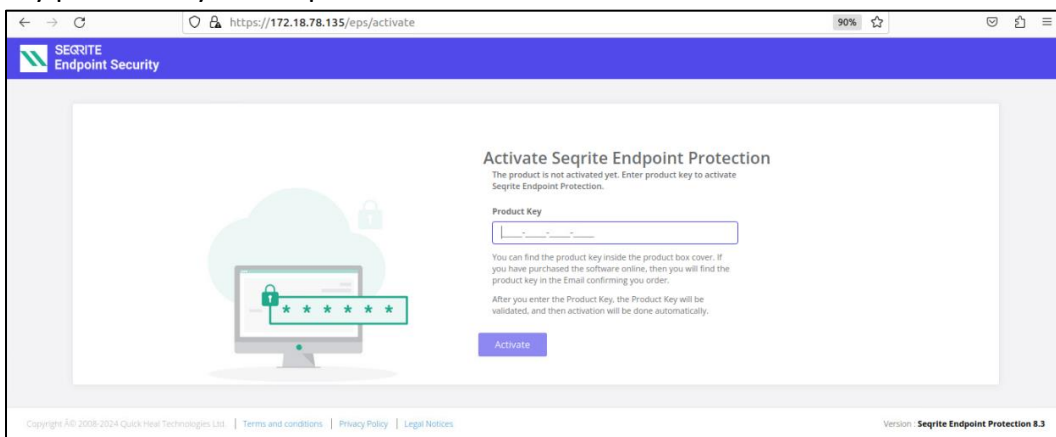
Now you need to activate the EPP central console to be able to manage/onboard the site servers.

Steps to Activate the Console

1. For the console link, you can either use the ip address or the host name of your server machine.

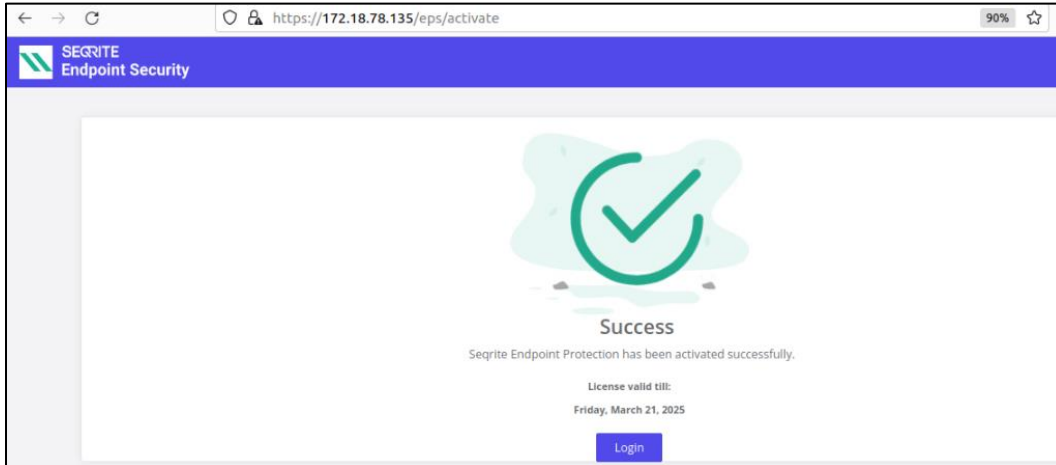
For example, if you used the ip address while configuring the server, the link would be: <https://<ipaddress>/eps/activate>.

In the following example, it is: <https://172.18.78.135/eps/activate>. Enter the product key provided by the Seqrite team. Click **Activate**. OR

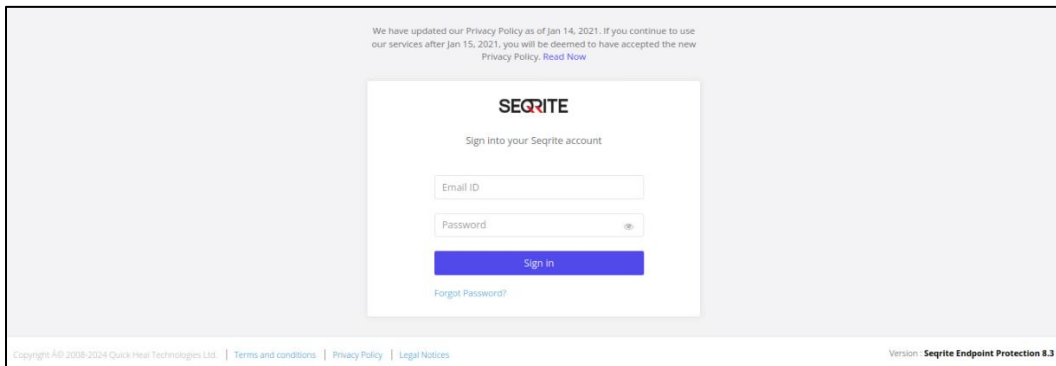


If you used the hostname while configuring the server, activate it using <https://<hostname>/eps/activate>. Enter the product key provided by the Seqrite team. Click **Activate**.

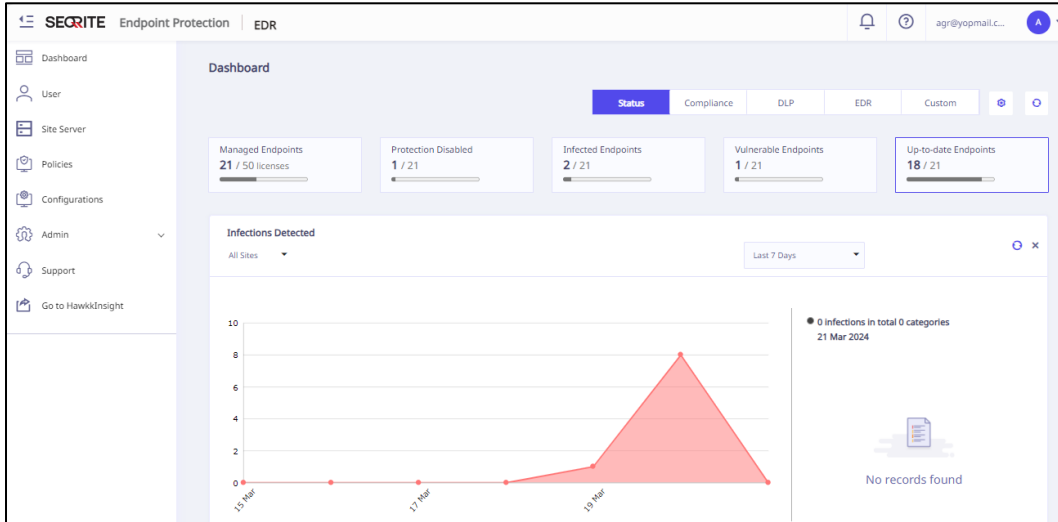
2. A success message appears. Click **Login**.



- 3.
4. It redirects you to the console login page. Enter the details you provided during registration. Click **Sign In**.



It takes you to the dashboard. For more details, see [EPP Control Center Console Dashboard](#).



Site Server

A Site Server can be installed at different locations. It manages local clients, and it reports important statistics to the Control Center Server.

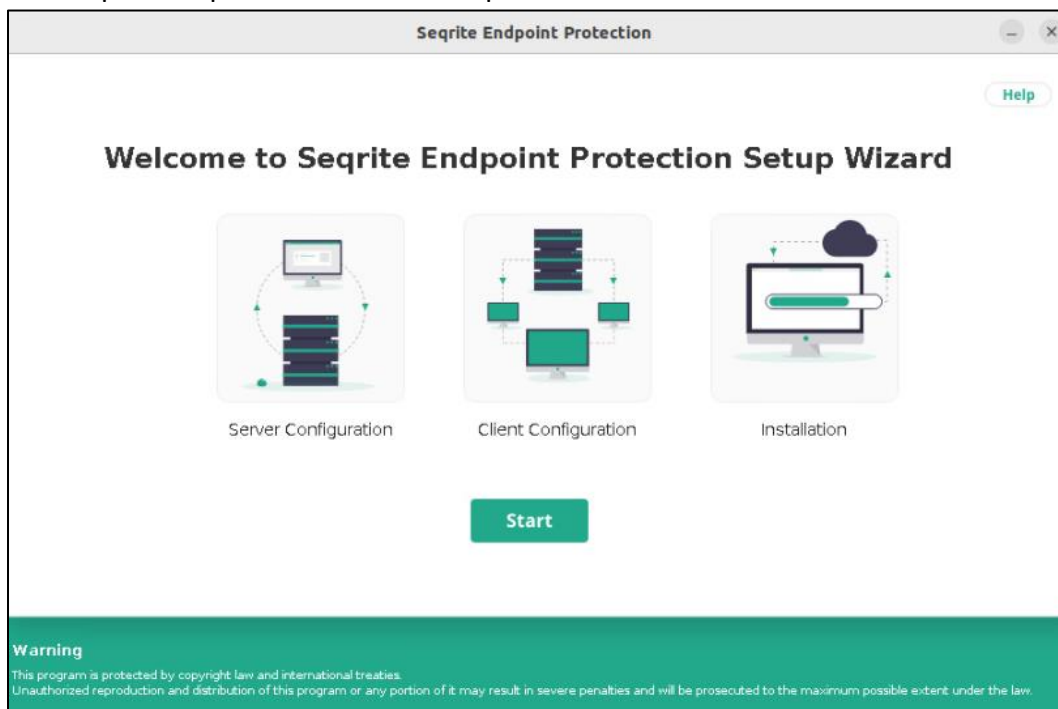
SSR Installation Steps.

To begin the installation of Seqrite Endpoint Protection Site Server, follow these steps:

1. Open the terminal on your Ubuntu endpoint and log in as a root user.
2. Execute the installer by typing the following command:

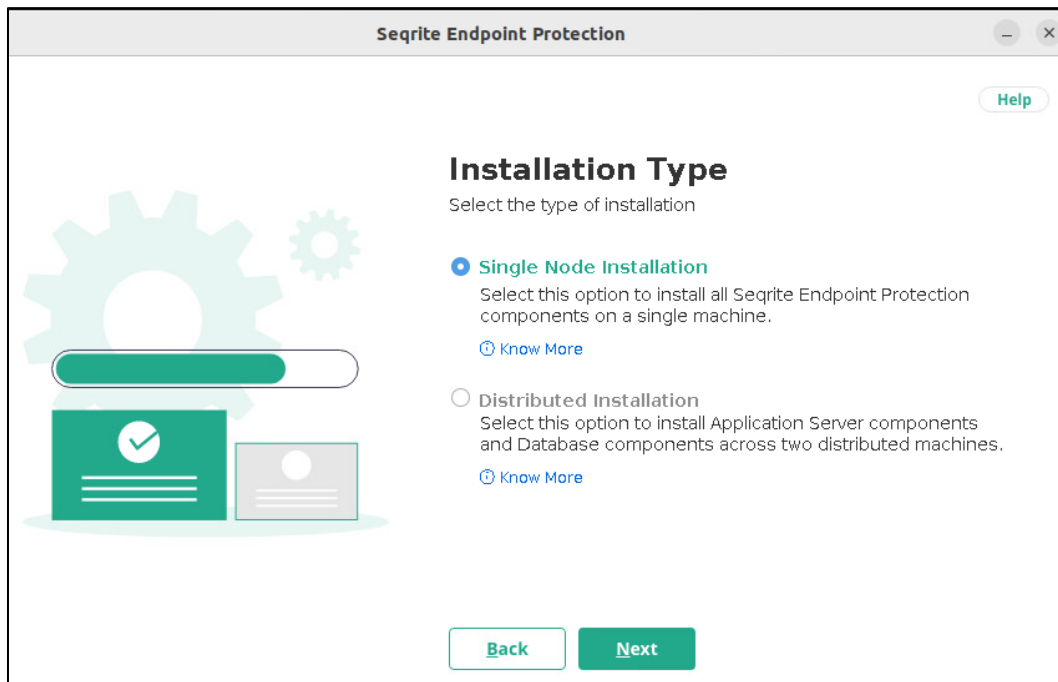
```
bash Seqrite_EndPoint_Security_8_3.sh -c
```

The Seqrite Endpoint Protection setup wizard starts.



3. Click **Start**.
4. The license Control Centereement appears. Read the License Control Centereement carefully. Installation and usage of Seqrite Endpoint Protection is subject to your formal acceptance of the Seqrite Endpoint Protection end-user license terms and conditions. Press the **R** key to read more. Click **Yes, I Control Centeree** to continue.

5. The Installation Type screen appears.



- Single Node Installation – Type **S** and hit [Enter].
- Distributed Installation – Type **D** and hit [Enter].

6. The Customer Information screen appears. Enter the details step by step. This information is important to activate Seqrite EPP on your machine.

The setup installs Seqrite Endpoint Protection in the default folder. The folder path appears. Available and required disk space is calculated automatically and the figures are displayed.

7. To continue, hit [Enter]. Ensure that there is the required space available on the disk.
8. The Server Configuration screen appears. Here for Private IP or Public or FQDN installation, select IP Address or Domain Name from the list. To continue, hit [Enter].

Note: Default values of HTTP Port and SSL Port appear. To continue with default values, hit [Enter]. Else type the port values and hit [Enter]. The port connections are tested, and port numbers are validated. This port number serves as a listening port for the server. With Seqrite Endpoint Protection server address, you can launch the console.

9. If you select Distributed Installation on the **Installation Type** screen, then only Distributed Server Configuration screen appears. Else, the Proxy Settings screen appears, go to next step.
- a. Type IP address or hostname of the Distributed Server and hit [Enter].
 - b. Type Username and hit [Enter].

- c. Type Password and hit [Enter]. You cannot view the typed password.
10. The Proxy Settings screen appears. If you are using a proxy server to connect to the Internet, type 1 and hit [Enter].

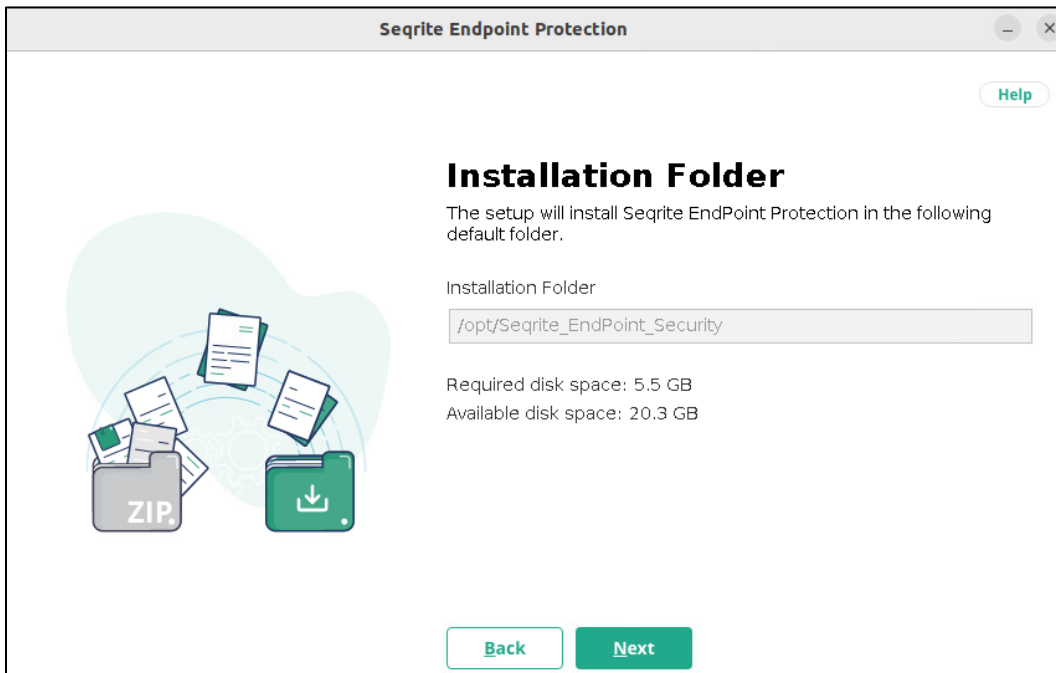
If you want to continue without enabling Proxy Settings, type 2 and hit [Enter]. The Proxy Setting information is used by EPP server for internet connectivity, activation, and for downloading updates. To enable and configure proxy settings:

- a. Type the IP address of the proxy server or domain name (For example, proxy.yourcompany.com) and hit [Enter].
- b. Type the port number of the proxy server (For example: 80) and hit [Enter].
- c. Type 1 to authenticate to connect through the proxy server. Type 2 to continue without authentication.
- d. Type Username.

The success message appears if the connection to the proxy server is successful.

11. The Installation Folder screen appears. Seqrite client is installed on the endpoint as per the path specified in this screen.

Required disk space and available disk space is shown.



12. To continue hit [Enter].
13. The Authentication screen appears. Create Seqrite Endpoint Protection administrator password to access the Web console and endpoint password to access the endpoint

settings at the endpoint side.

Seqrite Endpoint Protection

Help

Authentication

Prevent unauthorized access to Seqrite Endpoint Protection

Provide Administrator credentials here. To access EPP console, use these credentials after installation.

Administrator Email Address

SSR@yopmail.com

Password Confirm Password

You can provide Client password here. To access EPP Client, use this password after installation. (Optional)

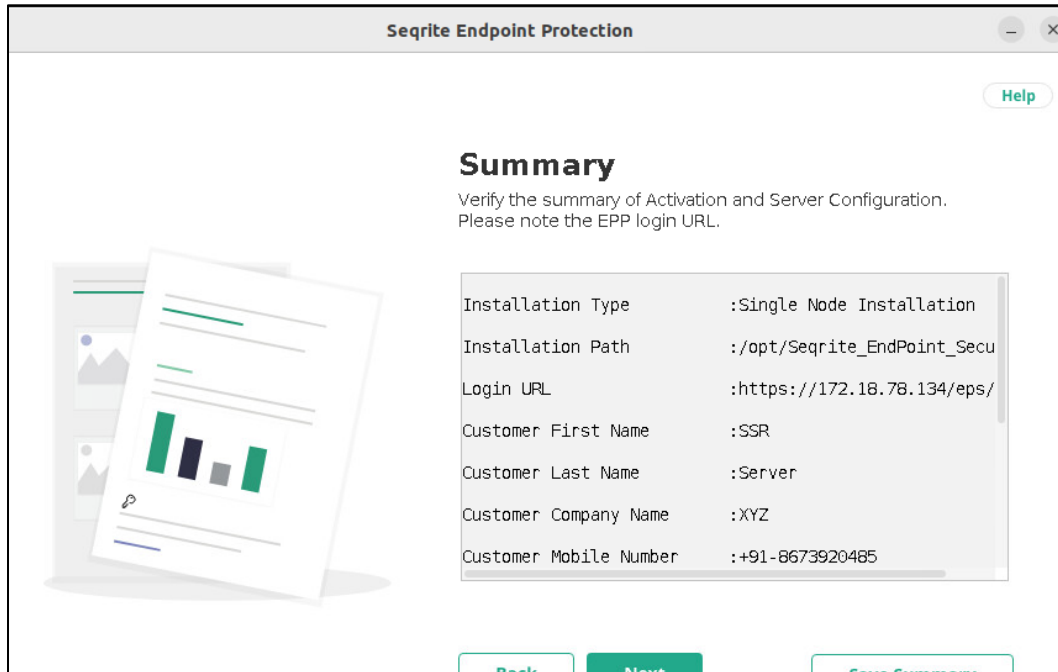
Password Confirm Password

Password Confirm Password

Back Next

- Type in Administrator Email Address and hit [Enter] or you can continue with the Email address appeared. To continue, hit [Enter].
- Type in your password and hit [Enter]. Type password again to confirm the password and hit [Enter]. You cannot view the typed password.
- You can provide client credentials. This is optional. Type 1 to specify client credentials and hit [Enter]. Type in client password and hit [Enter]. Type client password again to confirm the password and hit [Enter]. You cannot view the typed password.
- This helps prevent unauthorized users from accessing the Web console and make changes in your settings or remove the endpoints.
- Type 2 to continue without providing client credentials and hit [Enter].

14. The installation summary screen appears. Activation and Server Configuration data is displayed. Ensure to note the **EPP Login URL**.

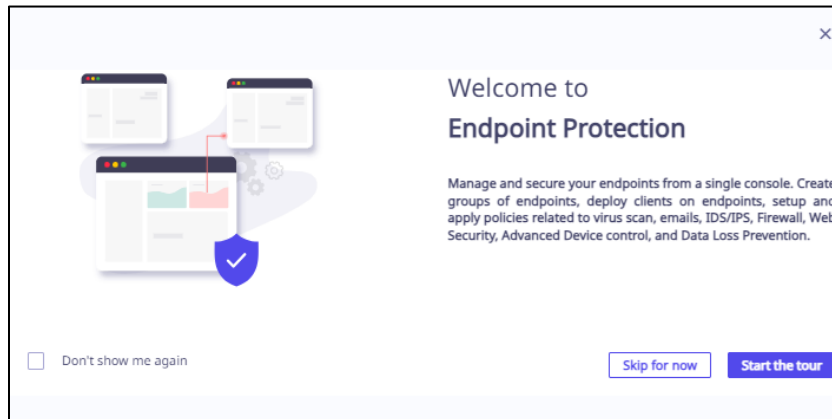


- a. Click **Save Summary** to save summary file at path/opt and hit [Enter].
 - b. Click **Next** to continue without saving and hit [Enter].
15. Once the installation process is complete, the success screen appears.

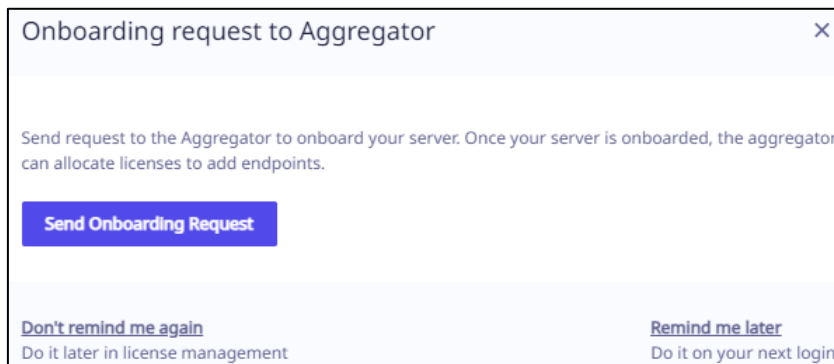
Note: Re-installation of EPP Site Server. In Minimal/CLI Mode for UBUNTU 22.04 LTS after uninstalling EPP 8.1, you cannot install EPP 8.2 server with the same product key.

Site Server Onboarding from the SSR Console

As soon as you log in to the SSR console, an EPP console tour window appears. If you start the tour, at the end of it, a pop up appears asking you to onboard the SSR to Control Center.



Even if you skip the tour, the same pop up appears asking you to onboard the SSR to Control



Center.

- Click the **Send Onboarding Request** button to go to the Configuration/Onboard to Aggregator page.
- Click the **Don't remind me again** button to close the dialog box and stop these alerts from appearing.
- Click the **Remind me later** button to close the dialog box. It appears again on your next login.
- Click the cancel icon (**X**) to close the dialog box. It appears again on your next login.

Onboarding Steps after Configuring SSR

Follow these steps to onboard the site server from the site server console.

1. On the SSR console, go to **Configurations > Onboarding to Control Center**.
2. Enter the **Aggregator Host Name/IP Address** of the Control Center to which this site server needs to be connected.
3. Enter the **Aggregator Port** number.
4. Click **Send Onboarding Request** to continue.

The request goes to the Control Center. An alert is displayed on the Control Center dashboard requesting to approve the onboarding request. Wait for the approval. Once approved, then the SSR details are reflected in the [site server](#) list on the Control Center console and on the **Configurations > Onboarding to Aggregator** page of the SSR.

While the request is sent from the SSR, it shows Pending for Approval with the following details on the **Onboarding to Aggregator** page of the SSR console.

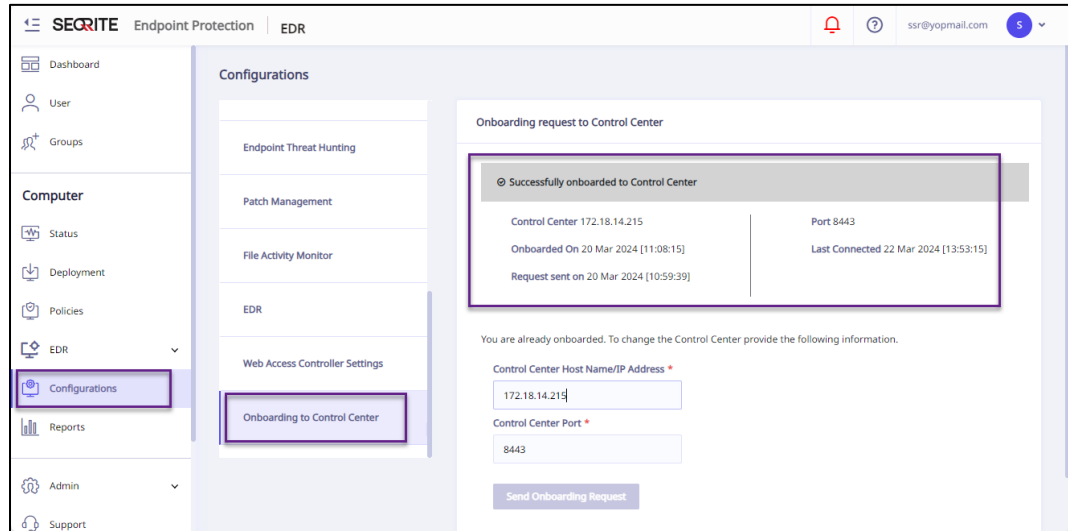
Pending onboarding with Aggregator:

- Aggregator IP
- Port Number
- Request sent on date and time

Once approved, it shows Successful Onboarding message with these details:

- Aggregator IP
- Port Number
- Onboarded on Date and Time

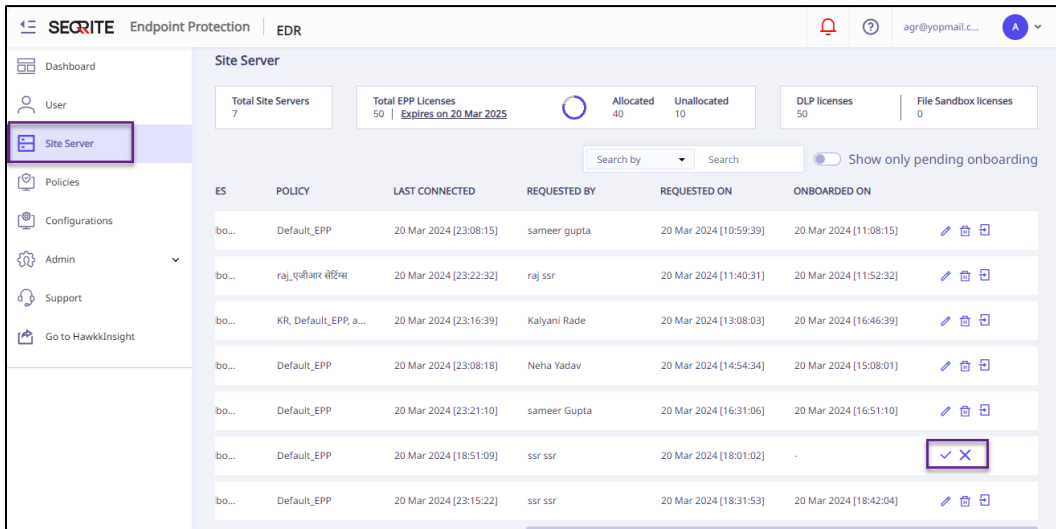
- Last Connected Date and Time



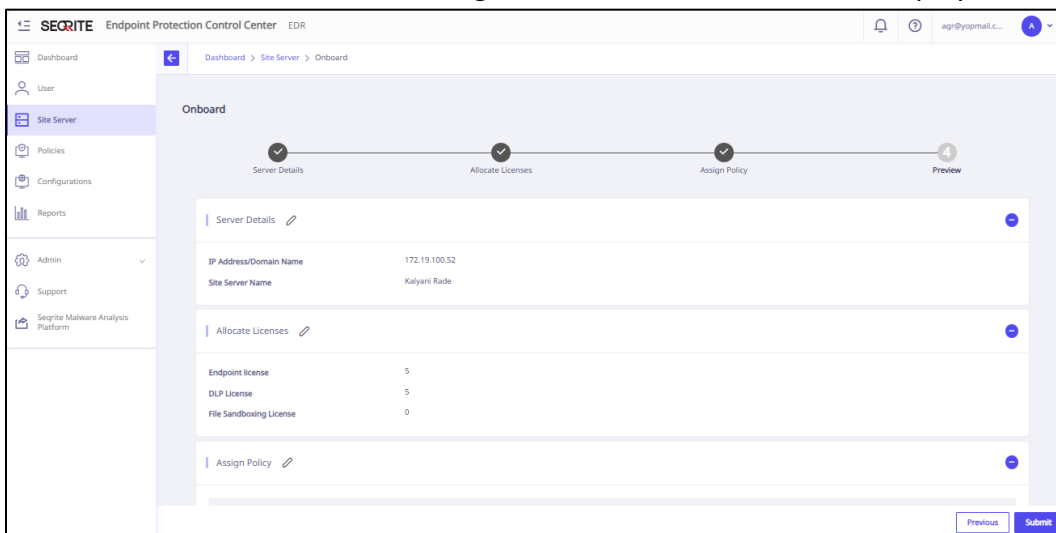
Site Server Approval/Rejection Steps from the Control Center Console

Follow these steps to onboard the site server from the Control Center console.

1. Log in to the Control Center console.
2. Click **Site Server**. The Site Server list appears. Click the tick/cross icon from the last column to approve/reject the SSR onboarding request.

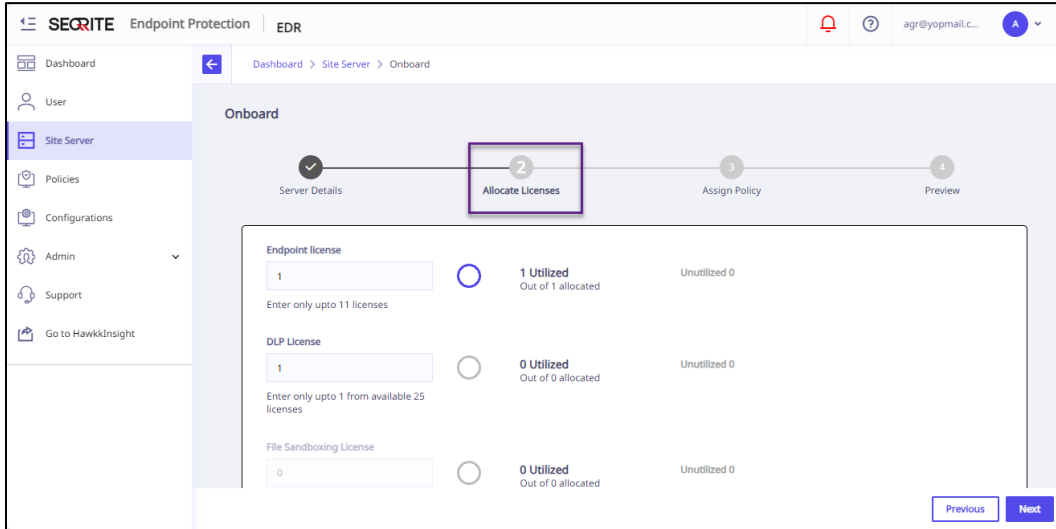


Click the tick icon to start onboarding the SSR. The Onboard screen displays.

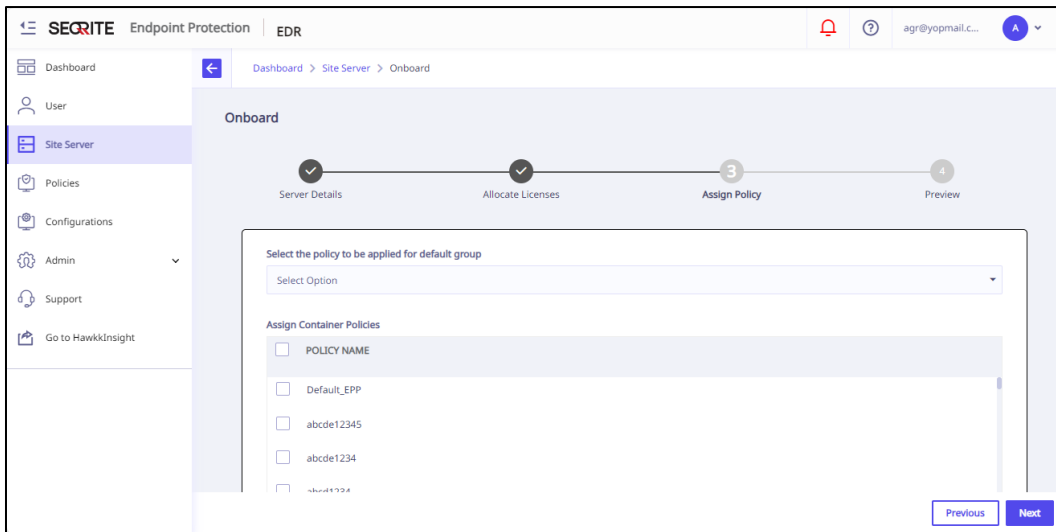


3. The site server **IP Address** is displayed.
4. The **Site Server Name** already appears. You can change it, if required.
5. Click **Next** or click the page name from the progress bar.

6. Allocate the endpoint and other licenses as required on the **Allocate Licenses** screen.

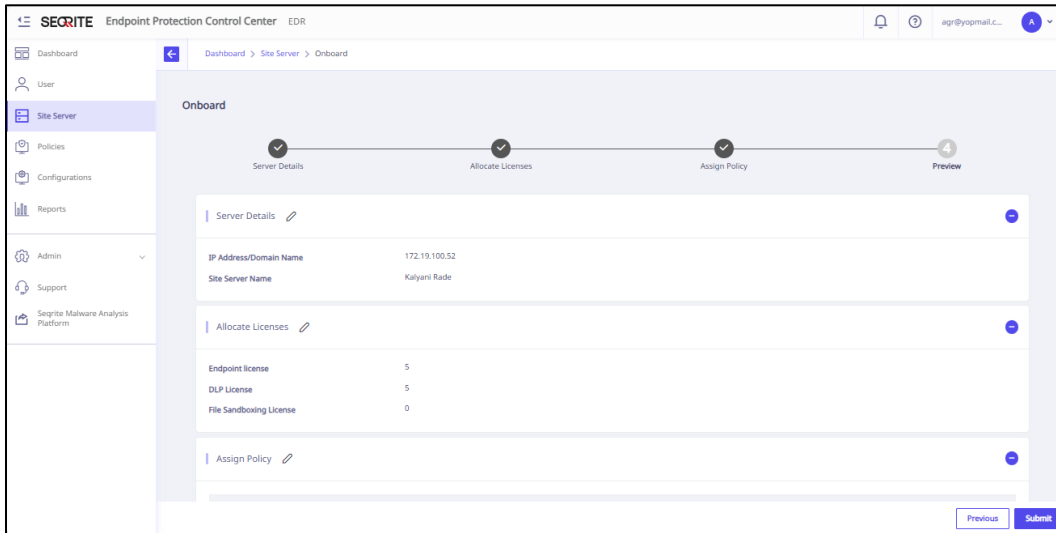


7. Select the policy name from the **Container Policy** drop-down list. Note that the policy created on the Control Center is applied to the default group of SSR. However, multiple policies from the Control Center can be enforced on the SSRs in one go.



Once the onboarding is approved from the Control Center, the policy along with its configuration values is applied to the SSR.

8. Check the details on the **Preview** screen. It shows all page details in accordion form. Click the pencil icon if you need to edit the details.

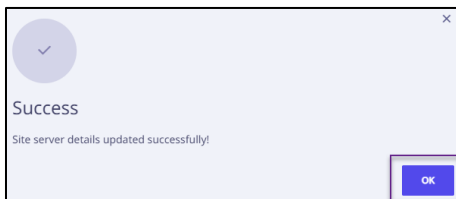


9. Click **Submit**. A confirmation message appears.

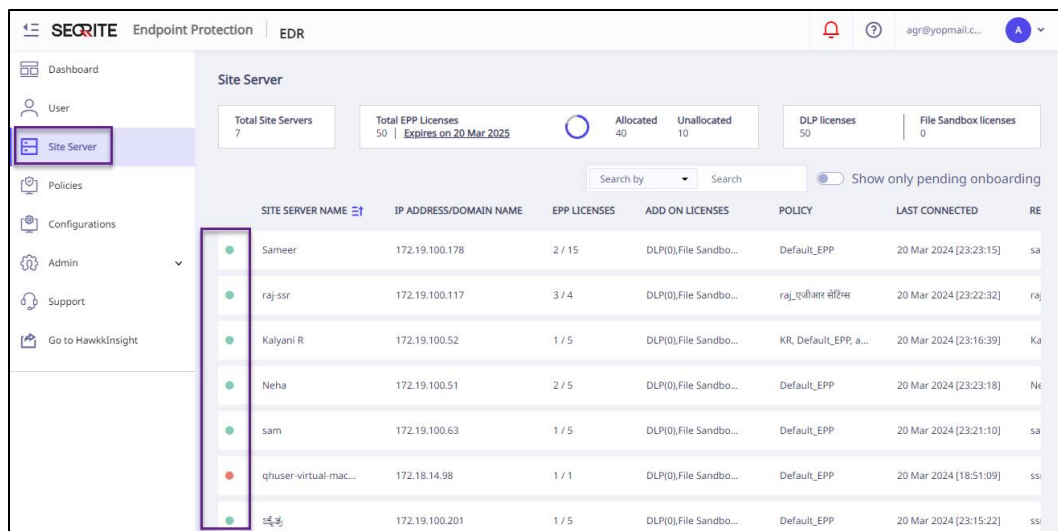


10. Click **Yes**. A request is sent to update the details.

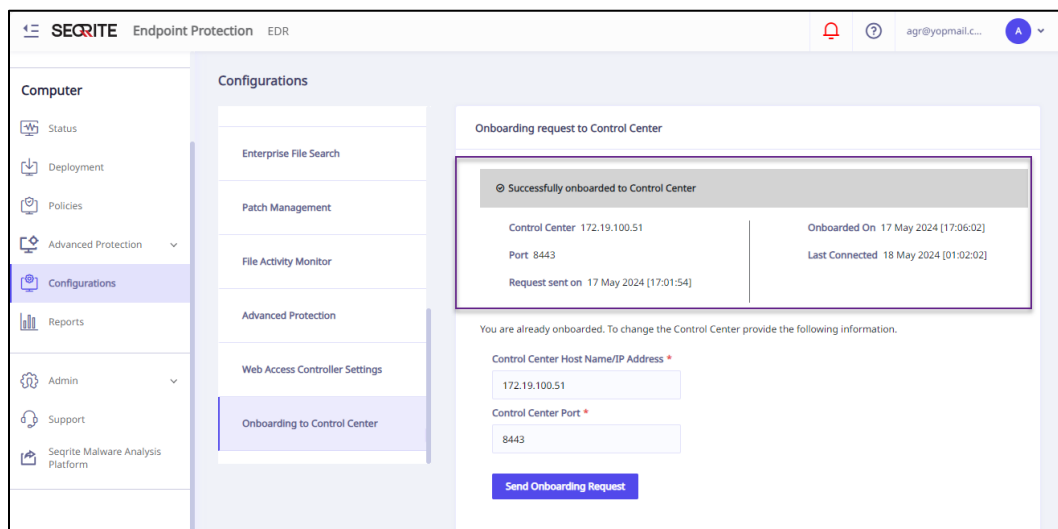
11. A success response confirmation message appears. Click **Ok**.



The onboarded/pending approval SSR details are reflected on the [Site Server](#) list page. Approved SSRs are marked with a green dot, pending SSRs with a red dot, and SSRs in queue with a mustard yellow dot.



The SSR onboarding approved or rejected status is also reflected on the SSR console at **Configurations > Onboarding to Aggregator.**



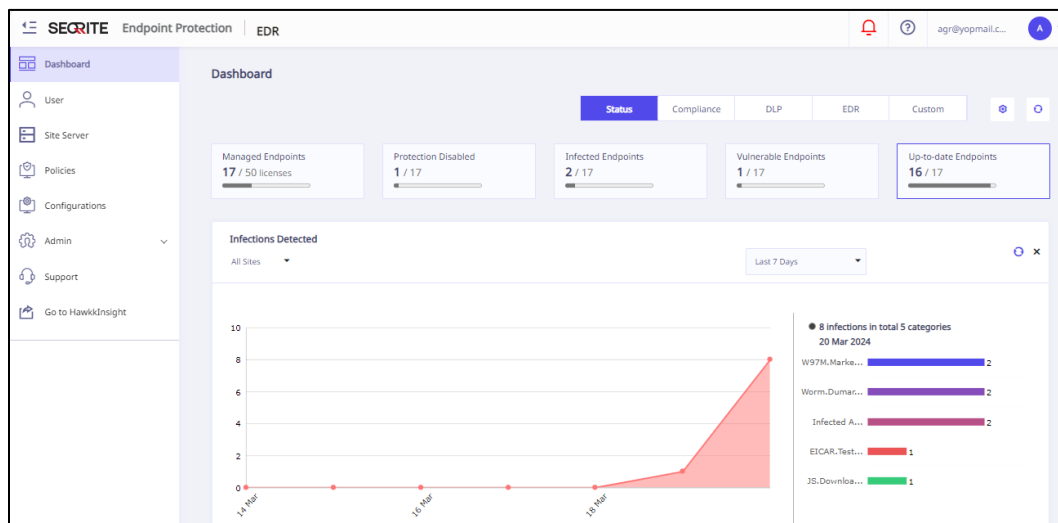
Once an SSR is successfully onboarded, any activity happening on the SSR is communicated to the Control Center. For example, if there is a virus outbreak, then an alert is sent to the Control Center.

EPP Control Center Console

Dashboard

The Dashboard displays the statistics and charts only when the site servers are deployed. As a new user, when you land on this page, the message appears to deploy the site servers.

Note: You can click the Site Server button if you want to deploy the SSRs at that moment.



Status

- **Managed Endpoints:** Displays a total number of endpoints in the network at that time. Click the card to go to [site server](#) screen.
- **Protection Disabled:** Displays a total number of endpoints on which the following features are disabled:
 - Virus Protection
 - Phishing Protection
 - Browsing Protection

When the above features are enabled on all the endpoints, **All Endpoints are Protected** message appears.

Clicking on the card redirects you to **Protection Disabled** reports screen.

- **Infected Endpoints:** Displays a total number of infected endpoints in the last 7 days. If no virus attacks are found, **All Endpoints are Clean** message appears. Clicking on the card redirects you to **Virus Scan** reports screen.
- **Vulnerable Endpoints:** Displays number of vulnerable endpoints in the network.

When no vulnerabilities are found, it displays as **0**.

Clicking on the card redirects you to **Vulnerability Scan** reports screen.

- Up-to-date Endpoint: Displays a number of total endpoints on which the virus definitions are up to date.

Clicking on the tab redirects you to **Up-to-date Endpoints** reports screen.

The Dashboard on the Home page displays the widgets for Infections Detected, Host Integrity Report, Up-to-date Endpoints, Connected Endpoints, Top 10 Malwares, Operating System Distribution, and Agent Versions. You can refresh the widget with the refresh button. You can remove the widget with the remove icon (X). The removed widget name appears in the Customize Dashboard > Unassigned Widgets section.

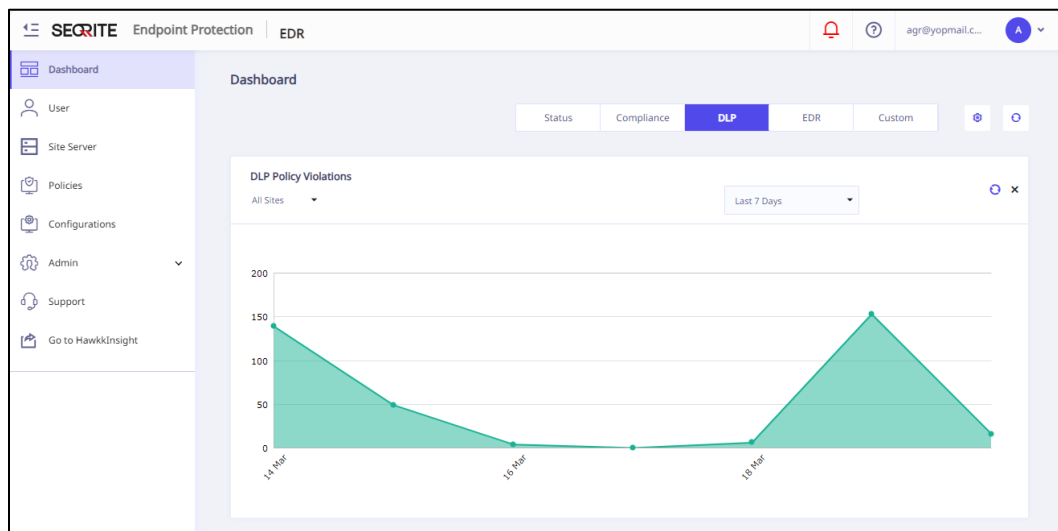
Widget Name	Description
Top 10 Malwares	Gives a progress bar chart that displays the top 10 malware detected systems in the network for the selected time. Clicking the Detection count redirects to the Anti-Malware Scan report page.
Up-to-date Endpoints	Displays a bar graph illustrating the total count of endpoints associated with each SSR on which the virus definitions are up to date.
Host Integrity Report	Gives a doughnut chart that displays the number of compliant and non-compliant endpoints. An endpoint is protected and compliant if all the following conditions are true. <ul style="list-style-type: none">• Client Agent version is the latest.• Virus Database is updated.• Virus protection is enabled.• Behavior Detection System is enabled.• No malware is found on it.
Infections Detected	Gives a graphical representation that displays a total number of infected endpoints. Select the duration and the SSR name from the drop-down values.
Connected Endpoints	Gives a doughnut chart which displays the number of endpoints

	which are connected last and not connected for last 3, 7, 15 and 30 days.
Operating System Distribution	Gives a doughnut chart which displays the distribution of each operating system. You have the option to apply filters based on Site Server (SSR) specifications.

Compliance

- Top 10 Blocked Website Categories
- Top 10 Blocked Website URLs
- Top 5 Blocked Devices
- Top 10 vulnerabilities

DLP



DLP Policy Violations: Gives a graphical representation of DLP policy violations detected on the selected endpoint for the selected time period. It could be past seven, 15, or 30 days.

Data Leaks through data transfer channel

Advanced Protection

- Overall Incident Summary
- Affected Endpoints
- MITRE Attack Metrics

- Affected Incident Rate
- Top 5 Incidents

Custom

Customize Dashboard

To customize the dashboard view, drag and drop the widgets. You can also change the sequence of the dashboard views by drag and drop.

Refresh

Refresh takes you back to the default dashboard settings.

User

The User screen displays the information of all the users including Active Directory Users in the table format. The table includes information such as User Name, User Role, Email, and so on.

You can customize the User table as per column names. You can search the user with the help of search criteria.

The Seqrite EPP users can:

- fully access this page.
- add, delete, edit User from this page.
- change the password of the user except for Active Directory User.
- view the details of the user.
- create a user and assign user role.
- rename, edit or delete the user.
- enable or disable the user.

The User session is timed out if the current session is inactive for 20 minutes.

Important to know:

- Access to the site server via the Control Center console through SSO is restricted to users with the **Admin and Super Admin** roles.
- The user roles of **Admin and Super Admin** established within the Control Center are mirrored in the SSR as well.

Adding a User

Follow these steps to create a user and assign user roles.

To add a user, follow these steps:

1. Log on to the Seqrite Endpoint Protection.
2. Click User from the left panel. The Users page appears displaying list of users.
3. Click **Add User** button. A prompt appears asking if you want to add or import a user.
4. Click **Add**. The **Add User** dialog appears.
5. Active Directory User switch appears only when Active Directory settings are enabled from Configurations. Keep the switch at the **No** position.
6. Enter First Name, Last name, Email ID, Password, Confirm Password, and Mobile No.

7. Select the desired User Role from the drop-down list values. The selected role will be assigned to the user. The User role can be changed to the other role as and when required.

For more information, see [User Roles](#).

8. If you assign the User Role as Group Admin, click **Next**.
9. In the dialog, a list of groups appears. Select the group to be assigned to the Group Admin. Only one group can be assigned to the Group Admin here. If the Parent group is selected, all child and sub child group are selected automatically. You can select only one child or a sub-child group from the hierarchy. One group can have multiple Group Admins.
10. Click **Add**.

The new user is added to the list. You can create a maximum of 49 users.

When you log on to Seqrite Endpoint Protection as Group Administrator, the Status page is displayed by default.

Adding an Active Directory User

To add an Active Directory (AD) user, follow these steps:

1. Log on to the Seqrite Endpoint Protection.
2. Click **User** from the left panel. The Users page appears displaying a list of users.
3. Click **Add User** button. A prompt appears asking if you want to add or import a user.
4. Click **Add**. The **Add User** dialog appears. Active Directory User switch appears only when Active Directory settings are enabled from Configurations.
5. Toggle the Active Directory User switch to **Yes**.
6. Enter AD User name. AD Username is required for authentication The Password and Confirm Password fields are disabled as AD credentials of the user are used for authentication.
7. Enter First Name, Last name, Email ID, and Mobile No.
8. Select the User Role from the list. The selected role will be assigned to the user.
9. Click **Add**. The new AD user is added to the list.

When you log on to Seqrite Endpoint Protection as an AD User, you need to provide AD credentials.

Enabling a User

To enable a user, follow these steps:

1. On the **User** screen, select the check box of the user that you want to enable. An action bar is enabled above the table.
2. Select **Enable**.
3. Click **Submit** button.
4. The confirmation message appears. Click **Yes**.
The selected user is enabled.

Disabling a User

To disable a user, follow these steps:

1. On the **User** screen, select the check box of the user that you want to disable. An action bar is enabled above the table.
2. Select **Disable**.
3. Click **Submit** button.
4. The confirmation message appears. Click **Yes**.
5. The selected user is disabled.

Note: The disabled user cannot log on the Seqrite Endpoint Protection portal.

Deleting a User

To delete the user, follow these steps:

1. Log on to the Seqrite Endpoint Protection.
2. Click **User** from the left panel. The Users page appears displaying a list of users.
3. Select the check box of the user that you want to delete. An action bar is enabled above the table.
4. Select **Delete**.
5. Click **Submit**.
6. The confirmation message appears. Click **Yes**.
The selected user is removed.

Note:

- You cannot edit or delete the default user.
- If you delete the Group Admin, the policies created by the Group Admin can be deleted if the policies are not assigned to any group and endpoints.

Editing a User

To edit the user, follow these steps:

1. Log on to the Seqrite Endpoint Protection.
2. Click **User** from the left panel. The Users page appears displaying a list of users.
3. Click the **Edit** icon for the user that you want to edit.
4. The **Edit User** dialog appears.
5. Make the desired changes.
6. If you assign the User Role as Group Admin, click **Next**.
7. In the dialog, a list of groups appears. Select the group to be assigned to the Group Admin. If the Parent group is selected, all child and sub child group are selected automatically. You can select only one child or a sub-child group from the hierarchy.
8. Click **Save**.

User information is updated.

Note: You cannot edit or delete the default user.

Changing Password of User

Note that the password cannot be changed for Active Directory User.

To change the password of the EPP User, follow these steps:

1. Log on to the Seqrite Endpoint Protection.
2. Click **User** from the left panel. The page appears displaying a list of users.
3. Click **Change Password** link for the user for which you want to change the password. The **Change Password** dialog appears.
4. Enter a new password. Enter the new password again to confirm.
5. Click **Change Password**.

The password of the user is changed.

Importing a user

You can import maximum 49 users at a time through a CSV file.

To import the users, follow these steps:

1. Log on to the Seqrite Endpoint Protection.
2. Click **Users** from the left panel. The Users page appears displaying a list of users.

3. Click **Add User > Import**.
4. In the **Import User** dialog, import a CSV file by clicking **Browse**. The file size must be less than or equal to 1 MB.

Ensure that the CSV file content is in the following format:

First Name	Last Name	EMAIL	Password	Confirm Password	Country Code	Mob Num	User Role Name	Domain Name	Active Dir User Name
aaa	rrr	aaa@mail.com	*****	*****	+91	1111111111	ADMIN	EPP.com	Administrator
bbb	sss	bbb@gmail.com	*****	*****	+44	2222222222	REPORT_ONLY		
bbb	sss	bbb@gmail.com	*****	*****	+44	2222222222	REPORT_ONLY		

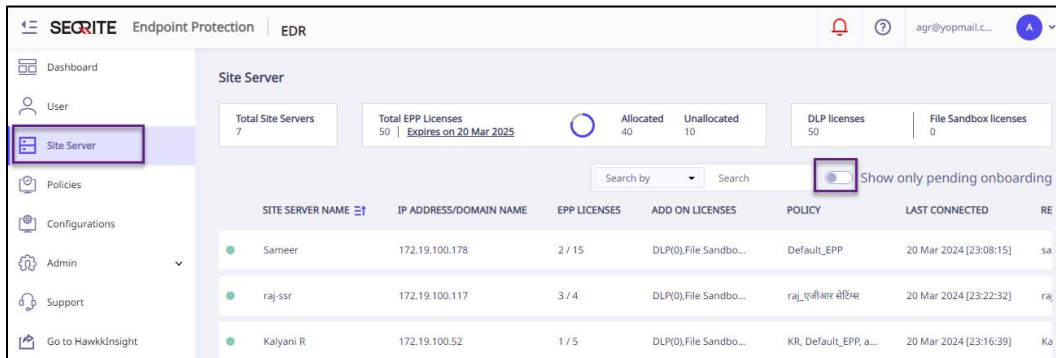
Important to know:

- Password must contain 6 to 19 characters. There must be at least one uppercase letter, 1 lowercase letter, a number, and a special character.
- As you see in the above example, the Country Code should contain + sign.
- The User Role name (REPORT_ONLY, ADMIN) should be in Capital letters.
- Only for the Active directory user, Domain Name and ActiveDir User Name are required. For the EPP user, these columns should be blank.

5. Click **Import**.

Site Server


This page shows a list of the site servers. Toggle the **Show only pending onboarding** button to true, to view the list of site servers that are waiting to be onboarded.



Note:

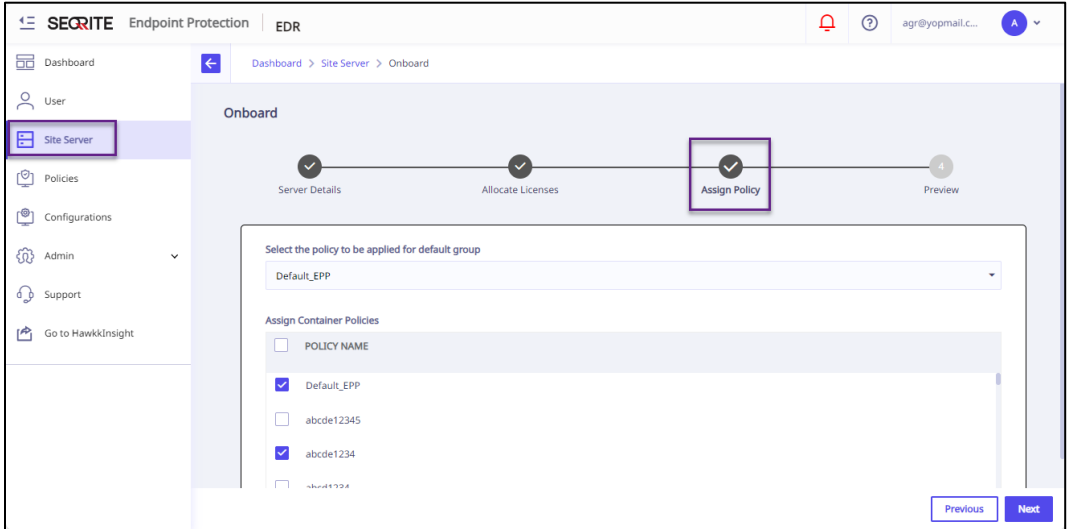
- Approved Site servers are marked in green color and pending site servers are marked in red color.
- You can search for a site server by entering the site server name on the Search by text box.
- You can sort the names once the searched site server name list appears.

Column Name	Description
Site Server Name	Displays the name of the site server that is onboarded/waiting/failed to be onboarded.
IP Address/Domain Name	Displays the IP Address/Domain Name of the site server that is onboarded/waiting to be onboarded.
EPP Licenses	Displays the number of EPP licenses assigned to the site server.
Add On Licenses	Displays the name and number of the add on licenses assigned to the site server. For example, DLP, File Sandbox, and so on.
Policy	<p>Displays the name of the policy that is assigned to the site server, or the status as follows:</p> <ul style="list-style-type: none"> • Pending: This status is displayed if <ul style="list-style-type: none"> ○ Control Center sends a policy to SSR and the SSR is yet to accept. ○ Control Center modifies a policy which is applied

	<p>on the SSR and the SSR is yet to accept.</p> <ul style="list-style-type: none"> Policy Name: The name of the policy is displayed once the SSR accepts the policy request.
Requested By	Displays the username of the user who requested to onboard the site server.
Requested On	Displays the date and the time when the site server onboarding request was sent.
Onboarded On	Displays the date and the time when the site server was onboarded.
Last Connected	Displays the date and the time when the site server was online. It is the time of the last heartbeat interval.
 (applicable to the already onboarded servers)	<ul style="list-style-type: none"> Click the pencil icon to make changes in the server, license, or policy details. Refer the Onboarding Steps section for details. Click the trash icon to remove the site server from the list. <ul style="list-style-type: none"> The server would be offboarded from the Control Center. Provided only one default client is installed under that SSR. If more than one license is already used, an error message is displayed as Please free already used licenses, then try again. As soon as the delete command is received, the SSR is deactivated, and the entry for the deleted site server gets removed from the Site Server list page on the Control Center console. Activity log in case of Delete Activity on Control Center is logged in the activity log. Also, a failed deletion is logged too. Delete notification to SSR Admin is send on an Email (when SMTP not configured) If SSR is offline when the delete command is sent, deletion takes place once the device is online. Click the arrow icon to go to the site server console. You are logged in as a super admin on the site server console.

<p>✓ ✕ (applicable to the onboarding pending servers)</p>	<ul style="list-style-type: none"> • Click the tick icon to approve the onboard request. • Click the cross icon to reject the onboard request.
---	--

While onboarding the SSR, single or multiple container policies can be sent to SSR. The policy selected from the drop-down menu is assigned to the default group within the SSR. Whereas, the container policies selected from the list are transferred to the SSR without specific group assignment.



On the **Site Server > edit > Assign Policy** screen, you can select the desired policy/policies to send to the SSR.

Policies that have been sent are stored at the Site Server (SSR) end in a read-only format. They are identified as enforced policies, denoted by an information icon.

If a policy with an existing name already exists and was previously enforced or sent, it will be overwritten. If this policy is applied to the default group, it should be reapplied.

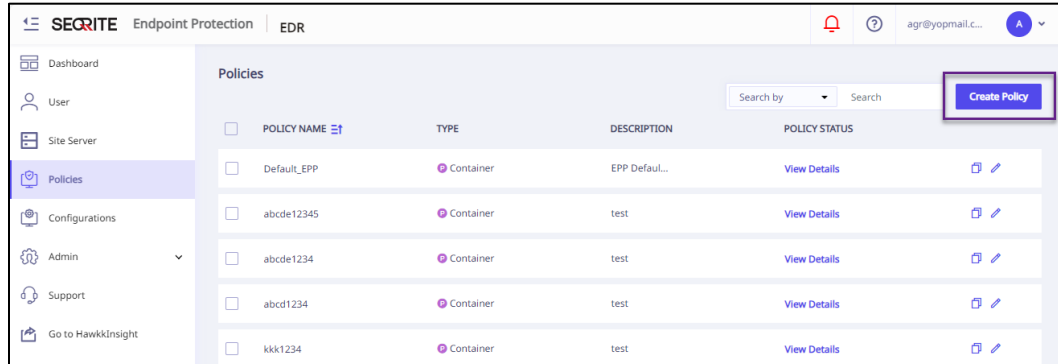
If the policy is created on the Control Center with the same name as the SSR, then the SSR policy will be renamed and appended with the timestamp and enforced name remains on the SSR.


Deployment

Seqrite advises clients currently utilizing EPS On-Prem 7.x to migrate to Seqrite EPP 8.3. You can initiate the migration process from EPS version 7.x to EPP version 8.3 directly from this interface.

Policies

Policies feature helps you to create policies that help centrally control and manage the users belonging to a group. The policy created on Control Center is applied to the default group of SSR.



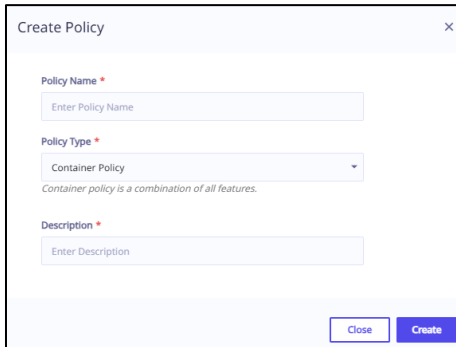
Column Name	Description
Policy Name	Displays the name of the policy applied to the SSR.
Type	Displays the type of the policy.
Description	Displays the policy description.
Policy Status	Click View Details to access the following tabs: <ul style="list-style-type: none"> Applied Groups Applied Endpoints Pending Endpoints
	<ul style="list-style-type: none"> Click the duplicate icon to clone the policy. Click the edit icon to make changes to the policy settings.

Creating a Policy

To create a new policy, follow these steps:

1. Go to the console > **Policies**.

2. Click the **Create Policy** button. The **Create Policy** window appears.



3. Enter the details.
4. Click **Create**.

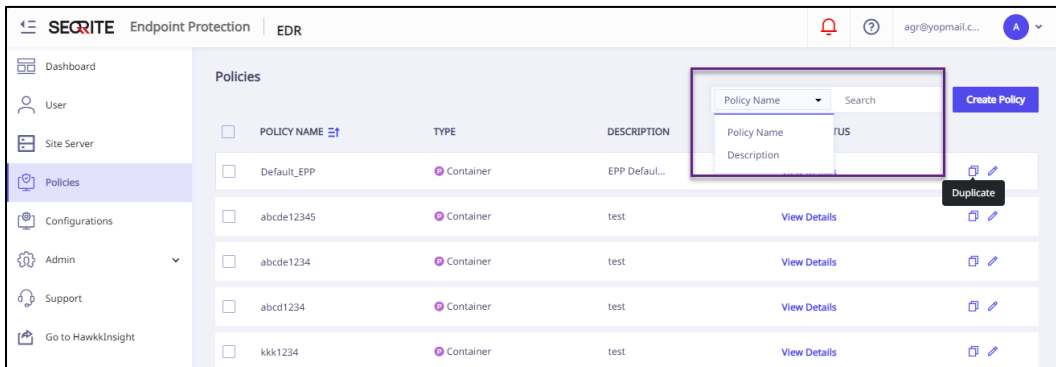
Note:

- A change made in the policy on the Control Center console is directly reflected on the SSR at the next heartbeat time.
- Applied policy is read only.
- Label is displayed for inherited policy.

Searching for a Policy

To search for a particular policy that you need, follow these steps:

1. Go to the console > **Policies**. A list of policies appears.



POLICY NAME	TYPE	DESCRIPTION
Default_EPP	Container	EPP Defaul...
abcde12345	Container	test
abcde1234	Container	test
abcd1234	Container	test
kkk1234	Container	test

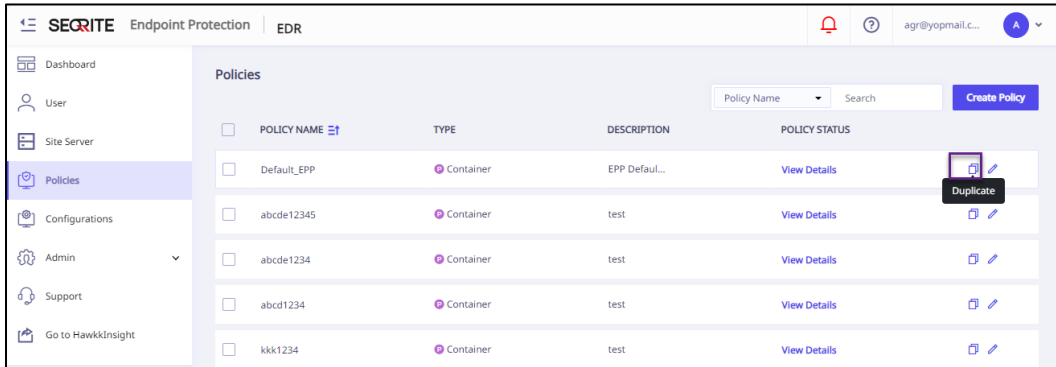
2. Select a value from the **Search by** drop-down box. You can either
 - a. search by Policy Name OR
 - b. search by Description
3. Enter the policy name/description in the Search text box.
4. Hit [Enter].

The desired policy appears.

Duplication of Policy

To duplicate a policy, follow these steps:

1. Go to Policies. The Policies page appears displaying a list of policies.



2. Click the duplicate icon of the policy that you want to duplicate.
3. The duplicated policy appears in the next row. Edit the name of the policy. Click the tick mark icon to save the policy. The selected policy is duplicated. The policy settings remain the same. You can also change the policy settings if required.
4. To save your setting, click **Save Policy**.

Configurations

On this page, you can configure the following settings:

- **Active Directory:** Active Directory (AD) is a database and set of services that connect users with the network resources they need to get their work done.

In organizations (Medium/Large), Active Directory is used for maintaining user databases, configuring central policies, and pushing applications to users. For any organization, it is very important that you can log in to any application using existing active directory users. You don't have to create other users specific to the application itself.

Active Directory Users can log in to any application within the network. Active Directory User credential is used to log in to the applications.

- **Device Control:** This feature helps you to add USB and other devices. If your organization has a large number of USB storage devices of the same make and model, you can add these USBs by model name. You can also add Scanner, Card Reader, Local printers, Mobile phones, and so on.
- **Data Loss Prevention:** You can add certain key words, or phrases that might contain, or refer to confidential information in the User Defined Dictionary. If any of the documents on your endpoints contains the text or phrase that you have added to the User Defined

Dictionary, the Data-At-Rest Scan or Data Loss Prevention feature displays the path or location of these documents.

On this page, User Defined Dictionaries can be created or managed which will be monitored through Data Loss Prevention Settings.

The user has the ability to configure custom DLP actions for each file type and custom extension, confidential data such as PAN, PIN, Phone, and so on.

Similarly, you can also add the applications that you need to monitor or exclude from the DLP.

- **Application Control:** This feature allows you to add a new application to the default list. Adding and unauthorized an application or file that belongs to the operating system or other system specific aspects may cause system malfunction. Hence, it is advised to add an application that is not a part of the operating system or other system related programs.
- **SMTP Settings:** This feature helps you set the SMTP Host Details. All emails from Seqrite Endpoint Protection such as Notification mails and Report mails will be sent to the SMTP Server for further routing.
- **Internet Settings:** On this page you can provide the Proxy Server details, if you are using proxy settings to connect to the Internet.
- **Enterprise File Search:** This feature helps you identify and mitigate potential threats on the endpoints within a network.
- **File Activity Monitor:** On this page, you can add file extensions and folders that you want to exclude from the File Activity Monitor policy.
- **Web Access Controller Settings:** This extension ensures that users within your organization can only sign into their Corporate Google Accounts on the Endpoint's Google Chrome or Microsoft Edge Browser for specific domains that are configured by the Administrator. This implementation ensures compliance and prevents any misuse or abuse.

Additionally, this extension offers an additional layer of security by restricting users within your organization from watching YouTube videos solely on Endpoint's Google Chrome or Microsoft Edge Browser. Users can only access videos of specific categories, channels, and publishers, enhancing compliance and preventing unauthorized usage.

This extension must be used with Seqrite Endpoint Protection; cannot be used independently.

Reports

Report Name	Description
Virus Scan	Displays the virus incidents on the selected site server. You can also view the statistics of unscanned endpoints since the last 7 ,15, and 30 days.
Anti-Malware Scan	Displays the malware incidents after scanning the clients.
Web Security	Displays statistics of Web sites blocked through the Browsing Protection, Phishing Protection, or block Web site modules. In the tabular report, you can view whether YouTube videos have been blocked.
Advanced Device Control	Displays whether removable devices have been blocked and what actions were taken against unauthorized device access.
Data Loss Prevention	Displays statistics about attempts of sending the data outside the organization in an unauthorized manner. Data-at-Rest scan reports are included in DLP on demand report. You can view the information related to the detected confidential data such as; the file path, threat type, and matched text. You can generate a DLP report for a single endpoint at a time.
Vulnerability Scan	Displays reports of vulnerabilities present on the endpoints in the network.
Host Integrity	Displays reports of compliant and non-compliant endpoints. This report is only in the tabular format, not in the chart format.
Connected Endpoints	Displays information regarding endpoints that have not been connected for a specified duration of days.
Up-to-date Endpoints	Displays the endpoint details, including the associated site server and whether they have been updated or not.
OS Distribution Report	Displays the endpoint details, including the associated site server, the installed OS and version.
Protection Disabled	Displays the number of unprotected endpoints along with the site server details.

Version Distribution	Displays the number of endpoints as per the site server selection. It displays the associated site server name, and the installed client agent version.
----------------------	---

Admin

License

On this page, you can manage Seqrite Endpoint Protection licenses. You can check the status of your Seqrite Endpoint Protection license, DLP licenses, and File Sandbox license information. For postpaid license, license information is not displayed.

If there is a change in the license at the SSR, it is communicated to the Control Center. The action is taken at the heartbeat interval.

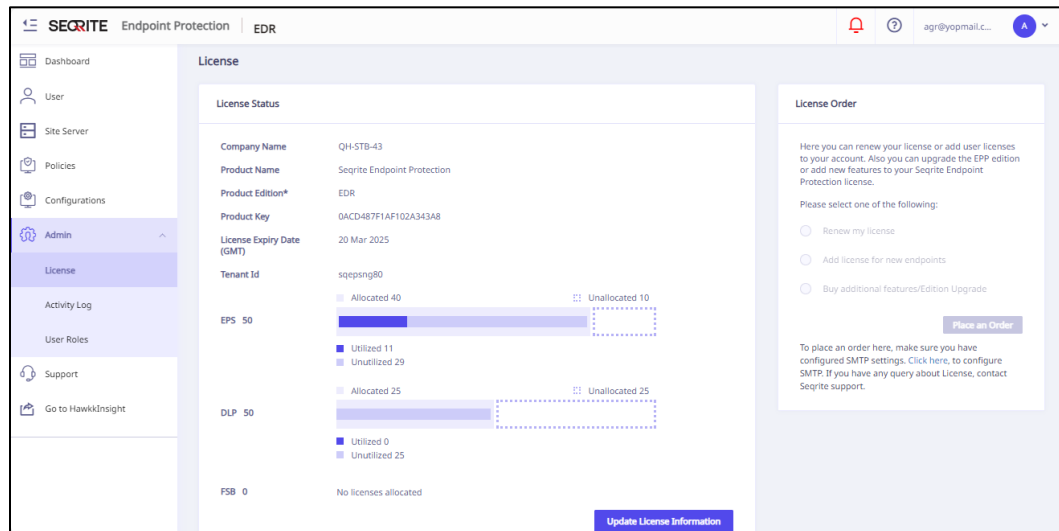


Figure 1: License Details on Control Center Console

If there are any pending commands at Control Center for SSR, the SSR fetches it. The cron job is run on heartbeat interval at SSR and performs the required action.

Activity Log

This page helps you check the activity logs of all the incidents that occurred on the server.

All the actions taken by Control Center admin about SSR are maintained in the Activity log. The onboarding approval or rejection, or removal is listed in the activity log. After a successful onboarding, if you change the license allocation, or make changes in policy, or change the SSR name. these actions are also logged. It also logs the user logging in via SSO.

You can select the number of days, either seven or 15, for which the activities are generated. By default, you can view logs of the last seven days. You can also select Custom option and then select the start and end dates for the activity logs.

The activity log is maintained for 90 days.

Activity log provides the details on:

- Date and time of activity
- user who performed the activity
- Action on
- Details of activity done

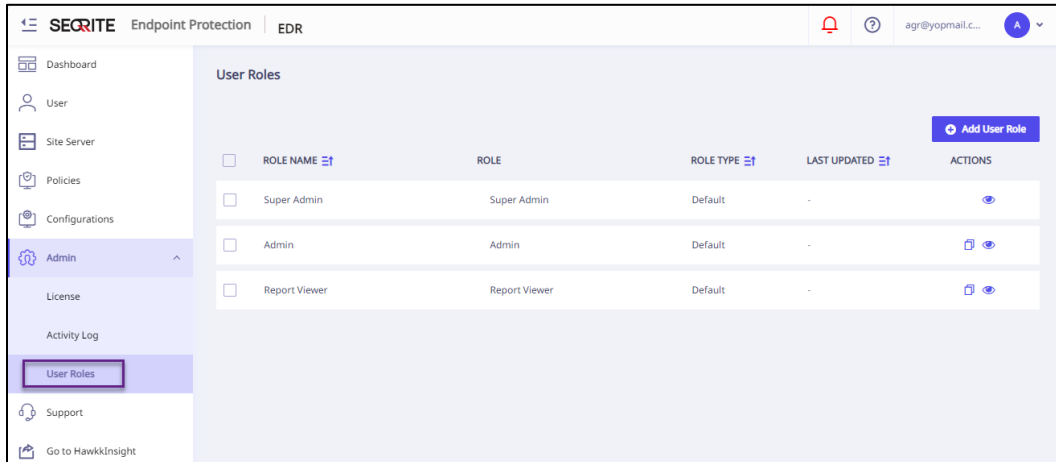
To export complete activity log, click the Export tab. The ActivityLog.csv file is downloaded.

DATE & TIME	USER NAME	ACTION ON	DESCRIPTION
20 Mar 2024 [22:52:37]	agr@yopmail.com	User	Last Logged On
20 Mar 2024 [19:34:05]	agr@yopmail.com	User	Last Logged On
20 Mar 2024 [19:05:57]	agr@yopmail.com	User	Last Logged On
20 Mar 2024 [18:41:15]	agr@yopmail.com	Site Server	*[redacted] site server has been onboar...
20 Mar 2024 [18:32:08]	agr@yopmail.com	User	Last Logged On
20 Mar 2024 [17:30:23]	agr@yopmail.com	User	Last Logged On
20 Mar 2024 [17:25:22]	agr@yopmail.com	Site Server	*Default_EPP, abcde12345, abcde1234...

User Roles

The User Roles page displays information such as Role Name, Role Type, and so on. You can view the user role privileges of the default role types by clicking the view icon.

This feature helps you create, modify, duplicate, and delete roles for different types of user roles.



The following are default user roles.

- **Super Admin** - A Super Admin user has all the privileges to access, manage and delete the features of Seqrite Endpoint Protection. You cannot edit the privileges. The role type is default. There can be only one user with Super Admin privileges.
- **Admin** - A user with Admin privileges has authority to access, manage, and delete the features of Seqrite Endpoint Protection. You can create multiple user roles for Admin, if required.
- **Group Admin** - A Group Admin user can view and manage only the groups assigned to the Group Admin user. You can create Group Admin for each group. You can assign multiple Group Admins to one group.

Super Admin and Admin user can create/edit/delete the Group Admin user and assign/unassign the Group Admin to any group.

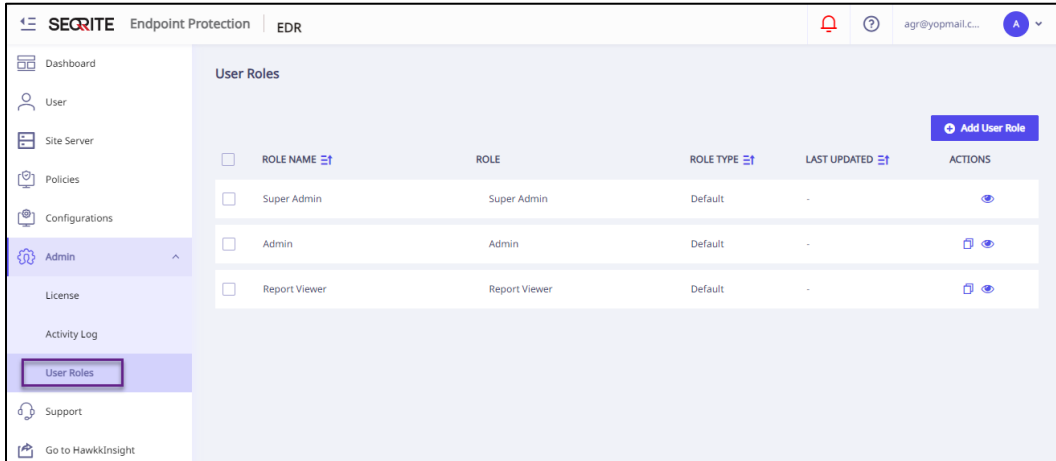
Group Admin can generate reports in table /chart formats for assigned groups only.

The group admin can move endpoints within its own group/subgroup.

When Group Admin logs on, the Status page is displayed by default. The Group Admin has limited access to pages of Seqrite Endpoint Protection. (This user role exists only on the SSR)

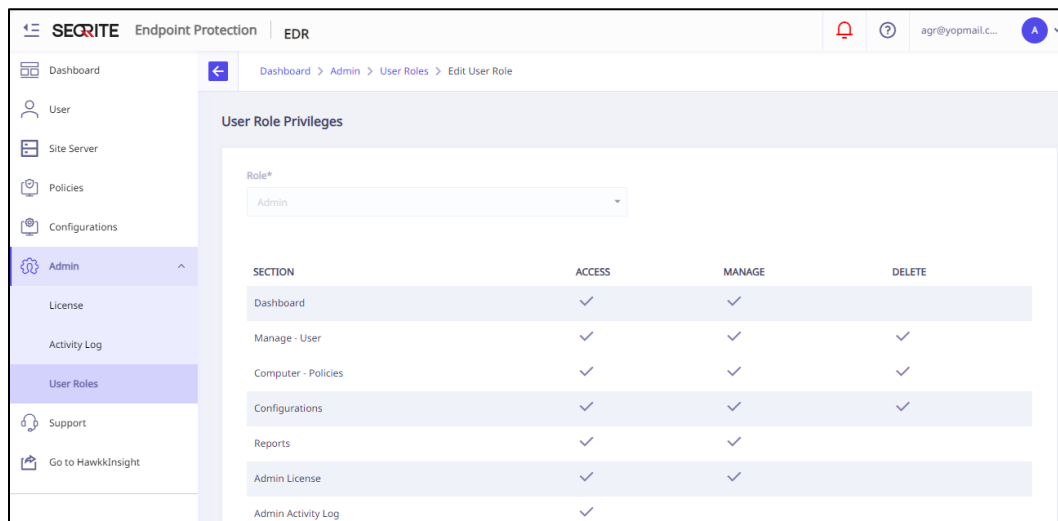
- **Report Viewer** - A user with the Report Viewer role has only access privileges, this user cannot manage or delete roles. The default user role name for Report Viewer is **Report Viewer**. You can create multiple user roles for Report Viewer, if required

- **Security OPS Manager:** Applicable only to SSR.
- **Security OPS Analyst:** Applicable only to SSR.



Click the View icon from the Actions column to view the user role privileges.

Click the Duplicate icon to create a custom role.



You can manage the privileges for the custom role by clicking the edit icon.

Note:

- You cannot delete default User Roles.
- You can create custom roles as per your requirement.

Support

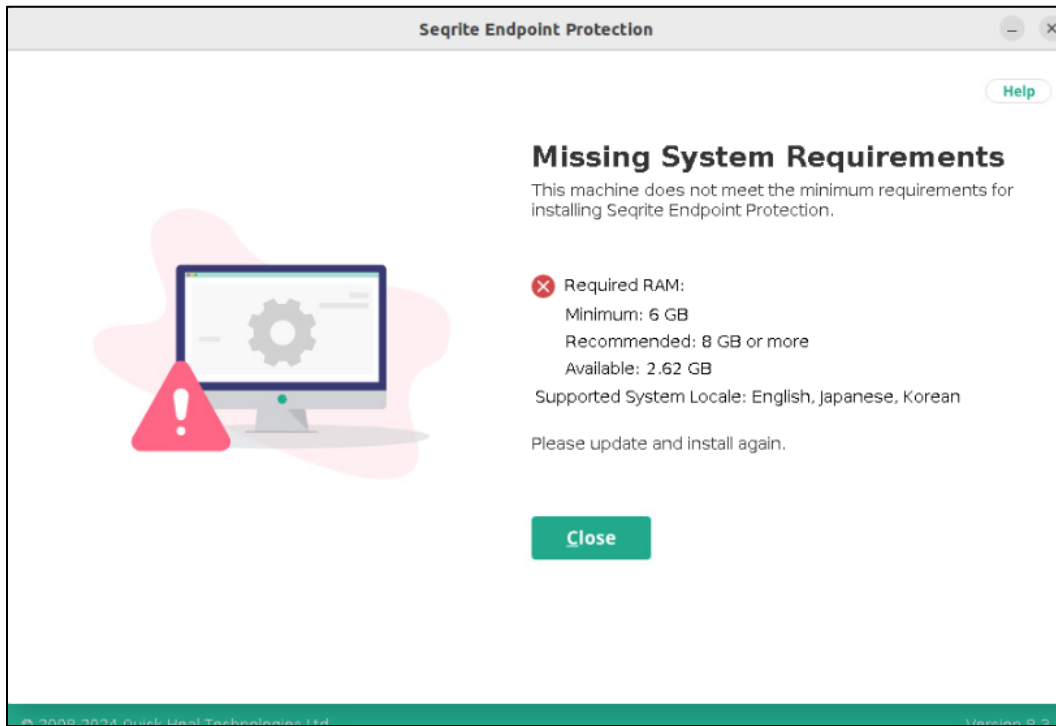
To know support contacts, please visit http://www.segrite.com/contact_support

Troubleshoot

Here are some common scenarios where an error message might appear.

Missing Requirements

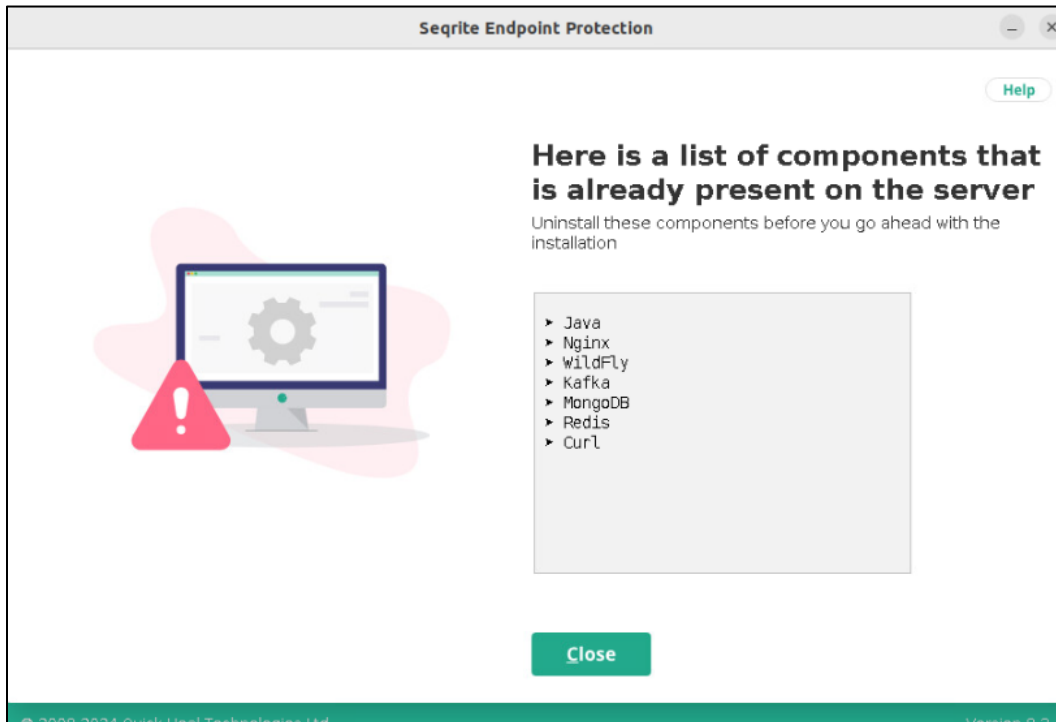
The system does not start the installation if you get this message on your screen.



Ensure that all the prerequisites are met before you start the installation.

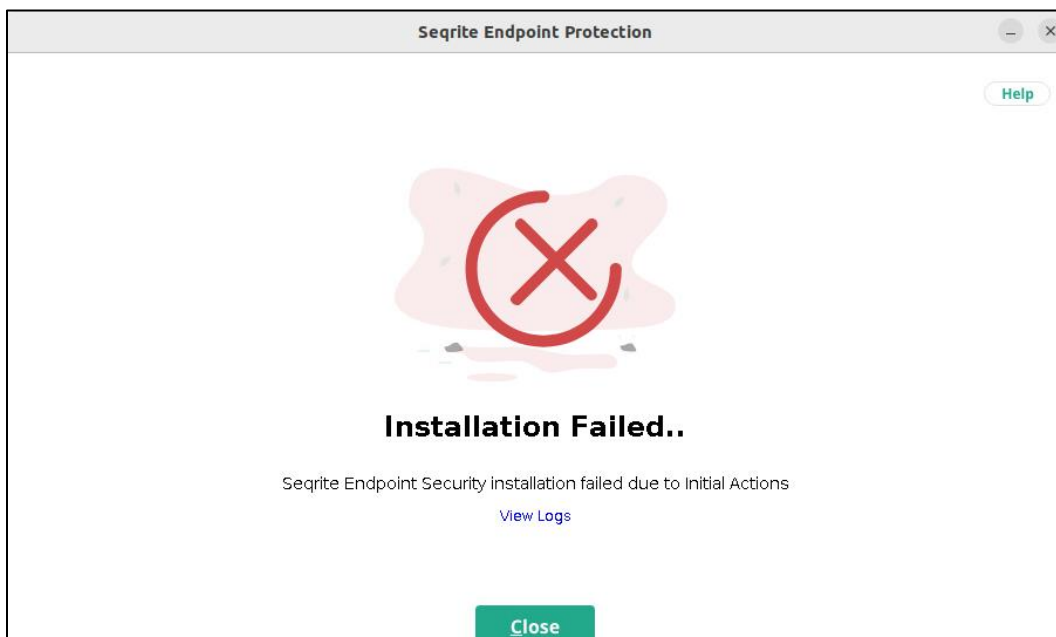
Uninstall Components

The system does not let you continue with the installation if you get a similar message on your screen.



You need to uninstall the listed components before proceeding with the installation.

Incorrect Initial Actions



Check the logs and get it resolved by the administrator/Seqrite support.