# User Guide

Seqrite
**Endpoint Security Cloud**

# Copyright Information



## Trademarks



## License Terms

Installation and usage of Seqrite Endpoint Security Cloud 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 Agreement for your product.

Release Date
February 1, 2020

# Contents

# Seqrite Endpoint Security

Welcome to the User Guide of Seqrite Endpoint Security Cloud!

Seqrite Endpoint Security Cloud is an integrated solution that allows the management and regulation of multiple Endpoint Security products deployed at different geographical locations. IT administrators from any location can easily connect to the cloud to view the latest security status, configure product policies, receive notifications and rectify critical network events from one single dashboard. It also facilitates policy configuration, backup and more on the cloud for Seqrite products.

## Available flavors

Seqrite Endpoint Security Cloud is available in three flavors of Standard, Advanced, and Premium.

The following table lists the features that are available in the flavors:

| Features / Edition | Standard | Advanced | Premium |
|---|---|---|---|
| Antivirus | ✓ | ✓ | ✓ |
| Antiransomware | ✓ | ✓ | ✓ |
| Email Protection | ✓ | ✓ | ✓ |
| IDS/IPS Protection | ✓ | ✓ | ✓ |
| Firewall | ✓ | ✓ | ✓ |
| Antiphishing | ✓ | ✓ | ✓ |
| Browsing Protection | ✓ | ✓ | ✓ |
| Antispam | | ✓ | ✓ |
| Web Security | | ✓ | ✓ |
| Advanced Device Control | | ✓ | ✓ |
| Application Control | | ✓ | ✓ |
| Asset Management | | | ✓ |
| Tuneup | | | ✓ |
| Data Loss Protection | **Available as add-on pack with Advanced and Premium** | | |

As per the flavor purchased, the features are available in the portal. In this guide, all the features are explained.

## Supported Web Browsers

The following Web browsers are supported for Seqrite Endpoint Security Cloud,

- Internet Explorer 10 and 11
- Microsoft Edge
- Google Chrome 60 and above
- Mozilla Firefox 55 and above
- Safari (Only Mac) 11, 12 and 13

## Recommendation for bulk client installation

If you want to install a large number of clients at a time, (Example: 500 clients), Seqrite recommends the following strategy,

**Installation using Remote Install tool**

To install 500 clients at a time, use the **"Remote Install"** method for client installation.

**Case 1: EPS is on-boarded by SSE or Reseller**

Install Seqrite client on one endpoint with Windows Vista and above Operating system.

After complete (Client agent + AntiVirus) installation of that client, assign Update Agent (UA) role to that client and download the AV builds.

Configure the UA as per the **Default_EPS** policy.

Download the Remote install tool on any windows OS.

In the remote install tool, add IP's of all the endpoints, on which Admin want to deploy Seqrite client.

Start installation process.

The Seqrite client will be installed on the selected endpoints and all the clients AV will be downloaded and installed from Update Agent configured in policy or AV will be downloaded from Internet, in this case if UA is not reachable to any of the client.

**Case 2: EPS is on-boarded by MSP**

After installation of Seqrite client using any method, Antivirus will be downloaded from internet because **Default_MSSP** policy cannot be edited so, you cannot configure Update Agent (UA) in the policy.

**Recommendation**

Use this method when all the endpoints are in the LAN where Admin want to install the protection.

Note:

- In the above case, client entry will be displayed immediately on the Server after installation.
- Client installation for 500 endpoints takes minimum 5 mins to maximum 35 mins depending upon on the available bandwidth.

**Installation using Email Install Link**

With this method, Admin can send the Emails to the geographically separated users to install the Seqrite clients on the endpoints.

1. Open the Email. Click the link.
2. When the URL is clicked, the client installation utility is downloaded.
3. This utility again when executed downloads client installer for applicable operating system.
4. After Seqrite client installation is finished, the Seqrite Antivirus installation will be initiated by the Seqrite client.

If UA is configured in the default policy, after Seqrite client installation, Antivirus will be downloaded from UA. If UA is not reachable, Antivirus will be downloaded from the internet.

**Installation using Client Installer**

**Case 1: Client Installer without Antivirus setup**

Create Client Installer based on the OS platform and systems architecture; also select the Group. (After client installation, clients reside in the selected group)

After client installation, antivirus will be downloaded from the UA if configured in the policy assigned to the selected group. If UA is not available, antivirus will be downloaded from Internet.

**Case 2: Client Installer with Antivirus setup**

Create Client Installer based on the OS platform and systems architecture; also select the Group. (After client installation, clients reside in selected group)

**Recommendation:** Use this method for low bandwidth.

**Installation using Active Directory tool**

The Active Directory tool helps you synchronize the EPS server group with active directory organizational unit (OU)/container/computer. After synchronization, the clients will be installed on all the endpoints of your domain network. A periodic check is carried out to find if any new endpoint is added to your network as per predefined settings. When a new endpoint is added, the client gets automatically installed on that endpoint.

# Dashboards

The Dashboard area displays the statistics and charts only when the endpoints are deployed. As a new user, when you land on this page, the message appears to deploy the endpoints. Click the Deployment button if you want to deploy the endpoints at that moment.

The Dashboard area on the Home page displays the widgets for Status, Compliance, DLP and Custom tabs. You can refresh the widget with the refresh button. You can remove the widget with the remove button (X). The removed widget name appears in the Customize Dashboard > Unassigned Widgets section.

### Current Status Summary

| Feature | Description |
|---|---|
| Endpoints | Displays total number of endpoints in the network at that time. |
| Protection Disabled<br>(All Endpoints are Protected) | • Displays number of endpoints on which the following features are disabled:<br>▪ Virus protection<br>▪ Phishing protection<br>▪ Browsing Protection<br>Clicking the icon below endpoint count, opens a window with details of the endpoints which are not protected.<br>• When the above features are enabled on all the endpoints, “All Endpoints are Protected” message appears. |
| Infected Endpoints<br>(All Endpoints are Clean) | • Displays number of infected endpoints in last 7 days.<br>Clicking the icon below endpoint count, opens a window with details of the endpoints infected.<br>• When no virus attacks are found, “All Endpoints are Clean” message appears. |

### Status

| Feature | Description |
|---|---|
| Infection Status | Gives a graphical representation of the infection in the network for the selected time period. The graphs can be viewed for the following time periods:<br>• Last 7 Days: Displays the report of the last seven days. |

| | |
|---|---|
| | • Last 15 Days: Displays the report of the last 15 days.<br>• Last 30 Days: Displays the report of the last 30 days.<br>Clicking the data points on the chart, opens a window with details of the endpoints. |
| Update Status | Gives a doughnut chart which displays the number of endpoints on which the virus definitions are up-to-date and not up to date for 1, 3, 7, 15 and 30 days.<br>Clicking the slice of the chart, opens a window with details of the endpoints. |
| Operating System | Gives a doughnut chart which displays the total number of endpoints installed on Windows, Linux and Mac platform.<br>Clicking the slice of the chart, opens a window with details of the endpoints. |
| Managed and Unmanaged Endpoints | Gives a bar graph which displays the number of managed and unmanaged endpoints. This is the enumeration result for the selected clients. For more information, see Enumerate Network.<br>Clicking the bar of the chart, opens a window with details of the endpoints. |
| License Usage Status | Gives two half pie charts, one chart for EPS License and the other for DLP License. The chart displays the number of licenses utilized and licenses remaining.<br>Clicking the slice of the chart, opens a window with details of the license.<br>This widget is not applicable for postpaid clients. |
| Last 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.<br>Clicking the slice of the chart, opens a window with details of the endpoints. |
| Agent Versions | Gives a doughnut chart which displays the agent versions of all the endpoints.<br>Clicking the slice of the chart, opens a window with details of the agent versions. |

## Compliance

| Feature | Description |
|---|---|
| Advanced Device Control | |
| Device Violations | Gives a graphical representation of the device violations on the endpoints for the selected time period. The graphs can be viewed for the following time periods:<br>• Last 7 Days: Displays the report of the last seven days.<br>• Last 15 Days: Displays the report of the last 15 days.<br>• Last 30 Days: Displays the report of the last 30 days.<br>Clicking the data points on the chart, opens a window with details of device violations. |
| Policy violations by Devices | Gives a doughnut chart which displays the number of policy violations by various devices for last 7, 15 and 30 days.<br>Clicking the slice of the chart, opens a window with details of policy violations by selected device. |
| Application Control | |
| Application Violations | Gives a graphical representation of the application violations on the endpoints for the selected time period. The graphs can be viewed for the following time periods:<br>Last 7 Days: Displays the report of the last seven days.<br>Last 15 Days: Displays the report of the last 15 days.<br>Last 30 Days: Displays the report of the last 30 days.<br>Clicking the data points on the chart, opens a window with details of application violations. |
| Policy violations by Applications | Gives a doughnut chart which displays the number of policy violations by various applications for last 7, 15 and 30 days.<br>Clicking the slice of the chart, opens a window with details of policy violations by selected application. |
| Web Security | |
| Blocked Websites | Gives a graphical representation of the Blocked Websites for the selected time period. The graphs can be viewed for the following time periods:<br>• Last 7 Days: Displays the report of the last seven days.<br>• Last 15 Days: Displays the report of the last 15 days. |

| | |
|---|---|
| | • Last 30 Days: Displays the report of the last 30 days. |
| Websites blocked by categories | Gives a doughnut chart which displays the number of Websites blocked by categories for last 7, 15 and 30 days. |
| Assets | |
| Hardware changes | Gives a graphical representation of hardware changes detected on endpoints with Windows and Mac operating systems for the selected time period. The graphs can be viewed for the following time periods:<br>• Last 7 Days: Displays the report of the last seven days.<br>• Last 15 Days: Displays the report of the last 15 days.<br>• Last 30 Days: Displays the report of the last 30 days.<br>Clicking the data points on the chart, opens a window with details of hardware changes. |
| Software changes | Gives a graphical representation of software changes detected on endpoints with Windows and Mac operating systems for the selected time period. The graphs can be viewed for the following time periods:<br>• Last 7 Days: Displays the report of the last seven days.<br>• Last 15 Days: Displays the report of the last 15 days.<br>• Last 30 Days: Displays the report of the last 30 days.<br>Clicking the data points on the chart, opens a window with details of software changes. |

Data Loss Prevention

| Feature | Description |
|---|---|
| DLP Violations | Gives a graphical representation of DLP violations detected on endpoints for the selected time period. The graphs can be viewed for the following time periods:<br>• Last 7 Days: Displays the report of the last seven days.<br>• Last 15 Days: Displays the report of the last 15 days.<br>• Last 30 Days: Displays the report of the last 30 days.<br>Clicking the data points on the chart, opens a window with details of DLP Violations. |

| | |
|---|---|
| Data Leaks through Data Transfer Channel | Gives a doughnut chart which displays the number of data leaks through data transfer channel for last 7, 15 and 30 days.<br>Clicking the slice of the chart, opens a window with details of data leaks by the selected data transfer channel. |
| Type of Data Leaks | Gives a doughnut chart which displays the type of data leaks for last 7, 15 and 30 days.<br>Clicking the slice of the chart, opens a window with details of data leaks by the selected type. |

## Custom Dashboard

You can create your own dashboard as per your requirement. The custom dashboard is displayed by default.

You can include widgets as per your choice. You can set the sequence of widgets as per your requirement.

### Customizing Dashboard

To create your own dashboard, follow these steps:

1. On the Dashboard page, click **Customize Dashboard** option.

   The Customize Dashboard window appears. The list of Unassigned widgets is shown.

   The four Dashboard Views columns are shown with their widgets.

2. Drag and drop the widgets in the Dashboard Views as per your requirement. You can drag the widgets from the Unassigned list and from other dashboard views and drop in the desired view.

3. Click **Save**.

   You can also edit the Dashboard View name.

   The custom dashboard is created.

## User

On the User page you can view the details of the user. Also, you can create a user, and assign user role. You can rename, edit or delete the user. You can enable or disable the user.

You can resend the activation link  to set the password to access the account.

The User page displays the information of all the users in the table format. The table includes information such as Username, User Role, Email, Mobile No., and Status.

You can customize the User table as per column names.

You can search the user with the help of search criteria.

To select all the users from the table, select the check box in the header row.

To select an individual user, select the check box in that row.

On this page, you can carry the following functions:

Adding a User

Deleting a User

Editing a User

Importing a user

Resend Activation Link

### Adding a User

This feature helps you create a user and assign user role.

To add a user, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. Go to **User**. The Users page appears displaying list of users.
3. Click **Add User** button.
4. Click **Add**.

   The Add User dialog appears.
5. Enter **First Name, Last name, Email ID**, and **Mobile No.**
6. Select the **User Role** from the list. The selected role will be assigned to the user. For more information about User Roles, see User Roles.
7. After you assign the User Role, an Email with activation link is sent to the Email ID provided. Click the link to set the password to access your account. The User role can be changed to the other role as and when required.

   If you assign the User Role as **Group Admin**, click **Next**.

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. One group can have multiple Group Admins.

8. Click **Add**.

If you assign the User Role other than User, an Email with activation link is sent to the Email ID provided. Click the link to set the password to access your account. The User role can be changed to the other role as and when required.

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

When you log on to Seqrite Endpoint Security Cloud as Group Administrator, the Status page is displayed by default. Only pages having privileges for Group Admin are displayed.

## Enabling a User

To enable a user, follow these steps:

1. 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. 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**.

The selected user is disabled.

Note

The disabled user cannot log on the Seqrite Endpoint Security Cloud portal.

## Deleting a User

To delete the user, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to User. The Users page appears displaying 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. Select **Submit** Button.
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.

If you delete the Group Admin, the policies created by the Group Admin cannot be deleted if the policies are assigned to any group and endpoints.

## Editing the User

Here you can edit the user information. You can edit name, Email address or mobile number of the user. You can also change the user role. If you change the role to Group Admin, you can assign group.

To edit the user, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to User. The Users page appears displaying list of users.
3. Click the **Edit** icon of the user that you want to edit.

   The Edit User dialog appears.
4. Edit the information.

   If you assign the User Role as **Group Admin**, click **Next**.

   In the dialog, a list of groups appears. A group without Group Admin is only available. Select the group to be assigned to the Group Admin. Only one group can be assigned to the Group Admin.
5. Click **Save**.

   User information is updated.

Note

You cannot edit or delete the default user.

## 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 Seqrite Endpoint Security Cloud.

2. Go to Users. The Users page appears displaying list of users.
3. Click Add User > Import.

   In the Import User dialog, import a CSV file by clicking **Browse**. The file size must be less than or equal to 1 MB. The CSV file content should be in the following format:

| First Name | Last Name | EMAIL | Country Code | MOBILE NUMBER | User RoleName |
|---|---|---|---|---|---|
| aaa | bbb | aaa@mail.com | +91 | 1111111111 | ADMIN |
| ccc | ddd | ccc@mail.com | +44 | 2222222222 | REPORT_ONLY |
| mmm | nnnn | mmm@mail.com | + 1 | 3333333333 | ADMIN |

   As you can see in the above example, the Country Code should contain + sign.

   The User Role name (REPORT_ONLY, ADMIN) should be in Capital letters.

4. Click **Import**.

### Resend the activation link

For the User Roles, Administrator and Report Viewer, an Email with activation link can be sent to the Email ID provided. User need to click the link to set the password to access the account. The link is valid for specific period only. If the link expires or user does not receive the Email, you can resend the activation link.

To resend the activation link, follow these steps:

1. Lon to Seqrite Endpoint Security Cloud.
2. Go to User. The Users page appears displaying list of users.
3. Select the check box of the user to which you want to send the activation link. An action bar is enabled above the table.
4. Select **Resend Activation Link**.
5. Click **Submit** button.
6. The confirmation message appears. Click **Yes**.

   The activation link is sent to the selected user.

## Groups

On the Groups page, you can view, create, and manage groups and subgroups. In the left pane, a tree like structure of groups and subgroups is displayed. The synchronized groups with Active Directory have AD tag in their name. In the right pane, the group name and number of endpoints assigned to that group is displayed. One group may have multiple Group Admins. Names of Group Admins are also displayed. You can edit Group Admin.

In the ‘Assigned policies to the group’ section, a table shows the assigned policies to the selected group. The policy applied on the group is applicable to all the endpoints within the group.

This feature helps you create groups and subgroups and apply a policy to a group (or a subgroup). You can delete or rename a group or set different policies for different groups. You can also change Group Admin of the group.



## Adding a Group

To add a new group, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Groups.
3. Select the root if you want to create the new group at the root level. Select a group to create subgroup.
4. Click the **Add Group** button.

   The Add Group screen appears.
5. In the Group Name text box, type a group name.
6. Select the policy for endpoint from the list.
7. Click **Add**.

   The new group/subgroup is added.

Note

No subgroup can be created under the Default group.

## Setting Policy to a Group

Policies may include different client settings for different groups in an organization.

If the policy is pushed from MSSP, it will get applied on default EPS group and that policy will be read only.

To set a policy to a group, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Groups.
3. In the left pane, select a group to apply the policy. The list of policies for endpoints is displayed.

4. To change the policy, click Change Policies option. The Change Computer Policies dialog appears.
5. In the Default Policies tab, select the policy that you want to apply.
6. In the Override Policies tab, select the features for which you want to override the policy.
7. Click **Assign**.

   The policy is applied to the selected group.

   The policy created by Super Admin or Admin when applied on the group is read only for Group Admin.

For more information about policies, see Policies.

## Deleting a Group

To delete a group/subgroup, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Groups.
3. In the left pane, select a group/subgroup.

   Note

   You cannot delete the group if Group Admin is assigned to that group.
4. In the right pane, click the Delete button.

   A confirmation message is displayed.
5. Click **Yes**.

   The selected group/subgroup is deleted.

If you delete the group, all the subgroups available under that group will be deleted. The endpoints assigned to the subgroup and groups will be moved to Default group. The policy of default group is applied on the moved endpoints except the feature policy assigned on the endpoint.

If you delete the subgroup, the endpoints assigned to the subgroup will be moved under its parent group and policy of parent group is applied on the moved endpoints except the feature policy assigned on the endpoint.

## Moving Group

To move a group/subgroup, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Groups.
3. In the left pane, select a group/subgroup. Drag the group to a desired group where you want to move.

The endpoints and policies associated with the group remain the same, but under new parent group.

## Renaming a Group

To rename a group, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Groups.
3. In the left pane, select a group/subgroup to rename. The Group details appears in the right pane.
4. Click the edit icon in the Group Name. Edit the Group Name.
5. To save changes, click the tick mark.

The group/subgroup name is modified. However, the policy applied earlier to this group does not change. To change a policy, you have to apply a new policy.

## Changing Group

To change a group/subgroup assigned to Group Admin, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Groups.
3. In the left pane, select a group/subgroup.
4. In the right pane, the details of the group appear. The names of Groups Admins with edit icon appears. Click the edit icon of the Group Admin that you want to change.
5. The Change Group dialog appears. 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. One group can have multiple Group Admins.
6. Click **Apply**.

   The changed group is assigned to the Group Admin.

## Status

The Status page displays the current status of all the endpoints of the selected group. The status includes information such as the endpoint name, group name, domain name, IP and MAC addresses, etc. Endpoint Status column provides information whether the endpoint is online or offline. Endpoint status is changed to offline according to set missed heartbeat count to turn endpoint offline. For more details, see Admin > Settings.

The following options help to customize and search the desired endpoints:

- Columns: You can use this option to customize the status list as per column names.
- Filter by: You can use this option to filter the status list according to the Operating Systems platforms and Endpoint with DLP. The legend for DLP License Assigned is displayed for the respective endpoints.
- Endpoint Name: You can use this option to search the endpoints with different parameters.

You can initiate client actions by selecting the endpoint. The list of client actions is OS specific.

To select all the endpoints from the list, select the check box in the header row.

To select an individual endpoint, select the check box in that row.

### Viewing status of selected endpoint

To view status of an endpoint, click the name of the endpoint for which you want to view the status. The Endpoint Status page appears displaying detailed status of the endpoint. For more details, see Endpoint Status.

## Update Agent

Update Agent helps you to download and manage the updates for Seqrite Endpoint Security Cloud. It provides you the flexibility to download the updates on a single machine. All the Seqrite Endpoint Security clients fetch the updates from this centralized location. It also provides the facility of automatically updating Seqrite Endpoint Security for enhancements or bug fixes.

### Viewing Update Agent Status

You can view information of all types of updates downloaded by the Update Agent.

To view the update agent status, follow these steps:

1. On the Status page, identify and click the endpoint name with update agent role.
2. The Endpoint Status page appears. You can see the label as Update Agent. Click the Switch to Update Agent button.
3. The Update Agent page appears. The endpoint name and IP address of the endpoint where update agent is installed is displayed.

4. In the Status tab, the status of the update Agent is shown in the tabular format with the following details:

| Fields | Description |
|---|---|
| Product Name | Displays the name of the Seqrite product for which update can be downloaded. |
| Version | Displays the version of the Seqrite product. |
| Service Pack | Displays information about the service pack. |
| Virus Database Date | Displays the updated Virus Database date. |

A label 'Outdated' is displayed for the product only if the product is not updated since last 72 hours.

5. You can do one of the following:
   - **Update Now** - Click this button to send a Notification to the Update Agent to download the updates.
   - **Rollback** - Click this button to take the Update Agent back to the previous update state.

### Update Agent Settings

To do the update agent setting, follow these steps:

1. On the Status page, identify and click the endpoint name with update agent role.
2. The Endpoint Status page appears. You can see the label as Update Agent. Click the **Switch to Update Agent** button.
3. The Update Agent page appears. The endpoint name and IP address of the endpoint where update agent is installed is displayed.
4. In the **Settings** tab, you can see the following list of settings with expand sign and toggle button. Expand and enable settings.
   - Update Settings
   - Proxy Settings
5. To save the changes, click **Save**.

### Update Settings

1. Under Update Type, you can select either of the following update options:

- **Automatic**: Select this option to enable automatic update of Seqrite Endpoint Security Cloud. However, this feature is enabled by default. It is recommended that you do not disable this feature.

- **Custom**: If you select this option, configure the following options:
    i. In **Frequency**, select either the Daily or Weekly option. If you select the Weekly option, select the weekday from the list.
    ii. In **Start At**, set time in hours and minutes.
    iii. If you want to repeat the update of the Update Agent, select the Repeat Update check box and set the frequency in hours to repeat the update.

2. Select the update mode from the following options:

- **Download from Internet Center**: Helps you download the updates from the default Internet Center.
- **Download from Specified URL**: Helps to obtain the updates from a specified endpoint that has the updates downloaded by the connected system.
    i. In the **Server** text box, type the URL.
    ii. In the **Port** text box, type the port number.
    The msg32.htm file should be present at the update location in the system with Internet connection.
    To create the msg32.htm file, rename a text file as msg32.htm file.
- **Pick from specified path**: Helps you pick the updates from a specified local folder from your computer without Internet connection. You can specify the path of the local folder from where the updates are to be copied.
    For example, if you have downloaded the updates on other system, you can copy them into a CD/DVD or pen drive and then paste in the local folder. Update Agent will fetch the updates from this local folder path.
    i. Select the **Pick from specified Path** option.
    ii. Type the path to the folder from where the updates need to be copied.

3. Select the updates available for download from the list.
4. Under Other Settings, select the **Download the endpoint security service pack** check box. This feature is enabled by default.
5. Select the **Always take backup before downloading new update** check box. Helps you take the backup of the existing updates before new updates are downloaded. These backups are used in case a rollback to previous update is required. This feature is enabled by default.
6. Select the **Restrict download speed (kbps)** check box if you want to restrict the download speed. Enter the speed in the text box.
7. Select the **Delete report after** check box. This helps you delete the reports as per the time interval selected by you. This feature is enabled by default. The default value of time interval is 10 days.
8. Verify the path mentioned in Download updates to box. All the Seqrite Endpoints Security products will take the updates from this centralized location.

### Proxy Settings

1. Select Proxy Type from the list.
2. In the **Server** text box, type the IP address of the proxy server or domain name (Example: proxy.yourcompany.com).
3. In the **Port** text box, type the port number of the proxy server (Example: 80).
4. Under Authenticate in case of firewall or proxy server section, type your logon credentials in the **Username** and **Password** boxes to authenticate.
5. To save the changes, click **Save**.

## Action Log

### View Action Log of selected endpoint

You can view the action log (history) of all actions performed on the endpoints. To view the action log, click the row of the endpoint for which you want to view the history. The action log appears in the lower pane of the page in the tabular format. The Action Status column displays the corresponding status of the action. The status and meanings are as follows:

- Queued – After initiating, the action is in the queued state until the endpoint pulls the action.
- Success – The initiated action has been reached the endpoint. The endpoint has acknowledged the request to the server.
- Skipped – The multiple requests for the same action are skipped.
- Failed –The scenario can be one of the following:
    - The similar action is in progress at the endpoint side.
    - The antivirus is not installed so cannot carry the selection action.
    - The action is not applicable for the selected endpoint.

By default, you can view the action log of last 7 days. You can view the log for last 3,7, and 15 days by selecting the dropdown list.

The activity logs will be deleted as per settings done in Admin > Settings.

Note:

If the antivirus is not installed, the action logs about only the following actions are displayed:

- Enumerate Network
- Remote Uninstall
- Remove selected endpoints
- Temporary Device Access

Provides the facility of automatically updating Seqrite Endpoint Security Cloud for enhancements or bug fixes.

## Endpoint Status

You can keep a watch on the system information, hardware information, and software installed. You can also view the hardware changes, if any, that are made to the configuration of the systems in your network. You can also keep a tab on the list of the endpoints where the changes have been carried out.

To view status of an endpoint, click name of the endpoint for which you want to view the status. The Endpoint Status page appears displaying detailed status of the endpoint.

The System Details tab displays the system information in detail. OS Product key of the Windows OS appears.

Note

The OS Product key is available only in the clients with Windows Vista and above operating systems.

The Hardware and Software details tab will be displayed only after Asset scan. For more information, see Asset Management.

The Hardware Details tab displays the hardware information in detail.

The Software details tab displays the details of software installed on the system.

Note

The MS Office Product key is available only for MS Office 2010 and above.

The Product key of MS Office is not available in the clients with MAC operating system.

The license status of MS Office appears in the License column.

The following table mentions possible License status and their description in the tooltip for MS Office.

| License status | Description |
|---|---|
| Unlicensed | The product is not licensed. |
| Licensed | The product is licensed. |
| OOBGrace | The MS Office license is in the grace period. |
| OOTGrace | The MS Office license requires reactivation. |
| NonGenuineGrace | The MS Office license has failed online validation and is in the grace period. |
| ExtendedGrace | The grace period of the MS Office license is extended. |

| | |
|---|---|
| Notification | The MS Office license is either out of the grace period or failed validation. |

## Export

1. To export status in the CSV format, click **CSV** button.

   Export To CSV File dialog appears.

2. Select one of the following,

- Export data displayed on Status page only. If you select this option, <client>.csv is downloaded.
- Export comprehensive data of endpoints listed on Status Page. The data includes System details, Software and Hardware details and System User Details. If you select this option, Comprehensive Asset Reports zip file is downloaded.

3. Click **Export**.

## Client Action

Using the options in the Client Action list, you can perform different actions on the endpoints.

You can remotely initiate scan for individual endpoints or endpoints in a group, customize scan settings, and stop scanning as per your preference. You can improve the performance of your endpoints by initiating Tune-up scan which can clean up disk space, registry entries, and schedule defragmentation at next boot. You can update the Seqrite Endpoint Security Cloud virus database for the endpoints.

The following table shows a comparison of the features in Client Action that are applicable for different Seqrite Endpoint Security clients on different operating systems:

| **Features** | **Clients** | | |
|---|---|---|---|
| | **Windows** | **Mac** | **Linux** |
| Scan | ✓ | ✓ | ✓ |
| Update | ✓ | ✓ | ✓ |
| Tuneup | ✓ | **X** | **X** |
| Temporary Device Access | ✓ | ✓ | **X** |
| Enumerate Network | ✓ | **X** | **X** |

| | | | |
|---|---|---|---|
| Remote Uninstall | ✓ | ✓ | ✓ |
| DLP | ✓ | ✓ | X |
| Update Agent Role | ✓ | X | X |
| Delete Backup Data | ✓ | X | X |
| Assign Custom Policy | ✓ | ✓ | ✓ |
| Upgrade Clients | ✓ | ✓ | X |
| Application Control | ✓ | X | X |
| Move to Group | ✓ | ✓ | ✓ |
| Remove Selected Endpoint(s) | ✓ | ✓ | ✓ |

The **Client Actions** button helps you to initiated actions on the selected endpoints.

The following actions you can perform on the selected endpoints:

Scan

Update

Tuneup

Temporary Device Access

Enumerate Network

Remote Uninstall

DLP

Update Agent Role

Delete Backup Data

Assign Custom Policy

Upgrade Clients

Application Control

Move to Group

Remove selected endpoints

### Scan

This feature allows to initiate scanning on remote endpoints. You can initiate a manual scan with preconfigured policies or custom scan. This feature reduces the additional task of personally overseeing each target endpoint.

To initiate scanning, follow these steps:

1. On the Status page, select the endpoints you want to scan.
2. The client action bar is enabled above the table. In the Client Actions dropdown, select **Scan**.
3. In the Please Select list, select **Start Scan**.
4. Click **Submit**.
5. Start Scan dialog appears.
6. Click **Start Scan** to start the scan of the selected endpoints. The action will be initiated on the client as per set polling interval.

   You can stop scanning by clicking **Stop Scan** at any time you prefer.

   You can customize the scan settings if required.
7. To customize the scan settings, click Scan Settings.
8. In the Scan Settings section, do the following:
   i. In Scan type section, select either Quick Scan or Full System Scan. Quick Scan includes scanning of the drive where operating system is installed, and Full System Scan includes scanning of all fixed drives.
   ii. Select Scan Priority. The Scan Priority is Normal by default. You can change the priority to Low or High, if required.
   iii. Select either **Automatic** or **Advanced** scan mode.

   Automatic scanning involves optimum scanning and is selected by default.

   When the Advanced scan mode option is selected, all the related attributes get enabled. Do the following:

   a. From the Select the items to scan options, select either Scan executable files option or Scan all files option. Scanning of all files takes a longer time.
   b. The Scan packed files and Scan archive files check boxes are selected, by default. You can select the Scan mailboxes checkbox if required.
   c. In Archive Scan Level, set the scan level.

      You can set the level for scanning in an archive file up to 16. The default scan level is 2. Increasing the default scan level may affect the scanning speed.

d. To remove an infected file from your system, Select action from the dropdown list:

   Select action when a virus is found in the archive file, whether you want to delete, quarantine, or skip the file.

   Select action when a virus is found in your active folder/drives, whether you want to delete, quarantine, or skip the file.

iv. Under Antimalware Scan Settings, Perform Antimalware scan is selected, by default.

v. Select action when a malware is found, whether you want to clean or skip the file.

   The action selected here will be taken automatically.

vi. Under Boot Time Scan Settings, select **Perform Boot Time Scan** check box.

   The Select Boot Time Scan Mode option is activated.

   Select one of the following scan options:

   - Quick Scan
   - Full System Scan

vii. After configuring the scan setting, click **Apply Settings**.

The new setting is applied. You can reset the Scan setting to default with Reset to Default button, if required.

Note

Scan packed files, Scan mailboxes, Antimalware Scan Settings, and Boot Time Scan Settings are available only in the clients with Windows operating systems.

Notification for Scan from the Seqrite Endpoint Security Cloud console will not be sent if the user is not logged on to the Mac system.

### Update

Seqrite releases updates regularly to fix technical issues and provide protection against new threats. Hence, it is recommended that you update the virus definitions of your software protection regularly. Using this feature, you can take the update remotely.

To take the update, follow these steps:

1. On the Status page, select the endpoints you want to update.
2. The client action bar is enabled above the table. In the Client Actions list, select Update.
3. Click **Submit**. The action will be initiated on the client as per the set polling interval.

The selected endpoints are updated with the latest virus definitions.

### Tuneup

This facility improves the performance of the endpoints by defragmentation and by cleaning unwanted and junk files and invalid and obsolete registry entries. While you work in applications, computers write junks on the drives or when you visit any Websites, the temporary files are created on your computer. Such junks and files occupy spaces in the

memory resulting in slowing down of the endpoints. Tuning up your computers cleans up these files by improving their performance.

Tuneup settings allow you to carry out different types of clean-ups such as; disks, registry entries, or schedule a defragmentation at next boot.

**Disk Cleanup**: Helps you find and remove invalid and unwanted junk files from the hard disk. These files consume hard disk space and slow down the system considerably. Disk Cleanup deletes these files and provide free space that can be used for other applications and helps in improving system performance. This feature also deletes temporary files, Internet cache files, improper shortcut files, garbage name files, and empty folders.

**Registry Cleanup**: Helps you remove invalid and obsolete registry entries from the system, such entries may appear due to improper uninstallation, non-existent fonts, etc. Sometimes during uninstallation, the registry entries are not deleted. This leads to slower performance of the system. The Registry Cleanup removes such invalid registry entries to increase the performance of the system.

Defragment: Helps you defragment vital files, such as page files and registry hives for improving the performance of the endpoint. Files are often stored in fragments in different locations slowing down the system performance. Defragmentation reduces the number of fragments and clubs all the fragments into one contiguous chunk to improve your endpoint performance.

Note

The Tuneup feature is available only in the clients with Windows Desktop operating systems.

The Tuneup feature is not available for Windows Server operating system.

To tune up the endpoints, follow these steps:

1. On the Status page, select the endpoints you want to tuneup.
2. The client action bar is enabled above the table. In the **Client Actions** dropdown, select Tuneup.
3. In the **Please Select** dropdown, select **Start Scan**.
4. Click **Submit**.

Start Scan dialog appears.

Click **Start Scan** to start the scan of the selected endpoints. The action will be initiated on the client as per set polling interval.

Tuneup notifications are sent to the selected endpoints and tune up is performed on those endpoints.

You can stop Tuneup activity by clicking **Stop Scan** at any time you prefer.

You can customize the Tuneup settings if required.

5. To customize the Tuneup settings, click **Tuneup Settings**.

6. Select any of the following:
   - Disk Cleanup
   - Registry Cleanup
   - Defragment at next boot

   However, all these options are selected by default.
7. To save your settings, click **Apply Changes**. You can reset the Tuneup settings to default with Reset button, if required.

### Temporary Device Access

This feature allows you to permit temporary access to a device on the client for a specific period. If a user wants temporary access to a device on the client, the user can send a request to the Administrator to grant temporary access. The Administrator will generate OTP and will share with the user. The client uses this OTP to access the device for the specific period.

To enable Temporary Device Access, follow these steps:

1. On the Status page, select the endpoints to send the temporary device access request.
2. The client action bar is enabled above the table. In the Client Actions list, select **Temporary Device Access**.
3. Click **Submit**.
4. On the Temporary Device Access dialog, in the Allow temporary access for list, select minutes.
5. In the Use OTP within list, select minutes.
6. Click **Generate OTP**. The OTP appears.
7. Click **Notify By Emai**l and the email containing the OTP is automatically received by the client. Temporary access is allowed as per the settings effective from that minute. The action will be initiated on the client as per set polling interval.

At the client side, after successful validation of the OTP, temporary device access is enabled for the specific period.

### Enumerate Network

This feature allows you to get a list of all the unmanaged endpoints available in the client network.

To generate a list of unmanaged endpoints, follow these steps:

1. On the Status page, select the endpoints to send the request.
2. The client action bar is enabled above the table. In the Client Actions list, select **Enumerate Network**.
3. Click **Submit**. The action will be initiated on the client as per set polling interval.

The enumeration result will appear on the EPS console dashboard based on the Heartbeat interval set for the client. You can view the enumeration results on the dashboard widget only.

### Remote Uninstall

With Remote Uninstall, you can initiate remote uninstallation of Seqrite client along with the antivirus program from the computers on your network.

To uninstall the client through Remote Uninstall, follow these steps:

1. On the Status page, select the endpoints you want to uninstall.
2. The client action bar is enabled above the table. In the Client Actions list, select **Remote Uninstall**.
3. In the Please Select dropdown, select **Start**.
4. Click **Submit**.

The uninstallation initiates on the selected endpoints as per set polling interval.

To stop the remote uninstallation, In the Client Actions list, select Remote Uninstall > Stop.

Click **Submit**. The Stop command will be executed only if the uninstallation is not started.

### DLP

#### Assign DLP License

This feature allows you to assign Data Loss Prevention (DLP) license to the selected endpoint.

To assign the DLP license, follow these steps:

1. On the Status page, select the endpoints you want to assign the DLP license.
2. The client action bar is enabled above the table. In the **Client Actions** list, select **DLP**.
3. In the Please Select dropdown, select **Assign DLP License**.
4. Click **Submit**.
5. A confirmation message appears. Click **OK**.

The DLP license is assigned to the selected endpoint. On the Status page, the legend for DLP License Assigned is displayed for the respective endpoints.

#### Revoke DLP License

This feature allows you to revoke the DLP license to the selected endpoint.

To unassign the DLP license, follow these steps:

1. On the Status page, select the endpoints you want to unassign the DLP license.
2. In the Client Actions dropdown, select **DLP**.
3. In the Please Select dropdown, select **Revoke DLP License**.

4. Click **Submit**.
5. A confirmation message appears. Click **OK**.

The DLP license is unassigned to the selected endpoint.

**Data-At-Rest Scan**

Using Data-At-Rest Scan, you can scan and detect any confidential data present in your endpoints and removable devices. You can scan the desired location such as; drive, folder, or removable devices on the endpoints and detect the confidential or sensitive information present. You can view the information related to the detected confidential data such as; the file path, threat type, and matched text.

Note

To perform Data-At-Rest scan, you must enable DLP on the endpoints.

**Start Data-At-Rest scan**

To initiate scanning, follow these steps:

1. On the Status page, select the endpoints you want to scan.
2. The client action bar is enabled above the table. In the Client Actions list, select **DLP.**
3. In the Please Select dropdown, select Start Data-At-Rest Scan.
4. Click **Submit**.

   Start Scan dialog appears.

   Click **Start Scan** to start the scan of the selected endpoints. The action will be initiated on the client as per set polling interval.

   The selected endpoints are scanned for compliance.

   You can customize the Data-At-Rest scan settings if required.

**Customize the DAR scan settings**

To customize the DAR scan settings, click **Data-At-Rest Scan Settings** and select one of the following:

- Quick Scan: Select this option to scan the drive on which your operating system is installed.
- Full System: Select this option to scan all the drives.
- Scan Specific Folder(s): Select this option to scan a particular folder(s). To scan specific folder, follow these steps:
  i. Click **Configure**.
  ii. Enter the path of the folder that you want to scan.
  iii. Click **Add**.
  iv. You can also choose to scan the subfolders by selecting the Include Subfolder check box.
  v. You can also remove a path from the list by clicking **Delete**.
  vi. Click **Apply**.

vii. Select **Scan Priority**. The Scan Priority is Normal by default. You can change the priority to Low or High, if required.

viii. In the Select data to scan section, click the **File Types** tab.

ix. Select the file types (format) that you want to scan.

x. Click the **Confidential Data** tab.

xi. Select the Confidential Data to scan.

xii. Click the **User Defined Dictionaries** tab and select the User Defined Dictionaries to scan.

xiii. Click **Apply Changes**.

You can reset the DAR scan settings to default with Reset button, if required.

xiv. Click **Start Scan**.

Note

Email Notifications are not supported for Data-At-Rest Scan feature.

Data-At-Rest Scan feature will be available only if DLP feature pack is enabled for that EPS server.

**Exclusion**

You may exclude folders for scanning.

To exclude the folder, enter the name of the folder in the text box and click **Add**.

To remove the folder from the excluded folders list, select the folder from the list and click **Delete**.

**Stop Data-At-Rest scan**

To stop Data-At Rest scanning, follow these steps:

1. On the Status page, select the endpoints you want to stop Data-At-Rest scan.
2. The client action bar is enabled above the table. In the Client Actions list, select **DLP.**
3. In the Please Select dropdown, select **Stop Data-At-Rest Scan.**
4. Click **Submit**.

The Stop command has been sent.

### Update Agent Role

This feature allows you assign update agent role to the selected endpoint. The Update Agent downloads and manages the updates for Seqrite Endpoint Security Cloud. The Update Agent provides you the flexibility to download the updates on a single machine. All the Seqrite Endpoint Security clients fetch the updates from this centralized location. It also provides the facility of automatically updating Seqrite Endpoint Security clients for enhancements or bug fixes.

To assign the update agent role, follow these steps:

1. On the Status page, select the endpoints you want to assign the update agent role.

2. The client action bar is enabled above the table. In the Client Actions dropdown, select **Update Agent Role**.
3. In the Please Select dropdown, select **Assign**.
4. Click **Submit**.
5. A confirmation message appears. Click **OK**.
6. The update agent role is assigned to the selected endpoint. On the Status page, the legend for Update Role Assigned is displayed for the respective endpoint.

**Revoke Update Agent Role**

This feature allows you to revoke the update agent role for the selected endpoint.

To revoke the update agent role, follow these steps:

1. On the Status page, select the endpoints for which you want to revoke the update agent role.
2. In the Client Actions dropdown, select **Update Agent Role**.
3. In the Please Select dropdown, select **Revoke**.
4. Click **Submit**.
5. A confirmation message appears. Click **OK**.

The update agent role is revoked for the selected endpoint.

### Delete Backup Data

Data Backup feature automatically takes a backup of  files for ransomware protection. This feature takes backup as per predefined configuration in the Miscellaneous policy. Here you can delete the backup data. For more information, see Miscellaneous policy.

To delete Backup Data, follow these steps:

1. On the Status page, select the endpoints for which you want to delete the backup data.
2. The client action bar is enabled above the table. In the Client Actions list, select **Delete Backup Data**.

   In the Miscellaneous policy, the current option you have selected for Backup location is where your current backup data gets stored on the endpoint.

   The backup data stored at the location other than current location is old backup data.
3. In the **Please Select** list, select one of the following:
   - **Old Backup Data** - If you select this option, the old backup data will be deleted.
   - **Current Backup Data** - If you select this option, the current backup data will be deleted.

Note

You cannot delete backup data stored at Network Path Location.

4. Click **Submit**. The action will be initiated on the client as per the set polling interval.

   The backup data will be deleted.

### Assign Custom Policy

This feature allows you to assign custom policy to the selected endpoint. You can override the settings of Container policy by selecting the custom policies.

To assign custom policy, follow these steps:

1. On the Status page, select the endpoints you want to assign the policy.
2. The client action bar is enabled above the table. In the Client Actions list, select **Assign Custom Policy**.
3. Click **Submit**. The Assign Custom Policy dialog appears.

The list of custom policies appears. Select the policies and click **Assign**.

The policies are assigned to the selected endpoint. You can view the assigned policies on the Status page and in the Assign Custom Policy dialog.

### Upgrade Clients

To upgrade the clients, follow these steps:

1. On the Status page, select the endpoints you want to upgrade the clients.
2. The client action bar is enabled above the table. In the Client Actions list, select **Upgrade Clients**.
3. Click **Submit**. The action will be initiated on the client as per the set polling interval.

   The client will be upgraded with the latest version.

### Application Control

This feature allows you to check whether security compliance policies framed by your organization are being followed on each endpoint. It also helps you in verifying whether endpoints have any unauthorized applications other than the authorized ones running on them.

The Application Control scan is done in the following two ways,

1) When you request the scan through Client Action. For details, see Application Control Scan.

2) When you set the Application Control policy. 'On access' reports are generated in this case. For details, see Application Control policy.

**Application Control Scan**

To initiate scanning, follow these steps:

1. On the Status page, select the endpoints you want to scan.
2. The client action bar is enabled above the table. In the Client Actions dropdown, select Application Control.
3. In the Please Select list, select **Start Scan**.
4. Click **Submit**.

   Start Scan dialog appears.
5. Click **Start Scan** to start the scan of the selected endpoints. The action will be initiated on the client as per set polling interval.

   You can stop scanning by clicking Stop Scan at any time you prefer.

   You can customize the scan settings if required.
6. To customize the scan settings, click Application Control Settings.
7. Select one of the following scan options:
   - Unauthorized applications: Helps you initiate scanning only for the unauthorized applications present on a client machine.
   - Unauthorized and authorized applications: Helps you initiate scanning for both, unauthorized and authorized applications present on the client machine.
   - All installed applications: Helps you initiate scanning for all applications installed on a client.

   Scanning by first two options may take longer time.
8. Select Scan Priority. The Scan Priority is Normal by default. You can change the priority to Low or High, if required.
9. After configuring the scan setting, click **Apply Changes.**

The new setting is applied. You can reset the Scan setting to default with Reset button, if required.

### Move to Group

This feature allows you to move the selected endpoint to a group.

To move the endpoint, follow these steps:

1. On the Status page, select the endpoints you want to move.
2. The client action bar is enabled above the table. In the Client Actions list, select **Move to Group**.
3. Click **Submit**. The Assign to Group dialog appears.
4. Select a group/subgroup where you want to move the selected endpoint.

5. Click **Move**.
6. A confirmation message appears. Click **OK**.

The policies of the parent group are applied to the moved endpoint.

### Remove selected endpoints

This feature allows you to remove the clients from a group.

To remove the client, follow these steps:

1. On the Status page, select the endpoints you want to remove.
2. The client action bar is enabled above the table. In the Client Actions dropdown, select **Remove Selected Endpoint(s)**.
3. Click **Submit**.
4. A confirmation message appears. Click **OK**.

The endpoints are removed.

## Deployment

The Deployment page helps you to deploy the Endpoint Security client on different endpoints.

### Deployment Methods

Select one of the following methods to deploy the Endpoint Security client as applicable. A brief about each method is mentioned below.

Online Installer: Create and download client installer for manual installation.

Standalone Installer: Download Standalone Installer and then create a client installer.

Email Install Link: Send e-mail notification containing URL to install the client.

Remote Installer: Download Remote Installer, which helps you to remotely deploy Seqrite Endpoint Security clients on Microsoft Windows and Mac endpoints.

Active Directory: Download Active Directory Tool, which helps you to deploy Seqrite Endpoint Security clients with help of active directory synchronization.

The following table shows different operating systems that support the client deployment methods:

| Features | Clients | | |
|---|---|---|---|
| | Windows | Mac | Linux |
| Online Installer | ✓ | ✓ | ✓ |
| Standalone Installer | ✓ | ✓ | ✓ |

| | | | |
|---|---|---|---|
| Email Install Link | ✓ | ✓ | X |
| Remote Installer | ✓ | ✓ | X |
| Active Directory | ✓ | X | X |

This page helps you to create and download the Client Installer for manual installation of client on different endpoints.

## Automatic uninstallation of EPS clients

If you start deploying client on the endpoints which already has on-premises EPS client, the on-premises client will be uninstalled, and Seqrite Endpoint Security client will be installed on the endpoint.

This feature is available in the clients with Windows and Mac operating systems.

**Supported EPS versions**

Windows client - EPS version 6.0 and later

Mac client - EPS version 6.4 and later

## System Requirements

For Installing Seqrite Endpoint Security client through client install utility, the System requirements are as follows:

- Minimum 3.10 GB free hard disk space
- Internet Explorer 7 or above
- Any one of the following operating systems:
    - Windows OS
        - Microsoft Windows XP SP3 (32-bit)
        - Microsoft Windows Vista Home Basic/ Premium / Business / Enterprise / Ultimate (32-bit/64-bit)
        - Microsoft Windows 2008 Server R2 Web / Standard / Enterprise / Datacenter (64-bit)
        - Microsoft Windows 2008 Server Web / Standard / Enterprise (32-bit/64-bit) / Datacenter (64-bit)
        - Microsoft Windows 7 Home Basic/ Premium / Professional / Enterprise / Ultimate (32-bit/64-bit)
        - Microsoft Windows SBS 2011 Standard / Essentials
        - Microsoft Windows Server 2012 R2 Standard / Datacenter (64-bit)
        - Microsoft Windows Server 2012 Standard / Essentials / Foundation / Storage Server / Datacenter (64-bit)
        - Microsoft Windows 8 Professional / Enterprise (32-bit/64-bit)
        - Microsoft Windows 8.1 Professional / Enterprise (32-bit/64-bit)

        - Microsoft Windows 10 Home / Pro / Enterprise / Education (32-Bit / 64 -Bit)
        - Microsoft Windows Server 2016
        - Microsoft Windows Server 2019 (64-bit)
        - Windows 10 November 2019 Update
    - Mac
        - Mac OS X 10.9 to MacOS 10.15
    - Linux 32 bit
        - BOSS 6
        - Fedora 14, 18, 19, 20, 21, 22, 23, 24, 25
        - openSUSE 11.4, 12.2, 12.3, 13.2, 42.2
        - Linux Mint 13, 14, 15, 16, 17.3, 18
        - Ubuntu 10.10, 11.4, 12.04 LTS, 12.04.3 LTS, 13.04, 13.10, 14.04, 14.10, 15.04, 16.04 LTS, 16.10
        - CentOS 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9
        - RHEL 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9
    - Linux 64 bit
        - Fedora 14, 18, 19, 20, 21, 22, 23, 24, 25
        - openSUSE 11.4, 12.2, 12.3, 42.3
        - Linux Mint 13, 14, 15, 16, 17.3, 18
        - Ubuntu 10.10, 11.4, 12.04.2 LTS, 13.04, 13.10, 14.04, 14.10, 15.04, 16.04 LTS, 16.10, 17.04
        - CentOS 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 7.0
        - RHEL 6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 7.0, 7.1, 7.2, 7.3
        - SUSE Linux 11.00, 12.00, 12.2
        - Amazon Linux 2

Note

- For Windows 2016 Server and Windows 2019 Server, uninstall Windows Defender before installing Seqrite EPS client.
- If you are upgrading the EPS client to Windows 2016 Server or Windows 2019 Server, uninstall Windows Defender after upgrade.

## Online Installer

This tab displays the default client installer packages in table format.  There are default installers for different operating systems. You can download the installer, if it matches your system requirements.

### Online Installer

The Online Installer will take you to next dialog to build Client Installer set up. This may take a longer time to download the Client Installer set up.

To create a new client installer, follow these steps:

1. Click the **Create Client Installe**r button to create the Client Installer.
2. In the Create Client Installer window that opens, enter the required information in the Create Installer, Proxy Settings, Set Password tabs.
3. Click **Create**.

   The Client Installer is ready for download.
4. To install Seqrite Client, see Installing Seqrite Client.

## Standalone Installer

The standalone installer will download a Client Installer. If network speed is slow and you want to create client installer faster, use this option. This requires at least one system with Windows platform.

To create a new client installer, follow these steps:

1. Click Standalone Installer button.
2. The Client Installer zip file is downloaded. Extract the files.
3. Execute the Installer.
4. In the Client Installer, enter the required information in the **Create Installer, Proxy Settings** and **Password** tabs.
5. Click **Create**.

   A help file is provided in the Client Installer.

   To install Seqrite Client, see Installing Seqrite Client.

## Email Install Link

This facility allows you to send an email with a Client Installer download link for client installation to the endpoints.

To send Email with the link, do the following,

1. In the To text box, enter the Email address.
2. Click Send Email. A confirmation message appears.
3. Click **OK**. The Email is sent from the EPS console.

### Installing Seqrite Client on Windows

1. Open the link in the Email on Windows system.
2. Download Windows client.

   The cainstlr.zip file is downloaded.
3. Extract the zip file.
4. Execute camininst.exe file.

   This installs clients on the system.

5. After Seqrite client installation is finished, the Seqrite Antivirus installation will be initiated by the Seqrite client.

### Installing Seqrite Client on Mac

1. Open the link in the Email on Mac system.
2. Download Mac client.

   The tar file is downloaded.
3. Extract the tar file.
4. Execute MCLAGNT.DMG file.

   This installs clients on the system.
5. After Seqrite client installation is finished, the Seqrite Antivirus installation will be initiated by the Seqrite client.

## Remote Installer

This page helps you to download Remote Installer Utility, which allows you to remotely deploy Seqrite Endpoint Security Cloud on all supported Windows and Mac endpoints.

### Installing Seqrite Windows Client

To do remote Installation on multiple Windows endpoints, follow these steps:

1. Download Remote Installer.
2. Run Remote Installer.
3. You can initiate remote installation in one of the following ways:
   - Add endpoints by selecting from the list
   - Add by IP Address
4. Enter the IP Address.
5. Click **Add** to add endpoints.
6. In the Add User dialog, type the **User Name** and **Password** with Administrator privilege.
7. Click **Finish** to add all selected endpoints to the installation list.
8. Click **Install** to initiate installation.
9. This feature allows you to deploy the client on all supported Windows operating systems at a time.

### Installing Seqrite Mac client

You can install Seqrite Mac client in one of the following ways:

- Installing using Apple Remote Desktop or Casper
- Connecting remotely using Secure Shell
- Using Terminal (for Mac and Linux OS)

- Using PuTTY (for Windows OS)

  For more information, see Remote Installation Guide.

## Active Directory

This page helps you to download Active Directory Tool. With Active Directory Tool you can synchronize the EPS server group with active directory organizational unit (OU)/container/computer. After synchronization, the clients will be installed on all the endpoints of your domain network. A periodic check is carried out to find if any new endpoint is added to your network. When a new endpoint is added, the client gets automatically installed on that endpoint.

You can also exclude certain endpoints from the EPS server group so that the client is not installed on these endpoints.

Note

- This installation method is available only with Microsoft Windows operating system.
- To synchronize the EPS server with Active Directory OU, the Active Directory Tool should be installed on the domain machine or should be a member of the domain.
- Synchronization cannot be done with Default group.
- On the Groups page, groups are shown with AD tag, which are already synchronized with Active Directory.
- The user should have permissions of Domain Admins to synchronize with Active Directory.

## Synchronizing with Active Directory

To install Seqrite Active Directory Tool on your computer, follow these steps:

1. Click **Active Directory Installer** button.
2. The Active Directory zip file is downloaded. Extract the files.
3. Double click adinst.msi file.

   The Active Directory installer opens and guides you through the steps required to install Seqrite Active Directory Tool on your computer.

   Note

   This system should be powered on 24X7 for periodic check in synchronization process.
4. Follow the instructions in the wizard. Seqrite Active Directory Tool will be installed on your computer.
5. Launch the Seqrite Active Directory Tool.

   A help file is provided in the Seqrite Active Directory Tool.

## Installing clients on different operating systems

The procedure to install Seqrite Client on different operating systems is as follows,

### Installing Seqrite Client on Windows

Copy the Client Installer created from Online/Standalone Installer to Windows system.

Extract the zip file on the system.

Execute the installer file. The name of installer file, as per the options selected is as follows,

- 32-bit with AV - clagav32
- 32-bit without AV - clagnt32
- 64-bit with AV - clagav64
- 64-bit without AV - clagnt64
- Minimal - minimal.exe

On executing the installer file, the Seqrite Client Agent is installed.

### Installing Seqrite Client on Mac

1. Download the <Package Name>.TAR file from the Seqrite console.
2. Extract the tar file.
3. Double-click the installer file (MCLAGNT.DMG).

   The Endpoint Security icon is mounted on the desktop.
4. Double click the **Endpoint Security** icon.

   An installer window will appear.
5. Double click the **Seqrite Installer** icon in the window. “Verifying Client Agent installer” message is displayed.
6. After the verification is complete, a message appears, "Client Agent Installer” is an app downloaded from the Internet. Are you sure you want to open it?”
7. Click **Open** button.
8. Provide username and password of the system when prompted by the installer.
9. Click **OK**.

   Note

   If password-protected Client Installer is being executed, then it will ask for Client Installer password first and then it will ask for System password.

   The Client Agent will be installed. A message, “Endpoint Security Client installed successfully” appears.
10. Click **OK.**

    The AV will be automatically downloaded and installed in the background. After installation, AV will get activated and its status will be sent to the server.

### Installing Seqrite Client on Linux

1. Log in as root and go to the terminal.

2. Go to the directory containing Seqrite Endpoint Security Cloud installation folder and run ./install script. The installation script will copy the necessary files to the /usr/lib/Seqrite/Seqrite folder.
3. Configure Seqrite and save your settings.

## Policies

Policies feature helps you to create policies that help centrally control and manage the users belonging to a group. You can create two types of policies,

- Container policy - Container policy is a combination of all features.
- Feature policy - Feature policy is used for specific feature. The feature policy overrides the container policy.

On the Policies page, you can manage policies.

On this page, you can perform the following functions:

Creating a new policy

Duplicating a policy

Updating a policy

Deleting a policy

The list of feature policies is as follows:

Scan

Email

IDS/IPS

Firewall

Web Security

Application Control

Advanced Device Control

Data Loss Prevention

Update

Internet

Miscellaneous

Once a policy is created, it can be easily applied to a group. The users under a group or a subgroup may inherit different policies. You should create groups before you create a policy setting. The container policy cannot be applied on an individual endpoint. The feature policy remains as it is, even if the endpoint is moved to another group.

On the policies page, you can see the table of default and created policies. Default_EPS is the default EPS policy. If the user is on boarded with MSSP, Default_MSSP also appears in the list.

## Managing Policy

### Creating a new policy

To create a new policy, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Policies. The Policies page appears displaying list of policies.
3. Click **Create Policy** button.
4. The Create Policy dialog appears. Enter Policy Name.
5. Select the Policy Type, either Container Policy or Feature Policy.

   If you select the Feature policy option, select the feature from the list.
6. Enter Description of the policy.
7. Click **Create**.

   The Policy Settings page appears. Configure the policy.
8. Click Save Policy.

   The name of the policy owner and date of policy creation appears.

### Deleting a policy

To delete a policy, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Policies. The Policies page appears displaying list of policies.
3. Select the policy that you want to delete, and then click Delete button.

   A confirmation message appears.
4. If you are sure to delete the selected policy, click **YES**.

   If the selected policy is applied to a group, it cannot be deleted, and a failure message appears.

Note

- You cannot delete the default policy.

- If a policy is applied to a group or to an endpoint and you want to delete it, then apply a different policy to that group or unassign the policy applied to the endpoint. Then you can delete the policy.

### Duplicating a policy

To duplicate a policy, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Policies. The Policies page appears displaying list of policies.
3. Click the duplicate icon of the policy that you want to duplicate.
4. The duplicated policy appears in the next row. Edit the name of the policy. Click icon to save the policy.

The selected policy is duplicated. The policy settings remain same.

You can also change the policy settings if required.

5. To save your setting, click **Save Policy**.

### Updating a policy

To update a policy, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Policies. The Policies page appears displaying list of policies. The name of the policy owner and date of policy creation appears.
3. Click the edit icon of the policy that you want to update.

   The Policy Settings page appears.
4. Update the settings.
5. To save your setting, click **Save Policy**.

Note

You cannot update Default_MSSP policy.

## Feature Policies

### Scan

This feature allows you to define a policy on how to initiate the scan of the endpoints. The policy can be refined to enable Virus Protection or DNA scanning or include blocking of any suspicious packed files, and other settings.

The following table shows a comparison of the features in Scan on different operating systems:

Comparison Table

| | Clients |
|---|---|

| Features | Windows | Mac | Linux |
|---|---|---|---|
| Automatic scan mode | ✓ | ✓ | ✓ |
| Scan executable files | ✓ | ✓ | ✓ |
| Scan all files (Takes longer time) | ✓ | ✓ | ✓ |
| Scan packed files | ✓ | X | ✓ |
| Scan mailboxes | ✓ | X | ✓ |
| Scan archives files | ✓ | ✓ | ✓ |

To configure policy for Scan, follow these steps:

1. Create feature policy as Scan.
2. On the Feature Policy page, you can see the following list of settings with expand sign and toggle button. Expand and enable settings that you want to configure.

   Scanner

   Virus Protection Settings

   Exclude Files and Folders

   Exclude Extensions

   Advanced DNAScan

   Block suspicious packed files

   Automatic Rogueware Scan

   Scan External Drive

   Autorun Protection

3. To save your settings, click **Save Policy**.

   Importantly, if you have customized the settings and later you want to revert to the default settings, you can do so by clicking the Reset Default button.

**Scanner**

Under Scanner, you can select either of the following scanning options:

- **Automatic***: This is the default scan setting that ensures optimum protection to the clients.

- **Advanced**: If you select this option, you may further need to customize the configuration of scanning options as per your requirement. When you select this option, other features are activated that are described as follows:

| Features | Description |
|---|---|
| Select items to scan | Select either of the options to scan:<br>Scan executable files: Includes scanning of executable files only.<br>Scan all files: Includes scanning of all files but takes longer time for scanning. |
| Scan Packed Files* | Scans packed files inside an executable file. |
| Scan Mailboxes* | Scans Emails inside the mailbox files. |
| Scan Archive Files* | Scans compressed files such as ZIP and ARJ files including other files. |
| Archive Scan Level | You can set the level for scanning in an archive file. The default scan level is set to 2. You can increase the scan level up to 16, however, that may affect the scanning speed. |
| Action to be performed when virus is found in archive file. | You can select an action that you want to take when a virus is found in archive file during an on-demand scan. You can select any one of the following actions:<br>• Delete – Deletes the entire archive file even if a single file within the archive is infected.<br>• Quarantine – Quarantines the archive containing the infected files.<br>• Skip – Takes no action even if a virus is found in an archive file. |
| Action to be performed when a virus is found. | You can select an action that you want to take when a virus is found during manual scan. You can select any one of the following actions:<br>• Repair – All the infected files are repaired automatically. The files that are not repairable are deleted. |

- Delete – All the infected files are deleted automatically.
- Skip – Takes no action even if a virus is found in a file.

To know for which clients the features marked with asterisk are applicable, see the comparison table.

**Virus Protection Settings**

This feature helps you continuously monitor the endpoints against viruses that may infiltrate from sources such as email attachments, Internet downloads, file transfer, and file execution. By default, Virus Protection is enabled to keep the endpoints clean and secure from any potential threats.

The following table shows a comparison of the features in Virus Protection Settings on different operating systems:

| Features | Clients | | |
|---|---|---|---|
| | Windows | Mac | Linux |
| Load Virus Protection at Startup | ✓ | ✓ | ✓ |
| Display alert messages | ✓ | ✓ | X |
| Report source of infection | ✓ | X | X |
| Select action to be performed when a virus is found | ✓ | ✓ | X |

With Virus Protection, you can configure the following:

| Features | Description |
|---|---|
| Load Virus protection at Startup | Enables real-time protection to load every time the system is started. |
| Display Alert messages | Displays an alert message with virus name and file name, whenever any infected file is detected by the virus protection. |
| Report source of infection | Displays the source IP address of the system where the virus is detected. |

| | |
|---|---|
| Select action to be performed when a virus is found | You can select an action that you want to take when a virus is found during manual scan. You can select any one of the following actions:<br>• Repair – All the infected files are repaired automatically. The files that are not repairable are deleted.<br>• Delete – All the infected files are deleted automatically.<br>• Deny Access – Access to an infected file is blocked. |

**Exclude Files and Folders**

This feature helps you decide which files and folders should be omitted from scanning for known viruses, Advanced DNAScan, and Suspicious Packed files. It is helpful in case you trust certain files and folders and want to exclude them from scanning.

The following table shows a comparison of the features in Exclude Files and Folders on different operating systems:

| Features | Clients | | |
|---|---|---|---|
| | Windows | Mac | Linux |
| Exclude from: Known Virus Detection | ✓ | ✓ | X |
| Exclude from: DNAScan | ✓ | X | X |
| Exclude from: Suspicious Packed Files Scan | ✓ | X | X |
| Exclude from: Behavior Detection | ✓ | X | X |

To add a file or a folder, follow these steps:

1. In Exclude File and Folders section, click Add.
2. On the Exclude Item screen, select either of the following:
    - **Exclude Folder**: If you select Exclude Folder, type the folder path in the Enter folder path text box.

      If you want to exclude a subfolder also from scanning, select **Include Subfolder**.
    - **Exclude File**: If you select Exclude File, type the file path in the Enter file path text box.
- **Exclude MD5 checksum**: If you select Exclude MD5 Checksum, type the checksum in Exclude MD5 Checksum text box.

MD5 checksum is a 32-character hexadecimal number which is the fingerprint of the file. With MD5 checksum, you can verify whether your downloaded file got corrupted or not in transit.

3. In Exclude from section, select the following options as per your requirement:
   - Known Virus Detection
   - DNAScan
   - Suspicious Packed Files Scan
   - Behavior Detection
4. To save your settings, click **OK**.

Note

- If you select Known Virus Detection, DNAScan and Suspicious Packed File Scan will also be enforced, and all the three options will be selected.
- If you select DNAScan, Suspicious Packed File Scan will also be enforced, and both the options will be selected.

- However, you can select Suspicious Packed File Scan or Behavior Detection as a single option.

**Exclude Extensions**

This feature helps you to exclude the files from scanning using their extensions to provide a real-time virus protection. This is helpful in troubleshooting performance related issues by excluding certain categories of files that may be causing the issue.

To exclude a file extension from scanning, follow these steps:

1. Type an extension in the Enter Extension text box, and then click Add.
2. The file extension should be without any dots in the following format: xml, html, zip etc.

Note

The Exclude Extensions feature is available only in the clients with Windows and Mac operating systems.

**Advanced DNAScan**

Helps you safeguard the client systems even against new and unknown malicious threats whose signatures are not present in the virus definition database. DNAScan is an indigenous technology of Seqrite to detect and eliminate new types of malware in the system. DNAScan technology successfully traps suspected files with very less false alarms.

Advanced DNAScan Settings also includes the following:

| Features | Description |
|---|---|

| | |
|---|---|
| Enable DNAScan | Helps in scanning the systems based on Digital Network Architecture (DNA) pattern. |
| Enable Behavior detection system | Helps in scanning the files and systems based on their behavior. If the files or systems behave suspiciously or their behavior changes by itself is considered as suspicious. This detection can be categorized based on their criticality level as Low, Moderate, and High. You can select the detection criticality level depending on how often the suspicious files are reported in your systems. |
| Submit suspicious files | Helps in submitting suspicious files to the Seqrite research lab automatically for further analysis. |
| Show notification while submitting files | Displays a notification while submitting DNA suspicious files. |

Note

- The Advanced DNAScan Settings feature is available only in the clients with Windows operating systems.
- The 'Behavior detection system' scan setting is not applicable for Windows Server platforms.

**Block suspicious packed files**

This feature helps you identify and block access to the suspicious packed files. Suspicious packed files are malicious programs that are compressed or packed and encrypted using a variety of methods. These files when unpacked can cause serious harm to the endpoint systems.

It is recommended that you always keep this option enabled to ensure that the clients do not access any suspicious files and thus prevent the spread of infection.

Note

The Block suspicious packed files feature is available only in the clients with Windows operating systems.

**Automatic Rogueware Scan**

This feature automatically scans and removes rogueware and fake antivirus software. If this feature is enabled, all the files are scanned for possible rogueware present in a file.

Note

The Automatic Rogueware Scan feature is available only in the clients with Windows operating systems.

**Scan External Drives**

Whenever your system comes in contact with any external devices, your system is at risk that viruses and malwares may infiltrate through them. This feature allows you to set protection rules for external devices such as; CDs, DVDs, and USB-based drives.

With External Drives Settings, you can scan the USB-based drives as soon as they are attached to your system. The USB-based drives should always be scanned for viruses before accessing it from your system, as these devices are convenient mediums for transfer of viruses and malwares from one system to another.

**Autorun Protection**

The Autorun Protection protects your system from autorun malware that tries to sneak into the system from USB-based devices or CDs/DVDs using the autorun feature of the installed operating system.

### Email

This feature allows you to customize the protection rules for receiving emails from various sources. You can set rules for blocking spam, phishing, and virus infected emails.

The following table shows a comparison of the features in Email Settings on different operating systems:

| Features | Clients | | |
|---|---|---|---|
| | Windows | Mac | Linux |
| Enable Email Protection | ✓ | ✓ | X |
| Enable Trusted Email Clients Protection | ✓ | X | X |

To configure policy for Email Settings, follow these steps:

1. Create feature policy as Email Settings.

2. On the Feature Policy page, you can see the following list of settings with expand sign and toggle button. Expand and Enable settings that you want to configure.

   Email Protection

   Trusted Email Client Protection

   Spam Protection

3. To save your settings, click **Save Policy**.

Importantly, if you have customized the settings and later you want to revert to the default settings, you can do so by clicking the Reset Default button.

**Email Protection**

With this feature, you can apply the protection rules to all incoming emails. These rules include blocking infected attachments (malware, spam, and viruses) in the emails.

This feature is turned on by default which provides the optimal protection to the mailbox from malicious emails. We recommend that you always keep Email Protection turned on to ensure email protection. Once the feature is enabled, all the incoming emails will be scanned before they are sent to the Inbox.

1. The **Block attachments with multiple extensions** check box is selected by default. This option helps you block attachment in emails with multiple extensions. Worms commonly use multiple extensions which you can block using this feature.
2. The **Block emails crafted to exploit vulnerability** check box is selected by default. This option helps you block emails whose sole purpose is to exploit vulnerabilities of mail clients. Emails such as MIME, IFRAME contain vulnerability.
3. The **Enable attachment control** option helps you block email attachments with specific extensions or all extensions. If you select this option, the following options are enabled:
   - Block all attachments: Helps you block all types of attachments in emails.
   - Block user specified attachments: Helps you block email attachments with certain extensions. If you select this option, the **Configure** button is activated. For further settings, click **Configure** and set the following options:

   i. In the User Specified Extensions dialog, select the extensions so that the email attachments with such extensions are blocked.
   ii. If certain extensions are not in the list that you want to block, type such extensions in the Enter Extension text box and then click Add to add them in the list.
   iii. Click OK to save changes.
4. Select the **Enable Email scanning over SSL** check box to enable incoming mail scanning for mail accounts configured over SSL. Ensure that you perform the procedure to import the certificate for the mail client that you are using. This feature is available only in the clients with Microsoft Windows operating system.

Note

The Email Protection feature is available only in the clients with Microsoft Windows and Mac operating systems.

**Configuring Email Clients**

For MS Outlook mail client, Seqrite Email Scanner certificate is imported automatically. No action required.

For your reference, procedure to import Seqrite Email Scanner certificate for Mozilla Thunderbird mail client is quoted here,

1. Launch Thunderbird mail client.
2. Select Options menu > Advanced > Certificates tab.
3. Click View Certificates.
4. In Certificate Manager dialog, select Authorities tab, click **Import**.
5. Select Seqrite Email Scanner CA.der certificate from <installation directory>\Seqrite\Seqrite.
6. Click the Trust this CA to identify websites check box and click Ok.
7. In Certificate Manager dialog, click **Ok**.
8. In Options dialog, click **Ok**.

Similarly, for other mail clients, to import Seqrite Email Scanner certificate, refer their technical documentation.

**Trusted Email Clients Protection**

Since email happens to be the most widely used medium of communication, it is used as a convenient mode to deliver malware and other threats. Virus authors always look for new methods to automatically execute their viral codes using the vulnerabilities of popular email clients. Worms also use their own SMTP engine routine to spread their infection.

Trusted Email Clients Protection is an advanced option that authenticates email-sending application on the system before it sends the emails. This option prevents new worms from spreading further. It includes a default email client list that is allowed to send emails. Email clients in the default list includes Microsoft Outlook Express, Microsoft Outlook, Eudora, and Netscape Navigator.

Trusted Email Clients Protection supports most of the commonly used email clients such as; Microsoft Outlook Express, Microsoft Outlook, Eudora, and Netscape Navigator. If your email client is different from the ones mentioned, you can add such email clients in the trusted email client list.

Note

The Trusted Email Clients Protection feature is available only in the clients with Windows operating systems.

**Spam Protection**

This feature allows you to differentiate genuine emails and filter out unwanted email such as; spam, phishing, and adult emails. We recommend you to always keep Spam Protection enabled. If you enable Spam Protection, the Spam Protection Level, White list, and Blacklist options are also activated.

The following table shows a comparison of the features in Spam Protection on different operating systems:

| Features | Clients | | |
|---|---|---|---|
| | Windows | Mac | Linux |
| Spam Protection | ✓ | ✓ | X |
| Spam Protection Level | ✓ | X | X |
| Enable White list | ✓ | ✓ | X |
| Enable Blacklist | ✓ | ✓ | X |

**Whitelist**

Whitelist is the list of trusted email addresses. The content from the whitelisted email IDs is allowed to skip the spam protection filtering policy and is not tagged as SPAM.

This is helpful if you find that some genuine email IDs are detected as SPAM or if you have blacklisted a domain but want to receive emails from certain email addresses from that domain.

**Blacklist**

Blacklist is the list of email addresses from which all emails are filtered irrespective of their content. All the emails from the addresses listed here are tagged as "[SPAM] -".

This feature is useful particularly if your server uses an open mail relay, which is used to send and receive emails from unknown senders. This mailer system can be misused by spammers. With blacklist, you can filter incoming emails that you do not want or are from unknown senders both by email IDs and domains.

**Configuring Spam Protection**

1. Under Spam protection level, set the protection level from the following:
   - **Soft**: Applies soft filtering spam protection policy.
   - **Moderate**: Ensures optimum filtering. It is always recommended to enable the moderate filtering. However, this is selected by default.
   - **Strict**: Enforces strict filtering criteria. However, it is not ideal as it may even block genuine emails. Select strict filtering only if you receive too many junk emails.
2. Select **Enable white lis**t to implement protection rules for whitelisted emails.
3. In the Email ID text box, type an email address or a domain and then click **Add**.

   You can import email addresses or domains from text file using the Import button.
4. Select **Enable email black list** to implement the protection rules for blacklisted emails.
5. In the **Email ID** text box, type an email address or a domain and then click **Add**.

   You can import email addresses or domains from text file using the Import button.

Note

- An email address should be in the format: abc@abc.com.
- A domain name should be in the format: *@mytest.com.
- The same email ID cannot be entered in both blacklist and whitelist.

6. To save your settings, click **Save Policy**.

### Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

When you create a network where numerous machines are deployed, security is of paramount concern. With IDS/IPS, you can detect attacks. This detection implements a security layer to all communications and cordons your systems from unwanted intrusions or attack. You can also take actions like blocking the attackers for certain time and send an alert message to the administrator.

Note

The IDS/IPS feature is available only in the clients with Microsoft Windows.

You can create different policies with varying IDS/IPS settings and apply them to the groups so that each has separate policies based on the requirement.

To configure policy for IDS/IPS, follow these steps:

1. Create feature policy as IDS/IPS.
2. On the Feature Policy page, from the following options, select an action to be performed when attack is detected:

- Block Attackers IP for … Minutes. By default, this option is selected.

  Select the time.
- Display alert message when attack is detected.

This option helps you to take an appropriate action when attack is detected.

3. To save your settings, click **Save Policy**.

Importantly, if you have customized the settings and later you want to revert to the default settings, click the **Reset Default** button.

### Firewall

Firewall shields your endpoint by monitoring both inbound and outbound network connections. It analyzes all incoming connections whether it is secure and should be allowed through, and checks whether the outgoing communication follows the compliance that you have set for security policies. Firewall works silently in the background and monitors network activity for malicious behavior.

You can create different policies for various groups/departments like enabling Firewall protection, applying Firewall security level with an exception rule and other settings according to the requirements. For example, you can apply security level as High for the Accounts Department and apply an exception rule by entering the policy with additional policy settings. You can also apply the Display alert message when firewall violation occurs and Enable firewall reports options. While for Marketing Department, you can create a policy with security level as Low without an exception rule and apply the Enable firewall reports options only.

Note

The Firewall feature is available only in the clients with Microsoft Windows.

**Configuring Firewall**

To configure policy for Firewall, follow these steps:

1. Create feature policy as Firewall.
2. On the Feature Policy page, you can see the following list of settings with expand sign and toggle button. Expand and Enable settings that you want to configure.

- Firewall
- Exceptions

3. To save your settings, click **Save Policy**.

   Importantly, if you have customized the settings and later you want to revert to the default settings, you can do so by clicking the Reset Default button.

**Firewall**

1. In the Level option, select one of the following:

- Block all
- High
- Medium
- Low

| Level | Description |
|---|---|
| Block all | Blocks all Inbound and Outbound connections without any exception. This is the strictest level of security. |
| High | Blocks all Inbound and Outbound connections with an exception rule. The exception policy can be created for allowing or denying connections either for inbound or outbound through certain communication protocols, IP address, and Ports such as TCP, UDP, and ICMP. |
| Medium | Blocks all Inbound and allows all Outbound connections with an exception rule.<br>The exception policy can be created for allowing or denying either inbound or outbound connections through certain communication protocols, IP address, Ports such as TCP, UDP, and ICMP. For example, if you allow receiving data from a certain IP address, the users can receive data but cannot send to the same IP address.<br>To take more advantage of this security level policy, it is advisable that you allow receiving inbound connections and block outbound connections. |
| Low | Allows all Inbound and Outbound connections.<br>When you apply Low security level, it is advisable that you create an exception rule for denying particular inbound or outbound data with the help of certain Protocols, IP address, and Ports to take more advantage of the security level policy. |

2. By default, the **Monitor Wi-Fi Networks** check box is selected. This option helps to receive alert messages when connected with unsecured Wi-Fi network and when an attempt is detected to access unsecured client Wi-Fi (hotspot). Also, the reports are generated at the server.
3. If you want an alert message about firewall violation, select the **Display alert message when firewall violation occurs** check box.
4. If you want reports for all blocked connections, select the **Enable firewall reports** check box.

Note

If the Firewall policy is set as **Block All**, Firewall will block all connections and generate many reports that may impact your network connection.

**Exceptions**

With Exceptions, you can allow genuine programs to perform communication irrespective of the Firewall level whether set as High or Medium. With Exceptions, you can block or allow Inbound and Outbound communication through IP addresses and ports.

**Creating the Exceptions**

1. In Exceptions section, the list of Exceptions appears.
2. To create new exception, click **Add**.
3. On the Add/Edit Exception screen, type a name in the Exception Name text box and select a protocol.

   The protocol includes TCP, UDP, and ICMP.
4. Click **Next**.
5. In Local IP Address section, type an IP address or IP range, and then click Next.

   If you select Any IP Addresses, you need not type an IP address.
6. Under Local TCP/UDP Ports, type a port or port range, and then click Next.

   If you select All Ports, you need not type a port as all ports are selected. If you mention Local IP Address or IP range or port, this exception will be applicable for incoming communications.
7. In Remote IP Address section, type an IP address or IP range and then click Next.

   If you select Any IP Addresses, you need not type an IP address as all IP addresses will be blocked. If you mention remote IP or port, that exception will be for outgoing communications.
8. In Remote TCP/UDP Ports section, type a port or port range, and then click Next.

   If you select All Ports, you need not type a port as all ports are selected.
9. In Action, select either **Allow** or **Deny**.
10. Click **Finish**.

    The Exception is added at top position in the Exceptions list. The sequence of the exceptions decides the precedence of the rule. The precedence is in descending order.

**Editing the Exceptions rule**

You can edit the exceptions rule which are created by you. To edit the Exceptions rule, follow these steps:

1. In Exceptions section, select the exception that you want to edit.
2. On the Add/Edit Exception screen, you can edit the name in the Exception Name text box and edit the protocol.

   The protocol includes TCP, UDP, and ICMP.
3. Click **Next**.

4. Edit Local IP Address if required, and then click **Next**.
5. Edit Local TCP/UDP Ports if required, and then click **Next**.
6. Edit Remote IP Address if required, and then click **Next**.
7. Edit Remote TCP/UDP Ports if required, and then click **Next**.
8. Under Action, you can select either **Allow** or **Deny**.
9. Click **Finish**.
10. Click **Save Policy**.

**Deleting the Exceptions rule**

You can delete the exceptions rule that you have created. To delete the Exceptions rule, follow these steps:

1. In Exceptions section, select the exception that you want to delete.
2. Click **Delete**.

   The selected exception rule is deleted.
3. Click Save Policy.

**Exporting the Exceptions rule**

You can export the exceptions rule that you have created. To export the Exceptions rule, follow these steps:

1. In Exceptions section, select the exceptions that you want to export.
2. Select Action > Export.

   The Opening firewall_exception.json dialog appears.
3. Select Save File.
4. Click **Ok**.

   The database file, `firewall_exception.json` is downloaded.

**Importing the exceptions rule**

You can import the exceptions rule that you have created in the earlier versions of EPS. To import the Exceptions rule, follow these steps:

1. In Exceptions section, click Add > Import.

   The File Upload dialog appears.
2. Select the database file, `firewall_exception.json`.
3. Click Open.

   The database file, `firewall_exception.json` is imported.

## Web Security

This feature helps you create security policies for an endpoint or group where Browsing and Phishing Protection can be enabled. This blocks malicious and phishing Web sites. You can restrict or allow access to the internet and Web sites as per your requirement.

The following table shows a comparison of the features in Web Security on different operating systems:

| Features | Clients | | |
|---|---|---|---|
| | Windows | Mac | Linux |
| Browsing and Phishing | ✓ | ✓ | ✓ |
| Web Categories | ✓ | ✓ | ✓ |
| Block Specific Websites | ✓ | ✓ | ✓ |
| Schedule Internet Access | ✓ | X | X |
| Alerts and Reports | ✓ | X | ✓ |

The following settings are provided under Web Security:

Browsing and Phishing

Web Categories

Block Specific Websites

Schedule Internet Access

Alerts and Reports

**Browsing Protection**

While users visit malicious Web sites some files may get installed on their systems. These files can spread malware, slow down the system, or corrupt other files. These attacks can cause substantial harm to the system.

Browsing Protection ensures that malicious Web sites are blocked while the users in a group are accessing the Internet. Once the feature is enabled, the site that is accessed is scanned and is blocked if found to be malicious.

**Phishing Protection**

Phishing is a fraudulent attempt, usually made through email, to steal your personal information. These emails usually appear to have been sent from seemingly well-known organizations and sites such as banks, companies and services seeking for your personal

information such as credit card number, social security number, account number or password.

Administrators can enable Phishing Protection that prevents users from accessing phishing and fraudulent Web sites. As soon as a site is accessed, it is scanned for any phishing behavior. If found fraudulent, then it is blocked to prevent any phishing attempts.

**Web Categories**

There are certain concerns that most organizations may face:

- System infection by malware.
- Users browsing unwanted Web sites.
- The employees idling away time.

To avoid these concerns the administrators need to have a policy that regulates users and their Web access activities.

The Web Categories feature helps the administrators centrally control and manage the browsing behavior of the users. The administrators can create different security policies for different groups according to their requirements and priorities.

**Creating a new Web Security policy**

To configure policy for Web Security, follow these steps:

1. Create feature policy as Web Security.
2. On the Feature Policy page, you can see the following list of settings with expand sign and toggle button. Expand and Enable settings that you want to configure.

- Browsing and Phishing
- Web Categories
- Block Specific Websites
- Schedule Internet Access
- Alerts and Reports

3. Expand **Browsing and Phishing**. For exclusion, see Exclusion for Browsing Protection and Phishing Protection.
4. Enable **Display Alert Message** to get an alert message when a blocked Web site is accessed by a user.
5. Enable and Expand Web Categories. This restricts or allows access to the Web sites based on their categories as per the security policy of your organization. If you block a category, all the Web sites referring to the category will be blocked.
    i. The Web categories are enabled, and you can allow or deny access to each category.
    From Status column, select either Allow or Deny.
    For exclusion, see Exclusion for Web Categories.

6. Enable and expand Block specified websites. You can enter the Web sites that you want to block. For details, see Block specified websites.
7. Enable and expand Schedule Internet Access and do the following:
    i. Select one of the following options:
        - Always allow access to the internet
        - Allow access to the internet as per schedule

        When you select the option, **Allow access to the internet as per schedule**, you can add the schedule time.
    ii. Click **Add** to add the schedule.

        Add Time Interval dialog appears.
    iii. Select the Weekday from the list.
    iv. Select the Start at and End at hours.
    v. Click **OK**.

    You can delete the schedule entry if the entry is not required.

Note

SSL versions earlier than 3.1 are not supported for Schedule Internet Access.

8. Enable and expand Alerts and Reports to generate reports for all blocked Web sites.

    If you select this option, a large number of reports will be generated depending upon the Web usage.
9. To save your settings, click **Save Policy**.

    Importantly, if you have customized the settings and later you want to revert to the default settings, click the Reset Default button.

**Exclusion for Browsing Protection and Phishing Protection**

Exclusion enables you to apply an exception rule to the protection policy for Browsing Protection and Phishing Protection. This helps you exclude the URLs of the sites that are genuine but get erroneously detected either as malicious or phishing sites. You are recommended to exclude only those URLs that you trust to be safe and genuine.

You can exclude the URLs in the following way:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to **Policies > Container Policies > Web Security**.
3. In the Browsing and Phishing section, under Exclude URLs, type the URL and then click **Add**.

    The Report Miscategorized URL dialog appears. You can report about miscategorization of the URL to the Seqrite lab if the URL is detected as malicious or phishing site.
4. Select one of the reasons from the following:

- URL is getting detected as Malicious

- URL is getting detected as Phishing

5. To report about miscategorization, click **Yes**. If you do not want to report about miscategorization, click **No**.

   The URL is added in the Exclude URL list.

6. To save your settings, click **OK**.

   In the action bar, you can perform the following actions:

| Action | Description |
|---|---|
| Add | Helps you exclude a URL from being detected as malicious or phishing. |
| Delete | Helps you delete a URL from the Excluded URL list. |
| Report | Helps you report if a URL is miscategorized. |

**Exclusion for Web Categories**

Exclusion helps you apply an exception rule to the protection policy for Web Categories. This helps you when you want to restrict access to a Web site category, but you want to allow certain Web sites from the restricted category.

You can enlist such Web sites in the Exclusion list in the following way:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to **Policies > Container Policies > Web Security**.
3. Click the **Exclusion** button.

   The Exclude URLs dialog appears.

4. Type the URL and then click **Add**.

   The URL is added in the Exclude URL list.

5. To exclude the subdomains, in the column Exclude Subdomain, select option **Yes** or **No**.
6. To save your settings, click **OK**.

| Action | Description |
|---|---|
| Add | Helps you exclude a URL from being restricted even if it belongs to the blocked category. |
| Delete | Helps you delete a URL from the Excluded URL list. |

**Block specified websites**

This feature is helpful in restricting access to certain Web sites or when a Web site does not fall into an appropriate category. It is also helpful if you have a shorter list of the Web sites that you would prefer to restrict the Web sites than blocking the entire category.

To block Web sites, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Policies > Container Policies > Web Security.

   The Block specified websites features (Add, Delete, Delete All) are activated.
3. Type a URL and then click **Add**.
4. If you want to block the subdomains, select the option Yes or No in Block Subdomains column. For example, if you block www.google.com and enable 'Block Subdomains', all its subdomains such as mail.google.com will also be blocked.

You can delete the URL, if required.

Note

The Block Subdomains feature is not applicable for the clients with Mac operating systems.

### Application Control

Organizations usually face the following concerns while using applications:

- No illegal or fake applications should be installed on client systems.
- Malicious applications should not infect the systems.
- Unnecessary applications should not clog the systems.

With this feature, you can authorize or unauthorize the users to access and work with certain applications, so that no one accesses an unwanted application.

You can create various policies based on the requirement of the groups or departments. For example, for the users of the Marketing Department, you can allow access to File Sharing Applications and Web Browser while restrict access to all other applications. For the Accounts Department, you can allow access to Archive Tools and Web Browsers only.

Note

The Application Control feature is available only in the clients with Windows operating systems.

**Application Control**

To configure policy for Application Control, follow these steps:

1. Create feature policy for Application Control.
2. On the Feature Policy page, If you want to send a notification when a blocked application is accessed, select Notify clients when an unauthorized application is blocked.
3. Select **Authorized** or **Unauthorized** or **Custom** option for each application category as per your requirement. The list of applications under the selected category is displayed in the below table.
4. Click **Save Policy**.

## Advanced Device Control

While working with data storage devices such as CD/DVDs and USB-based devices such as pen drives, organizations are concerned with the following:

- Autorun feature does not activate any infection.
- Unnecessary data or applications do not clog the systems.

This feature allows the administrators to create policies with varying rights. For example, administrators can block complete access to removable devices, give read-only and no write access so that nothing can be written on the external devices. They can also customize access to admin configured devices. Once the policy is applied to a group, the access rights are also applied. You can use the exception list to exclude the devices from the device control policy.

**Advanced Device Control**

To configure policy for Advanced Device Control, follow these steps:

1. Create feature policy for Advanced Device Control.
2. On the Feature Policy page, you can see list of settings with expand sign and toggle button. Expand and enable settings that you want to configure.
3. Enable Advanced Device Control.
4. Expand Storage Devices. The following list of storage devices is displayed:

- USB Storage Device
- Internal CD/DVD
- Internal Card Reader
- Internal Floppy Drive
- ZIP Drive

For the above devices, select the permissions as per your requirement.

5. Enable and expand **Card Readers**. The following list of Card Readers is displayed:

- Card Reader Device (MTD)
- Card Reader Device (SCSI)

For the above devices, select the permissions as per your requirement.

6. Enable and Expand **Wireless**. The following list of Wireless networks is displayed:

- Wi-Fi
- Bluetooth

For the above network, select the permissions as per your requirement.

7. Enable and expand **Mobile & Portable Devices**. The following list of Mobile & Portable Devices is displayed:

- iPhone

- SmartPhone (USB Sync)
- SmartPhone (Symbian)
- iPad
- iPod
- BlackBerry
- Mobile Phones (Symbian)
- Scanner & Imaging Devices

For the above devices, select the permissions as per your requirement.

8. Enable and expand **Interface**. The following list of Interface mode is displayed:

- FireWire Bus
- Serial Port
- SATA controller
- Thunderbolt
- PCMCIA Device
- USB

For the above interfaces, select the permissions as per your requirement.

9. Enable and expand **Camera**. For Webcam, select the permissions as per your requirement.
10. Enable and expand **Others**. The following list of other devices is displayed:

- Local Printers
- Teensy Board
- Network Share
- Unknown Device

For the above devices, select the permissions as per your requirement.

11. Enable and expand **Exceptions**. Ensure that you have added the devices in Configuration > Device Control > Add devices. Then do the following:
    i. Click **Add**.
    ii. Select one or more devices to add to the exception list.
    iii. Click **OK**.
    iv. On the Managed Devices confirmation dialog, click **Yes**.
    v. Set the access permissions as required.
12. To save your setting, click **Save Policy**.

    This policy is applied to all the devices that are configured in the list. Even if you add a device, the same policy will apply unless you customize the policy.

    Importantly, if you have customized the settings and later you want to revert to the default settings, click the **Reset Default** button.

Note

**For Windows Clients**

- Only NTFS is supported for Partial encryption.
- USB Pen Drives with GUID Partition Table (GPT) Partition Style cannot be added for authorization.
- If an authorized and encrypted device is formatted, the device will be treated as unauthorized. Hence, Administrator will need to add the device again in Device Control and configure the policies accordingly.
- Some devices (e.g. Nokia phones, BlackBerry phones) may need system reboot or device reattachment for device access rights to be applied.
- On blocking SATA Controller from Advanced Device Control, you may frequently see SATA Controller blocked prompts even when actual blocking is not performed.
- While any ongoing session of Webcam or Bluetooth is in progress, changing access right to block will not interrupt this current ongoing session. The device may need reattachment or system reboot for access rights to be applied.

**For Mac Clients**

- If the option Read only is selected in Advanced Device Control of SEPS and a USB device is attached, such a device may not be accessible from the left pane in Finder for some time.
- If a USB device is already attached to the machine and you are installing Mac client, the device may not be shown as mounted for a fraction of seconds.
- If an NTFS USB device is attached to the machine during installation of Mac client, two copies of the attached USB may be visible for a few seconds.
- If a USB device is to be shown as mounted or un-mounted using terminal commands, the Device Control policy will not apply to that device.
- If you are installing Mac client on Mac OSx 10.9 while a FAT USB device is attached to the machine, such a device will not be displayed as mounted. To show the device mounted, you need to disconnect the device and reconnect it.
- iDevices, Internal Card Reader, Webcam, CD-DVD, mobile phones and HFS encrypted devices may need device reattachment for device access rights to be applied.
- Exception functionality will not be applicable for Bluetooth, Wi-Fi, Webcam, External CD-DVD.
- Mobile phones except iDevices that are connected in ‘USB Mass Storage’ mode will be detected under USB storage device category.
- Mobile phones connected in MTP mode will be detected under ‘Windows Portable Devices’ category.
- Blocking functionality will not work for Blackberry mobile if the mobile is connected to Mac system in Sync Media.

- USB storage device would not be formatted with Mac OS extended (Journaled, Encrypted) file format.

**For Linux clients**

- MTP/PTP based phones are not supported, whereas UMS based phones are supported.
- The Read only option set for internal CD/DVD on the EPS server, is treated as Blocked on the Linux client.
- Wireless adapters are not supported.
- Bluetooth USB dongle may not be supported on some operating systems.
- In all supported Linux OS, internal CD-DVD tray will not open if block mode is set for CD-DVD"
- If DC configuration is changed from Read-only mode to Allow mode, the USB drives may not work accordingly.
- UMS Mobile Phones do not work in Read-only mode. Changing the mode using the option available in the device will connect it to the endpoint. If the device is plugged out, the device in a particular mode does not change the mode automatically.

### Data Loss Prevention

You can prevent unauthorized loss, pilferage, or leakage of confidential company data using the Data Loss Prevention (DLP) feature.

It is necessary to enable DLP on endpoints. To do this, see DLP License.

The DLP policy can stop an unauthorized activity that is carried out through the following channels:

- Using the Print Screen option to save the screenshot (Applicable only for Windows platform). The file/data is not monitored.
- Using Removable Devices to copy data (Applicable only for Windows platform)
- For selected File Types, the Removable Devices go to 'Read Only' mode when 'Monitor Removable Devices' option is selected.
- Using Network Share accessed using UNC Path or Mapped Network Drive (Applicable only for Windows platform).
- Using the Clipboard to paste information from one application to another.
- Using printer activity, printing through local and network printer. The file/data is not monitored. (Applicable only for Windows platform)
- Using online services of third-party Application/Services to send data such as email, file sharing apps, cloud services, Web browsers and other applications using social media.

Note

- User need to purchase a DLP pack separately to avail this policy.

**Data Loss Prevention**

To configure policy for Data Loss Prevention, follow these steps:

1. Create feature policy for Data Loss Prevention.
2. On the Feature Policy page, you can see list of settings with expand sign and toggle button. Expand and enable settings that you want to configure.

- Data Loss Prevention
- Data Transfer Channels
- Data Settings
- Exceptions

3. Enable Data Loss Prevention. Select the **Display alert message on DLP policy violation** check box.
4. Select Action to configure the action to be performed after the attempts is carried out, either **Report only** or **Block and Report**.

   Alert prompts will not be displayed for Report Only action.

5. Expand Data Transfer Channels.

   Select the channels that you want to monitor from the following options:

- Print Screen (applicable only in Windows platforms)
- Removable Devices (applicable only in Windows platforms)
- Network Share (applicable only in Windows platforms)
- Clipboard
- Printer Activity (applicable only in Windows platforms)
- Application/Online Services

6. Select the applications that you want to monitor for attempts at data pilferage by clicking the Applications list. Do one of the following:

   You can select all the applications in the group.

- Select the applications one by one after expanding the group caret.
- Select all Mac platform applications by clicking the Mac group icon.
- Select all Windows applications by clicking on the Windows icon.
- Select all Web Browsers or one by one after expanding the group caret.
- Select all E-mail applications or one by one after expanding the group caret.
- Select all Instant Messaging applications or one by one after expanding the group caret.
- Select all File Sharing/Cloud Services applications or one by one after expanding the group caret.
- Select All Social Media/Others applications or one by one after expanding the group caret.

7. To configure email SSL settings, select the **Enable Email scanning over SSL** check box. This is applicable only when you select Email option in the Application / Online Service. Ensure that you perform the procedure to import the certificate for the mail client that you are using. This feature is available only in the clients with Microsoft Windows operating system.
8. Expand **Data Settings** to configure the settings for File Types, Confidential Data, and User Defined Dictionary.
9. Select the **Monitor File Types** check box. Select the File Types caret from the following:

- Graphic Files (Audio, Video, Images)
- Office Files (MS Office, Open Office, Kingsoft Office)
- Programming Files
- Other Files (Compressed files etc.)

10. To add the Custom Extensions, do the following:
    i. Select the **Custom Extensions** check box.
    ii. Click **Add** button. Add Custom Extensions dialog appears.
    iii. Type an extension in the text box and press enter.
    iv. Click **Add**.

    You can delete the custom extension with the help of delete icon.
11. Select the **Monitor Confidential Data** check box. Select the Confidential data carets from the following:

- Confidential data such as Credit/Debit Cards
- Personal information such as Social Security Number (SSN), Email ID, Phone Numbers, Driving License Number, Health Insurance Number, Passport Number, ID, International Banking Account Number (IBAN), Individual My Number, Corporate My Number, Pin Code, Aadhar Number and Vehicle Registration Number.
- Select the **Monitor User Defined Dictionary** check box. The User Defined Dictionaries are created at Data Loss Prevention.
- The words/strings must be flagged if used in communication.

Note

You can either choose to be notified through email notification when an attempt is made to leak information or prevent the attempt from being carried out successfully.

12. Expand **Action** to configure the action to be performed after the attempts is carried out, either Block and Report or Report only.

    Alert prompts will not be displayed for Report Only action.
13. Expand **Exceptions**. To add the domain names that you want to exclude from Data Loss Prevention, do the following:
    i. Enter the domain name in the text box.

ii. Click **Add**.

You can see the list of domain names. You can edit, delete and export the domain names.

iii. To import the domain name, click **Import**.

The File Upload dialog appears.

iv. Select the valid exported domain data file.

v. Click **Open**.

The database file is imported.

14. In Application Whitelisting, you can import application in .dat file format to exclude applications from Data Loss Prevention. Do the following:

i. To download DLP Application Whitelisting Tool, click **Download**.

ii. After downloading the Whitelisting Tool, add applications for DLP whitelisting in the tool.

iii. Generate DLPAppWhiteList.dat file.

iv. Click **Import** to import DLPAppWhiteList.dat file.

The applications are whilelisted.

15. To add the network paths, do the following:

i. Enter the Network path the text box.

ii. Click **Add**.

iii. You can see the list of Network path. You can edit, delete and export the Network path.

iv. To import the Network path, click **Import**.

The File Upload dialog appears.

v. Select a valid exported network share data file.

vi. Click Open.

The database file is imported.

Note

Domain Exceptions and Network path support the Windows platform only.

16. Click **Save Policy**.

Note

For Mac Client:

- Confidential & User Dictionary Data will not be blocked in subject line, message body of email or messenger communication.
- Prompts and report will be generated in case if monitored file type is downloaded.
- Certain file types (POT, PPT, PPTX, DOC, DOCx, XLS, XLSX, RTF) containing unicode data will not be blocked.
- Seqrite provides you an advanced scanning feature, Data-At-Rest Scan. With this feature you can search for a particular type of data in various formats.

### Update

When a work environment has a large number of systems installed, the challenge that the administrators usually face is how to update all the endpoints for security patches.

This feature allows you to create policies for taking the updates automatically for the endpoints. You can create policies that help different clients take the updates from different sources. Taking the updates from different sources reduce the load on a single server.

The following table shows a comparison of the features in Update Settings that are applicable for different Seqrite Endpoint Security clients on different operating systems:

| Features | Clients | | |
|---|---|---|---|
| | Windows | Mac | Linux |
| Enable Automatic Update | ✓ | ✓ | ✓ |
| Show update notification window | ✓ | ✓ | X |
| Frequency | ✓ | ✓ | X |
| Update Mode | ✓ | ✓ | ✓ |

To configure policy for Update Settings, follow these steps:

1. Enable and expand **Automatic Update**.
2. To display notification window when the updates are taken, select the **Show update notification window** check box.
3. Under Frequency, set the schedule when you want to take the updates.

- Automatic
- Custom

  If you select **Custom, Daily Start at** and Repeat after, lists are activated, you can set the schedule as per your requirement.

4. Under Update Mode, when EPS is installed on private IP (Private IP natted to Public IP), the following update settings can be configured:

- Download from Internet
- Download from Specified Update Servers

If you select Download from Specified Update Servers, server list is activated. Select the Update Server from the list.

5. To save your settings, click **Save Policy**.

   Importantly, if you have customized the settings and later you want to revert to the default settings, you can do so by clicking the Reset Default button.

### Internet

This feature gives the administrators a wider choice of creating policies for the client modules that need Internet connection to function. You can configure different settings for the server and port so that the client modules such as; Quick Update, Spam Protection, Web Security, and Messenger have Internet connection. This is very helpful in allowing the client modules to function in a secure work environment where default Internet connection is not allowed.

To configure policy with Internet Settings, follow these steps:

1. Enable Proxy Setting.

   The proxy settings details are activated.

2. Select the Proxy Type as HTTP Proxy, Socks V 4 or SOCKS V 5 as per your settings.
3. In the **Proxy Server** text box, type the IP address of the proxy server or domain name (For example, proxy.yourcompany.com).
4. In the **Port** text box, type the port number of the proxy server (For example: 80).
5. In the **User Name** and **Password** text boxes, type in your proxy server credentials.
6. Click **Next**.
7. To save your settings, click **Save Policy**.

   Importantly, if you have customized the settings and later you want to revert to the default settings, you can use the **Reset Default** button.

Note

The Internet Settings feature is applicable for the clients such as Microsoft Windows, and Mac operating systems.

### Miscellaneous

This feature helps to receive notification to the given Email ID, give access to client settings.

This feature allows you to create a policy that authorizes the clients to receive notification to the given Email ID, to access client settings and change their own password, enable or disable Safe Mode Protection, Self Protection, and News Alert.

The following table shows a comparison of the features in Miscellaneous that are applicable for different Seqrite Endpoint Security clients on different operating systems:

| Features | Clients | | |
|---|---|---|---|
| | Windows | Mac | Linux |
| SNMP Configuration | ✓ | X | X |
| Authorize access to the client (Client password) | ✓ | ✓ | ✓ |
| Safe Mode Protection | ✓ | ✓ | X |
| Self Protection | ✓ | ✓ | X |
| Data Backup | ✓ | X | X |

**Miscellaneous**

1. Create feature policy for Miscellaneous.
2. Enable and expand **Notification**.
3. Select the following check boxes as per requirement to receive the notification when the incidents occur:
   - Virus detected on endpoints
   - Intrusion detected on endpoints
   - Attempt to breach device control policy
   - Attempt to breach DLP policy
   - Hardware change detected on endpoints
   - Endpoint virus definition is older than N days
   - Attempt to access unauthorized application
   - Virus active on endpoints
4. Select the Email Address from the list to receive the notifications. You can also add new Email Address.

   Enter new Email Address in the text box and click **Add**. You can delete the Email Address with the help of Delete button.
5. Enable and expand SNMP Configuration.

   Here you can enter the IP address of the Simple Network Management Protocol (SNMP) server in your network. This SNMP Server IP Address is sent to the client. As soon as the virus/ransomware attack incident occurs, the client sends SNMP notification to the SNMP server and to the EPS server also. In the network without SNMP server, the virus

attack notification is sent to the EPS server only as per heartbeat interval set for the client. Enter the SNMP Server **IP Address** in the text box.

6. The Trap notifications can be viewed in the SNMP server where the configuration file, seqrite.mib is imported. Download the seqrite.mib file from the following SNMP Trap KB article,

   http://esupport.seqrite.com/support/solutions/articles/23000018039-how-to-configure-snmp-under-eps-products-

7. To give access to the client settings, Enable and expand **Client Password**.
8. In Enter Password, type the password and then re-type the same password in Confirm Password field.

   The clients will have to use these passwords for accessing the client settings.

   The **Safe Mode Protection** check box is selected by default. Seqrite recommends that you do not disable this feature.

9. The **Self Protection** setting is enabled by default. Seqrite recommends that you do not disable this feature.
10. Expand Data Backup. Data Backup automatically and periodically (multiple times a day) takes a backup of all your important and confidential files present on the endpoint. If you update any file, then this feature automatically takes backup of the latest copy. In the Data Backup section, do the following,

    i. **Default Backup Location** is selected by default. The backup data is stored at the default location, by default. EPS server searches all volumes on the local PC and then selects the drive with maximum free space to store the backup data locally.

    ii. Select **New Backup Location** option if you want to store your backup data at other location. Enter the folder path.

    iii. Select **Network Path Location** option if you want to store your backup data of all machines on a particular system in the network. Enter the Network Path Location.

    iv. Enter **Username** and **Password**.

    v. You can view the list of default extensions by clicking the **View** Button.

    vi. You can add custom extensions to the list as per your requirement. Enter **extension** and maximum file size in the text boxes.

    vii. Click **Add**. You can delete the extension with Delete button.

    viii. To exclude file extension from the data backup, enter the extension in Exclude File Extension box. Click **Add**. You can delete the excluded extension with **Delete** button.

    While performing backup, avoid including large size files such as PST, media files to ensure stable system performance and network operations. After successful client installation, backup starts after 6 hours.

    Disable this feature if you have any other provision for data backup (Example: File server backup, Data backup server, etc.)

    We have provided a backup facility with EPS. To restore your data, contact EPS Support Team.

11. To save your setting, click **Save Policy**.

## Schedule Settings

Scanning regularly keeps the systems clean and safe. In a large organization the client systems may be installed in physically separated environments.

To centrally manage all the systems about how to scan and when to initiate scanning, the administrator must have a policy. This feature helps you create policies for scheduling scans for the client systems.

To configure policy for Schedule Settings, follow these steps:

1. On the Feature Policy page, you can see the following list of settings with expand sign and toggle button. Expand and enable settings that you want to configure.

   Scheduled Tuneup

   Scheduled Client Scan

   Data-At-Rest Scan

   Asset Management

   Application Control

2. To save your settings, click **Save Policy**.

   Importantly, if you have customized the settings and later you want to revert to the default settings, you can do so by clicking the **Reset Default** button.

**Scheduled Tuneup**

Scheduled Tuneup setting allow you to carry out different types of cleanups such as; disks, registry entries, or schedule a defragmentation at scheduled time at next boot.

To schedule Tuneup settings, follow these steps:

1. In Frequency (Weekly), select a day of the week.
2. In Start At, set time in hours and minutes.
3. Select the Run task immediately if missed check box if you want to run the scan immediately if missed the set schedule.
4. In Tuneup settings, select either or all the following options:

- Disk cleanup
- Registry cleanup
- Defragment at next boot

However, all these options are selected by default.

**Scheduled Client Scan**

This feature allows you to create policies to initiate scanning the clients automatically at a convenient time. You can define whether the scan should run daily or weekly, select scan mode (Quick Scan, Full System Scan). You can also enable Antimalware while scanning. This

will supplement other automatic protection features to ensure that the client systems remain malware-free.

1. In Frequency, select either the **Daily** or **Weekly** option.
2. In **Start At**, set time in hours and minutes.
3. If you want to repeat scanning of your clients, select Repeat Scan and set the frequency after what interval the scan should be repeated.
4. Select the **Run task immediately if missed** check box if you want to run the scan immediately if missed the set schedule.

Note

- Missed schedule scan is not supported on Windows XP SP3 (32- bit) operating system.
- For Microsoft Windows Vista and above operating systems, missed schedule scan will not work if Schedule task is not run at least once.

5. In Scanner Settings section, Under How to Scan, select a scan mode from the following:

- Quick Scan (Scan Drive where operating system is installed)
- Full System Scan (Scan all the fixed drives)

6. Select **Scan Priority.** The Scan Priority is Low by default. You can change the priority to Normal or High, if required.
7. Under Select scan mode, to set optimal setting, select the **Automatic** option.
8. To set advanced setting, select the **Advanced** option.
9. If you select the Advanced option, further settings such as, scan items and scan types are activated.
10. Under Select items to scan, select any of the following:
    - Scan executable files
    - Scan all files (Takes longer time)
    - Scan packed files
    - Scan mailboxes
    - Scan archives files
11. If you select the Scan archives files option, you can set the following also:
    - Archive Scan Level: You can set up to level 16.
    - Select action to be performed when virus is found in archive file: You can select one of the actions from Delete, Quarantine, and Skip.
12. In Select action to be performed when a virus is found section, select an action from the following: Repair, Delete, and Skip.
13. To enable scanning for malware, select the **Perform Antimalware scan** check box.

14. In Select action to be performed when malware found, select an action from the following: Clean and Skip.
15. Under Boot Time Scan Settings, select **Perform Boot Time Scan** check box.
16. Select **Boot Time Scan Mode** option from the following,

    - **Quick Scan** (Scan the areas where operating system and applications are installed)
    - **Full System Scan** (Scan all the fixed drives)

    Boot time scan will be executed whenever the endpoint system restarts.

    Note

    Scan packed files, Scan mailboxes, and Antimalware Scan Settings are available only in the clients with Windows operating system.

**Data-At-Rest Scan**

With Data-At-Rest scan, you can search for a particular type of data in various formats and detect any confidential data that is present in your endpoints and removable devices. To perform Data-At-Rest scan, you must enable DLP on the endpoints. To do this, see DLP License.

1. In Frequency, select either the Daily or Weekly option.
2. In Start At, set time in hours and minutes.
3. If you want to repeat scanning of your clients, select Repeat Scan and set the frequency to repeat the scan.
4. Select the Run task immediately if missed check box if you want to run the scan if missed the set schedule.
5. Select a scan mode from the following:

- Quick Scan (Scan Drive where operating system is installed)
- Full System Scan (Scan all the fixed drives)
- Scan Specific Folder(s): Select this option to scan a folder(s).
    i. Click **Configure**.
    ii. Enter the path of the folder that you want to scan.

        You can also choose to scan the subfolders by selecting the **Include Subfolder** check box.

    iii. Click **Add**.

        You can also remove a path from the list by clicking **Remove**.

    iv. Click **Apply**.

6. Select Scan Priority. The Scan Priority is Low by default. You can change the priority to Normal or High, if required.
7. Configure the settings for File Types, Confidential Data, and User Defined Dictionary.

**Asset Management**

Assets Management helps you keep a watch on the system information, hardware information, and software installed. You can also view the hardware changes and software changes, if any, that are made to the configuration of the systems.

Select the following check boxes:

- Track Software Changes
- Track Hardware Changes. This check box is selected by default.

**Application Control**

Application Control helps you define schedules to scan applications at a preferred or specified frequency.

To configure Application Control Schedule Scan, follow these steps:

1. In **Frequency**, select either the Daily or Weekly option. If you select the Weekly option, select the weekday from the list.
2. In **Start At**, set time in hours and minutes.
3. If you want to repeat scanning for the applications, select the **Repeat Scan** check box and set the frequency of interval after which the scan should be repeated.
4. Select the Run task immediately if missed check box.
5. Select one of the following scan options:
    - Unauthorized applications: Helps you initiate scanning only for the unauthorized applications present on a client machine.
    - Unauthorized and authorized applications: Helps you initiate scanning for both, unauthorized and authorized applications present on the client machine.
    - All installed applications: Helps you initiate scanning for all applications installed on a client.
6. Select Scan Priority. The Scan Priority is Low by default. You can change the priority to Normal or High, if required.

## Configurations

On the Configurations page, you can perform the following,

Verify the Client Installation path

Add devices

Data Loss Prevention

Application Control

Asset Management

### Client Installation

On this page, client installation path appears. The client will be installed at this path.

You can modify the path if required.

This feature is applicable only for the clients with Microsoft Windows operating system.

### Add devices

This feature helps you to add USB. 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.

#### Adding a device

To add USB device, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to **Configurations > Device Control**.
3. The list of devices which are already added appears. Click the **Add devices** button and select USB Devices.

   The Add Device dialog appears.
4. Follow the procedure mentioned in the dialog.
5. Click **Browse** to upload the Device Control file.
6. Click **Add**.

#### Adding USB device by Model name

To add USB device by Model name, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Configurations > Device Control.
3. The list of devices which are already added appears. Click the **Add devices** button and select **USB by Model** to add device by Model.

   The Add Device by Model Name dialog appears.
4. Enter Device name.

5. Select a mode from the Mode to add Model Name list. Select one of the following modes:

- From the list: A list of pre-specified device model names appears. Select a model name from the list.
- Manually: Enter model name.

6. Follow the procedure mentioned in the For Windows / For MAC tab as per the endpoint operating system.
7. Click **Add**.

Note:

To add multiple USB devices, remove all the connected USB devices. Attach the USB device that you want to add and follow the above procedure.

8. Select the devices that you want to manage from the displayed list and click **OK**.

After the device appears in the list, toggle the button under Authorized to Yes or No as required. You can also use the Edit icon that appears to change the device name as it appears or use the Trash box icon to delete the device from the list.

Note

If you set the device authorized permission to 'No', then that device cannot be added to the exceptions list.

9. To add the device to the exceptions list, go to Policies > Advanced Device Control.
10. Click Exceptions.
11. Click **Add**. The Managed Devices dialog box displays the list of authorized devices.
12. Toggle the **Add to Exceptions** button for that device.
13. Click **OK**.
14. Click **Yes** on the Managed Devices confirmation dialog box. The device is now added in the list of exceptions.
15. To delete a device, select the device, and then click the Trash icon that appears.
16. Set the access permissions as required.
17. Click Save Policy.

Note:

To add multiple USB devices, remove all the connected USB devices. Attach the USB device that you want to add and follow the above procedure.

### Viewing details of devices

To view details of devices, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.

2. Go to Configurations > Device Control.

The list of devices which are already added appears.

The list displays the following details of the devices:

| Fields | Description |
|---|---|
| Device Name | Displays the device name. |
| Device Type | Displays the device type of the device. |
| Model Name | Displays the model name of the device. |
| Authorized | Displays status of the authorization, whether 1 / 0. |

### Deleting the device

To delete the device, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Configurations > Device Control.

The list of devices which are already added appears.

3. Select the device that you want to delete.
4. Click **Delete** button.

### Updating the device

To update the device, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Configurations > Device Control.

   The list of devices which are already added appears.
3. Click the Update icon for the device that you want to update.
4. Edit Device name dialog appears. Update the device name.
5. Click **Save**.

## 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.

### Adding Dictionary

To add dictionary, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Configurations > Data Loss Prevention.
3. Click Add > Add.
4. Enter the details such as name, description and the word that you want to add.
5. Click **Add**.

   You can add multiple words to the dictionary.

   You can delete a word from the list by selecting a particular word and clicking Delete.

### Importing Dictionary

You can also import a dictionary that you prefer to use.

To import the dictionary, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Configurations > Data Loss Prevention.
3. Click Add > Import.
4. In the Import Dictionary dialog, click **Browse**.

   The File Upload dialog appears.
5. Select the valid exported dictionary json file (Example: DLP_Dictionary.`json`).
6. Click **Open**.

   The json file is imported.

## Application Control

This feature allows you to add a new application to the default list. Adding and unauthorizing 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 operating system or other system related programs. You can add an application as follows:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Configurations > Application Control.
3. To add an application, click the **Add Application** button.
4. To add an application, select one of the following option:

- Select Process Name and type process name.
- Application Signature Maker - You can import application signature file. To create application signature file, do the following:

i. To download Application Signature Maker, click Download.
ii. After downloading the Maker, add the application name to create the application signature.
iii. Click Save to File. The AppSignature.dat file is created.
iv. Click Browse and select the path of the AppSignature.dat file.

5. In the **Application Name** text box, type an application name.
6. In the **Application Category** list, select a category.
7. Write a reason for adding a new application to the default list of applications.

   This helps Seqrite to improve the quality of the software product.
8. You can also submit the application metadata to the Seqrite lab.
9. Click **Save**. The application is added in the 'User Added Applications' subcategory under the selected application category.

### Submit Application metadata to Seqrite lab

With this option, you can send metadata of an application to the Seqrite lab for including it in the application categories. Metadata includes information of application such as its Name, Version, Company Name, and MD5. You can also provide the reason for adding the application. This information will help us to improve the Application Control module.

Application Categories include thousands of applications based on their functionalities. If you block a category, all the applications in that category are blocked.

However, if you have unauthorized an application category but an application is not yet blocked, you can submit that application. Seqrite analyzes the application and then enlists it in the category.

- User may get application blocked prompt even while copying or renaming any unauthorized application.
- Some unauthorized applications may start in case the application executable is updated due to software update. Such applications can be added to Seqrite Endpoint Security Cloud and you are recommended to submit the Metadata to the Seqrite lab.

## Asset Management

To view the complete product key on the Endpoint Status page, select the OS Product key check box. If you do not select this check box, only partial product key will be displayed.

This feature is applicable only for the clients with Microsoft Windows operating system.

## Reports

Reports provides the latest information of all clients and keeps comprehensive logs about virus incidents, policies breaches, and updates.

You can view and generate reports for the listed categories. You can create your own custom category as per your requirement. There are default reports displayed for each category. You can create your own query and generate the custom reports. You can manage the generated queries.

On the reports page, you can do the following;

- View charts of the listed categories
- Create queries to generate reports
- Add custom category to generate reports

Note

Custom created reports can be viewed only by the user who has created the reports.

The following are the listed categories for the reports:

- **Virus Scan** – You can view the virus incidents after scanning the clients. You can also view the statistics of unscanned endpoints since last 1, 3, 7, 15, and 30 days.
- **Anti-Malware Scan** – You can view the malware incidents after scanning the clients.
- **Web Security** – You can view statistics of Web sites blocked through the Browsing Protection, Phishing Protection, or block Web sites modules.
- **Tune-up** – You can view the number of clients tuned up and how not tuned up at all.
- **Advanced Device Control** – You can view whether removable devices have been blocked and what actions were taken against unauthorized devices.
- **Data Loss Prevention** – You can view statistics about attempts of sending the data outside the organization in an unauthorized manner.
- **IDS/IPS** – You can view whether there was any attempt of intrusion, and actions taken.
- **Firewall** – You can view number of violations for Firewall such as; the blocked connection for communications (Inbound or Outbound) and Firewall security level.
- **Asset Management** – You can view reports related to the hardware/software assets of the Endpoints.
- **Application Control** – You can view statistics about how many applications were authorized or unauthorized applications. You can also view the application control scan reports here.
- **Backup for Ransomware Protection** – Reports are generated only if backup fails. This report is only in the tabular format, not in the chart format.

The procedures written below are same for all the above categories including custom category.

On the reports page, you can do the following;

View charts of the listed categories

View tabular report

Create and manage queries to generate reports

Add custom category to generate reports

## Viewing chart report

To view the reports, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. Go to **Reports**. Select the category for which you want to view the report.

   The default chart report of last 7 days appears. The chart reports are in Line and pie chart format. The data points on the line chart are interactive.
3. Hover the chart, a tooltip appears showing the count of that part.
4. Click the data point/slice, a pop-up appears displaying details of that part of chart.

You can generate a new chart by adding a query. You can create maximum 25 reports for each category. The reports are displayed in expand / collapse format.

The following table shows the types of chart reports per category.

| Category | Types of Reports |
|---|---|
| Virus Scan | Virus Incidents |
| Anti-Malware Scan | Anti-Malware Incidents |
| Web Security | • Blocked Websites<br>• Websites blocked by categories |
| Tune-up | Tune-up Status |
| Advanced Device Control | • Number of device violations<br>• Policy violations by devices |
| Data Loss Prevention | • DLP violations<br>• Data leaks through data transfer channel<br>• Type of Data Leaks |
| IDS/IPS | Intrusion Incidents |
| Firewall | No. of violations |

| | |
|---|---|
| Asset Management | • Software & Hardware changes<br>• Applications installed |
| Application Control | • Blocked Applications<br>• Blocked Applications as per category |
| Backup for Ransomware Protection | • Report is generated if backup fails. |

You can refresh the chart report with the Refresh icon for the latest data.

You can edit the chart report with the Edit icon.

You can remove the custom chart with the Close icon.

## Viewing tabular report

To view the reports, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. Go to **Reports**. Select the category for which you want to view the report.

   The default chart report appears.
3. To view the tabular report, click **Tabular** icon.

   The list of queries appears.
4. Click the **View** link of the query that you want to view.

   The Report page opens. The Group and Period appears as per the query.
5. To add filters, click Add Filters. The parameters in the Add Filters are Endpoint Name and User Name. Select or clear the filter that you want to add or remove.
6. To generate the report on the selected parameters, click **Generate**. Click **Save** to save the selected parameters. The filter is changed after saving.

   After clicking **Generate** button, the report in the tabular format will be displayed. In addition, if you want to change the columns then you can do it by using Columns list.

   You can save the report in the csv format using the CSV button.

## Managing query

There are default reports displayed for each category. You can create and manage your own query and generate the custom reports.

### Adding a query

To add a query, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.

2. Go to **Reports**. Select the category for which you want to create a chart.
3. The list of default queries appears. Click the **Add Report** button to create new query.
4. The Add Report dialog appears. Select the Sub-Type. The Sub-Type option is for Web Security, Advanced Device Control, Data Loss Prevention, Asset Management categories only.
5. Enter Report Name and Description.
6. By default, All Groups option is selected. You can select the group if required.
7. By default, Last 7 Days option is selected in Periods. You can change the period for report.
8. Click **Add**. The query is generated.

### Updating a query

To update the query, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. Go to **Reports**. Select the category for which you want to update the chart.
3. The list of queries appears. Click the Edit icon of the query that you want to update.

   The report page opens.
4. Select a Group or type the group name. By default, all groups option is selected.
5. In the Period list, select period of the report. Select number of days. You can also select Custom option and then select the start and end dates for the reports.
6. As per the filter, Endpoint Name and User Name parameters are displayed.

   If you want to generate reports for a group, leave the endpoint name text box blank. If you want to generate reports for an endpoint name, enter the endpoint name in the text box. The reports will be generated for that endpoint name.
7. Enter user name in the User Name text box.
8. To add filters, click Add Filters. The parameters in the Add Filters are Endpoint Name and User Name. Select or clear the filter that you want to add or remove.
9. Select the columns to be displayed in the report. By default, all parameters are selected.
10. To generate the report on the selected parameters, click **Generate Report**. You can save the set of parameters. Click **Save** to save the selected parameters. When you visit this page next time, the reports of this saved parameters are displayed. The filter is changed after saving.

Note

You cannot edit the default query.

### Deleting a query

To delete the query, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. Go to **Reports**. Select the category for which you want to delete the chart.

   The list of queries appears.
3. Select the check box of the query that you want to delete.
4. In The Please Select list, select **Remove Query**.
5. Click **Submit**.
6. The confirmation message appears. Click **OK**.

   The selected query is removed.

Note

You cannot delete the default query.

### Duplicating a query

To duplicate the query, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. Go to **Reports**. Select the category for which you want to duplicate the chart.

   The list of queries appears.
3. Click the duplicate icon of the query that you want to duplicate.
4. The duplicated query appears in the next row. Edit the name of the query. Click tick icon to save the query.

   The selected query is duplicated.

### Moving a query

You can move the query only to the custom category.

To move the query, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. Go to **Reports**. Select the category for which you want to move the chart.

   The list of queries appears.
3. Select the check box of the query that you want to move.
4. In The Please Select list, select **Move To**.
5. Select the custom category where you want to move the query.
6. Click **Submit**.
7. The confirmation message appears. Click **OK**.

The selected query is moved.

Note

You cannot move the default query.

### Custom Category

You can create a custom category as per your requirement. In this category, you can move queries from the other categories, generate queries as per your requirement and generate custom reports.

#### Adding a custom category

To add a custom category, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. Go to **Reports**. The Reports page opens.
3. Click the **Add Category** button to create new category.
4. Enter name of the new category.
5. Click **Add**.

   The new category is added in the category list.

   You can edit or delete the custom category with help of icons.

## Admin

On the Admin page, the following features are available,

License

Activity Logs

User Roles

Notifications

Admin Settings

### License

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

### License Status

In the License Status window, you can check the current status of your license information.

The license information includes the following details:

| Title | Description |
|---|---|
| Company Name | Displays the name of the company to which Seqrite Endpoint Security Cloud is registered. |
| Product Name | Displays the product name, Seqrite Endpoint Security Cloud. |
| Product Edition | Displays the product edition. |
| Product Key | Displays the Product Key of Seqrite Endpoint Security Cloud. |
| License Expiry Date (GMT+5:30) | Displays expiry date of the Seqrite Endpoint Security Cloud license.<br>This field is not shown if the license type is **Subscription**. |
| License Type | Displays type of the license from the following,<br>• Trial<br>• Commercial<br>• Subscription |

The license status displays two half pie charts, one chart for EPS License and the other for DLP License. The chart displays the number of licenses utilized and licenses remaining.

### Update License Information

This feature is useful to synchronize your existing license information with Seqrite Activation Server. You can update your license information whenever required by clicking the **Update License Information** button.

### Licence Order

In the License Order window, you can place an order to renew your license, add new licenses to your existing setup, or buy additional features packs.

To place an order, follow these steps:

1. Select one of the following options:

- Renew my license: Helps you renew your current license.
- Add license for new endpoints: Helps you buy additional licenses.
- Edition Upgrade/Buy additional feature: Helps you upgrade the edition or buy additional features packs as per the following table:

2. Click **Place an Order**.

An order is created, and an automated Email is sent to the Partner to process your order.

## Activity Logs

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

You can select the number of days, either 7 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.
You can also export complete activity log to a CSV file. To export log activity, click CSV button. ActivityLog.csv file is downloaded.

## Settings

On this page, you can configure an interval for deleting older Activity Logs, Action History, Reports, Notifications, Alerts and News. You can set Client-Server communication interval time.

To do Admin Settings, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. Go to **Admin > Settings**.

   The following actions are displayed in the tabular format. Set the interval in days/Minutes for these actions. Set the switch to ON or OFF to apply the action.

   - **Delete Activity Log older than** 7 or 15 days
   - **Delete Action History older than** 7 or 15 days
   - **Delete Reports older than** 30 or 60 days
   - **Delete Notifications older than** 7 or 15 days
   - **Delete Alerts older than** 7 or 15 days
   - **Store Data-At-Rest scan reports for last** 1, 2, 3 scans
   - **Heartbeat interval** of 15 to 120 minutes
   - **Set missed heartbeat count to turn endpoint offline**, 1 to 5. When you select the count, duration appears in minutes next to the count. This duration is calculated by multiplying Heartbeat interval time with set missed heartbeat count. After this duration, endpoint will be offline.

- **Store Application Control scan reports for last** 1, 2, 3 scans.

## User Roles

The User Roles page displays the list of all the user roles. The table of the user role displays information such as Role Name, Role, Role Type, and Last Updated.

To select all the user roles from the list, select the check box in the header row.

To select an individual user role, select the check box in that row.

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 different types of user roles:

### Super Admin

A Super Admin user has all the privileges to access, manage and delete the features of Seqrite Endpoint Security Cloud. You cannot edit the privileges. The role type is default. There can be only one user with Super Admin privilege. The default user role name for Super Admin is "Super Admin".

### Admin

User with Admin privileges has privileges to access, manage and delete the features of Seqrite Endpoint Security Cloud. The default user role name for Admin is "Admin"’. You can create multiple user roles for Admin, if required.

### Report Viewer

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

### Group Admin

A Group Admin user can view and manage its own group only. The default user role name for Group Administrator is "Group Admin". 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 group only.

When Group Admin logs on, the Status page is displayed by default. The Group Admin has limited access to pages of Seqrite Endpoint Security Cloud.

## Add User role

To add a user role, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. Go to **Admin > User Roles**.
3. On the User Roles page, click **Add User Role**.

   The Add User role page appears.
4. From the **Role** list, select the type of role for which you want to create a user role.
5. In the **Role Name** text box, type the name of the role.
6. Configure access rights by selecting/clearing the check boxes.
7. To save your access rights, click **Add**.

   To assign the user role to the user, see Adding a User

## Edit User role

### Modifying Existing User Role

To modify the settings of an existing user role, follow these steps:

1. Log on to Seqrite Endpoint Security Cloud.
2. Go to Admin > User Roles.

   A list of all user roles appears.
3. Click the **Edit** icon for the user role that you want to edit.
4. Modify the access rights.
5. To save the modified access rights, click **Save**.

Note

You cannot edit or delete the default user role.

### Deleting User Role

To delete an existing user role, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. Go to **Admin > User Roles**.

   A list of all user roles appears.
3. Select the user role that you want to delete.
4. The delete action bar is enabled above the table. Select **Delete**.

   You can delete a user role if you have the right privileges to do so.

   A confirmation message appears.
5. To delete the user role, click **Yes**.

Note

You cannot edit or delete the default user role.

### Duplicating the User Role

To duplicate the user role, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. Go to **Admin > User Roles**.

   A list of all user roles appears.
3. Click the duplicate icon of the user role that you want to duplicate.
4. The duplicated user role appears in the next row. Edit the name of the user role.
5. Click tick icon to save the user role.

   The selected user role is duplicated. The privileges remain same.

You can change the privileges if required.

## Notifications

This page helps you set rules for sending notifications for events such as when update Agent virus definition are older and virus outbreak.

You need to create a rule and a list of Email addresses to send the notifications.

### Set rules to send notification

1. Enable the option, **Update Agent virus definition is older than 15 Days**. You can change the number of days in the list.
2. Enable the option, **Virus Outbreak**.

   The Virus Outbreak section expands.
3. Select values for the following to send the notification when the values are attended:
   - Number of virus incidents exceeds
   - Number of affected endpoints
   - Time span (minutes)
4. Enable the option, Synchronization with Active Directory failed.
5. Add Email Addresses for event notification. When the set rule condition is attended, a notification is sent to the Email addresses added here.
6. Enter Email address in the text box and click **Add**.
7. Click **Save**.

## Support

Seqrite provides extensive technical support for the registered users. It is recommended that you have all the necessary details with you during the call to receive efficient support from the support executives of Seqrite.

The Support gives you options of Web Support where you can find answers to the most frequently asked questions, options to submit your queries, send emails about your queries, or contact us directly.

The Support page includes the following options:

- **Email Support**: Includes Submit Ticket that redirects you to our Support webpage. Here you can read some of the most common issues with answers. If you do not find an answer to your issue you submit a ticket.
- **Live Chat Support**: Using this option, you can chat with our support executives.

- **Support Contacts**: To know support contacts, please visit http://www.seqrite.com/contact_support

### Head Office Contact Details

Quick Heal Technologies Limited

(Formerly known as Quick Heal Technologies Pvt. Ltd.)

Reg. Office: Marvel Edge, Office No.7010 C & D, 7th Floor,

Viman Nagar, Pune 411014, Maharashtra, India.

Official Website: http://www.seqrite.com.

Email: support@seqrite.com

# Header Icons

## Alerts

The Alerts icon on the header displays alert messages for the following critical situations:

- Update Manager not updated
- License Suspended or Blocked
- License limit reached
- License about to expire
- DLP License count is updated

1. Click **Update Now** to update the selected alert. The request of update is sent.
2. Click **OK**.
3. Click **See all alerts**, to view the list of all alerts.
4. Click **Update Now** to update the selected alert. The request of update is sent.
5. Click **Delete** to delete the selected alert message. A confirmation message appears.
6. Click **OK** to confirm.

Renew/Buy option also available to renew expired licenses or add an additional endpoint.

## Notification

The Notification icon on the header displays the list of Notifications. Notifications such as Update Agent installation failed, and Client deployment failed are displayed. When you click the notification, a new window of Notification Details appears showing the details.

Click **See all Notification** to go to Notifications page.

The Notifications table appears. You can view details of the notification by clicking View icon.

### Deleting the notification

To delete the notification, follow these steps:

1. On the notification page, you can view list of notifications.
2. Select the check box of the notification that you want to delete. An action bar is enabled above the table.
3. Select **Delete**.
4. The confirmation message appears. Click **OK**.

## Editing the User Profile

User profile is the information about the registered user. You can view name, contact details and Role of the logged-on user.

To edit the user profile, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. On the header, click the arrow next to the human icon.
3. Click **Edit Profile**.
4. Edit the user details as per your requirement.
5. Click **Save**.

You can cancel the changes, with **Reset** button, if required.

## Change Password

To change the password, follow these steps:

1. Log on to **Seqrite Endpoint Security Cloud**.
2. On the header, click the arrow next to the human icon.
3. Click **Change Password**.

   The Change Password page appears.
4. Enter old password and new password. Enter the new password to confirm.
5. Click Change Password.

## Log off

To log off from the Seqrite Endpoint Security Cloud portal, follow these steps:

1. On the header, click the arrow next to the human icon.
2. Click **Logout**.

## News

The Alerts icon on the header displays the news published by Seqrite about security information, new service pack released, new Seqrite Endpoint Security Cloud version released etc.