eScan™

Enterprise Security

# eScan Enterprise DLP - Cloud

## User Guide

Product Version: 22.0.0000.xxxx

Document Version: 22.0.0000.xxxx

24x7 FREE
Online Technical Support

support@escanav.com
https://forums.escanav.com

An ISO 27001 Certified Company

www.escanav.com

Any technical documentation provided by MicroWorld is copyrighted and owned by MicroWorld. Although MicroWorld makes every effort to ensure that this information is accurate, MicroWorld will not be liable for any errors or omission of facts contained herein. This user guide may include typographical errors, technical or other inaccuracies.

MicroWorld does not offer any warranty to this user guide's accuracy or use. Any use of the user guide or the information contained therein is at the risk of the user. MicroWorld reserves the right to make changes without any prior notice. No part of this user guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of MicroWorld Software Services Private Limited.

The terms MicroWorld, MicroWorld Logo, eScan, eScan Logo, MWL, and MailScan are trademarks of MicroWorld. Microsoft, MSN, Windows, and Windows Vista are trademarks of the Microsoft group of companies. All other product names referenced in this user guide are trademarks or registered trademarks of their respective companies and are hereby acknowledged. MicroWorld disclaims proprietary interest in the marks and names of others.

The software described in this user guide is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

| | |
|---|---|
| **Document Number:** | **5BUG/04.08.2024/22.x** |
| **Current Software Version:** | **22.0.0000.xxxx** |
| **Technical Support:** | **support@escanav.com** |
| **Sales:** | **sales@escanav.com** |
| **Forums:** | **https://forums.escanav.com** |
| **eScan Wiki:** | **https://wiki.escanav.com/wiki/index.php/** |
| **Live Chat:** | **https://www.escanav.com/english/livechat.asp** |
| **Published by:** | **MicroWorld Software Services Private Limited** |
| **Date:** | **August, 2024** |

# Content

# Introduction

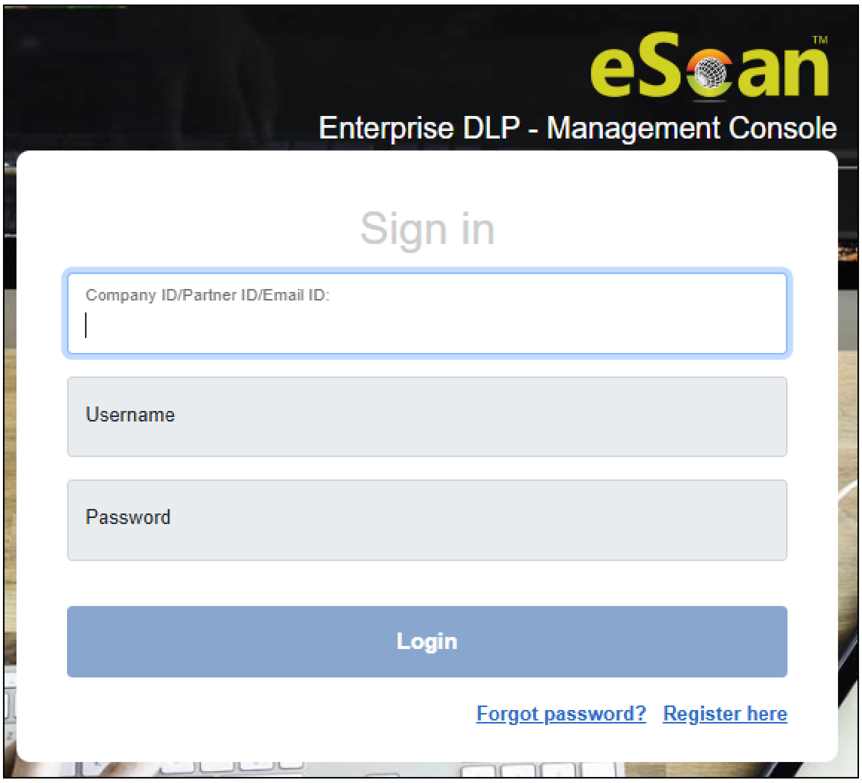
eScan Enterprise DLP (Data Leak Prevention) - Cloud Hosted is a data security solution for corporates. This excellent set of strategies, technologies, and techniques ensure that the end users do not transmit critical or sensitive data outside an organization network or its cloud infrastructure. Whether transmission of data is through message, email, file transfers, or certain other way, information can end up in unauthorized locations, leading to compliance issues, and this risk can be eliminated by eScan DLP.

As an Enterprise Solution, DLP needs to detect potential data breaches/data exfiltration attempts and prevent the same by monitoring, detecting and blocking sensitive data while in use (Endpoint actions), in motion (Network Traffic), and at rest (Data Storage). The DLP solution also needs to employ business rules to enforce regulatory compliance, classification and secure confidential information. With its advanced features, it gives protection against exfiltration attempts, monitors sensitive data access and/or leak, and permits 360 degree all round visibility of confidential file usage and protection of data tagged as critical by a user.

# Web Console Login

The web console login page can be accessed via this method.
To log in to the eScan Management Console, follow the steps given below:

1. Launch a web browser.
2. Enter the following URL: **dlp.escanav.com**
3. Web console login page appears.



eScan Enterprise DLP - Management Console

Sign in

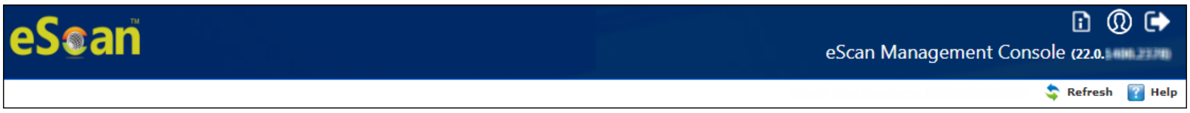
Company ID/Partner ID/Email ID:

Username

Password

4. Enter the login credentials defined during installation.
5. Click **Login**.

# Main Interface

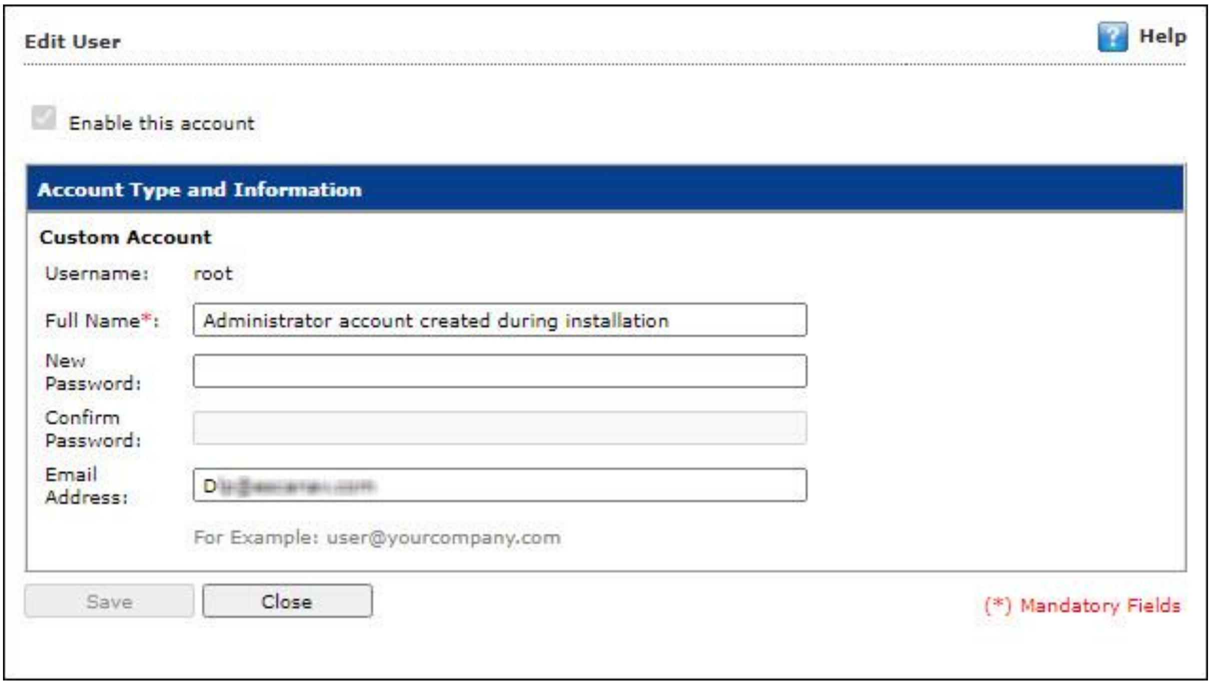


The links in the top right corner are explained below:

**About eScan**
Clicking **About eScan** opens MircoWorld's homepage in a new tab.

**Username**
Clicking **Username** lets you edit User Login details like Full name, Password and email address that you use to login in the eScan Management Console.

| | |
|---|---|
| Note | It is not allowed to configure your email address. |



Edit User

☑ Enable this account

Account Type and Information

Custom Account

Username: root

Full Name*: Administrator account created during installation

New Password:

Confirm Password:

Email Address: D[redacted]

For Example: user@yourcompany.com

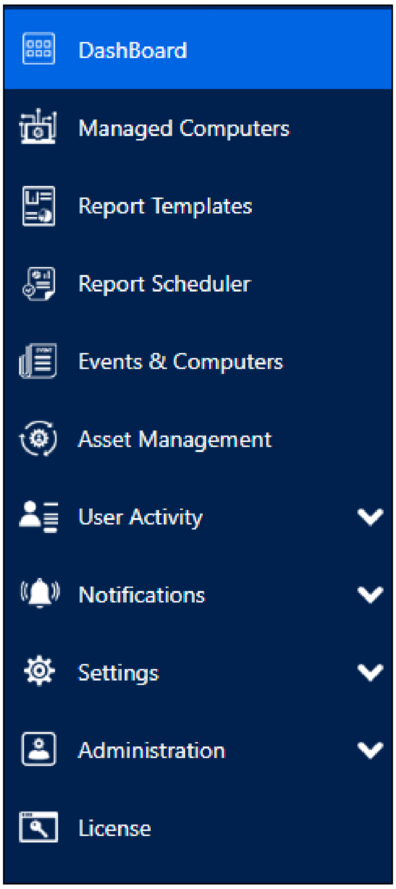
**Log off**
Clicking **Log off** logs you out of the eScan Management Console.

**Refresh**
Clicking **Refresh** let you refresh the eScan Management Console.

**Help**
This link displays the detailed information of eScan Management Console modules.

**Company Name**
This option displays user and company information.

# Navigation Panel



### Dashboard

The Dashboard module displays charts showing Deployment status, Protection status, DLP protection Status, Protection Statistics, DLP Statistics, Summary Top 10 and Asset Changes. The monitoring is done by escan Management Console of the computers for security violations. To learn more, click here.

### Managed Computers

The Managed Computers module lets you define/configure policies for computers. It provides various options for creating groups, adding tasks, moving computers from one group to the other and redefining properties of the computers from normal to roaming users and vice versa. To learn more, click here.

### Report Templates

The Report Templates module lets you create and view customized reports based on a given template, for a given period; sorted by date, computer, or action taken; and for a selected condition or target group. It also provides options for configuring or scheduling reports, viewing report properties, and refreshing or deleting existing reports. To learn more, click here.

### Report Scheduler

The Report Scheduler module lets you schedule a new reporting task, run an already created reporting schedule, or view its properties. To learn more, click here.

### Events and Computers

The Events and Computers module lets you monitor various activities performed on client's computer. You can view log of all events based on Event Status, Computer Selection or Software/ Hardware Changes on that client computer. Using the Settings option on the screen you can define settings as desired. To learn more, click here.

### Asset Management

The Asset Management module provides you the entire hardware configuration and list of software installed on computers in a tabular format. Using this module, you can easily keep a track of all the Hardware as well as Software resources installed on all the Computers connected to the Network. Based on different search criteria you can easily filter the information as per your requirement. It also lets you export the entire system information available through this module in PDF, Microsoft Excel or HTML formats. To learn more, click here.

### User Activity

The User Activity module lets you monitor different tasks/activities like printing, session login time or actions on files in the client computers. To learn more, click here.

### Notifications

The Notifications module provides you options to enable different notifications when different actions/incidents occur on the endpoints. You may choose to be notified or not to be notified based on the significance of these actions in your business. To learn more, click here.

### Settings

The Settings module lets you configure eScan Console timeout settings, dashboard settings, and exclude client settings for eScan. To learn more, click here.

### Administration

The Administration module lets you create User Accounts and allocate them Admin rights for using eScan Management Console. It is helpful in a large organization where installing eScan client on large number of computers in the organization may consume lot of time and efforts. By using this module, you can allocate rights to the other employees which will allow them to install eScan Client and implement policies and tasks on other computers. To learn more, click here.

**License**

The License module lets you manage license of users. You can add, activate, and view the total number of licenses available for deployment, number of licenses deployed, and number of licenses remaining with their corresponding values. You can also move the licensed computers to non-licensed computers and non-licensed computers to licensed computers. To learn more, click here.

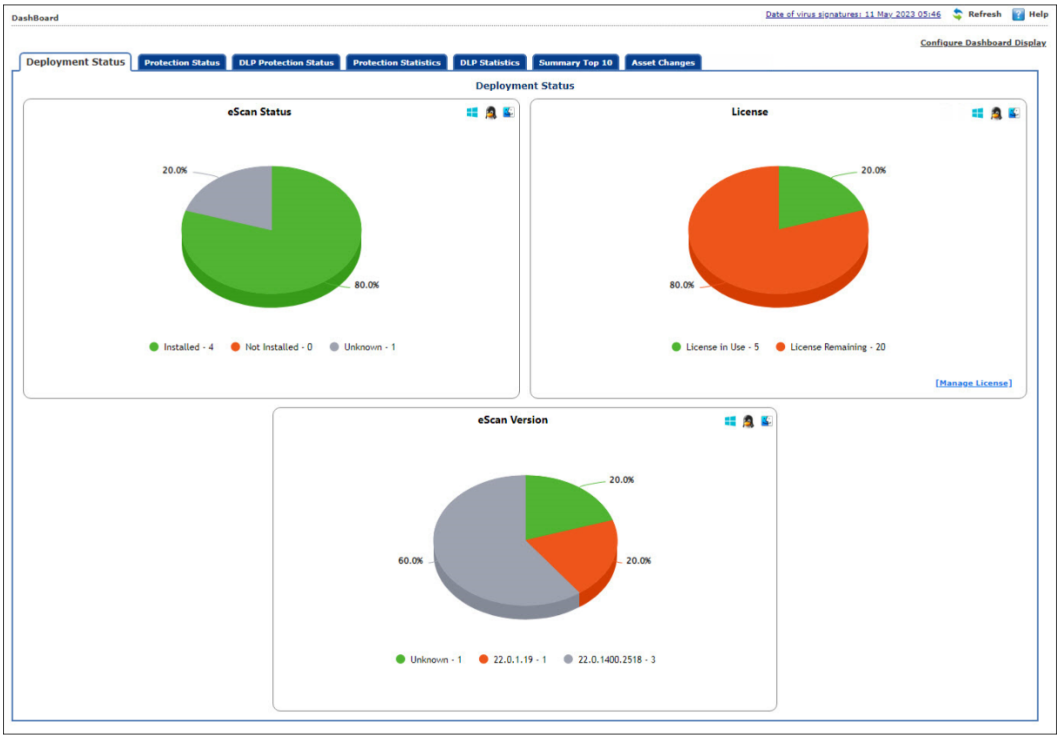
# Dashboard

The Dashboard module displays statistics and status of eScan Client installed on computers in the form of pie chart. It consists of following tabs:

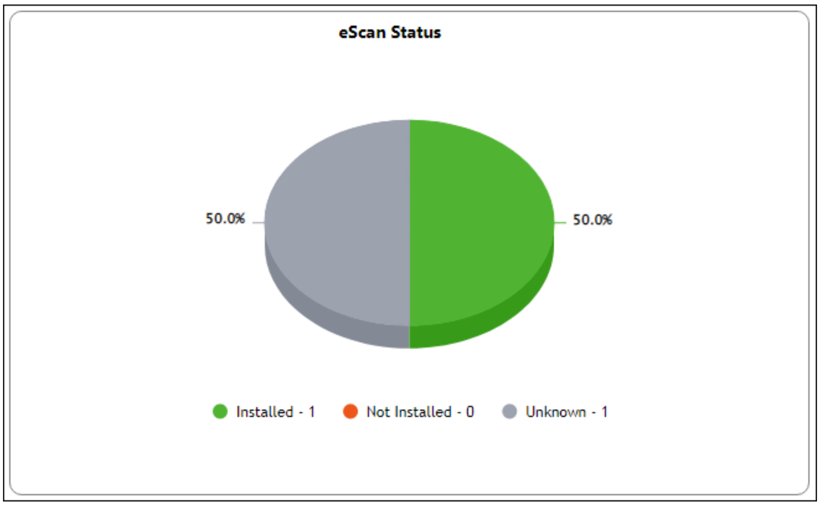
- **Deployment Status**
- **Protection Status**
- **DLP Protection Status**
- **Protection Statistics**
- **DLP Statistics**
- **Summary Top 10**
- **Asset Changes**

## Deployment Status

This tab displays information about eScan Client installed on computers, active licenses, and current eScan version number in use.

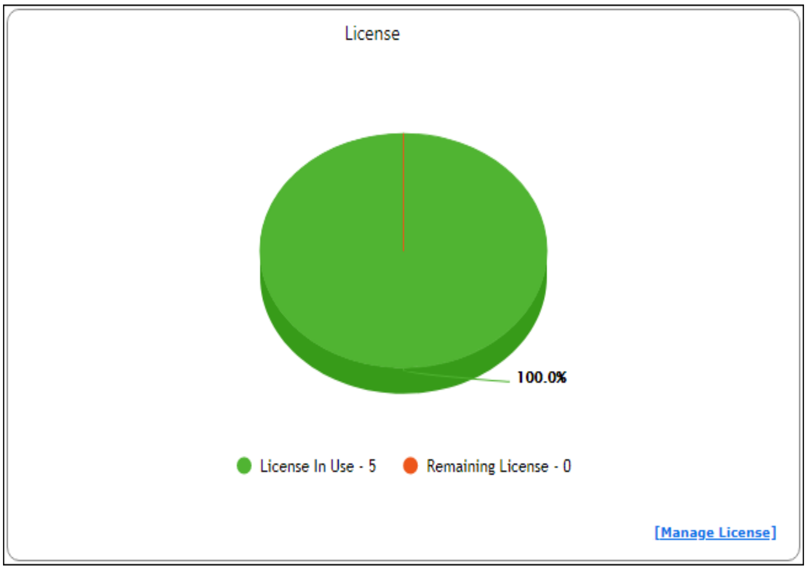


# eScan Status



**Installed** – It displays the number of computers on which eScan Client is installed.
**Not Installed -** It displays the number of computers on which eScan Client is not installed.
**Unknown -** It displays the number of computers on which Client installation status is unknown. (Server is unable to receive information from the computers for a long time)

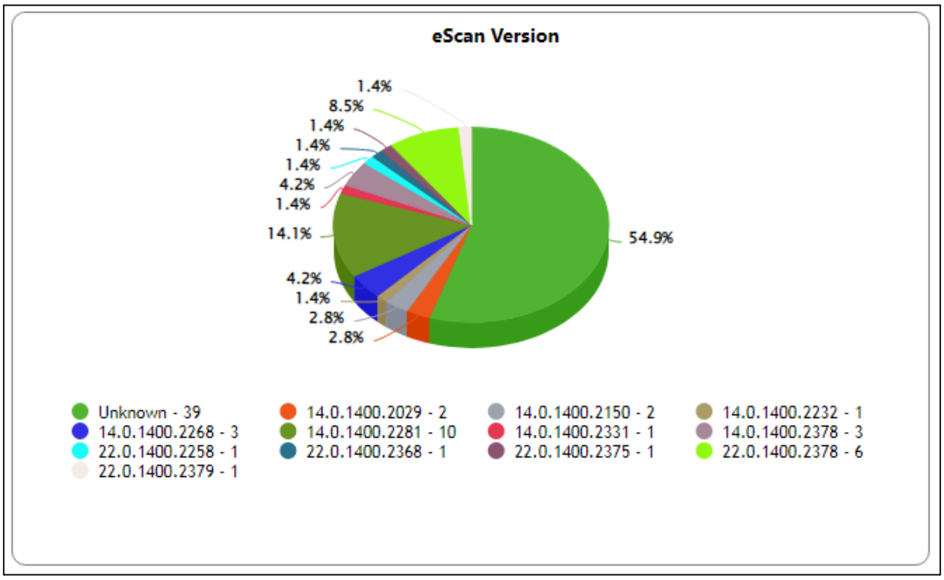
# License



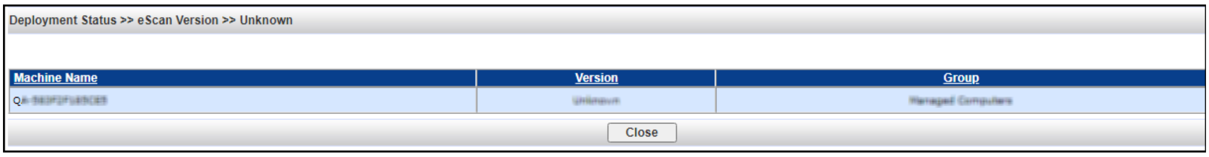
**License in Use -** It displays the number of licenses that are active.
**Licenses Remaining -** It displays the number of remaining licenses.

# eScan version

The eScan Version chart shows the total number of eScan versions installed on the computers in the network.



Click on the numbers on the right-side of the each version, you can view the details of the computers.

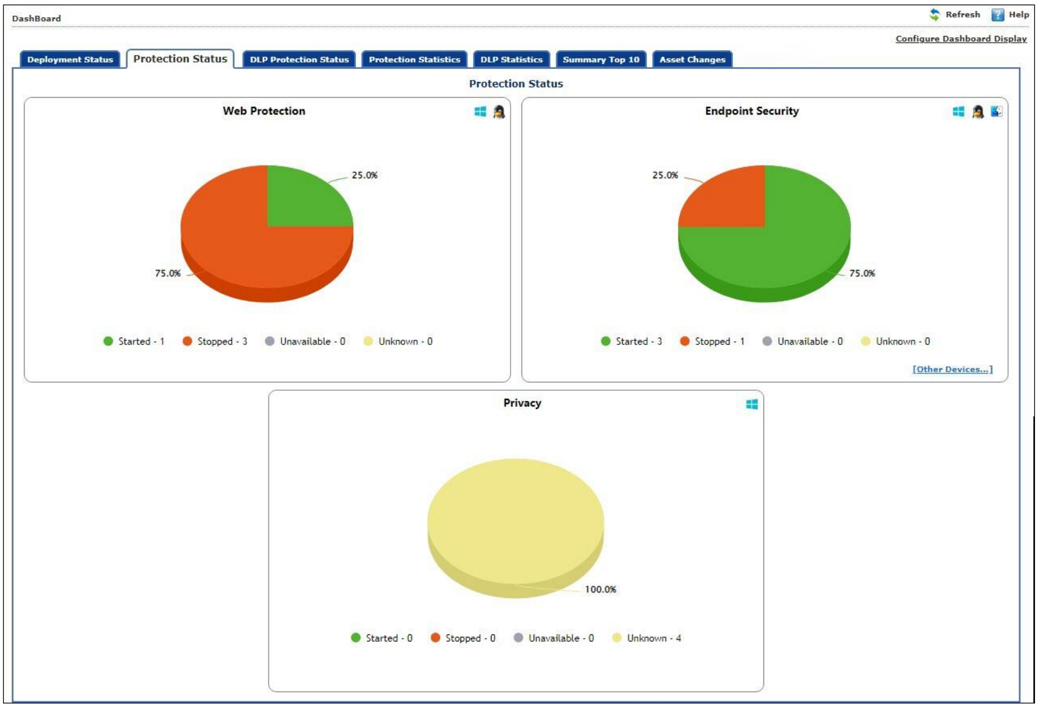

Deployment Status >> eScan Version >> Unknown

| Machine Name | Version | Group |
|---|---|---|
| [redacted] | [redacted] | [redacted] |

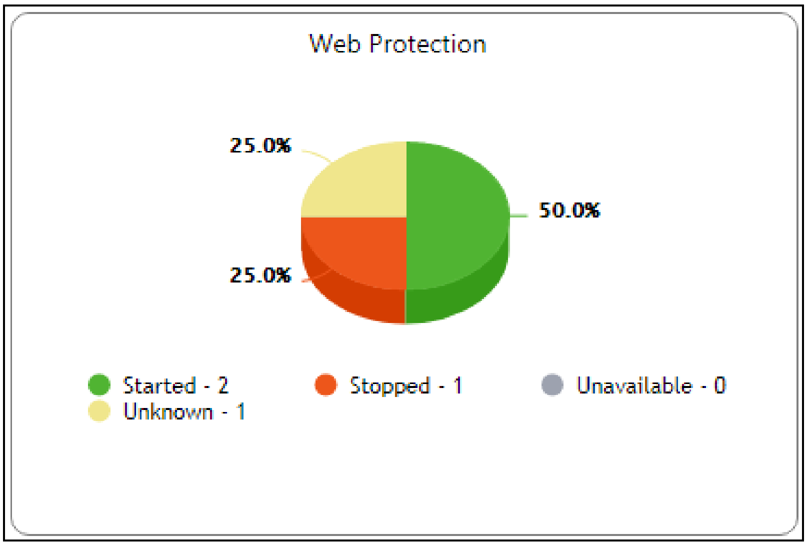
| NOTE | Clicking underlined numerical displays detailed information for computers. |
|---|---|

# Protection Status

This tab displays the status of eScan Client's modules along with the Update and Scan status since last 7 days.



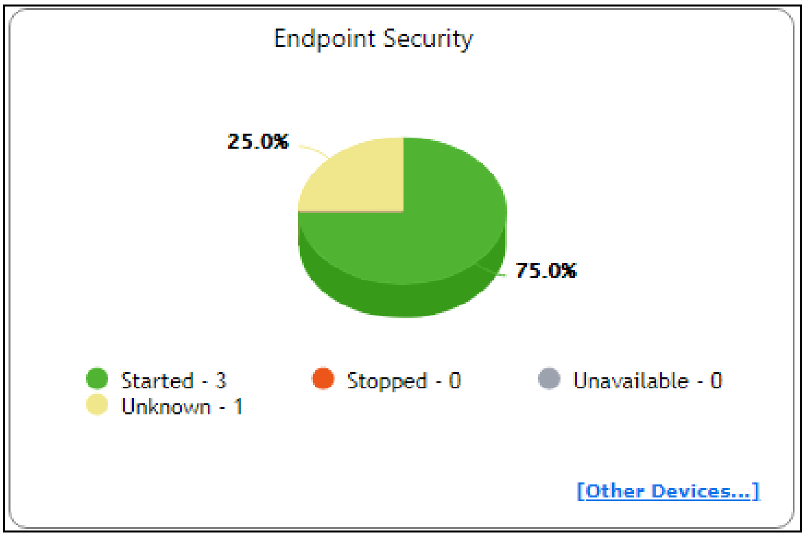
## Web Protection



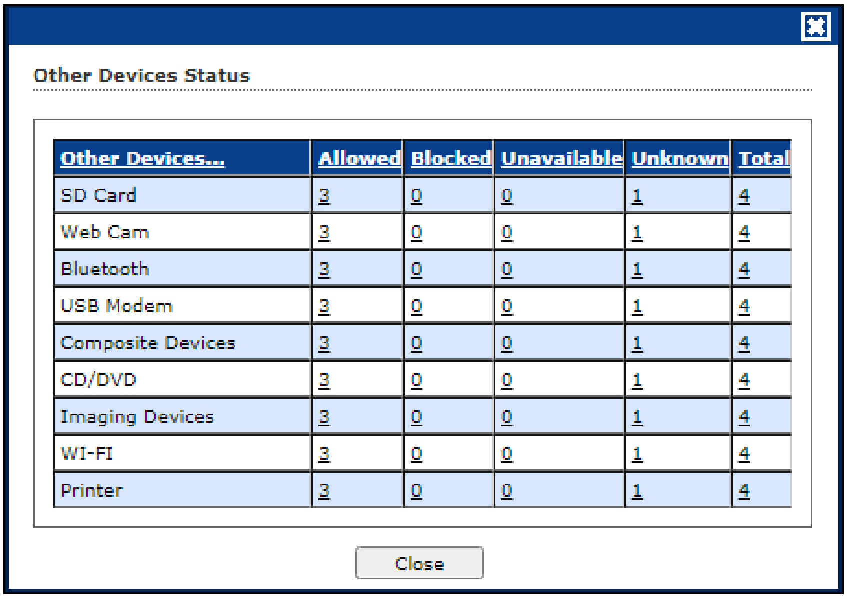
**Started** – It displays the number of computers on which the Web Protection module is in started state.
**Stopped** – It displays the number of computers on which the Web Protection module is in stopped state.
**Unavailable** – It displays the number of computers on which the Web Protection module is unavailable.

**Unknown** – It displays the number of computers on which the Web Protection module status is unknown.

# Endpoint Security



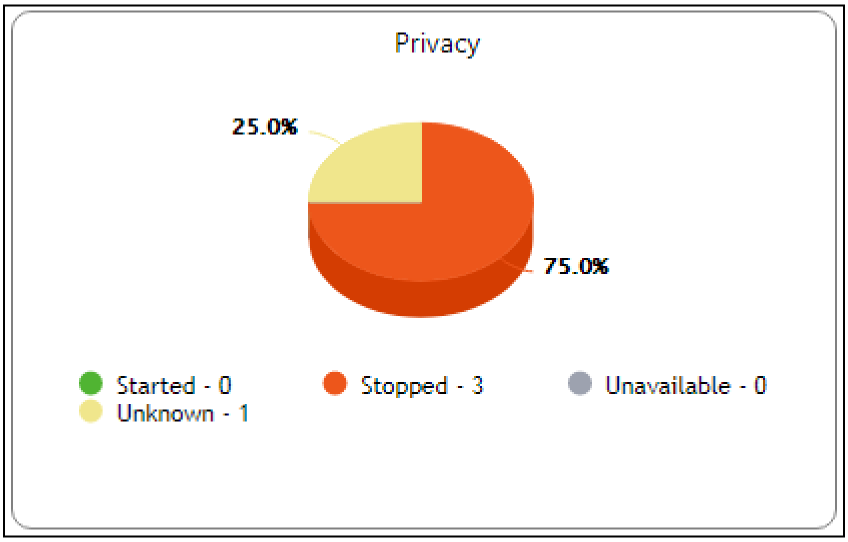
**Started -** It displays the number of computers on which the Endpoint Security module is in started state.
**Stopped -** It displays the number of computers on which the Endpoint Security module is in stopped state.
**Unavailable** – It displays the number of computers on which the Endpoint Security module is unavailable.
**Unknown -** It displays the number of computers on which the Endpoint Security module status is unknown.
Clicking **Other Devices** displays details about other devices.



Other Devices Status

| Other Devices... | Allowed | Blocked | Unavailable | Unknown | Total |
|---|---|---|---|---|---|
| SD Card | 3 | 0 | 0 | 1 | 4 |
| Web Cam | 3 | 0 | 0 | 1 | 4 |
| Bluetooth | 3 | 0 | 0 | 1 | 4 |
| USB Modem | 3 | 0 | 0 | 1 | 4 |
| Composite Devices | 3 | 0 | 0 | 1 | 4 |
| CD/DVD | 3 | 0 | 0 | 1 | 4 |
| Imaging Devices | 3 | 0 | 0 | 1 | 4 |
| WI-FI | 3 | 0 | 0 | 1 | 4 |
| Printer | 3 | 0 | 0 | 1 | 4 |

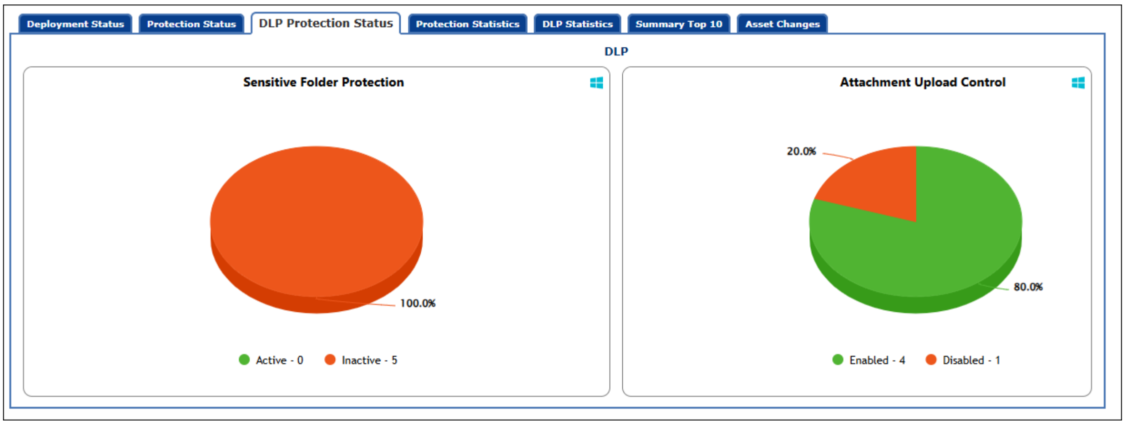
## Privacy



**Started -** It displays the number of computers on which the Privacy Control module is in started state.
**Stopped -** It displays the number of computers on which the Privacy Control module is in stopped state.
**Unavailable -** It displays the number of computers on which the Privacy Control module of eScan is unavailable.
**Unknown -** It displays the number of computers on which the Privacy Control module status is unknown.

# DLP Protection Status

This tab displays the protection status of DLP modules on all the managed computers with eScan client installed.

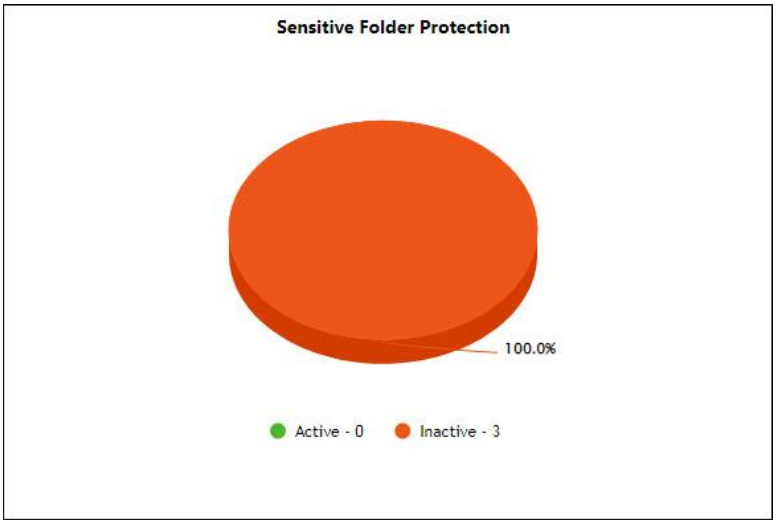


The DLP Protection Status tab contains the status information of the following modules:

- **Sensitive Folder Protection**
- **Attachment Upload Control**

## Sensitive Folder Protection

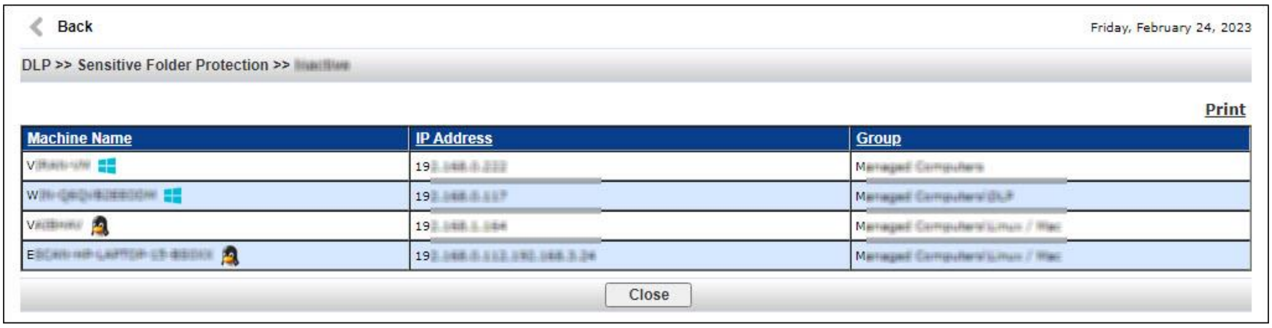
This chart displays the protection status of Sensitive Folder Protection module:



- **Active:** It shows the number of computers on which the Sensitive Folder Protection is active.
- **Inactive:** It shows the number of computers on which the Sensitive Folder Protection is not active.

| NOTE | You can view the computer details by clicking on the displayed numbers for each section of the module. |
|---|---|

After clicking on the displayed number, a window opens as shown below, displaying the computer details of the module:



Friday, February 24, 2023

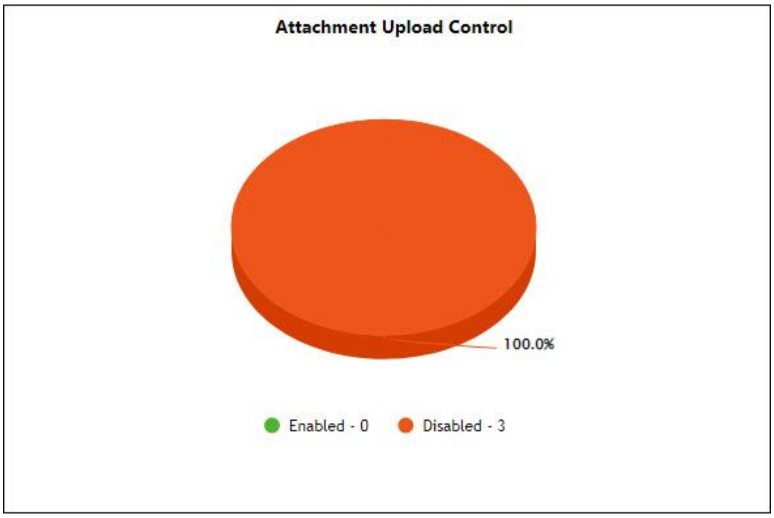
DLP >> Sensitive Folder Protection >> [redacted]

| Machine Name | IP Address | Group |
|---|---|---|
| V[redacted] | 19[redacted] | M[redacted] |
| W[redacted] | 19[redacted] | M[redacted] |
| V[redacted] | 19[redacted] | M[redacted] |
| E[redacted] | 19[redacted] | M[redacted] |

Additionally, you can print this data using **Print** option at the top-right corner in the same window.

# Attachment Upload Control

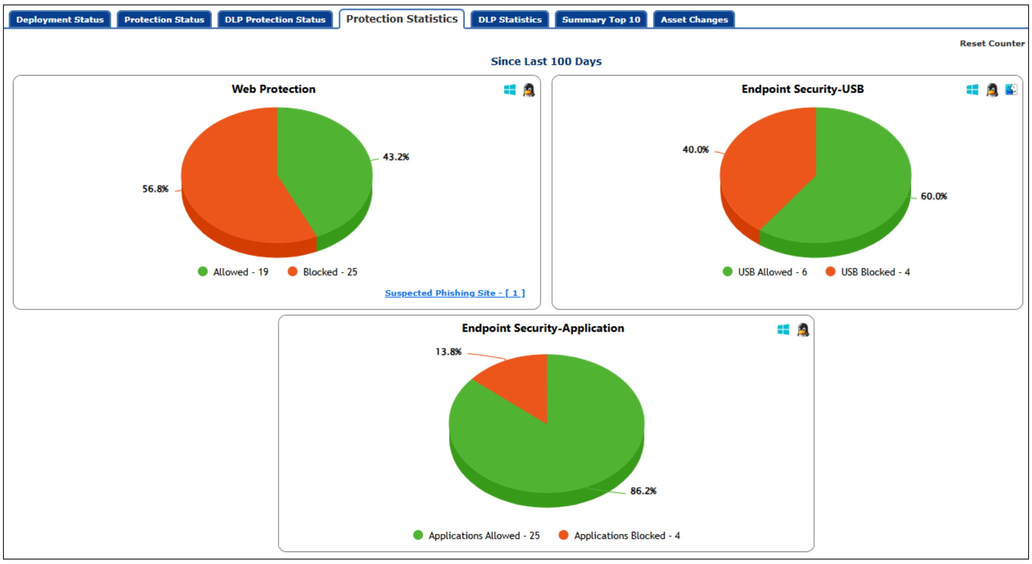
This chart displays the protection status of Attachment Upload Control module:



- **Enabled:** It shows the number of computers on which the Attachment Upload Control is turned on.
- **Disabled:** It shows the number of computers on which the Attachment Upload Control is turned off.

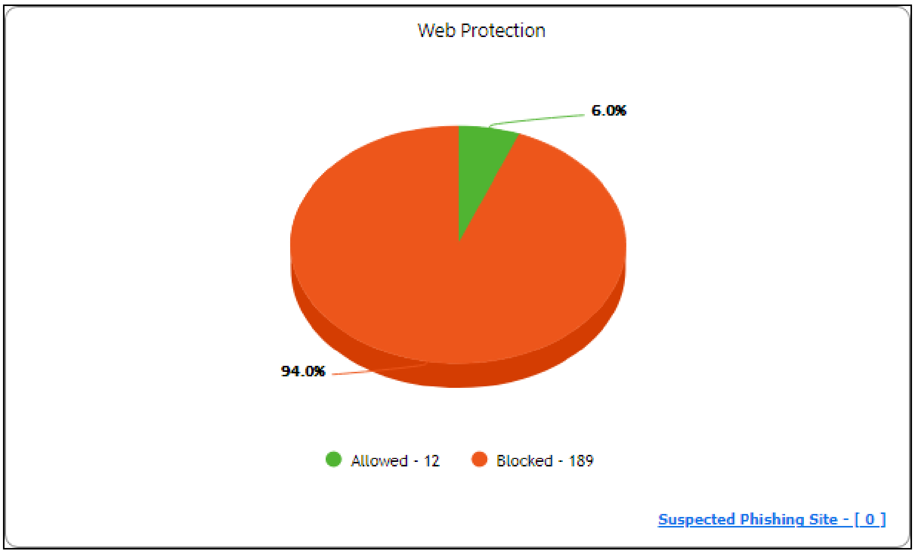
# Protection Statistics

This tab displays activity statistics and action taken by all modules of eScan Client since last seven days in pie chart format.



**Reset Counter**
Clicking **Reset Counter** resets all the statistics to zero.

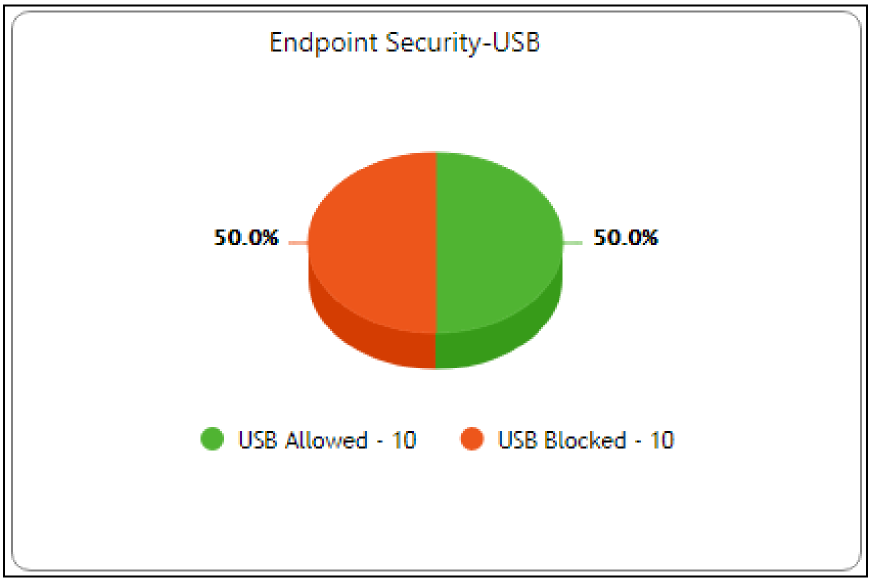
# Web Protection



**Allowed** – It displays the number of websites to which access was allowed by Web Protection module.
**Blocked** – It displays the number of websites to which access was blocked by Web Protection module.
**Suspected Phishing Site** – It displays the number of systems on which suspected phishing sites were blocked. After clicking the numerical, Suspected Phishing Site window appears displaying System Name, Site Status, and Computer Group.

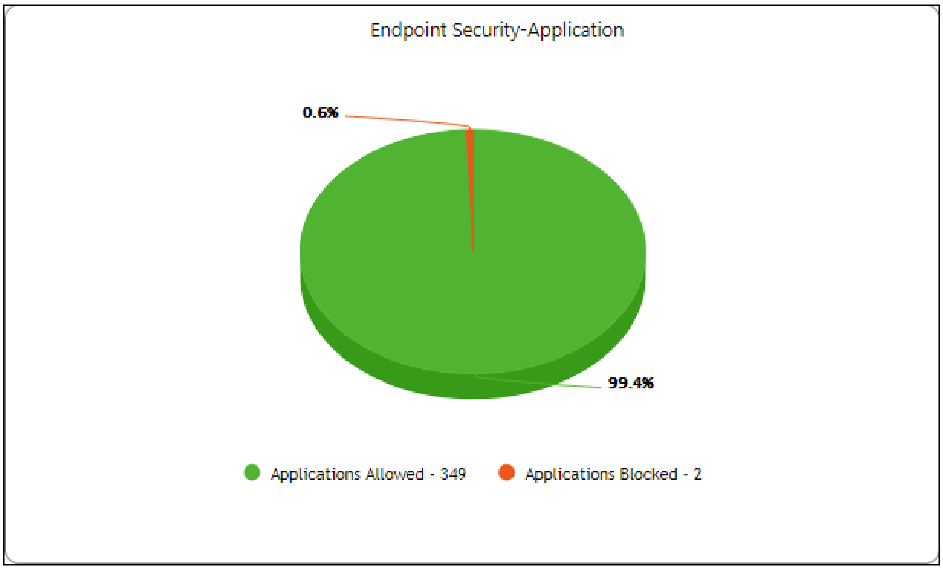
Clicking **Site Status** further displays Date, Time, Website name and action taken.

## Endpoint Security-USB



**USB Allowed** – It displays the number of USB access allowed along with the details for the same by Endpoint Security-USB module.
**USB Blocked** – It displays the number of USB access blocked along with the details for the same by Endpoint Security-USB module.

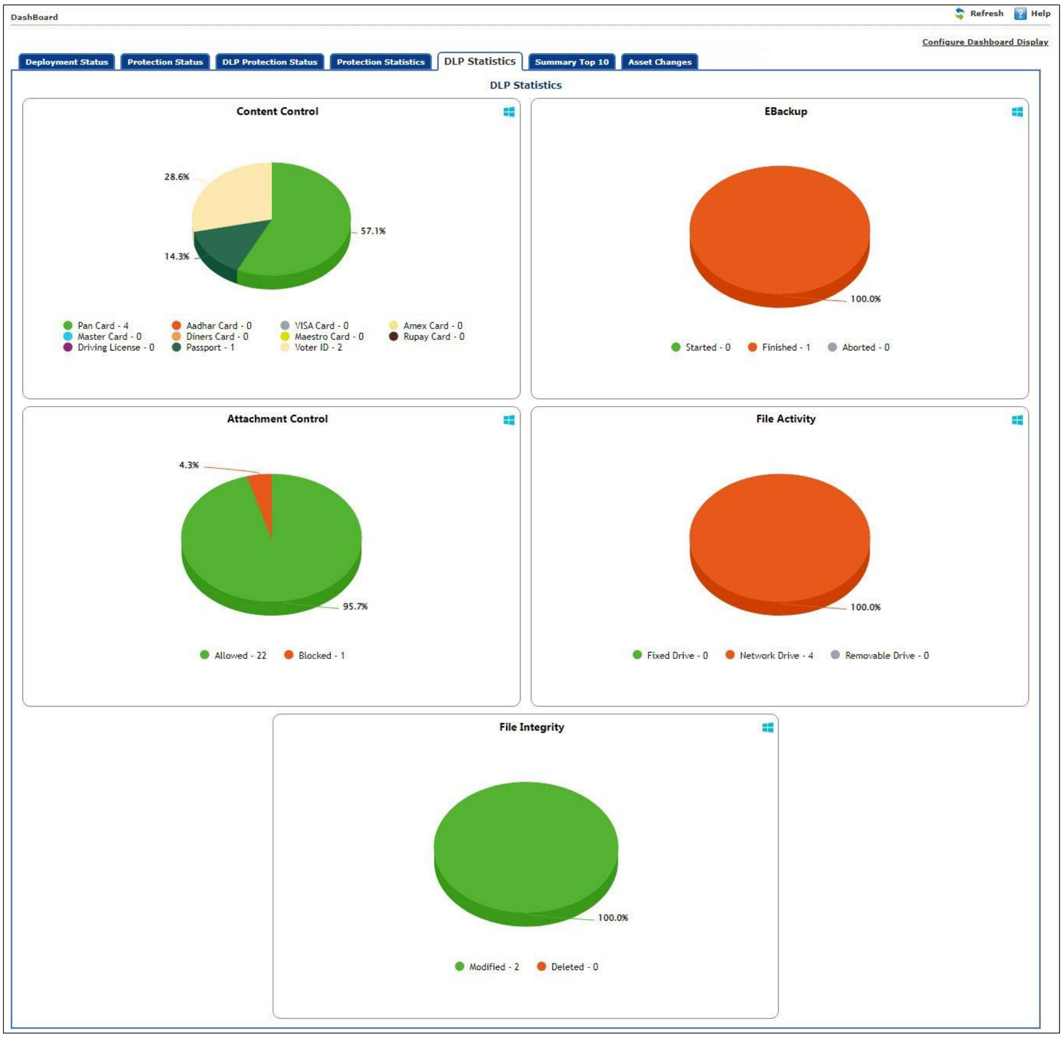
## Endpoint Security-Application



**Applications Allowed** – It displays the number of applications allowed by Endpoint Security-Application module.
**Applications Blocked** – It displays the number of applications blocked by Endpoint Security-Application module.

# DLP Statistics

This tab displays the protection statistics of DLP modules on all the managed computers with eScan client installed.

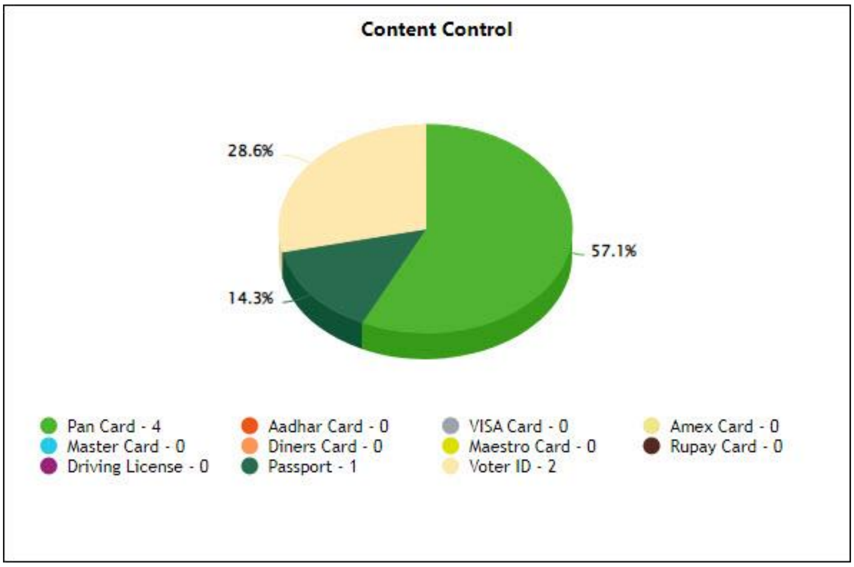


The DLP Statistics tab contains the statistical information of the following modules:

- **Content Control**
- **EBackup**
- **Attachment Control**
- **File Activity**
- **File Integrity**

# Content Control

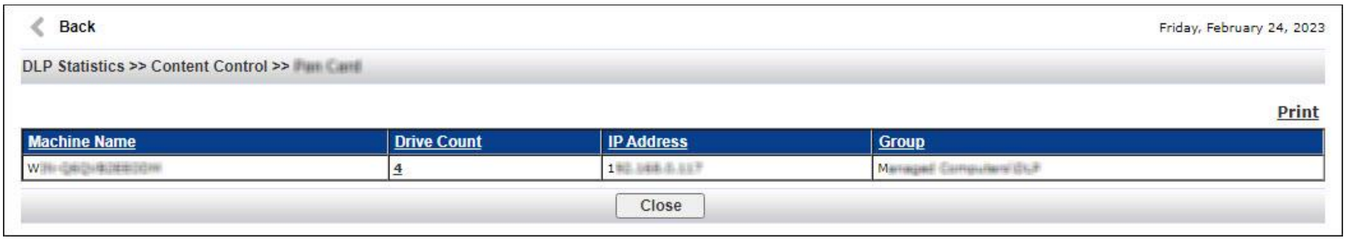
This chart displays the protection statistics of Content Control module:



- **Pan Card:** It displays the number of computers by which the Pan Card details have been uploaded.
- **Aadhar Card:** It displays the number of computers by which the Aadhar card details have been uploaded.
- **VISA Card:** It displays the number of computers by which the VISA Debit/Credit card details have been uploaded.
- **Amex Card:** It displays the number of computers by which the American Express Debit/Credit card details have been uploaded.
- **Master Card:** It displays the number of computers by which the Master Debit/Credit card details have been uploaded.
- **Diners Card:** It displays the number of computers by which the Diners card details have been uploaded.
- **Maestro Card:** It displays the number of computers by which the Maestro card details have been uploaded.
- **Rupay Card:** It displays the number of computers by which the Rupay Debit/Credit card details have been uploaded.
- **Driving License:** It displays the number of computers by which the Driving license details have been uploaded.
- **Passport:** It displays the number of computers by which the Passport details have been uploaded.
- **Voter ID:** It displays the number of computers by which the Voter ID card details have been uploaded.

| | |
|---|---|
| **NOTE** | • eScan blocks the attempts by user to upload/leak the Confidential information outside the network.<br>• You can view the sensitive file details that user attempted to upload (but blocked by eScan) along with the computer details by clicking on the displayed numbers for each object of the module. |

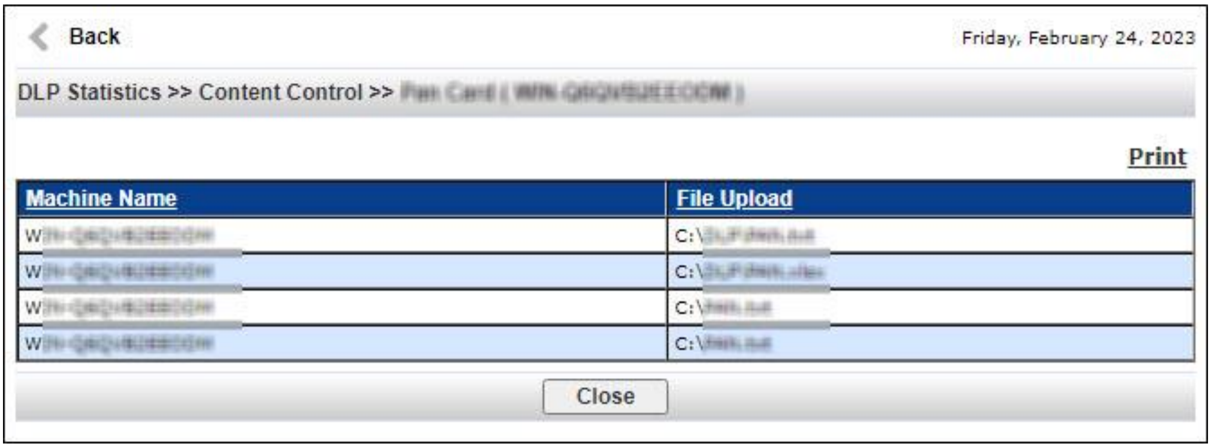
After clicking on the displayed number of particular document type, a window opens as shown below, displaying the computer details and drive count:



DLP Statistics >> Content Control >> [redacted]

| Machine Name | Drive Count | IP Address | Group |
|---|---|---|---|
| W[redacted] | 4 | 1[redacted] | [redacted] |

Click on the **Drive Count** to view the uploaded document details.
Another window opens as shown below displaying the computer name and the path from where the user attempted to upload/leak the confidential file.



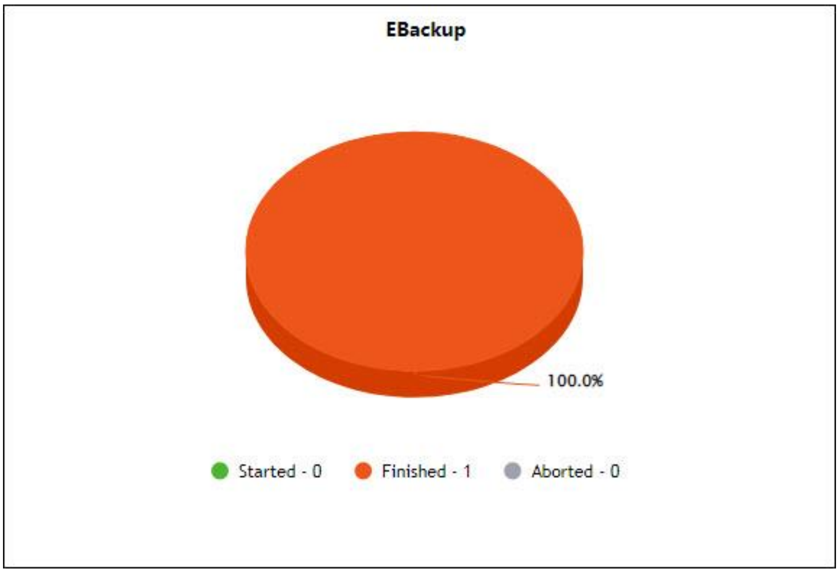
DLP Statistics >> Content Control >> [redacted]

| Machine Name | File Upload |
|---|---|
| W[redacted] | C:\[redacted] |
| W[redacted] | C:\[redacted] |
| W[redacted] | C:\[redacted] |
| W[redacted] | C:\[redacted] |

You can print this data using **Print** option at the top-right corner in the same window.

# EBackup

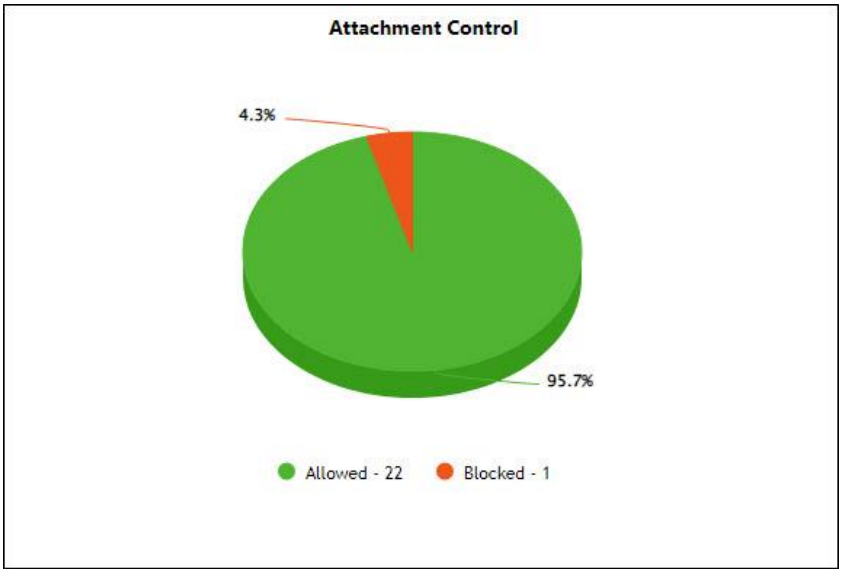
This chart displays the protection statistics of EBackup module:



- **Started:** It shows the number of computers on which the EBackup session has started.
- **Finished:** It shows the number of computers on which the EBackup session has completed.
- **Aborted:** It shows the number of computers on which the EBackup session has aborted.

# Attachment Control

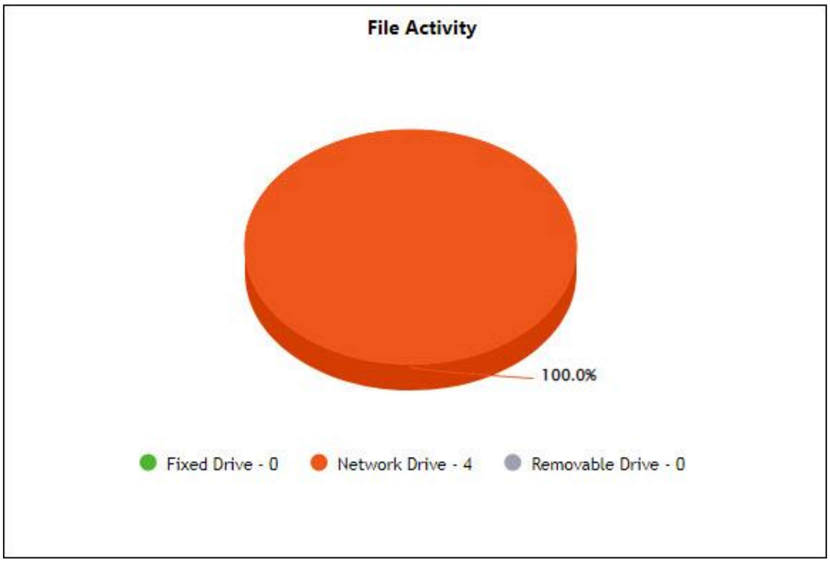
This chart displays the protection statistics of Attachment Control module:



- **Allowed:** It shows the number of attachments allowed from the managed computers.
- **Blocked:** It shows the number of attachments blocked from the managed computers.

# File Activity

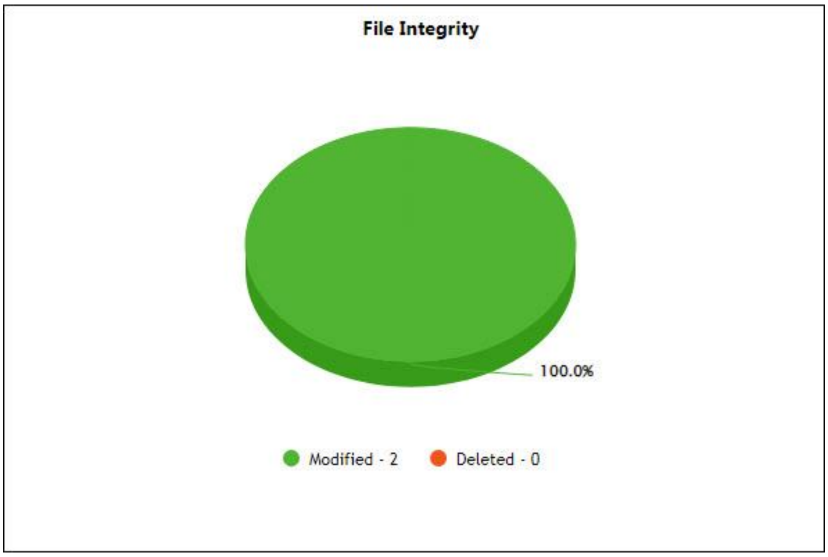
This chart displays the protection statistics of File Activity module:



- **Fixed Drive:** It shows the number of file activities in the fixed drive of managed computers.
- **Network Drive:** It shows the number of file activities in the network drive of managed computers.
- **Removable Drive:** It shows the number of file activities in the removable drive of managed computers.

# File Integrity

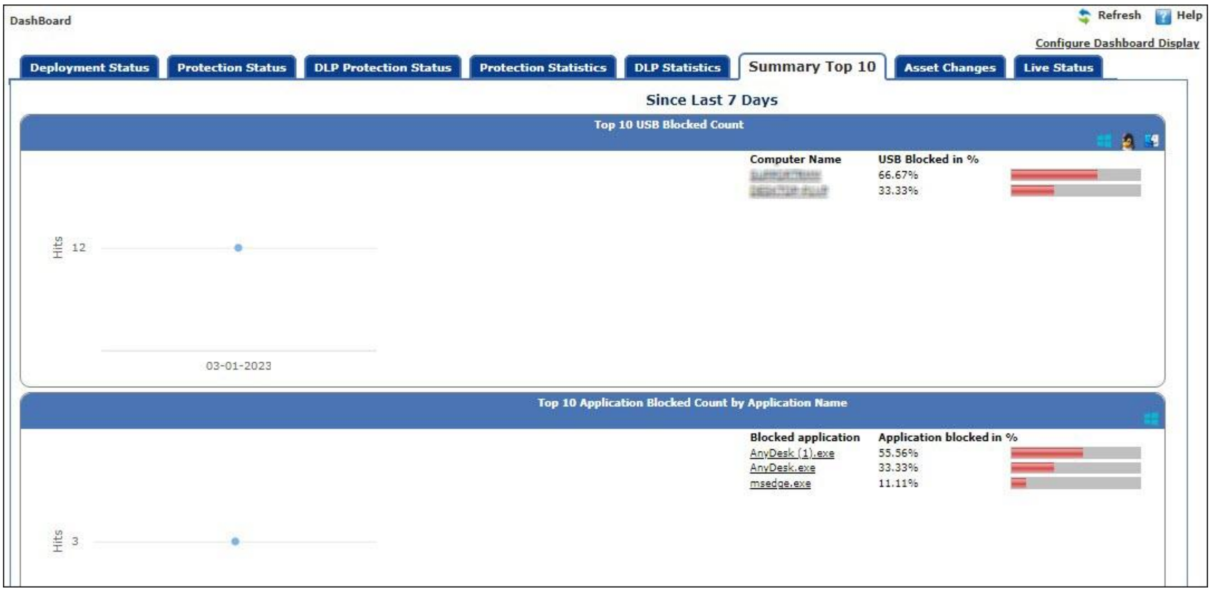
This chart displays the protection statistics of File Integrity module:



- **Modified:** It shows the number of files modified from the managed computers.
- **Deleted:** It shows the number of files deleted from the managed computers.

# Summary Top 10

This Tab displays top 10 Summary of various actions taken by eScan on all computers since last seven days along with bar chart and graph. This tab can be configured by clicking **Configure Dashboard Display**.



Since Last 7 Days

Top 10 USB Blocked Count

| Computer Name | USB Blocked in % |
|---|---|
| [redacted] | 66.67% |
| [redacted] | 33.33% |

Top 10 Application Blocked Count by Application Name

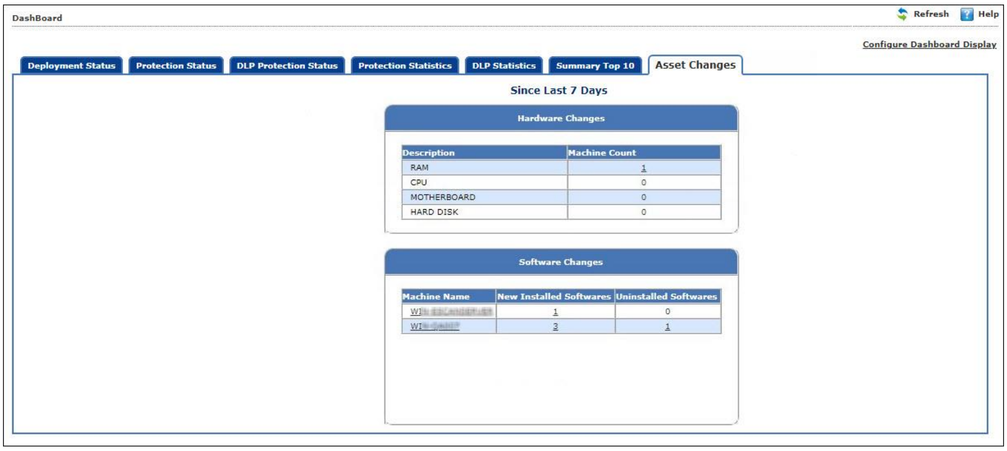
| Blocked application | Application blocked in % |
|---|---|
| AnyDesk (1).exe | 55.56% |
| AnyDesk.exe | 33.33% |
| msedge.exe | 11.11% |

The tab displays the summary for following parameters:

- Top 10 USB Blocked Count
- Top 10 Application Blocked Count by Application Name
- Top 10 Application Allowed Count by Application Name
- Top 10 Application Blocked Count by Computer Name
- Top 10 Application Allowed Count by Computer Name
- Top 10 Websites Blocked Count by Website Name
- Top 10 Websites Allowed Count by Website Name
- Top 10 Websites Blocked Count by Computer Name
- Top 10 Websites Allowed Count by Computer Name
- Top 10 Websites Blocked Count by Username
- Top 10 Websites Allowed Count by Username

# Asset Changes

This tab displays all hardware and software changes carried out on the endpoints since last seven days.



Since Last 7 Days

Hardware Changes

| Description | Machine Count |
|---|---|
| RAM | 1 |
| CPU | 0 |
| MOTHERBOARD | 0 |
| HARD DISK | 0 |

Software Changes

| Machine Name | New Installed Softwares | Uninstalled Softwares |
|---|---|---|
| WI[redacted] | 1 | 0 |
| WI[redacted] | 3 | 1 |

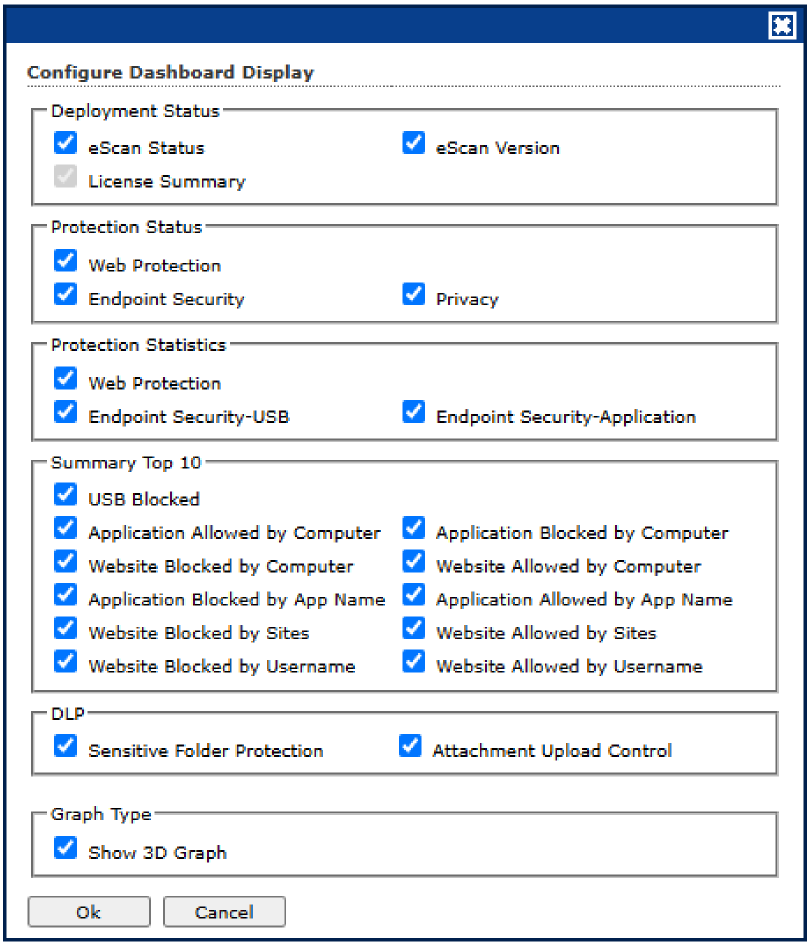
**Hardware Changes –** Clicking the underlined numerical displays hardware changes on computers since last seven days.

**Software Changes -** Clicking the underlined machine names displays softwares installed on the computers since last seven days. Clicking the underlined numerical displays installed / uninstalled softwares on computers since last seven days.

# Configure the Dashboard Display

To configure the Dashboard display:

1. In the Dashboard screen, at the upper right corner, click **Configure Dashboard Display**.
   Configure Dashboard Display window appears displaying tabs and their parameters.



Configure Dashboard Display

Deployment Status
- ☑ eScan Status
- ☑ eScan Version
- ☑ License Summary

Protection Status
- ☑ Web Protection
- ☑ Endpoint Security
- ☑ Privacy

Protection Statistics
- ☑ Web Protection
- ☑ Endpoint Security-USB
- ☑ Endpoint Security-Application

Summary Top 10
- ☑ USB Blocked
- ☑ Application Allowed by Computer
- ☑ Application Blocked by Computer
- ☑ Website Blocked by Computer
- ☑ Website Allowed by Computer
- ☑ Application Blocked by App Name
- ☑ Application Allowed by App Name
- ☑ Website Blocked by Sites
- ☑ Website Allowed by Sites
- ☑ Website Blocked by Username
- ☑ Website Allowed by Username

DLP
- ☑ Sensitive Folder Protection
- ☑ Attachment Upload Control

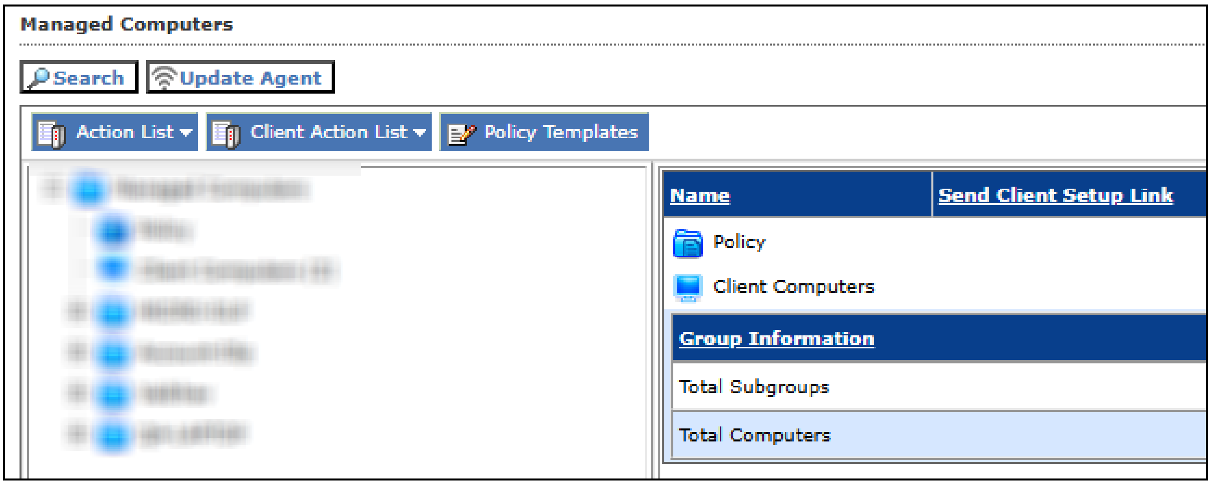
Graph Type
- ☑ Show 3D Graph

2. Select the parameters checkboxes to be displayed in the respective tabs.
3. Graph Type: select **Shows 3D Graph** checkbox to display 3D graph on dashboard.
4. Click **OK**.
   The tabs will be updated according to the changes.

# Managed Computers

To secure, manage, and monitor computers, it is necessary to add them in a group. The Managed Computers module lets you create computer groups, add computers to group, define policy templates for created groups and computers.
Based on the departments, user roles and designations, you can create multiple groups and assign them different policies. This lets you secure and manage computers in a better way.

In the navigation panel, click **Managed Computers**.
The Managed Computers screen appears on the right pane.



| Name | Send Client Setup Link |
|---|---|
| Policy | |
| Client Computers | |

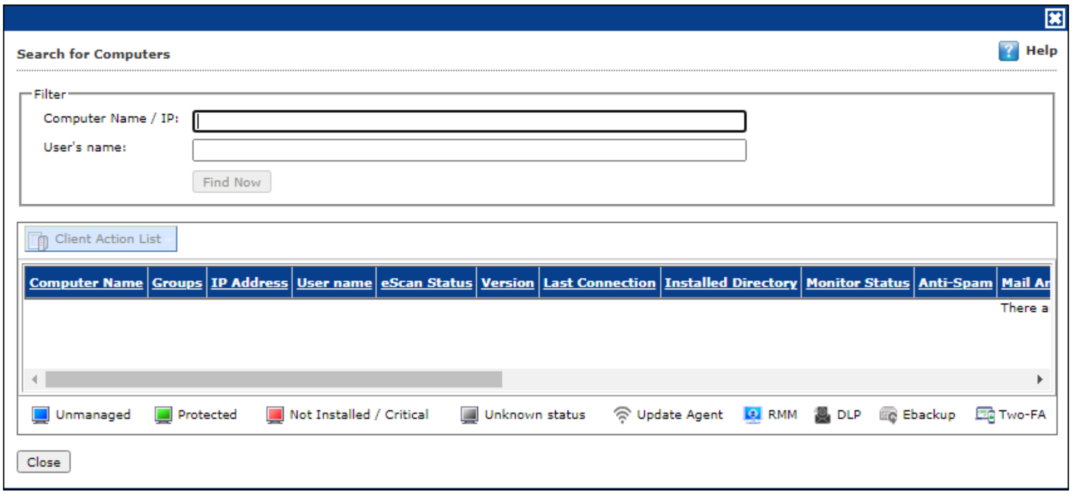
| Group Information |
|---|
| Total Subgroups |
| Total Computers |

The screen consists of following buttons:

- **Search**
- **Update Agent**
- **Action List**
- **Client Action List**
- **Policy Templates**

# Search

The Search feature lets you find any computer added in Managed Computers. After clicking **Search**, Search for Computers window appears.



**Computer Name/IP**
Enter a computer name or IP address.

**Username**
Enter a username.

Click **Find Now**.
The console will display the result.

**Client Action List**
Client Action List lets you take action for specific computer(s) in a group from search field.

# Update Agent

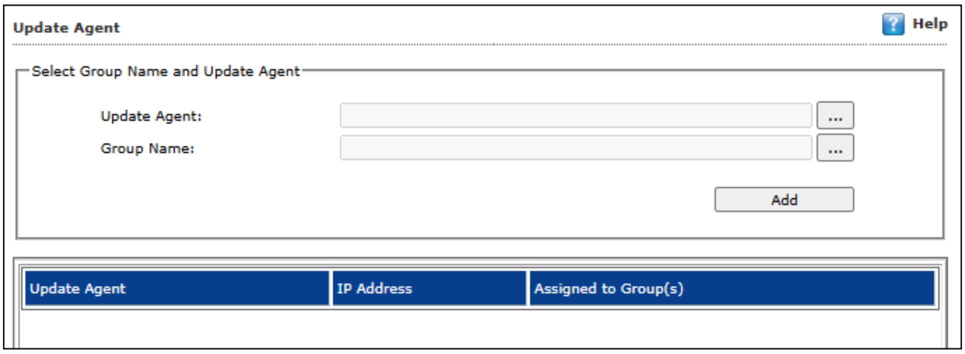
eScan lets you use a client computer as an update agent to deploy updates on group of computers. By default, eScan server distributes the virus definitions and policies to all the clients added in the web console. But, to reduce server's workload, you can create an Update Agent for the respective group(s). The Update Agent will receive virus definitions and policies from server and distribute it to the assigned group(s). For more details, please refer eScan Update Agents.

In Managed Computers screen, clicking **Update Agent** displays a list of computers that are acting as Update Agents for other computers in the group. This window also lets you add or remove Update Agents from this list. You can set an Update Agent for multiple groups.

## Adding an Update Agent

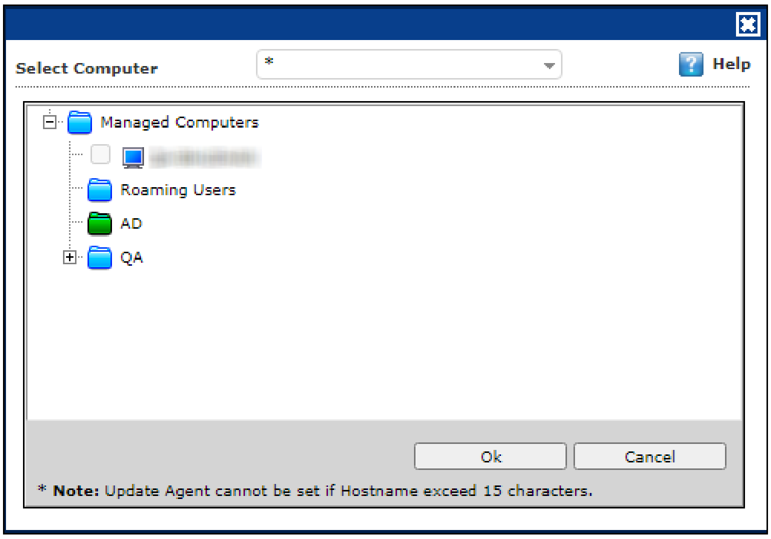
To add an Update Agent, follow the steps given below:

1. In Managed computers screen, click **Update Agent**.
   Update Agent window appears.



| Update Agent | IP Address | Assigned to Group(s) |
|---|---|---|

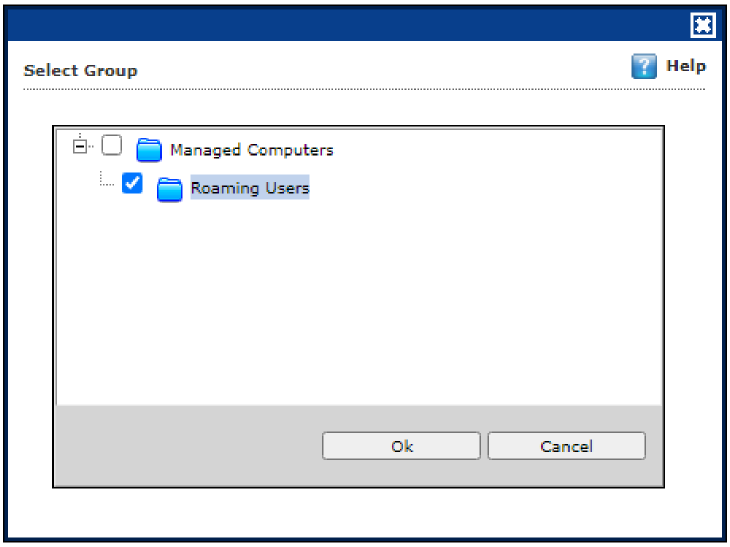
2. Click ... next to Update Agent field, to select the computer.
   Select Computer window appears.



* **Note:** Update Agent cannot be set if Hostname exceed 15 characters.

3. Select a computer and click **OK.**
4. Click ... next to Group Name field, to select the Group Name**.**

The computer will act as an Update Agent for selected group and provide updates to computers present in the group.



Select Group

☐ Managed Computers

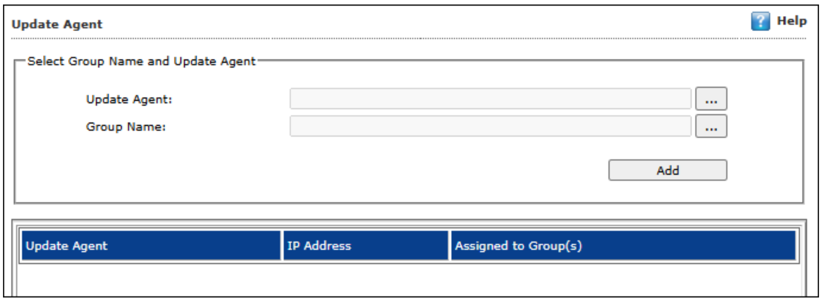
☑ Roaming Users

5. Select the Group and click **OK.**
6. Click **Add.**
   The Update Agent will be set for the selected group.

# Delete an Update Agent

To delete an Update Agent, follow the steps given below:

1. In Managed computers screen, click **Update Agent**.
   Update Agent window appears.



Update Agent

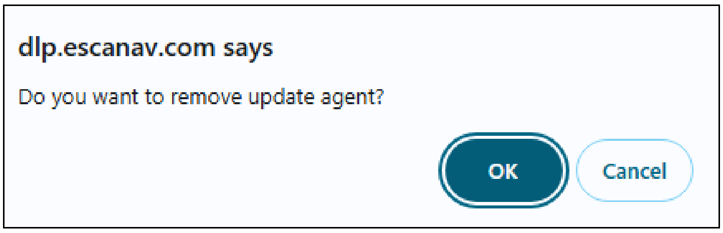
Select Group Name and Update Agent

Update Agent:

Group Name:

| Update Agent | IP Address | Assigned to Group(s) |
|---|---|---|

2. In the Assigned to Group(s) column, click 🗑 icon.
   A confirmation prompt appears.



dlp.escanav.com says

Do you want to remove update agent?

3. Click **OK**.
   The Update Agent will be deleted.

# Action List

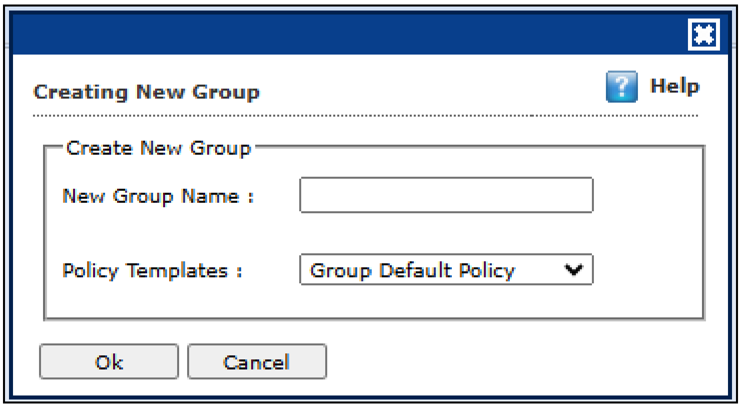
The Action List takes you action for a group. The drop-down contains following options:

- **New Subgroup**
- **Remove Group**
- **Create Client Setup** ⊞
- **Properties**

# Creating a Group

To create a group, follow the steps given below:

1. Click **Action List** > **New Subgroup**.
   Creating New Group window appears.

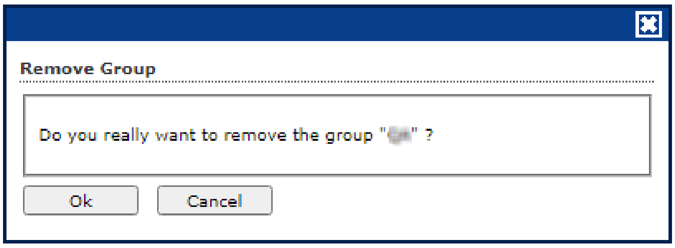


2. Enter a name for the group.
3. Click the **Policy Templates** drop-down and select a policy for the group.
4. Click **OK**.
   A new group will be created under the Managed Computers.

# Removing a Group

To remove a group, follow the steps given below:

1. Select a group.
2. Click **Action List** > **Remove Group**.
   A confirmation prompt appears.



Remove Group

Do you really want to remove the group "[redacted]" ?

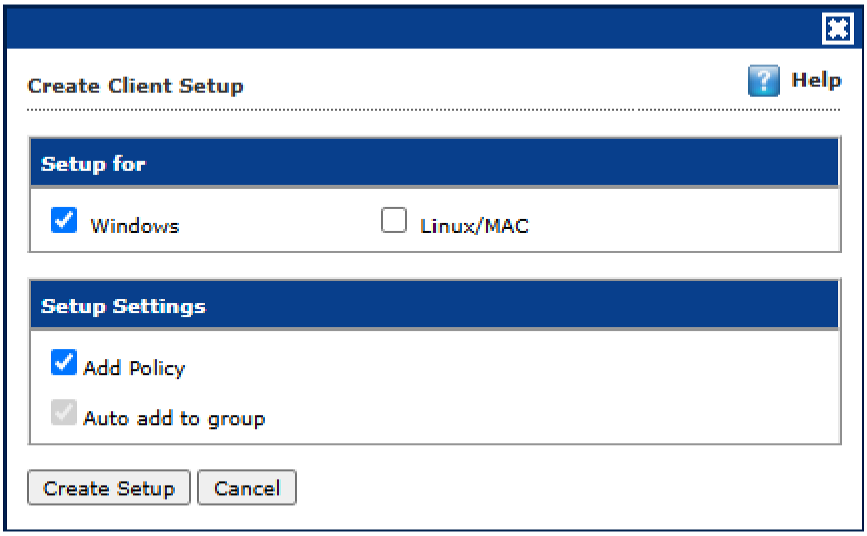
3. Click **OK**.
   The group will be removed.

| | |
|---|---|
| **NOTE** | A group will be removed only if it contains no computers. |

# Create Client Setup

To create a Client setup, follow the steps given below:

1. In the Managed Computers folder tree, select a group.
2. Click **Action List** > **Create Client Setup**.
   Create Client Setup window appears.



Create Client Setup

Help

Setup for

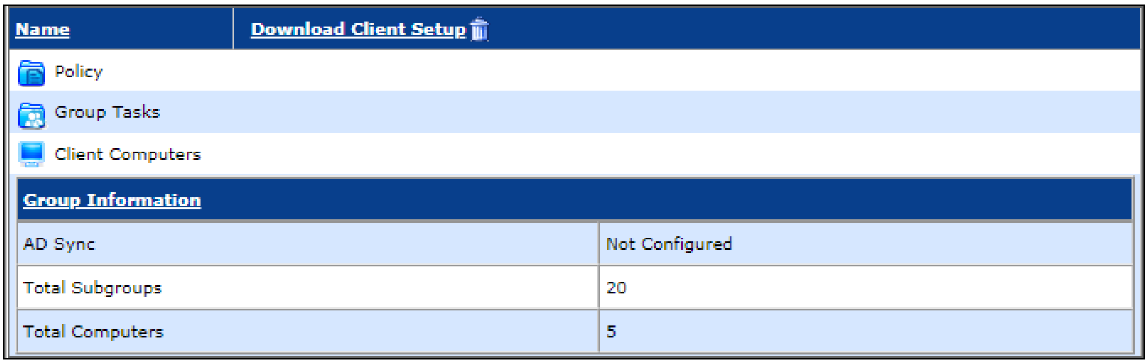
☑ Windows ☐ Linux/MAC

Setup Settings

☑ Add Policy

☑ Auto add to group

2. Select the necessary settings.
   - **Add Policy:** This option is enabled after the policy applied to client computers.
   - **Auto add to group:** This option will add the endpoint(s) to the respective group automatically after endpoint installation.
3. Click **Create Setup**.
   The Client setup will be created and a download link will be displayed in right pane.



| Name | Download Client Setup |
|---|---|
| Policy | |
| Group Tasks | |
| Client Computers | |

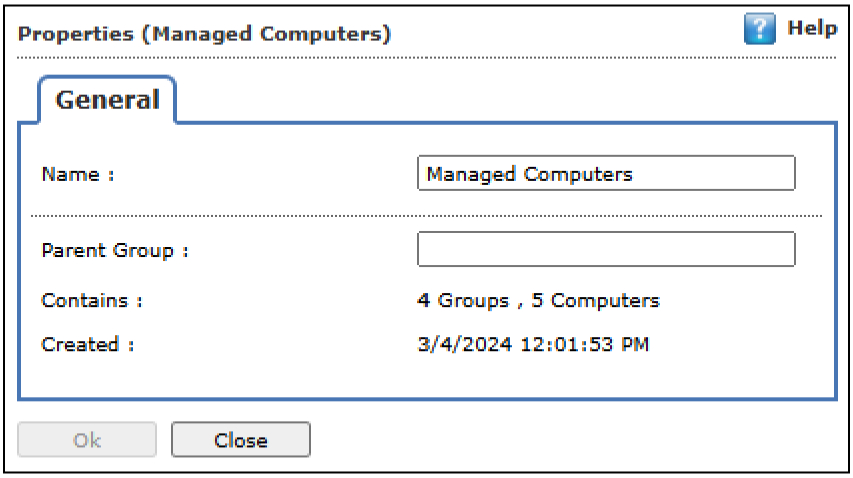
Group Information

| | |
|---|---|
| AD Sync | Not Configured |
| Total Subgroups | 20 |
| Total Computers | 5 |

# Properties of a group

To view the properties of a group, follow the steps given below:

1. Select a group.
2. Click **Action List** > **Properties**.
   Properties window appears.



Properties (Managed Computers)

Name : Managed Computers

Parent Group :

Contains : 4 Groups , 5 Computers

Created : 3/4/2024 12:01:53 PM

In Properties, **General** tab displays following details:

- Group Name
- Parent Group
- Contains – Number of Sub Groups and Computers in that Group
- Creation date of the Group

# Client Action List

The Client Action List lets you take action for specific computer(s) in a group. To enable this button, select computer and then click **Client Action List**.
The drop-down consists of following options:

- **Move to Group**
- **Remove from Group**
- **Refresh Client**
- **Export**
- **Show Installed Softwares**
- **Create OTP**
- **Properties**

The Client Action List contains few options similar to Action List. These options perform same, except they perform the action only for selected computer(s).

## Move to Group

To move computers from one group to other, follow the steps given below:

1. Go to **Managed Computers**.
2. Select the desired computers present in a group.
3. Click **Client Action List** > **Move to Group**.
4. Select the group in the tree to which you wish to move the selected computers and click **OK**.
   The computers will be moved to the selected group.

## Remove from Group

To remove computers from a group, follow the steps given below:

1. Go to **Managed Computers**.
2. Select the desired computers for removal.
3. Click **Client Action List** > **Remove from Group**.
   A confirmation prompt appears.
4. Click **OK**.
   The computers will be removed from the group.

## Refresh Client

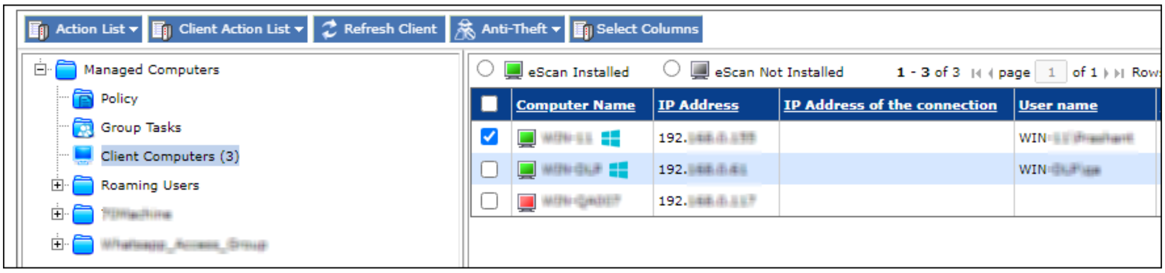
To refresh status of any client computer, follow the steps given below:

1. Under any group, click **Client Computers**.
   A list of computers appears on the right pane.
2. Select a computer.
3. Click **Refresh Client**.
   The Client status will be refreshed.

# Export

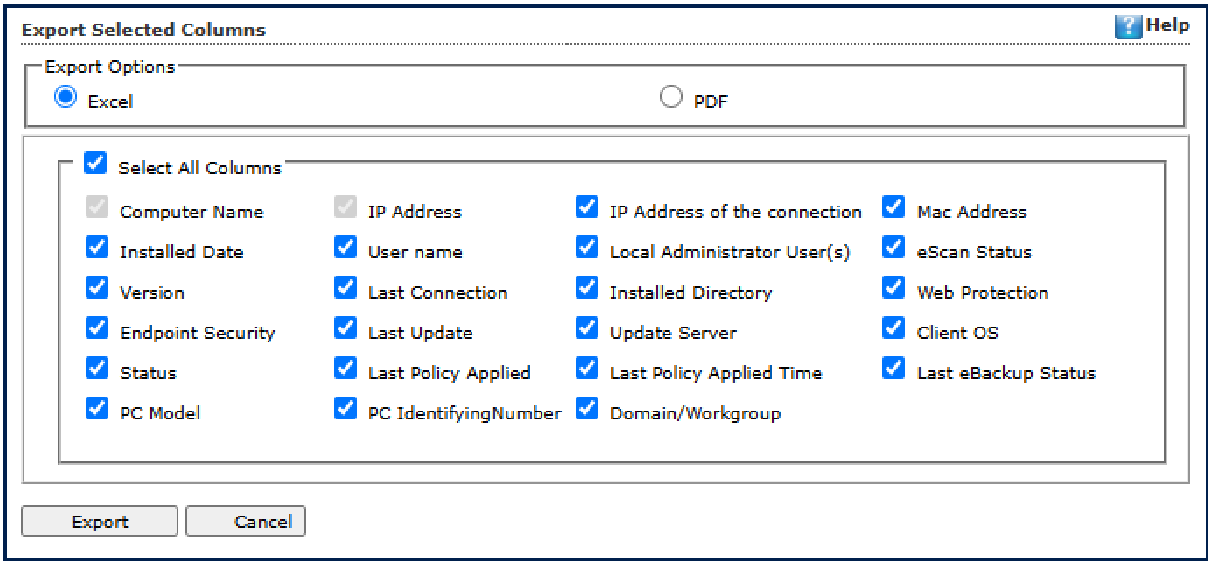
To export a client computer's data, follow the steps given below:

1. In the Managed Computers folder tree, select a group and then click **Client Computers**.
   The right pane displays the list of computers in the group and their detailed information.



| □ | Computer Name | IP Address | IP Address of the connection | User name |
|---|---|---|---|---|
| ☑ | [redacted] | 192.[redacted] | | WIN-[redacted] |
| □ | [redacted] | 192.[redacted] | | WIN-[redacted] |
| □ | [redacted] | 192.[redacted] | | |

2. Select a client computer and then click **Client Action List** > **Export**.
   Export Selected Columns window appears displaying export options and a variety of columns to be exported.



Export Selected Columns
Help

Export Options
● Excel ○ PDF

☑ Select All Columns

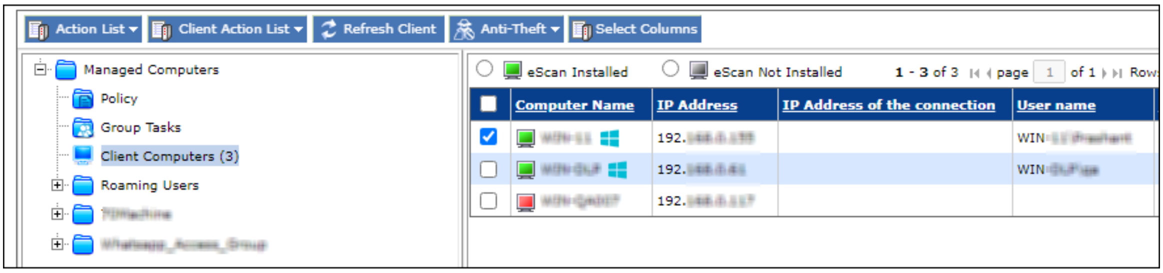
☑ Computer Name
☑ Installed Date
☑ Version
☑ Endpoint Security
☑ Status
☑ PC Model
☑ IP Address
☑ User name
☑ Last Connection
☑ Last Update
☑ Last Policy Applied
☑ PC IdentifyingNumber
☑ IP Address of the connection
☑ Local Administrator User(s)
☑ Installed Directory
☑ Update Server
☑ Last Policy Applied Time
☑ Domain/Workgroup
☑ Mac Address
☑ eScan Status
☑ Web Protection
☑ Client OS
☑ Last eBackup Status

3. Select the preferred export option.
4. Select the preferred report columns.
5. Click **Export**.
   The report will be exported as per your preferences.

# Show Installed Softwares

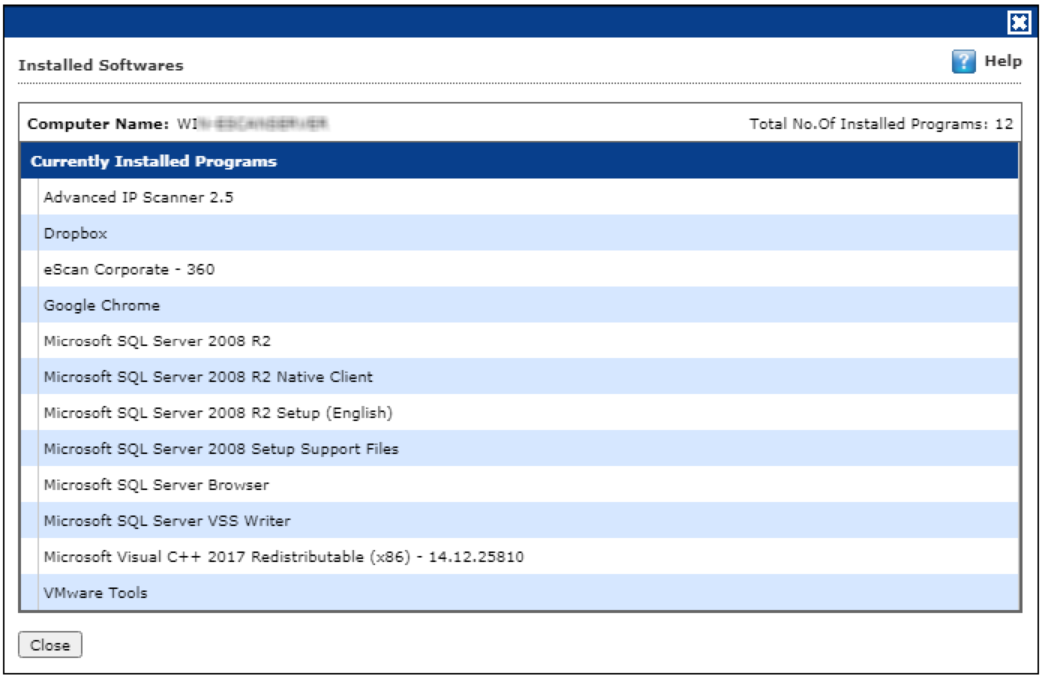
This feature displays a list of installed softwares on a computer.
To view the list of installed softwares, follow the steps given below:

1. In the Managed Computers folder tree, select a group and then click **Client Computers**. The right pane displays the list of computers in the group and their detailed information.



| □ | Computer Name | IP Address | IP Address of the connection | User name |
|---|---|---|---|---|
| ☑ | [redacted] | 192.[redacted] | | WIN-[redacted] |
| □ | [redacted] | 192.[redacted] | | WIN-[redacted] |
| □ | [redacted] | 192.[redacted] | | |

2. Select a client computer and then click **Client Action List** > **Show Installed Softwares**. Installed Softwares window appears displaying list of installed softwares and in the top right corner displays total number of installed softwares.



Computer Name: WI[redacted]

Total No.Of Installed Programs: 12

| Currently Installed Programs |
|---|
| Advanced IP Scanner 2.5 |
| Dropbox |
| eScan Corporate - 360 |
| Google Chrome |
| Microsoft SQL Server 2008 R2 |
| Microsoft SQL Server 2008 R2 Native Client |
| Microsoft SQL Server 2008 R2 Setup (English) |
| Microsoft SQL Server 2008 Setup Support Files |
| Microsoft SQL Server Browser |
| Microsoft SQL Server VSS Writer |
| Microsoft Visual C++ 2017 Redistributable (x86) - 14.12.25810 |
| VMware Tools |

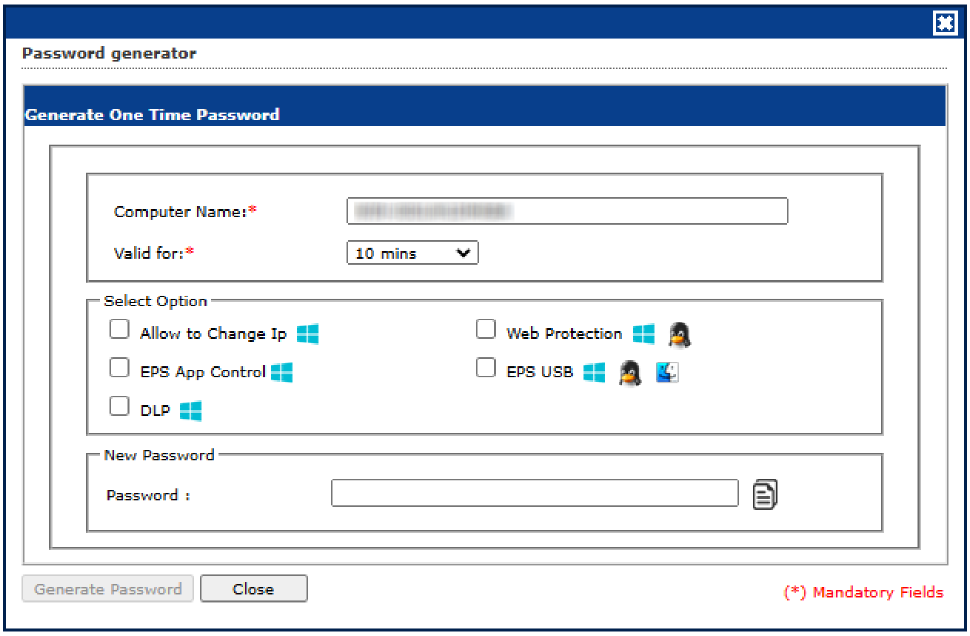
# Create OTP

The password protection restricts user access from violating a security policy deployed in a network. For example, the administrator has deployed a security policy to block all USB devices, but a user needs USB access for a genuine reason. In such situation, One Time Password (OTP) can be generated to disable USB block policy on specific computer. The administrator can define policy disable duration ranging from 10 minutes to an hour without violating existing policy.

# Generating an OTP

To generate an OTP, follow the steps given below:

1. In the Managed Computers screen, select the client computer for which you want to generate the OTP.
2. Click **Client Action List** > **Create OTP**.
   Password Generator window appears.



Password generator

Generate One Time Password

Computer Name:* [redacted]

Valid for:* 10 mins

Select Option

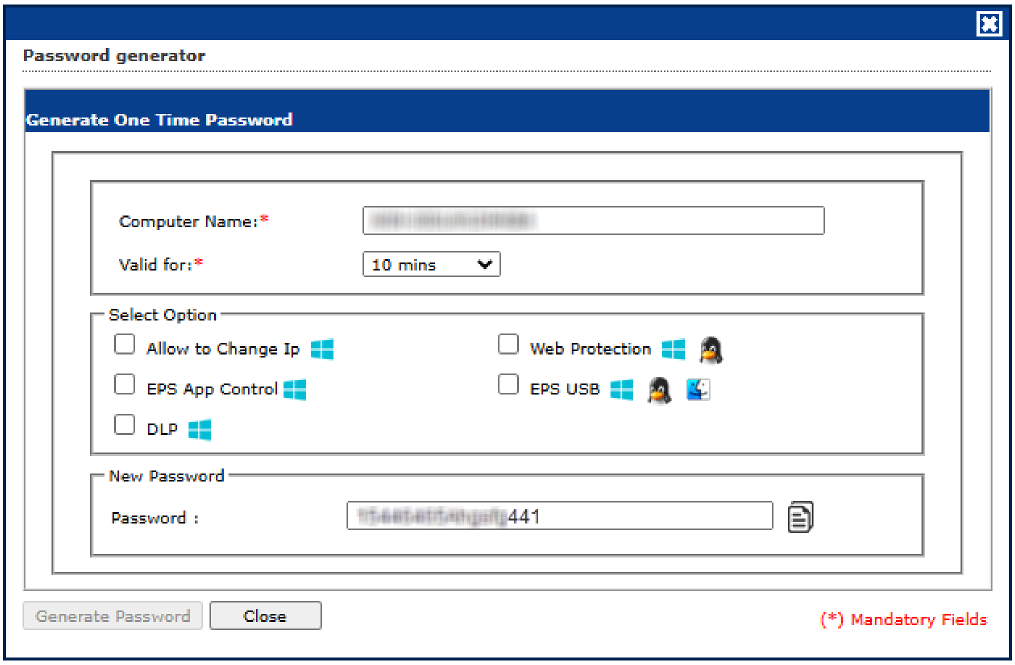
□ Allow to Change Ip
□ Web Protection
□ EPS App Control
□ EPS USB
□ DLP

New Password

Password :

(*) Mandatory Fields

3. In the **Valid for** drop-down, select the preferred duration to bypass the protection module.
4. In **Select Option** section, select the module you want to disable.
5. Click **Generate Password**.
   An OTP will be generated and displayed in **Password** field.



Password generator

Generate One Time Password

Computer Name:* [redacted]

Valid for:* 10 mins

Select Option

- ☐ Allow to Change Ip
- ☐ Web Protection
- ☐ EPS App Control
- ☐ EPS USB
- ☐ DLP

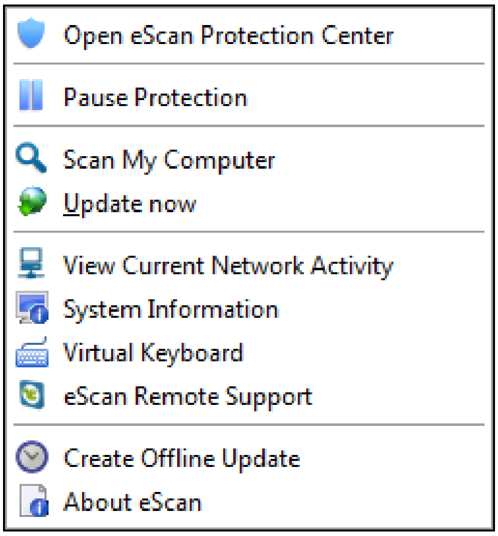
New Password

Password : [redacted]441

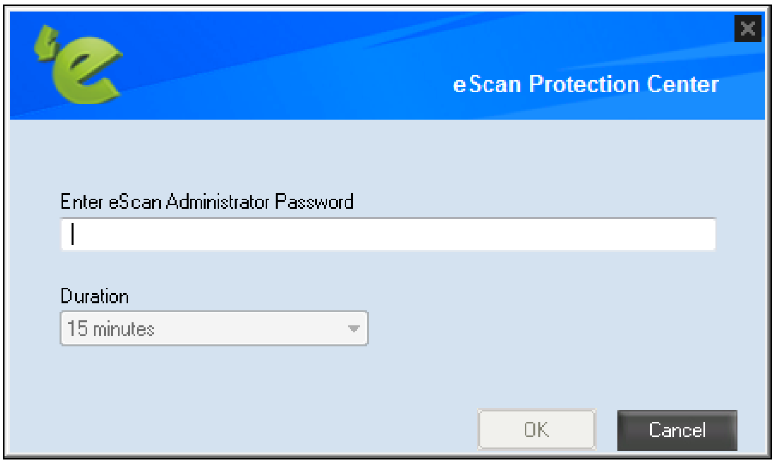
# Entering an OTP

To enter an OTP, follow the steps given below:

1. In the Taskbar, right-click the **eScan** icon.
   An option list appears.



2. Click **Pause Protection**.
   eScan Protection Center window appears.

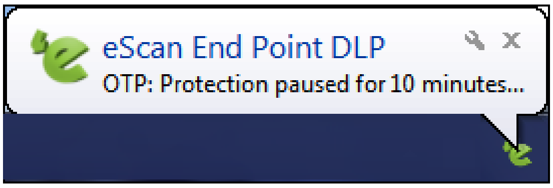


eScan Protection Center

Enter eScan Administrator Password

Duration: 15 minutes

3. Enter an OTP in the field.
4. Click **OK**.



eScan End Point DLP

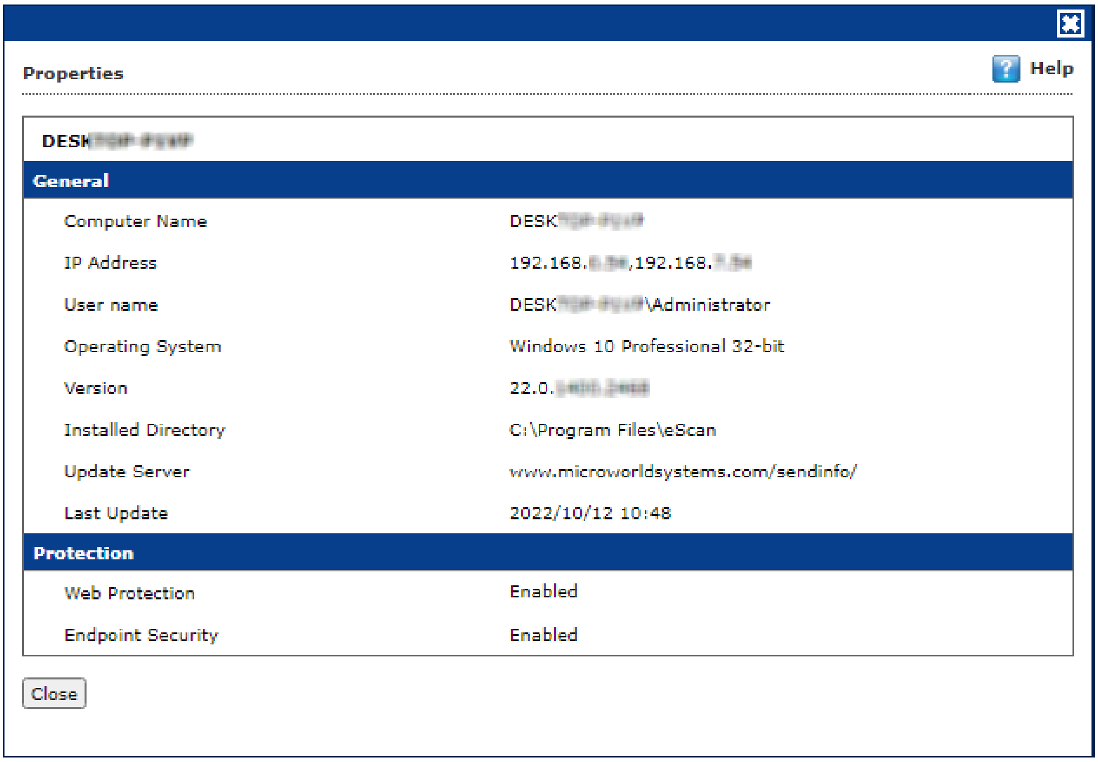
OTP: Protection paused for 10 minutes...

The selected module will be disabled for set duration.

# Properties of Selected Computer

To view the properties of a selected computer, follow the steps given below:

1. Select a computer.
2. Click **Client Action List** > **Properties**.
   Properties window appears displaying details.



DESK[redacted]

| General | |
|---|---|
| Computer Name | DESK[redacted] |
| IP Address | 192.168.[redacted],192.168.[redacted] |
| User name | DESK[redacted]\Administrator |
| Operating System | Windows 10 Professional 32-bit |
| Version | 22.0.[redacted] |
| Installed Directory | C:\Program Files\eScan |
| Update Server | www.microworldsystems.com/sendinfo/ |
| Last Update | 2022/10/12 10:48 |
| **Protection** | |
| Web Protection | Enabled |
| Endpoint Security | Enabled |

| NOTE | If multiple computers are selected, the **Properties** option will be disabled. |
|---|---|

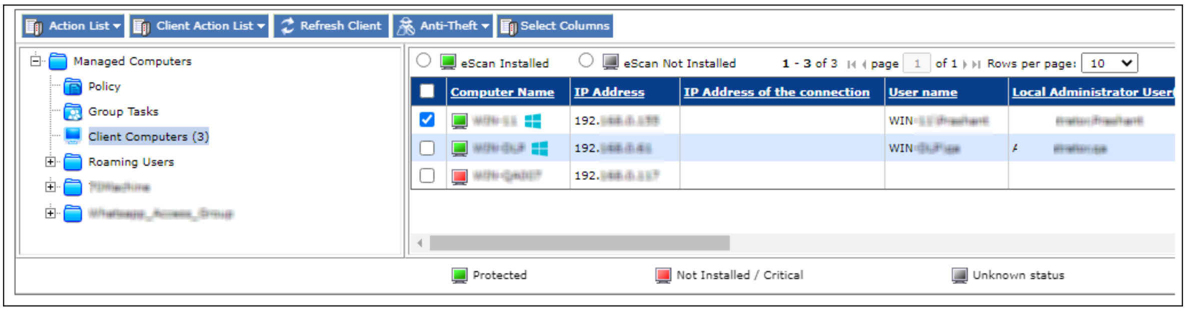
# Refresh Client

To refresh the status of any client computer, follow the steps given below:

1. Under any group, click **Client Computers**.
   A list of computers appears on the right pane.
2. Select a computer.
3. Click **Refresh Client**.
   The Client will be refreshed.

# Anti-Theft

The Anti-Theft module lets you remotely locate and lock a device. This module also lets you wipe the data available on a device.

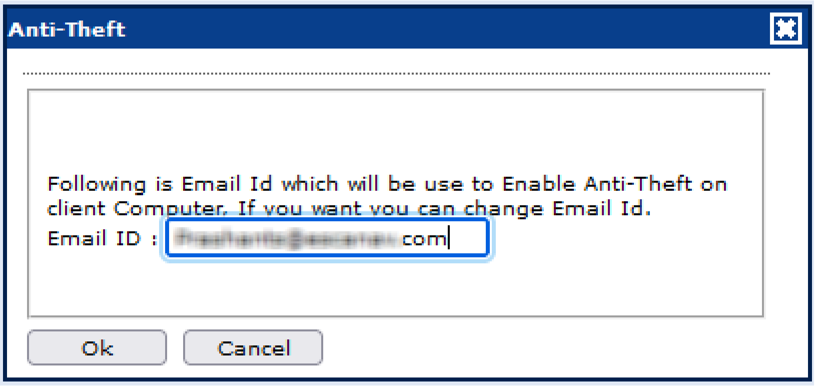


| ☐ | Computer Name | IP Address | IP Address of the connection | User name | Local Administrator User |
|---|---|---|---|---|---|
| ☑ | [redacted] | 192.[redacted] | | WIN-[redacted] | [redacted] |
| ☐ | [redacted] | 192.[redacted] | | WIN-[redacted] | [redacted] |
| ☐ | [redacted] | 192.[redacted] | | | |

## Anti-Theft Options

To add computers in an Anti-theft, follow the steps given below:

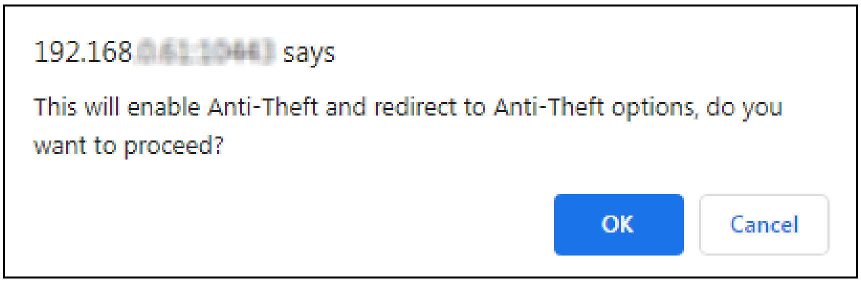
1. Go to **Managed Computers**.
2. Select the desired computers to add in Anti-theft Portal.
3. Click **Anti-Theft** > **Anti-Theft Options**.
4. Enter the **Email ID** then Click **OK.**
   The computer will add in Anti-Theft Portal.



Following is Email Id which will be use to Enable Anti-Theft on client Computer. If you want you can change Email Id.

Email ID : [redacted].com

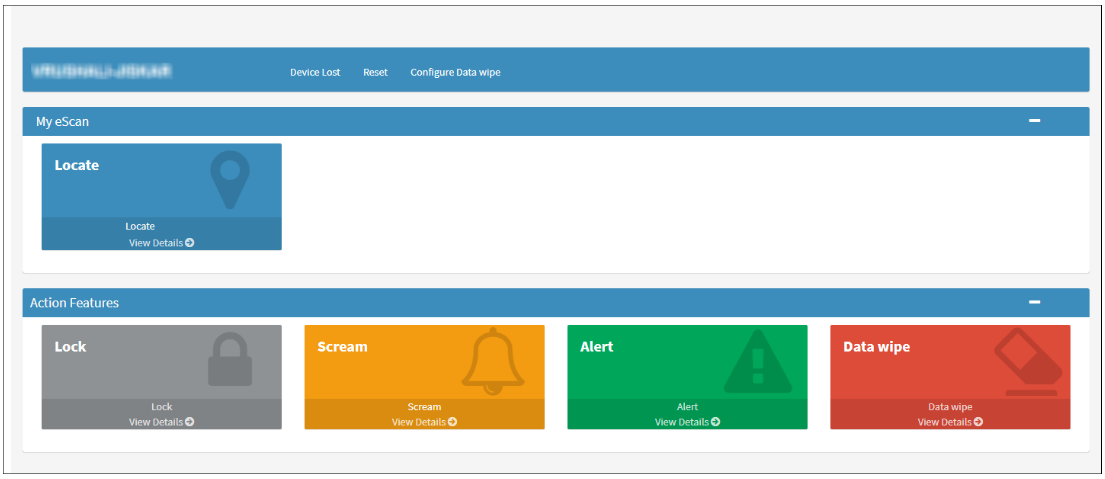
A confirmation prompt appears.



192.168[redacted] says

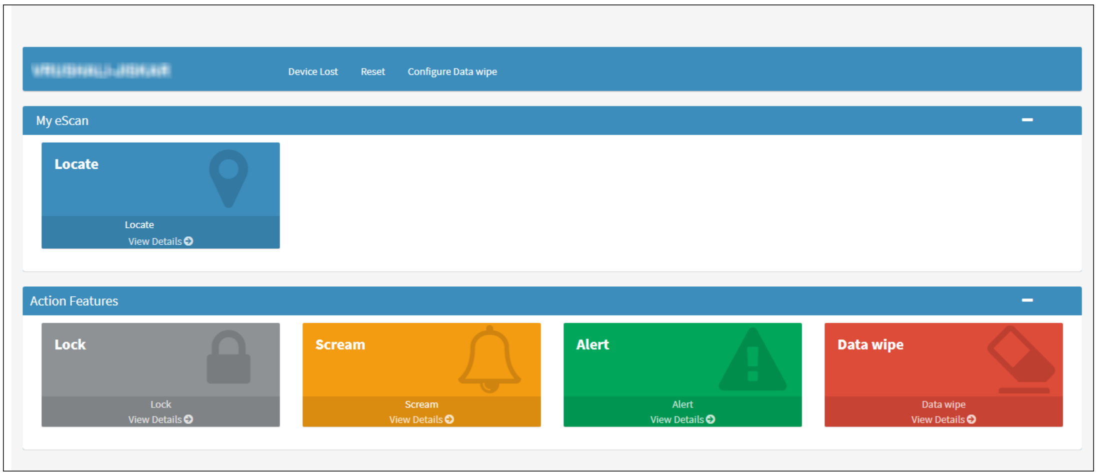
This will enable Anti-Theft and redirect to Anti-Theft options, do you want to proceed?

5. Click **OK**.
   This will redirect to Anti-Theft options.



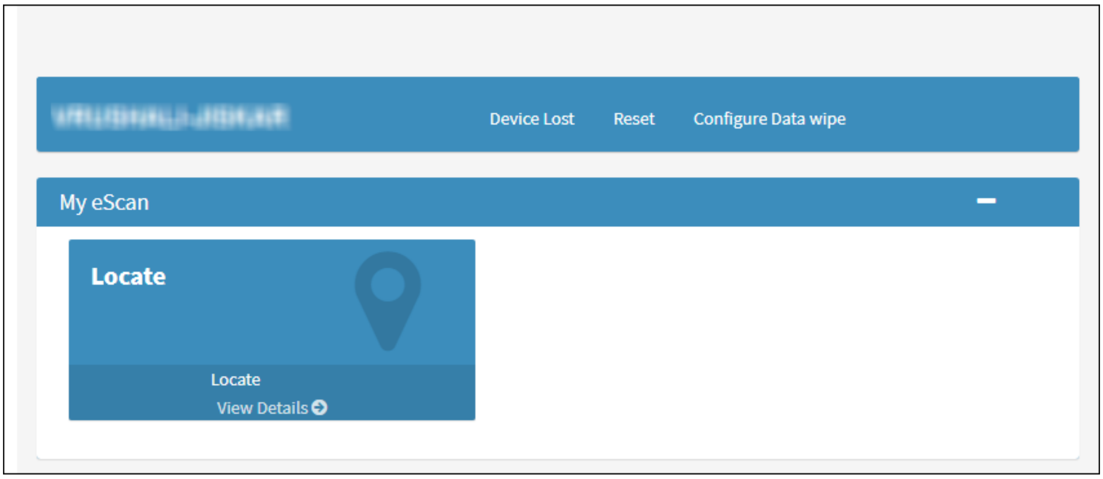
# Anti-Theft Portal

It will display the anti-theft features that you can activate in case your system is lost or stolen.

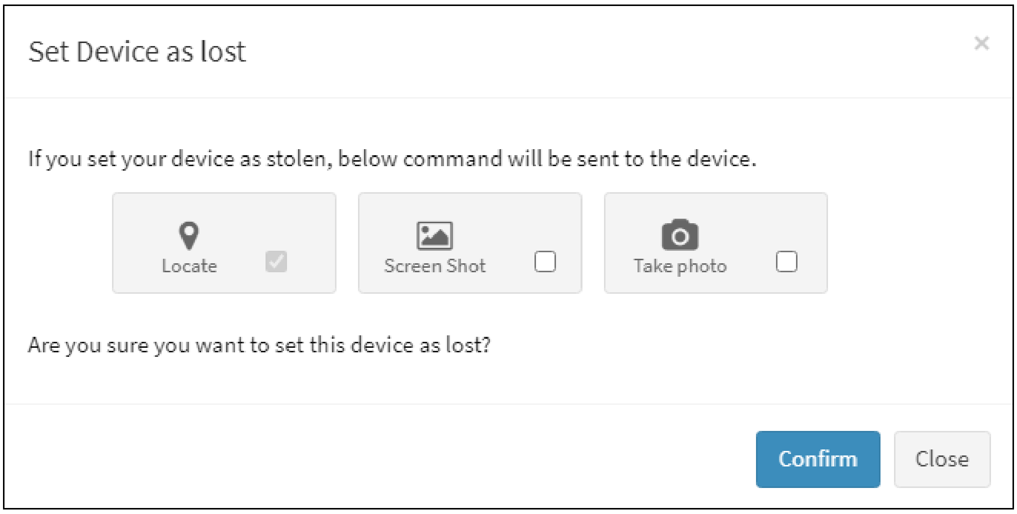


In case of loss or theft, click on the system name that has been lost or stolen, the status bar under it will display the system name again and when it was last seen.

1. Click **Device Lost**, this will allow you to enable the features locate, screenshot and take photo by selecting the desired options.



2. Click **Confirm** to confirm that your system has been lost and to execute the commands Locate, Screenshot, and Camera.



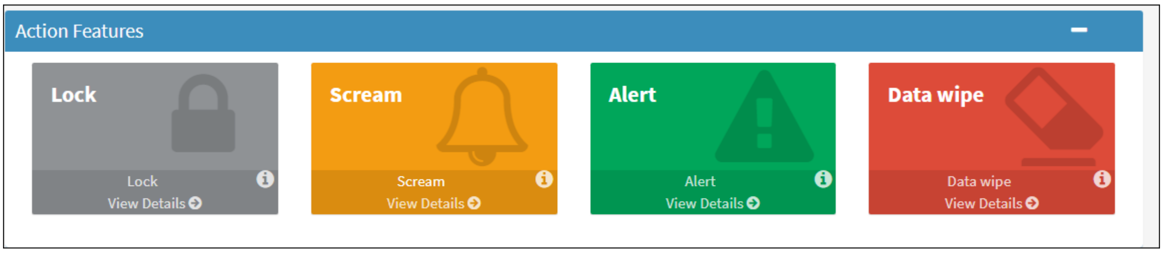
Set Device as lost

If you set your device as stolen, below command will be sent to the device.

Are you sure you want to set this device as lost?

- **Locate**: This option will allow you to locate the system in case of loss/theft. Click on the **Locate** option on the anti-theft portal and the last known location of the system will be displayed on the map. Procedure to Locate the system:
  1) Click **Locate**, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to locate the system is in progress.
  2) **View Details** displays the Last Location of your system on a map. It also shows details of last two successful executions of the Locate command.
- **Screenshot**: This option will allow you to take a screen shot of the system whenever it is synced to the server.
  1) Click **Screenshot**, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to take a screenshot is in progress.
  2) **View Details** displays the last two screenshots from the successful execution of the screenshot command.
- **Take Photo**: This option will allow you to take a snapshot of the current user of the system from the webcam on clicking the **Camera** option on the anti-theft portal.
  1) Click **Camera**, the status will change to Request Pending; the status will be updated as soon as the system is synced with the server. Request pending indicates that your request to take a snapshot is in progress.
  2) **View Details** displays the last two snapshots taken from your system.

Click **Reset** to reset the **Action Features** on the system; these actions can be performed on the system when it has been lost or stolen.



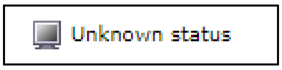
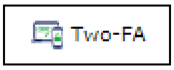
- **Lock:** The Lock feature will block the system from any further access. You will have to unblock the system by entering the pin provided on the anti-theft portal. On the anti-theft portal, select your System Alias name and then click **Lock** to remotely block your system, to unblock your system you will have to enter the **Secret Code** provided at the time of executing the lock command.
- **Scream**: Scream will allow you to raise a loud alarm on the system; this will allow you to trace the system if it is in the vicinity. Click **Scream** option to remotely raise a loud alarm on your system.
- **Alert**: This option will allow you to send an alert message (up to 200 characters) to the lost system. This alert message will be displayed on the screen; you can write and send any message for example: Request a call back or send your address or any kind of message to the current holder of your system. With this option there will be higher chance of your lost system being recovered. Click **Alert** option to remotely send a message to your lost system. Type in your message in the **send message** section and click **Confirm**.
- **Data wipe**: The Data Wipe feature will delete all the selected files and folders that have been added to the list to be deleted from the portal. Click **Data Wipe** option to remotely wipe all the selected files and folders or only delete the cookies and click **Confirm**. Select the **Delete Cookies** checkbox to delete cookies or select the **Data wipe** checkbox to wipe the data and click on **Confirm**.

## Disable Anti-Theft

To Disable Anti-Theft, follow the steps given below:

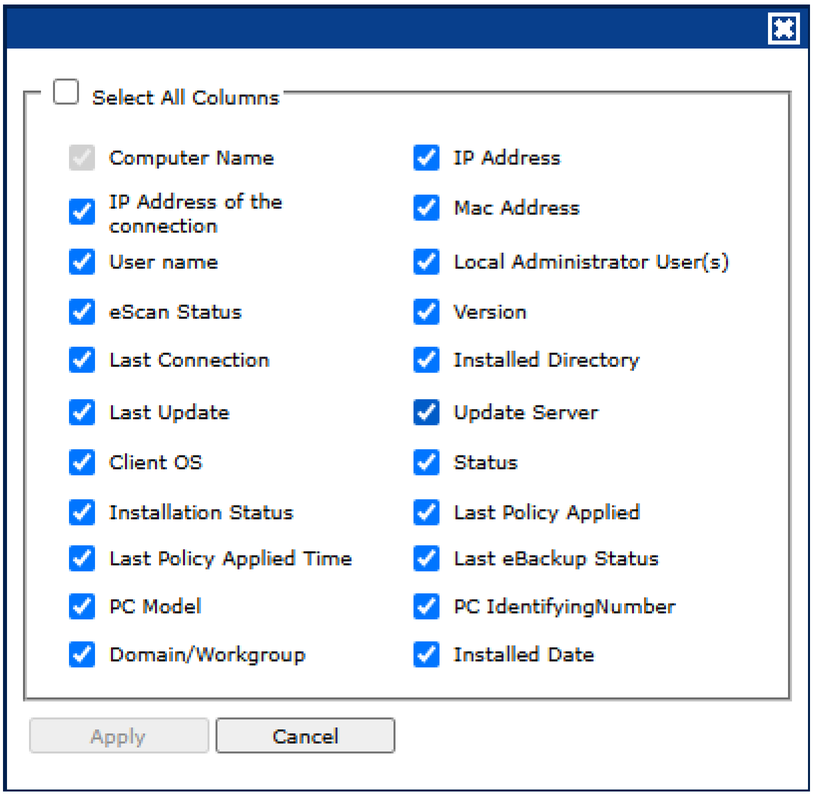
1. Go to **Managed Computers**.
2. Select the desired computers to disable Anti-theft Portal.
3. Click **Anti-Theft** > **Disable Anti-Theft**
   The Anti-Theft will be disabled on selected computer.

# Understanding the eScan Client Protection Status

| | |
|---|---|
| Protected | This status is displayed when the File anti-virus module of eScan Client is enabled and eScan was updated in last 2 days. |
| Not Installed / Critical | This status is displayed when either eScan is not installed on any computer or File AV/Real Time Protection is disabled. |
|  Unknown status | This status is displayed when communication is broken between Server and Client due to unknown reason. |
| Update Agent | This status is displayed when a computer is defined as an Update Agent for the group. |
|  Two-FA | This status is displayed when a computer is added to 2FA license. |
| DLP | This status is displayed when a computer is added to DLP license. |
| Anti-Theft | This status is displayed when a computer is added to Anti-Theft Portal. |

# Select Columns

You can customize the view regarding the details of devices, according to the requirement.



□ Select All Columns

☑ Computer Name
☑ IP Address of the connection
☑ User name
☑ eScan Status
☑ Last Connection
☑ Last Update
☑ Client OS
☑ Installation Status
☑ Last Policy Applied Time
☑ PC Model
☑ Domain/Workgroup
☑ IP Address
☑ Mac Address
☑ Local Administrator User(s)
☑ Version
☑ Installed Directory
☑ Update Server
☑ Status
☑ Last Policy Applied
☑ Last eBackup Status
☑ PC IdentifyingNumber
☑ Installed Date

To configure this, select the computer and click **Select/Add Columns** option. You can select and configure the required columns accordingly.

# Policy Template

This button allows you to add different security baseline policies for specific computer or group.

# Managing Policies

With the policies you can define rule sets for all modules of eScan client to be implemented on the Managed Computer groups. The security policies can be implemented for Windows as well as Linux and Mac systems connected to the network.

# Defining Policies Windows computers

On Windows OS policies can be defined for following eScan Client modules:

**Web Protection**
The Web Protection module lets you block offensive and unwanted websites. You can allow/block websites on time-based access restriction. To learn more, click here.

**Endpoint Security**
The Endpoint Security module monitors the applications on client computers. It allows/ restricts USB, Block list, White list, and defines time restrictions for applications. User can control the flow of attachments within an organization. To learn more, click here.

**Privacy Control**
The Privacy Control module lets you schedule an auto-erase of your cache, ActiveX, cookies, plugins, and history. You can also secure delete your files and folders where the files will be deleted directly without any traces. To learn more, click here.

**Administrator Password**
The Administrator Password lets you create and change password for administrative login and uninstallation password for eScan protection. To learn more, click here.

**MWL Inclusion List**
The MWL Inclusion List contains the name of all executable files which will bind itself to MWTSP.DLL. All other files are excluded. To learn more, click here.

**MWL Exclusion List**
The MWL Exclusion List contains the name of all executable files which will not bind itself to MWTSP.DLL. To learn more, click here.

**Notifications & Events**
The Notifications & Events allows you to allow/restrict the alerts that are sent to admin in case of any suspicious activity or events occurred on managed computers. To learn more, click here.

**Schedule Update**
The Schedule Update policy lets you schedule eScan database updates. To learn more, click here.

**Tools**
The Tools policy let you configure EBackup Settings. To learn more, click here.

# Defining Policies Mac or Linux computers

You can define policies for the following modules of eScan Client on Mac or Linux OS.

### Endpoint Security

The Endpoint Security module monitors the application on client computers. It allows/restricts USB, block listing, white listing, and defines time restrictions. You can monitor the difference between current file and original file status. This option is available for both Linux and Mac computers. To learn more, click here.

### Schedule Update

The Schedule Update module lets you schedule updates for Linux Agents. To learn more, click here.

### Administrator Password

The Administrator Password module for Linux and Mac lets you create and change password for administrative login of eScan protection center. It also lets you keep the password as blank, wherein you can login to eScan protection center without entering any password.
It lets you define uninstallation password which will be required before uninstalling eScan Client from managed computers manually. The user will not be able to uninstall eScan Client without entering uninstallation password. To learn more, click here.

### Web Protection

The Web Protection module for Linux feature is extremely beneficial to parents as it prevents kids from accessing websites containing harmful or restricted content. Administrators can also use this feature to prevent employees from accessing non-work-related websites during work hours. To learn more, **click here**.

### Network Security

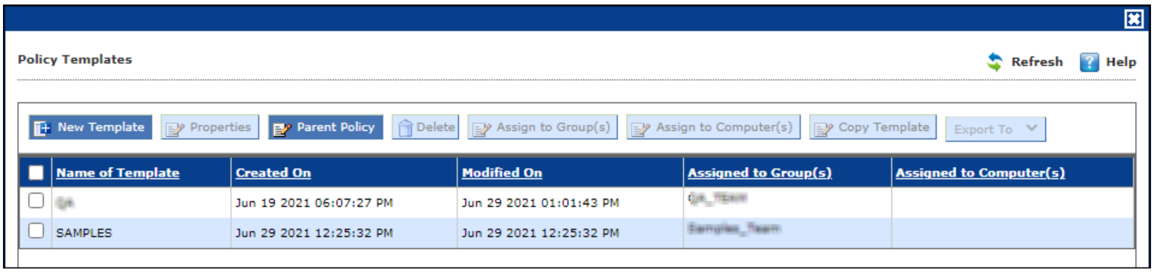
Network Security module helps to set Firewall to monitor all incoming and outgoing network traffic and protect your computer from all types of network based attacks. Enabling this features will prevents Zero-day attacks and all other cyber threats. To learn more, **click here**.

| | |
|---|---|
| **NOTE** | Priority will be given to Policy assigned through **Policy Criteria** first, then the policy given to a specific computer and lastly given to policy assigned to the group to which the computer belongs. |

# Creating Policy Template for a group/specific computer

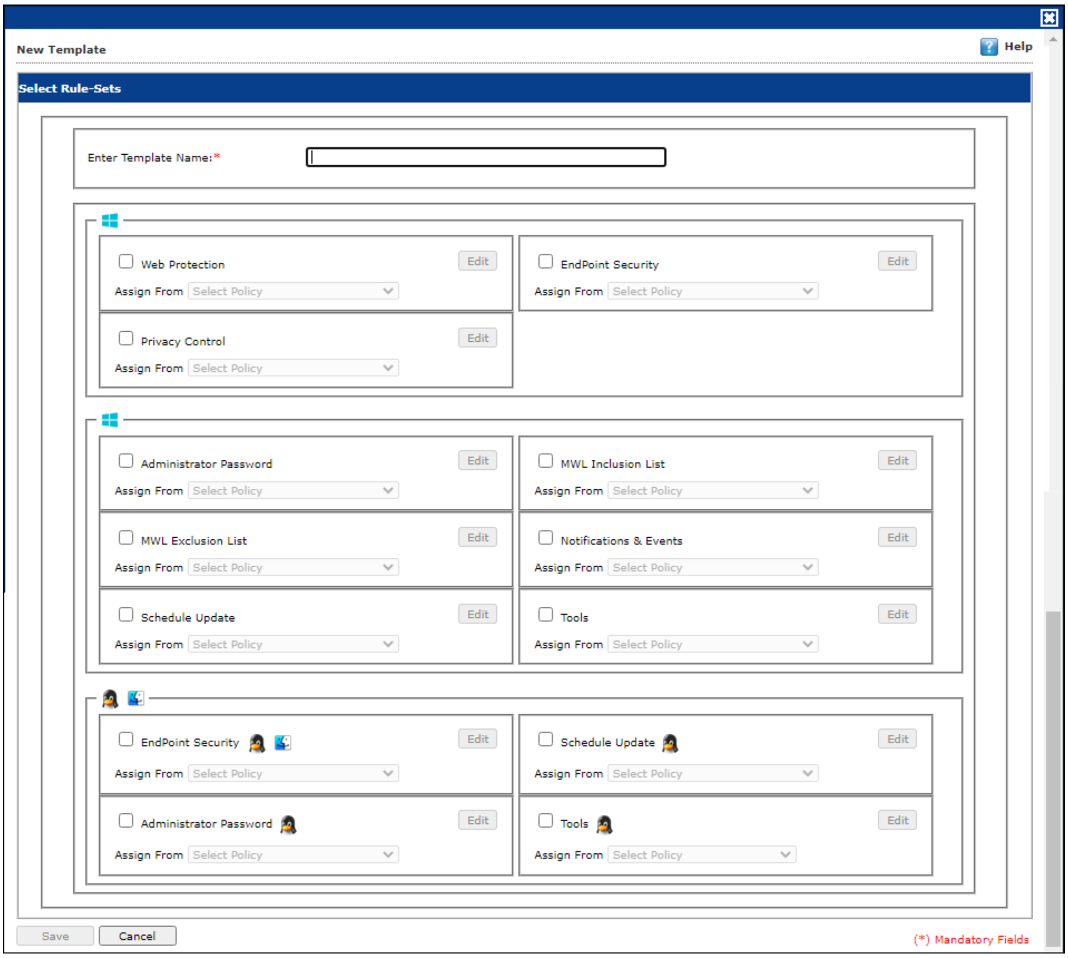
To create a Policy template for a group, follow the steps given below:

1. Click **Managed Computers**.
2. Select the desired group and then click **Policy Template**.
   Policy Template window appears.



| □ | Name of Template | Created On | Modified On | Assigned to Group(s) | Assigned to Computer(s) |
|---|---|---|---|---|---|
| □ | [redacted] | Jun 19 2021 06:07:27 PM | Jun 29 2021 01:01:43 PM | [redacted] | |
| □ | SAMPLES | Jun 29 2021 12:25:32 PM | Jun 29 2021 12:25:32 PM | [redacted] | |

3. Click **New Template**.
   New Templates screen appears displaying modules for Windows computers.



Enter Template Name:*

□ Web Protection — Edit — Assign From: Select Policy

□ EndPoint Security — Edit — Assign From: Select Policy

□ Privacy Control — Edit — Assign From: Select Policy

□ Administrator Password — Edit — Assign From: Select Policy

□ MWL Inclusion List — Edit — Assign From: Select Policy

□ MWL Exclusion List — Edit — Assign From: Select Policy

□ Notifications & Events — Edit — Assign From: Select Policy

□ Schedule Update — Edit — Assign From: Select Policy

□ Tools — Edit — Assign From: Select Policy

□ EndPoint Security — Edit — Assign From: Select Policy

□ Schedule Update — Edit — Assign From: Select Policy

□ Administrator Password — Edit — Assign From: Select Policy

□ Tools — Edit — Assign From: Select Policy

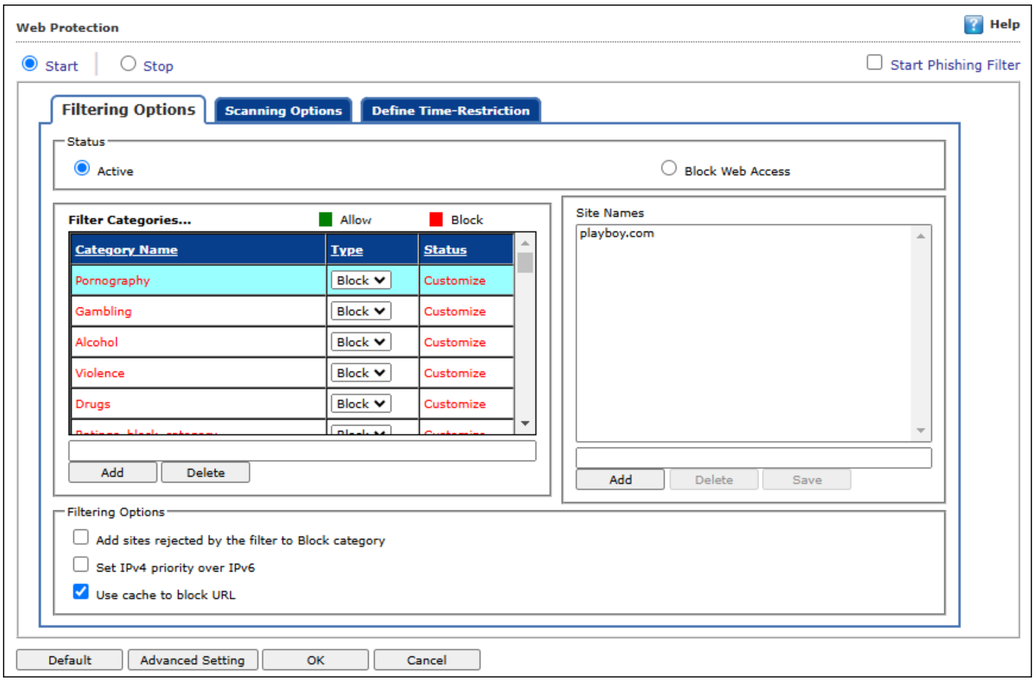
4. Enter name for Template.
5. To edit a module, select it and then click **Edit**.
6. Make a changes and click **Save**.
   The Policy Template will be saved.

# Configuring eScan Policies for Windows Computers

Each module of a policy template can be further edited to meet your requirements.

## Web Protection

The Web Protection module scans the website content for specific words or phrases. It lets you block websites containing pornographic or any offensive content. Administrators can use this feature to prevent employees from accessing non-work related websites during preferred duration.



Web Protection

● Start ○ Stop

□ Start Phishing Filter

Status

● Active ○ Block Web Access

Filter Categories... 🟩 Allow 🟥 Block

| Category Name | Type | Status |
|---|---|---|
| Pornography | Block | Customize |
| Gambling | Block | Customize |
| Alcohol | Block | Customize |
| Violence | Block | Customize |
| Drugs | Block | Customize |
| Ratings_block_category | Block | Customize |

Site Names

playboy.com

Filtering Options

□ Add sites rejected by the filter to Block category

□ Set IPv4 priority over IPv6

☑ Use cache to block URL

**Start/Stop**: It lets you enable or disable the Web Protection module. Click the appropriate option.

## Filtering Options

This tab has predefined categories that help you control access to the Internet.

### Status

This section lets you allow or block access to specific websites based on Filter Categories. You can set the status as Active or Block web access. Select the **Block Web Access** option if you want to block all the websites except the ones that have been listed in the **Filter Categories**. When you select this option, Filtering Options tab is available.

### Filter Categories

This section uses the following color codes for allowed and blocked websites.

### Green [Allow]

It represents an allowed websites category.

### Red [Block]

It represents a blocked websites category.

The filter categories used in this section include categories like Pornography, Gambling, Chat, Alcohol, Violence, Drugs, Ratings_block_category, Websites Allowed, etc. You can also add or delete filter categories depending on your requirement. User cannot delete the default filter categories.

### Category Name

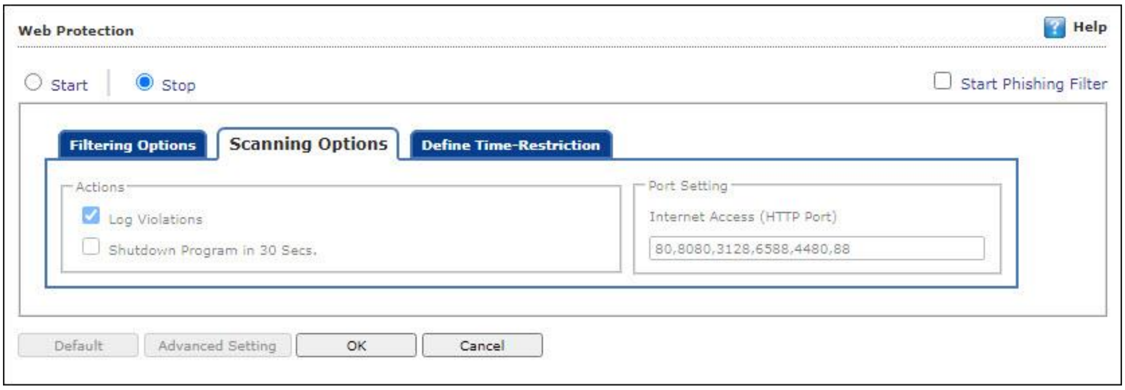
This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category.

### Filtering Options

**Add sites rejected by the filter to Block category** select this checkbox if you want eScan to add websites that are denied access to the Block category database automatically.

## Scanning Options

This tab lets you enable log violations and shutdown program if it violates policies. It also lets you specify ports that need monitoring.



### Actions

This section lets you select the actions that eScan should perform when it detects a security violation.

### Log Violations [Default]

Select this option if you want Web Protection to log all security violations for your future reference.

### Shutdown Program in 30 Secs

Select this option if you want Web Protection to shut down the browser automatically in 30 seconds when any of the defined rules or policies is violated.

### Port Setting

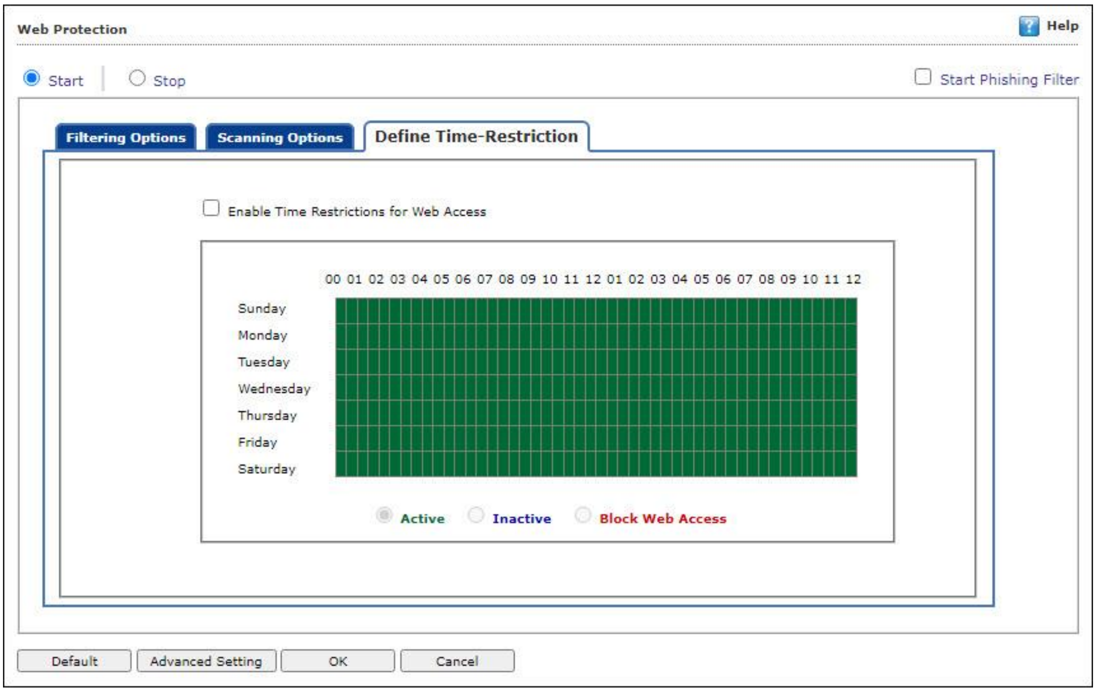
This section lets you specify the port numbers that eScan should monitor for suspicious traffic.

### Internet Access (HTTP Port)

Web browsers commonly use the port numbers 80, 8080, 3128, 6588, 4480, and 88 for accessing the Internet. You can add port numbers to the **Internet Access (HTTP Port)** box to monitor the traffic on those ports.

# Define Time Restriction

This section lets you define policies to restrict access to the Internet for preferred time period.



Web Protection

Help

● Start | ○ Stop

□ Start Phishing Filter

□ Enable Time Restrictions for Web Access

00 01 02 03 04 05 06 07 08 09 10 11 12 01 02 03 04 05 06 07 08 09 10 11 12

Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday

● Active ○ Inactive ○ Block Web Access

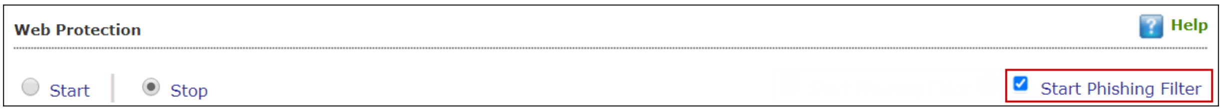
**Enable Time Restrictions for Web Access**
Select this option if you want to set restrictions on when a user can access the Internet. By default, all fields appear dimmed. The fields are available only when you select this option.
The time restriction feature is a grid-based module. The grid is divided into columns based on the days of the week vertically and the time interval horizontally.

**Active**
Click **Active** and select the appropriate grid if you want to keep web access active on certain days for a specific interval.

**Inactive**
Select this option if you want to keep web access inactive on certain days for a specific interval.

**Block Web Access**
Select this option if you want to block web access on certain days for a specific interval.

**Phishing Filter**
Under Web Protection eScan also provides options to enable Phishing filter which will detect and prevent any phishing attempts on the system. To enable the filter, select **Start Phishing Filter** checkbox.



Web Protection

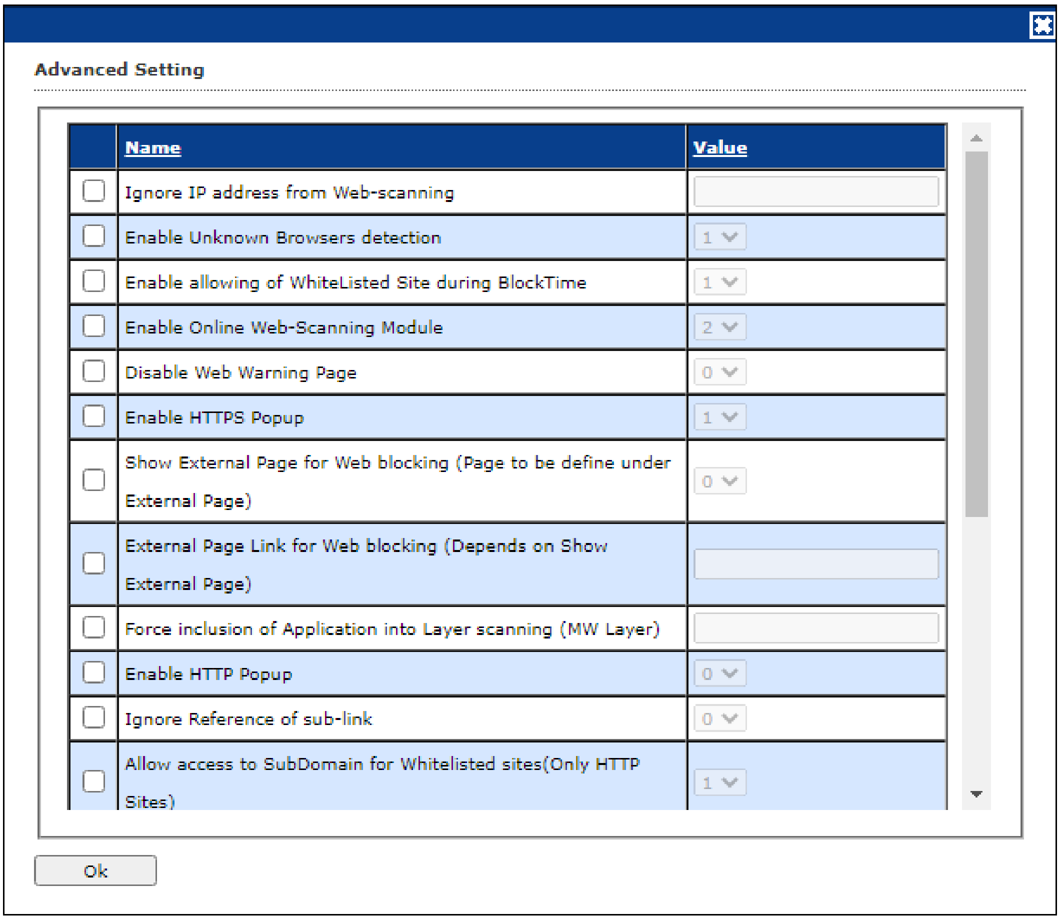
Help

○ Start | ● Stop

☑ Start Phishing Filter

## Advanced Settings

Clicking **Advanced** displays Advanced Settings.



Advanced Setting

|  | Name | Value |
|---|---|---|
| □ | Ignore IP address from Web-scanning |  |
| □ | Enable Unknown Browsers detection | 1 |
| □ | Enable allowing of WhiteListed Site during BlockTime | 1 |
| □ | Enable Online Web-Scanning Module | 2 |
| □ | Disable Web Warning Page | 0 |
| □ | Enable HTTPS Popup | 1 |
| □ | Show External Page for Web blocking (Page to be define under External Page) | 0 |
| □ | External Page Link for Web blocking (Depends on Show External Page) |  |
| □ | Force inclusion of Application into Layer scanning (MW Layer) |  |
| □ | Enable HTTP Popup | 0 |
| □ | Ignore Reference of sub-link | 0 |
| □ | Allow access to SubDomain for Whitelisted sites(Only HTTP Sites) | 1 |

**Ignore IP address from Web-scanning**
This option excludes entered IP address from web-scanning list and when you exclude IP Address, any file that the user downloads from any location within that domain is always allowed.

**Enable Unknown Browser detection (1 = Enable/0 = Disable)**
Select this option to enable/disable unknown browser detection.

**Enable allowing of WhiteListed Site during BlockTime (1 = Enable/0 = Disable)**
Select this option to enable/disable white listed site during block time.

**Enable Online Web-Scanning Module (2 =eScan Cloud Server/1 =Online database/0 = Offline database)**
Select this option to enable/disable online web-scanning module.

**Disable Web Warning Page (1 = Enable/0 = Disable)**
Select this option to enable/disable web warning page.

**Enable HTTPS Popup (1 = Enable/0 = Disable)**
Select this option to enable/disable HTTPS Popup.

**Show External Page for Web blocking (Page to be define under External Page) (1 = Enable/0 = Disable)**
Select this option to enable/disable external page for web blocking.

**External Page Link for Web blocking (Depends on Show External Page)**
Select this option to enter external page link for web blocking.

**Force inclusion of Application into Layer scanning (MW Layer)**
Select this option to enter Force inclusion of Application into Layer scanning.

**Enable HTTP Popup (1 = Enable/0 = Disable)**
Select this option to enable/disable HTTP pop-ups.

**Ignore Reference of sub-link (1 = Enable/0 = Disable)**
Select this option to enable/disable Ignore Reference of sub-link.

**Allow access to SubDomain for Whitelisted sites (Only HTTP Sites) (1 = Enable/0 = Disable)**
Select this option to enable/disable access to SubDomain for Whitelisted sites.

**Allow access to SubDomain for Whitelisted sites (Only HTTPS Sites) (1 = Enable/0 = Disable)**
Select this option to enable/disable access to SubDomain for Whitelisted sites.

**Enable logging of visited websites (1 = Enable/0 = Disable)**
Select this option to enable/disable logging of visited websites.

**Block EXE download from HTTP Sites (1 = Enable/0 = Disable)**
Select this option to enable/disable block download of .exe files from HTTP websites.

**Block HTTP Traffic only on Web Browser (1 = Enable/0 = Disable)**
Select this option to enable/disable blocks HTTP Traffic on Web Browser.

**Allow website list (Depends on "Block HTTP Traffic only on Web Browser")**
Select this option to enter the website name need to be allowed.

**Block Microsoft EDGE Browser (1 = Enable/0 = Disable)**
Select this option to enable/disable blocking Microsoft Edge browser.

**Enable Web Protection using Filter driver (1 = Enable/0 = Disable)**
Select this option to enable/disable web protection using filter driver.

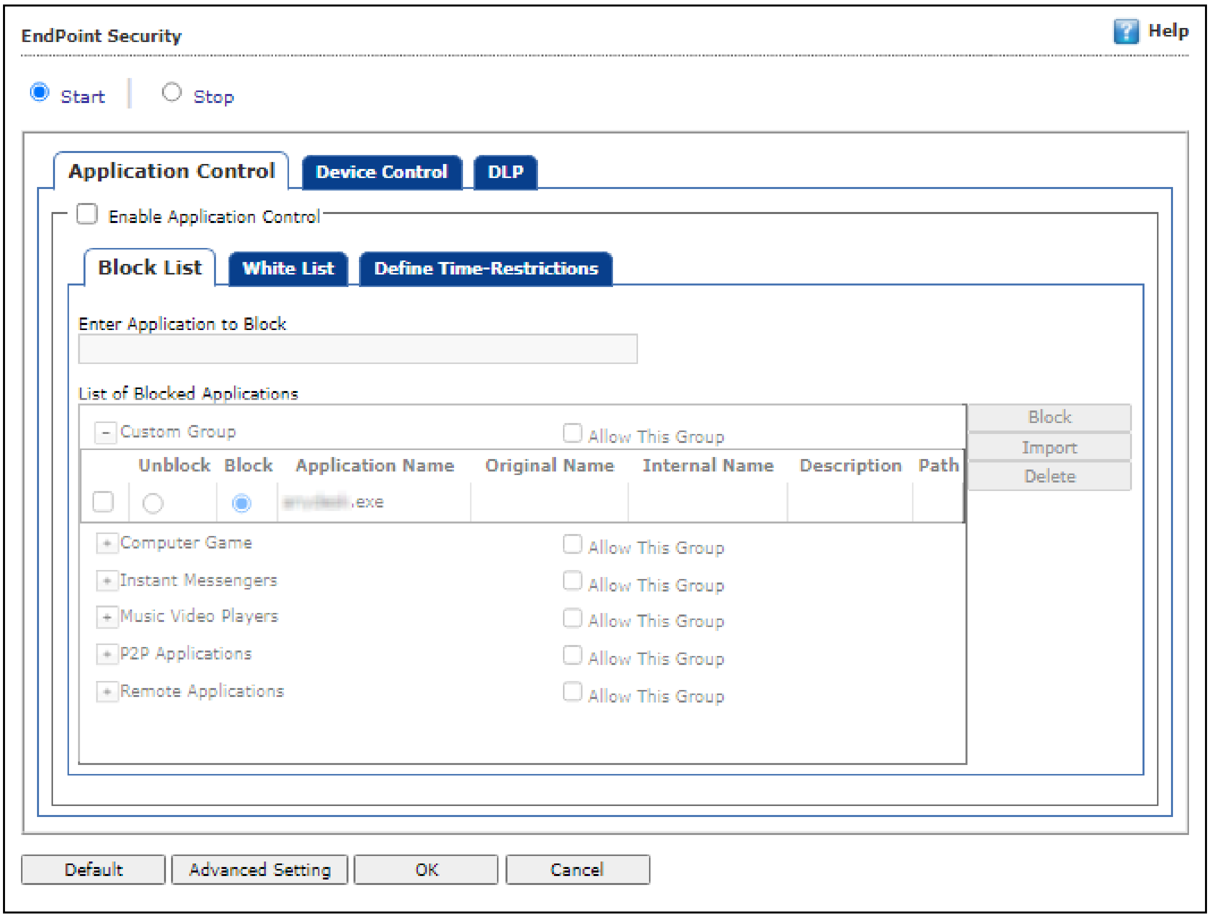
**Force Disable Web Protection using Filter driver (1 = Enable/0 = Disable)**
Select this option to force enable/disable web protection using filter driver.

**WFP Exclude IP List**
This option excludes entered IP address from web protect filter.

| | |
|---|---|
| **NOTE** | Click **Default** to apply default settings done during eScan installation. It loads and resets the values to the default settings. |

# Endpoint Security

Endpoint Security module protects your computer or Computers from data thefts and security threats through USB or FireWire® based portable devices. It comes with Application Control feature that lets you block unwanted applications from running on your computer. In addition, this feature provides you with a comprehensive reporting feature that lets you determine which applications and portable devices are allowed or blocked by eScan. The DLP (Attachment Control) allows you to block the attachments; the unauthorized user tries to send and keeps attachment flow secure.



EndPoint Security

● Start | ○ Stop

□ Enable Application Control

Enter Application to Block

List of Blocked Applications

| | | | | | | |
|---|---|---|---|---|---|---|
| − Custom Group | | | □ Allow This Group | | | |
| | Unblock | Block | Application Name | Original Name | Internal Name | Description | Path |
| □ | ○ | ● | [redacted].exe | | | | |
| + Computer Game | | | □ Allow This Group | | | |
| + Instant Messengers | | | □ Allow This Group | | | |
| + Music Video Players | | | □ Allow This Group | | | |
| + P2P Applications | | | □ Allow This Group | | | |
| + Remote Applications | | | □ Allow This Group | | | |

**Start/Stop**: It lets you enable or disable Endpoint Security module. Click the appropriate option.

There are three tabs – Application Control, Device Control, and DLP, which are as follows:

## Application Control

This tab lets you control the execution of programs on the computer. All the controls on this tab are disabled by default. You can configure the following settings.

**Enable Application Control**
Select this option if you want to enable the Application Control feature of the Endpoint Security module.

## Block List

**Enter Application to Block:** It indicates the name of the application you want to block from execution. Enter the name of the application to be blocked. Click **Block** to add application in Block List.

### List of Blocked Applications

This list contains blocked executables of applications that are predefined by MicroWorld. Each of the applications listed in the predefined categories are blocked by default. In addition, you can also add executables that you need to block only in the **Custom Group** category. If you want, you can unblock the predefined application by clicking the **UnBlock** checkbox from unblock column. The predefined categories include computer games, instant messengers, music & video players, P2P and remote applications.

### Allow This Group

Select this checkbox to allow the execution of all application from the particular group.

### Import

To block list applications from a CSV file, click **Import**. Click **Choose File** to import the file. Click **OK**.

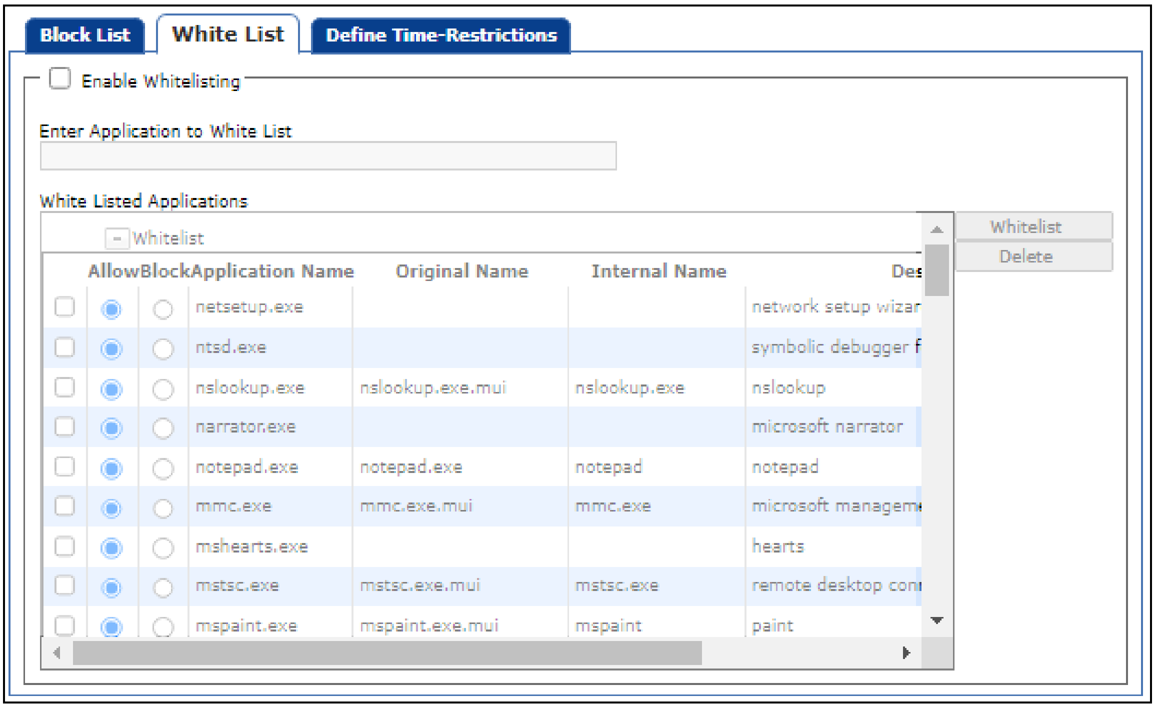
### Delete

Select the application and click **Delete** to remove the application from Blocked Application list.

## White List

### Enable Whitelisting

Select this checkbox to enable the whitelisting feature of the Endpoint Security module.



□ Enable Whitelisting

Enter Application to White List

White Listed Applications

⊟ Whitelist

| | Allow | Block | Application Name | Original Name | Internal Name | Des |
|---|---|---|---|---|---|---|
| □ | ● | ○ | netsetup.exe | | | network setup wizar |
| □ | ● | ○ | ntsd.exe | | | symbolic debugger f |
| □ | ● | ○ | nslookup.exe | nslookup.exe.mui | nslookup.exe | nslookup |
| □ | ● | ○ | narrator.exe | | | microsoft narrator |
| □ | ● | ○ | notepad.exe | notepad.exe | notepad | notepad |
| □ | ● | ○ | mmc.exe | mmc.exe.mui | mmc.exe | microsoft managem |
| □ | ● | ○ | mshearts.exe | | | hearts |
| □ | ● | ○ | mstsc.exe | mstsc.exe.mui | mstsc.exe | remote desktop con |
| □ | ● | ○ | mspaint.exe | mspaint.exe.mui | mspaint | paint |

**Enter Application to White List**
Enter the name of the application to be whitelisted. Click **Whitelist** to add application in White list.

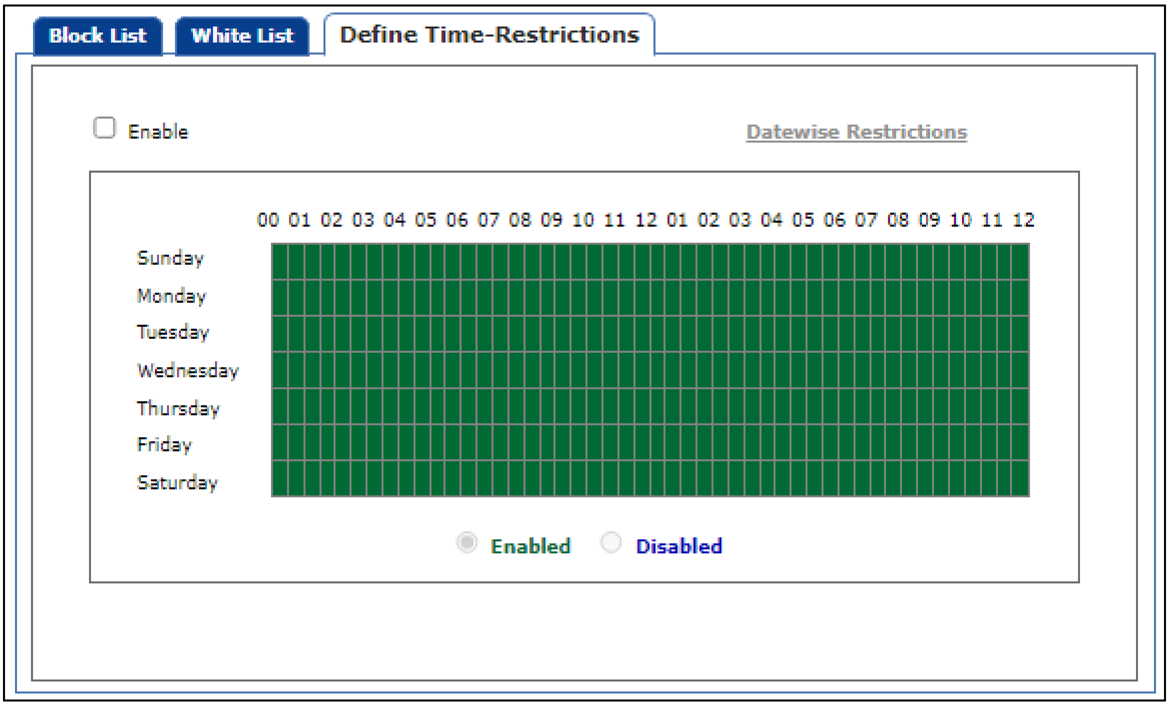
**White Listed Applications**
This list contains whitelisted applications that are predefined by MicroWorld. Each of the applications listed in the predefined categories are allowed by default. If you want to block the predefined categories, select the **Block** option.

**Delete**
Select the application and click **Delete** to remove the application from White listed Application.

## Define Time-Restrictions

This feature lets you define time restriction when you want to allow or block access to the applications based on specific days and between pre-defined hours during a day.

For example, the administrator can block computer games, instant messengers, for the whole day but allow during lunch hours without violating the Application Control Policies.



☐ Enable

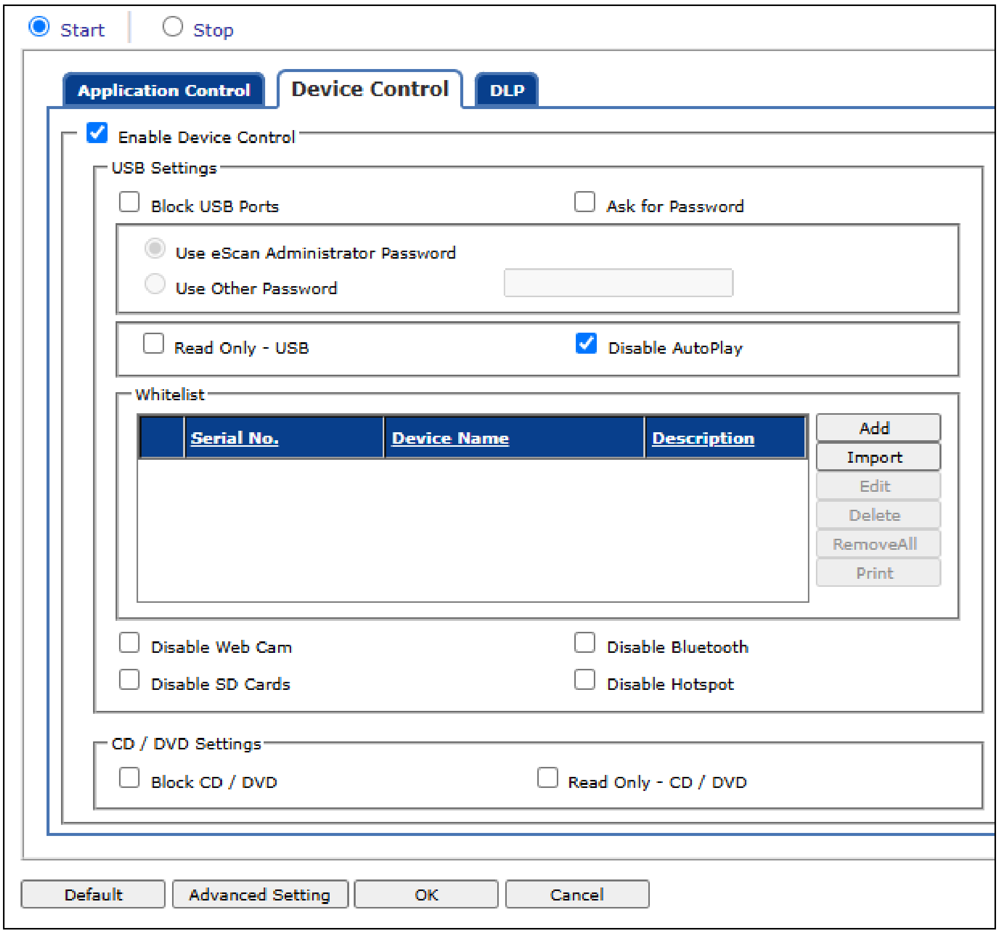
● Enabled ○ Disabled

**Enable**
This option lets you enable/disable Datewise Restriction feature.

**Datewise Restrictions**
This option lets you define datewise restrictions when you want to allow or block access to the applications based on specific dates and between pre-defined hours during that date.

## Device Control

The Endpoint Security module protects your computer from unauthorized portable storage devices prompting you for the password whenever you plug in such devices. The devices are also scanned immediately when connected to prevent any infected files running and infecting the computer.



● Start | ○ Stop

☑ Enable Device Control

USB Settings

□ Block USB Ports □ Ask for Password

○ Use eScan Administrator Password

○ Use Other Password

□ Read Only - USB ☑ Disable AutoPlay

Whitelist

| | Serial No. | Device Name | Description |
|---|---|---|---|

□ Disable Web Cam □ Disable Bluetooth

□ Disable SD Cards □ Disable Hotspot

CD / DVD Settings

□ Block CD / DVD □ Read Only - CD / DVD

**Enable Device Control [Default]**

Select this option if you want to monitor all the USB storage devices connected to your endpoint. This will enable all the options on this tab.

**USB Settings**

This section lets you customize the settings for controlling access to USB storage devices.

**Block USB Ports**

Select this option if you want to block all the USB storage devices from sharing data with endpoints.

**Ask for Password**

Select this option, if you want eScan to prompt for a password whenever a USB storage device is connected to the computer. You have to enter the correct password to access USB storage device. It is recommended that you always keep this checkbox selected. Following options are available only when you select the **Ask for Password** checkbox.

- **Use eScan Administrator Password**: Click this option if you want to assign eScan Administrator password for accessing USB storage device.

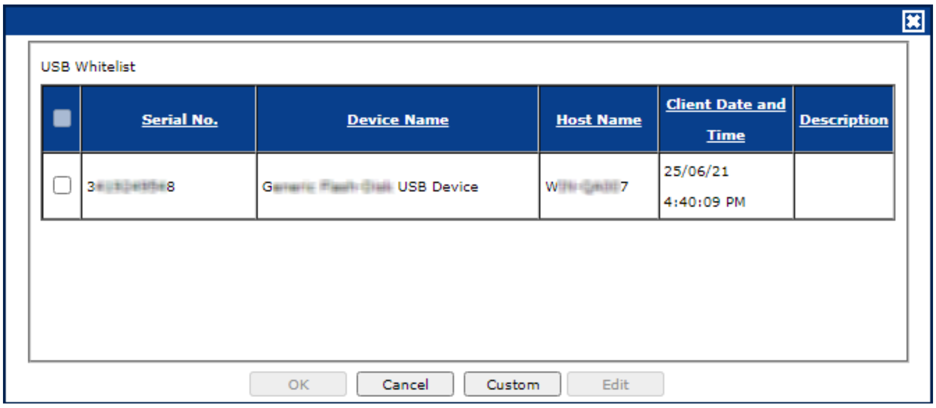
- **Use Other Password**: Click this option if you want assign a unique password for accessing USB storage device.

**Read Only –USB**
Select this option if you want to allow access of the USB device in read-only mode.

**Disable AutoPlay [Default]**
When you select this option, eScan disables the automatic execution of any program stored on a USB storage device when you connect the device.

**Whitelist**
eScan provides a greater level of endpoint security by prompting you for a password whenever you connect a USB drive. To disable password protection for a specific device, you can add it along with its serial number to the whitelist. The next time when you connect the device it will not ask for a password it will directly display the files or folders stored on the device. This section displays the serial number and device name of each of the whitelisted devices in a list. You can add devices to this list by clicking **Add**. The Whitelist section displays the following buttons.

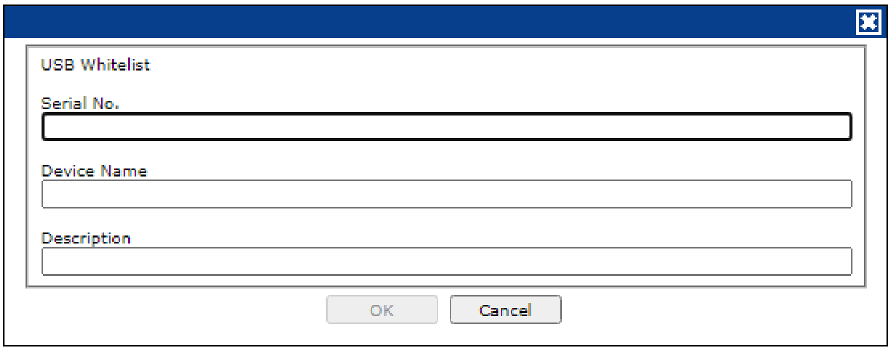
- **Add**
  Click **Add** to whitelist USB devices.
  USB Whitelist window appears.



USB Whitelist

| □ | Serial No. | Device Name | Host Name | Client Date and Time | Description |
|---|---|---|---|---|---|
| □ | 3[redacted]8 | [redacted] USB Device | W[redacted]7 | 25/06/21<br>4:40:09 PM | |

To whitelist the USB device, its details are required. If a USB device is connected to any eScan installed endpoint, the USB details are sent to the server. The administrator will have to manually whitelist the USB device. To manually add a USB device in USB Whitelist without connecting to an endpoint, click **Custom**.



USB Whitelist

Serial No.

Device Name

Description

Enter the USB details and then click **OK**.
The USB device will be added and whitelisted.

- **Import**
  To whitelist USB devices from a CSV file, click **Import**. Click **Choose File** to import the file. Click **OK.**

| | |
|---|---|
| ❗<br>NOTE | The list should be in following format:<br>Serial No 1, Device Name 1, Device Description 1(Optional)<br>Serial No 2, Device Name 2<br>**For Example:** SDFSD677GFQW8N6CN8CBN7CXVB, USB Drive 2.5, Whitelist by<br>xyzDFRGHHRS54456HGDF347OMCNAK, Flash Drive 2.2 |

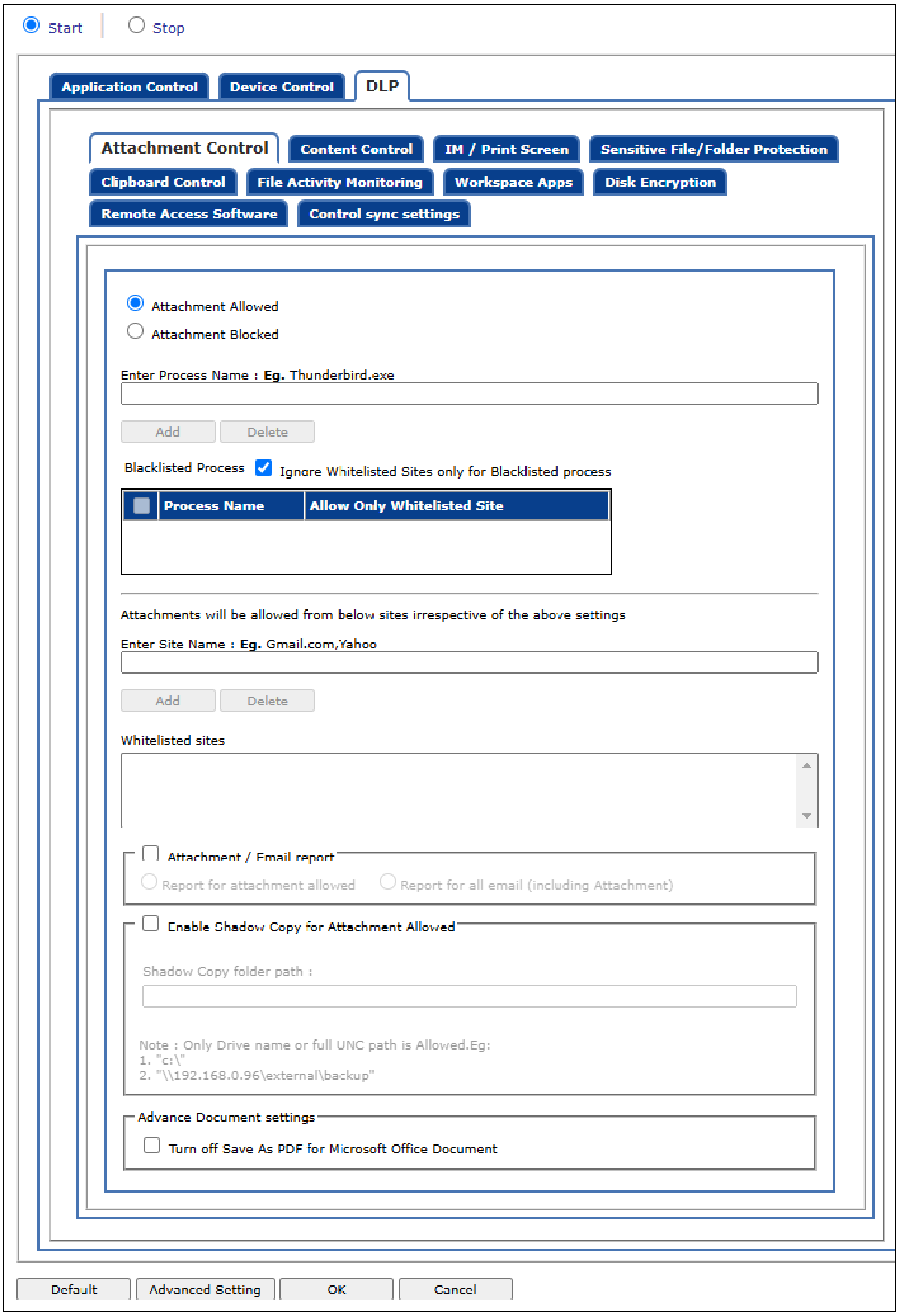
- **Edit:** Click **Edit** to edit the description of the USB devices.
- **Delete**: Select the USB device and click **Delete** to remove the device from the list.
- **Remove All**: To remove all the USB devices from the list, click **Remove All**.
- **Print**: This will print all the USB devices in the list along with details for the same.

**Disable Web Cam**: Select this option to disable Webcams.
**Disable SD Cards**: Select this option to disable SD cards.
**Disable Bluetooth**: Select this option to disable Bluetooth.
**Disable Hotspot:** Select this option disable Hotspot.

**CD/DVD Settings**
**Block CD / DVD:** Select this option to block all CD/DVD access.
**Read Only - CD / DVD:** Select this option to allow read-only access for CD/DVD.

## DLP

The DLP tab lets you control attachment flow within your organization. You can block/allow all attachments the user tries to send through specific processes that can be defined. You can exclude specific domains/subdomains that you trust, from being blocked even if they are sent though the blocked processes mentioned before.



● Start | ○ Stop

● Attachment Allowed
○ Attachment Blocked

Enter Process Name : **Eg.** Thunderbird.exe

Blacklisted Process ☑ Ignore Whitelisted Sites only for Blacklisted process

| □ | Process Name | Allow Only Whitelisted Site |
|---|---|---|

Attachments will be allowed from below sites irrespective of the above settings

Enter Site Name : **Eg.** Gmail.com,Yahoo

Whitelisted sites

□ Attachment / Email report
○ Report for attachment allowed ○ Report for all email (including Attachment)

□ Enable Shadow Copy for Attachment Allowed

Shadow Copy folder path :

Note : Only Drive name or full UNC path is Allowed.Eg:
1. "c:\"
2. "\\192.168.0.96\external\backup"

Advance Document settings
□ Turn off Save As PDF for Microsoft Office Document

## Attachment Control

The Attachment Control tab lets you control attachment flow within your organization.

**Attachment Allowed [Default]**
Select this option if you want attachments to be allowed through all processes except a specific set of processes mentioned below.

**Attachment Blocked**
Select this option if you want attachments to be blocked through all processes except a specific set of processes mentioned below.

**Configure Extension/Group based Whitelisting**
This option allows you to select/add groupwise file extensions in the whitelist in order to allow the attachments of those formats via mails and other processes. Apart from default extension groups, you can add new group of extensions using the **CUSTOM** group.

**Enter Process Name**
Enter the name of the processes that should be excluded from the above selection. Enter process name and then click **Add**. To delete the added process, select particular process in Blacklisted Process column and then click **Delete**.

**Blacklisted Process**
This will display a list of process you excluded when you selected the **Attachment Allowed** option. eScan will block all attachments through this process.

**Whitelisted Process**
This will display a list of process you excluded when you selected the **Attachment Blocked** option. eScan will allow all attachments through this process.

**Ignore Whitelisted Sites only for Blacklisted process [Default]**
Select this checkbox to ignore the whitelisted sites for process mentioned in Blacklist.

**Enter Site Name**
Enter the name of the websites through which attachments should be allowed irrespective of the above settings. To add site, enter site name and then click **Add**. To delete the added whitelisted site, select particular site in Whitelisted sites section and then click **Delete.**

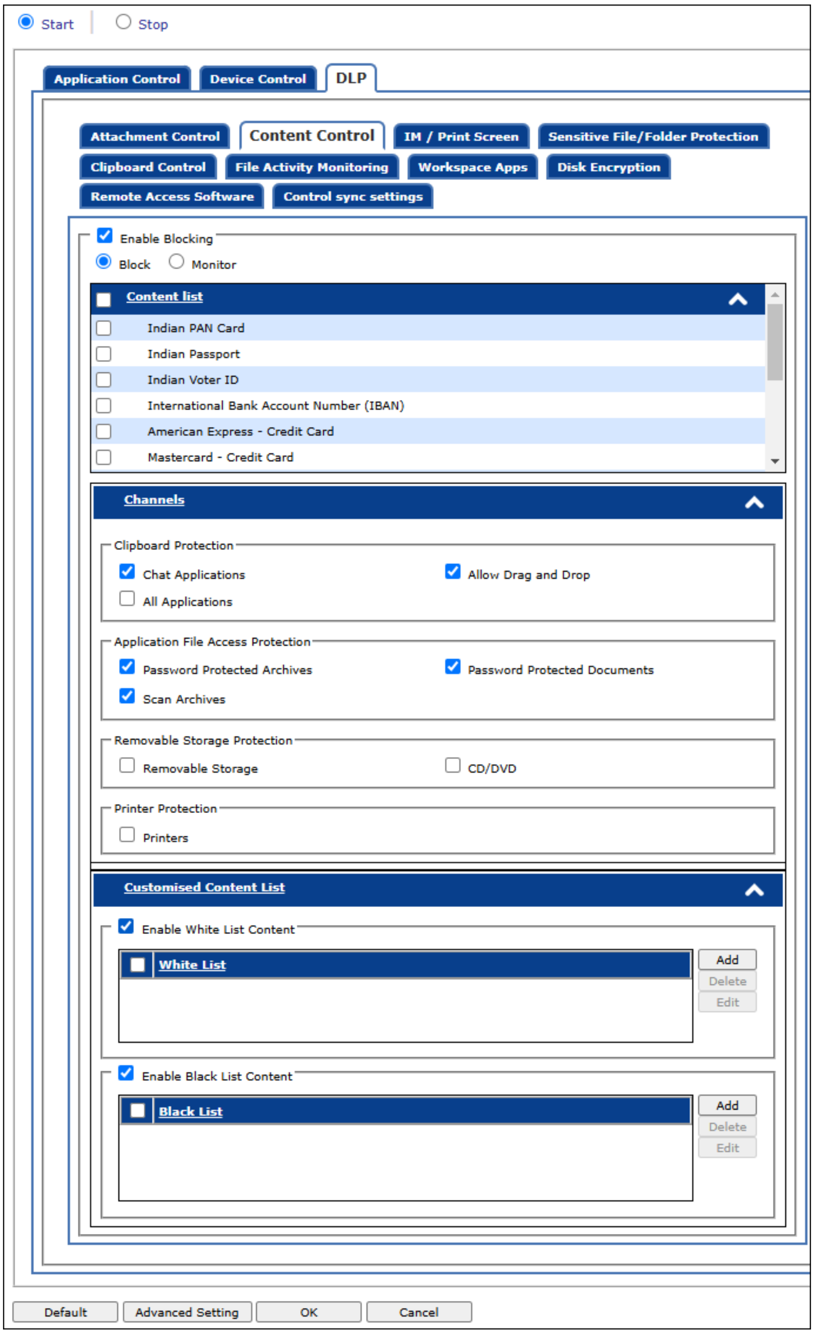
**Whitelisted Sites**
The websites added above to be white listed are displayed in this list.

**Attachment / Email report**
**Report for Attachment Allowed**
This will list all the attachment allowed along with Application used to send attachment. E.g. Google chrome, Firefox, Outlook, Skype, yahoo messenger, etc.

**Report for all email (Including Attachment)**
This will list all the email attachment uploaded along with Application used and subject of the email.

## Content Control

This tab enables the administrator to monitor & control the type of information which can be sent outside of the endpoints.



● Start ○ Stop

☑ Enable Blocking

● Block ○ Monitor

□ Content list

- □ Indian PAN Card
- □ Indian Passport
- □ Indian Voter ID
- □ International Bank Account Number (IBAN)
- □ American Express - Credit Card
- □ Mastercard - Credit Card

Channels

Clipboard Protection

☑ Chat Applications ☑ Allow Drag and Drop

□ All Applications

Application File Access Protection

☑ Password Protected Archives ☑ Password Protected Documents

☑ Scan Archives

Removable Storage Protection

□ Removable Storage □ CD/DVD

Printer Protection

□ Printers

Customised Content List

☑ Enable White List Content

□ White List

☑ Enable Black List Content

□ Black List

**Enable Blocking**

Select this option if you want to block all types of content, such as identity cards and personal details connected to your endpoint. This will enable all the options on this tab.

Block

Monitor

**Content List**

Select this option to block all lists of content as per the requirement.

**Channels**
You can configure all types of channel, where you can transfer the content through this.

**Clipboard Protection**

- **Chat Applications [Default]:** Select this option to deny all chat applications from sharing the data.
- **Allow Drag and Drop [Default]:** Select this option to allow the Drag and Drop function of sensitive content.
- **All Applications:** Select this option to deny all the applications from sharing the data.

**Application File Access Protection**

- **Password Protected Archives [Default]:** Select this option to block all password protected archives and from sharing it.
- **Password Protected Document [Default]:** Select this option to block all password protected document and from sharing it.
- **Scan Archives [Default]:** select this option to scan all the archives files.

**Removable Storage Protection**

- **Removable Storage:** select this option to deny all removable storage attached to the computer from accessing the personal information.
- **CD/DVD:** Select this option to deny all CD/DVD access to confidential data.

**Printer Protection**

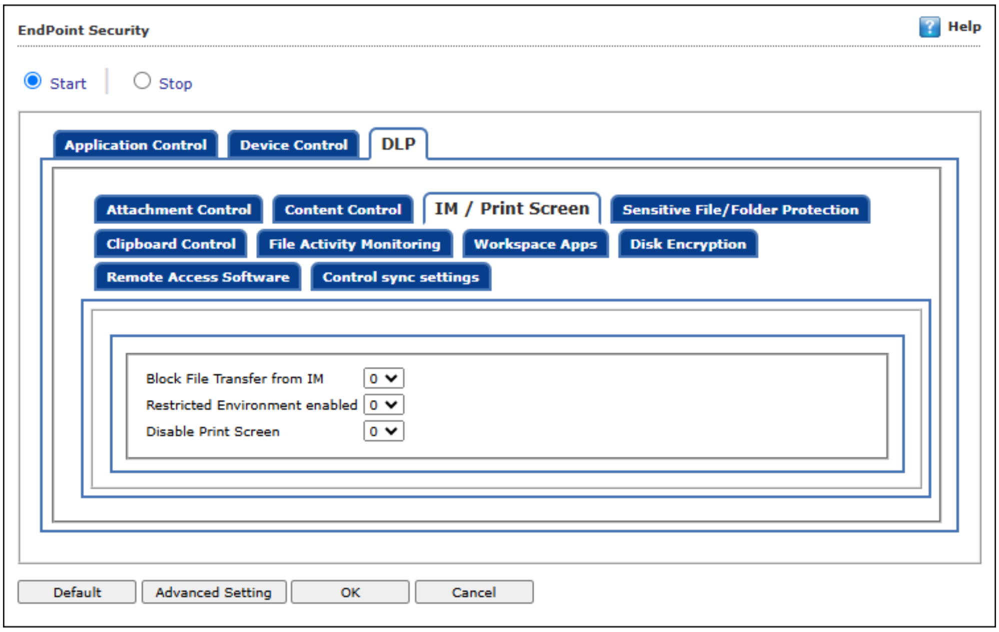
- **Printers:** Select this option to deny the use of network printers to print the sensitive data.

**Customized Content List**

- **Enable White List Content:** Select this option to allow all chat applications to share the whitelisted data such as bank statement number, MICR code, etc.
- **Enable Black List Content:** Select this option to deny all chat applications to share the blacklisted data.

## IM/Print Screen

The Advanced setting tab allows user to configure settings such as blocking file transfer via Instant messenger, disabling print screen, and screen capture options.



Block File Transfer from IM 0
Restricted Environment enabled 0
Disable Print Screen 0

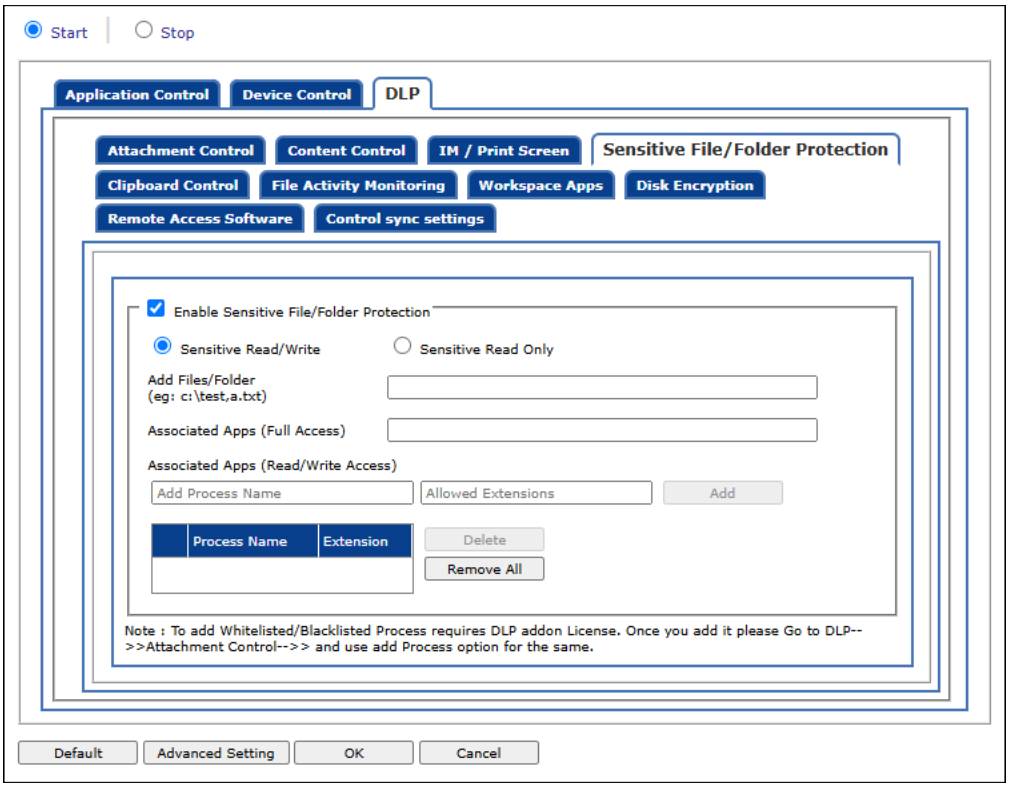
**Block File Transfer from IM (1 = Enable/0 = Disable)**
Select this option to allow/block file transfer from Instant Messengers.

**Restricted Environment enabled (1 = Enable/0 = Disable)**
Selecting this option lets you enable/disable protected environment settings.

**Disable Print Screen (1 = Enable/0 = Disable)**
Select this option to enable/disable use of print screen feature.

## Sensitive File/Folder Protection

The Sensitive File/Folder Protection tab ensures that sensitive data cannot be accessed using any other application except the default application specified. Once a folder is classified as a "Sensitive", its contents cannot be changed / deleted in any way. The files can be accessed using only the associated apps and any kind of editing is blocked to avoid data modification.



● Start ○ Stop

☑ Enable Sensitive File/Folder Protection

● Sensitive Read/Write ○ Sensitive Read Only

Add Files/Folder (eg: c:\test,a.txt)

Associated Apps (Full Access)

Associated Apps (Read/Write Access)

Note : To add Whitelisted/Blacklisted Process requires DLP addon License. Once you add it please Go to DLP-->>Attachment Control-->> and use add Process option for the same.

**Enable Sensitive File/Folder Protection**

Select this Checkbox to enable the Sensitive File and Folder protection.

- **Sensitive Read/Write [Default]:** Select this option to allow read/write access for sensitive files/folders.
- **Sensitive Read Only:** Select this option to allow read-only access for sensitive files/folders.

**Add Folder/Files**

Enter the folder or file name to classify as a sensitive.

**Associated Apps (Full Access)**

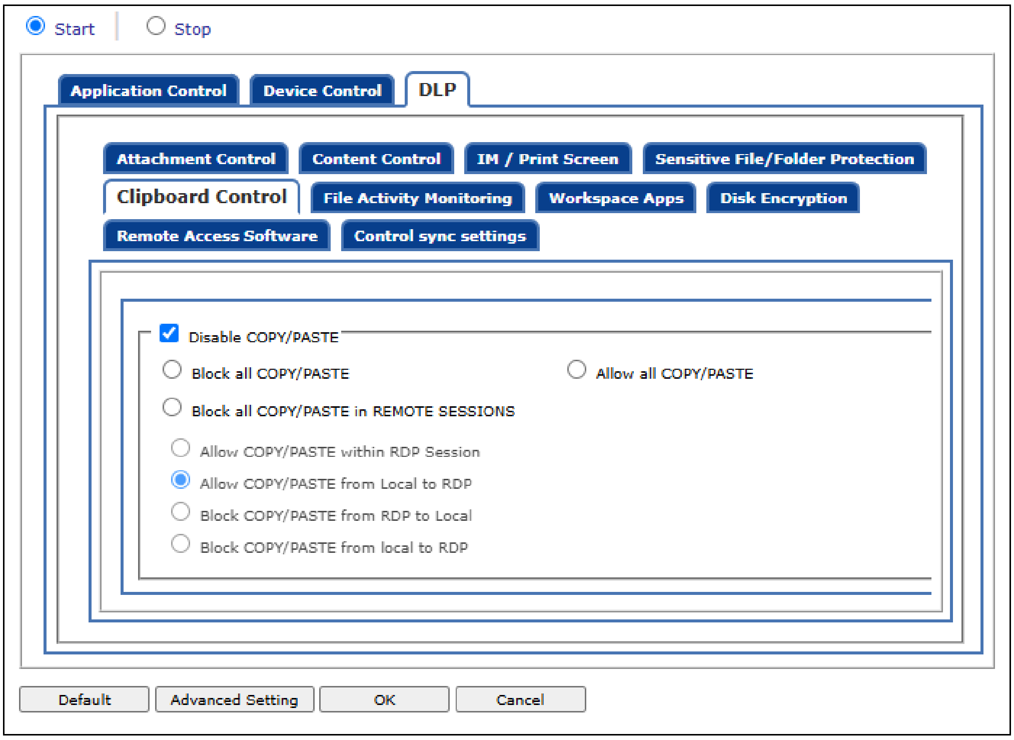
Enter the associated application name that has full access on sensitive files/folders.

**Associated Apps (Read/Write Access)**

Enter the associated application name that has read/write access on sensitive files/folders.

## Clipboard Control

For a device, once data is copied into the clipboard by any app, it can also be accessed from any other app. With Copy/Paste option disabled, a user is prohibited from copying any information to the clipboard.



● Start ○ Stop

☑ Disable COPY/PASTE

○ Block all COPY/PASTE ○ Allow all COPY/PASTE

○ Block all COPY/PASTE in REMOTE SESSIONS

○ Allow COPY/PASTE within RDP Session

● Allow COPY/PASTE from Local to RDP

○ Block COPY/PASTE from RDP to Local

○ Block COPY/PASTE from local to RDP

**Disable COPY/PASTE**

Select this option if you want to disable copy/paste action performed on computer. This will enable all the options on this tab.

**Block all COPY/PASTE:** Select this option to block all copy/paste actions.

**Allow all COPY/PASTE:** Select this option to allow all copy/paste actions.

**Block all COPY/PASTE in REMOTE SESSIONS:** Select this option to block all copy/paste actions perform in remote sessions.

**Allow COPY/PASTE within RDP Session:** Select this option to allow all copy/paste actions perform within RDP sessions.

**Allow COPY/PASTE from local to RDP [Default]:** Select this option to allow all copy/paste actions from local to RDP.

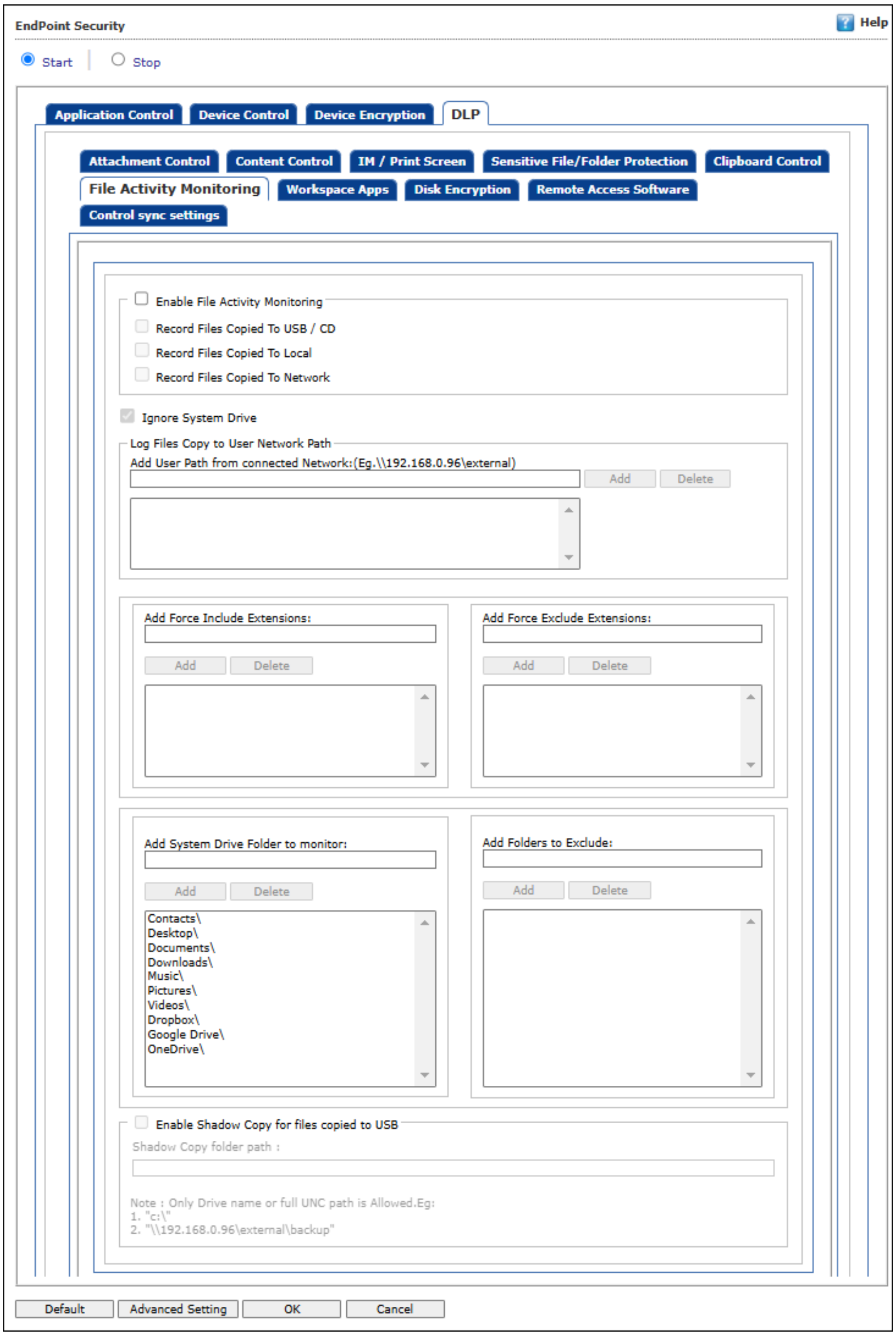
**Allow COPY/PASTE from RDP to local:** Select this option to allow all copy/paste actions from RDP to local.

**Block COPY/PASTE from Local to RDP:** Select this option to block all copy/paste actions in Local to RDP.

| | |
|---|---|
| ❗<br>**NOTE** | To add Whitelisted/Blacklisted Process requires DLP add-on License. Once you add it please Go to **DLP-->>Attachment Control-->>** and use add Process option for the same. |

## File Activity Monitoring

The File Activity Monitoring tab generates a record of the files created, copied, modified, and deleted on computers. Additionally, in case of misuse of any official files, the same can be tracked down to the user through the details captured in the report.



● Start ○ Stop

□ Enable File Activity Monitoring
□ Record Files Copied To USB / CD
□ Record Files Copied To Local
□ Record Files Copied To Network

☑ Ignore System Drive

Log Files Copy to User Network Path
Add User Path from connected Network:(Eg.\\192.168.0.96\external)

Add Force Include Extensions:

Add Force Exclude Extensions:

Add System Drive Folder to monitor:
Contacts\
Desktop\
Documents\
Downloads\
Music\
Pictures\
Videos\
Dropbox\
Google Drive\
OneDrive\

Add Folders to Exclude:

□ Enable Shadow Copy for files copied to USB
Shadow Copy folder path :

Note : Only Drive name or full UNC path is Allowed.Eg:
1. "c:\"
2. "\\192.168.0.96\external\backup"

### Enable File Activity Monitoring

Select this checkbox if you want to enable monitoring of file activity on computer. This will enable all the options on this tab.

### Record Files copied To USB/CD

Select this checkbox if you want eScan to create a record of the files copied from the system to USB drive.

**Record Files Copied To Local**
Select this checkbox if you want eScan to create a record of the files copied from one drive to another drive on the system. Please note that if you have selected "**Ignore System Drive**" along with this option no record will be captured if the files are copied from system drive (the drive in which OS is installed) to another drive.

**Record Files Copied To Network**
Select this checkbox if you want eScan to create a record of the files copied from managed computers to the network drive connected to it.

**Ignore System Drive**
Select this checkbox in case if you do not want eScan to record files that are copied from system drive of managed computers to either network drive or any local drive.

**Log Files Copy to User Network Path**
**Add User Path from connected Network: (Eg.\\192.168.0.96\external)**
Enter the user path from connected network to monitor. You can add or delete user path from connected network from the list of by clicking **Add/Delete**.

**Add Force Include Extensions**
Select this option to include File Extension for File Activity Monitoring (e.g. EXE). You can add or delete included extensions from the list of by clicking **Add/Delete**.

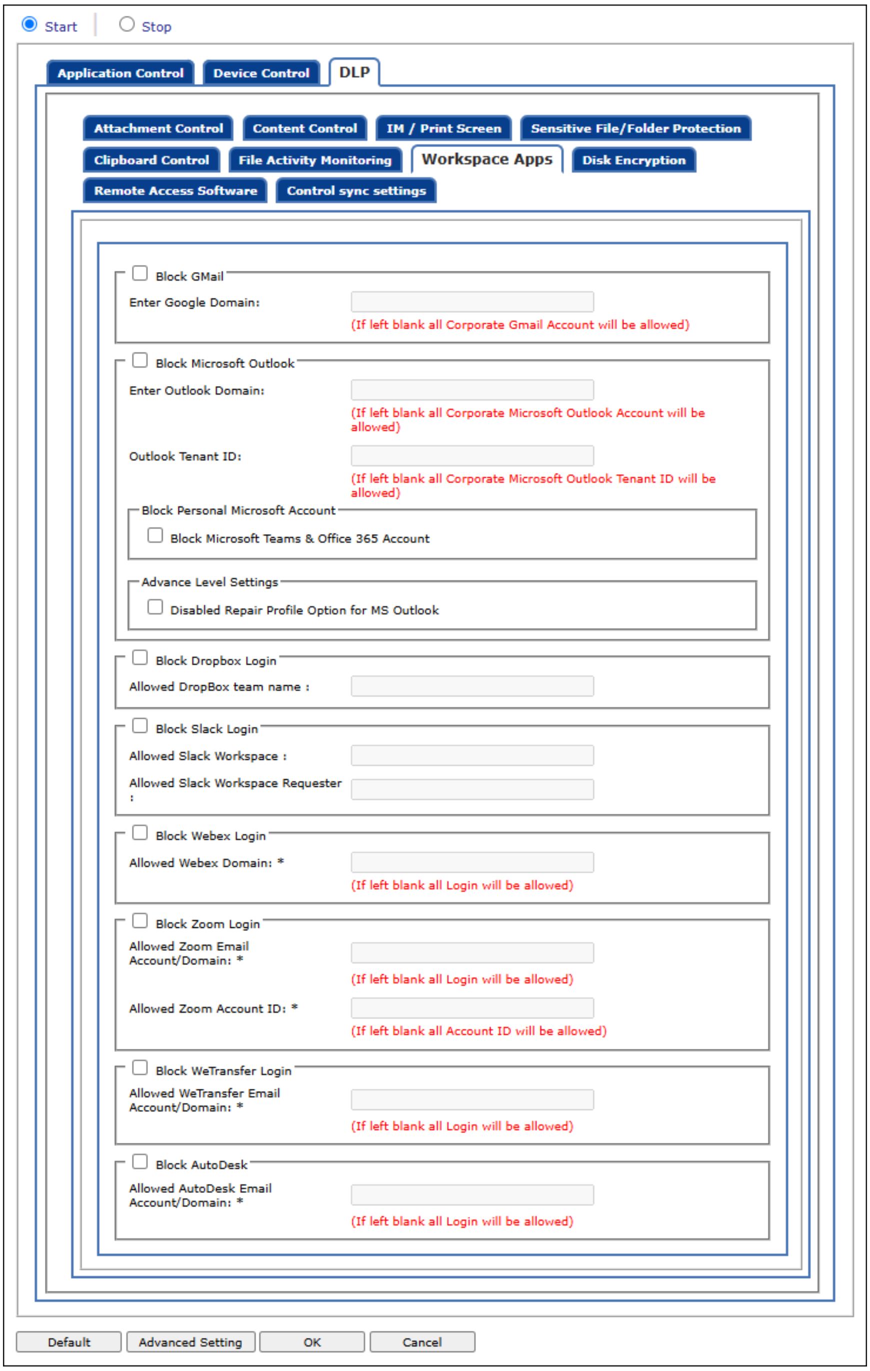
**Add Force Exclude Extensions**
Select this option to exclude File Extension for File Activity Monitoring (e.g. EXE). You can add or delete excluded extensions from the list of by clicking **Add/Delete**.

**Add System Drive Folder to monitor**
Select this option if you want eScan to monitor all the system drives installed on the computer. You can add or delete system drive folder from the list of by clicking **Add/Delete**.

**Add Folder to Exclude**
Select this check box if you want to exclude all the listed files, folders, and sub folders while it is monitoring folders. You can add or delete files/folders from the list of by clicking **Add/Delete**.

## Workspace Apps

To avoid any possible leak, eScan DLP provides functionality to block personal account access to Cloud-hosted services. This tab ensures that team members can only access the services using their corporate login credentials and not their personal credentials.



□ Block GMail

Enter Google Domain:

(If left blank all Corporate Gmail Account will be allowed)

□ Block Microsoft Outlook

Enter Outlook Domain:

(If left blank all Corporate Microsoft Outlook Account will be allowed)

Outlook Tenant ID:

(If left blank all Corporate Microsoft Outlook Tenant ID will be allowed)

Block Personal Microsoft Account

□ Block Microsoft Teams & Office 365 Account

Advance Level Settings

□ Disabled Repair Profile Option for MS Outlook

□ Block Dropbox Login

Allowed DropBox team name :

□ Block Slack Login

Allowed Slack Workspace :

Allowed Slack Workspace Requester :

□ Block Webex Login

Allowed Webex Domain: *

(If left blank all Login will be allowed)

□ Block Zoom Login

Allowed Zoom Email Account/Domain: *

(If left blank all Login will be allowed)

Allowed Zoom Account ID: *

(If left blank all Account ID will be allowed)

□ Block WeTransfer Login

Allowed WeTransfer Email Account/Domain: *

(If left blank all Login will be allowed)

□ Block AutoDesk

Allowed AutoDesk Email Account/Domain: *

(If left blank all Login will be allowed)

**Block Gmail**

Select this checkbox to block the personal Gmail account.

- **Allowed Corporate Gmail Account:** Enter the corporate email id to be allowed.

**Block Outlook Account**

Select this checkbox to block the personal Microsoft Outlook account.

- **Allowed Corporate Microsoft Outlook Account:** Enter the Microsoft Outlook account email id to be allowed.
- **Allowed Corporate Microsoft Outlook Tenant ID:** Enter the Microsoft Outlook Tenant id to be allowed.

**Block Dropbox Login**

Select this checkbox to block the Dropbox login.

- **Allowed DropBox team name:** Enter the team name of DropBox to be allowed.

**Block Slack Login**

Select this checkbox to block the Slack login.

- **Allowed Slack Workspace:** Enter the workspace email id to be allowed.
- **Allowed Slack Workspace Requester:** Enter the workspace requester's email id to be allowed.

**Block Webex Login**

Select this checkbox to block the Webex login.

- **Allowed Webex domain:** Enter a domain name to be allowed.

**Block Zoom Login**

Select this checkbox to block the zoom login.

- **Allowed Zoom Email Account/Domain:** Enter the zoom email id to be allowed.
- **Allowed Zoom Account ID:** Enter the account Id to be allowed.

**Block WeTransfer Login**

Select this checkbox to block the WeTransfer Login**.**

- **Allowed WeTransfer Email Account/Domain:** Enter the WeTransfer email id to be allowed.

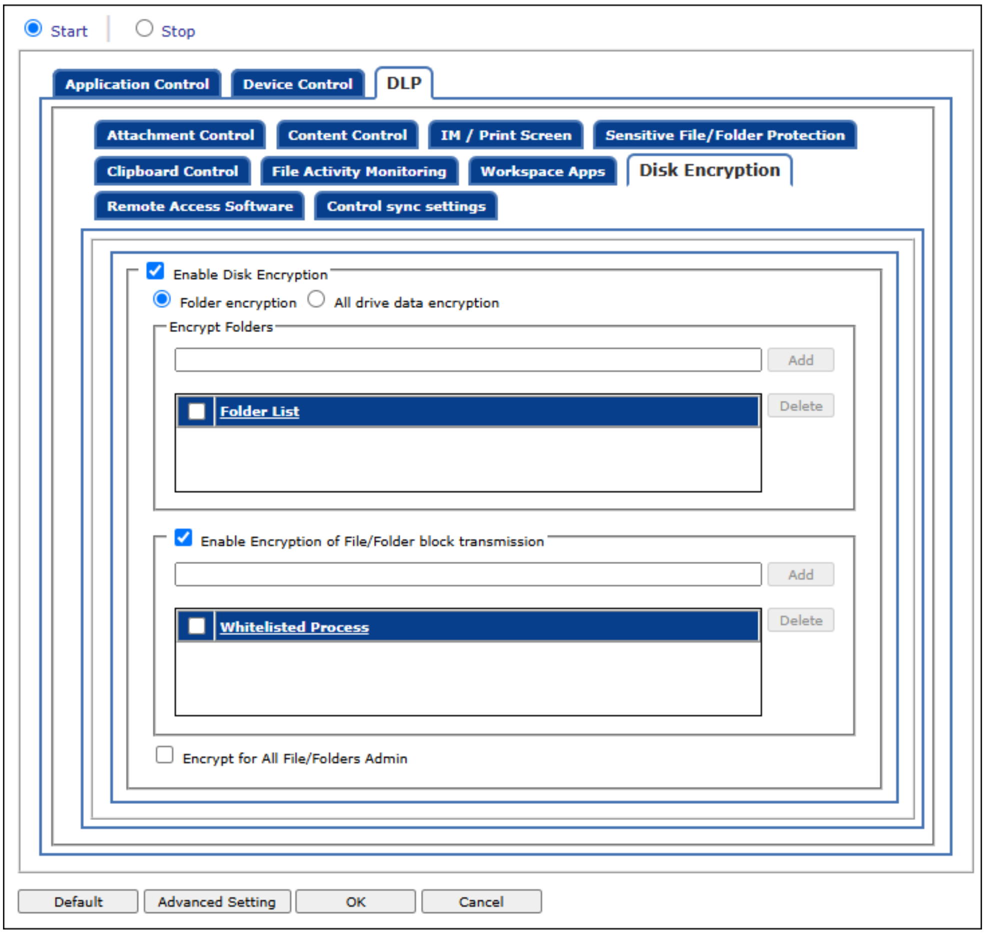
**Block AutoDesk**

Select this checkbox to block AutoDesk login.

- **Allowed AutoDesk Email Account/Domain:** Enter the Autodesk email id to be allowed.

## Disk Encryption

The Disk Encryption feature allows you to protect the data by encrypting particular folder or all the drives in a client computer. A data from an encrypted folder or drives cannot be modified or transferred to another location through any process.



● Start ○ Stop

☑ Enable Disk Encryption

● Folder encryption ○ All drive data encryption

Encrypt Folders

☑ Enable Encryption of File/Folder block transmission

□ Encrypt for All File/Folders Admin

Select the checkbox **Enable Disk Encryption** to enable the configuration of Disk Encryption settings.

### Folder Encryption

This option allows you to encrypt particular folder(s) in a client computer. Enter the folder path in the provided field to encrypt the same. All the data from these folders will be protected by EndPoint DLP.

Follow the steps mentioned below to encrypt the folder(s):

1. In the Disk Encryption window, select the checkbox **Enable Disk Encryption**.
2. Select the option **Folder encryption**.
3. Enter the folder path in the provided field in Encrypt Folders section.
4. Click on **Add**.
   The folder will be added in the list below and will get encrypted.

### All drive data encryption

Selecting this option will encrypt all the drives of a computer in order to protect the data from being exploited.

### Enable Encryption of File/Folder block transmission

This option allows you to whitelist the processes through which the data from encrypted files/folders can be transmitted without encryption.

Follow the steps mentioned below to whitelist the processes:

1. In the Disk Encryption window, select the checkbox **Enable Encryption of File/Folder block transmission**.
2. Enter the application name with extension in the provided field.
3. Click **Add**.
   The process will be whitelisted for transmitting the encrypted data.

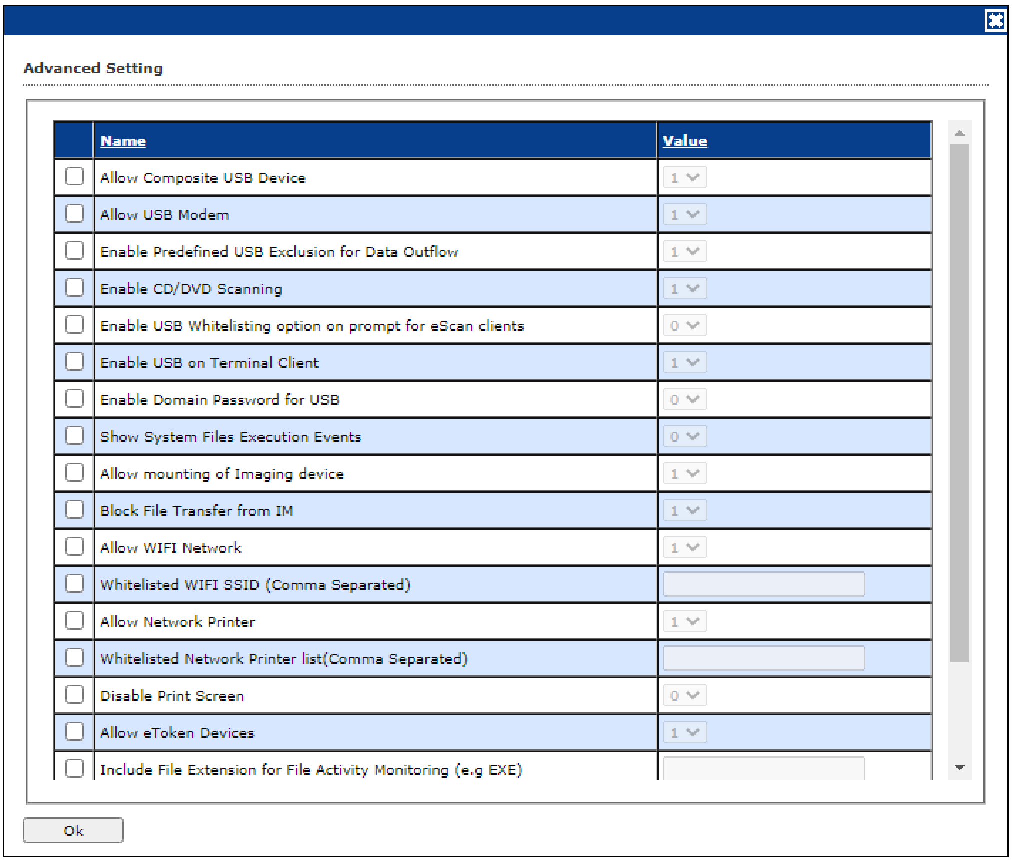
### Encrypt for All File/Folders Admin

Select this checkbox to enable the encryption of all the files/folders for the Administrator profile of particular computer.

| | |
|---|---|
| ❗<br>NOTE | • This option will encrypt only folders if **Folder encryption** option is selected.<br>• If the **All drive data encryption** is selected, it will encrypt folders as well as files. |

## Advanced Settings

Clicking **Advanced** displays Advanced Settings.



Advanced Setting

| | Name | Value |
|---|---|---|
| □ | Allow Composite USB Device | 1 |
| □ | Allow USB Modem | 1 |
| □ | Enable Predefined USB Exclusion for Data Outflow | 1 |
| □ | Enable CD/DVD Scanning | 1 |
| □ | Enable USB Whitelisting option on prompt for eScan clients | 0 |
| □ | Enable USB on Terminal Client | 1 |
| □ | Enable Domain Password for USB | 0 |
| □ | Show System Files Execution Events | 0 |
| □ | Allow mounting of Imaging device | 1 |
| □ | Block File Transfer from IM | 1 |
| □ | Allow WIFI Network | 1 |
| □ | Whitelisted WIFI SSID (Comma Separated) | |
| □ | Allow Network Printer | 1 |
| □ | Whitelisted Network Printer list(Comma Separated) | |
| □ | Disable Print Screen | 0 |
| □ | Allow eToken Devices | 1 |
| □ | Include File Extension for File Activity Monitoring (e.g EXE) | |

**Allow Composite USB Device (1 = Enable/0 = Disable)**
Select this option to allow/block use of composite USB devices.

**Allow USB Modem (1 = Enable/0 = Disable)**
Select this option to allow/block use of USB modem.

**Enable Predefined USB Exclusion for Data Outflow (1 = Enable/0 = Disable)**
Select this option to enable/disable use of predefined USB.

**Enable CD/DVD Scanning (1 = Enable/0 = Disable)**
Select this option enable/disable scanning of CD/DVD.

**Enable USB Whitelisting option on prompt for eScan clients (1 = Enable/0 = Disable)**
Select this option to enable/disable USB Whitelisting option on prompt for eScan clients.

**Enable USB on Terminal Client (1 = Enable/0 = Disable)**
Select this option to enable/disable USB on terminal client.

**Enable Domain Password for USB (1 = Enable/0 = Disable)**
Select this option to enable/disable domain password for USB.

**Show System Files Execution Events (1 = Enable/0 = Disable)**
Select this option to allow/block system files execution events.

**Allow mounting of Imaging device (1 = Enable/0 = Disable)**
Select this option to allow/block mounting of imaging devices.

**Block File Transfer from IM (1 = Enable/0 = Disable)**
Select this option to allow/block file transfer from Instant Messengers.

**Allow Wi-Fi Network (1 = Enable/0 = Disable)**
Select this option to allow/block use of Wi-Fi networks.

**Whitelisted WIFI SSID (Comma Separated)**
Select this option to whitelist WIFI SSID. Enter the WIFI SSID in comma separated format.

**Allow Network Printer (1 = Enable/0 = Disable)**
Select this option to allow/block use of network printers.

**Whitelisted Network Printer list (Comma Separated)**
Select this option to whitelist network printer list. Enter the name of printers in comma separated format.

**Disable Print Screen (1 = Enable/0 = Disable)**
Select this option to enable/disable use of printer screen.

**Allow eToken Devices (1 = Enable/0 = Disable)**
Select this option to allow/block use of eToken devices.

**Include File Extension for File Activity Monitoring (e.g EXE)**
Select this option to include File Extension for File Activity Monitoring.

**Exclude File Extension for File Activity Monitoring (e.g EXE)**
Select this option to exclude File Extension for File Activity Monitoring (e.g EXE).

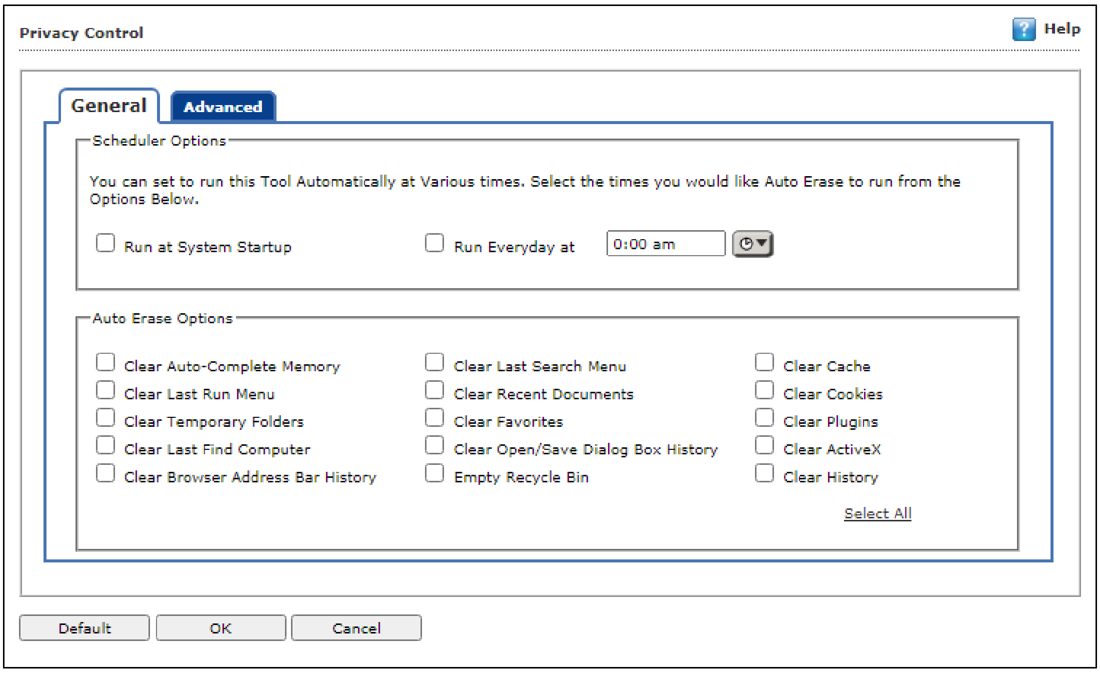
**Auto Whitelist BitLocker encrypted USB Devices (1 = Enable/0 = Disable)**
Select this option to allow/block auto whitelist BitLocker encrypted USB devices.

**Ask Password for whitelisted Devices only (1 = Enable/0 = Disable)**
Select this option to allow/block ask password for whitelisted devices.

| | |
|---|---|
| ❗<br>**NOTE** | Click **Default** to apply default settings done during eScan installation. It loads and resets the values to the default settings. |

# Privacy Control

The Privacy Control module protects your confidential information from theft by deleting all the temporary information stored on your computer. This module lets you use the Internet without leaving any history or residual data on your hard drive. It erases details of sites and web pages you have accessed while browsing.



Scheduler Options

You can set to run this Tool Automatically at Various times. Select the times you would like Auto Erase to run from the Options Below.

□ Run at System Startup

□ Run Everyday at 0:00 am

Auto Erase Options

□ Clear Auto-Complete Memory
□ Clear Last Run Menu
□ Clear Temporary Folders
□ Clear Last Find Computer
□ Clear Browser Address Bar History
□ Clear Last Search Menu
□ Clear Recent Documents
□ Clear Favorites
□ Clear Open/Save Dialog Box History
□ Empty Recycle Bin
□ Clear Cache
□ Clear Cookies
□ Clear Plugins
□ Clear ActiveX
□ Clear History

It consists following tabs:

- **General**
- **Advanced**

## General

This tab lets you specify the unwanted files created by web browsers or other installed software that should be deleted. You can configure the following settings:

### Scheduler Options

You can set the scheduler to run at specific times and erase private information, such as your browsing history from your computer. The following settings are available in the **Scheduler Options** section.

### Run at System Startup

It auto executes the Privacy Control module and performs the desired auto erase functions when the computer starts up.

### Run Everyday at

It auto executes the Privacy Control module at specified times and performs the desired auto erase functions. You can specify the time within the hours and minutes boxes.

### Auto Erase Options

The browser stores traceable information of the websites that you have visited in certain folders. This information can be viewed by others. eScan lets you remove all traces of websites that you have visited. To do this, it auto detects the browsers that are installed on your computer. It then displays the traceable component and default path where the temporary data is stored on your computer. You can select the following options based on your requirements.

**Clear Auto-Complete Memory**
Auto Complete Memory refers to the suggested matches that appear when you enter text in the Address bar, the Run dialog box, or forms in web pages. Hackers can use this information to monitor your surfing habits. When you select this checkbox, Privacy Control clears all this information from the computer.

**Clear Last Run Menu**
When you select this option, Privacy Control clears this information in the Run dialog box.

**Clear Temporary Folders**
When you select this option, Privacy Control clears files in the Temporary folder. This folder contains temporary files installed or saved by software. Clearing this folder creates space on the hard drive of the computer and boosts the performance of the computer.

**Clear Last Find Computer**
When you select this option, Privacy Control clears the name of the computer for which you searched last.

**Clear Browser Address Bar History**
When you select this checkbox, Privacy Control clears the websites from the browser's address bar history.

**Clear Last Search Menu**
When you select this option, Privacy Control clears the name of the objects that you last searched for by using the Search Menu.

**Clear Recent Documents**
When you select this checkbox, Privacy Control clears the names of the objects found in Recent Documents.

**Clear Favorites**
This checkbox clears Favorites added by the user in the computer.

**Clear Open/Save Dialog Box History**
When you select this checkbox, Privacy Control clears the links of all the opened and saved files.

**Empty Recycle Bin**
When you select this checkbox, Privacy Control clears the Recycle Bin. Use this option with caution as it permanently clears the recycle bin.

**Clear Cache**
When you select this checkbox, Privacy Control clears the Temporary Internet Files.

**Clear Cookies**
When you select this checkbox, Privacy Control clears the Cookies stored by websites in the browser's cache.

**Clear Plugins**
When you select this checkbox, Privacy Control removes the browser plug-in.

**Clear ActiveX**
When you select this checkbox, Privacy Control clears the ActiveX controls.

**Clear History**

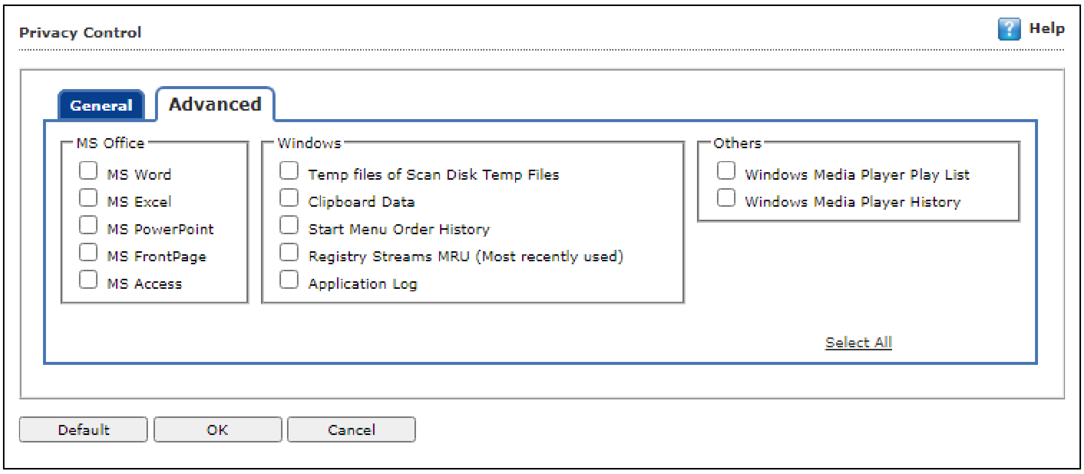
When you select this checkbox, Privacy Control clears the history of all the websites that you have visited.

In addition to these options, the **Auto Erase Options** section has below option as well.

**Select All/ Unselect All**
Click this button to select/unselect all the auto erase options.

## Advanced

This tab lets you select unwanted or sensitive information stored in MS Office, other Windows files and other locations that you need to clear.



Privacy Control

Help

General | Advanced

MS Office
- □ MS Word
- □ MS Excel
- □ MS PowerPoint
- □ MS FrontPage
- □ MS Access

Windows
- □ Temp files of Scan Disk Temp Files
- □ Clipboard Data
- □ Start Menu Order History
- □ Registry Streams MRU (Most recently used)
- □ Application Log

Others
- □ Windows Media Player Play List
- □ Windows Media Player History

Select All

**MS Office**
The most recently opened MS office files will be cleared if these options are selected**.**

**Windows**
The respective unwanted files like temp files will be cleared.

**Others**
The recent Windows media player playlist and its history will be cleared.

**Select All/ Unselect All**
Click this button to select/unselect all the options in Advanced tab.

| NOTE | Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings. |
|---|---|

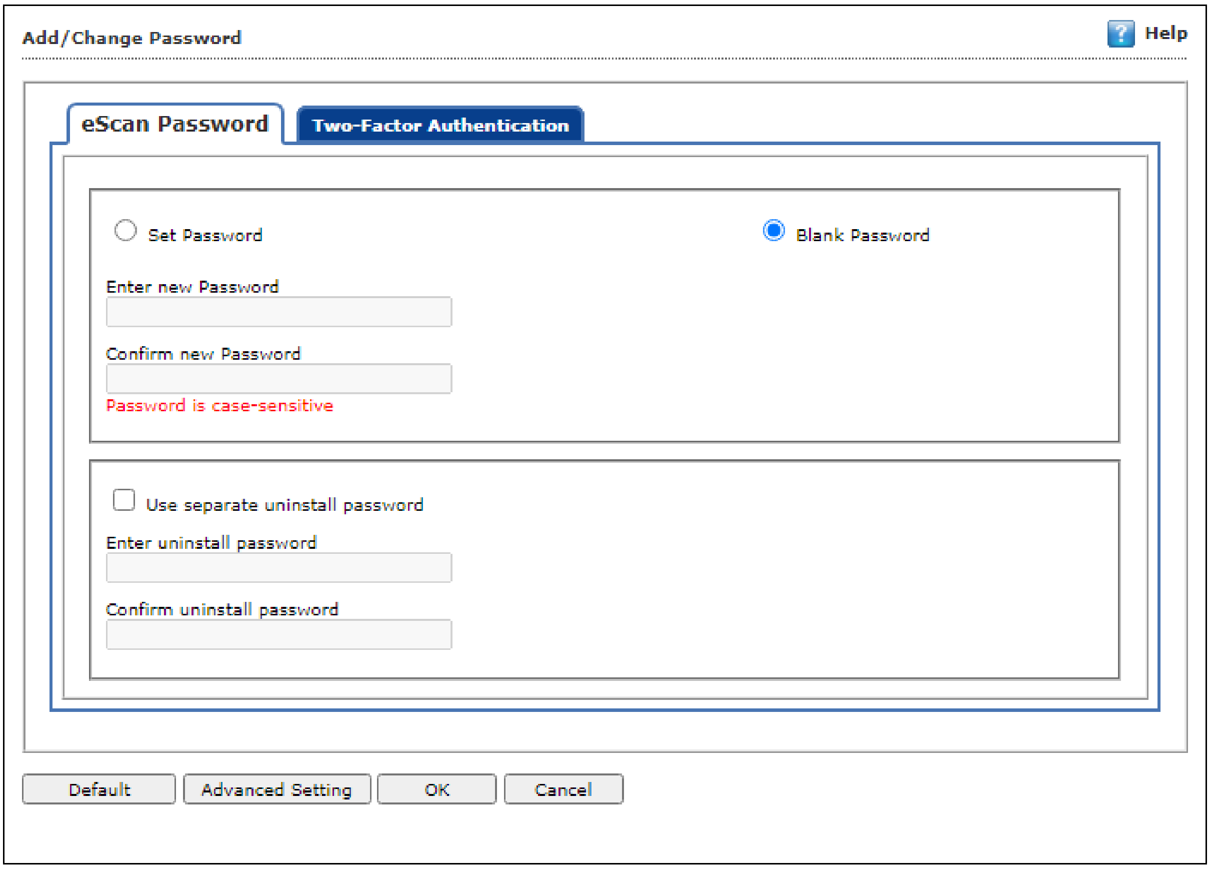
Policy Details also lets you do the following for Windows Operating System.

# Administrator Password

Administrator Password module lets you create and change password for administrative login of eScan protection center, additionally allows to set the uninstallation password.

## eScan Password

It also lets you keep the password as blank, wherein you can login to eScan protection center without entering any password for read-only access or you can set a password for Login.



Add/Change Password

○ Set Password

● Blank Password

Enter new Password

Confirm new Password

Password is case-sensitive

□ Use separate uninstall password

Enter uninstall password

Confirm uninstall password

There is also an option to set a uninstall password. An uninstallation password prevents personnel from uninstalling eScan client from their endpoint. Upon selecting **Uninstall** option, eScan asks them for uninstall password. To set an uninstall password, select checkbox **Use separate uninstall password**.

| | |
|---|---|
| **NOTE** | Click **Default** to apply default settings done during eScan installation. It loads and resets the values to the default settings. |

# Two-Factor Authentication

Your default system authentication (login/password) is Single-Factor Authentication which is considered less secure as it may put your organization's data at high risk of compromise. The Two-Factor Authentication, commonly known as 2FA, adds an extra layer of protection to your basic system logon. The 2FA feature requires personnel to enter an additional passcode after entering the system login password. So, even if an unauthorized person knows your system credentials, the 2FA feature secures a system against unauthorized access.

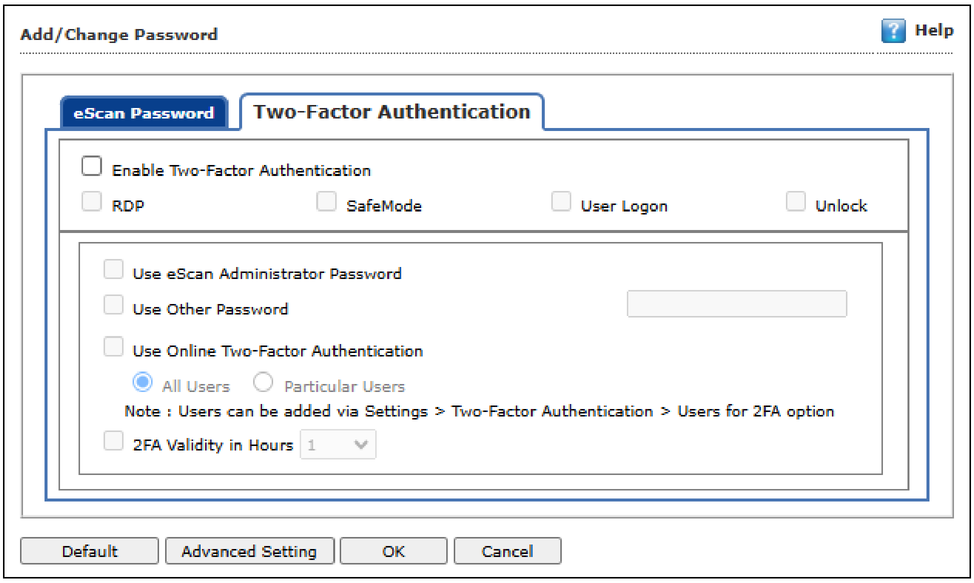
With the 2FA feature enabled, the system will be protected with basic system login and eScan 2FA. After entering the system credentials, eScan Authentication screen will appear as shown in the below image. The personnel will have to enter the 2FA passcode to access the system. A maximum of three attempts are allowed to enter the correct passcode. If the 2FA login fails, the personnel will have to wait for 30 seconds to log in again. Read about managing 2FA license.

To enable the Two-Factor Authentication feature, follow the steps given below:

1. In the eScan web console, go to **Managed Computers**.
2. Click **Policy Templates** > **New Template.**

| | |
|---|---|
| **NOTE** | You can enable the 2FA feature for existing Policy Templates by selecting a Policy Template and clicking **Properties**. Then, follow the steps given below. |

3. Select **Administrator Password** checkbox and then click **Edit**.
4. Click **Two-Factor Authentication** tab.
   Add/Change Password window appears.



Add/Change Password

□ Enable Two-Factor Authentication

□ RDP □ SafeMode □ User Logon □ Unlock

□ Use eScan Administrator Password

□ Use Other Password

□ Use Online Two-Factor Authentication

● All Users ○ Particular Users

Note : Users can be added via Settings > Two-Factor Authentication > Users for 2FA option

□ 2FA Validity in Hours 1

5. Select the checkbox **Enable Two-Factor Authentication**.
   The Two-Factor Authentication feature gets enabled.

## Login Scenarios

The 2FA feature can be used for all the following login scenarios:

### RDP

RDP stands for Remote Desktop Protocol. Whenever someone takes remote connection of a client's system, the personnel will have to enter system login credentials and 2FA passcode to access the system.

### Safe Mode

After a system is booted in Safe Mode, the personnel will have to enter system login credentials and 2FA passcode to access the system.

### User Logon

Whenever a system is powered on or restarted, the personnel will have to enter system login credentials and 2FA passcode to access the system.

### Unlock

Whenever a system is unlocked, the personnel will have to enter login credentials and 2FA passcode to access the system.

## Password Types

If the policy is applied to a group, the 2FA passcode will be same for all group members.
The 2FA passcode can also be set for specific computer(s).
You can use following all password types to log in:

### Use eScan Administrator Password

You can use the existing eScan Administrator password for 2FA login. This password can be set in **eScan Password** tab besides the **Two-Factor Authentication** tab.

### Use Other Password

You can set a new password, which can be a combination of uppercase, lowercase, numbers, and special characters.

### Use Online Two-Factor Authentication

This option can be enabled for all users or for particular user according to the requirement.
To learn more about adding user and enabling the 2FA, **click here**.

| | |
|---|---|
| **NOTE** | Users can be added via **Settings** > **Two-Factor Authentication** > **Users for 2FA** option. |

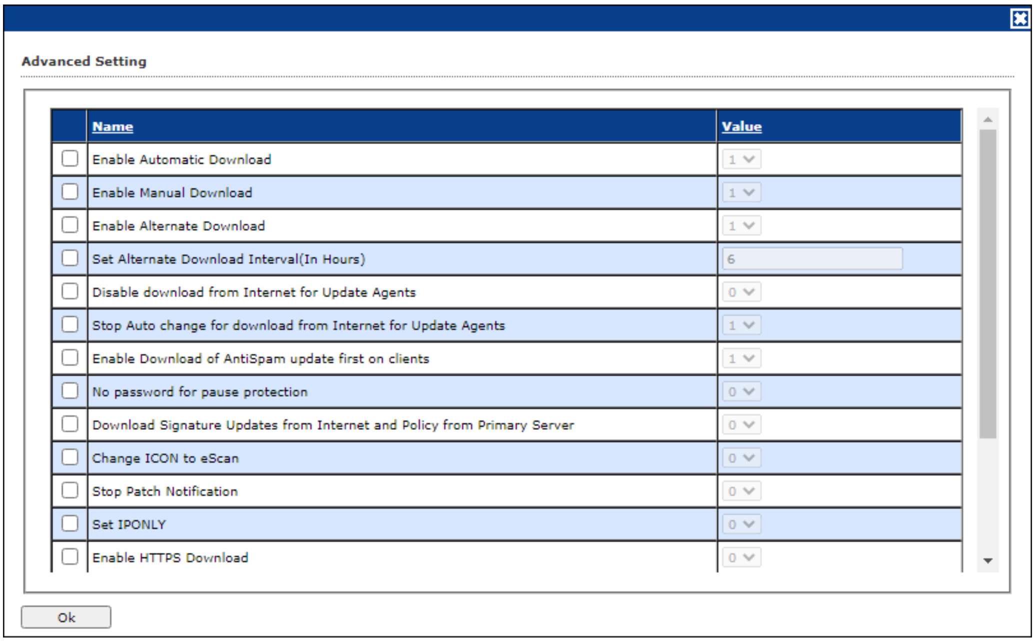
To use this feature, follow the steps given below:

1. Install the Authenticator app from Play Store for Android devices or App Store for iOS devices.
2. Open the Authenticator app and tap **Scan a barcode**.
3. Select the checkbox **Use Online Two-Factor Authentication**.
4. Go to **Managed Computers** and below the top right corner, click **QR code for 2FA**.
   A QR code appears.
5. Scan the onscreen QR code via the Authenticator app.
   A Time-based One-Time Password (TOTP) appears on smart device.

Forward this TOTP to personnel for login.

## Advanced Setting

Clicking **Advanced Setting** displays Advance setting.



Advanced Setting

| | Name | Value |
|---|---|---|
| □ | Enable Automatic Download | 1 |
| □ | Enable Manual Download | 1 |
| □ | Enable Alternate Download | 1 |
| □ | Set Alternate Download Interval(In Hours) | 6 |
| □ | Disable download from Internet for Update Agents | 0 |
| □ | Stop Auto change for download from Internet for Update Agents | 1 |
| □ | Enable Download of AntiSpam update first on clients | 1 |
| □ | No password for pause protection | 0 |
| □ | Download Signature Updates from Internet and Policy from Primary Server | 0 |
| □ | Change ICON to eScan | 0 |
| □ | Stop Patch Notification | 0 |
| □ | Set IPONLY | 0 |
| □ | Enable HTTPS Download | 0 |

**Enable Automatic Download (1 = Enable/0 = Disable)**
It lets you Enable/Disable Automatic download of Antivirus signature updates.

**Enable Manual Download (1 = Enable/0 = Disable)**
It lets you Enable/Disable Manual download of Antivirus signature updates.

**Enable Alternate Download (1 = Enable/0 = Disable)**
It lets you Enable/Disable download of signatures from eScan (Internet) if eScan Server is not reachable.

**Set Alternate Download Interval (In Hours)**
It lets you define time interval to check for updates from eScan (Internet) and download it on managed computers.

**Disable download from Internet for Update Agents (1 = Enable/0 = Disable)**
Selecting this option lets you disable Update Agents from downloading the virus signature from internet.

**Stop Auto change for download from Internet for Update Agents (1 = Enable/0 = Disable)**
This option is used when an Update Agent didn't find the primary server to download virus signature , then it tries to get virus signature from internet, so to stop Update Agent from downloading from internet this option is to be set to 1(one).

**Enable Download of Anti-Spam update first on clients (1 = Enable/0 = Disable)**
Normally while updating a system for virus signatures, we first download the anti-virus signature and then anti-spam signature. This option lets you first download Anti-spam updates on clients.

**No password for pause protection**
Selecting this option will let you pause the eScan protection without entering password.
Download Signature Updates from Internet and Policy from Primary Server.

**Change ICON to eScan (1= Enable/0=Disable)**
Selecting this option will allow you to change the icon of the eScan.

**Stop Patch Notification (1= Enable/ 0 = Disable)**
This option allows you to enable/disable the patch notification option.

**Set IPONLY (1=Enable/0=Disable)**
Select enable/disable to set the IP ONLY option.

**Enable HTTPS Download (1=Enable/0=Disable)**
This option allows you to enable/ disable the HTTPS Download option.

**Show Protection Center in Read Only Mode (Applicable only on icon Click)**
Select enable/ disable to show Protection Center in Read Only Mode option.

**Enable Policy REAPP (1=Enable/0=Disable)**
Select this option to enable Policy REAPP option.

**Disable Policy REAPP REG Only (1=Enable/0=Disable)**
Select this option to disable the Policy REAPP REG only option.

**Enable Win Patch download (1=Enable/0=Disable)**
Select this option to enable Win Patch Download option.

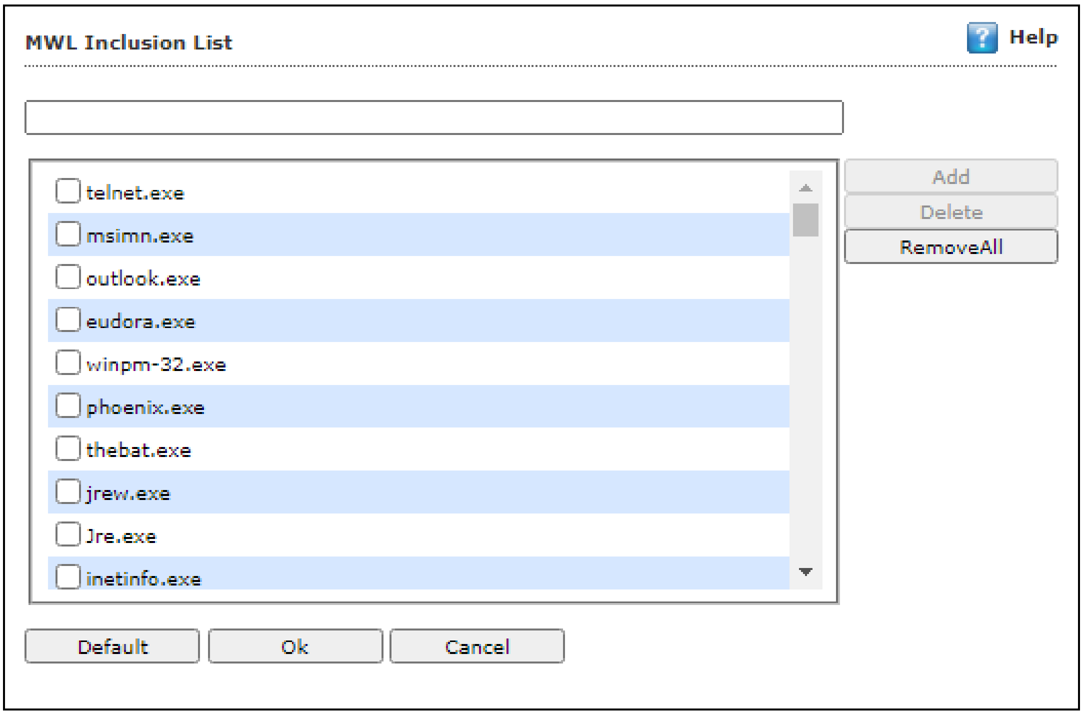
**Enable ALL Win Patch Download (1=Enable/0=Disable)**
Select this option to enable ALL Win Patch Download option.

# MWL (MicroWorld WinSock Layer)

eScan's "MicroWorld-WinSock Layer" (MWL) is a revolutionary concept in scanning Internet traffic on a real-time basis. It has changed the way the world deals with Content Security threats. Unlike the other products and technologies, MWL tackles a threat before it reaches your applications. MWL is technically placed above the WinSock layer and acts as a "Transparent Gatekeeper" on the WinSock layer of the operating system. All content passing through WinSock has to mandatorily pass through MWL, where it is checked for any security violating data. If such data occurs, it is removed and the clean data is passed on to the application.

# MWL Inclusion List

The MWL Inclusion List contains the name of all executable files which will bind itself to MWTSP.DLL. All other files are excluded.



MWL Inclusion List

- □ telnet.exe
- □ msimn.exe
- □ outlook.exe
- □ eudora.exe
- □ winpm-32.exe
- □ phoenix.exe
- □ thebat.exe
- □ jrew.exe
- □ Jre.exe
- □ inetinfo.exe

## Add files to Inclusion List

To add executable files to the Inclusion List, follow the steps given below:

1. Enter the executable file name and then click **Add**.
   The executable file will be added to the Inclusion List.

## Delete files from Inclusion List

To delete executable files from the Inclusion List, follow the steps given below:

1. Select the appropriate file checkbox, and then click **Delete**.
   A confirmation prompt appears.
2. Click **OK**.
   The executable file will be deleted from the Inclusion List.

## Remove all files from Inclusion List

To remove all executable files from the Inclusion List, follow the steps given below:

1. Click **Remove All**.

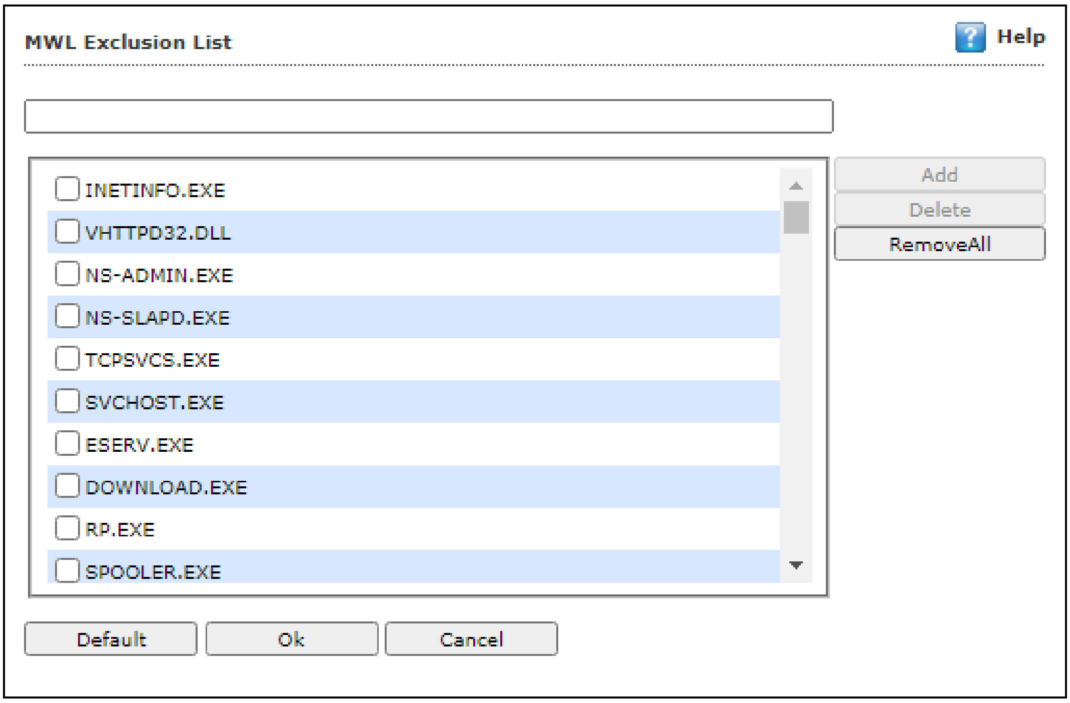
A confirmation prompt appears.

2. Click **OK**.
   All executable files will be removed from the Inclusion List.

| | |
|---|---|
| ❗<br>**NOTE** | Click **Default** to apply default settings, done during eScan installation. It loads and resets the values to the default settings. |

# MWL Exclusion List

The MWL (MicroWorld WinSock Layer) Exclusion List contains the name of all executable files which will not bind itself to **MWTSP.DLL**.



□ INETINFO.EXE
□ VHTTPD32.DLL
□ NS-ADMIN.EXE
□ NS-SLAPD.EXE
□ TCPSVCS.EXE
□ SVCHOST.EXE
□ ESERV.EXE
□ DOWNLOAD.EXE
□ RP.EXE
□ SPOOLER.EXE

## Adding files to Exclusion List

To add executable files to the Exclusion List, follow the steps given below:

1. Enter the executable file name and then click **Add**.
   The executable file will be added to the Exclusion List.

## Deleting files from Exclusion List

To delete executable files from the Exclusion List, follow the steps given below:

1. Select the appropriate file checkbox, and then click **Delete**.
   A confirmation prompt appears.
2. Click **OK**.
   The executable file gets deleted from the Exclusion List.

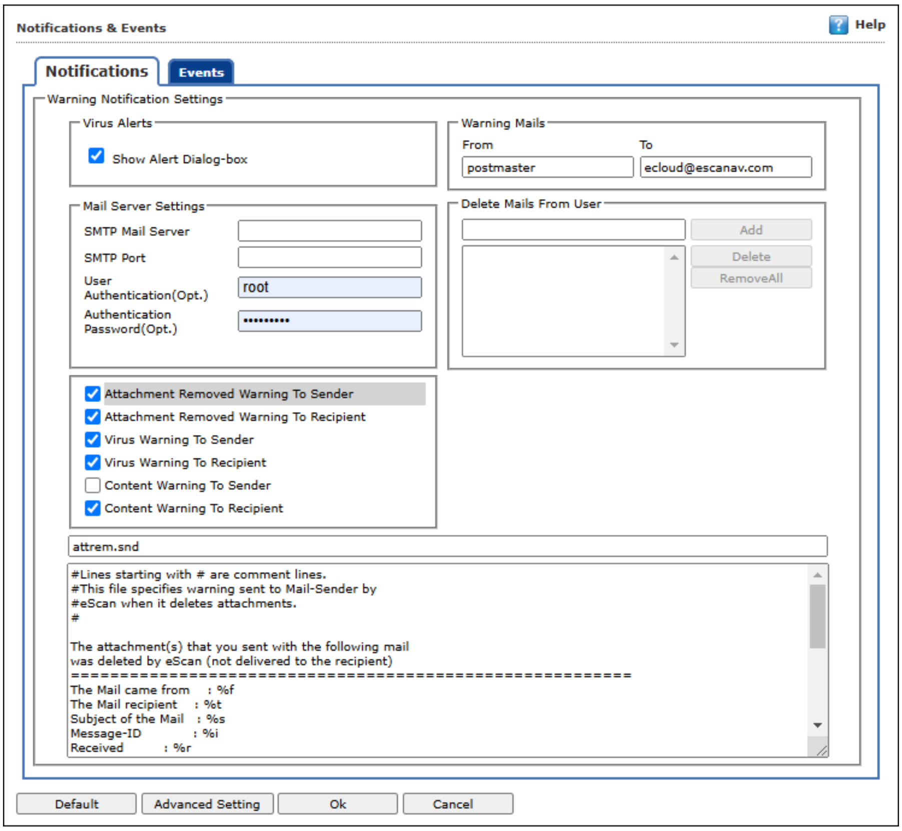
## Removing all files from Exclusion List

To remove all executable files from the Exclusion List, follow the steps given below:

1. Click **Remove All**.
   A confirmation prompt appears.
2. Click **OK**.
   All executable files get removed from the Exclusion List.

| | |
|---|---|
| NOTE | Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings. |

# Notifications and Events



Notifications & Events

Warning Notification Settings

Virus Alerts

☑ Show Alert Dialog-box

Warning Mails

From: postmaster

To: ecloud@escanav.com

Mail Server Settings

SMTP Mail Server:

SMTP Port:

User Authentication(Opt.): root

Authentication Password(Opt.): •••••••••

Delete Mails From User

☑ Attachment Removed Warning To Sender
☑ Attachment Removed Warning To Recipient
☑ Virus Warning To Sender
☑ Virus Warning To Recipient
☐ Content Warning To Sender
☑ Content Warning To Recipient

attrem.snd

```
#Lines starting with # are comment lines.
#This file specifies warning sent to Mail-Sender by
#eScan when it deletes attachments.
#

The attachment(s) that you sent with the following mail
was deleted by eScan (not delivered to the recipient)
==========================================================
The Mail came from    : %f
The Mail recipient    : %t
Subject of the Mail   : %s
Message-ID            : %i
Received         : %r
```

## Notifications

Notifications tab lets you configure the notification settings. It lets you send emails to specific recipients when malicious code is detected in an email or email attachment. It also lets you send alerts and warning messages to the sender or recipient of an infected message. You can configure the following settings:

### Virus Alerts [Default]

This section contains **Show Alert Dialog box** option. Select this option if you want Mail Anti-Virus to alert you when it detects a malicious object in an email.

### Warning Mails

Configure this setting if you want Mail Anti-Virus to send warning emails and alerts to a given sender or recipient. The default sender is **postmaster** and the default recipient is **postmaster**.

### Attachment Removed Warning to Sender [Default]

Select this checkbox if you want Mail Anti-Virus to send a warning message to the sender of an infected attachment. Mail Anti-Virus sends this email when it encounters a virus infected attachment in an email. The email content is displayed in the preview box.

**Attachment Removed Warning to Recipient [Default]**
Select this checkbox if you want Mail Anti-Virus to send a warning message to the recipient when it removes an infected attachment. The email content is displayed in the preview box.

**Virus Warning to Sender [Default]**
Select this checkbox if you want Mail Anti-Virus to send a virus warning message to the sender. The email content is displayed in the preview box.

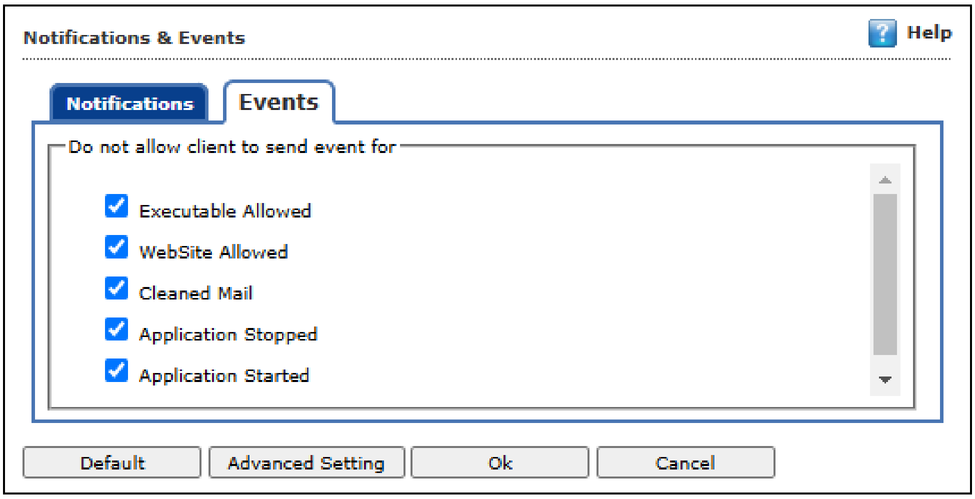
**Virus Warning to Recipient [Default]**
Select this checkbox if you want Mail Anti-Virus to send a virus warning message to the recipient. The email content is displayed in the preview box.

**Content Warning to Sender**
Select this checkbox if you want Mail scanner to send a content warning message to the sender. The email content is displayed in the preview box.

**Content Warning to Recipient [Default]**
Select this checkbox if you want Mail scanner to send a content warning message to the recipient. The email content is displayed in the preview box.

**Delete Mails from User**
You can configure eScan to automatically delete emails that have been sent by specific users. For this, you need to add the email addresses of such users to the **Delete Mails From User** field. The **Add**, **Delete**, and **Remove All** buttons appear as dimmed. After you enter text in the **Delete Mails From User** field, the buttons get enabled.

## Events


Notifications & Events

Do not allow client to send event for

☑ Executable Allowed
☑ WebSite Allowed
☑ Cleaned Mail
☑ Application Stopped
☑ Application Started

Events tab lets you define the settings to allow/restrict clients from sending alert for following events:

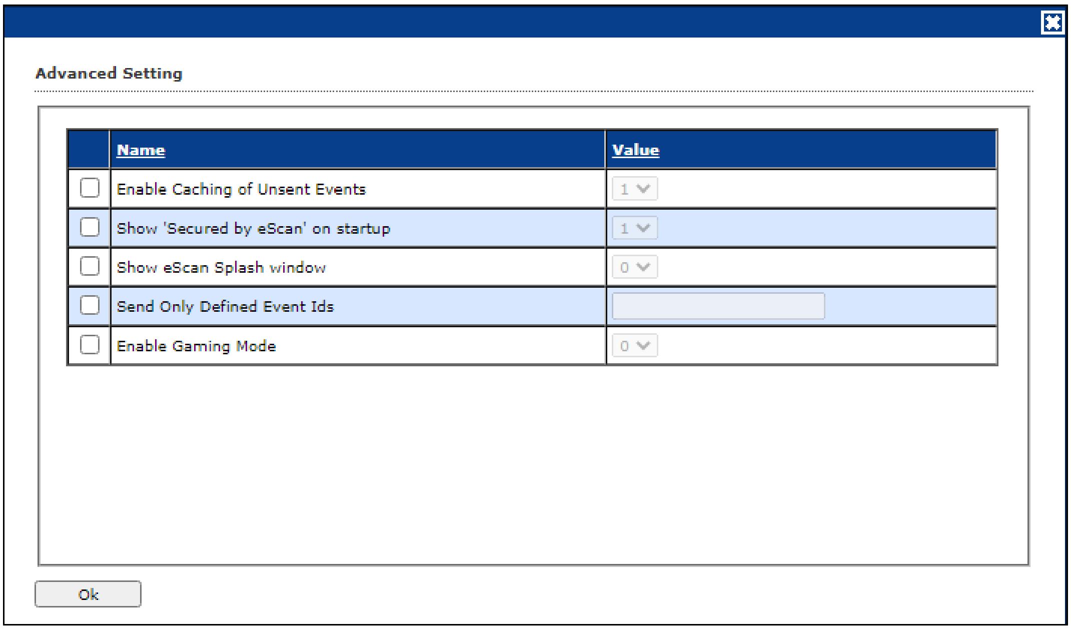
- Executable Allowed
- Website Allowed
- Cleaned Mail
- Application Stopped
- Application Started

By default, all events are selected.

| NOTE | Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings. |
|---|---|

## Advanced Settings

Clicking **Advanced Setting** displays Advance setting.



Advanced Setting

| | Name | Value |
|---|---|---|
| □ | Enable Caching of Unsent Events | 1 |
| □ | Show 'Secured by eScan' on startup | 1 |
| □ | Show eScan Splash window | 0 |
| □ | Send Only Defined Event Ids | |
| □ | Enable Gaming Mode | 0 |

**Enable Caching of Unsent Events (1 = Enable/0= Disable)**
It lets you Enable/Disable automatic caching of unsent events.

**Show 'Secured by eScan' on startup (1 = Enable/0= Disable)**
It lets you Enable/Disable the display of 'Secured by eScan' at the startup of the computers.

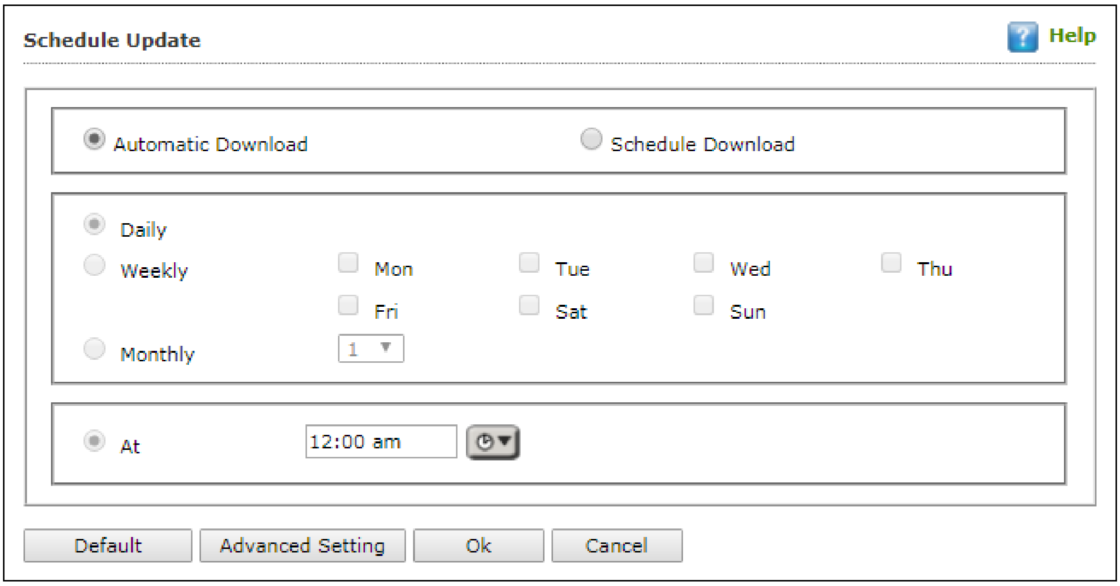
**Show eScan Splash window (1 = Enable/0= Disable)**
It lets you Enable/Disable display of eScan Splash Window.

**Send Only Defined Event Ids**
It lets you send only the defined events such as File Antivirus IDs, Mail Antivirus IDs, and more.

**Enable Gaming Mode (1 = Enable/0 = Disable)**
It lets you Enable/Disable the gaming mode on the computer.

# Schedule Update

The Schedule Update lets you schedule eScan database updates.



Schedule Update

● Automatic Download ○ Schedule Download

● Daily

○ Weekly □ Mon □ Tue □ Wed □ Thu

□ Fri □ Sat □ Sun

○ Monthly 1

● At 12:00 am

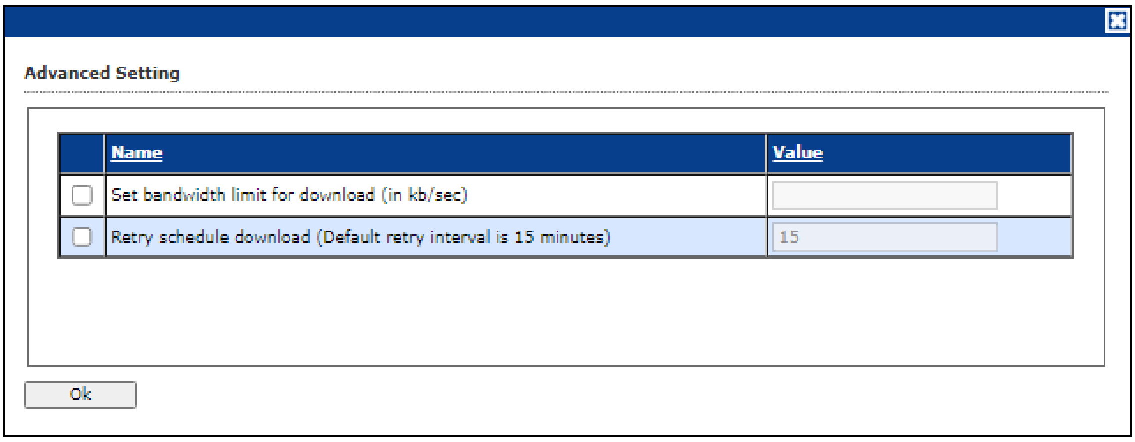
The updates can be downloaded automatically with **Automatic Download [Default]** option.

-OR-

The updates can be downloaded on a schedule basis with **Schedule Download** option. Select intervals and time basis as per your preferences.

## Advanced Settings

Clicking **Advanced Setting** displays Advance setting.



Advanced Setting

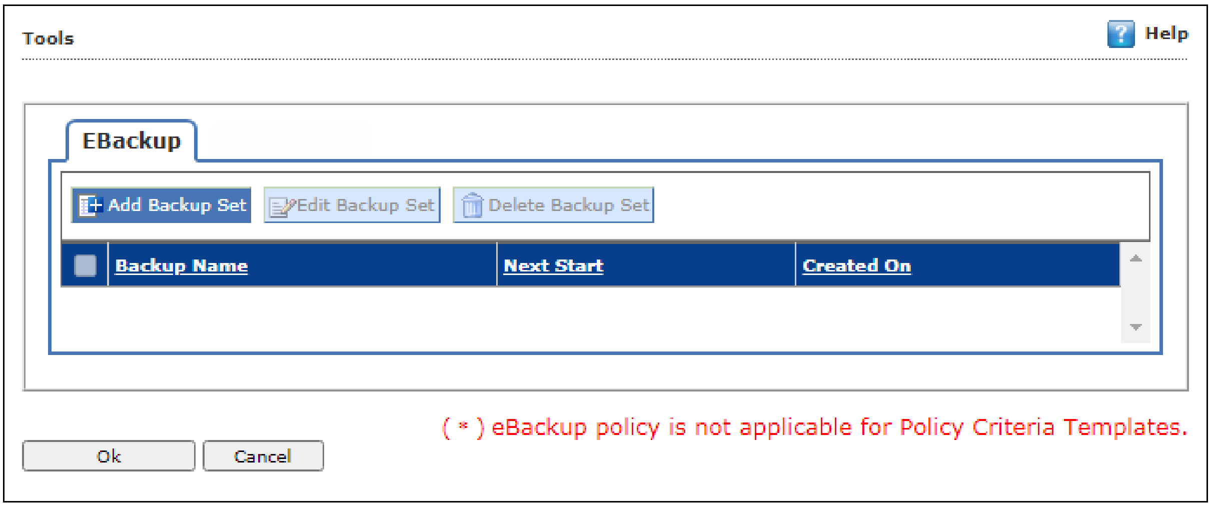
| | Name | Value |
|---|---|---|
| □ | Set bandwidth limit for download (in kb/sec) | |
| □ | Retry schedule download (Default retry interval is 15 minutes) | 15 |

**Set bandwidth limit for download (in kb/sec)**
It lets you define bandwidth limit for download on managed computers.

**Retry schedule download (Default retry interval is 15 minutes)**
It lets you define time to retry for download updates (Default retry interval is 15 minutes) on managed computers.

# Tools

The Tools lets you configure EBackup Settings.



( * ) eBackup policy is not applicable for Policy Criteria Templates.

## eBackup

Taking regular backup of your critical files stored on your computer is very important, as files may get misplaced or damaged due to issues such as virus outbreak, modification by a ransomware or another user. This feature of eScan allows you to take backup of your important files stored on your computer such as documents, photos, media files, music files, contacts, and so on. It allows you to schedule the backup process by creating tasks. The backed up data is stored in an encrypted format in a folder secured by eScan's real-time protection. You can create Backup jobs by adding files, folders to take a backup either manually or schedule the backup at a defined time or day.

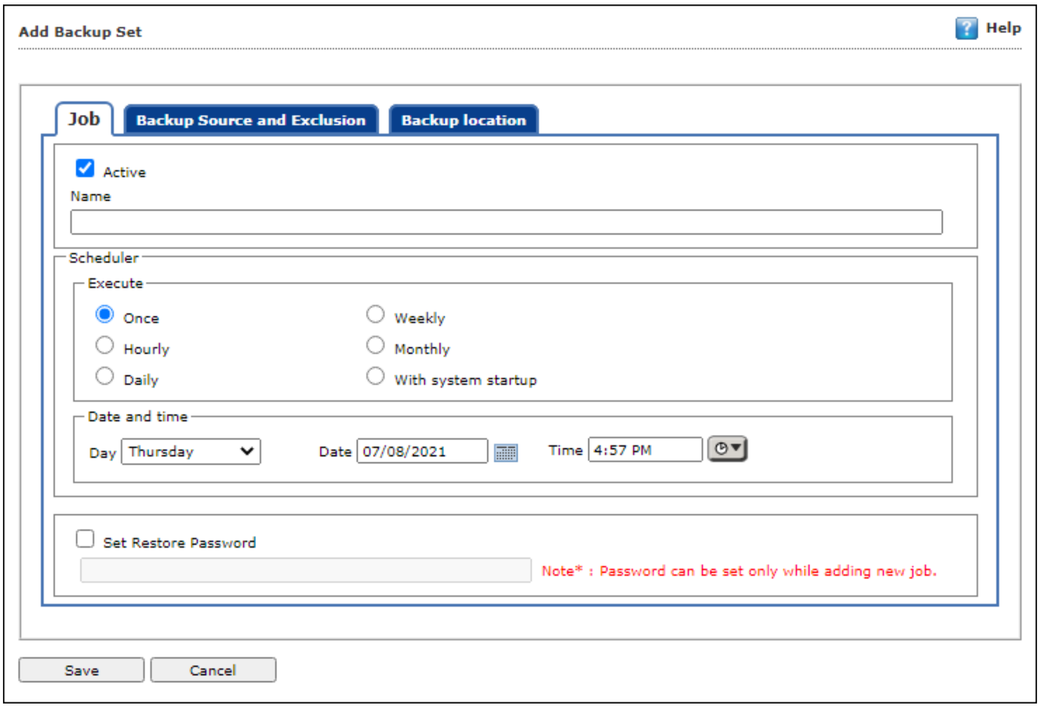
With eBackup tab you can:

- Create, schedule, edit, and delete backup jobs as per requirement.
- Take a backup of specific folder(s)/file extension(s) on local endpoint, external drives or network drive.
- Exclude specific folder(s)/file extension(s) from being backed up.
- Add specific file extensions to be backed up along with regular backup as per requirement.
- Save the backup data in external hard drive or local drive.

To add a backup set, click **Add Backup Set** option. Following tabs are appears.

## Job

This tab you can schedule the eBackup option.



Add Backup Set

☑ Active

Name

Scheduler

Execute

● Once ○ Weekly

○ Hourly ○ Monthly

○ Daily ○ With system startup

Date and time

Day Thursday Date 07/08/2021 Time 4:57 PM

□ Set Restore Password

Note* : Password can be set only while adding new job.

### Active

Select this option to set the configuring eBackup option as active.

### Name

Enter a name for an eBackup task.

### Scheduler

This option allows you to schedule the eBackup to repeat the process Once, Hourly, Daily, Weekly, Monthly, or with system startup.

### Date and time

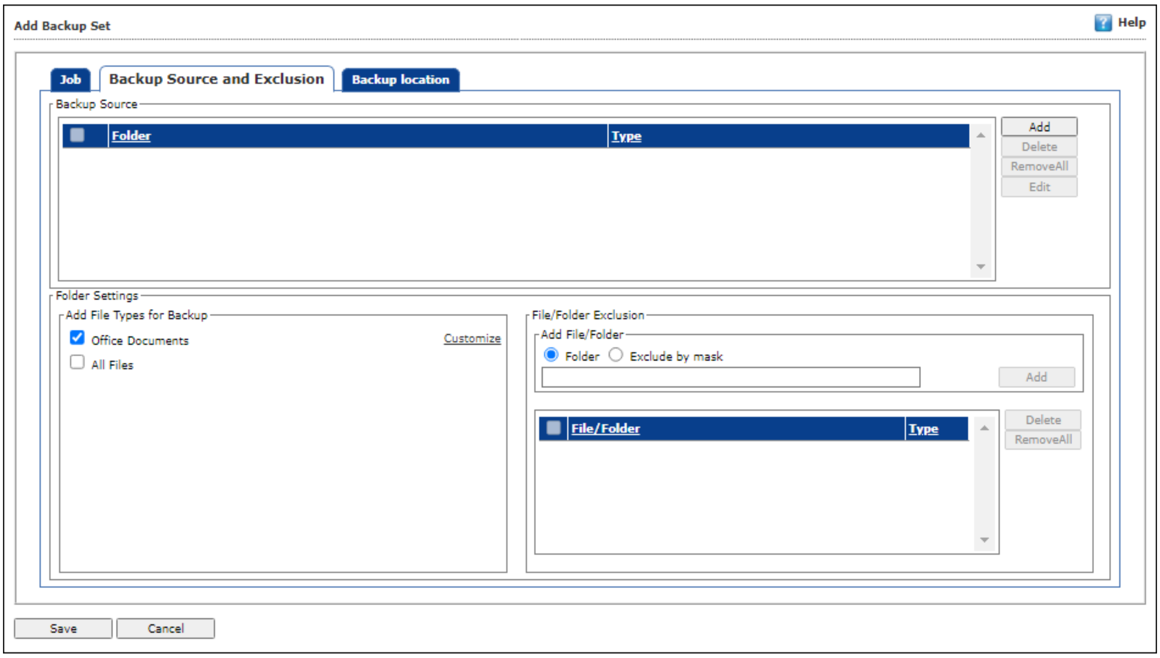
This option allows you to select the day, time, and date for running the scheduled eBackup task.

### Set Restore Password

Select this option to set a password for restoring backup file on the computer.

## Backup Source and Exclusion

This tab allows you to include and exclude the folder and files for backup.



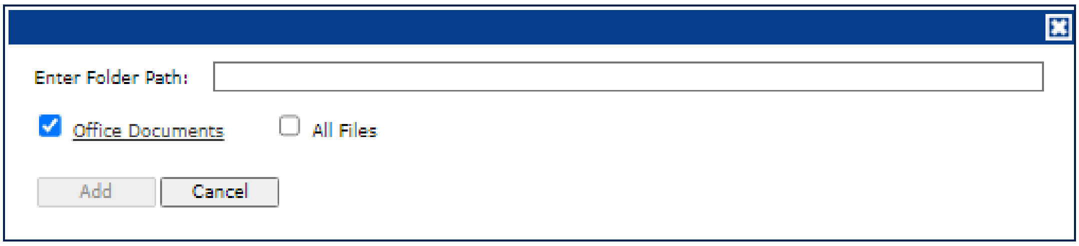
☑ Office Documents

□ All Files

● Folder ○ Exclude by mask

### Backup Source

Click on **Add**, to add the folder path for backup. Clicking Add, following window appears.



Enter Folder Path:

☑ Office Documents □ All Files

Select whether you want to backup the offline documents or all files. Click **Add**.

- Click **Delete**, to delete the added folder path.
- To remove all paths at a time, click **Remove All**.
- To modify, select folder and click **Edit**.

### Folder Settings

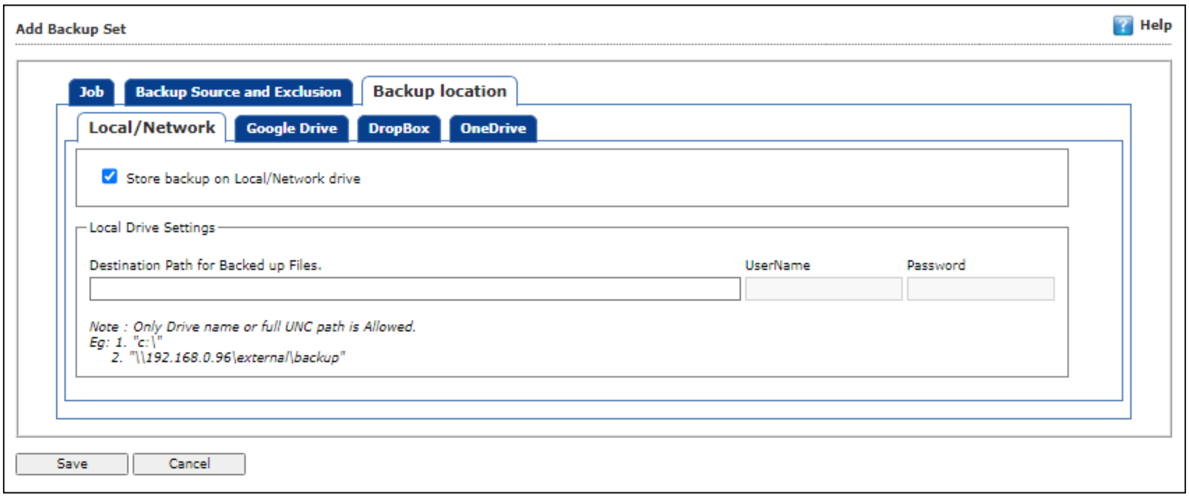
- **Add File Type for Backup**: Select the type of files for backup. By default, Office Documents option is selected.

### File/Folder Exclusion

In this section, you can exclude a specific folder or a file format from getting backed up. You can add, delete, and remove the files for the same.

## Backup Location

This tab allows you to define the storage location for the backup created.



Add Backup Set

Local Drive Settings

Store backup on Local/Network drive ☑

Destination Path for Backed up Files.

Note : Only Drive name or full UNC path is Allowed.
Eg: 1. "c:\"
2. "\\192.168.0.96\external\backup"

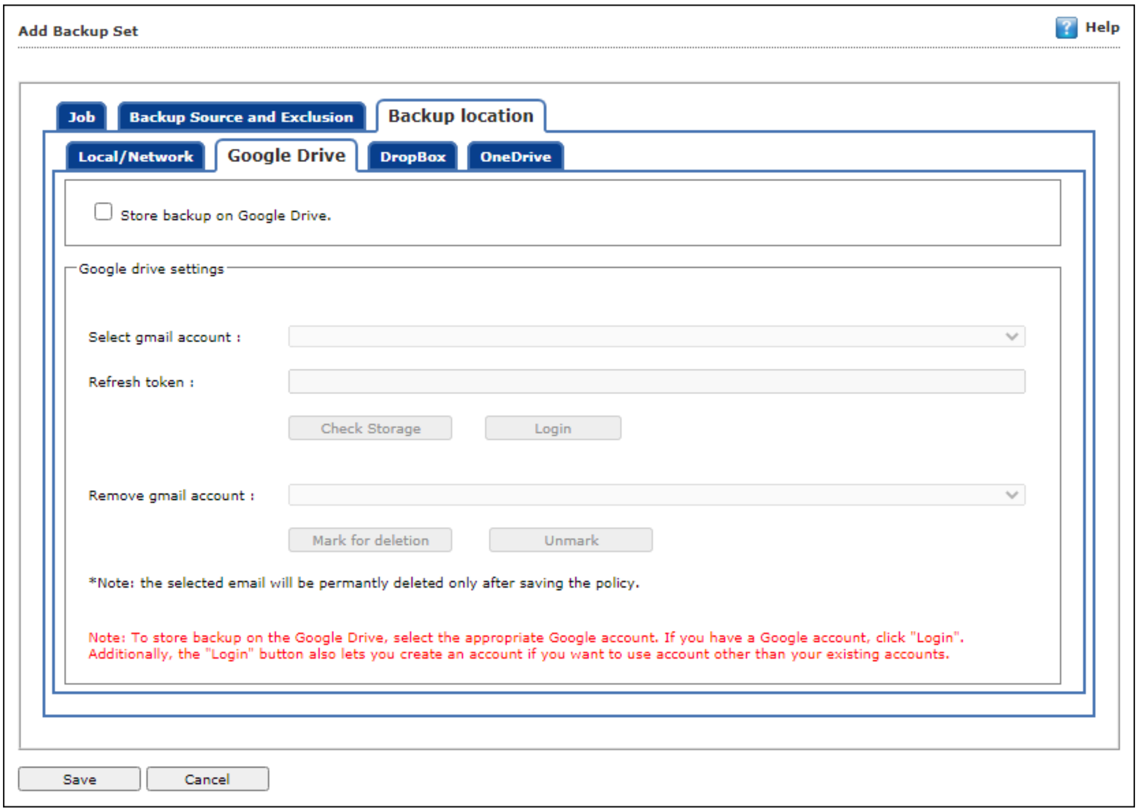
## Local/Network

Administrator can save the backup set in the Local/Network Drive by providing the path of the drive and Username and password for the network drive.

| | |
|---|---|
| NOTE | Network storage for backup set will be available in the trail period. To continue the use of this feature user need to avail the license for the same.<br>In case of system crash or hardware failure, user can recover the created data backup, so storing the backup in the network drive, mapped drive, or NAS drive would be useful in such scenarios. |

## Google Drive

Administrator can save the backup set in the Google Drive by selecting the appropriate Gmail account and password for the same.



□ Store backup on Google Drive.

Google drive settings

Select gmail account :

Refresh token :

Remove gmail account :

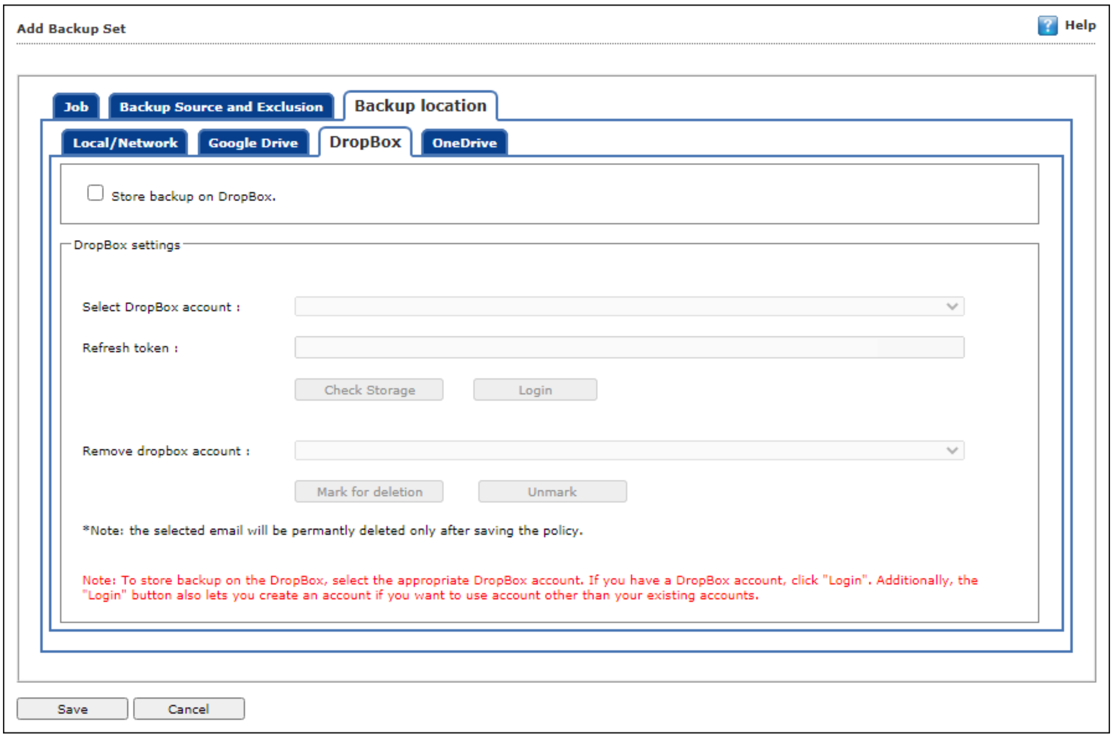
*Note: the selected email will be permantly deleted only after saving the policy.

Note: To store backup on the Google Drive, select the appropriate Google account. If you have a Google account, click "Login". Additionally, the "Login" button also lets you create an account if you want to use account other than your existing accounts.

| | |
|---|---|
| **NOTE** | To store backup on the Google Drive, select the appropriate Google account. If you have a Google account, click "**Login**". Additionally, the "**Login**" button also lets you create an account if you want to use account other than your existing accounts. |

### DropBox

Administrator can save the backup set in the DropBox by selecting the appropriate DropBox account and password for the same.



□ Store backup on DropBox.

DropBox settings

Select DropBox account :

Refresh token :

Remove dropbox account :

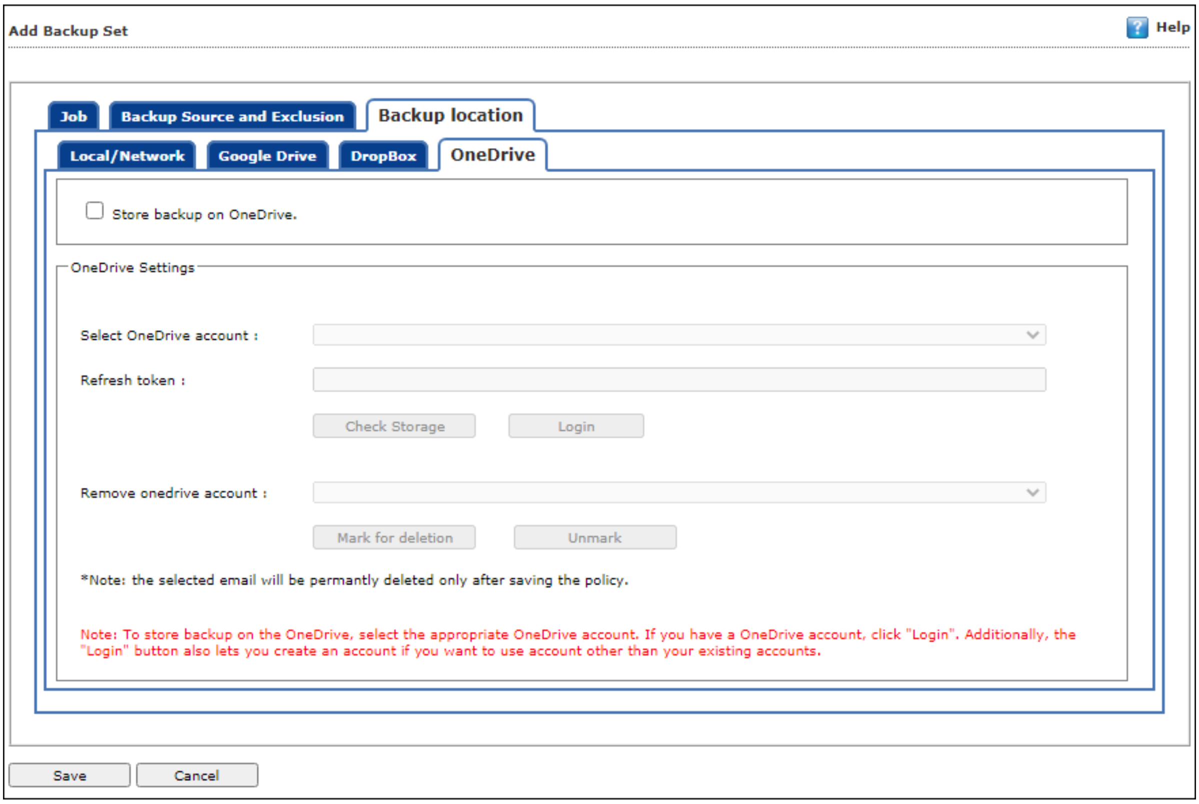
*Note: the selected email will be permantly deleted only after saving the policy.

Note: To store backup on the DropBox, select the appropriate DropBox account. If you have a DropBox account, click "Login". Additionally, the "Login" button also lets you create an account if you want to use account other than your existing accounts.

| | |
|---|---|
| **NOTE** | To store backup on the DropBox, select the appropriate DropBox account. If you have a DropBox account, click "**Login**". Additionally, the "**Login**" button also lets you create an account if you want to use account other than your existing accounts. |

**OneDrive**

Administrator can save the backup set in the OneDrive by selecting the appropriate OneDrive account and password for the same.



□ Store backup on OneDrive.

OneDrive Settings

Select OneDrive account :

Refresh token :

Remove onedrive account :

*Note: the selected email will be permantly deleted only after saving the policy.

Note: To store backup on the OneDrive, select the appropriate OneDrive account. If you have a OneDrive account, click "Login". Additionally, the "Login" button also lets you create an account if you want to use account other than your existing accounts.

| | |
|---|---|
| NOTE | To store backup on the OneDrive, select the appropriate OneDrive account. If you have an OneDrive account, click "**Login**". Additionally, the "**Login**" button also lets you create an account if you want to use account other than your existing accounts. |

**Add Backup Set**

To create a Backup Set, follow the steps mentioned below:

1. Go to **Managed Computers**.
2. Click **Policy Templates** > **New Template.**

| | |
|---|---|
| NOTE | You can add the backup set for existing Policy Templates by selecting a Policy Template and then clicking **Properties**. Then, follow the steps given below: |

3. Select **Tools** checkbox and then click **Edit**.
4. Click **Add Backup Set**.
   Add Backup Set window appears.
5. In Job tab, enter a name.
6. In the Scheduler section, select a preferred interval for backup execution.
7. Click **Backup Source and Exclusion** tab and configure the same accordingly.
8. Click **Backup Location** tab, select the appropriate option to save the backup file.
9. Click **Save**.
   The Backup Set will be created.

| | |
|---|---|
| NOTE | By default, **Active** option is selected. If **Active** option is not selected, a Backup Set will be created but eScan won't backup data. |

### Edit Backup Set

To edit a Backup Set, follow the steps given below:

1. Select a Backup Set.
2. Click **Edit Backup Set**.
3. After making the necessary changes, click **Save**.
   The Backup Set will be edited and saved.

### Delete Backup Set

To delete a Backup Set, follow the steps given below:

1. Select a Backup Set.
2. Click **Delete Backup Set**.
   A confirmation prompt appears.
3. Click **OK**.
   The Backup Set will be deleted.

# Configuring eScan Policies for Linux and Mac Computers

eScan lets you define settings for Endpoint Security, Administrator password and Schedule update module for Linux and Mac computers connected to the network. Click **Edit** to configure the eScan module settings for computers with respective operating systems.

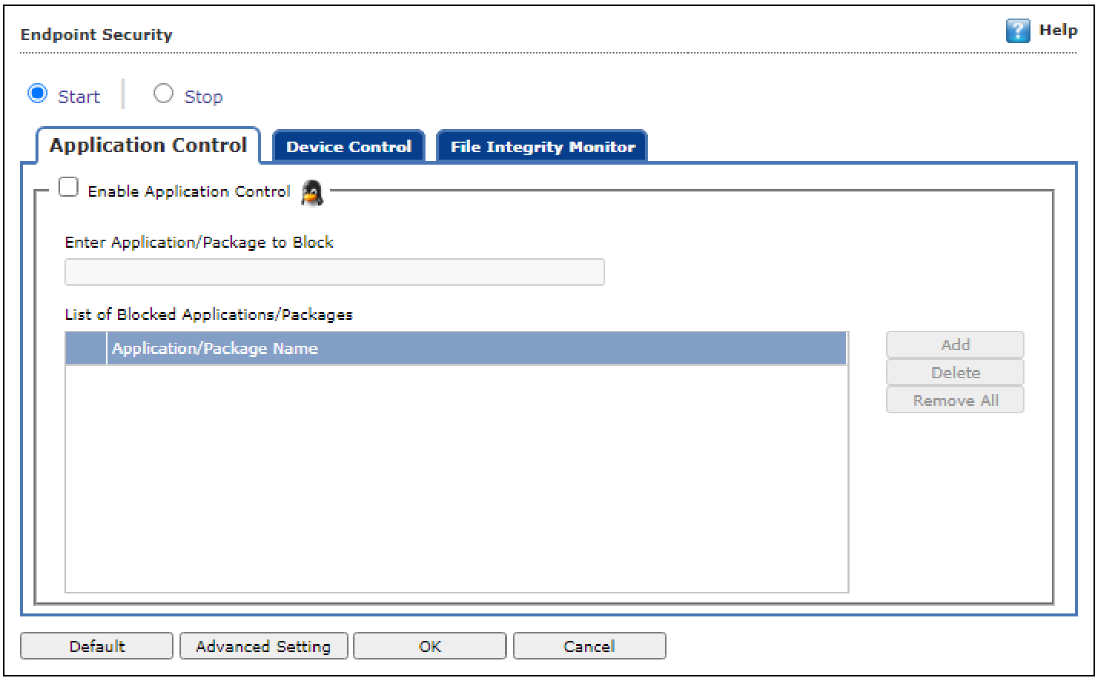
| NOTE | Icons next to every module displays that the settings are valid for the respective operating systems only.<br>It lets you define settings for Scanning; you can also define action to be taken in case of an infection. It also lets you define the number of days for which the logs should be kept as well as create list for Masks, Files or Folders to be excluded from scanning. |
|---|---|

## Endpoint Security

The Endpoint Security module lets you centrally manage all endpoints on your network and closely monitor all USB activities in real-time. With eScan USB control, you can prevent data theft by blocking all except your trusted USB storage devices and stop your files from being taken away on thumb drives, iPod, mp3 players and portable USB hard drives. It allows you to monitor and detect the modifications in the files using File Integrity Monitor feature.

### Application Control

The Application Control tab allows you to block the execution of application or package on Linux computers.



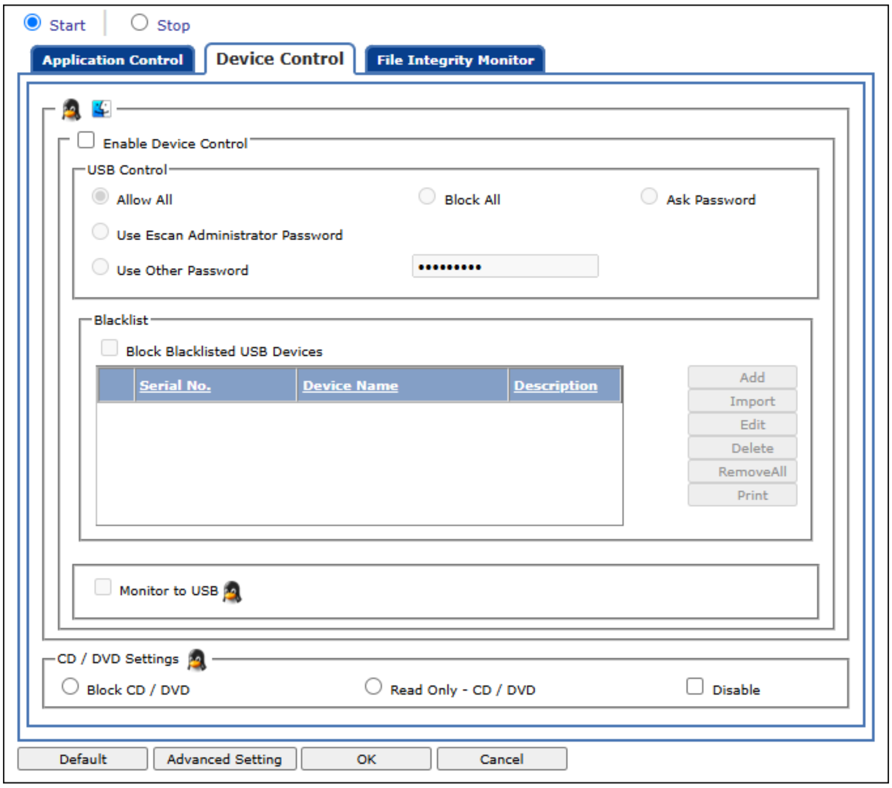
**Start/Stop**: It lets you enable/disable Endpoint Security module. Click the appropriate option.

**Enable Application Control**
Select this checkbox to enable the Application Control feature.

**Enter Application/Package to block**
Enter the application or package name to add them to the list of applications/packages blocked. Click **Add**. The application will be blocked.
To delete the application/package, select the specific app/package name and click **Delete**.
To delete all the application from the list, click **Remove All**.

## Device Control

The Device Control tab helps to allow/block the USB/CD/DVD access on Linux and Mac systems.



**Enable Device Control**
Select this checkbox to configure the Device Control settings.

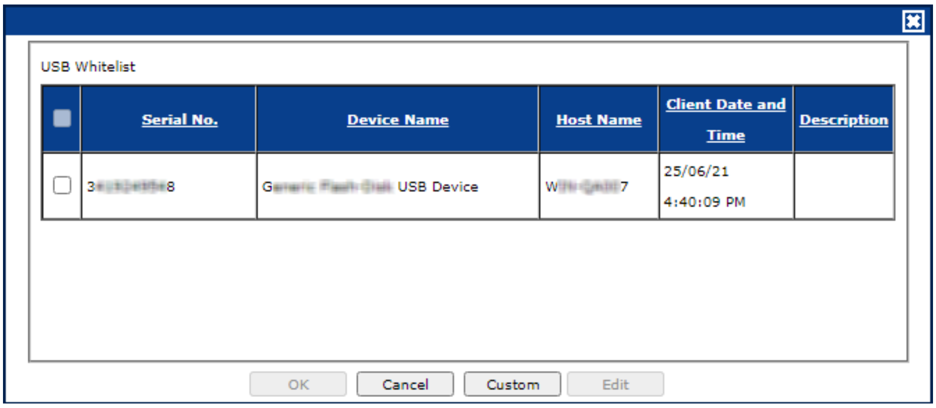
**USB Control**
This option lets you to allow, block, or ask password for the USB device connected to the endpoint. It has following options:

- **Allow All:** Select this option to allow all the connected USB devices.
- **Block All:** Select this option to block all the connected USB devices.
- **Ask Password:** Select this option to set password for the connected USB devices. This will ask password before allowing USB devices to connect to the system. You can either set a password or use the administrator password using options **Use Other Password** and **Use Escan Administrator Password** respectively.

**Blacklist**
This option is enabled when you select **Allow All** option in USB Control section. This option allows you to add USB devices to the Blacklist. Select the **Block Blacklisted USB Devices** checkbox to block all the USB devices from the Blacklist. You can add, delete, and modify using the following options:

- **Add**

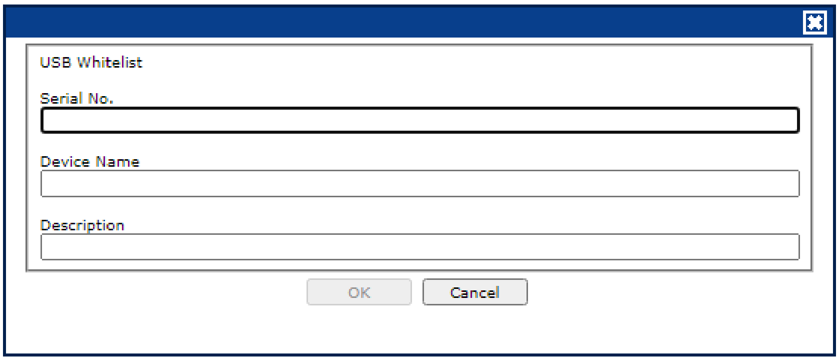
Click **Add** to blacklist the USB devices.
USB Blacklist window appears.



USB Whitelist

| □ | Serial No. | Device Name | Host Name | Client Date and Time | Description |
|---|---|---|---|---|---|
| □ | 3[redacted]8 | [redacted] USB Device | W[redacted]7 | 25/06/21<br>4:40:09 PM | |

- To blacklist the USB device, its details are required. If a USB device is connected to any eScan installed endpoint, the USB details are sent to the server. The administrator will have to manually whitelist the USB device.
- To manually add a USB device in USB Blacklist without connecting to an endpoint, click **Custom**. Enter the USB Details and click **OK**.



USB Whitelist

Serial No.

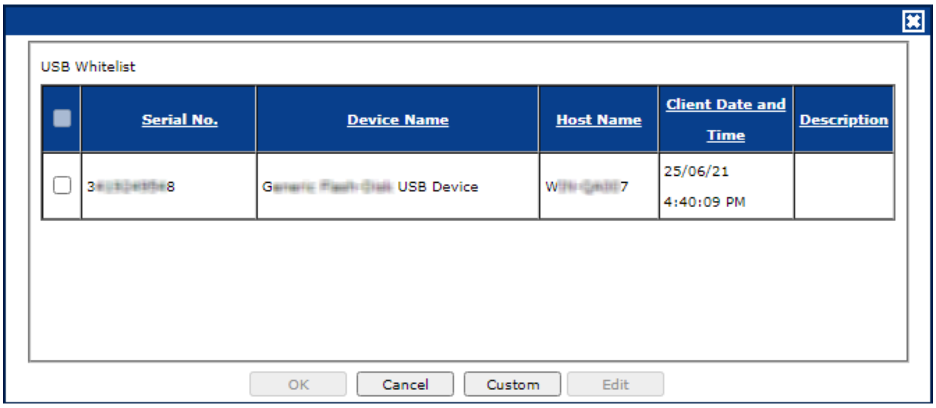
Device Name

Description

- **Edit:** Click **Edit** to edit the details of the USB devices.
- **Delete**: Select the USB device and click **Delete** to remove the device from the list.
- **Remove All**: To remove all the USB devices from the list, click **Remove All**.
- **Print**: This will print all the USB devices in the list along with details for the same.

**Whitelist**
This option is enabled when you select the **Block All** option in the USB Control section. This option lets you add USB devices to the Whitelist. You can add, delete, and modify using the following options:

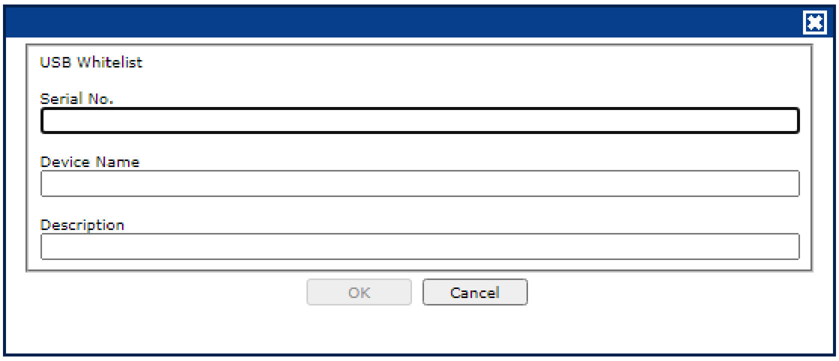
- **Add**
  Click **Add** to whitelist USB devices.
  USB Whitelist window appears.



USB Whitelist

| ☐ | Serial No. | Device Name | Host Name | Client Date and Time | Description |
|---|---|---|---|---|---|
| ☐ | 3[redacted]8 | [redacted] USB Device | W[redacted]7 | 25/06/21<br>4:40:09 PM | |

- To whitelist the USB device, its details are required. If a USB device is connected to any eScan installed endpoint, the USB details are sent to the server. The administrator will have to manually whitelist the USB device.
- To manually add a USB device in USB Whitelist without connecting to an endpoint, click **Custom**. Enter the USB Details and click **OK**.



USB Whitelist

Serial No.

Device Name

Description

- **Edit:** Click **Edit** to edit the details of the USB devices.
- **Delete**: Select the USB device and click **Delete** to remove the device from the list.
- **Remove All**: To remove all the USB devices from the list, click **Remove All**.
- **Print**: This will print all the USB devices in the list along with details for the same.

**Monitor to USB**

Select this checkbox to monitor all the connected USB devices to the endpoints.

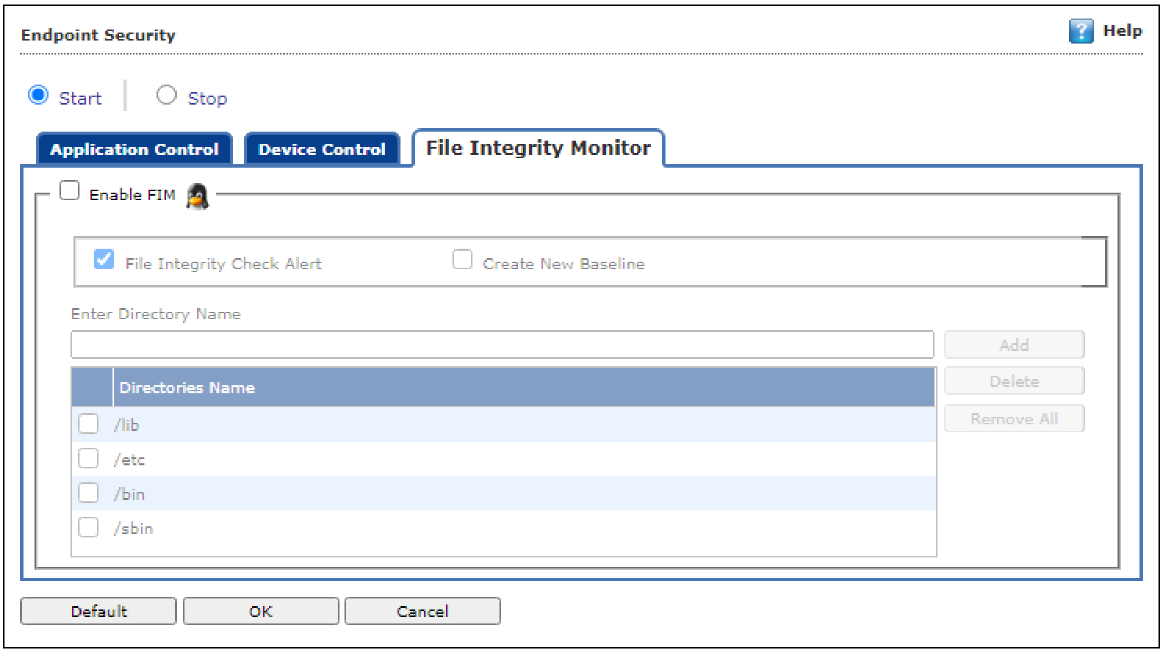
**CD/DVD Settings**

This option lets administrator to block, allow, and disable the CD/DVD. You have following options to configure:

- **Block CD/DVD:** This option blocks all the CD and DVD.
- **Read Only CD/DVD:** This option allows the user to only read the content on CD and DVD.
- **Disable:** This option disables all the CD and DVD.

## File Integrity Monitor

Cybercriminals are using malware and advanced methods to compromise the important system files, folders, registries, and data in order to conduct cyber attacks. The File Integrity Monitor features monitors and detects the changes in the any object of the Linux systems.



Endpoint Security

● Start | ○ Stop

Application Control | Device Control | File Integrity Monitor

□ Enable FIM

☑ File Integrity Check Alert □ Create New Baseline

Enter Directory Name

| | Directories Name |
|---|---|
| □ | /lib |
| □ | /etc |
| □ | /bin |
| □ | /sbin |

### Enable FIM

Select this checkbox to enable the File Integrity Monitoring.

- **File Integrity Check Alert [Default]**: This checkbox will check the file integrity and alert the admin accordingly.
- **Create New Baseline**: This checkbox will create a baseline for the selected directories and the FIM will begin monitoring changes for the selected directories.

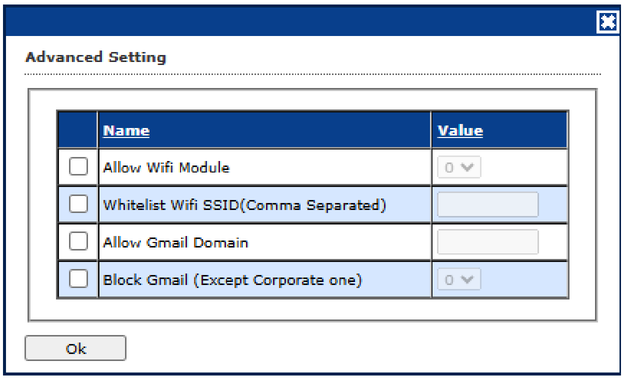
### Enter Directory Name

Enter the directory name to add it to the integrity monitoring. You can also select the directory name from the pre-defined list in the below table to add them to monitoring.

To delete a specific directory from monitoring, select the directory, and click **Delete**.
To remove all the directory from monitoring, click **Remove All**.

| NOTE | Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings. |
|---|---|

## Advanced Settings



Advanced Setting

| | Name | Value |
|---|---|---|
| □ | Allow Wifi Module | 0 |
| □ | Whitelist Wifi SSID(Comma Separated) | |
| □ | Allow Gmail Domain | |
| □ | Block Gmail (Except Corporate one) | 0 |

**Allow Wifi Module (1 = Enable/0= Disable)**
Select this option to enable/disable wifi module.

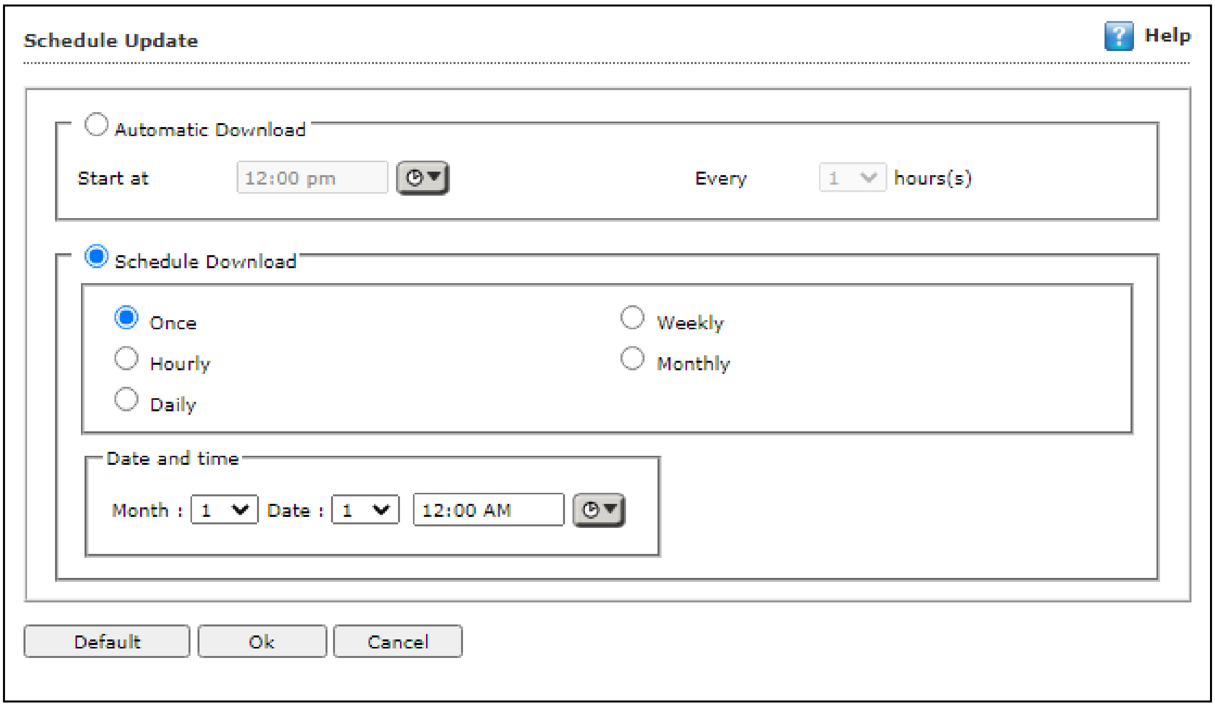
**Whitelist Wifi SSID (1 = Enable/0= Disable)**
Select this to enable/disable whitelisting wifi SSID.

**Allow Gmail Domain (1 = Enable/0= Disable)**
Select this option to enable/disable gmail domain.

**Block Gmail (Except Corporate one)**
Select this option to block gmail account.

## Schedule Update

This module lets you schedule the updates for Linux computers.



Schedule Update

○ Automatic Download

Start at 12:00 pm — Every 1 hours(s)

● Schedule Download

● Once ○ Weekly
○ Hourly ○ Monthly
○ Daily

Date and time

Month : 1 Date : 1 12:00 AM

The updates can be downloaded automatically with **Automatic Download** option.

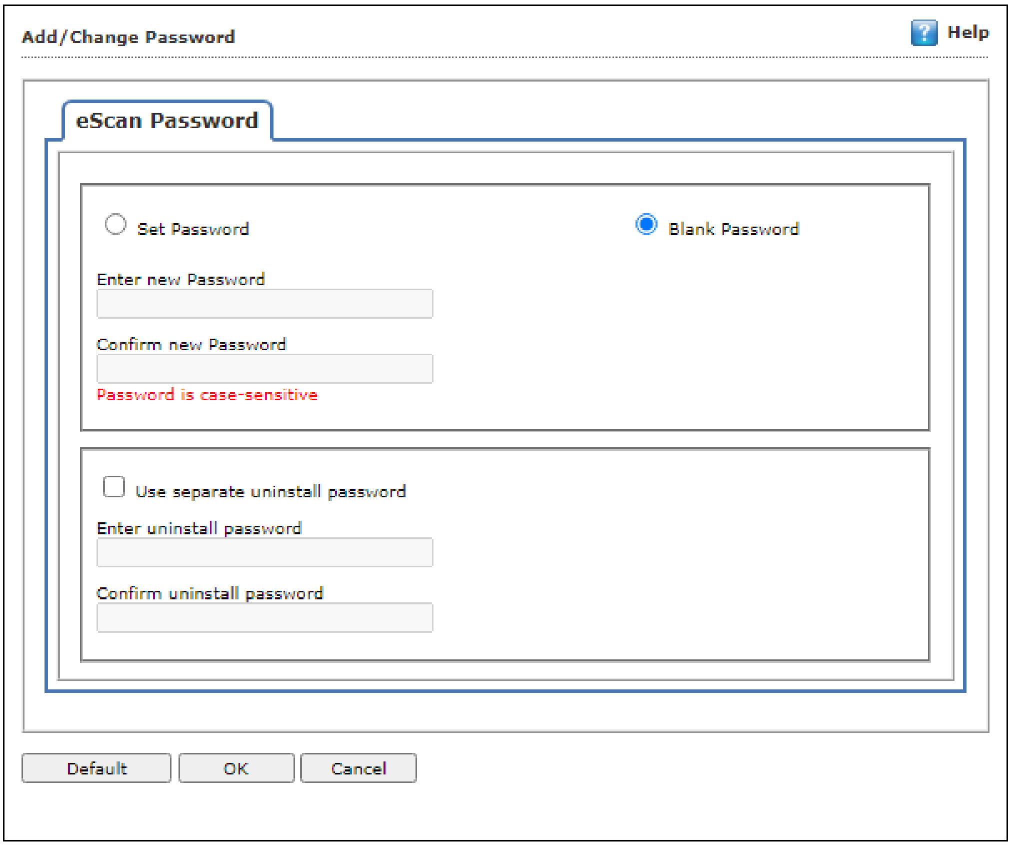
OR

The updates can be downloaded on a schedule basis with **Schedule Download** option. Select intervals and time basis as per your preferences.

| | |
|---|---|
| **NOTE** | Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings. |

# Administrator Password

Administrator Password lets you create and change password for administrative login of eScan protection center for Linux computers. It also lets you keep the password as blank, wherein you can login to eScan protection center without entering any password. It also lets you define uninstallation password which will be required before uninstalling eScan Client from managed computers manually. The user will not be able to uninstall eScan Client without entering uninstallation password.



Add/Change Password

○ Set Password ● Blank Password

Enter new Password

Confirm new Password

Password is case-sensitive

□ Use separate uninstall password

Enter uninstall password

Confirm uninstall password

**Set Password**
Click this option, if you want to set password.

**Blank Password**
Click this option, if you do not want to set any password for login.
When you click this option, the **Enter new Password** and **Confirm new Password** fields become unavailable.

**Enter new Password**
Enter the new password.

**Confirm new Password**
Re-enter the new password for confirmation.

**Use separate uninstall password**
Click this option, if you want to set password before uninstallation of eScan Client.

**Enter uninstall Password**
Enter the uninstallation password.

**Confirm uninstall Password**
Re-enter the uninstallation password for confirmation.

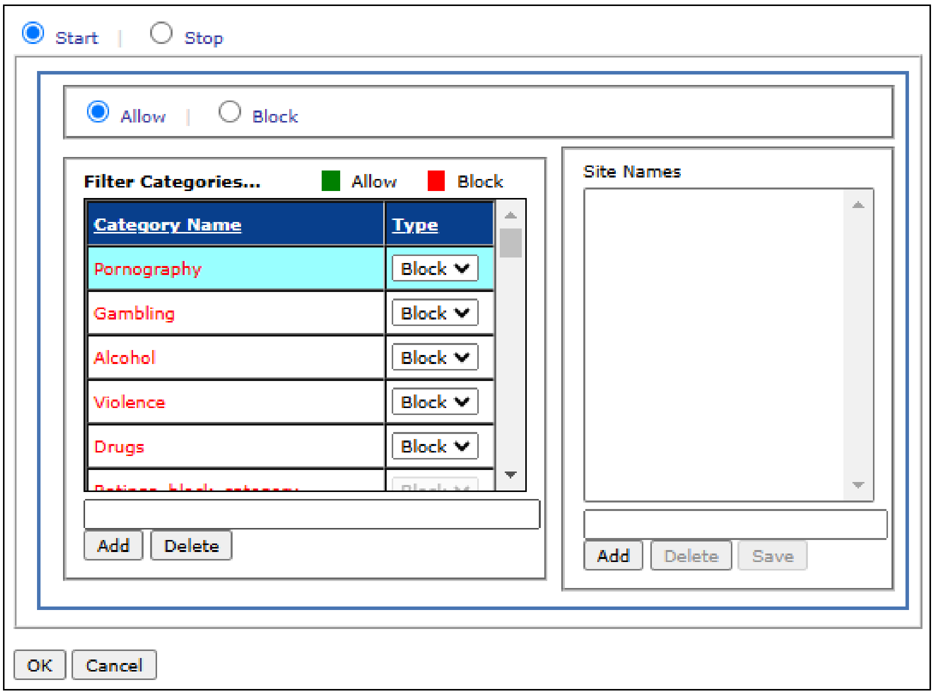
After filling all fields, click **OK**.
The Password will be saved.

| NOTE | Click **Default** to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings. |
|---|---|

# Web Protection

Web Protection module lets you block websites containing pornographic or offensive material for Linux computers. This feature is extremely beneficial to parents because it prevents kids from accessing websites containing harmful or restricted content. Administrators can also use this feature to prevent employees from accessing non-work-related websites during work hours. You can configure the following settings:

**Start/Stop**
It lets you enable/disable **Web-Protection** module. Click the appropriate option.



● Start | ○ Stop

● Allow | ○ Block

Filter Categories... 🟩 Allow 🟥 Block

| Category Name | Type |
|---|---|
| Pornography | Block |
| Gambling | Block |
| Alcohol | Block |
| Violence | Block |
| Drugs | Block |

You can configure the following settings.

## Filtering Options

This tab has predefined categories that help you control access to the Internet.

**Status**
This section lets you allow or block access to specific websites based on Filter Categories. You can set the status as **Active** or **Block** web access. Select the **Block Web Access** option if you want to block all the websites except the ones that have been listed in the **Filter Categories**. When you select this option, only **Filtering Options** and **Pop-up Filter** tabs are available.

**Filter Categories**

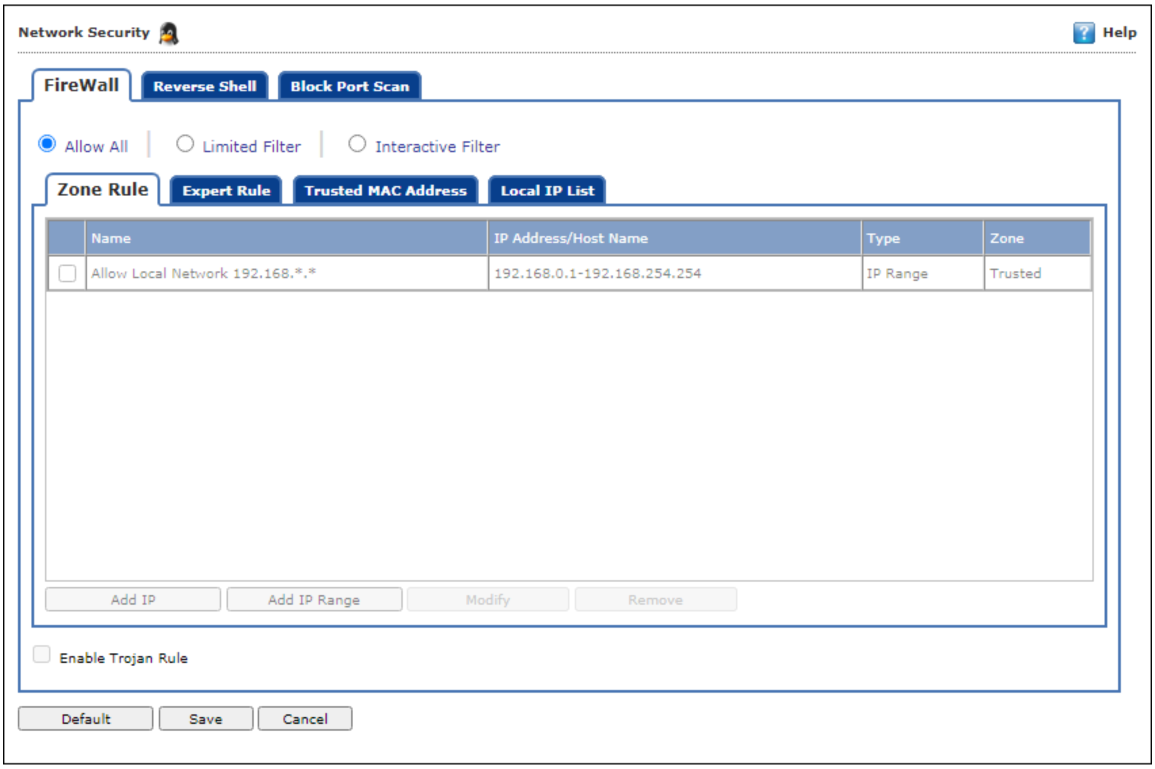
This section uses the following color codes for allowed and blocked websites.

- **Green**: It represents an allowed websites category.
- **Red**: It represents a blocked websites category.
  The filter categories used in this section include categories like Pornography, Gambling, Chat, Alcohol, Violence, Drugs, Ratings block category, Websites Allowed, etc. You can also add or delete filter categories depending on your requirement.

**Category Name**
This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category. You can also add or delete filter categories depending on your requirement.

## Network Security

Network Security module helps to set Firewall configuration to monitor all incoming and outgoing network traffic and protect your computer from all types of network based attacks. It also prevents the Reverse Shell Exploits and blocks the Port Scan. Enabling this feature will prevent the Zero-day attacks and all other cyber threats.



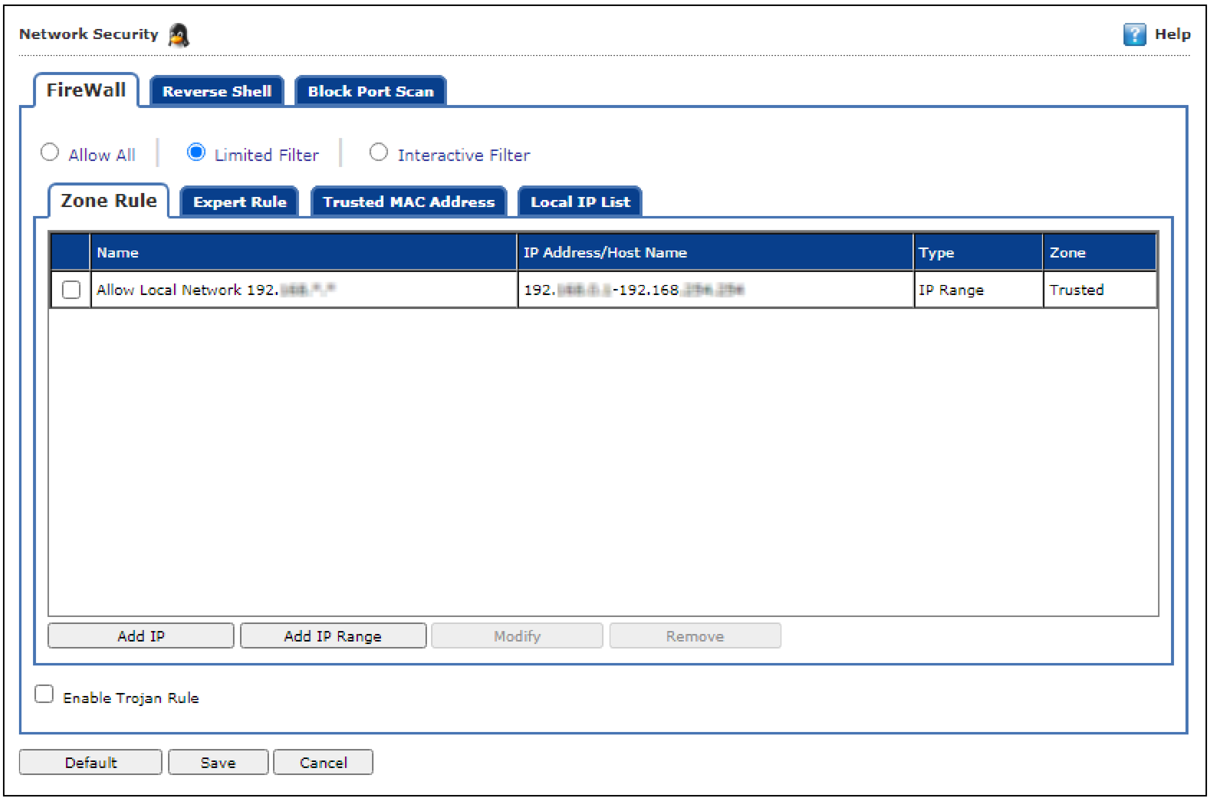
● Allow All ○ Limited Filter ○ Interactive Filter

| | Name | IP Address/Host Name | Type | Zone |
|---|---|---|---|---|
| □ | Allow Local Network 192.168.*.* | 192.168.0.1-192.168.254.254 | IP Range | Trusted |

□ Enable Trojan Rule

## Firewall

This tab is designed to monitor all incoming and outgoing network traffic and protect your endpoint from all types of network based attacks. eScan includes a set of predefined access control rules that you can remove or customize as per your requirements. These rules enforce a boundary between your computer and the network. These rules include Zone Rules, Expert Rules, Trusted Media Access Control (MAC) Address, and Local IP list.



○ Allow All | ● Limited Filter | ○ Interactive Filter

| | Name | IP Address/Host Name | Type | Zone |
|---|---|---|---|---|
| ☐ | Allow Local Network 192.[redacted] | 192.[redacted]-192.168.[redacted] | IP Range | Trusted |

☐ Enable Trojan Rule

You can configure the following settings to be deployed to the eScan client systems.
**Allow All** – Clicking **Allow All** disables the eScan Firewall i.e. all the incoming and outgoing network traffic will not be monitored/filtered.

**Limited Filter** – Clicking **Limited Filter** enables eScan Firewall in limited mode which will monitor all incoming traffic only and will be allowed or blocked as per the conditions or rules defined in the Firewall.

**Interactive** – Clicking **Interactive** enables eScan Firewall to monitor all the incoming and outgoing network traffic and will be allowed or blocked as per the conditions or rules defined in the Firewall.

Following tabs are available:

- **Zone Rule**
- **Expert Rule**
- **Trusted MAC Address**
- **Local IP List**

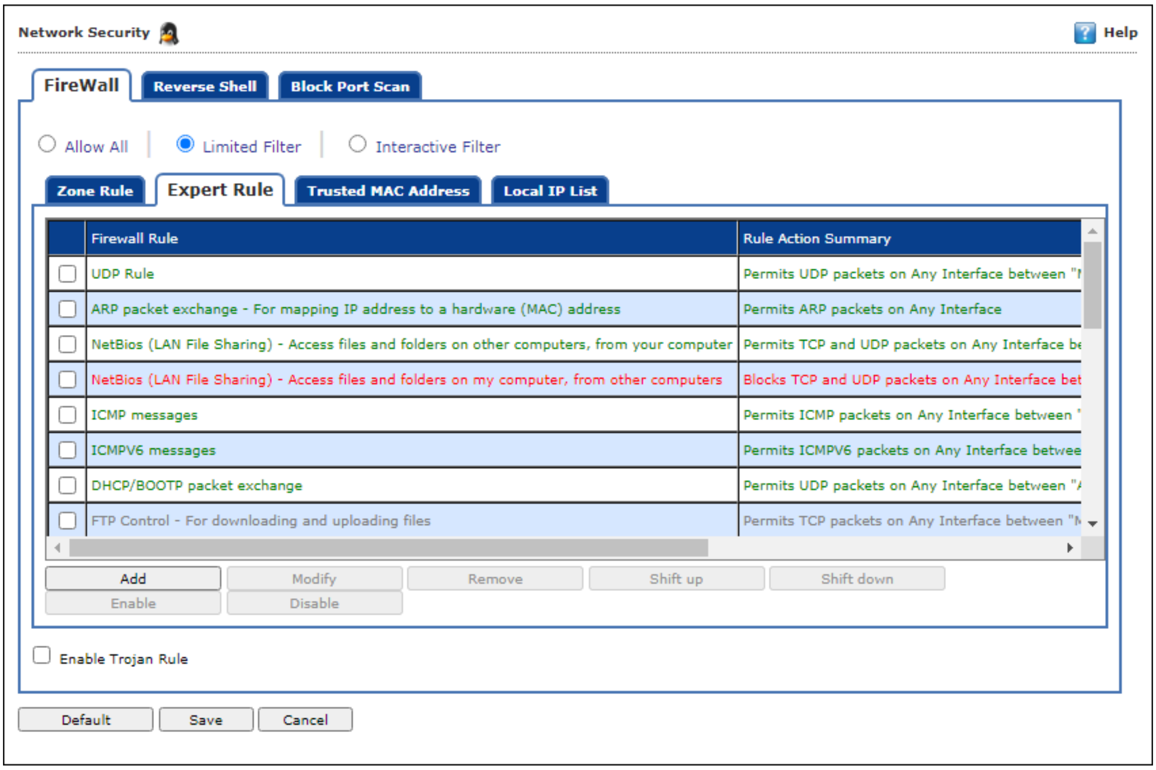
## Zone Rule

This is a set of network access rules to make the decision of allowing/blocking of the access to the system. This will contain the source IP address or source Host name or IP range either to be allowed or blocked. The following buttons are available for configuring zone rule:

- **Add IP** – This option lets you add an IP address of a system to be added in the zone rule. After clicking **Add IP**, enter the IP address of the system, select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the Zone Rule.
- **Add IP Range** – This option lets you add an IP range to be added in the zone rule. After clicking **Add IP Range**, add the IP Range (i.e. a range of IP that the zone rules should be applied), select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the zone rule.
- **Modify –** To modify/change any listed zone rule(s), select the zone rule to be modified and then click **Modify**.
- **Remove -** To remove any listed zone rule(s), select the zone rule and then click **Remove**.

## Expert Rule

This tab lets you specify advanced rules and settings for the eScan firewall. You can configure expert rules on the basis of the various rules, protocols, source IP address and port, destination IP address and port, and ICMP types. You can create new expert rules.



○ Allow All | ● Limited Filter | ○ Interactive Filter

| | Firewall Rule | Rule Action Summary |
|---|---|---|
| □ | UDP Rule | Permits UDP packets on Any Interface between "I |
| □ | ARP packet exchange - For mapping IP address to a hardware (MAC) address | Permits ARP packets on Any Interface |
| □ | NetBios (LAN File Sharing) - Access files and folders on other computers, from your computer | Permits TCP and UDP packets on Any Interface be |
| □ | NetBios (LAN File Sharing) - Access files and folders on my computer, from other computers | Blocks TCP and UDP packets on Any Interface bet |
| □ | ICMP messages | Permits ICMP packets on Any Interface between " |
| □ | ICMPV6 messages | Permits ICMPV6 packets on Any Interface betwee |
| □ | DHCP/BOOTP packet exchange | Permits UDP packets on Any Interface between "A |
| □ | FTP Control - For downloading and uploading files | Permits TCP packets on Any Interface between "N |

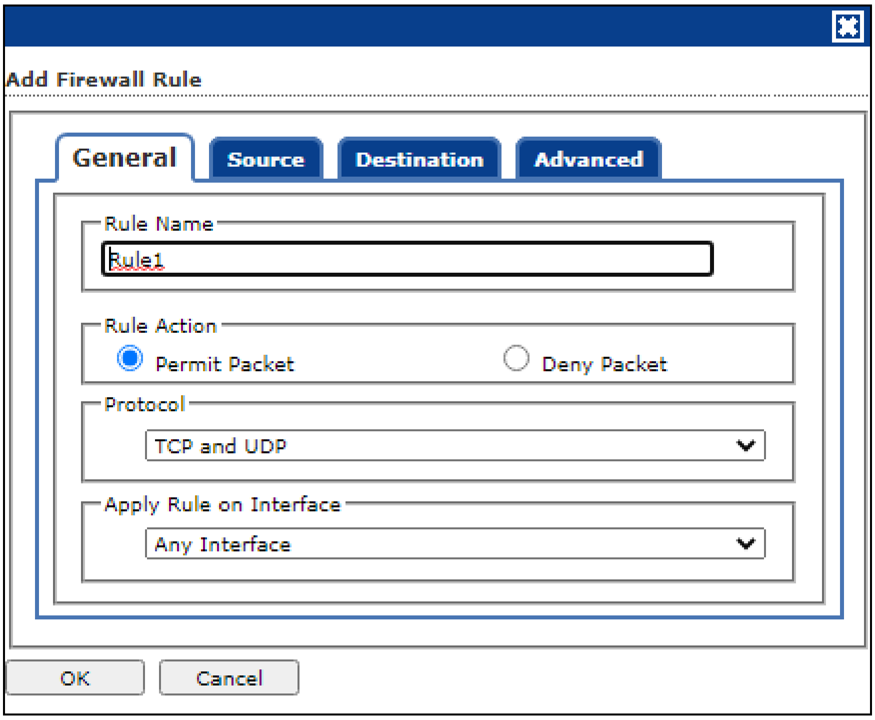
□ Enable Trojan Rule

However, configure these rules only if you are familiar with firewalls and networking protocols.

- Source IP Address/Host Name
- Source Port Number
- Destination IP Address/Host Name
- Destination Port Number

The following buttons are available to configure an Expert Rule:

1. **Add** – Click **Add** to create a new Expert Rule. In the Add Firewall Rule Window:



Add Firewall Rule

General | Source | Destination | Advanced

Rule Name: Rule1

Rule Action: ● Permit Packet ○ Deny Packet

Protocol: TCP and UDP

Apply Rule on Interface: Any Interface

**General tab**

In this section, specify the Rule settings:

**Rule Name –** Provide a name to the Rule.

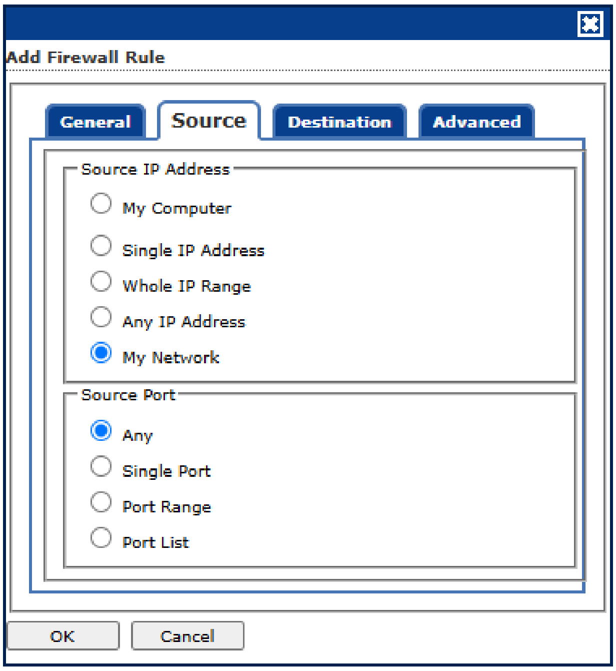
**Rule Action –** Action to be taken, whether to Permit Packet or Deny Packet.

**Protocol –** Select the network protocol (e.g. TCP, UDP, ARP) on which the Rule will be applied.

**Apply rule on Interface –** Select the Network Interface on which the Rule will be applied.

### Source tab

In this section, specify/select the location from where the outgoing network traffic originates.



Add Firewall Rule

Source IP Address

○ My Computer
○ Single IP Address
○ Whole IP Range
○ Any IP Address
● My Network

Source Port

● Any
○ Single Port
○ Port Range
○ Port List

### Source IP Address:

**My Computer –** The rule will be applied for the outgoing traffic originating from your computer.

**Single IP Address –** The rule will be applied for the outgoing traffic originating from the computer as per the IP address specified.

**Whole IP Range –** To enable the rule on a group of computers in series, you can specify a range of IP address. The rule will be applied for the outgoing traffic from the computer(s) which is within the defined IP range.

**Any IP Address –** When this option is selected, the rule will be applied for the traffic originating from ANY IP address.

**My Network –** The rule will be applied for the outgoing traffic to the networked computer(s).

### Source Port:

**Any –** When this option is selected, the rule gets applied for outgoing traffic originating from any port.

**Single Port –** When this option is selected, the rule gets applied for the outgoing traffic originating from the specified/defined port.

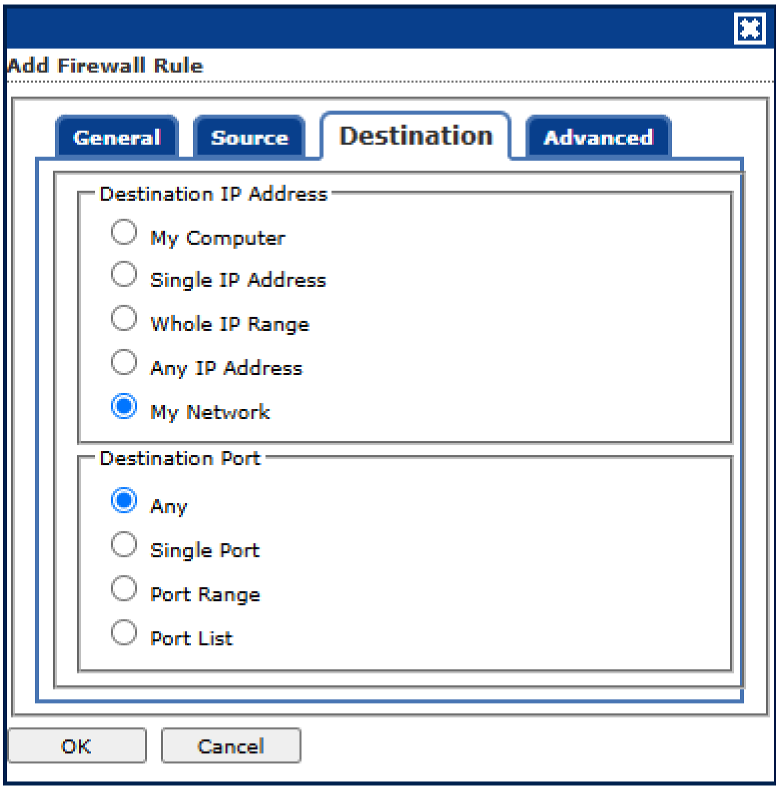
**Port Range –** To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the outgoing traffic originating from the port which is within the defined range of ports.

**Port List –** A list of ports can be specified. The rule will be applied for the outgoing traffic originating from the ports as per specified in the list.

| | |
|---|---|
| **NOTE** | The rule will be applied when the selected Source IP Address and Source Port matches together. |

**Destination tab**

In this section, specify/select the location of the computer where the incoming network traffic is destined.



Add Firewall Rule

Destination IP Address
○ My Computer
○ Single IP Address
○ Whole IP Range
○ Any IP Address
● My Network

Destination Port
● Any
○ Single Port
○ Port Range
○ Port List

## Destination IP Address:

**My Computer –** The rule will be applied for the incoming traffic to your computer.

**Single IP Address –** The rule will be applied for the incoming traffic to the computer as per the IP address specified.

**Whole IP Range –** To apply the rule on a group of computers in series, you can specify a range of IP address. The rule will be applied for the incoming traffic to the computer(s) which is within the defined IP range.

**Any IP Address –** When this option is selected, the rule will be applied for the incoming traffic to ANY IP Addresses.

**My Network –** The rule will be applied for the outgoing traffic to the networked computer(s).

## Destination IP Port:

**Any –** After selecting this option, the rule will be applied for the incoming traffic to ANY port.

**Single Port –** After selecting this option, the rule will be applied for the incoming traffic to the specified/defined port.

**Port Range –** To enable the rule on a group of ports in series, you can specify a range of ports.

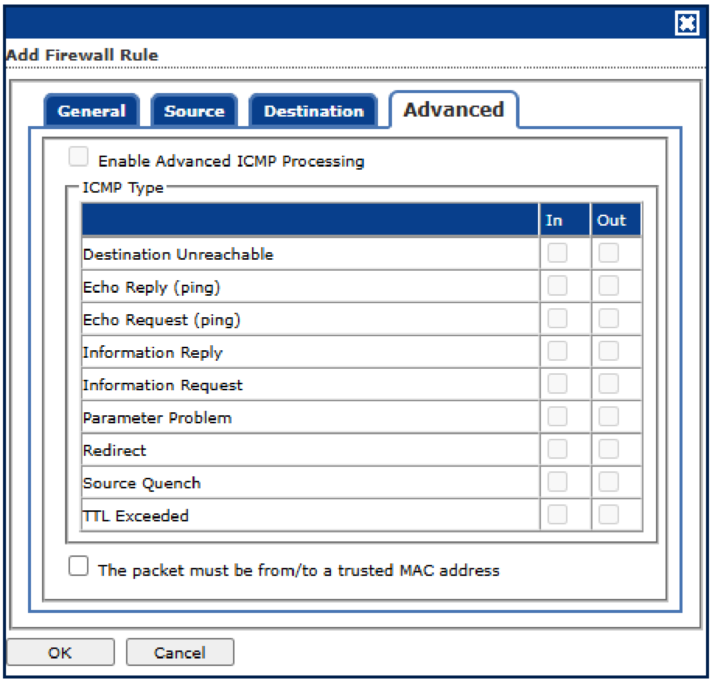
**Port List –** A list of port can be specified or added. The rule will be applied for incoming traffic originating from the ports as per specified in the list.

| ! | The rule will be applied when the selected Destination IP Address and Destination Port |
|---|---|

| | |
|---|---|
| **NOTE** | matches together. |

**Advanced tab**

This tab contains advance setting for Expert Rule.



Add Firewall Rule

□ Enable Advanced ICMP Processing

ICMP Type

| | In | Out |
|---|---|---|
| Destination Unreachable | □ | □ |
| Echo Reply (ping) | □ | □ |
| Echo Request (ping) | □ | □ |
| Information Reply | □ | □ |
| Information Request | □ | □ |
| Parameter Problem | □ | □ |
| Redirect | □ | □ |
| Source Quench | □ | □ |
| TTL Exceeded | □ | □ |

□ The packet must be from/to a trusted MAC address

**Enable Advanced ICMP Processing -** This is activated when the ICMP protocol is selected in the General tab.

**The packet must be from/to a trusted MAC address –** When this option is selected, the rule will only be applied on the MAC address defined/listed in the Trusted MAC Address tab.

Use the following buttons in this tab as and when required:

**Modify** – Clicking **Modify** lets you modify any Expert Rule.

**Remove** – Clicking **Remove** lets you delete a rule from the Expert Rule.

**Shift Up and Shift Down**– The UP and DOWN arrow button will enable to move the rules up or down as required and will take precedence over the rule listed below it.

**Enable Rule/Disable Rule** – These buttons lets you enable or disable a particular selected rule from the list.

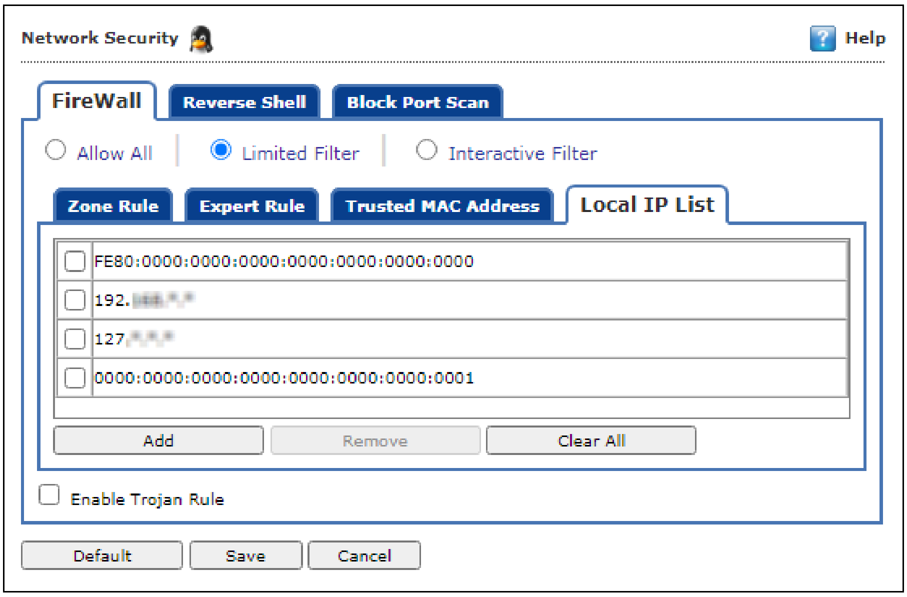
## Trusted MAC Address

This section contains the information of the MAC address of the system. A MAC address is a hardware address that uniquely identifies each node of a network. The Trusted MAC address list will be checked along with the Expert Rule only when "The packet must be from/to a trusted MAC address" option is checked and the action will be as per specified in the rule. (Refer to the *Advance Tab* of the Expert Rule). The following buttons are available to configure the Trusted Mac Address:

- **Add –** To add a MAC address click on this button. Enter the MAC address to be added in the list for e.g. 00-13-[redacted]
- **Edit –** To modify/change the MAC Address, click **Edit**.
- **Remove –** To delete the MAC Address, click **Remove**.
- **Clear All –** To delete the entire listed MAC Address, click **Clear All**.

## Local IP List

This section contains a list of Local IP addresses.



Network Security
Help

FireWall | Reverse Shell | Block Port Scan

○ Allow All | ● Limited Filter | ○ Interactive Filter

Zone Rule | Expert Rule | Trusted MAC Address | Local IP List

□ FE80:0000:0000:0000:0000:0000:0000:0000
□ 192.[redacted]
□ 127.[redacted]
□ 0000:0000:0000:0000:0000:0000:0000:0001

Add | Remove | Clear All

□ Enable Trojan Rule

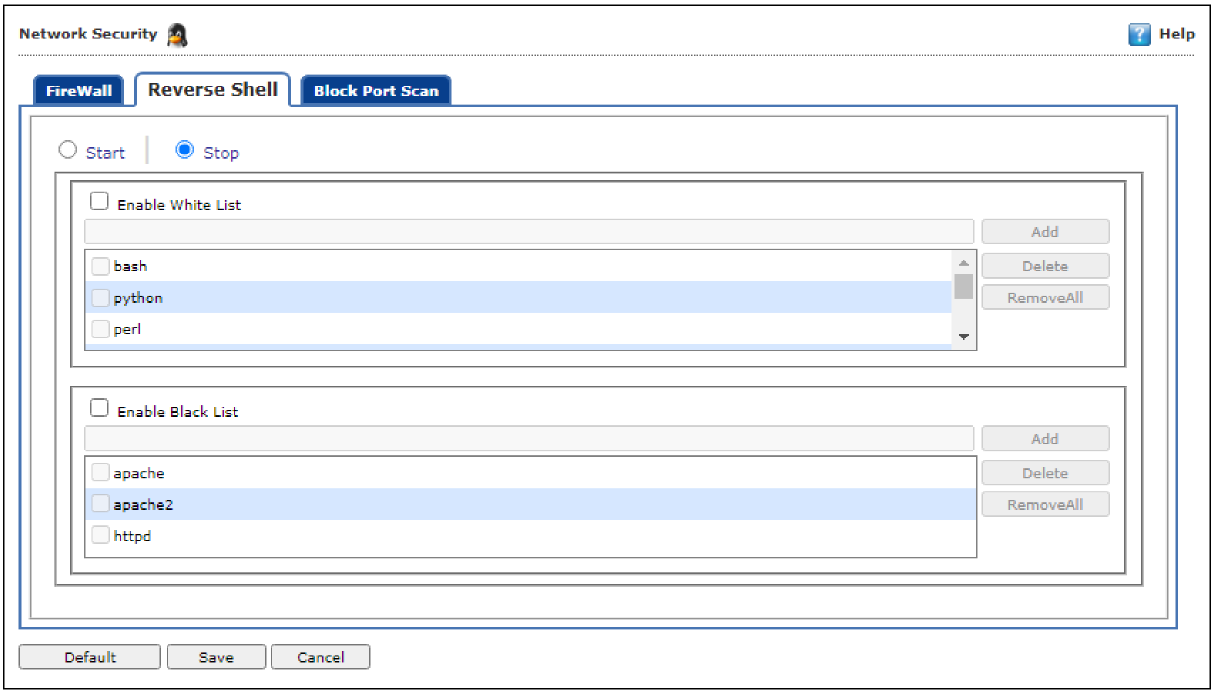
Default | Save | Cancel

**Add –** To add a local IP address, click **Add**.
**Remove –** To remove a local IP address, click **Remove**.
**Clear All –** To clear all local IP addresses, click **Clear All**.

**Enable Trojan Rule**
Select this checkbox, to enable the Trojan Rule.

## Reverse Shell

This tab allows you to block the reverse shell attacks by blocking the script languages that the attackers use to initiate remote shell connection with the networked endpoint.



○ Start | ● Stop

☐ Enable White List

☐ bash
☐ python
☐ perl

☐ Enable Black List

☐ apache
☐ apache2
☐ httpd

### Start/Stop

It allows you enable/disable **Network Security** module.

After enabling this, you can configure the following settings:

### Enable White List

Select this checkbox to whitelist the trusted script languages, such as Bash, Python, Perl, and more. You can add and delete the script languages from whitelisting.

- **Add**: To add a script language, select the language and click **Add**.
- **Delete**: To delete a script language, select a language and click **Delete**.
- **Remove All**: To remove all the whitelisted script language, click **Remove All**.

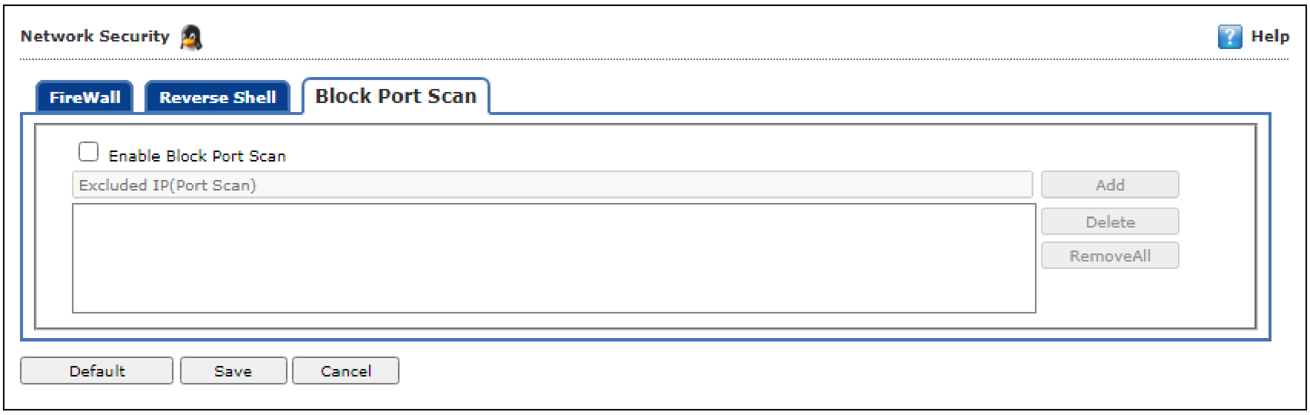
### Enable Black List

Select this checkbox to blacklist the untrusted and risky script languages.

- **Add**: To add a script language, select the language and click **Add**.
- **Delete**: To delete a script language, select a language and click **Delete**.
- **Remove All**: To remove all the blacklisted script language, click **Remove All**.

## Block Port Scan

This tab allows admin to configure the port scan option.



### Enable Block Port Scan

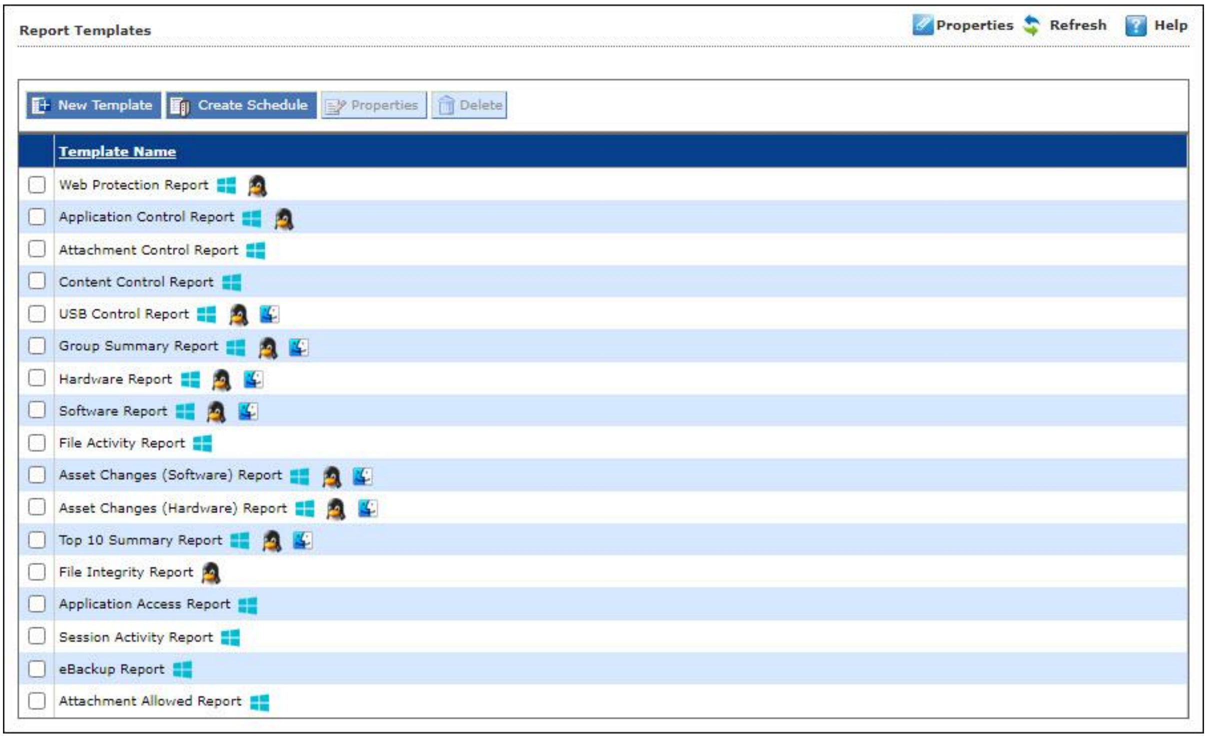
Select this checkbox to enable the port scan option. You can add and delete the IP addresses that need to exclude from the port scan.

- **Add**: To add an IP, enter the IP address and click **Add**.
- **Delete**: To delete an IP, select the IP address and click **Delete**.
- **Remove All**: To remove all the excluded IP addresses, click **Remove All**.

The Policy Template gets saved.

# Report Templates

The Report Templates module lets you create template and schedule them according to your preferences. The module also consists of pre-loaded templates according to which the report can be created and scheduled.



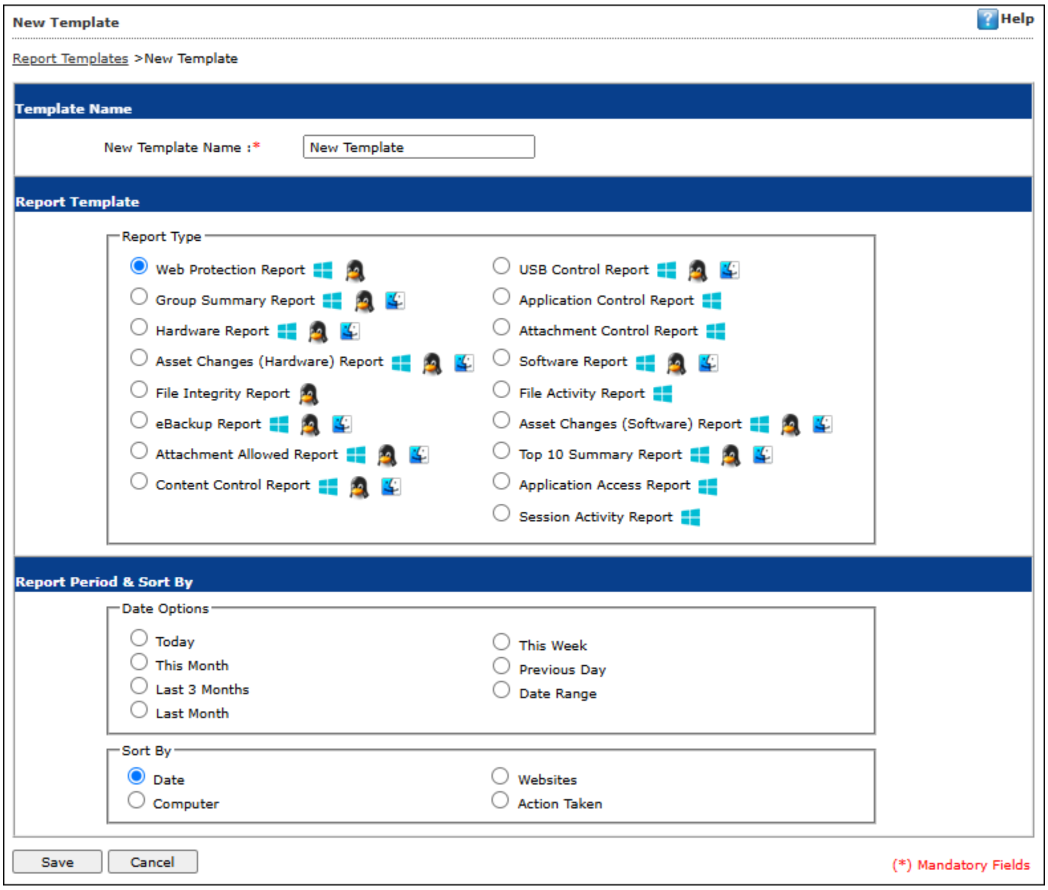
Report Templates

| | Template Name |
|---|---|
| ☐ | Web Protection Report ⊞ 🐧 |
| ☐ | Application Control Report ⊞ 🐧 |
| ☐ | Attachment Control Report ⊞ |
| ☐ | Content Control Report ⊞ |
| ☐ | USB Control Report ⊞ 🐧 🍎 |
| ☐ | Group Summary Report ⊞ 🐧 🍎 |
| ☐ | Hardware Report ⊞ 🐧 🍎 |
| ☐ | Software Report ⊞ 🐧 🍎 |
| ☐ | File Activity Report ⊞ |
| ☐ | Asset Changes (Software) Report ⊞ 🐧 🍎 |
| ☐ | Asset Changes (Hardware) Report ⊞ 🐧 🍎 |
| ☐ | Top 10 Summary Report ⊞ 🐧 🍎 |
| ☐ | File Integrity Report 🐧 |
| ☐ | Application Access Report ⊞ |
| ☐ | Session Activity Report ⊞ |
| ☐ | eBackup Report ⊞ |
| ☐ | Attachment Allowed Report ⊞ |

# Creating a Report Template

To create a Report Template, follow the steps given below:

1. In the navigation panel, click **Report Templates**.
2. Click **New Template**.
   New Template screen appears.



New Template — Help

Report Templates >New Template

**Template Name**

New Template Name :* New Template

**Report Template**

Report Type

| | |
|---|---|
| ● Web Protection Report | ○ USB Control Report |
| ○ Group Summary Report | ○ Application Control Report |
| ○ Hardware Report | ○ Attachment Control Report |
| ○ Asset Changes (Hardware) Report | ○ Software Report |
| ○ File Integrity Report | ○ File Activity Report |
| ○ eBackup Report | ○ Asset Changes (Software) Report |
| ○ Attachment Allowed Report | ○ Top 10 Summary Report |
| ○ Content Control Report | ○ Application Access Report |
| | ○ Session Activity Report |

**Report Period & Sort By**

Date Options

| | |
|---|---|
| ○ Today | ○ This Week |
| ○ This Month | ○ Previous Day |
| ○ Last 3 Months | ○ Date Range |
| ○ Last Month | |

Sort By

| | |
|---|---|
| ● Date | ○ Websites |
| ○ Computer | ○ Action Taken |

(*) Mandatory Fields

3. Enter a name for report template.
4. Select a **Report Type**.
   Depending upon the report type, the additional setting varies.
5. After making the necessary selections/filling data, click **Save**.
   The template will be created according to your preferences.

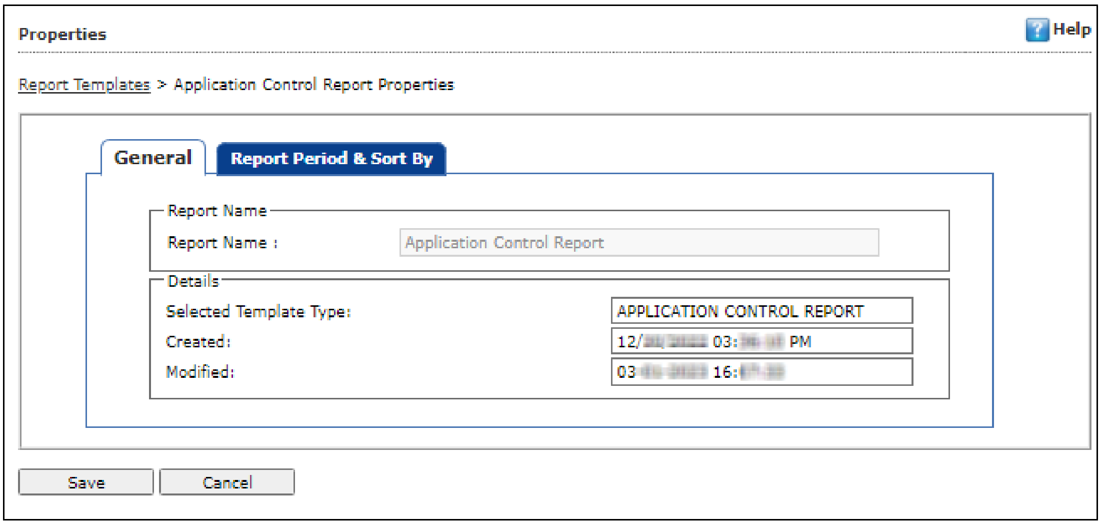
# Creating Schedule for a Report Template

The Report Template module lets you create a new schedule for the report templates. To learn more, click here.

# Viewing Properties of a Report Template

To view the properties of Report Template, follow the steps given below:

1. Select the Report Template whose properties you want to view.
2. Click **Properties**.
   Properties screen appears.



Properties

Report Templates > Application Control Report Properties

Report Name

Report Name : Application Control Report

Details

Selected Template Type: APPLICATION CONTROL REPORT

Created: 12/[redacted] 03:[redacted] PM

Modified: 03[redacted] 16:[redacted]

| NOTE | Depending upon the Report Template enter, the Properties varies. |
|---|---|

3. After making the necessary changes, click **Save**.
   The Report Template's properties will be updated.

# Deleting a Report Template

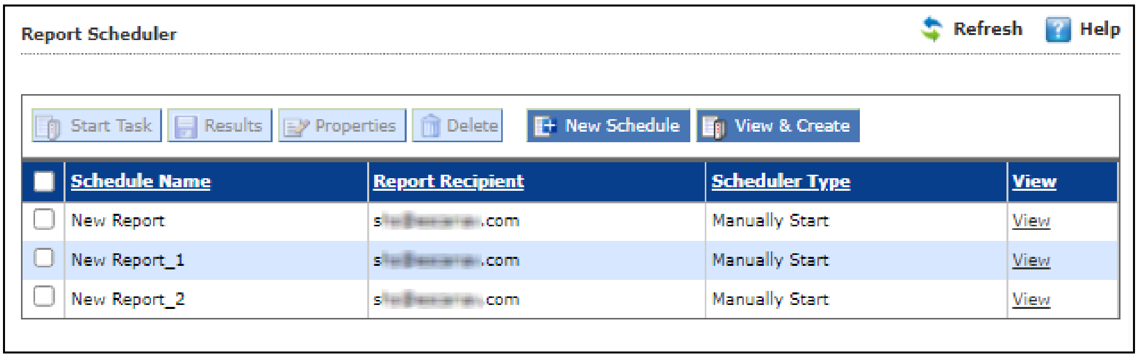
To delete a Report Template, follow the steps given below:

1. Select the template you want to delete.
2. Click **Delete**.
   A confirmation prompt appears.
3. Click **OK**.
   The Report Template will be deleted.

| NOTE | Default Report Templates cannot be deleted. |
|---|---|

# Report Scheduler

The Report Scheduler module lets you create schedule, update and run the task according to your preferences.



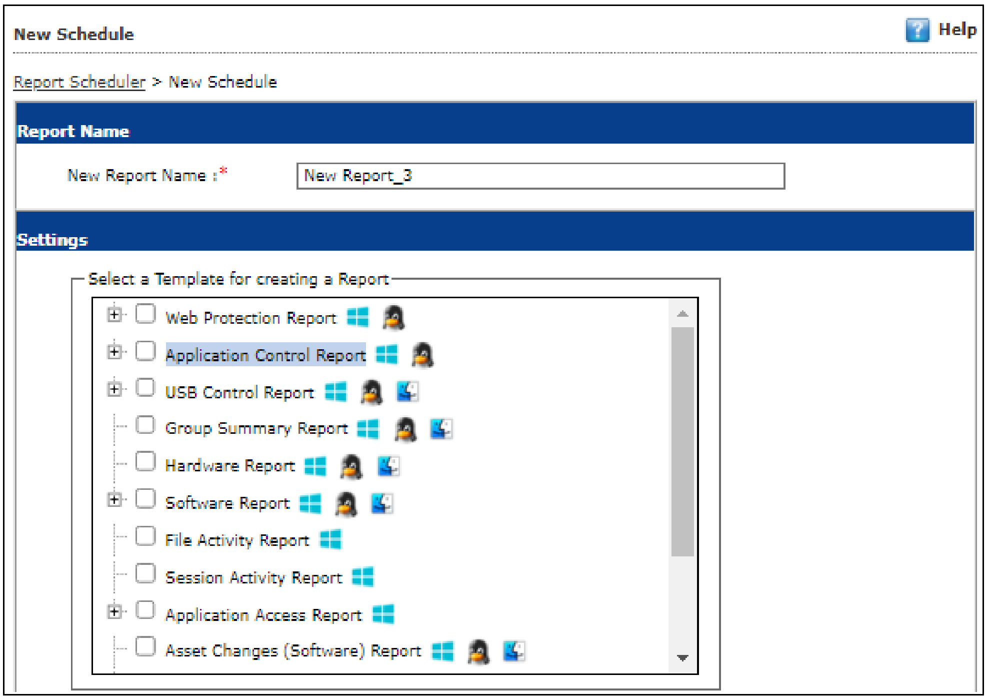
Report Scheduler

| ☐ | Schedule Name | Report Recipient | Scheduler Type | View |
|---|---|---|---|---|
| ☐ | New Report | [redacted].com | Manually Start | View |
| ☐ | New Report_1 | [redacted].com | Manually Start | View |
| ☐ | New Report_2 | [redacted].com | Manually Start | View |

# Creating a Schedule

To create a Schedule, follow the steps given below:

1. In the Report Scheduler screen, click **New Schedule**.
   New Schedule screen appears.



New Schedule

Report Scheduler > New Schedule

**Report Name**

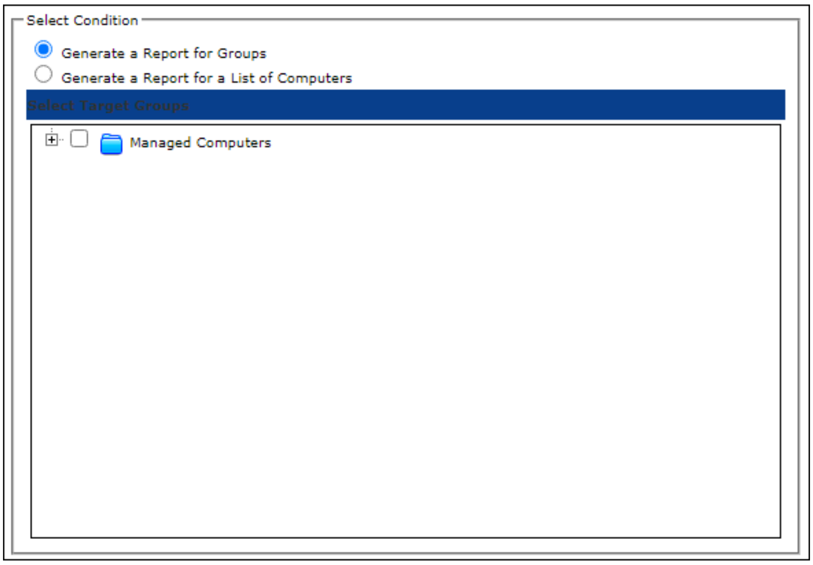
New Report Name :* New Report_3

**Settings**

Select a Template for creating a Report

- ☐ Web Protection Report
- ☐ Application Control Report
- ☐ USB Control Report
- ☐ Group Summary Report
- ☐ Hardware Report
- ☐ Software Report
- ☐ File Activity Report
- ☐ Session Activity Report
- ☐ Application Access Report
- ☐ Asset Changes (Software) Report

2. Enter a name for a new report schedule.
3. In the **Settings** section, select preferred report template.
4. In the **Select Condition** section, select a condition for groups or specific computers.



Select Condition

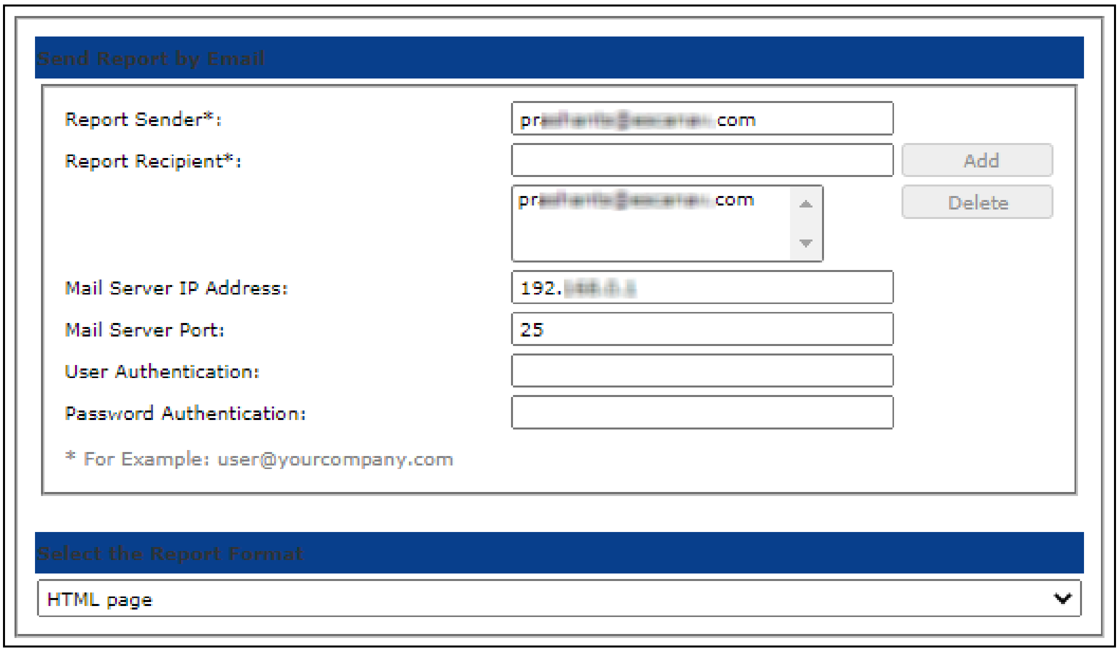
● Generate a Report for Groups

○ Generate a Report for a List of Computers

Select Target Groups

⊞ □ Managed Computers

5. In the **Send Report by email** section, fill the required information to receive reports via email.



Send Report by Email

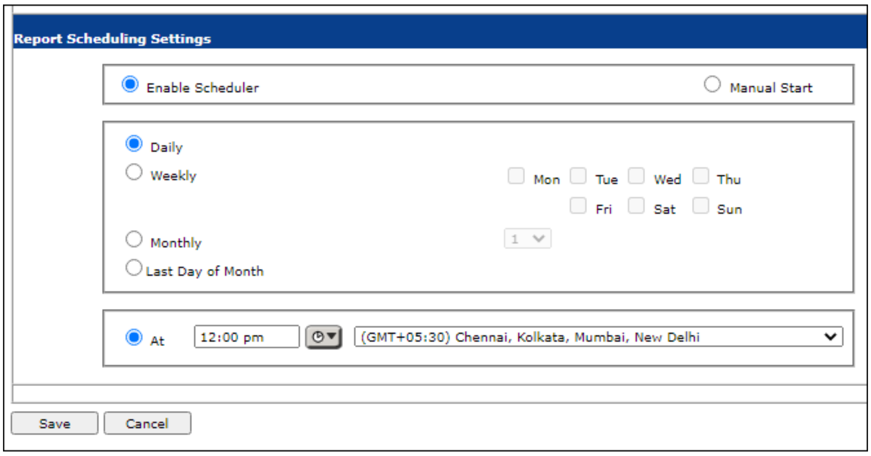
| | |
|---|---|
| Report Sender*: | pr[redacted] com |
| Report Recipient*: | |
| | pr[redacted] com |
| Mail Server IP Address: | 192.[redacted] |
| Mail Server Port: | 25 |
| User Authentication: | |
| Password Authentication: | |

* For Example: user@yourcompany.com

Select the Report Format

HTML page

6. Select the preferred report format.
7. In **Report Scheduling Settings** section, make the necessary changes.



Report Scheduling Settings

● Enable Scheduler ○ Manual Start

● Daily

○ Weekly □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sun

○ Monthly 1

○ Last Day of Month

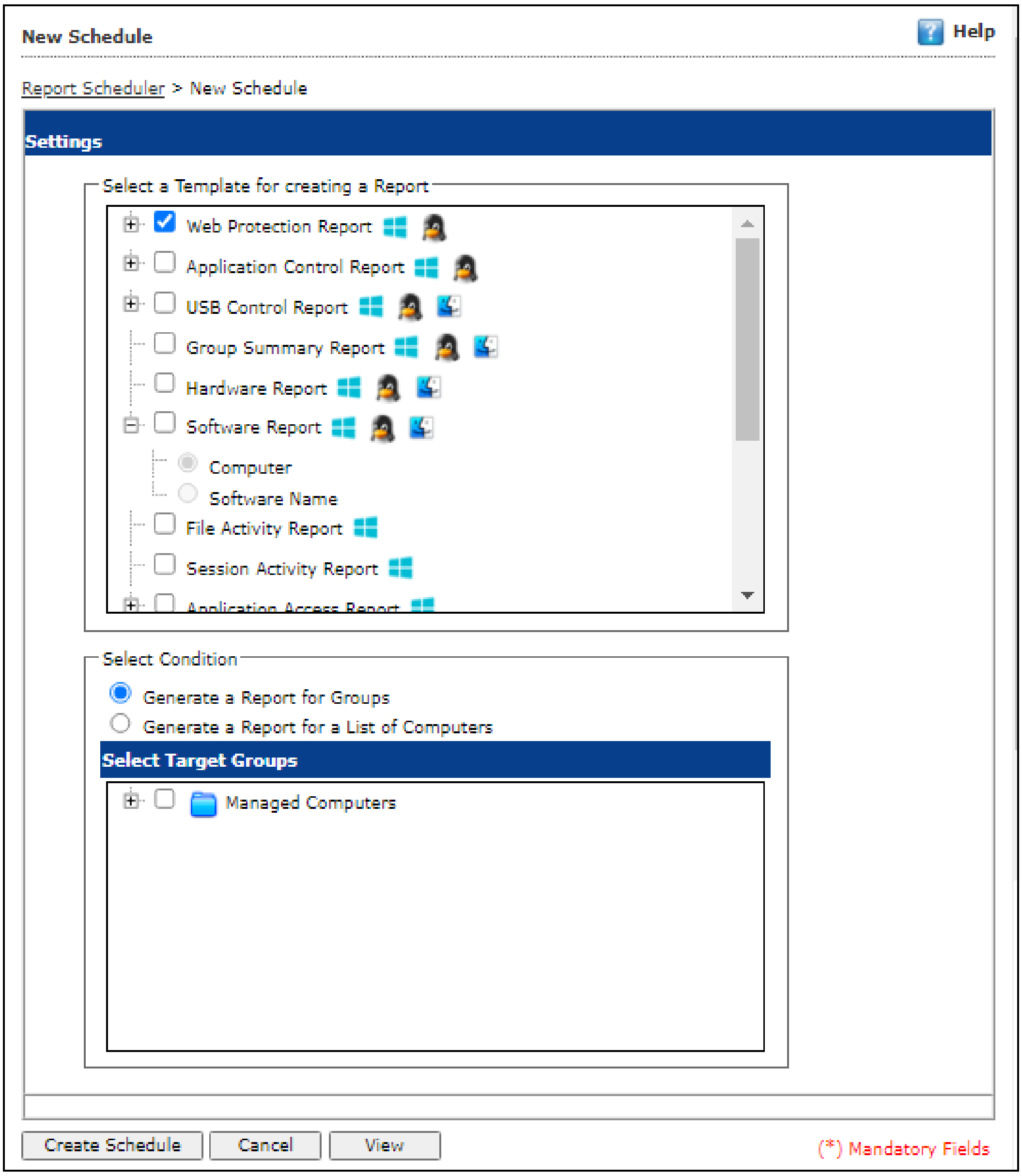
● At 12:00 pm (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi

8. Click **Save.**
   New schedule will be created.

# Viewing Reports on Demand

To view a report or a set of reports immediately, follow the steps given below:

1. Click **Report Scheduler** > **View & Create**.
   New Schedule screen appears.



New Schedule

Report Scheduler > New Schedule

Settings

Select a Template for creating a Report

- ☑ Web Protection Report
- ☐ Application Control Report
- ☐ USB Control Report
- ☐ Group Summary Report
- ☐ Hardware Report
- ☐ Software Report
  - ○ Computer
  - ○ Software Name
- ☐ File Activity Report
- ☐ Session Activity Report
- ☐ Application Access Report

Select Condition

- ● Generate a Report for Groups
- ○ Generate a Report for a List of Computers

Select Target Groups

- ☐ Managed Computers

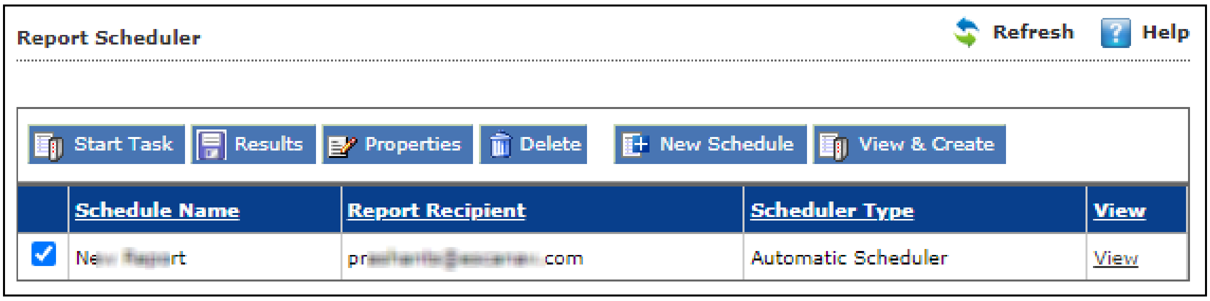
(*) Mandatory Fields

2. Select the **Template** options, the **Condition** and the **Target Groups**.
3. Click **View**.
   A new window appears displaying the created report.

Clicking **Create Schedule** lets you create a new Schedule.

# Managing Existing Schedule

The Report Scheduler module lets you manage the existing schedules.



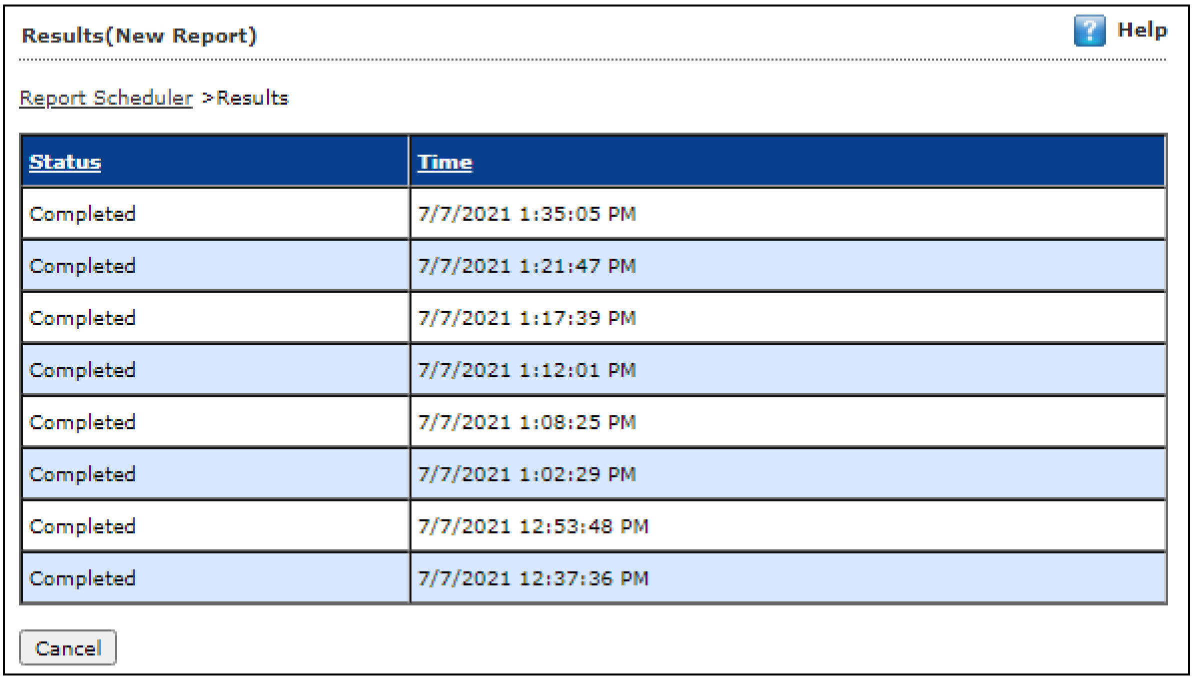
| | Schedule Name | Report Recipient | Scheduler Type | View |
|---|---|---|---|---|
| ☑ | Ne[redacted]rt | pr[redacted].com | Automatic Scheduler | View |

## Generating Task Report of a Schedule

To generate a task report, select the preferred report schedule name and then click **Start Task**. A task window appears displaying the name of the report being generated.

## Viewing Results of a Schedule

To see the results of a schedule and its time stamp, select the report schedule and then click **Results**. Results screen appears.

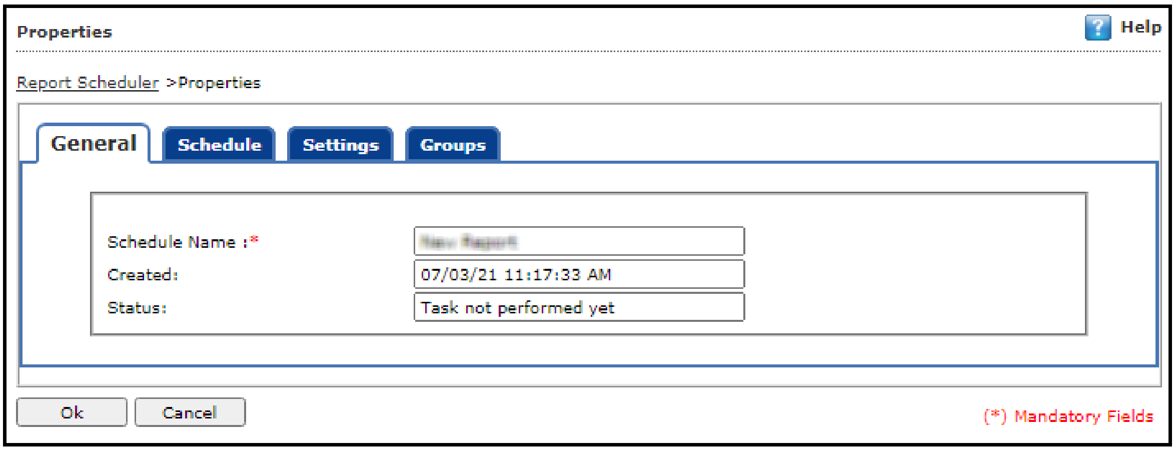


| Status | Time |
|---|---|
| Completed | 7/7/2021 1:35:05 PM |
| Completed | 7/7/2021 1:21:47 PM |
| Completed | 7/7/2021 1:17:39 PM |
| Completed | 7/7/2021 1:12:01 PM |
| Completed | 7/7/2021 1:08:25 PM |
| Completed | 7/7/2021 1:02:29 PM |
| Completed | 7/7/2021 12:53:48 PM |
| Completed | 7/7/2021 12:37:36 PM |

# Viewing Properties of a Schedule

To view the properties of a schedule, follow the steps given below:

1. Select a schedule.
2. Click **Properties**.
   Properties screen appears.



Properties

Report Scheduler >Properties

Schedule Name :* [illegible]
Created: 07/03/21 11:17:33 AM
Status: Task not performed yet

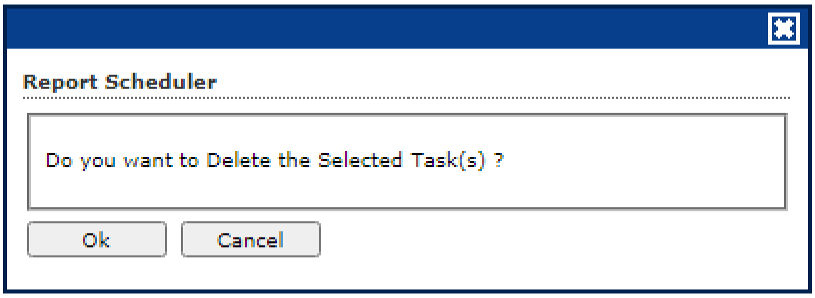
(*) Mandatory Fields

The properties screen displays general properties and lets you configure Schedule, Settings and Groups settings.

# Deleting a Schedule

To delete a report schedule, follow the steps given below:

1. Select a schedule.
2. Click **Delete**.
   A confirmation prompt appears.



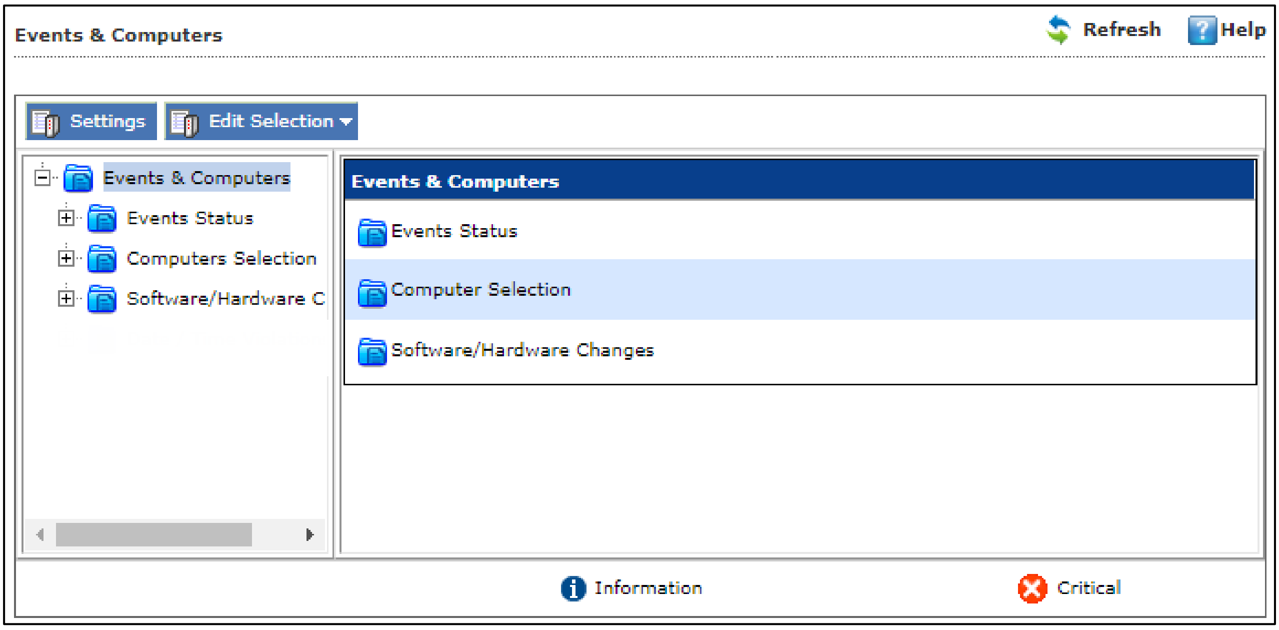
Report Scheduler

Do you want to Delete the Selected Task(s) ?

3. Click **OK**.
   The schedule will be deleted.

# Events and Computers

eScan Management Console maintains the record of all the events sent by the client computer. Through the events & computers module, the administrator can monitor the Events and Computers; this module lets you sort the computer with specific properties.



## Events Status

The Event Status subfolder is divided into following sections:

- **Recent**
- **Critical**
- **Information**

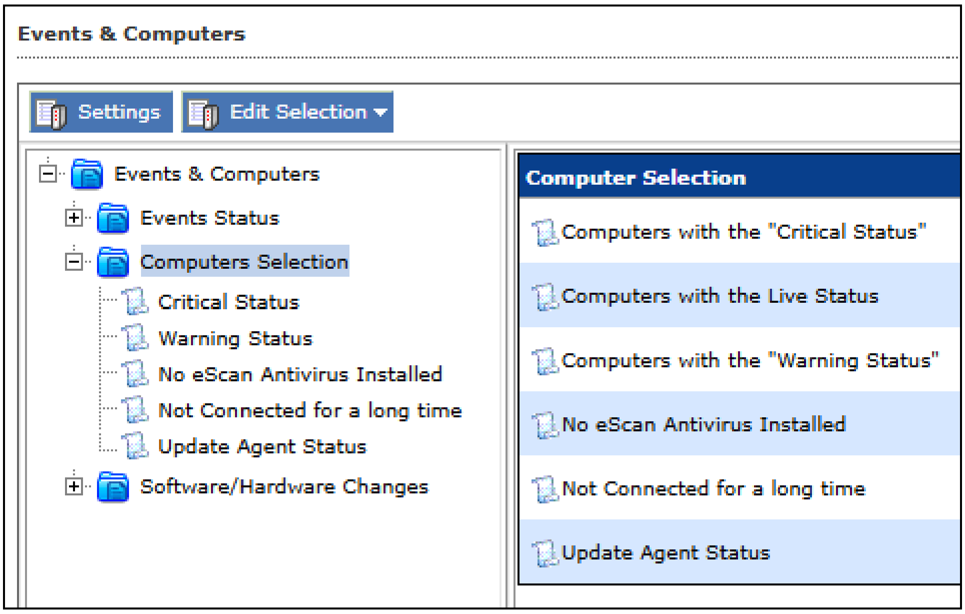
**Recent**
The Recent section displays both Information and Critical events.

**Critical** ⊗
The Critical section displays Critical events and immediate attention.
For example, Virus detection, Monitor disabled.
The Critical events can be filtered on the basis of date range and the report can be exported in .xls or .html format.

**Information** ⓘ
The Information section displays basic information events.
For example, Virus database update, Status.

# Computer Selection

The Computer Selection subfolder displays computers that fall under different categories. It lets you select the computer and take the preferred action. You can also set the criteria for each section and sort the computer accordingly.


Events & Computers
Settings
Edit Selection
Events & Computers
Events Status
Computers Selection
Critical Status
Warning Status
No eScan Antivirus Installed
Not Connected for a long time
Update Agent Status
Software/Hardware Changes
Computer Selection
Computers with the "Critical Status"
Computers with the Live Status
Computers with the "Warning Status"
No eScan Antivirus Installed
Not Connected for a long time
Update Agent Status

The Computer Selection subfolder consists following sections:

- **Computers with the critical status**
- **Computers with the live status**
- **Computer with warning status**
- **No eScan Antivirus Installed**
- **Not connected for a long time**
- **Update Agent Status**

**Computers with the critical status**
This section displays computers marked with Critical status.

| | |
|---|---|
| **NOTE** | The required action can be performed only if the endpoint system is online.<br>The ✓ symbol indicates that the endpoint is online and ✗ symbol indicates that the system is offline. |

**Computers with warning status**
This section displays computer with a warning status.

**No eScan Antivirus installed**
This section displays computers on which eScan is not installed.

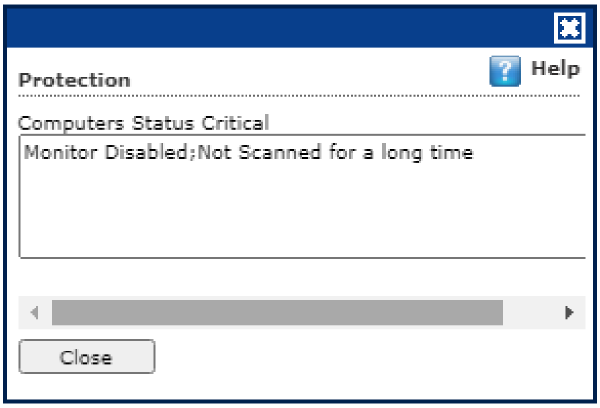
**Not connected for a long time**
This section displays the computers which didn’t connect to the eScan server for the set duration.

**Update Agent Status**
This section displays the status of computers assigned as Update Agent.
The additional settings vary depending upon the Computer Status.

# Edit Selection

This drop-down menu allows to configure various option based on selected options. The following options are present in the menu:

- **Protection**: This option displays the protection status of the selected computer.

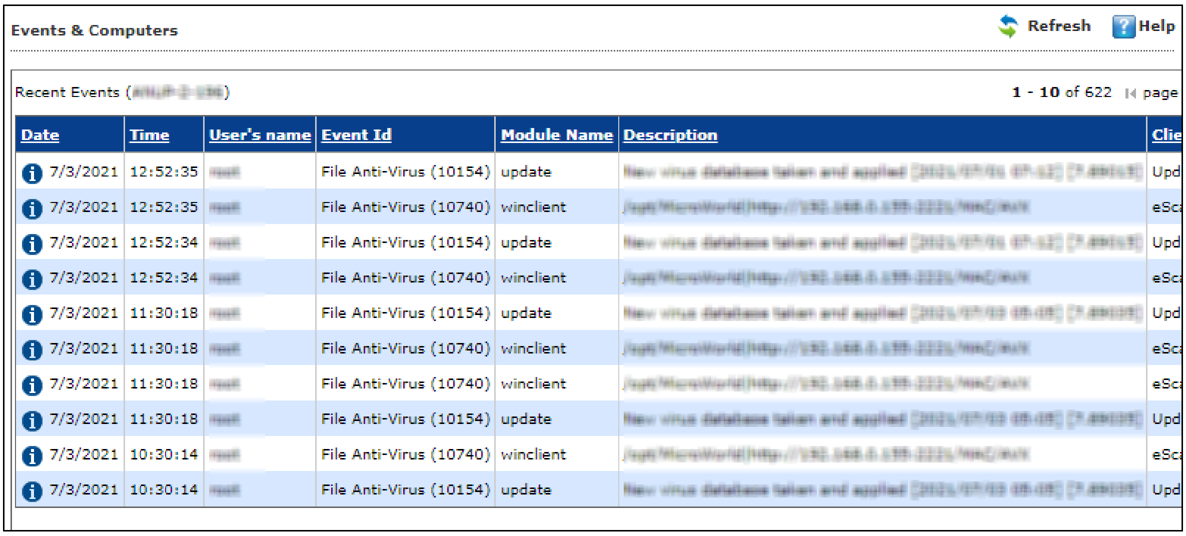


Protection

Computers Status Critical

Monitor Disabled;Not Scanned for a long time

- **Events**: This option displays the events that were performed in the particular computer.



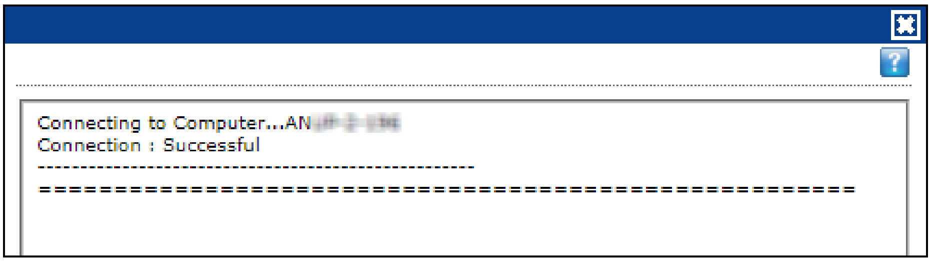
Events & Computers

Recent Events ([redacted])

1 - 10 of 622

| Date | Time | User's name | Event Id | Module Name | Description | Clie |
|---|---|---|---|---|---|---|
| 7/3/2021 | 12:52:35 | [redacted] | File Anti-Virus (10154) | update | [redacted] | Upd |
| 7/3/2021 | 12:52:35 | [redacted] | File Anti-Virus (10740) | winclient | [redacted] | eSca |
| 7/3/2021 | 12:52:34 | [redacted] | File Anti-Virus (10154) | update | [redacted] | Upd |
| 7/3/2021 | 12:52:34 | [redacted] | File Anti-Virus (10740) | winclient | [redacted] | eSca |
| 7/3/2021 | 11:30:18 | [redacted] | File Anti-Virus (10154) | update | [redacted] | Upd |
| 7/3/2021 | 11:30:18 | [redacted] | File Anti-Virus (10740) | winclient | [redacted] | eSca |
| 7/3/2021 | 11:30:18 | [redacted] | File Anti-Virus (10740) | winclient | [redacted] | eSca |
| 7/3/2021 | 11:30:18 | [redacted] | File Anti-Virus (10154) | update | [redacted] | Upd |
| 7/3/2021 | 10:30:14 | [redacted] | File Anti-Virus (10740) | winclient | [redacted] | eSca |
| 7/3/2021 | 10:30:14 | [redacted] | File Anti-Virus (10154) | update | [redacted] | Upd |

- **Deploy/Upgrade Client**: To learn about this option, click here.
- **Check Connection**: This option will verify if the client machine is online or offline.



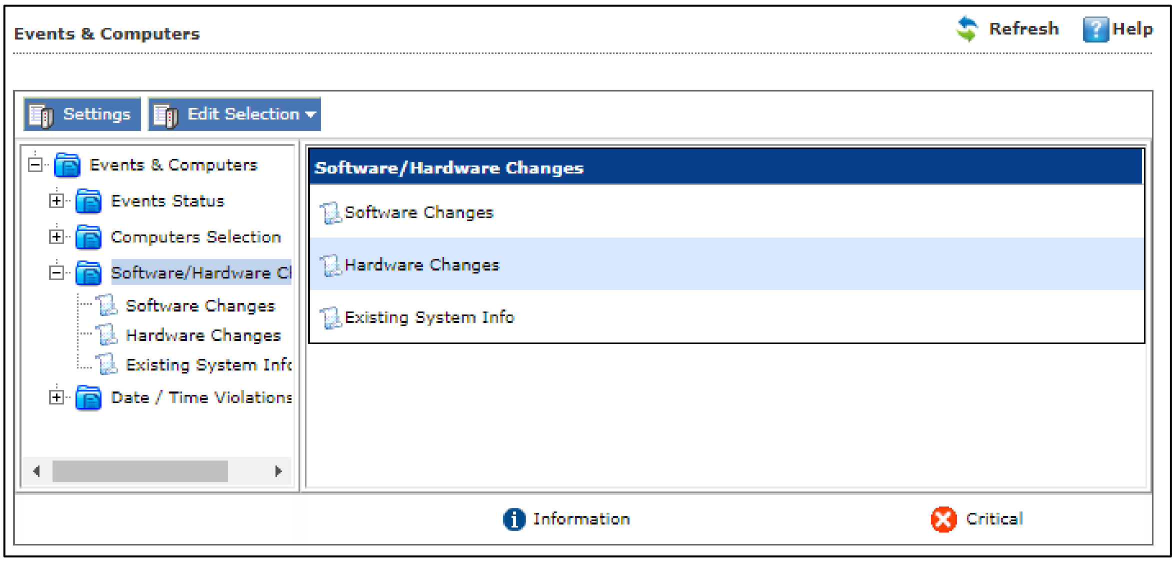
```
Connecting to Computer...AN[redacted]
Connection : Successful
------------------------------------------------
============================================================
```

- **Remove from Group**: To learn about this option, click here.
- **Connect to Client (RMM)**: To learn about this option, click here.
- **Force Download**: To learn about this option, click here.
- **Send Message**: To learn about this option, click here.
- **Check escan Port(s)**: To learn about this option, click here.
- **Properties**: To learn about this option, click here.

# Software/Hardware Changes

This subfolder displays all software/ hardware changes that occurred on computers. It consists following sections:

- **Software Changes**
- **Hardware changes**
- **Existing System Info**



### Software Changes

This section displays software changes i.e. installation, uninstallation or software upgrades.

### Hardware changes

This section displays hardware changes that occurred on computers. For example, IP address,Hard Disk, RAM etc.

### Existing System Info

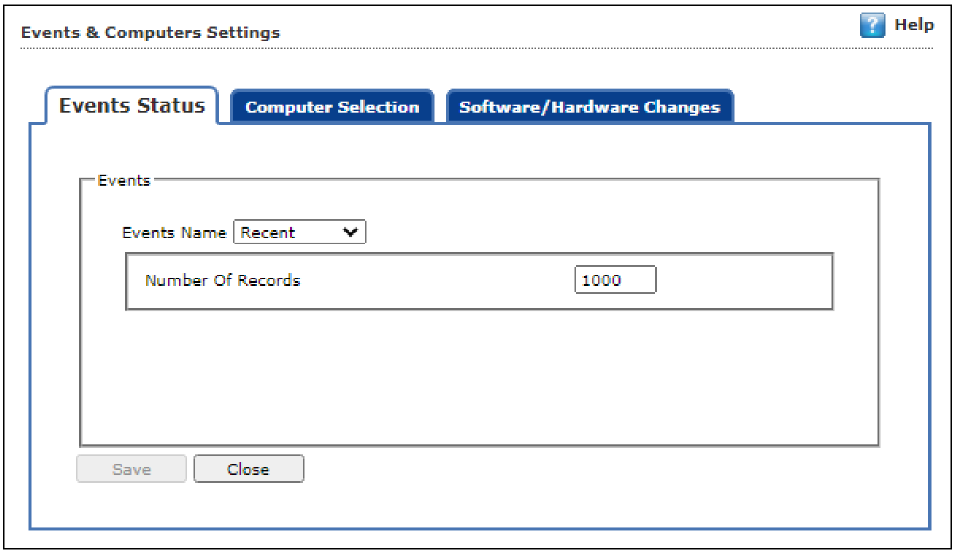
This section displays a computer's existing hardware information.

# Settings

You can define the Settings for Events, Computer Selection and Software/Hardware changes by clicking on the **Settings** option and defining the desired settings using the tabs and options present on the Events and Computers settings window.

## Event Status

Basically, events are activities performed on client's computer.



Events & Computers Settings

Events Name: Recent

Number Of Records: 1000

On the basis of severity, the events are categorized in to the following types:

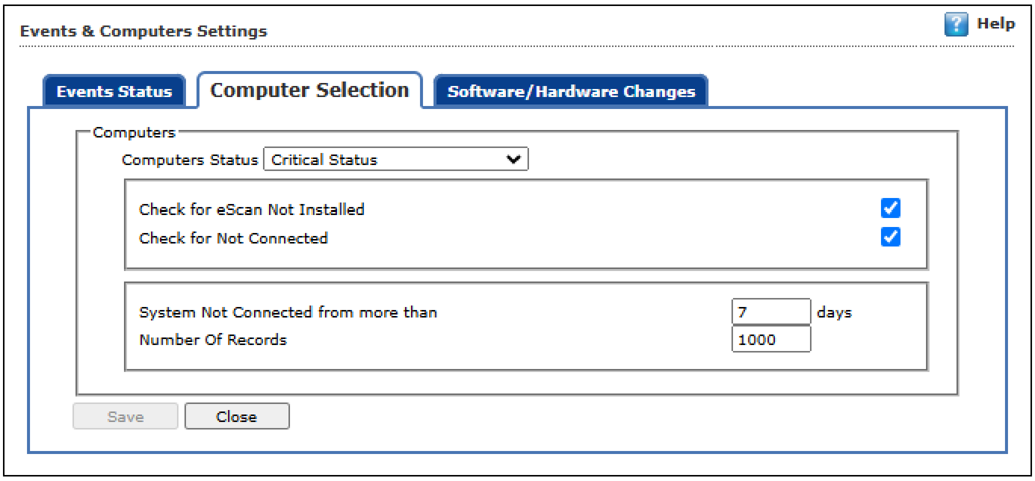
- **Recent:** It displays both critical and information events that occurred recently on managed client computers.
- **Information:** It displays all informative types of events, such as virus database update, status, and so on.

**Steps to define event status settings:**

Perform the following steps to save the event status settings:

1. Select the appropriate **Events Name**.
2. Enter the number of events that you want to view in a list, in the **Number of Records** field.
3. Click **Save**.
   The settings get saved.

# Computer Selection



Events & Computers Settings

Computers

Computers Status: Critical Status

Check for eScan Not Installed ☑

Check for Not Connected ☑

System Not Connected from more than 7 days

Number Of Records 1000

The Computer Selection lets you select and save the computer status settings. This module lets you do the following activities:

**Critical Status:** It displays a list of computers that are critical in status, as per the criteria's selected in computer settings. Specify the following field details:

- **Check for eScan Not Installed**: Select this checkbox to view the list of client systems under managed computers on which eScan has not been installed.
- **Check for Not Connected**: Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **System Not Connected from more than**: Enter the number of days from when the client system has not been connected to eScan server.
- **Number of Records**: Enter the number of client systems that you want to view in the list.

**Warning Status:** It displays the list of systems which are warning in status, as per the criteria's selected in computer settings. Specify the following field details:

- **Check for Not Connected**: Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **System Not Connected from more than**: Enter the number of days from when the client system has not been connected to eScan server.
- **Number Of Virus**: Enter the number of viruses detected on client system.
- **Number Of Records**: Enter the number of client system that you want to view in the list.

**No eScan Antivirus Installed:** It displays the list of systems on which eScan has not been installed. Specify the following field detail:

- **Number of Records**: Enter the number of client system that you want to view in the list.

**Not connected for a long time:** It displays the list of systems which have not been connected to the server from a long time. Specify the following field details:

- **System Not Connected from more than**: Enter the number of days from when the system has not been connected.
- **Number of Records**: Enter the number of client system that you want to view in the list.

**Update Agent Status:** It displays the list of systems that has been assigned as an Update Agent. Specify the following in detail:

- **Number of Records**: Enter the number of client system that you want to view in the list.

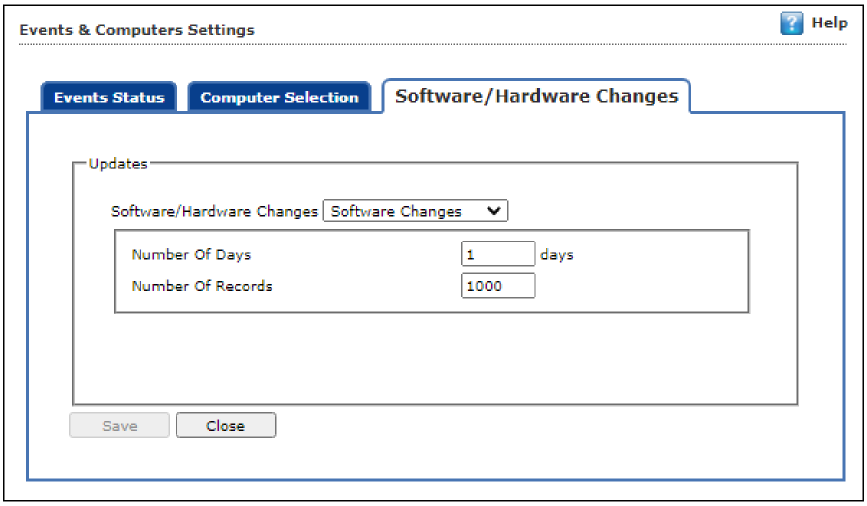
## Steps to define computer settings

To save the computer settings, follow the steps given below:

1. Click **Computers Selection** tab.
2. Select a type of status for which you want to set criteria, from the **Computer status** drop-down.
3. Select the appropriate checkboxes, and then enter field details in the available fields. For more information, refer [Types and criteria of computer status] section.
4. Click **Save**.
   The settings will be saved.

# Software/ Hardware Changes Setting

You can set these settings, if you want to get updates on any changes made in the software, hardware, and to existing system.



Events & Computers Settings

Software/Hardware Changes: Software Changes

Number Of Days: 1 days

Number Of Records: 1000

The Software/ Hardware Changes enable you to do the following activities:
Type of Software/Hardware Changes

- **Software changes**
- **Hardware changes**
- **Existing system info**

To Change software/hardware settings, follow the steps given below:

1. Click the **Software/Hardware Changes** tab.
2. Specify the following field details.
   - **Software/Hardware Changes**: Click the drop-down and select the changes made.
   - **Number of Days**: Enter the number of days, to view changes made within the specified days.
   - **Number of Records**: Enter the number of client systems that you want to view in the list.

3. Click **Save**.
   The settings get saved.

**Existing system info:** It displays the list of existing systems on which software/hardware changes made for any module, as per the protection criteria's selected in computer settings. Specify the following field detail.

**Number of Records**: Enter the number of client system that you want to view in the list.

# Performing an action for computer

To perform an action for a computer, follow the steps given below:

1. Select a computer.
2. Click **Edit Selection** drop-down. To learn more click here.
3. Click the preferred action.

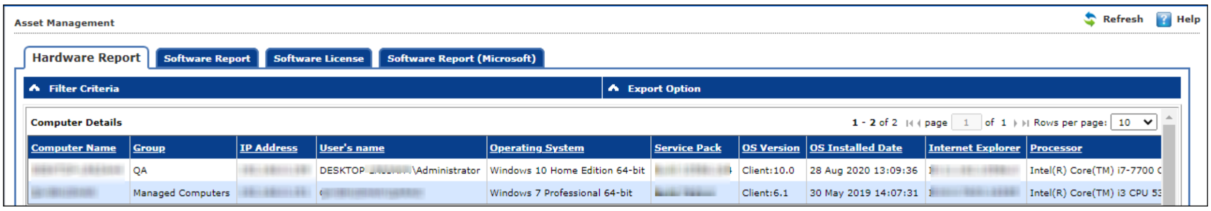
# Asset Management

This module displays list of hardware configuration, software installed, software version number and a software report for Microsoft software installed on Managed Computers. The Asset Management module consists following tabs:

- **Hardware Report**
- **Software Report**
- **Software License**
- **Software Report (Microsoft)**

## Hardware Report

The Hardware Report tab displays hardware configuration of all Managed Computers.



| Computer Name | Group | IP Address | User's name | Operating System | Service Pack | OS Version | OS Installed Date | Internet Explorer | Processor |
|---|---|---|---|---|---|---|---|---|---|
| [redacted] | QA | [redacted] | DESKTOP [redacted]\Administrator | Windows 10 Home Edition 64-bit | [redacted] | Client:10.0 | 28 Aug 2020 13:09:36 | [redacted] | Intel(R) Core(TM) i7-7700 ( |
| [redacted] | Managed Computers | [redacted] | [redacted] | Windows 7 Professional 64-bit | [redacted] | Client:6.1 | 30 May 2019 14:07:31 | [redacted] | Intel(R) Core(TM) i3 CPU 53 |

The tab displays following details of managed computers:

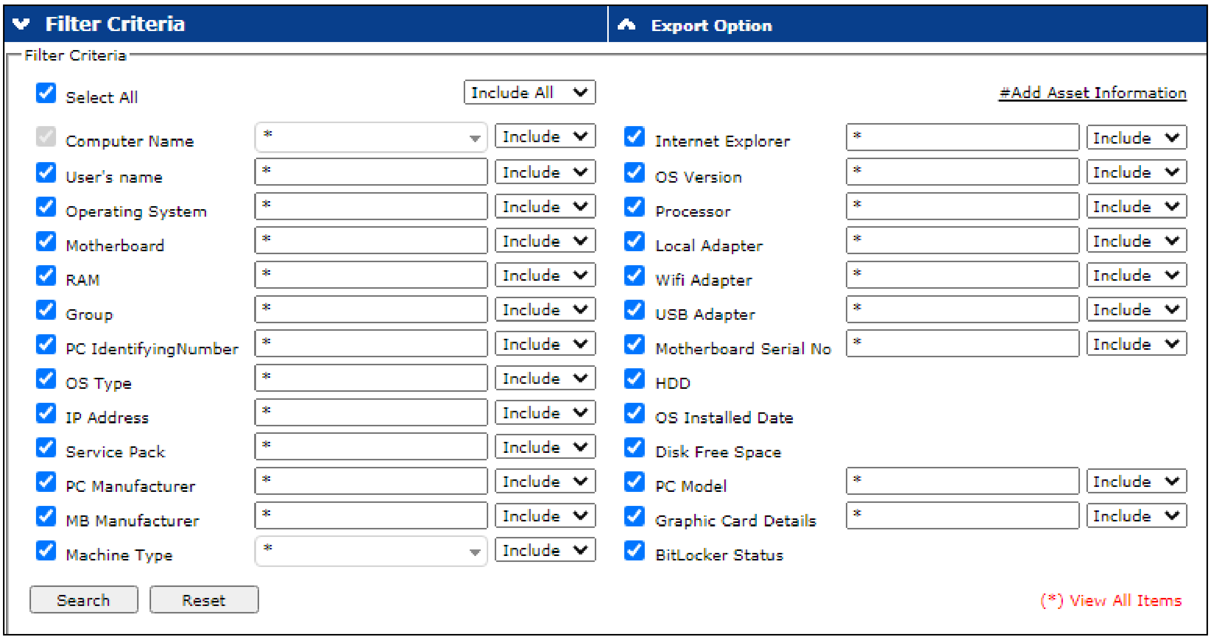
- Computer Name
- Group
- IP Address
- User's name
- Operating System
- Service Pack
- OS Version
- OS Installed Date
- Internet Explorer
- Processor
- Motherboard
- RAM
- HDD
- Local MAC Adapter
- Wifi MAC [Adapter]
- USB MAC [Adapter]
- PC Identifying Number
- Motherboard Serial No
- Network Speed
- Disk Free Space
- PC Manufacturer
- PC Model
- MB Manufacturer
- Graphic Card Details
- Machine Type
- BitLocker Status

- Software

To view the list of Software along with the installation dates, click **View** in **Software** column.

# Filtering Hardware Report

To filter the Hardware Report as per your requirements, click **Filter Criteria** field.
Filter Criteria field expands.



▾ Filter Criteria | ▴ Export Option

Filter Criteria

| | | | | | |
|---|---|---|---|---|---|
| ☑ Select All | | Include All | | | #Add Asset Information |
| ☑ Computer Name | * | Include | ☑ Internet Explorer | * | Include |
| ☑ User's name | * | Include | ☑ OS Version | * | Include |
| ☑ Operating System | * | Include | ☑ Processor | * | Include |
| ☑ Motherboard | * | Include | ☑ Local Adapter | * | Include |
| ☑ RAM | * | Include | ☑ Wifi Adapter | * | Include |
| ☑ Group | * | Include | ☑ USB Adapter | * | Include |
| ☑ PC IdentifyingNumber | * | Include | ☑ Motherboard Serial No | * | Include |
| ☑ OS Type | * | Include | ☑ HDD | | |
| ☑ IP Address | * | Include | ☑ OS Installed Date | | |
| ☑ Service Pack | * | Include | ☑ Disk Free Space | | |
| ☑ PC Manufacturer | * | Include | ☑ PC Model | * | Include |
| ☑ MB Manufacturer | * | Include | ☑ Graphic Card Details | * | Include |
| ☑ Machine Type | * | Include | ☑ BitLocker Status | | |

Search | Reset (*) View All Items

Select the parameters you want to be included in the filtered report.

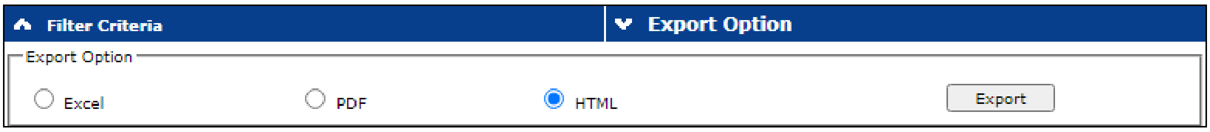
**Include/Exclude**
Selecting **Include/Exclude** for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search.**
The Hardware Report will be filtered according to your preferences.

Reset all filter criteria in all field, click **Reset**.

# Exporting Hardware Report

To export the Hardware Report, click **Export Option**.
Export Option field expands.

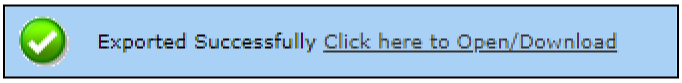


▴ Filter Criteria | ▾ Export Option

Export Option

○ Excel ○ PDF ● HTML Export

Select the preferred option and then click **Export**.
A success message appears.

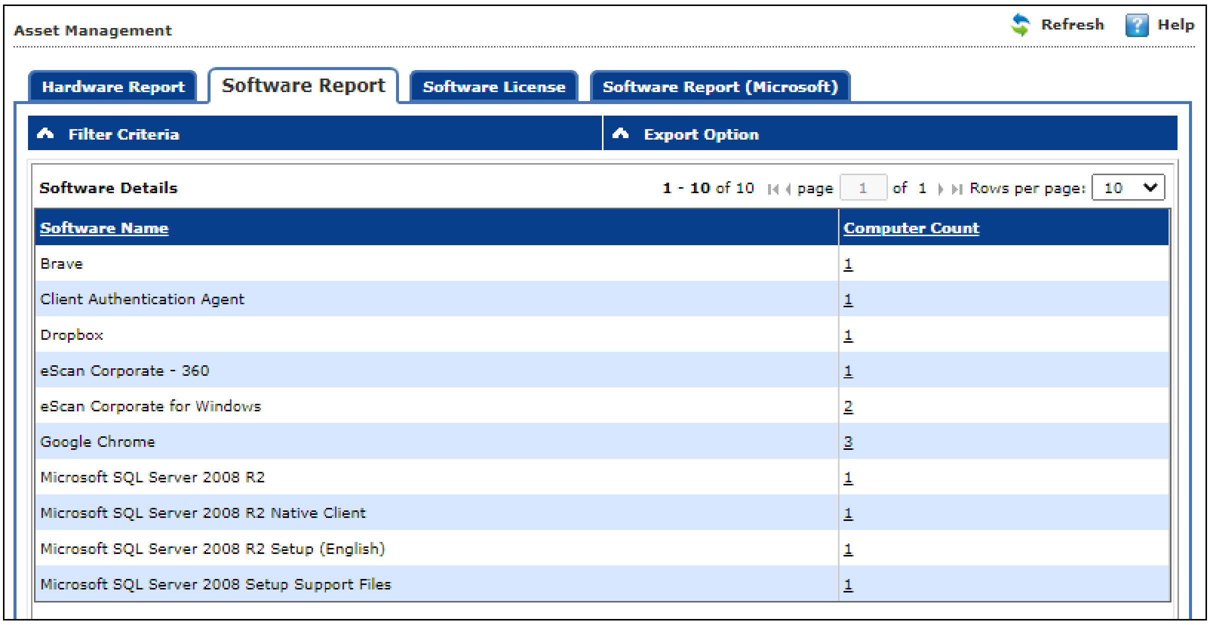


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

# Software Report

The Software Report tab displays list of Software along with the number of computers on which they are installed.



Asset Management — Refresh — Help

Hardware Report | Software Report | Software License | Software Report (Microsoft)

Filter Criteria — Export Option

Software Details — 1 - 10 of 10 — page 1 of 1 — Rows per page: 10

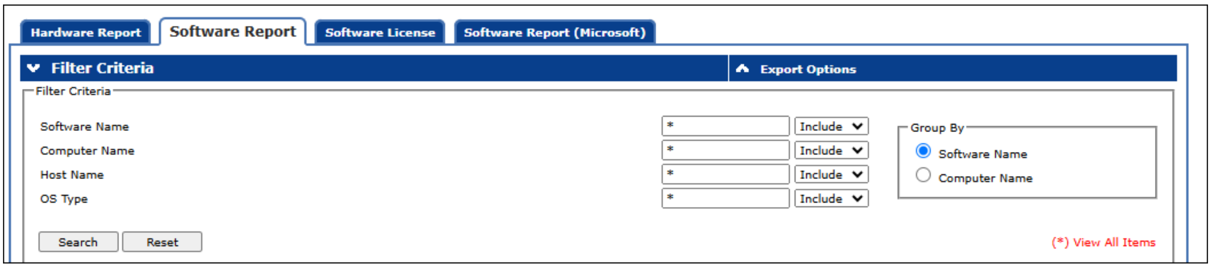
| Software Name | Computer Count |
|---|---|
| Brave | 1 |
| Client Authentication Agent | 1 |
| Dropbox | 1 |
| eScan Corporate - 360 | 1 |
| eScan Corporate for Windows | 2 |
| Google Chrome | 3 |
| Microsoft SQL Server 2008 R2 | 1 |
| Microsoft SQL Server 2008 R2 Native Client | 1 |
| Microsoft SQL Server 2008 R2 Setup (English) | 1 |
| Microsoft SQL Server 2008 Setup Support Files | 1 |

To view the computers on which the specific software is installed, click the numerical in Computer Count Column.
Computer list window appears displaying following details:

- Computer Name
- Group
- IP Address
- Operating System
- Software Version
- Installed Date

# Filtering Software Report

To filter Software Report, click **Filter Criteria** field.
Filter Criteria field expands.



Hardware Report | Software Report | Software License | Software Report (Microsoft)

Filter Criteria — Export Options

Filter Criteria

| | | |
|---|---|---|
| Software Name | * | Include |
| Computer Name | * | Include |
| Host Name | * | Include |
| OS Type | * | Include |

Group By
● Software Name
○ Computer Name

Search — Reset

(*) View All Items

**Software Name**
Entering the Software name displays suggestions. Select the appropriate software.

**Computer Name**
Click the drop-down and select the preferred computer(s).

**OS Type**
Enter the OS type.

**Include/Exclude**
Selecting **Include/Exclude** for a parameter lets you include or exclude it from the report.

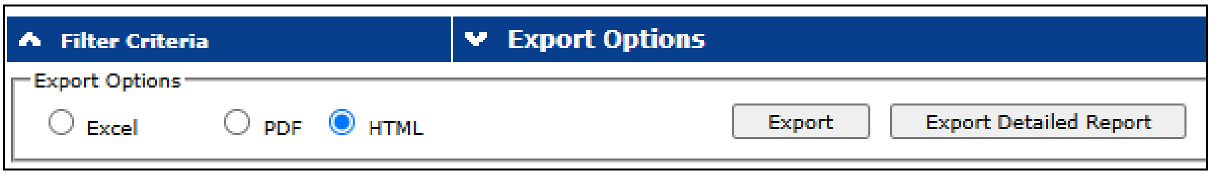
**Group By**
The results can be grouped by Software name, Computer name or Group.
If Group option is selected, the report can be filtered for a specific group.

After entering data in all fields, click **Search**.
The Software Report will be filtered according to your preferences.

Reset all filter criteria in all field, click **Reset**.

## Exporting Software Report

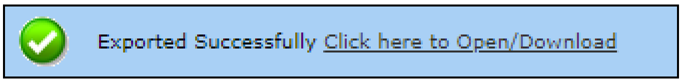
To export the Software Report, click **Export Option**.
Export Option field expands.



Select the preferred option and then click **Export**.

OR

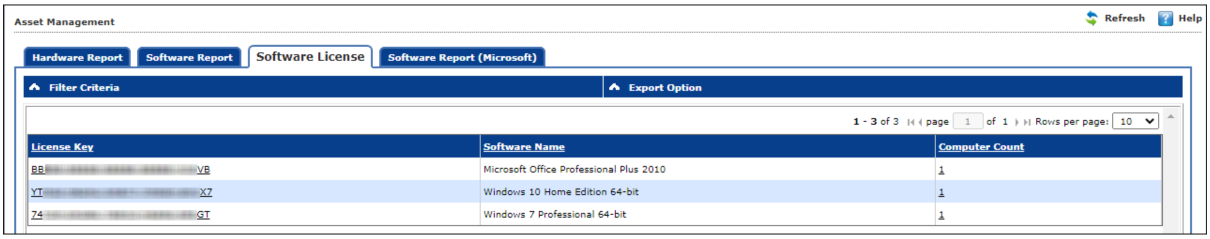
To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

# Software License

The Software License tab displays list of Software Licenses of managed computers.



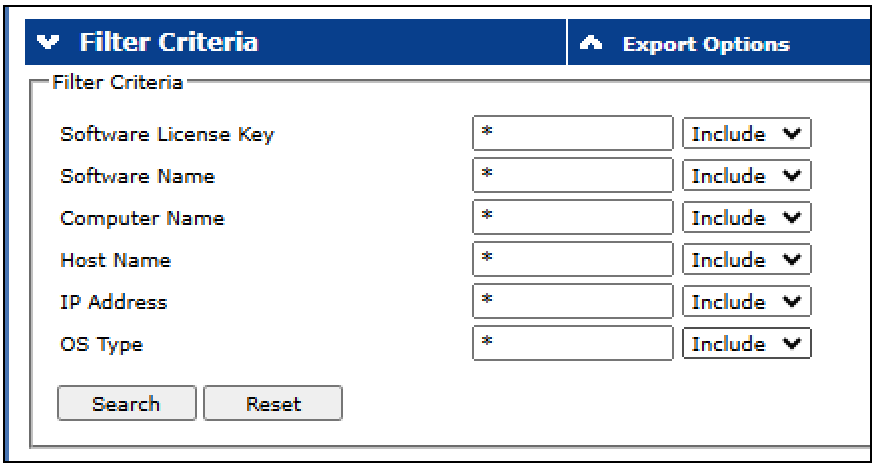
1 - 3 of 3 page 1 of 1 Rows per page: 10

| License Key | Software Name | Computer Count |
|---|---|---|
| BB[redacted]VB | Microsoft Office Professional Plus 2010 | 1 |
| YT[redacted]X7 | Windows 10 Home Edition 64-bit | 1 |
| 74[redacted]GT | Windows 7 Professional 64-bit | 1 |

The log displays License Key, Software Name, and Computer Count.
To see more details of the computer's license key installed, click the numerical value in License Key or Computer Count Column.

# Filtering Software License Report

To filter Software Report, click **Filter Criteria** field.
Filter Criteria field expands.



| | | |
|---|---|---|
| Software License Key | * | Include |
| Software Name | * | Include |
| Computer Name | * | Include |
| Host Name | * | Include |
| IP Address | * | Include |
| OS Type | * | Include |

**Software License Key**
Entering the license key displays suggestions. Select the appropriate key.

**Software Name**
Entering the Software name displays suggestions. Select the appropriate software.

**Computer Name**
Click the drop-down and select the preferred computer(s).

**Host Name**
Enter the Host Name displays suggestions. Select the appropriate key.

**IP Address**
Entering the IP address displays suggestions. Select the appropriate IP address.

**OS Type**
Enter the OS type.

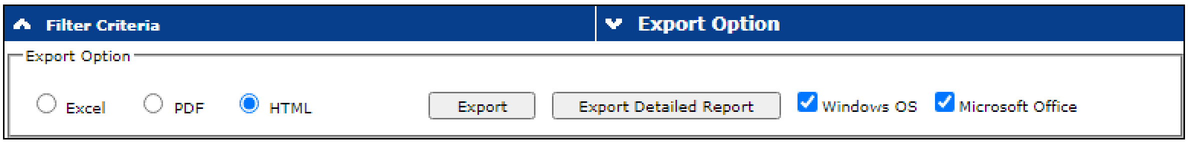
**Include/Exclude**
Selecting **Include/Exclude** for a parameter lets you include or exclude it from the report.

After entering data in all fields, click **Search**.
The Software License Report will be filtered according to your preferences.

Reset all filter criteria in all the fields, click **Reset.**

## Exporting Software License Report

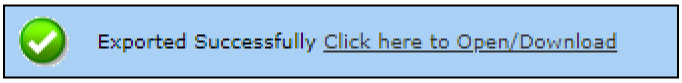
To export the Software License Report, click **Export Option**.
Export Option field expands.



Select whether you want report for **Windows OS** and **Microsoft Office.**
Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.

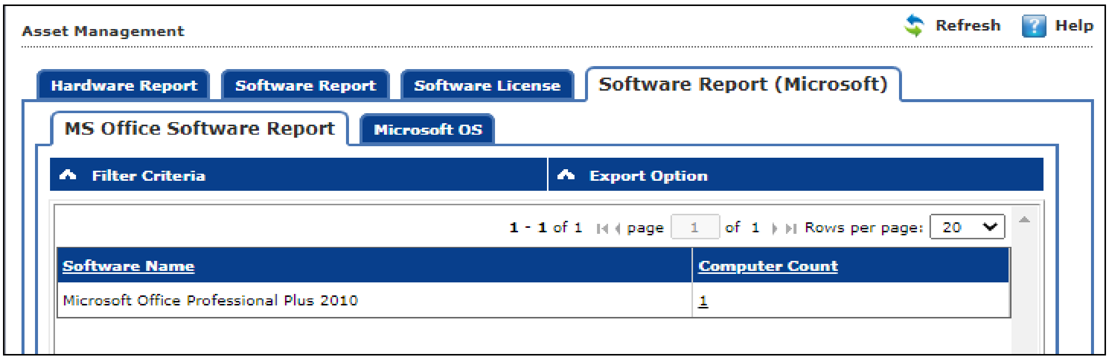


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

# Software Report (Microsoft)

The Software Report (Microsoft) displays details of the Microsoft Software installed on the computers.



1 - 1 of 1 page 1 of 1 Rows per page: 20

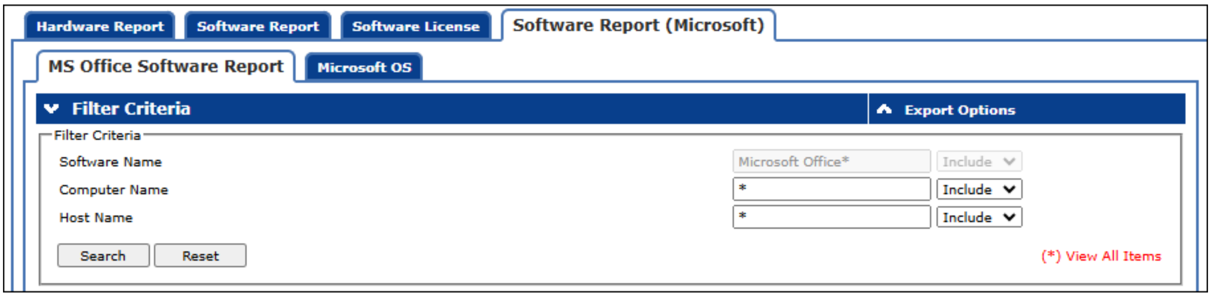
| Software Name | Computer Count |
|---|---|
| Microsoft Office Professional Plus 2010 | 1 |

The tab consists following subtabs:

**MS Office Software Report** – It displays Microsoft software name and computer count.
**Microsoft OS** – It displays Operating System, Service Pack, OS version and computer count.

## Filtering MS Office Software Report

To filter Software Report (Microsoft), click **Filter Criteria** field.
Filter Criteria field expands.



Filter Criteria

| | | |
|---|---|---|
| Software Name | Microsoft Office* | Include |
| Computer Name | * | Include |
| Host Name | * | Include |

**Software Name**
Entering the Software name displays suggestions. Select the appropriate software.

**Computer Name**
Click the drop-down and select the preferred computer(s).

**Host Name**
Enter the Host Name displays suggestions. Select the appropriate key.

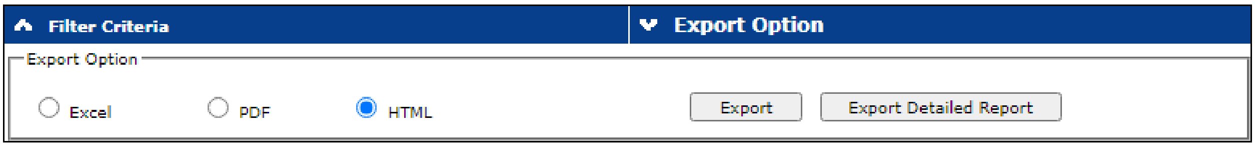
**Include/Exclude**
Selecting **Include/Exclude** for a parameter lets you include or exclude it from the report.

After entering data in all fields, click **Search**.
The Software Report (Microsoft) will be filtered according to your preferences.

Reset all filter criteria in all the fields, click **Reset.**

# Exporting MS Office Software Report

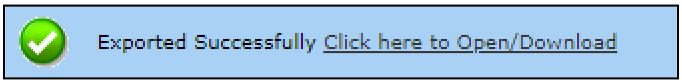
To export the Software Report (Microsoft), click **Export Option**.
Export Option field expands.



Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.

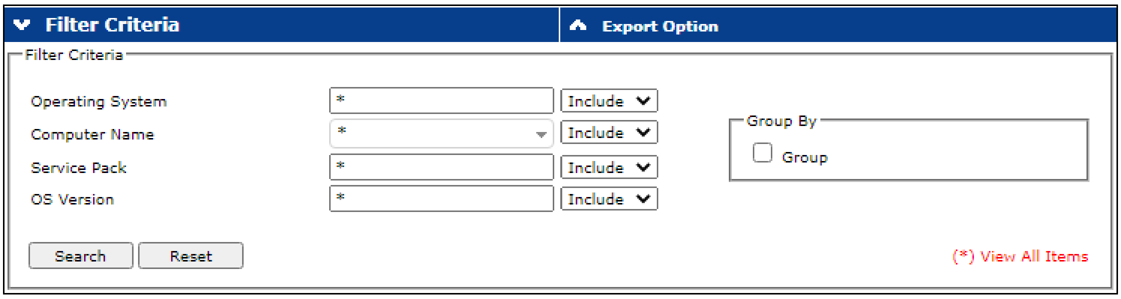


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

# Filtering Microsoft OS Report

To filter the Microsoft OS report, click **Filter Criteria** field.
Filter Criteria field expands.



**Operating System**
Entering the operating system name displays list of suggestions. Select the appropriate OS.

**Computer Name**
Click the drop-down and select the preferred computer(s).

**Service Pack**
Entering the service pack name displays list of suggestions. Select the appropriate Service Pack.

**OS Version**
Entering the OS version displays list of suggestions. Select the appropriate OS version.

**Include/Exclude**
Selecting **Include/Exclude** for a parameter lets you include or exclude it from the report.

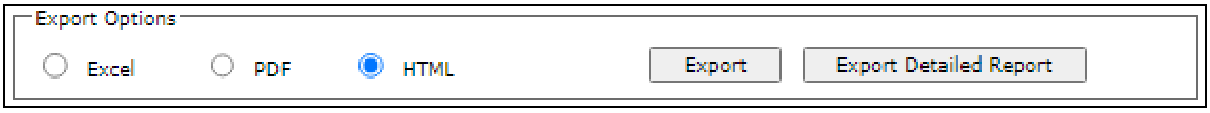
**Group By**
If **Group** option is selected, the report can be filtered for a specific group.

After filling all the fields, click **Search**.
The Microsoft OS report will be filtered according to your preferences.

Reset all filter criteria in all the fields, click **Reset.**

## Exporting Microsoft OS Report

To export the Microsoft OS Report, click **Export Option**.
Export Option field expands.



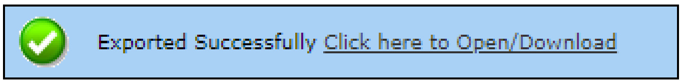
Export Options

○ Excel ○ PDF ● HTML [Export] [Export Detailed Report]

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.



Exported Successfully Click here to Open/Download

Click the link to open/download the file.

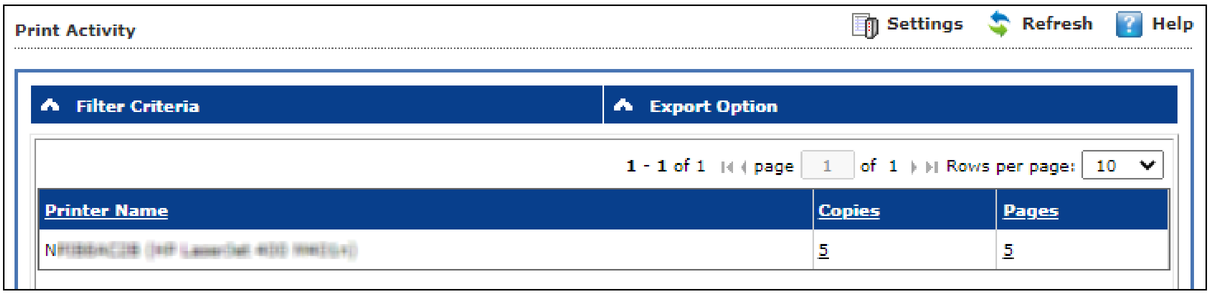
# User Activity

The User Activity module lets you monitor Print, Session and File activities occurring on the client computers. It also provides the reports of the running applications. It consists following sub modules:

- **Print Activity**
- **Session Activity Report**
- **File Activity Report**
- **Application Access Report**

# Print Activity

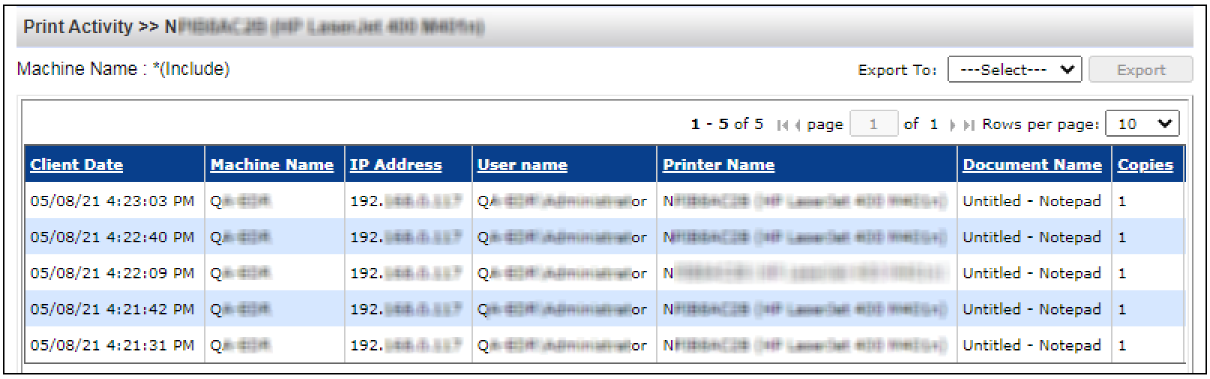
The Print Activity sub module monitors and logs print commands sent by all computers. It also lets you filter the logs on the basis of Computer name, Printer and Username. Furthermore, the module lets you export a detailed print activity report in XLS, PDF, and HTML formats. The log report generated consist information such as Print Date, Machine Name, IP Address, Username, Printer Name, Document Name along with number of Copies and Pages.



| Printer Name | Copies | Pages |
|---|---|---|
| N[redacted] | 5 | 5 |

## Viewing Print Activity Log

To view the Print log of a Printer, click its numerical value under **Copies** or **Pages** column. Print Activity window appears displaying details.



Print Activity >> N[redacted]
Export To: ---Select---
Export
1 - 5 of 5 page 1 of 1 Rows per page: 10

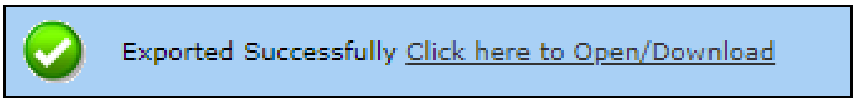
Machine Name : *(Include)

| Client Date | Machine Name | IP Address | User name | Printer Name | Document Name | Copies |
|---|---|---|---|---|---|---|
| 05/08/21 4:23:03 PM | Q[redacted] | 192.[redacted] | Q[redacted]or | N[redacted] | Untitled - Notepad | 1 |
| 05/08/21 4:22:40 PM | Q[redacted] | 192.[redacted] | Q[redacted]or | N[redacted] | Untitled - Notepad | 1 |
| 05/08/21 4:22:09 PM | Q[redacted] | 192.[redacted] | Q[redacted]or | N[redacted] | Untitled - Notepad | 1 |
| 05/08/21 4:21:42 PM | Q[redacted] | 192.[redacted] | Q[redacted]or | N[redacted] | Untitled - Notepad | 1 |
| 05/08/21 4:21:31 PM | Q[redacted] | 192.[redacted] | Q[redacted]or | N[redacted] | Untitled - Notepad | 1 |

## Exporting Print Activity Log

To export this generated log, follow the steps given below:

1. Click the Export to drop-down.
2. Select a preferred format.
3. Click **Export**.
   A success message appears.

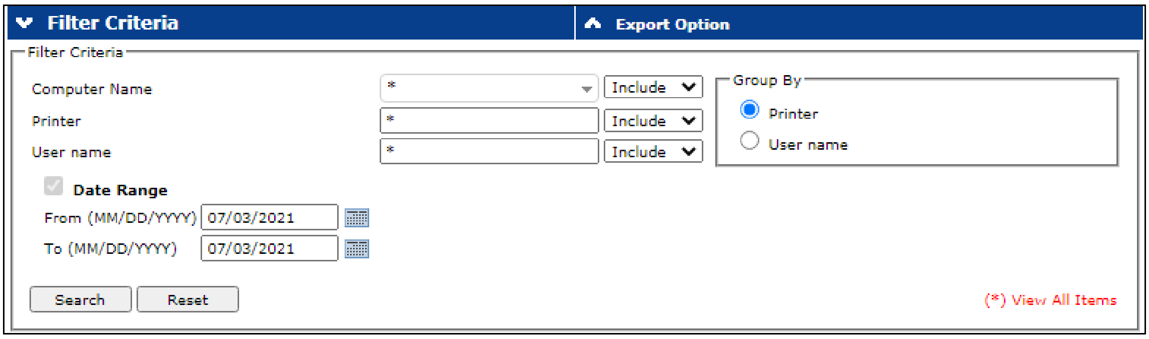


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

# Filtering Print Activity Log

To filter the print activity log, click **Filter Criteria**.
Filter criteria field expands.



Filter Criteria

| | | |
|---|---|---|
| Computer Name | * | Include |
| Printer | * | Include |
| User name | * | Include |

Group By: ● Printer ○ User name

☑ Date Range
From (MM/DD/YYYY) 07/03/2021
To (MM/DD/YYYY) 07/03/2021

**Computer Name**
Click the drop-down and select the preferred computer.

**Printer**
Enter the printer's name.

**User Name**
Enter the User's name.

**Include/Exclude**
Selecting **Include/Exclude** for a Machine or Printer lets you include or exclude it from the log.

**Date Range**
To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the **calendar** icon and select **From** and **To** dates.

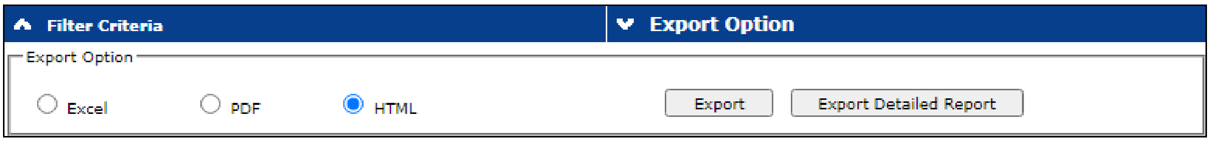
After filling all fields, click **Search**.
The Print activity log will be filtered and generated according to your preferences.

Reset all filter criteria fields, click **Reset.**

**Group By**
To view results by specific printer, select **Printer**, Date Range and then click **Search**.
To view results by specific user name, select **User name**, Date Range and then click **Search**.

# Exporting Print Activity Report

To export the generated log, click **Export Option**.
Export Option field expands.



Export Option: ○ Excel ○ PDF ● HTML

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.

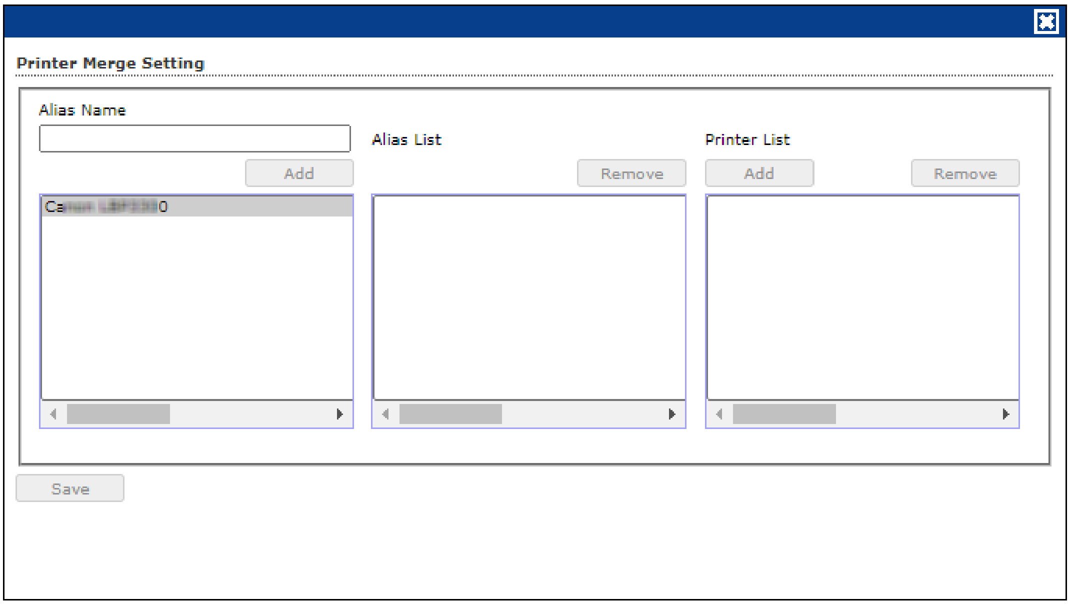
Exported Successfully Click here to Open/Download

Click the link to open/download the file.

# Print Activity Settings

The Print Activity Settings lets you keep track of printers by adding them in a group and assigning it an alias name. The printers can be added or removed from this alias group.
To configure Print Activity Settings, follow the steps given below:

1. In the Print Activity screen, at the top right corner, click **Settings**.
   Printer Merge Setting window appears.



2. Enter name in Alias Name field.
3. Select printer(s) for the alias.
4. Click **Add**.
   The printer(s) will be added to the alias.
5. Click **Remove.**
   The printer(s) will be removed from the alias/printer list.
6. Click **Save**.
   The Print Activity Settings will be saved.

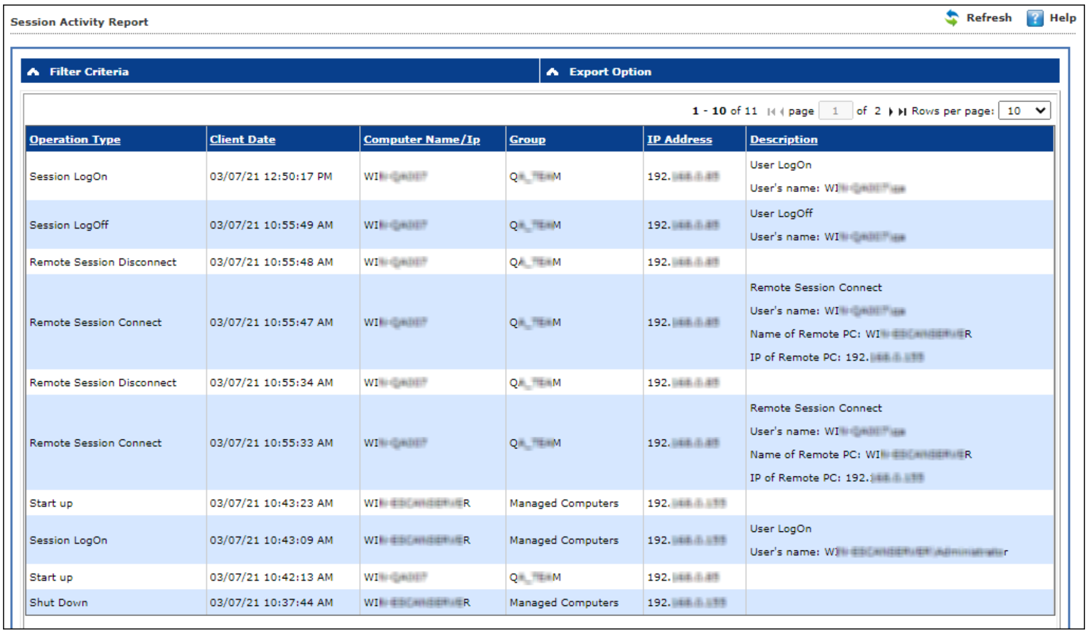
# Session Activity Report

This sub module monitors and logs the session activity of the managed computers. It displays a report of the Operation type, Date, Computer name, Group, IP address and event description. With this report the administrator can trace the user Logon and Logoff activity along with remote sessions that took place on all managed computers.

## Viewing Session Activity Log

In the navigation panel, click **User Activity** > **Session Activity Report**.

The log displays list of session activities and type of operation performed. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

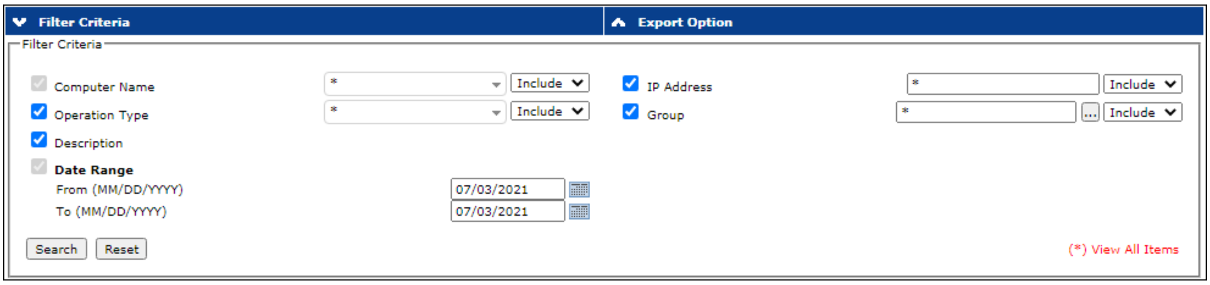


| Operation Type | Client Date | Computer Name/Ip | Group | IP Address | Description |
|---|---|---|---|---|---|
| Session LogOn | 03/07/21 12:50:17 PM | WI[redacted] | QA_[redacted]M | 192.[redacted] | User LogOn<br>User's name: WI[redacted] |
| Session LogOff | 03/07/21 10:55:49 AM | WI[redacted] | QA_[redacted]M | 192.[redacted] | User LogOff<br>User's name: WI[redacted] |
| Remote Session Disconnect | 03/07/21 10:55:48 AM | WI[redacted] | QA_[redacted]M | 192.[redacted] | |
| Remote Session Connect | 03/07/21 10:55:47 AM | WI[redacted] | QA_[redacted]M | 192.[redacted] | Remote Session Connect<br>User's name: WI[redacted]<br>Name of Remote PC: WI[redacted]R<br>IP of Remote PC: 192.[redacted] |
| Remote Session Disconnect | 03/07/21 10:55:34 AM | WI[redacted] | QA_[redacted]M | 192.[redacted] | |
| Remote Session Connect | 03/07/21 10:55:33 AM | WI[redacted] | QA_[redacted]M | 192.[redacted] | Remote Session Connect<br>User's name: WI[redacted]<br>Name of Remote PC: WI[redacted]R<br>IP of Remote PC: 192.[redacted] |
| Start up | 03/07/21 10:43:23 AM | WI[redacted]R | Managed Computers | 192.[redacted] | |
| Session LogOn | 03/07/21 10:43:09 AM | WI[redacted]R | Managed Computers | 192.[redacted] | User LogOn<br>User's name: W[redacted]r |
| Start up | 03/07/21 10:42:13 AM | WI[redacted] | QA_[redacted]M | 192.[redacted] | |
| Shut Down | 03/07/21 10:37:44 AM | WI[redacted]R | Managed Computers | 192.[redacted] | |

## Filtering Session Activity Log

To filter session activities, click **Filter Criteria** field.

Filter Criteria field expands.



| | | | | | |
|---|---|---|---|---|---|
| ☑ Computer Name | * | Include | ☑ IP Address | * | Include |
| ☑ Operation Type | * | Include | ☑ Group | * | Include |
| ☑ Description | | | | | |
| ☑ **Date Range** | | | | | |
| From (MM/DD/YYYY) | 07/03/2021 | | | | |
| To (MM/DD/YYYY) | 07/03/2021 | | | | |

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

**Computer Name**

Click the drop-down and select the preferred computers.

**Operation Type**
Click the drop-down and select the preferred activities.

**Include/Exclude**
Selecting **Include/Exclude** for a parameter lets you include or exclude it from the log.

**Description**
Select this checkbox to display the description of the session in the report.

**IP Address**
Enter the IP address in this field.

**Group**

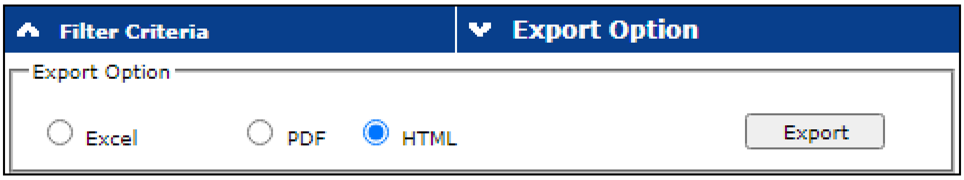
Enter the group's name or click ... and select a group.

**Date Range**
To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the **calendar** icon and select **From** and **To** dates.

After filling all fields, click **Search**.
Reset all filter criteria fields, click **Reset.**

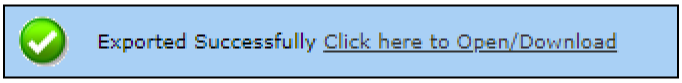
# Exporting Session Activity Report

To export the generated log, click **Export Option**.
Export Option field expands.



○ Excel ○ PDF ● HTML

Select the preferred option and then click **Export**.
A success message appears.



Exported Successfully Click here to Open/Download

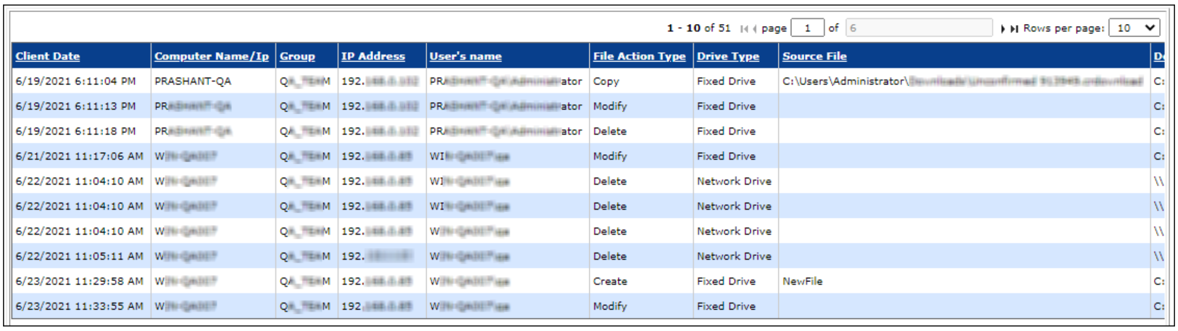
Click the link to open/download the file.

# File Activity Report

The File Activity sub module displays a report of the files created, copied, modified, and deleted on managed computers. The File Activity report will be generated when Record files copied is enabled in endpoint security. Additionally in case of a misuse of any official files can be tracked down to the user through the details captured in the report. Select and filter the report based on any of the details captured.

## Viewing File Activity Log

In the navigation panel, click **User Activity** > **File Activity Report**.
The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

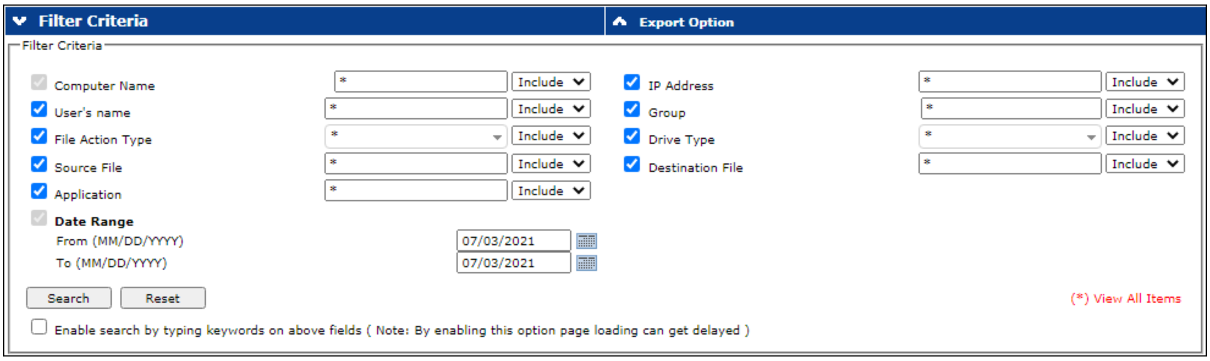


1 - 10 of 51 |◀ ◀ page 1 of 6 ▶ ▶| Rows per page: 10

| Client Date | Computer Name/Ip | Group | IP Address | User's name | File Action Type | Drive Type | Source File | D |
|---|---|---|---|---|---|---|---|---|
| 6/19/2021 6:11:04 PM | PRASHANT-QA | Q[redacted]M | 192.[redacted] | PR[redacted]ator | Copy | Fixed Drive | C:\Users\Administrator\[redacted] | C: |
| 6/19/2021 6:11:13 PM | PR[redacted] | Q[redacted]M | 192.[redacted] | PR[redacted]ator | Modify | Fixed Drive | | C: |
| 6/19/2021 6:11:18 PM | PR[redacted] | Q[redacted]M | 192.[redacted] | PR[redacted]ator | Delete | Fixed Drive | | C: |
| 6/21/2021 11:17:06 AM | W[redacted] | Q[redacted]M | 192.[redacted] | WI[redacted] | Modify | Fixed Drive | | C: |
| 6/22/2021 11:04:10 AM | W[redacted] | Q[redacted]M | 192.[redacted] | WI[redacted] | Delete | Network Drive | | \\ |
| 6/22/2021 11:04:10 AM | W[redacted] | Q[redacted]M | 192.[redacted] | WI[redacted] | Delete | Network Drive | | \\ |
| 6/22/2021 11:04:10 AM | W[redacted] | Q[redacted]M | 192.[redacted] | W[redacted] | Delete | Network Drive | | \\ |
| 6/22/2021 11:05:11 AM | W[redacted] | Q[redacted]M | 192.[redacted] | W[redacted] | Delete | Network Drive | | \\ |
| 6/23/2021 11:29:58 AM | W[redacted] | Q[redacted]M | 192.[redacted] | W[redacted] | Create | Fixed Drive | NewFile | C: |
| 6/23/2021 11:33:55 AM | W[redacted] | Q[redacted]M | 192[redacted] | W[redacted] | Modify | Fixed Drive | | C: |

## Filtering File Activity Log

To filter file activities, click **Filter Criteria** field.
Filter Criteria field expands.



Filter Criteria | Export Option

Filter Criteria

| | | | | | |
|---|---|---|---|---|---|
| ☑ Computer Name | * | Include | ☑ IP Address | * | Include |
| ☑ User's name | * | Include | ☑ Group | * | Include |
| ☑ File Action Type | * | Include | ☑ Drive Type | * | Include |
| ☑ Source File | * | Include | ☑ Destination File | * | Include |
| ☑ Application | * | Include | | | |

☑ **Date Range**
From (MM/DD/YYYY) 07/03/2021
To (MM/DD/YYYY) 07/03/2021

Search | Reset

(*) View All Items

□ Enable search by typing keywords on above fields ( Note: By enabling this option page loading can get delayed )

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

### Computer Name

Click the drop-down and select the preferred computers.

### Username

Enter the username of the computer.

### File Action type

Click the drop-down and select a preferred file action.

**Source File**
Enter the source file's name.

**Application**
Enter an application's name.

**Include/Exclude**
Selecting **Include/Exclude** for a parameter lets you include or exclude it from the log.

**IP Address**
Enter an IP address.

**Group**
Enter the group's name or click … and select a group.

**Drive Type**
Click the drop-down and select the drive type.

**Destination File**
Enter the file path.

**Date Range**
To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the **calendar** icon and select **From** and **To** dates.

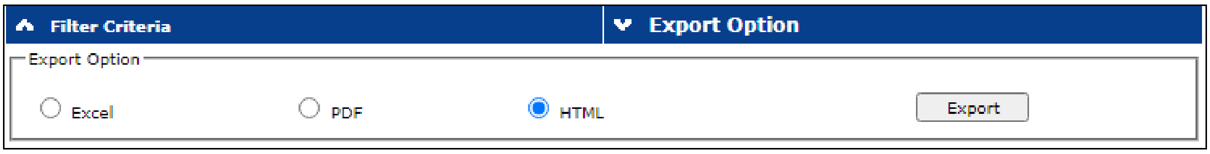
After filling all fields, click **Search**.
Reset all filter criteria fields, click **Reset.**

This checkbox **Enable search by typing keywords on above fields** allows you to search by typing keywords.

| | |
|---|---|
| **NOTE** | Select **"Enable search by typing keywords on above fields"** option page loading can get delayed. |

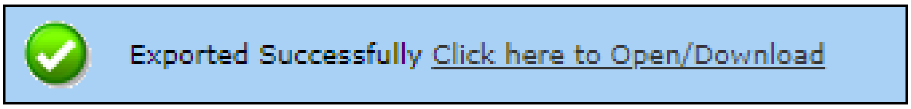
## Exporting File activity Report

To export the generated report, click **Export Option**.
Export Option field expands.



○ Excel ○ PDF ● HTML

Select the preferred option and then click **Export**.
A success message appears.



Exported Successfully Click here to Open/Download

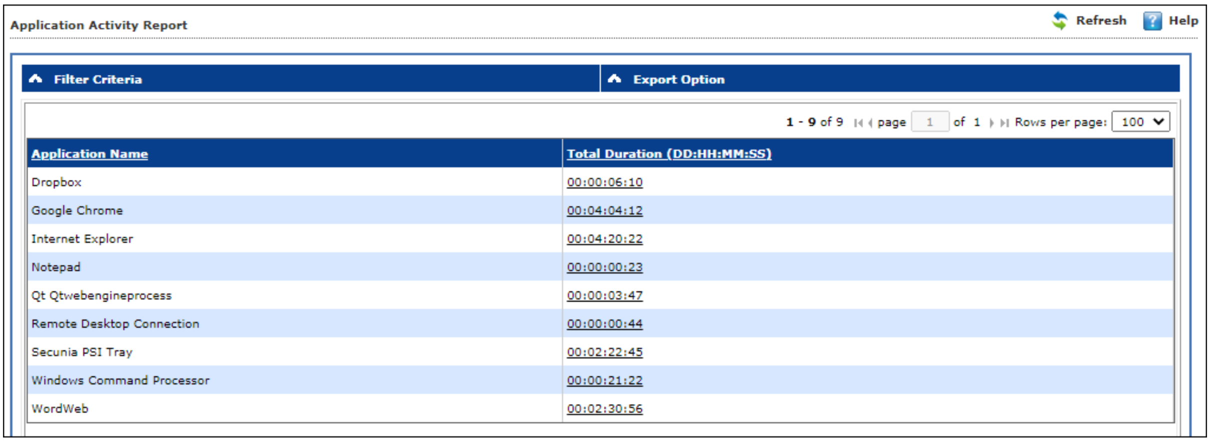
Click the link to open/download the file.

# Application Access Report

The Application Access Report sub module gives the detailed view of all the applications accessed by the computers in the Managed Computers.

## Viewing Application Access Report

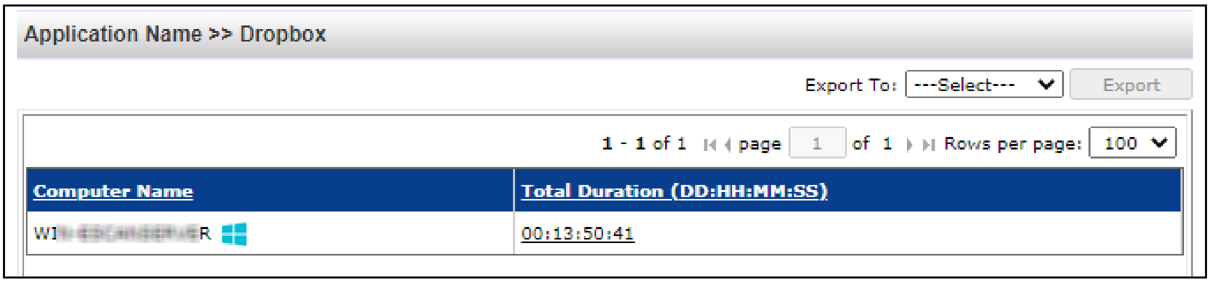
In the navigation panel, click **User Activity** > **Application Access Report**.
The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.



Application Activity Report

| Application Name | Total Duration (DD:HH:MM:SS) |
|---|---|
| Dropbox | 00:00:06:10 |
| Google Chrome | 00:04:04:12 |
| Internet Explorer | 00:04:20:22 |
| Notepad | 00:00:00:23 |
| Qt Qtwebengineprocess | 00:00:03:47 |
| Remote Desktop Connection | 00:00:00:44 |
| Secunia PSI Tray | 00:02:22:45 |
| Windows Command Processor | 00:00:21:22 |
| WordWeb | 00:02:30:56 |

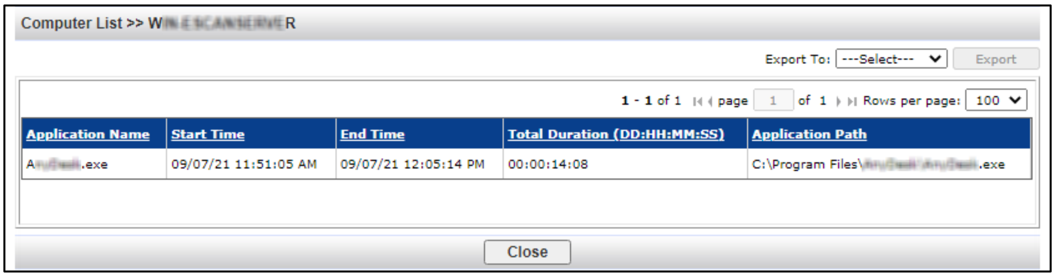
By clicking on the duration present under **Total Duration (DD:HH:MM:SS)** column, you will get the details of the computer name accessed the app and duration.



Application Name >> Dropbox

| Computer Name | Total Duration (DD:HH:MM:SS) |
|---|---|
| WI[redacted]R | 00:13:50:41 |

Again, if you click on the duration, you will get detailed view of the app accessed by the computer along with the date, time, and application path.



Computer List >> W[redacted]R

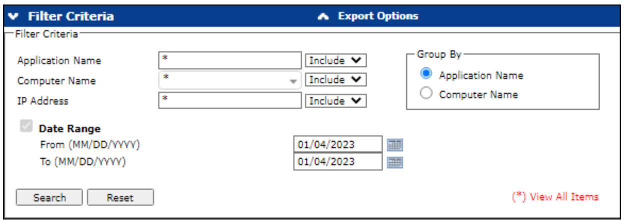
| Application Name | Start Time | End Time | Total Duration (DD:HH:MM:SS) | Application Path |
|---|---|---|---|---|
| A[redacted].exe | 09/07/21 11:51:05 AM | 09/07/21 12:05:14 PM | 00:00:14:08 | C:\Program Files\[redacted].exe |

You can export this report in various format such as PDF, CSV, and HTML.

## Filtering Application Access Report

To filter file activities, click **Filter Criteria** field.

Filter Criteria field expands.



Filter Criteria | Export Options

Filter Criteria

| | | |
|---|---|---|
| Application Name | * | Include |
| Computer Name | * | Include |
| IP Address | * | Include |

Group By
● Application Name
○ Computer Name

☑ Date Range
From (MM/DD/YYYY) 01/04/2023
To (MM/DD/YYYY) 01/04/2023

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

**Application Name**
Entering the Application name displays suggestions. Select the appropriate application.

**Computer Name**
Click the drop-down and select the preferred computer(s).

**IP Address**
Enter the IP address in this field.

**Include/Exclude**
Selecting **Include/Exclude** for a parameter lets you include or exclude it from the log.

**Group By**
The results can be grouped by Application name or Computer name.

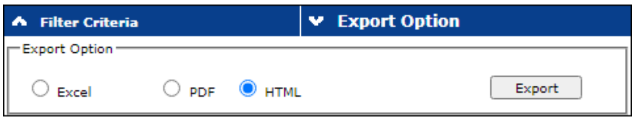
**Date Range**
To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

After entering data in all fields, click **Search**.
The Application Access Report will be filtered according to your preferences.

Reset all filter criteria fields, click **Reset.**

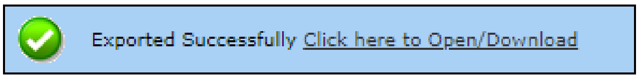
# Exporting Application Access Report

To export the generated report, click **Export Option**.
Export Option field expands.



Export Option
○ Excel ○ PDF ● HTML

Select the preferred option and then click **Export**.
A success message appears.



Exported Successfully Click here to Open/Download

Click the link to open/download the file.

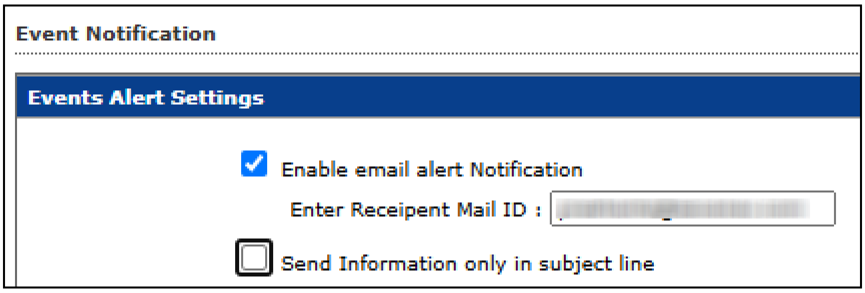
# Notifications

This module lets you configure notifications for different actions/incidents that occur on the server. The Notifications module consists following sub modules:

- **Event Alert**
- **Unlicensed Move Alert**

## Event Alert

This sub module lets you enable email notifications about any event that occurs on the client computers connected to the server.



Event Notification

Events Alert Settings

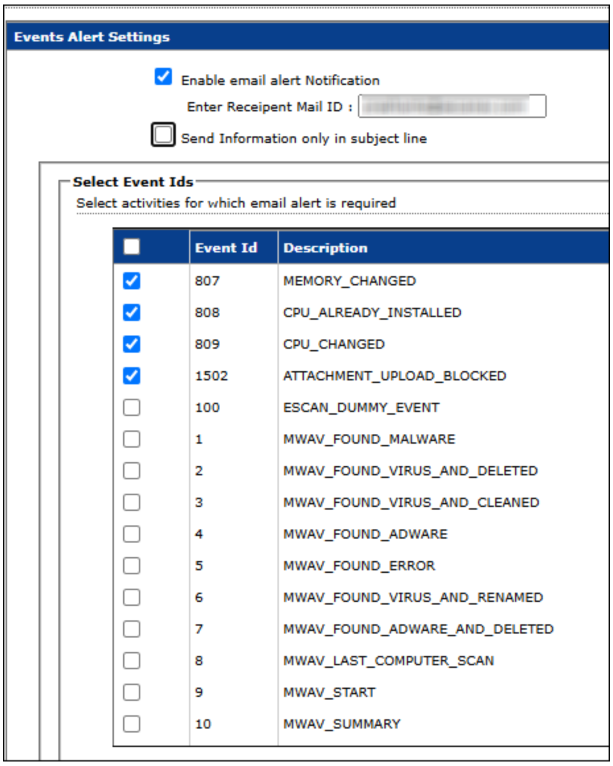
☑ Enable email alert Notification

Enter Receipent Mail ID : [redacted]

☐ Send Information only in subject line

To enable the event alert,

1. In the navigation panel, click **Notifications** > **Event Alert**.
2. Select the checkbox **Enable email alert Notification**.
3. Select the checkbox **Send Information only in subject line**.
   This checkbox enable after selecting enable email alert notification.
4. Select the events from the list for which you prefer an alert.



Events Alert Settings

☑ Enable email alert Notification

Enter Receipent Mail ID : [redacted]

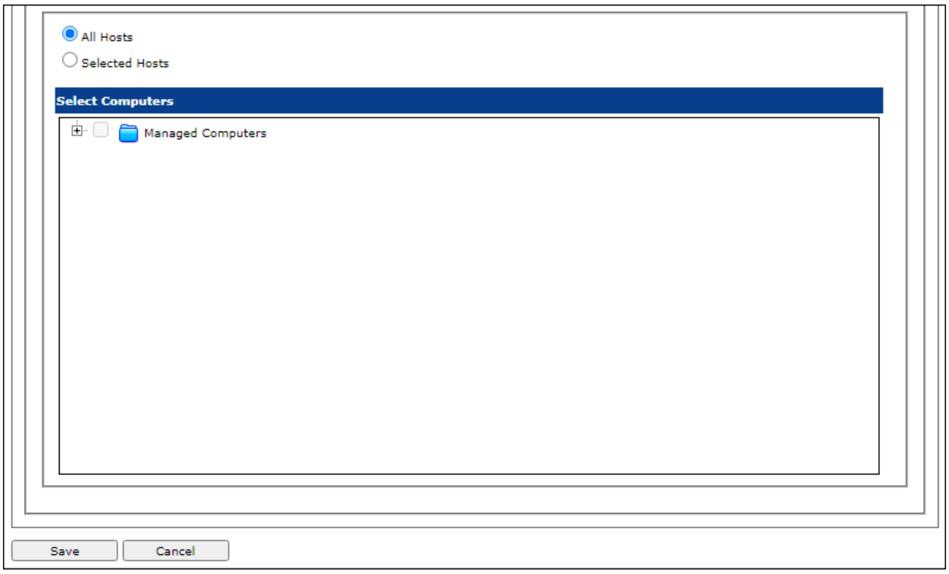
☐ Send Information only in subject line

Select Event Ids

Select activities for which email alert is required

| ☐ | Event Id | Description |
|---|---|---|
| ☑ | 807 | MEMORY_CHANGED |
| ☑ | 808 | CPU_ALREADY_INSTALLED |
| ☑ | 809 | CPU_CHANGED |
| ☑ | 1502 | ATTACHMENT_UPLOAD_BLOCKED |
| ☐ | 100 | ESCAN_DUMMY_EVENT |
| ☐ | 1 | MWAV_FOUND_MALWARE |
| ☐ | 2 | MWAV_FOUND_VIRUS_AND_DELETED |
| ☐ | 3 | MWAV_FOUND_VIRUS_AND_CLEANED |
| ☐ | 4 | MWAV_FOUND_ADWARE |
| ☐ | 5 | MWAV_FOUND_ERROR |
| ☐ | 6 | MWAV_FOUND_VIRUS_AND_RENAMED |
| ☐ | 7 | MWAV_FOUND_ADWARE_AND_DELETED |
| ☐ | 8 | MWAV_LAST_COMPUTER_SCAN |
| ☐ | 9 | MWAV_START |
| ☐ | 10 | MWAV_SUMMARY |

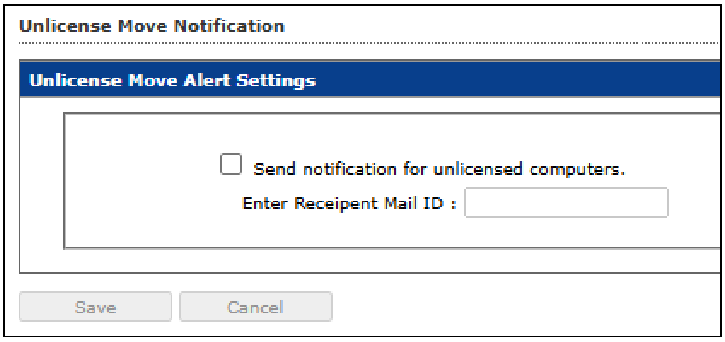
5. Select the required hosts or group.



6. Click **Save.**
   The Event Alert Settings will be saved.

# Unlicensed Move Alert

This sub module lets you enable notification alert when a computer automatically moves to Unlicensed Computers category based on the setting done (under events and computers) for the computer which is not connected to the server for a long time.



Unlicense Move Notification

Unlicense Move Alert Settings

□ Send notification for unlicensed computers.

Enter Receipent Mail ID :

To enable the unlicensed move alert, follow the steps given below:

1. In the navigation panel, click **Notifications** > **Unlicensed Move Alert**.
2. Select the checkbox **Send notification for unlicensed computers**.
3. Click **Save**.
   The Unlicensed Move Alert Settings will be saved.

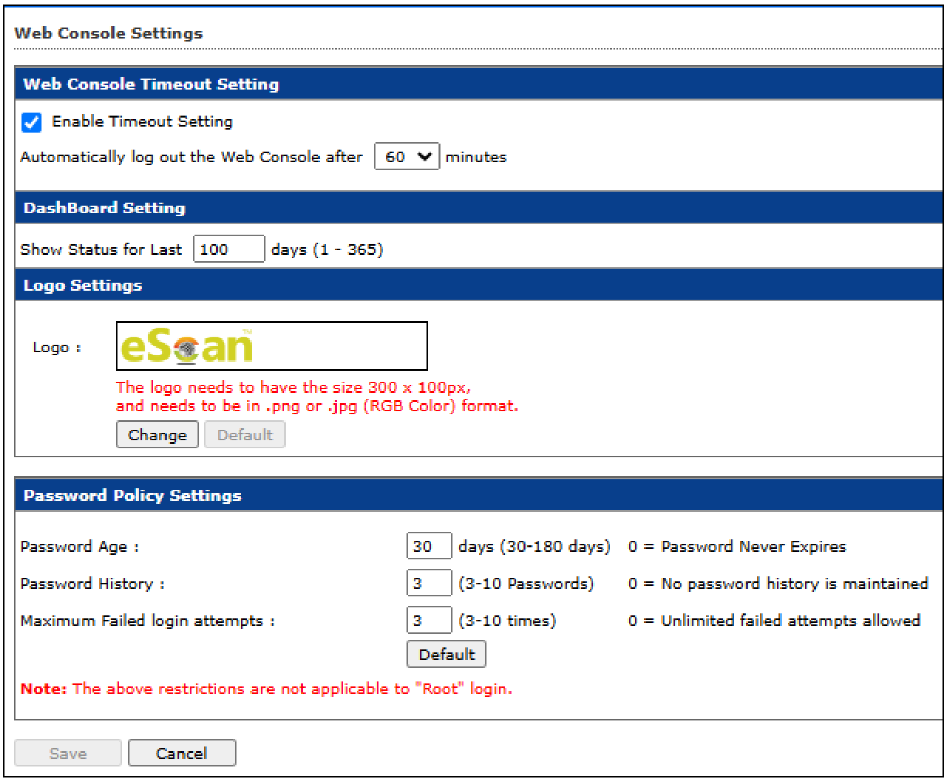
# Settings

The Settings module lets you configure general settings. It contains following sub modules.

- **Web Console Settings**: This sub module lets you define settings for web console timeout, Dashboard Settings, Login Page settings, SQL Server Connection settings, SQL Database compression settings.
- **Excluded Clients:** The Exclude Client module lets you configure the client list to exclude it from auto isolation.
- **Two-Factor Authentication**: This sub module lets you add extra layer of protection to your endpoints.

# Web Console Settings

Web Console Settings sub module lets you configure web console Timeout, Dashboard, Login Page, SQL Server Connection, SQL Database compression and Password Policy Setting.



Web Console Settings

**Web Console Timeout Setting**

☑ Enable Timeout Setting

Automatically log out the Web Console after 60 minutes

**DashBoard Setting**

Show Status for Last 100 days (1 - 365)

**Logo Settings**

Logo :

The logo needs to have the size 300 x 100px,
and needs to be in .png or .jpg (RGB Color) format.

Change Default

**Password Policy Settings**

| | | | |
|---|---|---|---|
| Password Age : | 30 | days (30-180 days) | 0 = Password Never Expires |
| Password History : | 3 | (3-10 Passwords) | 0 = No password history is maintained |
| Maximum Failed login attempts : | 3 | (3-10 times) | 0 = Unlimited failed attempts allowed |

Default

Note: The above restrictions are not applicable to "Root" login.

Save Cancel

### Web Console Timeout Settings

To enable web console Timeout, select **Enable Timeout Setting** option.
After selecting the checkbox, click the drop-down and select the preferred duration.

### Dashboard Setting

This setting lets you set number of days for which you wish to View the Status, Statistics and Protection Status Charts in the Dashboard. Enter the preferred number of days.

### Logo Settings

This setting allows you to add the organization logo in PNG or JPEG format. So the console and reports will have the uploaded logo for customization. To have the default eScan logo, click **Default**. To have customized logo, click **Change**.

### Password Policy Settings

This setting allows the admin to configure the password settings for other users.

- **Password Age**: Enter the preferred value (between 30-180); this will prompt user to reset the password after specified number of days. Here, 0 indicates that password never expires.
- **Password History**: Enter the preferred value (between 3-10); this maintains the password history for specified count. Here, 0 indicates, no password history is maintained.
- **Maximum Failed login attempts**: Enter the preferred value (between 3-10); this will restrict the user from logging after specified attempts. Here, 0 indicates unlimited login attempts.

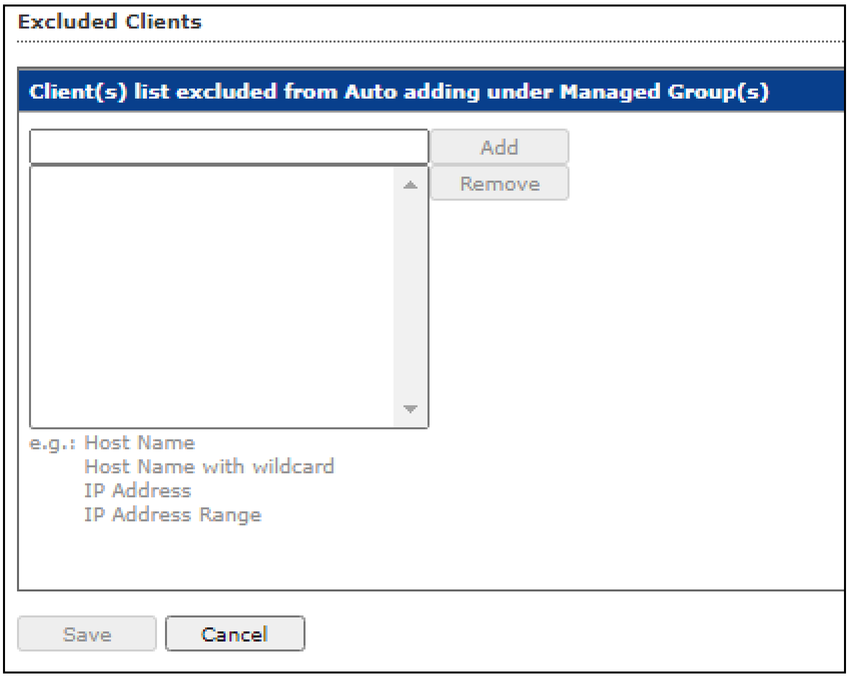
To restore the changes made, click **Default**.

| | |
|---|---|
| ❗<br>**NOTE** | This setting will not be applicable for the root login |

After making the necessary changes, click **Save.**
The web console Settings will be updated.

# Excluded Clients

The Exclude Client module lets you to configure the client list to exclude it from auto isolation.



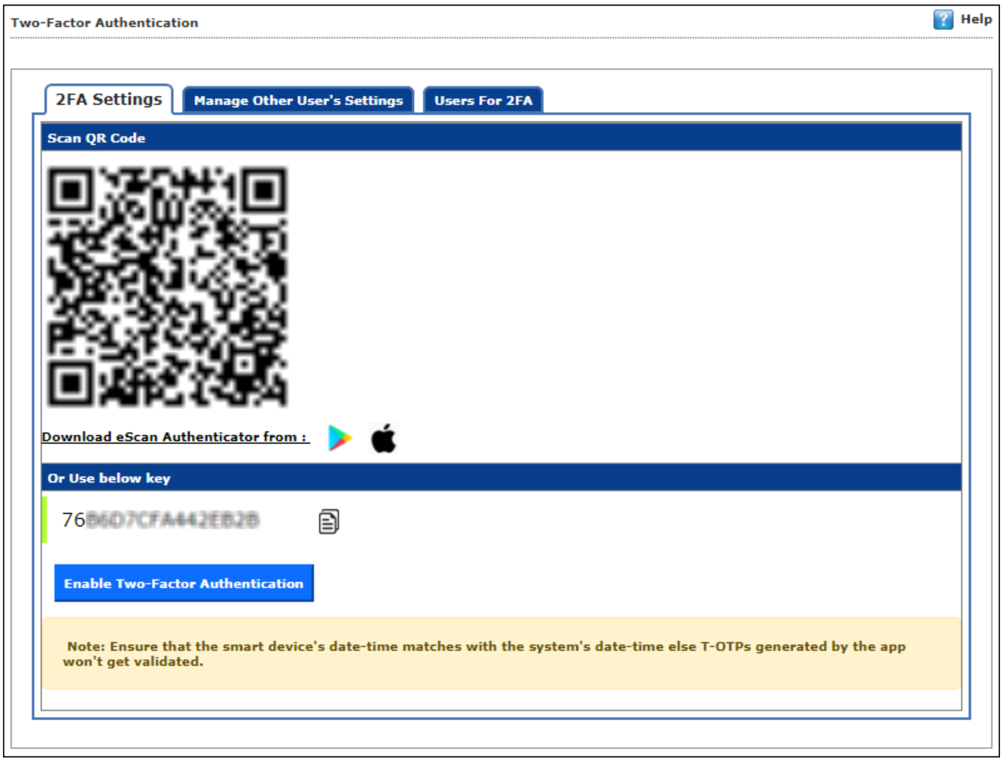
1. You can add/remove clients list to exclude it from auto isolation in the below table. To do the same, refer the following:
    - Enter the host name, IP Address, or IP address range and click **Add**.
    - To delete a particular client, select the client and click **Remove**.
2. After configuring accordingly, click **Save.** Excluded Client Settings will be saved.

# Two-Factor Authentication (2FA)

The system login password is Single-Factor Authentication which is considered unsecure as it may put your organization's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your eScan web console login.

The 2FA feature mandates you to enter a Time-based One-Time Password (TOTP) after entering eScan credentials. So, even if somebody knows your eScan credentials, the 2FA feature secures data against unauthorized logins. Only administrator can enable/disable the 2FA feature. It can also be enabled for added users as well.

To use 2FA login feature, you need to install the **Authenticator** app from Play Store for Android devices or from App Store for iOS devices. The Authenticator app needs camera access for scanning a QR code, so ensure you get an appropriate approval to use device camera in your organization. If a COD or BYOD policy restricts you from using device camera in your organization, enter the **Account Key** in the Authenticator app.


Two-Factor Authentication
Help
2FA Settings
Manage Other User's Settings
Users For 2FA
Scan QR Code
Download eScan Authenticator from :
Or Use below key
Enable Two-Factor Authentication

76[redacted]

Note: Ensure that the smart device's date-time matches with the system's date-time else T-OTPs generated by the app won't get validated.

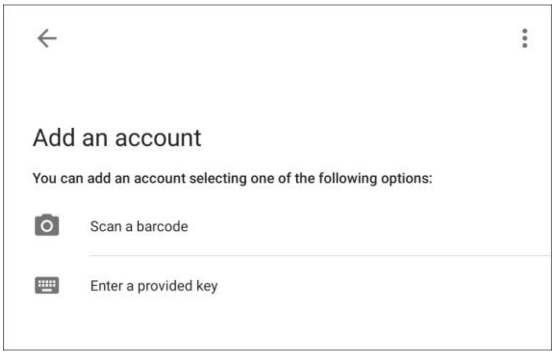
| NOTE | Ensure that the smart device's date and time matches with the system's date and time, else TOTPs generated by app won't get validated. |
|---|---|

| IMPORTANT | We recommend that you save/store the **Account Key** in offline storage or a paperback copy, in case you lose the account access. |
|---|---|

# Enabling 2FA login

To enable 2FA login, follow the steps given below:

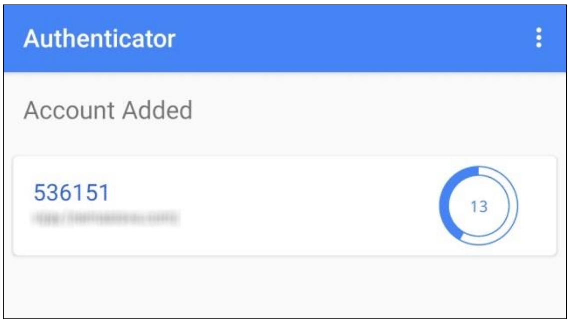
1. Go to **Settings** > **Two-Factor Authentication**.
2. Open the Authenticator app.
   After basic configuration following screen appears on smart device.



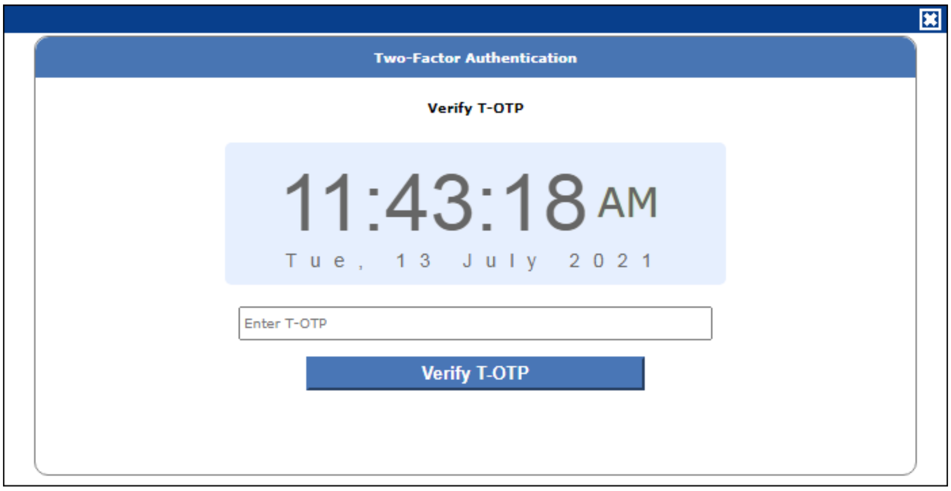
Add an account

You can add an account selecting one of the following options:

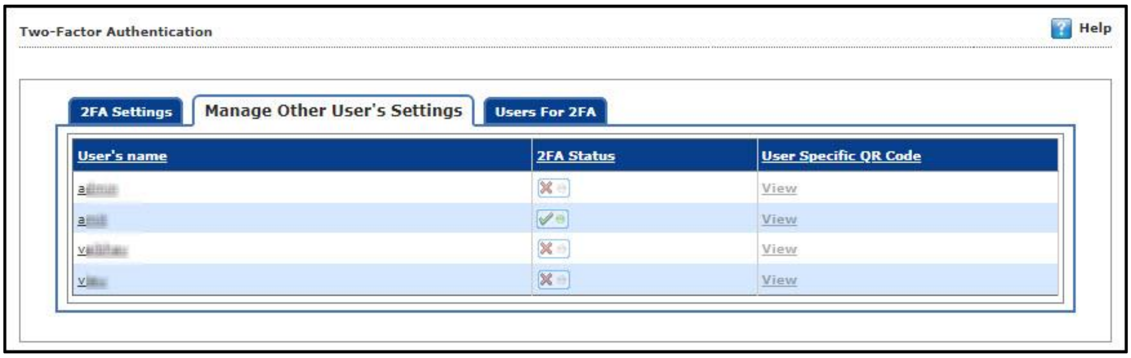
3. Select a preferred option. If you tapped **Scan a barcode**, scan the onscreen QR code via your smart device. If you tapped **Enter a provided key**, enter the Account Key and then tap **ADD**.
   After scanning the Account QR code or entering Account Key the eScan server account gets added to the Authenticator app. The app then starts displaying a Time-based One-Time Password (TOTP) that is valid for 30 seconds.



4. Click **Enable Two-Factor Authentication**.
   Verify TOTP window appears.



5. Enter the TOTP displayed on smart device and then click **Verify TOTP**.
   The 2FA login feature gets enabled.
6. To apply the login feature for specific users, click **Manage Other User Settings** tab. The tab displays list of added users and whether 2FA status is enabled or disabled.
   ✗ - 2FA Disabled
   ✓ - 2FA Enabled



Two-Factor Authentication

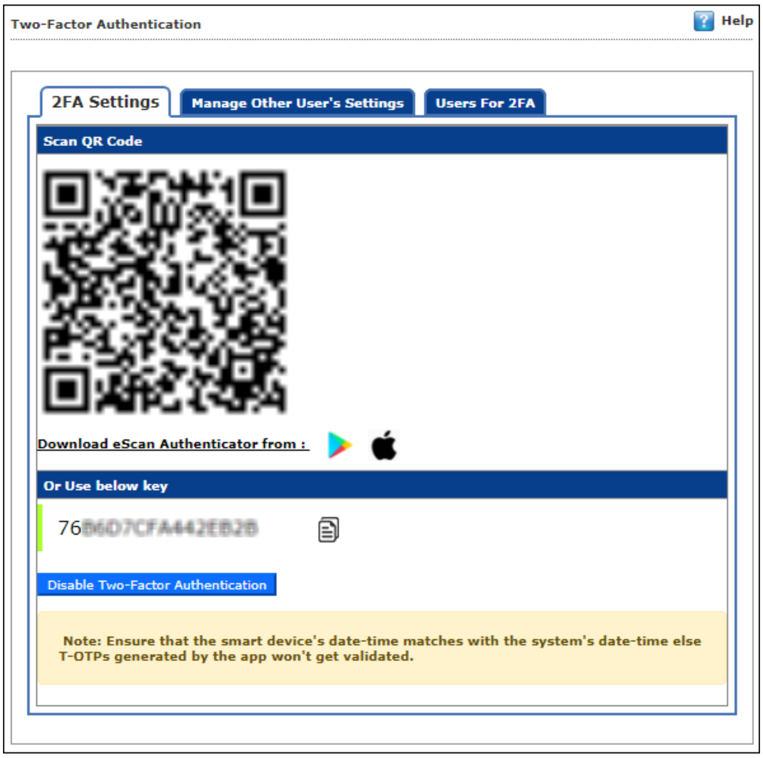
| User's name | 2FA Status | User Specific QR Code |
|---|---|---|
| a[redacted] | ✗ | View |
| a[redacted] | ✓ | View |
| v[redacted] | ✗ | View |
| v[redacted] | ✗ | View |

7. To enable 2FA login for an added user, click the button to check icon.
   The 2FA login for added users gets enabled. After enabling the 2FA login for users, whenever they log in to eScan web console Verify TOTP window appears.
8. To view the QR Code of specific user, click **View** option in the User Specified QR Code column.

# Disabling 2FA login

To disable 2FA login, follow the steps given below:

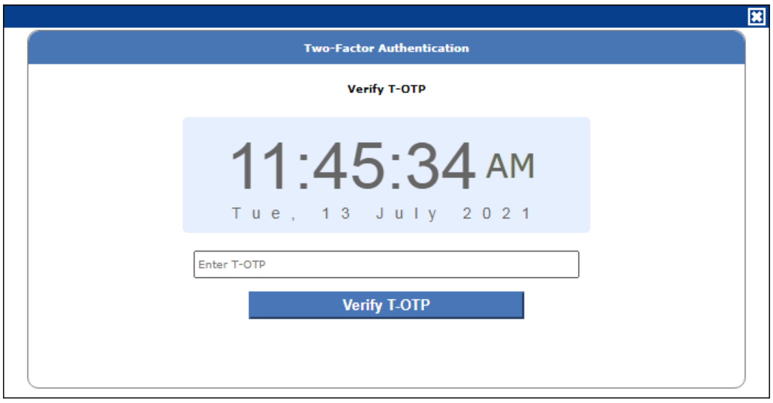
1. Go to **Settings** > **Two Factor Authentication**.
2. Click **Disable Two-Factor Authentication**.


Two-Factor Authentication
Help
2FA Settings
Manage Other User's Settings
Users For 2FA
Scan QR Code
Download eScan Authenticator from :
Or Use below key
Disable Two-Factor Authentication

76[redacted]

Note: Ensure that the smart device's date-time matches with the system's date-time else T-OTPs generated by the app won't get validated.

Verify TOTP window appears.

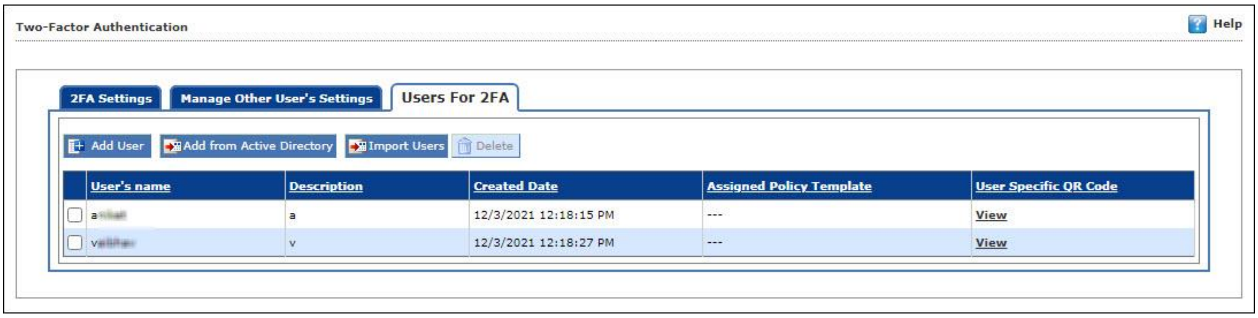


3. Enter the **TOTP** and then click **Verify TOTP**.
   The 2FA feature gets disabled.

| | |
|---|---|
| **NOTE** | After disabling the 2FA feature and enabling it again, the 2FA login status will be reinstated for added users. |

# Users For 2FA

This tab helps to add the users and apply 2FA to the endpoints via policy template. The users can be added directly or from Active directory.



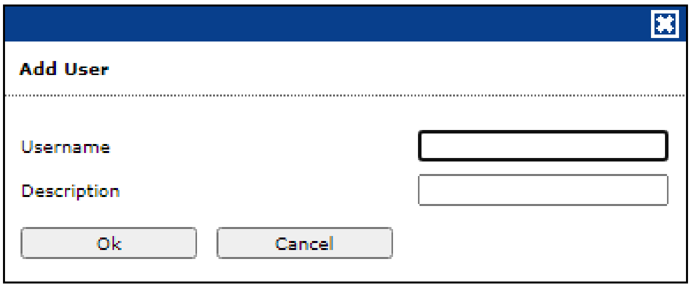
Two-Factor Authentication
Help
2FA Settings
Manage Other User's Settings
Users For 2FA
Add User
Add from Active Directory
Import Users
Delete

| | User's name | Description | Created Date | Assigned Policy Template | User Specific QR Code |
|---|---|---|---|---|---|
| □ | a[redacted] | a | 12/3/2021 12:18:15 PM | --- | View |
| □ | v[redacted] | v | 12/3/2021 12:18:27 PM | --- | View |

# Adding the User

To add users for the same, follow the steps given below:

1. Go to **Settings** > **Two-Factor Authentication** > **Users For 2FA**.
2. Click **Add User**.
   Add User window appears.



3. Enter the **Username** and **Description**.
4. Click **OK**.
   The user will be added for 2FA.

## Importing Users

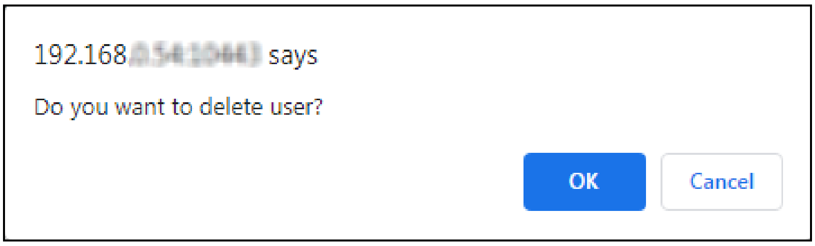
To import the users, follow the steps given below:

1. Go to **Settings** > **Two-Factor Authentication** > **Users For 2FA**.
2. Click **Import Users**.
   Import Users window appears.

## Deleting Users

To delete the users, follow the steps given below:

1. Go to **Settings** > **Two-Factor Authentication** > **Users For 2FA**.
2. Click **Delete**.
   The Confirmation prompt appears.



192.168[redacted] says

Do you want to delete user?

3. Click **OK**.
   The user will be deleted.

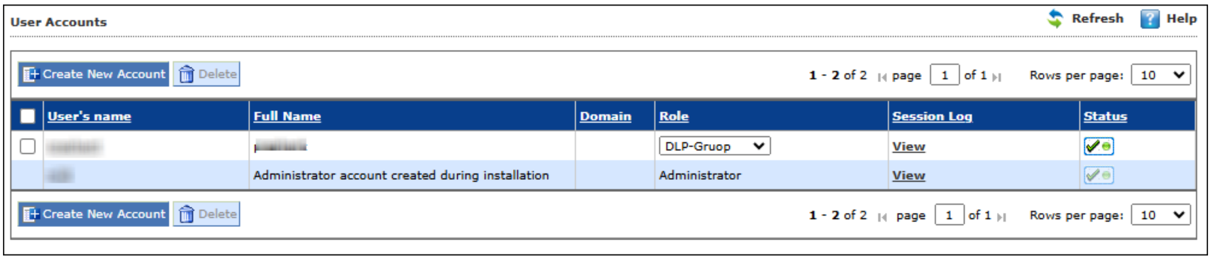
# Administration

The Administration module lets you create User Accounts and allocate them admin rights for using eScan Management Console. In a large organization, installing eScan client on all computers may consume lot of time and efforts. With this option, you can allocate admin rights to the other employees and allow them to install eScan Client, implement Policies and Tasks.
The Administration module consists following sub modules:

- **User Accounts**
- **User Roles**
- **Audit Trail**

# User Accounts

For a large organization, installing eScan Client and monitoring activities may become a difficult task. With User Accounts sub module, you can create new user accounts and assign Administrator role to added users and reduce the workload. This sub module displays a list of users and their details like Domain, Role, Session Log and Status.

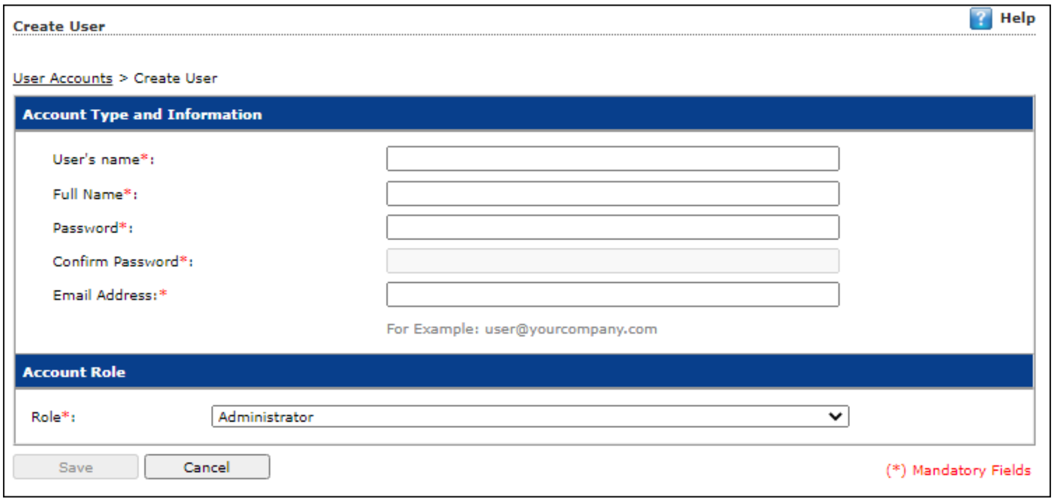


| □ | User's name | Full Name | Domain | Role | Session Log | Status |
|---|---|---|---|---|---|---|
| □ | [redacted] | [redacted] | | DLP-Gruop | View | ✓ |
| | [redacted] | Administrator account created during installation | | Administrator | View | ✓ |

## Create New Account

To create a User Account, follow the steps given below:

1. In the User Accounts screen, click **Create New Account**.
   Create User form appears.

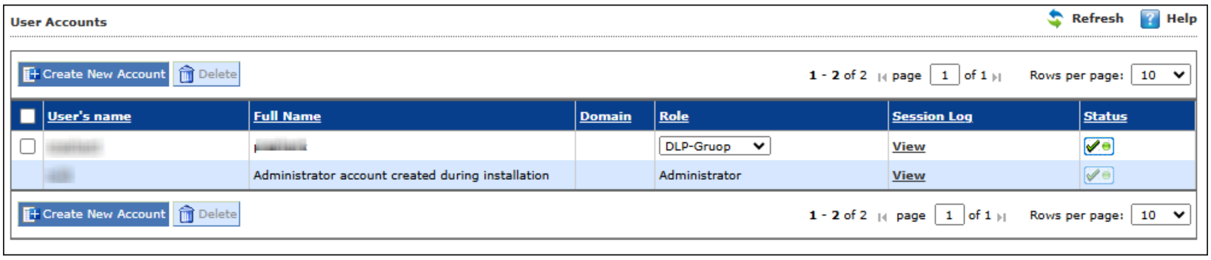


2. From **Account Role** field, click drop-down and assign the role to the account.
3. After filling all the details, click **Save**.
   The user will be added to the User Accounts list.

# Delete a User Account

To delete a user account, follow the steps given below:

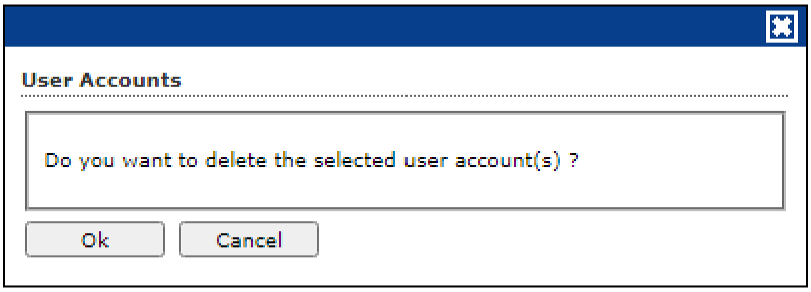
1. In the User Accounts screen, select the user you want to delete.



User Accounts

| ☐ | User's name | Full Name | Domain | Role | Session Log | Status |
|---|---|---|---|---|---|---|
| ☐ | [redacted] | [redacted] |  | DLP-Gruop | View | ✓ |
|  | [redacted] | Administrator account created during installation |  | Administrator | View | ✓ |

2. Click **Delete**.
   A confirmation prompt appears.



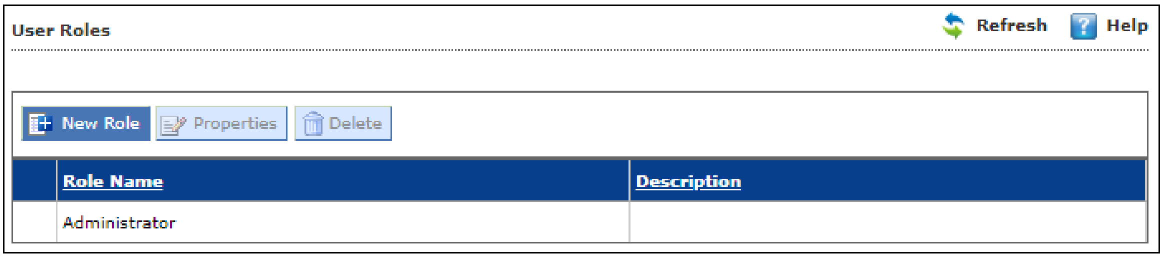
User Accounts

Do you want to delete the selected user account(s) ?

3. Click **OK**.
   The User Account will be deleted.

# User Roles

The User Roles sub module lets you create a role and assign it to the User Accounts with variable permissions and rights as defined in the role being assigned to them. It can be an Administrator role with set of permissions and rights Group Admin Role or a Read only Role.



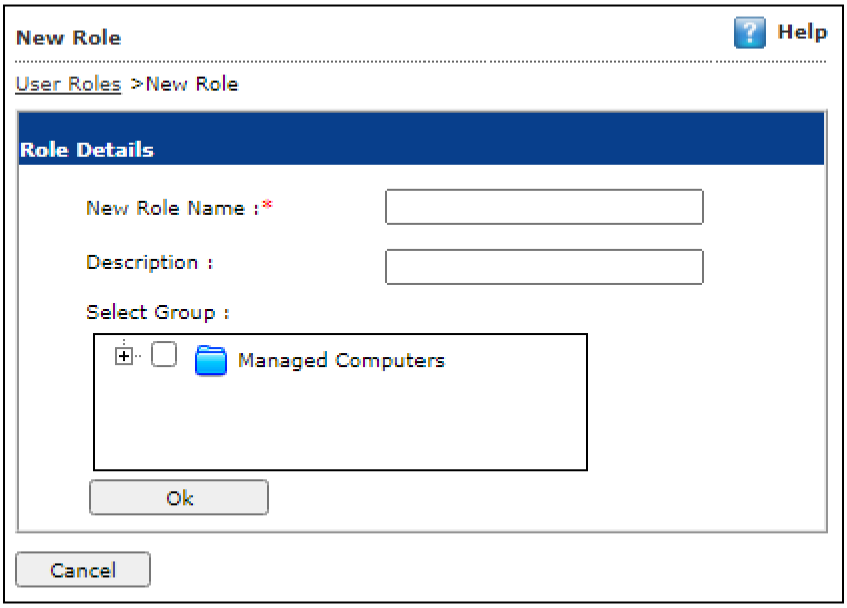
| Role Name | Description |
|---|---|
| Administrator | |

You can re-define the Properties of the created role for configuring access to various section of eScan Management Console and the networked Computers. It also lets you delete any existing role after the task is completed by them. It allows the administrator to give permission to sub administrators to access defined modules of eScan and perform installation/uninstallation of eScan Client on network computers or define policies and tasks for the computers allocated to them.

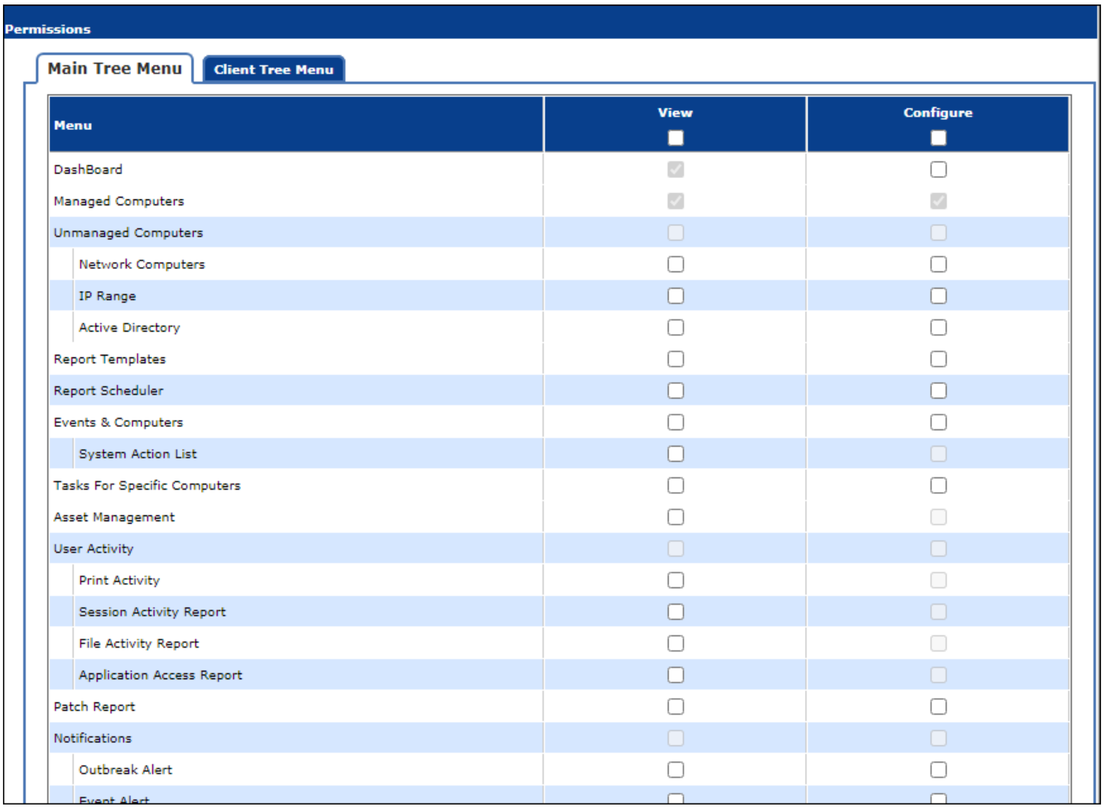
## New Role

To add a user role, follow the steps given below:

1. In the User Roles screen, click **New Role**.
   New Role form appears.



2. Enter name and description for the role.
3. Click **Managed Computers** and select the specific group to assign the role.
   The added role will be able to manage and monitor only the selected group's activities.
4. Click **OK.**
   Permissions section appears displaying Main Tree Menu and Client Tree Menu tabs. The Main Tree Menu consists of Navigation Panel Access permissions while the Client Tree Menu consists of selected groups on which permissions the user is allowed to take further.



Permissions

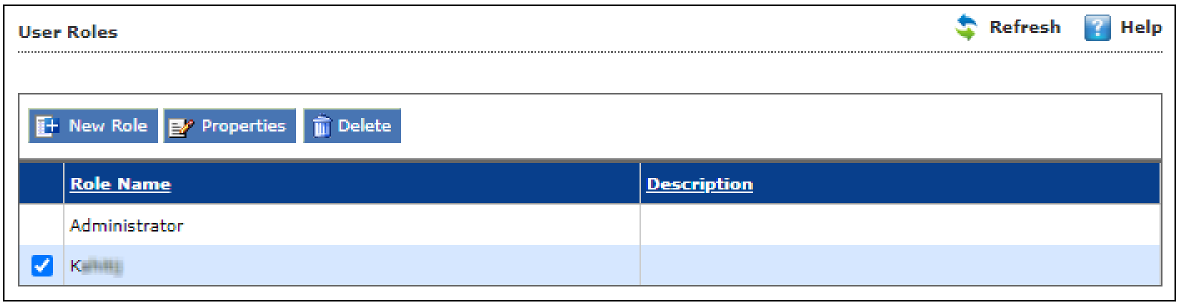
| Menu | View<br>□ | Configure<br>□ |
|---|---|---|
| DashBoard | ☑ | □ |
| Managed Computers | ☑ | ☑ |
| Unmanaged Computers | □ | □ |
| Network Computers | □ | □ |
| IP Range | □ | □ |
| Active Directory | □ | □ |
| Report Templates | □ | □ |
| Report Scheduler | □ | □ |
| Events & Computers | □ | □ |
| System Action List | □ | □ |
| Tasks For Specific Computers | □ | □ |
| Asset Management | □ | □ |
| User Activity | □ | □ |
| Print Activity | □ | □ |
| Session Activity Report | □ | □ |
| File Activity Report | □ | □ |
| Application Access Report | □ | □ |
| Patch Report | □ | □ |
| Notifications | □ | □ |
| Outbreak Alert | □ | □ |
| Event Alert | □ | □ |

5. Select the checkboxes that will allow the role to view/configure the module.
6. After selecting the necessary checkboxes, click **Save**.
   The role will be added to the User Roles list.

# View Role Properties

To view the properties of a role, follow the steps given below:

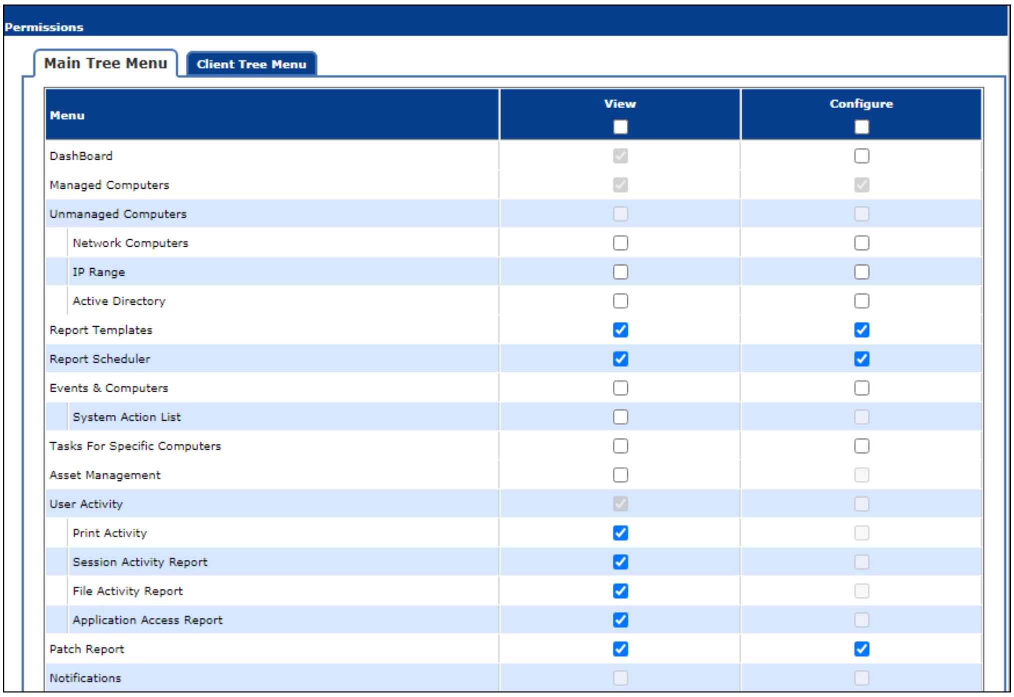
1. In the User Roles screen, select a role.
2. This enables Properties and Delete buttons.



User Roles

| | Role Name | Description |
|---|---|---|
| | Administrator | |
| ☑ | K[illegible] | |

3. Click **Properties**.
   Properties screen appears. It lets you modify role description, permissions for accessing and configuring modules and assign the role to other groups by clicking **Select Group Tree**.



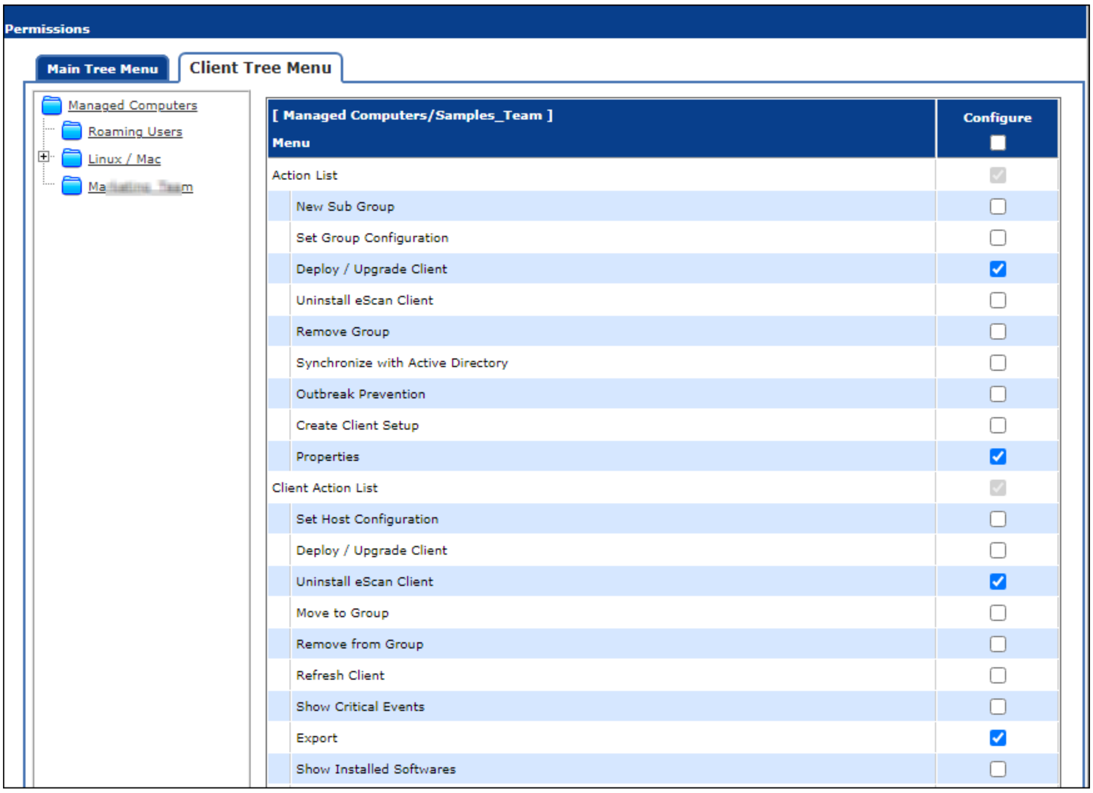
**Permissions**

Main Tree Menu | Client Tree Menu

| Menu | View<br>□ | Configure<br>□ |
|---|---|---|
| DashBoard | ☑ | □ |
| Managed Computers | ☑ | ☑ |
| Unmanaged Computers | □ | □ |
| Network Computers | □ | □ |
| IP Range | □ | □ |
| Active Directory | □ | □ |
| Report Templates | ☑ | ☑ |
| Report Scheduler | ☑ | ☑ |
| Events & Computers | □ | □ |
| System Action List | □ | □ |
| Tasks For Specific Computers | □ | □ |
| Asset Management | □ | □ |
| User Activity | ☑ | □ |
| Print Activity | ☑ | □ |
| Session Activity Report | ☑ | □ |
| File Activity Report | ☑ | □ |
| Application Access Report | ☑ | □ |
| Patch Report | ☑ | ☑ |
| Notifications | □ | □ |

4. To modify client configuration permissions, click **Client Tree Menu**.

   **Client Tree Menu**
   Define the Actions that the created role can configure for the allocated group. The menu has Action List, Client Action List, and Policy Template.



**Permissions**

Main Tree Menu | Client Tree Menu

- Managed Computers
  - Roaming Users
  - Linux / Mac
  - Ma[redacted]m

| [ Managed Computers/Samples_Team ]<br>Menu | Configure<br>□ |
|---|---|
| Action List | ☑ |
| New Sub Group | □ |
| Set Group Configuration | □ |
| Deploy / Upgrade Client | ☑ |
| Uninstall eScan Client | □ |
| Remove Group | □ |
| Synchronize with Active Directory | □ |
| Outbreak Prevention | □ |
| Create Client Setup | □ |
| Properties | ☑ |
| Client Action List | ☑ |
| Set Host Configuration | □ |
| Deploy / Upgrade Client | □ |
| Uninstall eScan Client | ☑ |
| Move to Group | □ |
| Remove from Group | □ |
| Refresh Client | □ |
| Show Critical Events | □ |
| Export | ☑ |
| Show Installed Softwares | □ |

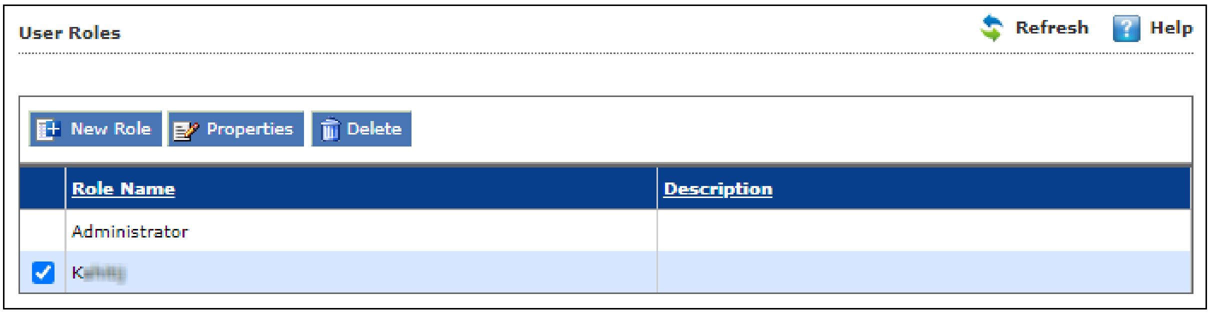
5. To let the role configure these actions, under the Configure column select the checkboxes of corresponding actions.

6. Click **Save**.
   The Role Properties will be updated accordingly.

# Delete a User Role

To delete a user role, follow the steps given below:

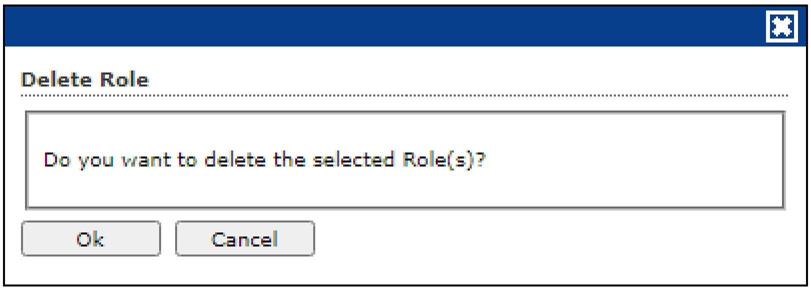
1. In the User Roles screen, select the user role you want to delete**.**



User Roles

| | Role Name | Description |
|---|---|---|
| | Administrator | |
| ☑ | K[redacted] | |

2. Click **Delete**.
   A delete confirmation prompt appears.



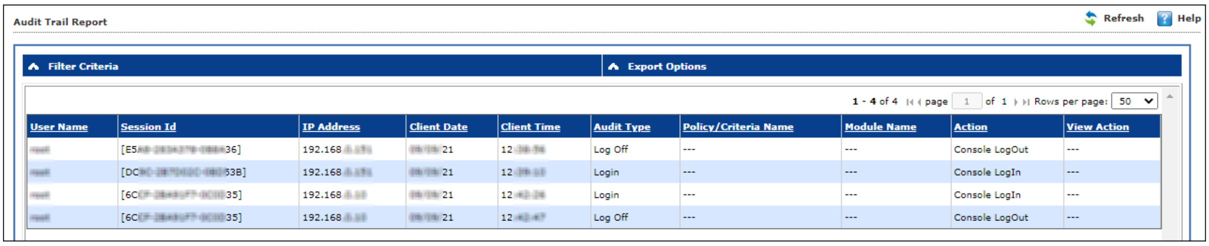
Delete Role

Do you want to delete the selected Role(s)?

3. Click **OK**.
   The User Role will be deleted.

# Audit Trail

The Audit Trail sub module let you record the security relevant data, operation, event, Action, policy updates.  Audit logs are used to track the date, time and activity of each user, including the policy/criteria that have been changed. A record of the changes that have been made to a database. You can get audit trail of user activity across all these systems.

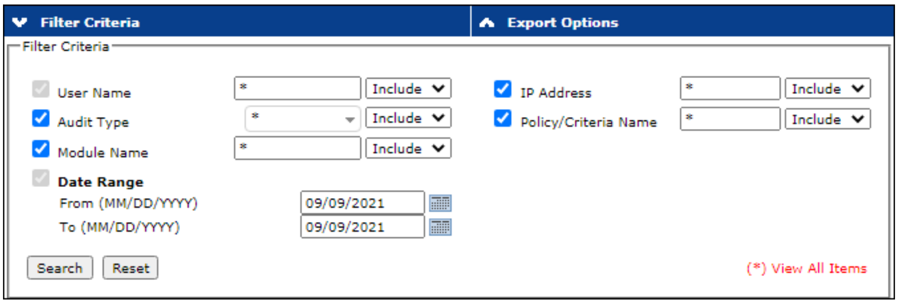


Audit Trail Report

| User Name | Session Id | IP Address | Client Date | Client Time | Audit Type | Policy/Criteria Name | Module Name | Action | View Action |
|---|---|---|---|---|---|---|---|---|---|
| [redacted] | [E5[redacted]36] | 192.168[redacted] | [redacted]21 | 12[redacted] | Log Off | --- | --- | Console LogOut | --- |
| [redacted] | [DC[redacted]53B] | 192.168[redacted] | [redacted]21 | 12[redacted] | Login | --- | --- | Console LogIn | --- |
| [redacted] | [6C[redacted]35] | 192.168[redacted] | [redacted]21 | 12[redacted] | Login | --- | --- | Console LogIn | --- |
| [redacted] | [6C[redacted]35] | 192.168[redacted] | [redacted]21 | 12[redacted] | Log Off | --- | --- | Console LogOut | --- |

## Filter all Audit Trail report

To filter the Audit Trail Report as per your requirements, click **Filter Criteria** field.
Filter Criteria field expands.



Filter Criteria

| | | | | | |
|---|---|---|---|---|---|
| ☑ User Name | * | Include | ☑ IP Address | * | Include |
| ☑ Audit Type | * | Include | ☑ Policy/Criteria Name | * | Include |
| ☑ Module Name | * | Include | | | |
| ☑ **Date Range** | | | | | |
| From (MM/DD/YYYY) | 09/09/2021 | | | | |
| To (MM/DD/YYYY) | 09/09/2021 | | | | |

(*) View All Items

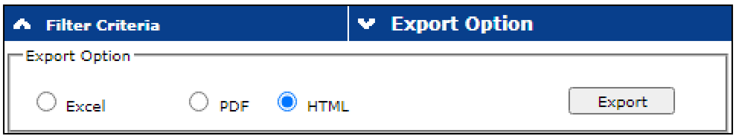
Select the parameters you want to be included in the filtered report.

**Include/Exclude**
Selecting **Include/Exclude** for a parameter lets you include or exclude it from the report.

After making the necessary selections, click **Search.**
The Audit Trail Report will be filtered according to your preferences.

## Exporting Audit Trail

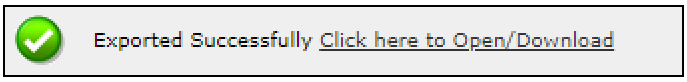
To export the Audit Trail Report, click **Export Option**.
Export Option field expands.



Export Option

○ Excel ○ PDF ● HTML

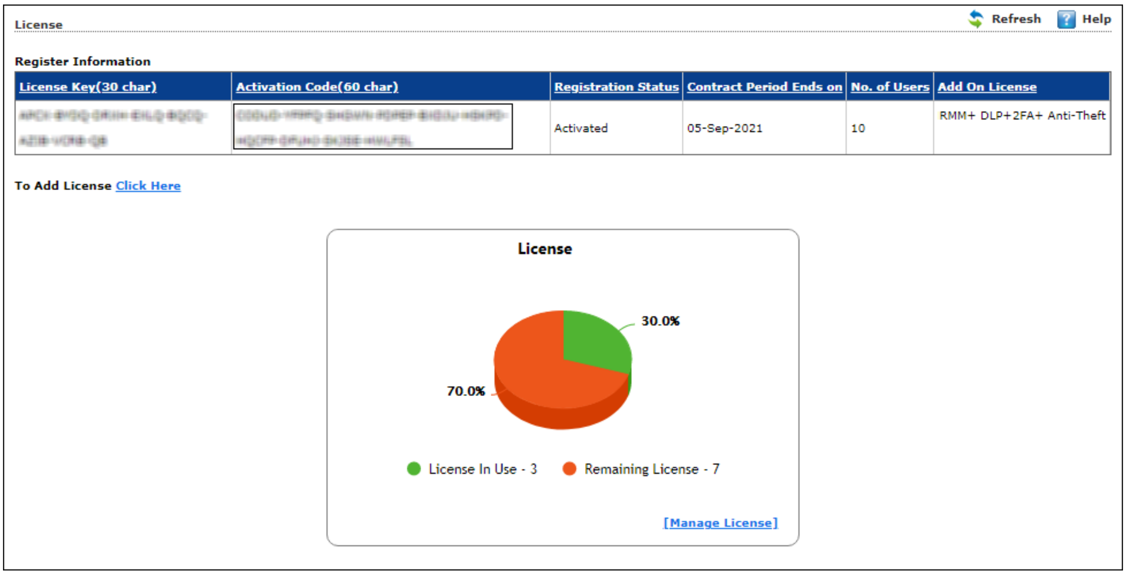
Select the preferred option and then click **Export**.
A success message appears.



Exported Successfully Click here to Open/Download

# License

The License module lets you manage user licenses. You can add, activate, and view the total number of licenses available for deployment, previously deployed, and licenses remaining with their corresponding values. The module also lets you move the licensed computers to non-licensed computers and vice versa. Here you can also view the number of add-on license along with the name of it. For example, as you can see here there are 15 add-on licenses for eBackup feature. The add-on license is available for RMM, 2FA, and DLP features.



License

Register Information

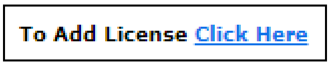
| License Key(30 char) | Activation Code(60 char) | Registration Status | Contract Period Ends on | No. of Users | Add On License |
|---|---|---|---|---|---|
| [redacted] | [redacted] | Activated | 05-Sep-2021 | 10 | RMM+ DLP+2FA+ Anti-Theft |

To Add License Click Here

## Adding and Activating a License

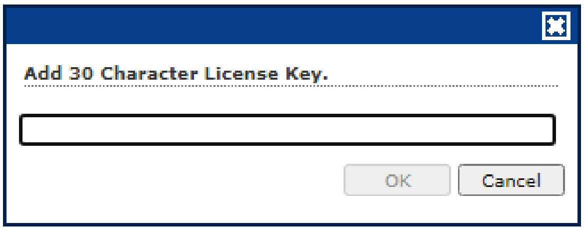
To add and activate a license,

1. In the License screen, click on **Click Here** link.



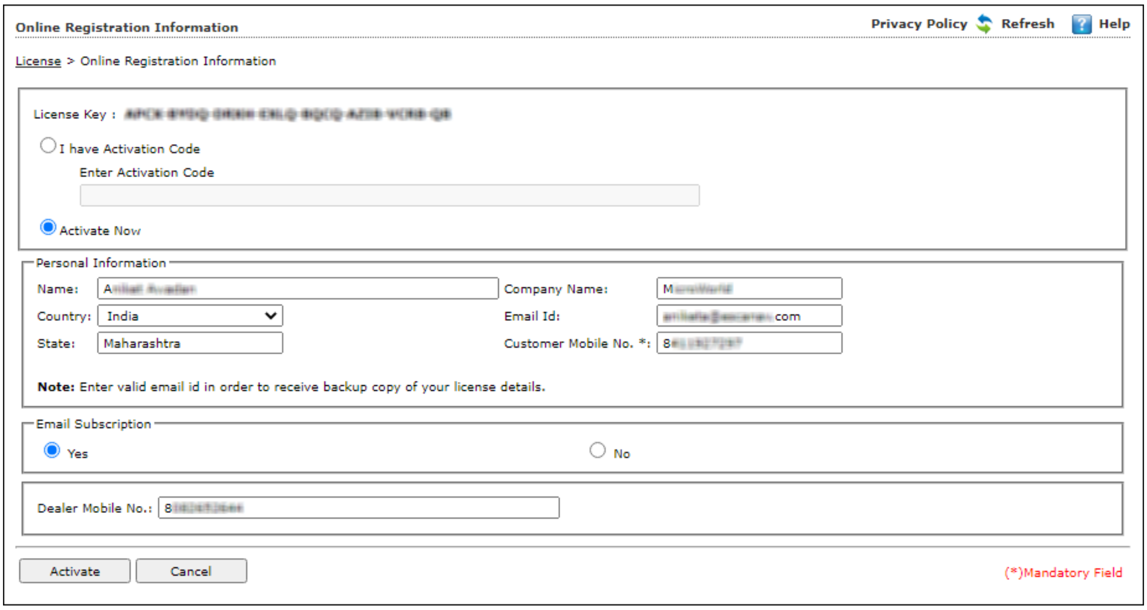
To Add License Click Here

   Add License Key dialog box appears.



Add 30 Character License Key.

2. Enter the license key and then click **OK**.
   The license key will be added and displayed in the **Register Information** table.
3. To activate the added license, click **Activate Now**.
4. Click **Activate now** link displayed in Activation Code column to activate the license key on eScan server system.
   Online Registration Information form appears.



Online Registration Information

Privacy Policy Refresh Help

License > Online Registration Information

License Key : [redacted]

○ I have Activation Code

Enter Activation Code

● Activate Now

Personal Information

| | | | |
|---|---|---|---|
| Name: | A[redacted] | Company Name: | M[redacted] |
| Country: | India | Email Id: | [redacted].com |
| State: | Maharashtra | Customer Mobile No. *: | 8[redacted] |

**Note:** Enter valid email id in order to receive backup copy of your license details.

Email Subscription

● Yes ○ No

Dealer Mobile No.: 8[redacted]

Activate Cancel

(*)Mandatory Field

5. Select a desired option for activation.
6. Enter details in **Personal Information** section.

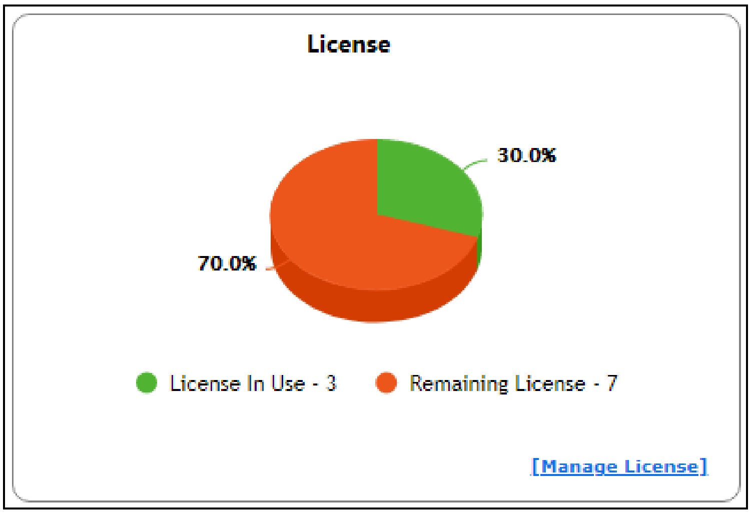
| NOTE | Enter valid email id in order to receive backup copy of your license details. |
|---|---|

7. Select a desired option for **Email Subscription**.
8. Enter the **Dealer Mobile Number**.
9. Click **Activate**. (Ensure that the Internet connection is Active.)

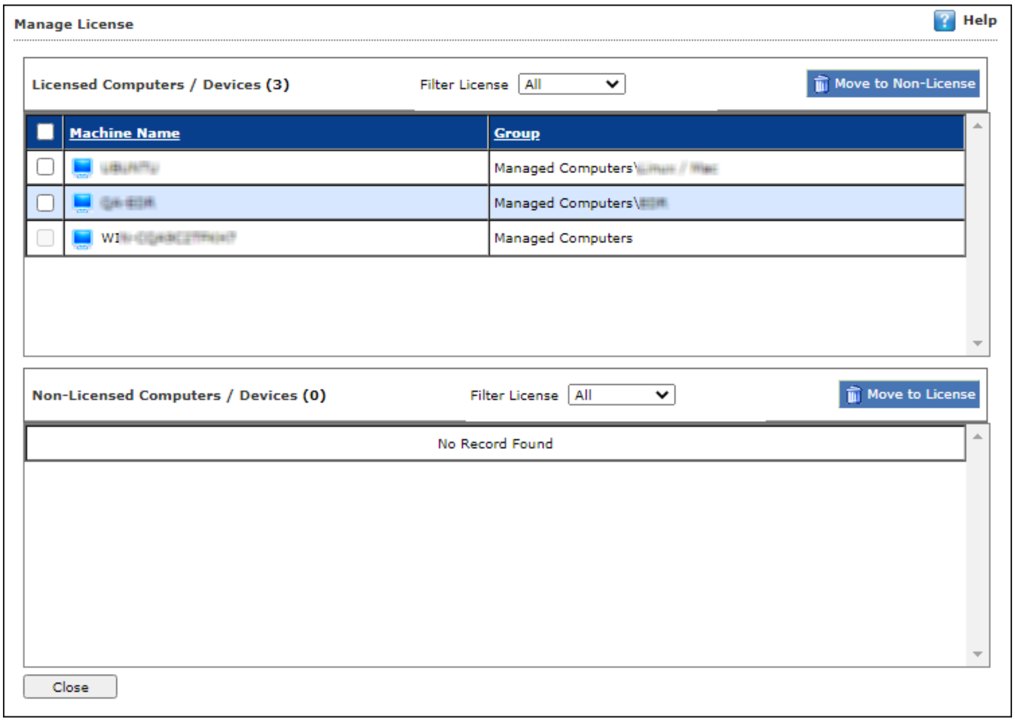
# Moving Licensed Computers to Non-Licensed Computers

To move licensed computers to non-licensed computers,

1. In the License statistics box, click **Manage License**.



Manage License window appears.



Manage License

Licensed Computers / Devices (3)

Filter License: All

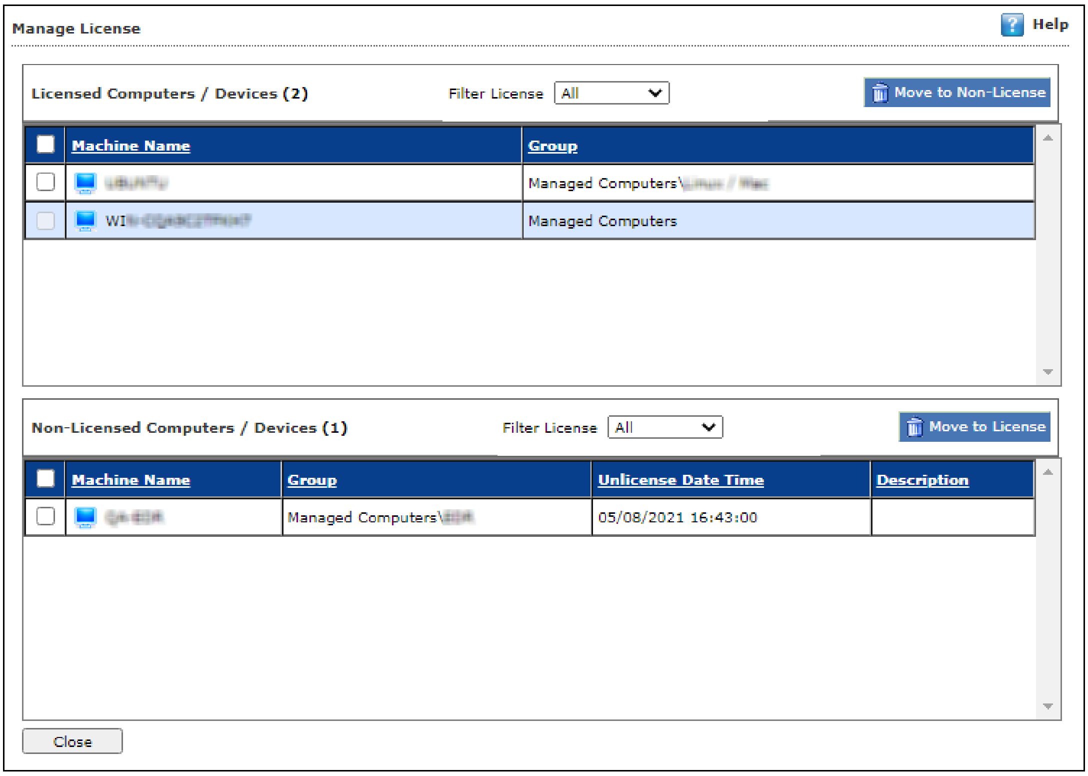
| □ | Machine Name | Group |
|---|---|---|
| □ | [redacted] | Managed Computers\\[redacted] |
| □ | [redacted] | Managed Computers\\[redacted] |
| □ | WI[redacted] | Managed Computers |

Non-Licensed Computers / Devices (0)

Filter License: All

No Record Found

2. Under the **Licensed Computers** section, select the computer(s) that you want to move to Non-Licensed Computers section.
3. Click **Move to Non-License**.
   The selected computer(s) will be moved to Non-Licensed computers section.



Manage License

Licensed Computers / Devices (2)

Filter License: All

| □ | Machine Name | Group |
|---|---|---|
| □ | [redacted] | Managed Computers\\[redacted] |
| □ | WI[redacted] | Managed Computers |

Non-Licensed Computers / Devices (1)

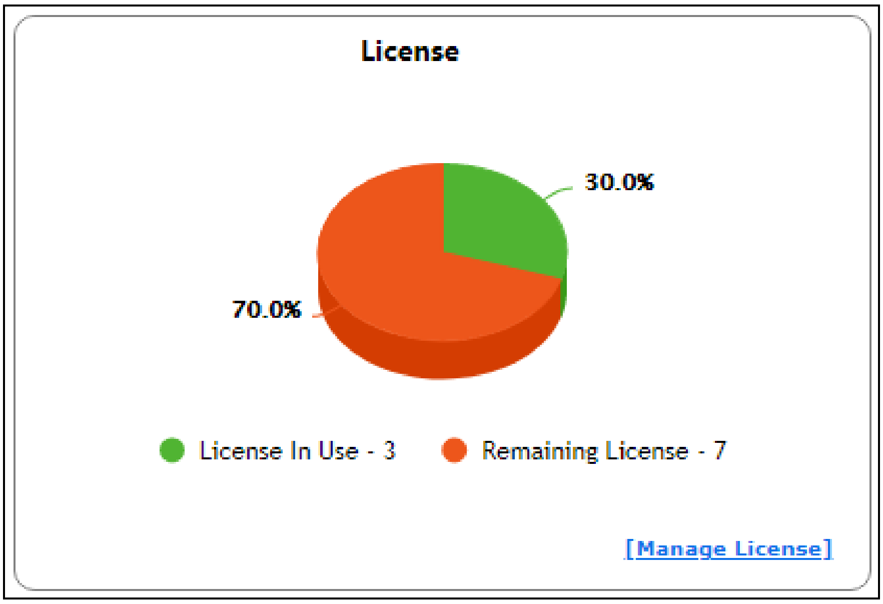
Filter License: All

| □ | Machine Name | Group | Unlicense Date Time | Description |
|---|---|---|---|---|
| □ | [redacted] | Managed Computers\\[redacted] | 05/08/2021 16:43:00 | |

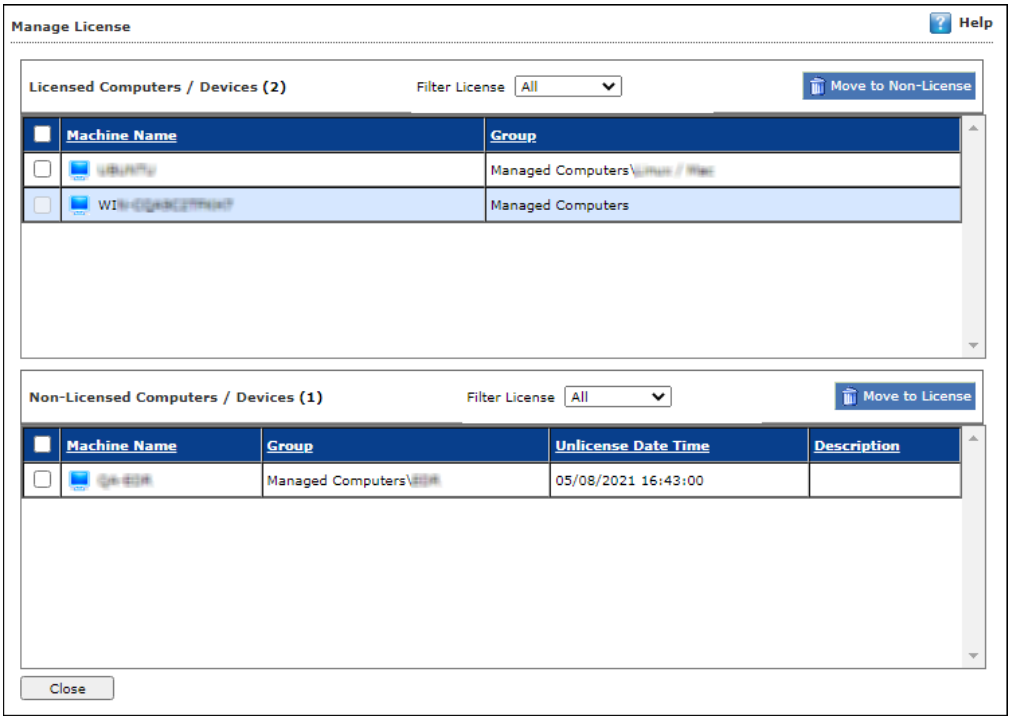
# Moving Non-Licensed Computers to Licensed Computers

To move licensed computers to non-licensed computers, follow the steps given below:

1. In the License statistics box, click **Manage License**.



Manage License window appears.



Manage License

Licensed Computers / Devices (2) Filter License All

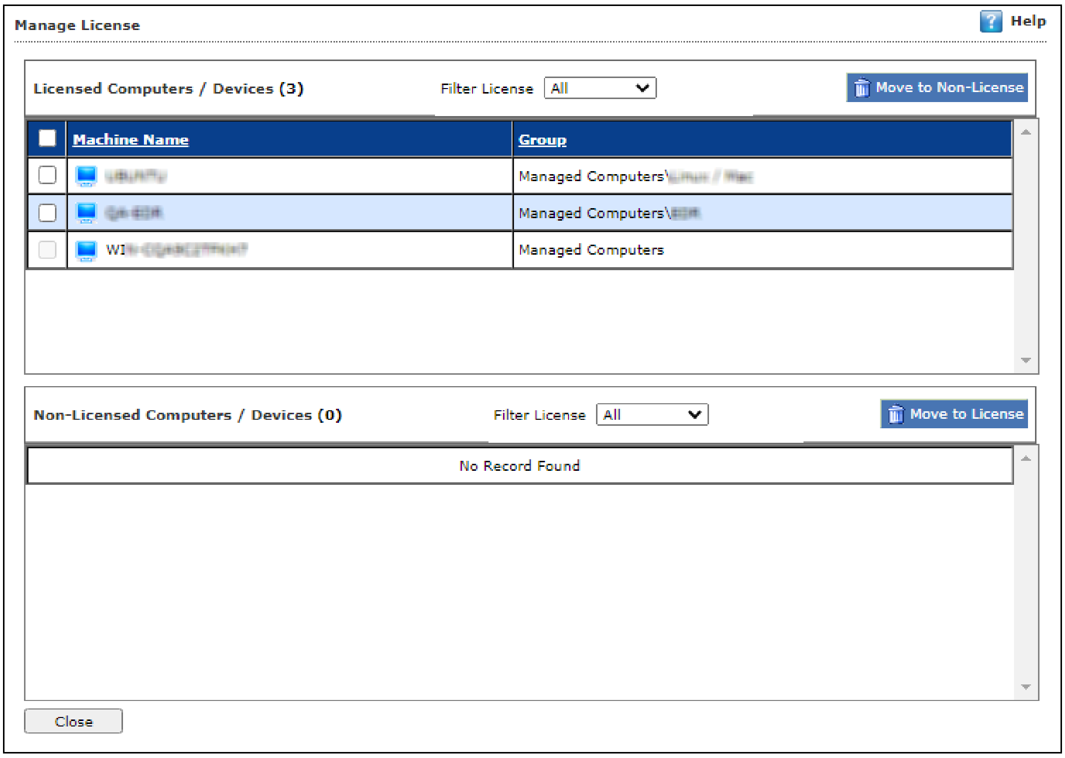
| □ | Machine Name | Group |
|---|---|---|
| □ | [redacted] | Managed Computers\[redacted] |
| □ | WI[redacted] | Managed Computers |

Non-Licensed Computers / Devices (1) Filter License All

| □ | Machine Name | Group | Unlicense Date Time | Description |
|---|---|---|---|---|
| □ | [redacted] | Managed Computers\[redacted] | 05/08/2021 16:43:00 | |

2. Under the **Non-Licensed Computers** section, select the computer(s) that you want to move to Licensed Computers section.

3. Click **Move to License**.
   The selected computer(s) will be moved to Licensed Computers section.



Manage License

Licensed Computers / Devices (3)

Filter License: All

| ☐ | Machine Name | Group |
|---|---|---|
| ☐ | [redacted] | Managed Computers\[redacted] |
| ☐ | [redacted] | Managed Computers\[redacted] |
| ☐ | WI[redacted] | Managed Computers |

Non-Licensed Computers / Devices (0)

Filter License: All

No Record Found

# Contact Us

We offer 24/7 free online technical support to our customers through email and live chat. We also provide free telephonic support to customers during our business hours.
Before you contact technical support team, ensure that your system meets all the requirements and you have Administrator access to it. Also, ensure that a qualified person is available at the system in case it becomes necessary to replicate the error/situation.

Ensure that you have the following information when you contact technical support:

- Endpoint hardware specifications
- Product version in use and patch level
- Network topology and NIC information
- Gateway, IP address and router details
- List of hardware, software and network changes if any carried out
- Step-by-step description of error/situation
- Step-by-step description of troubleshooting if any attempted
- Screenshots, error messages and log/debug files

In case you want the Technical Support team to take a remote connection:

- IP address and login credentials of the system

# Forums

Join the **Forum** to discuss eScan related problems with experts.

# Chat Support

The eScan Technical Support team is available round the clock to assist you with your queries via **Live Chat**.

# Email Support

If you have any queries, suggestions and comments regarding our products or this User Guide, write to us at **support@escanav.com**