eScan™

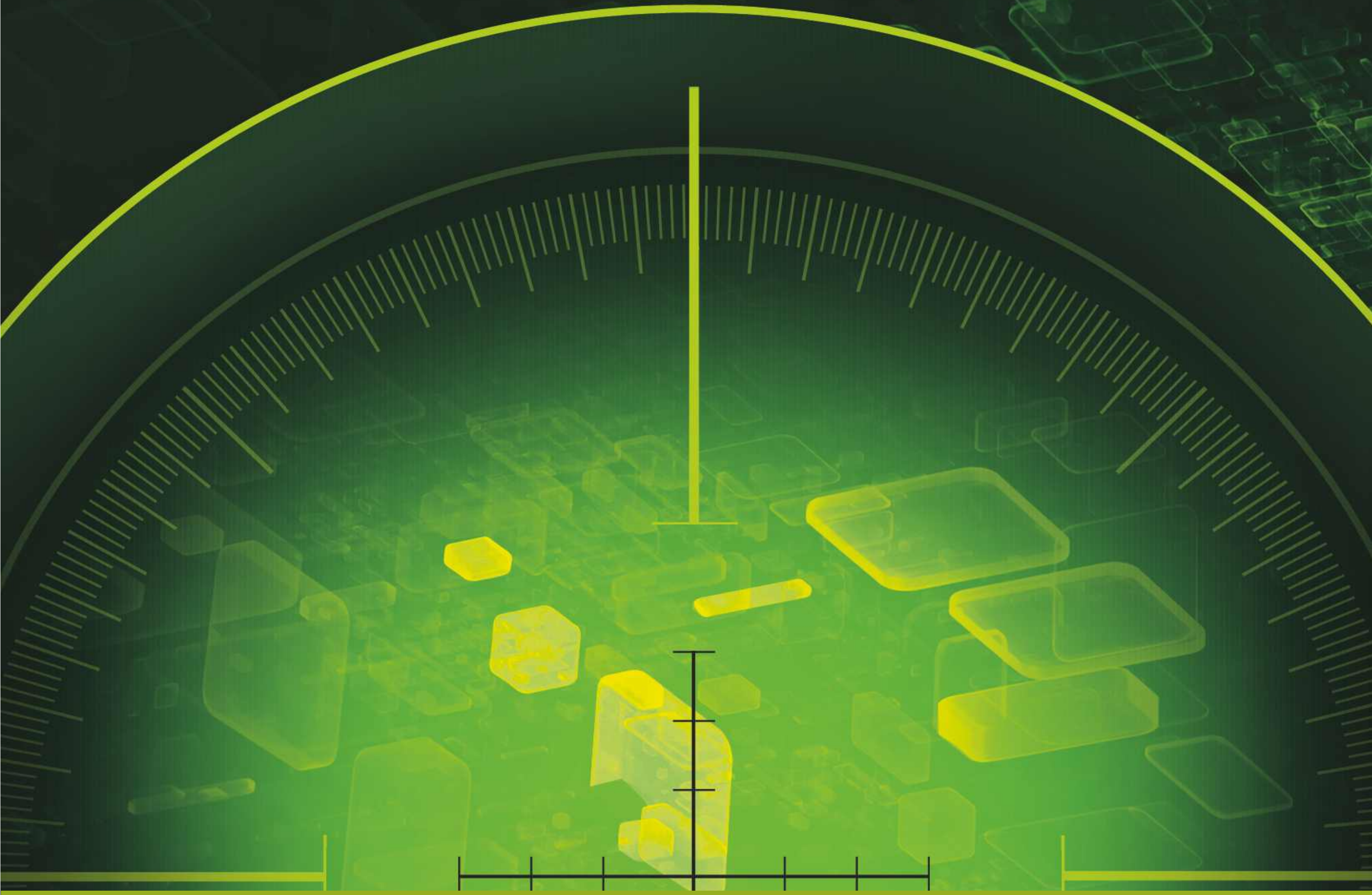
Enterprise Security

eScan Corporate Edition – Cloud

(With Hybrid Network Support)

User Guide

Product Version: 14.0.1400.xxxx
Document Version: 14.0.1400.xxxx



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 Version:	ESCL-UG-1401
Current Software Version:	14.0.1400.xxxx

Technical Support:	**support@escanav.com**
Sales:	**sales@escanav.com**
Forums:	**http://forums.escanav.com**
eScan Wiki:	**http://wiki.escanav.com/wiki/index.php/**
Live Chat:	**http://www.escanav.com/english/livechat.asp**
Printed by:	MicroWorld Software Services Private Limited
Date:	December, 2020

Content

Introduction

eScan Corporate Edition – Cloud (With Hybrid Network Support) is an IT security SaaS product that offers protection for client computers.

It is an easy to use Security-as-a-Service made up of sophisticated technologies that cater to SMB and Corporates.

It is a web based centralized Management Console that lets you do following activities

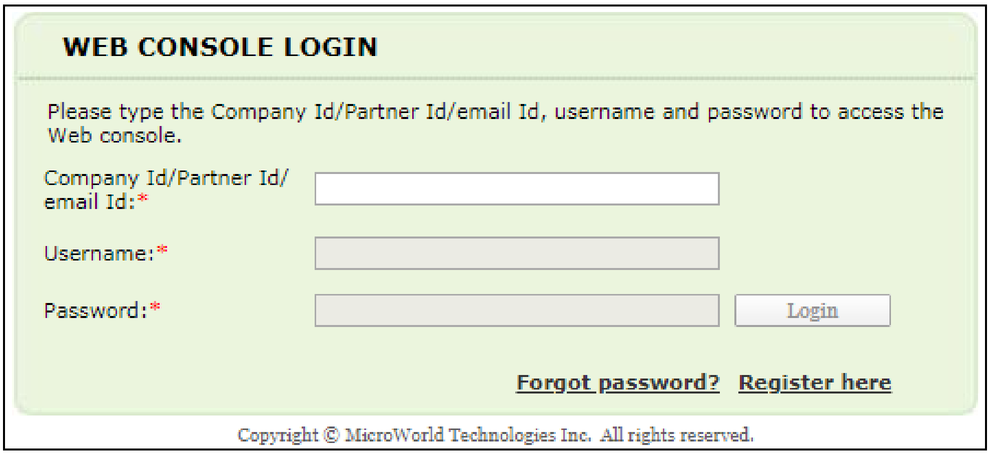
- Monitor the Security Status of all computers connected across the network
- Create and Manage policies for computers on your network.
- Create and View customized reports of the Security Status of the computers.
- Manage Notifications.
- View statistics for different modules in graphical format.

NOTE	If authentication for the mail server is mandatory for accepting emails, you will need a username and password to send emails.

Registration

To register eScan Corporate Edition – Cloud (With Hybrid Network Support)

1. Open a web browser.
2. Enter the URL – **https://cl.escanav.com**
   Login page appears.



WEB CONSOLE LOGIN

Please type the Company Id/Partner Id/email Id, username and password to access the Web console.

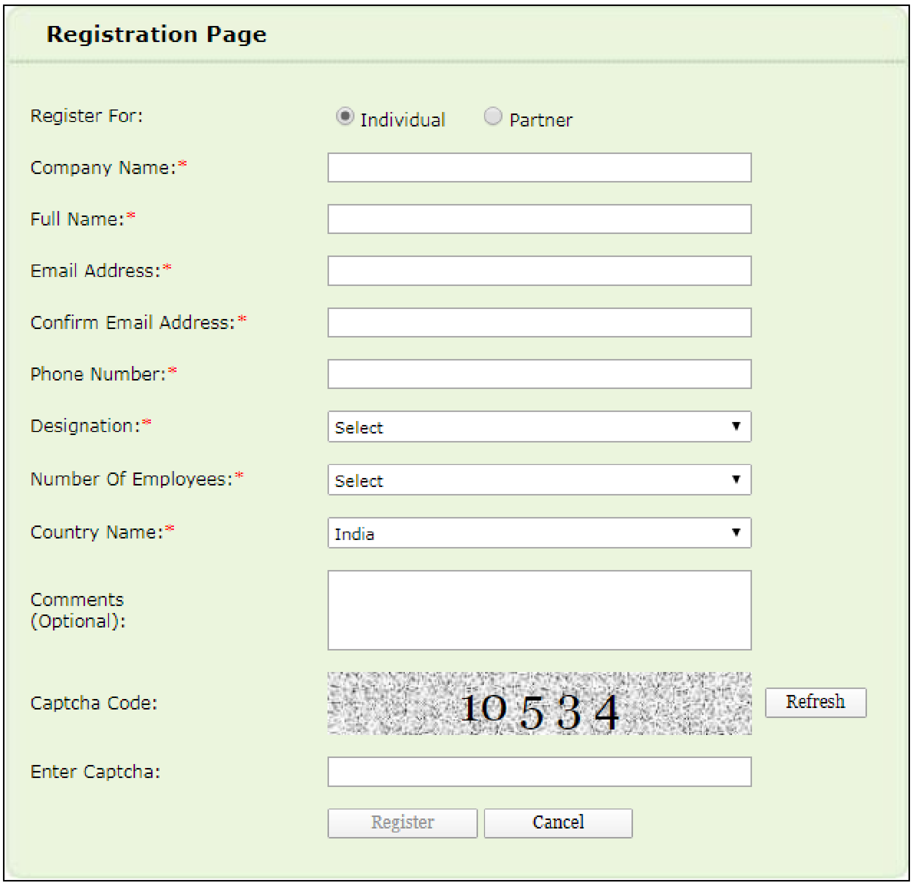
Company Id/Partner Id/ email Id:*

Username:*

Password:*

Copyright © MicroWorld Technologies Inc. All rights reserved.

3. Click **Register here**.
   You get redirected to the registration page.



Registration Page

Register For: ● Individual ○ Partner

Company Name:*

Full Name:*

Email Address:*

Confirm Email Address:*

Phone Number:*

Designation:* Select

Number Of Employees:* Select

Country Name:* India

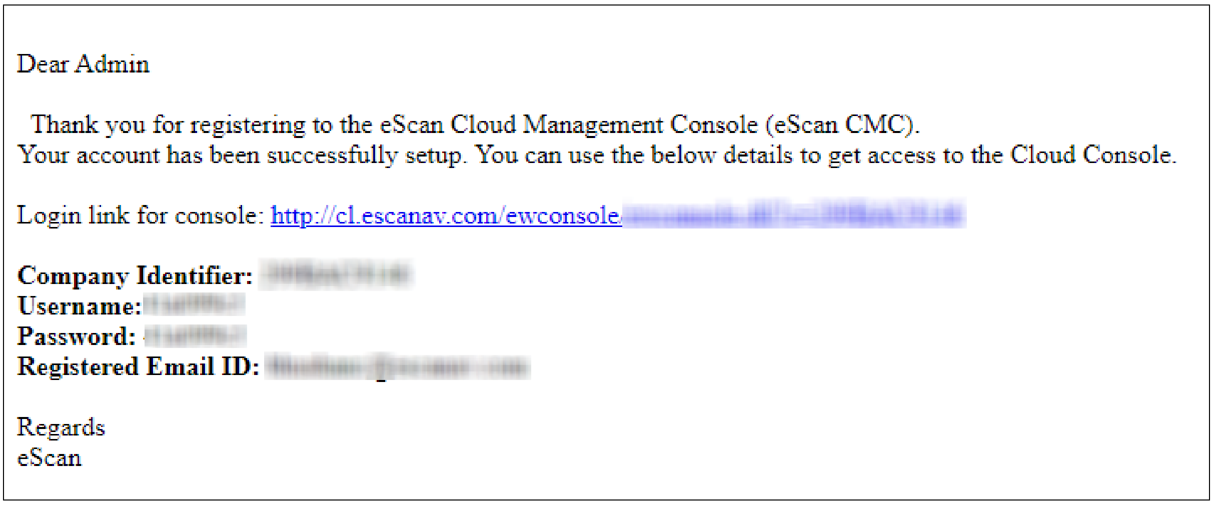
Comments (Optional):

Captcha Code: 10534

Enter Captcha:

4. Select whether you are registering as an **Individual** or **Partner**.

5. Enter the mandatory details and then click **Register**.
   You will receive a registration email containing a login link, Company ID, Username, Password, and Registered Email ID for eScan Corporate Edition – Cloud (With Hybrid Network Support) account.



Dear Admin

Thank you for registering to the eScan Cloud Management Console (eScan CMC).
Your account has been successfully setup. You can use the below details to get access to the Cloud Console.

Login link for console: http://cl.escanav.com/ewconsole/[redacted]

Company Identifier: [redacted]
Username:[redacted]
Password: [redacted]
Registered Email ID: [redacted]

Regards
eScan

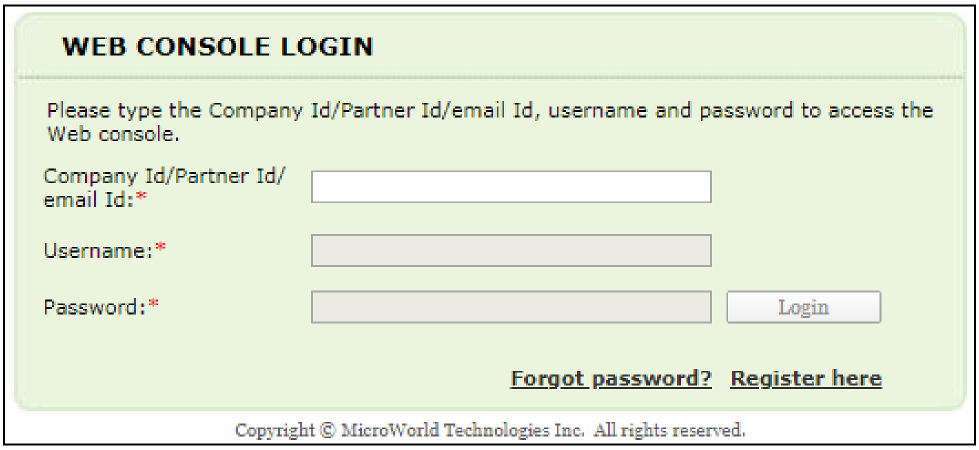
Your eScan Corporate Edition – Cloud (With Hybrid Network Support) account gets registered.

NOTE	Each **Company ID** is unique for every registration of eScan Corporate Edition – Cloud (With Hybrid Network Support) Management Console. After successful registration, a Company ID is provided on your registered email address.

Login

To log in to eScan Corporate Edition – Cloud (With Hybrid Network Support)

1. Open a web browser.
2. Enter the URL - **https://cl.escanav.com/**
   Login page appears.



WEB CONSOLE LOGIN

Please type the Company Id/Partner Id/email Id, username and password to access the Web console.

Company Id/Partner Id/ email Id:*

Username:*

Password:*

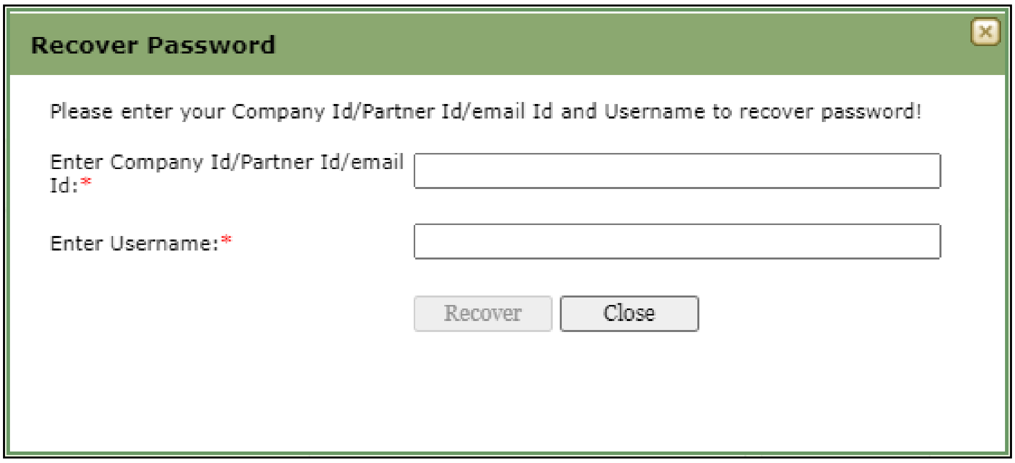
Copyright © MicroWorld Technologies Inc. All rights reserved.

3. Enter the company ID/Partner ID/email ID, login credentials, and then click **Login**.

Forgot Password

To recover the forgotten password,

1. Click **Forgot Password**.
   Recover Password window appears.



Recover Password

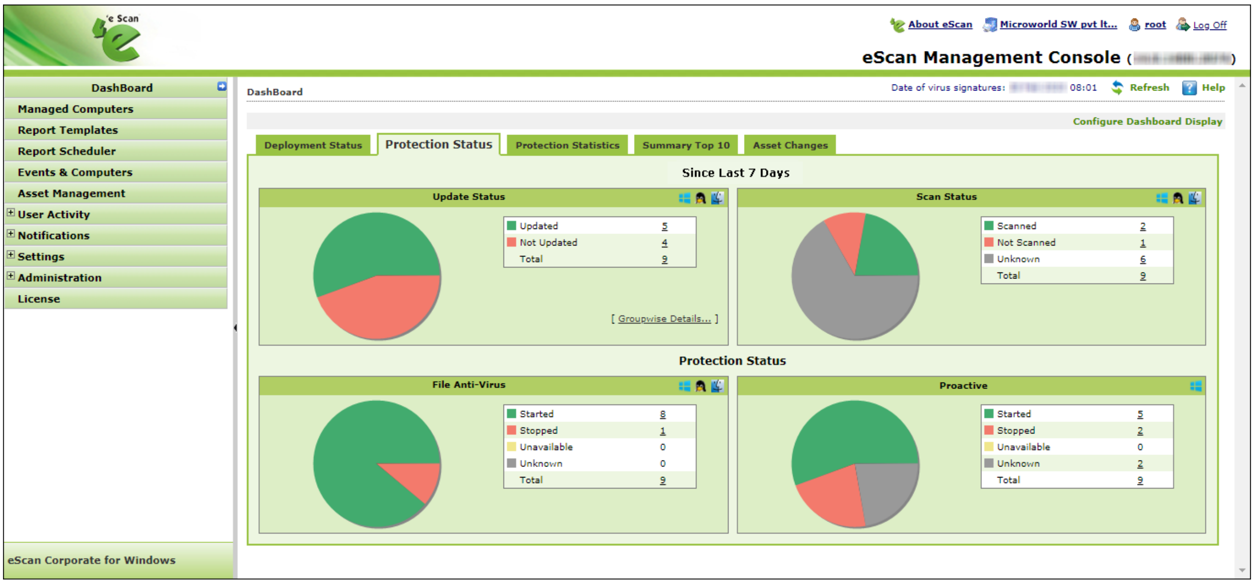
Please enter your Company Id/Partner Id/email Id and Username to recover password!

Enter Company Id/Partner Id/email Id:*

Enter Username:*

2. Enter your company ID/Partner ID/email ID and username.
3. Click **Recover**. An email containing login link, Company ID, Username, and Password and registration details will be sent to the registered email ID.

Main Interface



Update Status

🟩 Updated	5
🟥 Not Updated	4
Total	9

Scan Status

🟩 Scanned	2
🟥 Not Scanned	1
⬜ Unknown	6
Total	9

File Anti-Virus

🟩 Started	8
🟥 Stopped	1
🟨 Unavailable	0
⬜ Unknown	0
Total	9

Proactive

🟩 Started	5
🟥 Stopped	2
🟨 Unavailable	0
⬜ Unknown	2
Total	9

NOTE	Icons on every status Label denotes that the status is displayed for the computers having operating system as **Windows**, **MAC OS X** or **Linux**. The description of different link found on the main interface of the eScan console is listed in the table below.

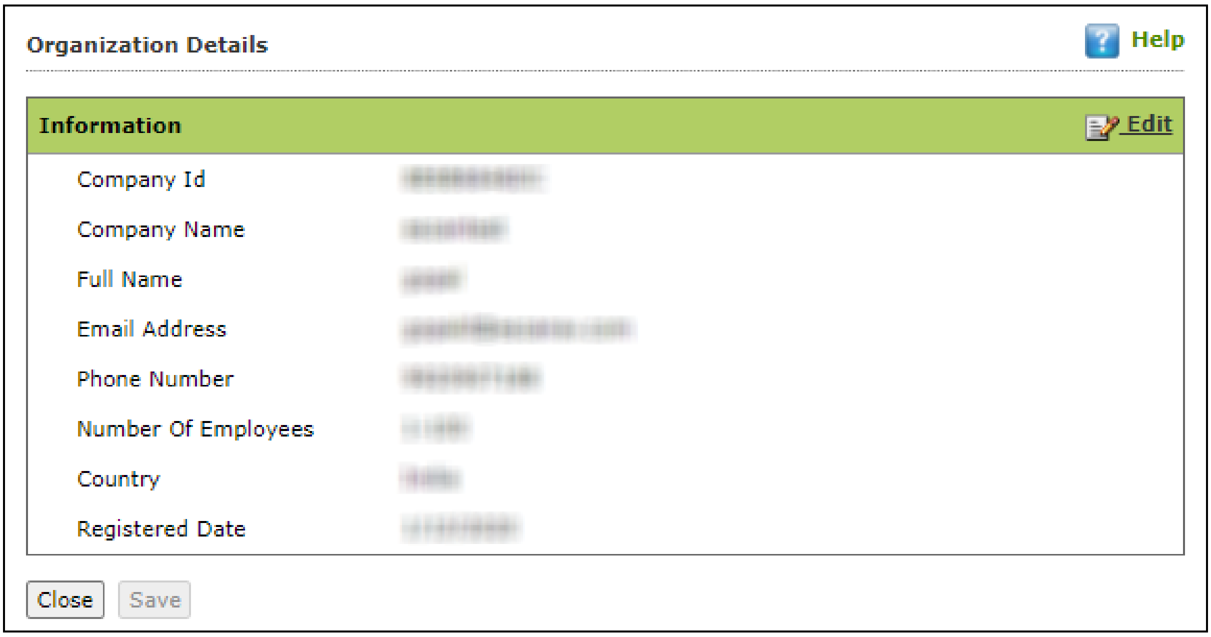
The links in the top right corner are explained below:

About eScan

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

Username

Clicking **Username** displays your registration details.



Organization Details

Information

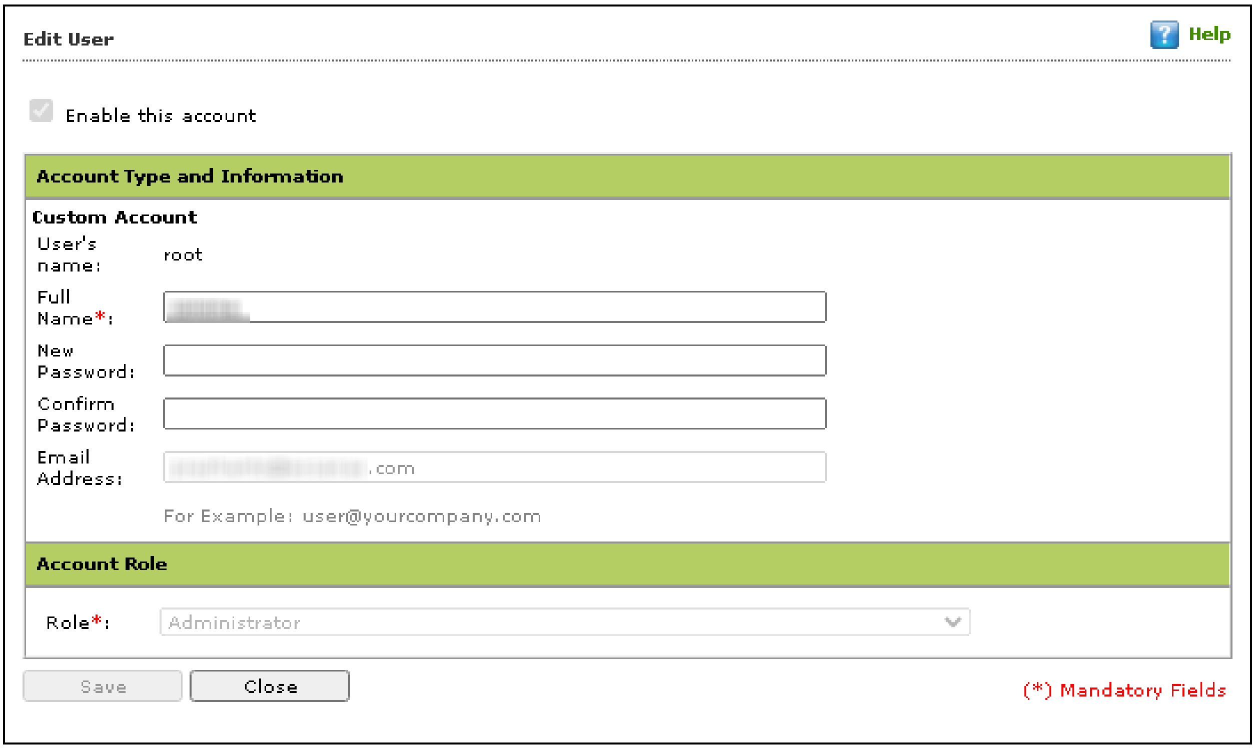
Company Id	[redacted]
Company Name	[redacted]
Full Name	[redacted]
Email Address	[redacted]
Phone Number	[redacted]
Number Of Employees	[redacted]
Country	[redacted]
Registered Date	[redacted]

Log off

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

root

This will be default username for the administrator created. Clicking **root** lets you change root account's password.



Edit User

Help

☑ Enable this account

Account Type and Information

Custom Account

User's name:	root
Full Name*:	[redacted]
New Password:	
Confirm Password:	
Email Address:	[redacted].com
	For Example: user@yourcompany.com

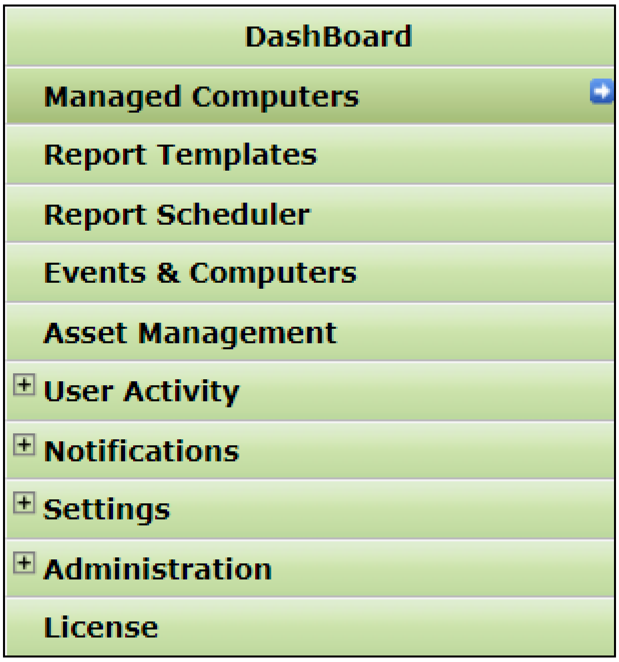
Account Role

Role*: Administrator

(*) Mandatory Fields

Enter the new password in **New Password** and **Confirm Password** boxes and then click **Save**. The password for root account gets saved and updated.

Navigation Panel


DashBoard
Managed Computers
Report Templates
Report Scheduler
Events & Computers
Asset Management
⊞ User Activity
⊞ Notifications
⊞ Settings
⊞ Administration
License

Dashboard
The Dashboard module displays charts showing Deployment status, Protection status, Protection Statistics, Summary Top 10, Asset Changes and the monitoring done by Management Console of the computers for virus infections and security violations.

Managed Computers
The Managed Computers module lets you can 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.

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.

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

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.

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.

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.

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.

Settings

The Settings module lets you configure eScan Console timeout settings, dashboard setting, exclude client settings for eScan.

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.

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.

NOTE	Icons on every status Label denotes that the status is displayed for the computers having operating system as **Windows,** **Mac OS X** or **Linux**.

Dashboard

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

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

In the top right corner there are additional links that are explained below:

Date of Virus Signatures

It displays the last date on which the Virus signatures were updated.

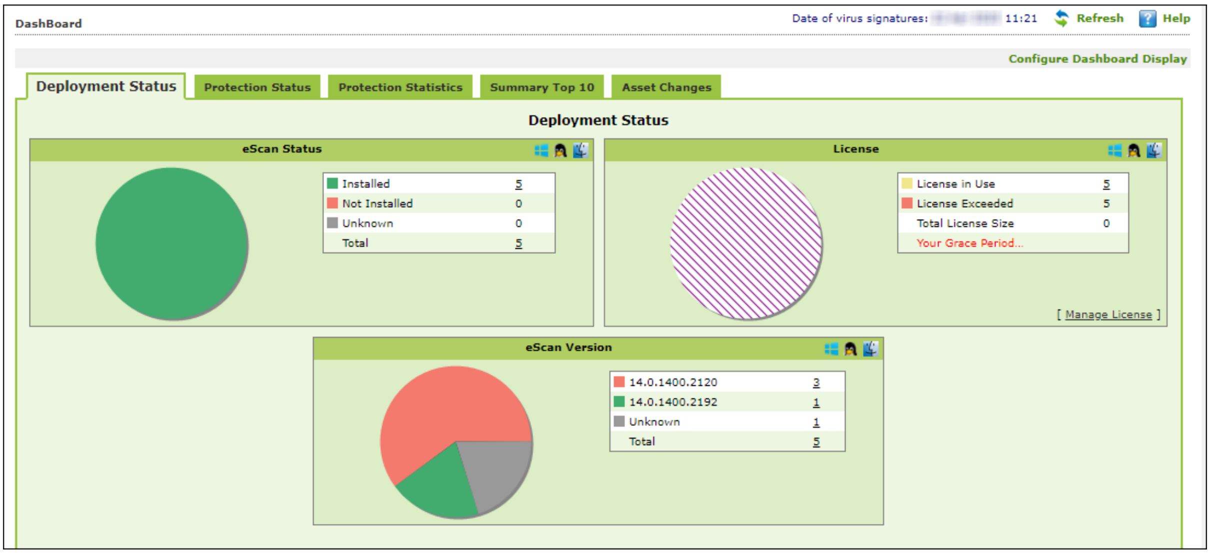
Refresh

Clicking **Refresh** refreshes the Dashboard information.

NOTE	Clicking underlined numerical displays detailed information for computers. The Windows, Mac, Linux Icons at the top of every chart denote that the information is displayed for the respective Operating Systems (OS).

Deployment Status

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



DashBoard

Date of virus signatures: [redacted] 11:21 Refresh Help

Configure Dashboard Display

Deployment Status

eScan Status

🟩 Installed	5
🟥 Not Installed	0
⬜ Unknown	0
Total	5

License

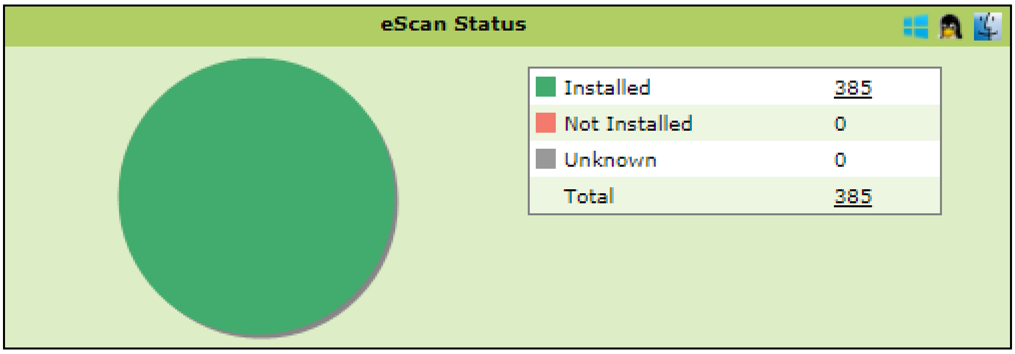
🟨 License in Use	5
🟥 License Exceeded	5
Total License Size	0
Your Grace Period...	

[Manage License]

eScan Version

🟥 14.0.1400.2120	3
🟩 14.0.1400.2192	1
⬜ Unknown	1
Total	5

eScan Status

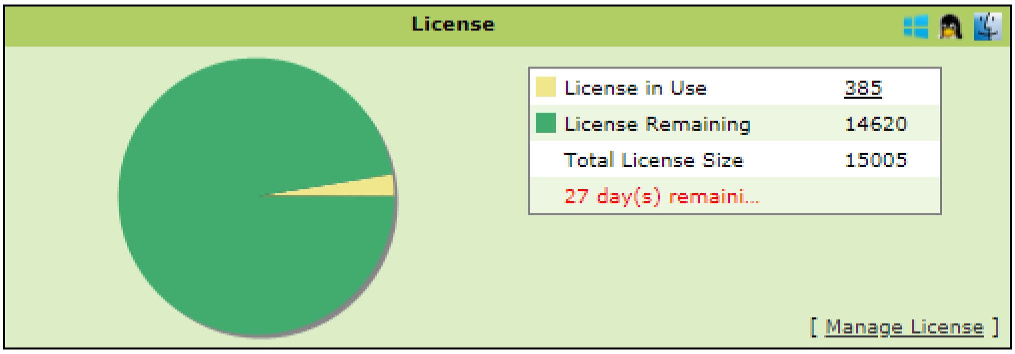


eScan Status

🟩 Installed	385
🟥 Not Installed	0
⬜ Unknown	0
Total	385

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. (eScan Corporate Edition – Cloud (With Hybrid Network Support) is unable to receive information from the computers for a long time)
Total – It displays the total number of computers connected across the network.

License



License

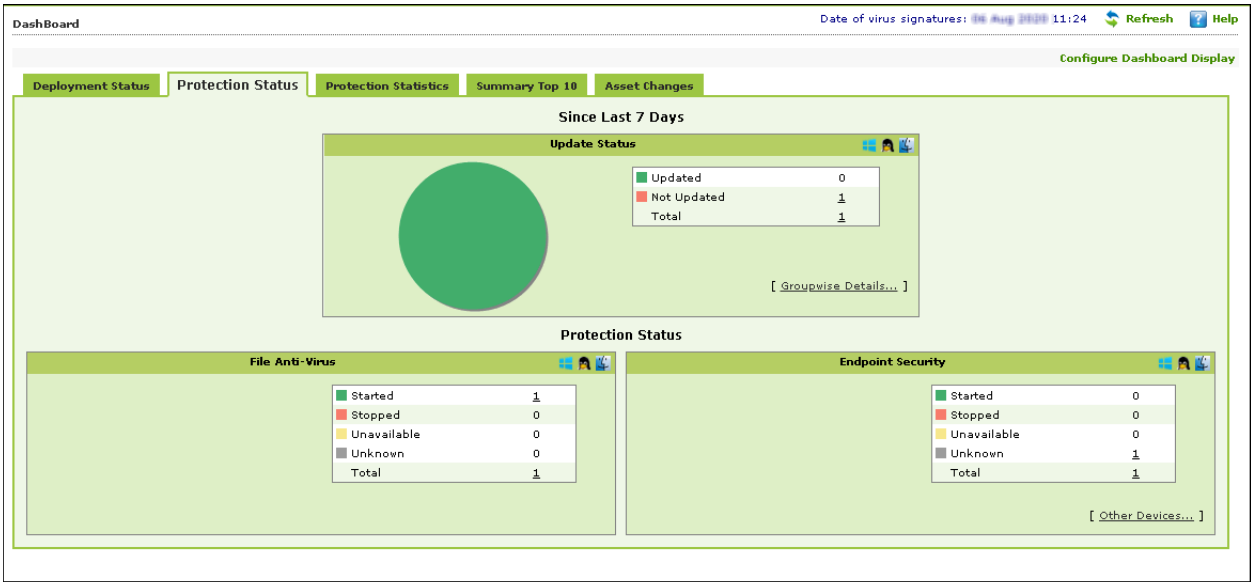
🟨	License in Use	385
🟩	License Remaining	14620
	Total License Size	15005
	27 day(s) remaini...	

[Manage License]

License in Use - It displays the number of licenses that are active.
Licenses Remaining - It displays the number of remaining licenses.
Total License Size - It displays the total number of licenses available.

Protection Status

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



DashBoard

Date of virus signatures: [redacted] 11:24 Refresh Help

Configure Dashboard Display

Since Last 7 Days

Update Status

🟩	Updated	0
🟥	Not Updated	1
	Total	1

[Groupwise Details...]

Protection Status

File Anti-Virus

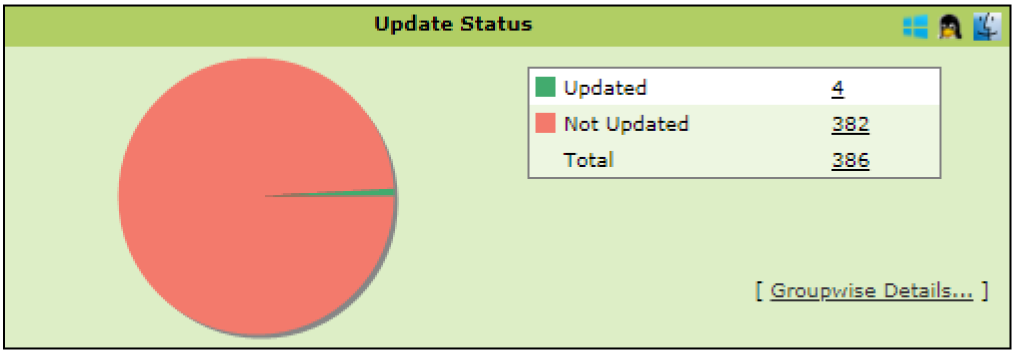
🟩	Started	1
🟥	Stopped	0
🟨	Unavailable	0
⬜	Unknown	0
	Total	1

Endpoint Security

🟩	Started	0
🟥	Stopped	0
🟨	Unavailable	0
⬜	Unknown	1
	Total	1

[Other Devices...]

Update Status



Update Status

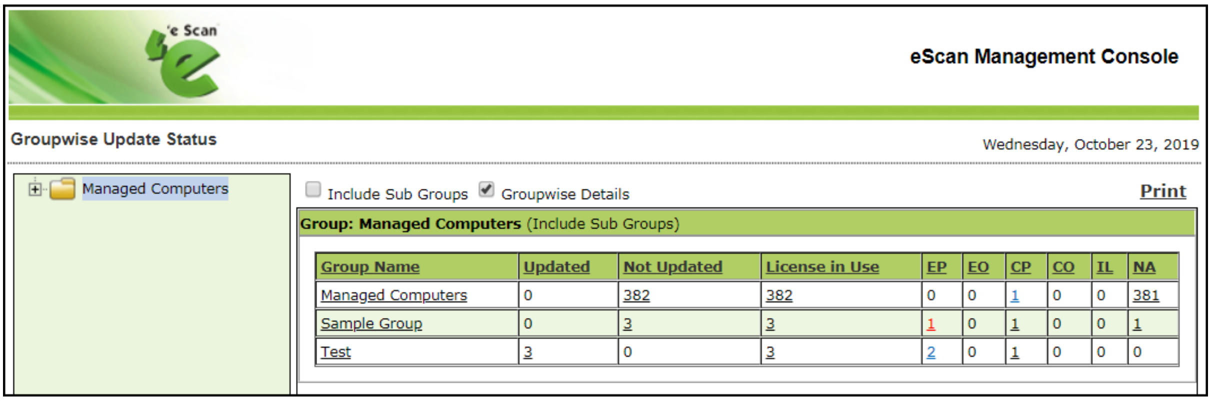
🟩	Updated	4
🟥	Not Updated	382
	Total	386

[Groupwise Details...]

399

Updated – It displays the number of computers on which virus signature database is updated.
Not Updated - It displays the number of computers on which virus signature database is not updated.
Total - It displays the total number of computers connected across the network.

Clicking **Groupwise Details** displays Groupwise Update Status window.



eScan Management Console

Groupwise Update Status

Wednesday, October 23, 2019

Managed Computers

□ Include Sub Groups ☑ Groupwise Details

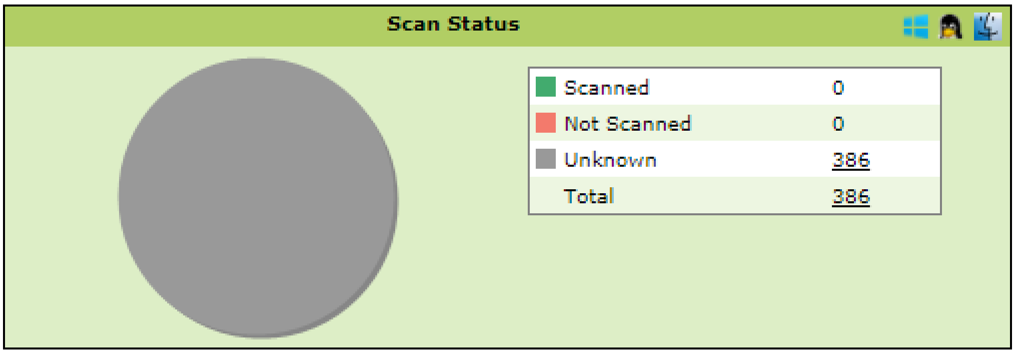
Print

Group: Managed Computers (Include Sub Groups)

Group Name	Updated	Not Updated	License in Use	EP	EO	CP	CO	IL	NA
Managed Computers	0	382	382	0	0	1	0	0	381
Sample Group	0	3	3	1	0	1	0	0	1
Test	3	0	3	2	0	1	0	0	0

It displays the number of computers on which virus database is Updated, Not Updated and Licenses in Use as per the group. Selecting **Include Sub Groups** check box will display the subgroups containing computers.

Scan Status



Scan Status

🟩	Scanned	0
🟥	Not Scanned	0
▨	Unknown	386
	Total	386

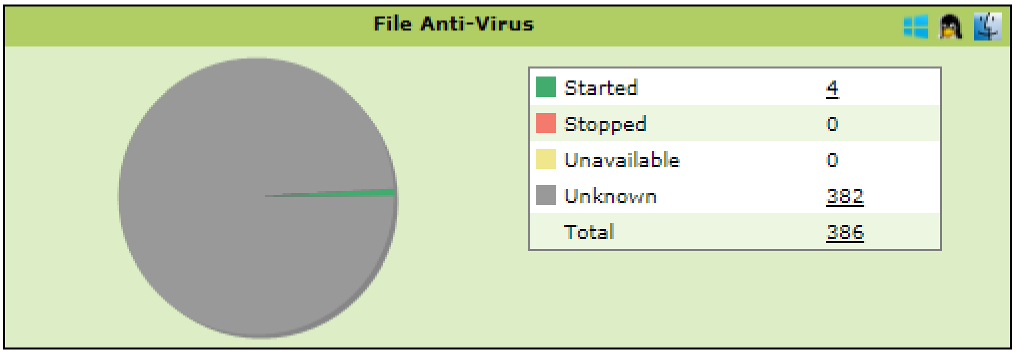
Scanned - It displays the number of computers that have been scanned in last 30 days for viruses and malware infections.

Not Scanned - It displays the number of computers that have not been scanned in last 30 days for viruses and malware infections.

Unknown - It displays the number of computers on which the scan status is unknown.

Total - It displays the total number of computers connected across the network.

File Anti-Virus



File Anti-Virus

🟩	Started	4
🟥	Stopped	0
🟨	Unavailable	0
▨	Unknown	382
	Total	386

Started – It displays the number of computers on which the File Anti-Virus module is in Started state.

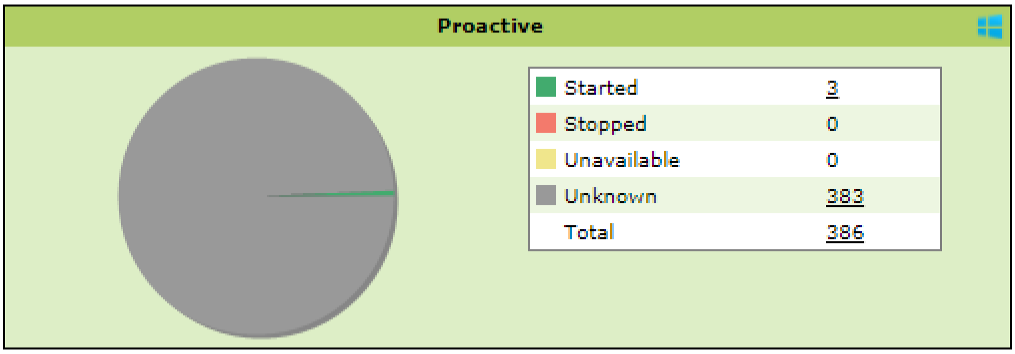
Stopped – It displays the number of computers on which the File Anti-Virus module is in Stopped state.

Unavailable – It displays the number of computers where the File Anti-Virus module is unavailable.

Unknown – It displays the number of computers where the File Anti-Virus module status is unknown.

Total – It displays the total number of computers connected across the network.

Proactive

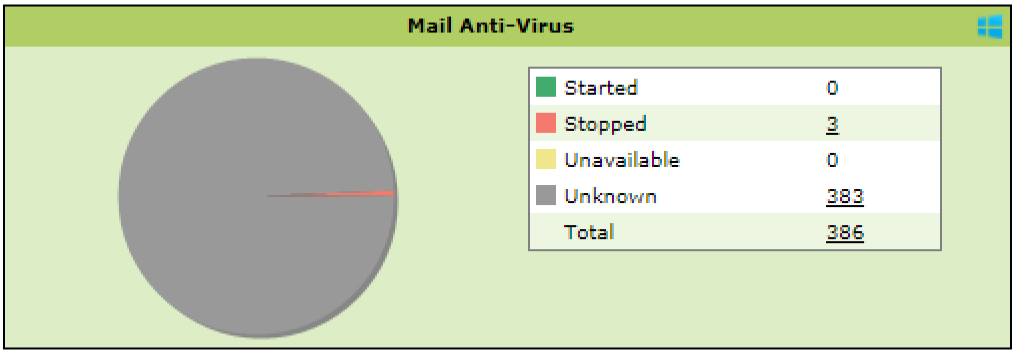


Proactive

🟩	Started	3
🟥	Stopped	0
🟨	Unavailable	0
◼	Unknown	383
	Total	386

Started - It displays the number of computers on which Proactive scanning service is running.
Stopped - It displays the number of computers on which Proactive scanning service is stopped.
Unavailable – It displays the number of computers where Proactive scanning service is unavailable. This module is available only in computers with Windows OS.
Unknown - It displays the number of computers on which the Proactive scanning service status is unknown.
Total - It displays the total number of computers connected across the network.

Mail Anti-Virus

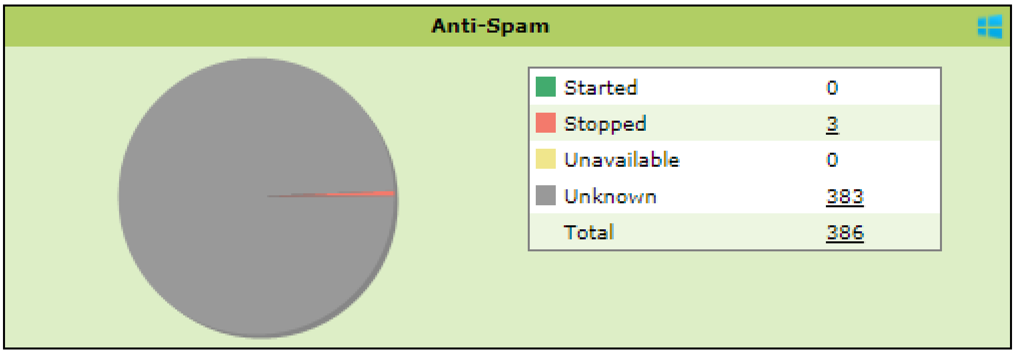


Mail Anti-Virus

🟩	Started	0
🟥	Stopped	3
🟨	Unavailable	0
◼	Unknown	383
	Total	386

Started – It displays the number of computers on which the Mail Anti-Virus module is in Started state.
Stopped – It displays the number of computers on which the Mail Anti-Virus module is in Stopped state.
Unavailable – It displays the number of computers on which the Mail Anti-Virus module is unavailable.
Unknown – It displays the number of computers on which the Mail Anti-Virus module status is unknown.
Total – It displays the total number of computers connected across the network.

Anti-Spam

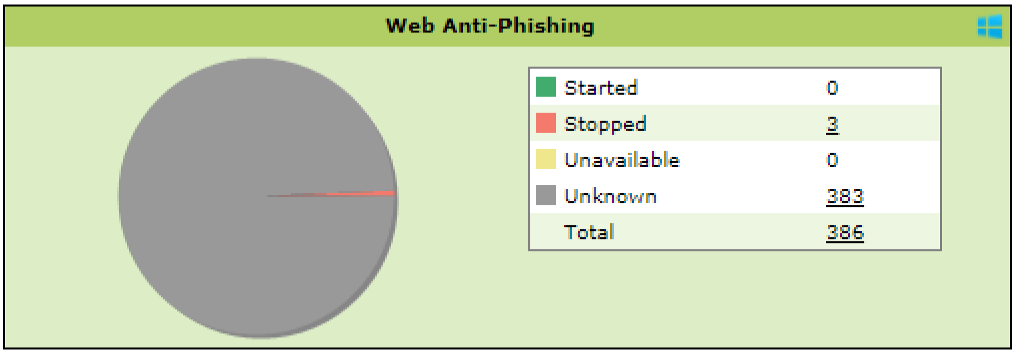


Anti-Spam

🟩	Started	0
🟥	Stopped	3
🟨	Unavailable	0
◼	Unknown	383
	Total	386

Started – It displays the number of computers on which the Anti-Spam module is in Started state.
Stopped – It displays the number of computers on which the Anti-Spam module is in Stopped state.
Unknown – It displays the number of computers on which the Anti-Spam module status is unknown.
Unavailable – It displays the number of computers on which the Anti-Spam module is unavailable.
Total – It displays the total number of computers connected across the network.

Web Anti-Phishing

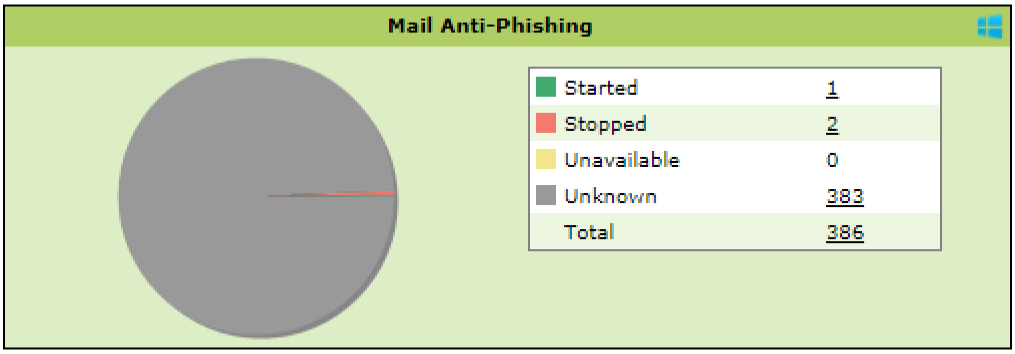


Web Anti-Phishing

🟩	Started	0
🟥	Stopped	3
🟨	Unavailable	0
◼	Unknown	383
	Total	386

Started – It displays the number of computers on which the web Anti-Phishing service is started.
Stopped – It displays the number of computers on which the web Anti-Phishing service is stopped.
Unknown – It displays the number of computers on which the web Anti-Phishing service status is unknown.
Unavailable - It displays the number of computers on which the web Anti-Phishing service is unavailable.
Total – It displays the total number of computers connected across the network.

Mail Anti–Phishing

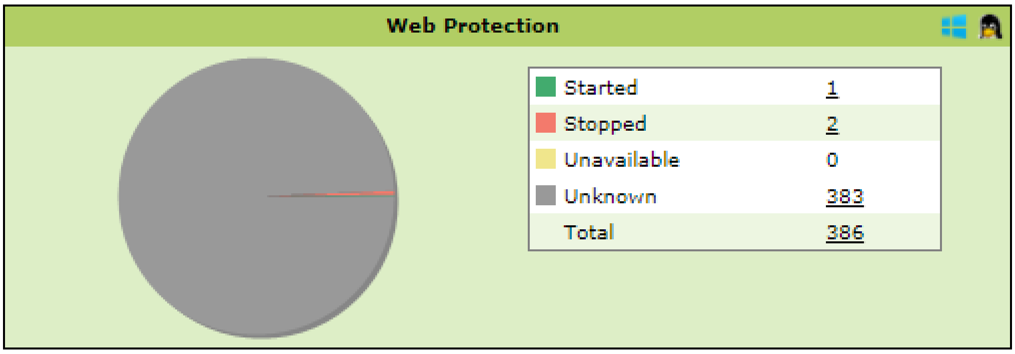


Mail Anti-Phishing

🟩	Started	1
🟥	Stopped	2
🟨	Unavailable	0
⬛	Unknown	383
	Total	386

Started – It displays the number of computers on which the Mail Anti-Phishing service is enabled.
Stopped – It displays the number of computers on which the Mail Anti-Phishing service is disabled.
Unknown – It displays the number of computers on which the Mail Anti-Phishing service status is unknown.
Unavailable – It displays the number of computers on which the Mail Anti-Phishing service is unavailable.
Total – It displays the total number of computers connected across the network.

Web Protection

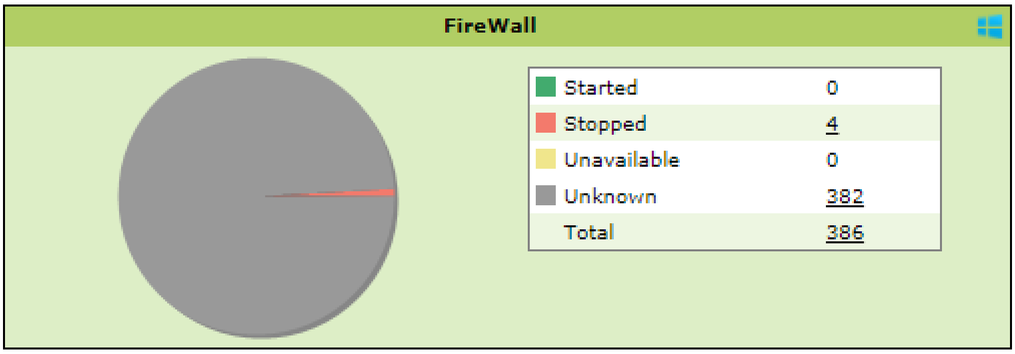


Web Protection

🟩	Started	1
🟥	Stopped	2
🟨	Unavailable	0
⬛	Unknown	383
	Total	386

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.
Total – It displays the total number of computers connected across the network.

Firewall

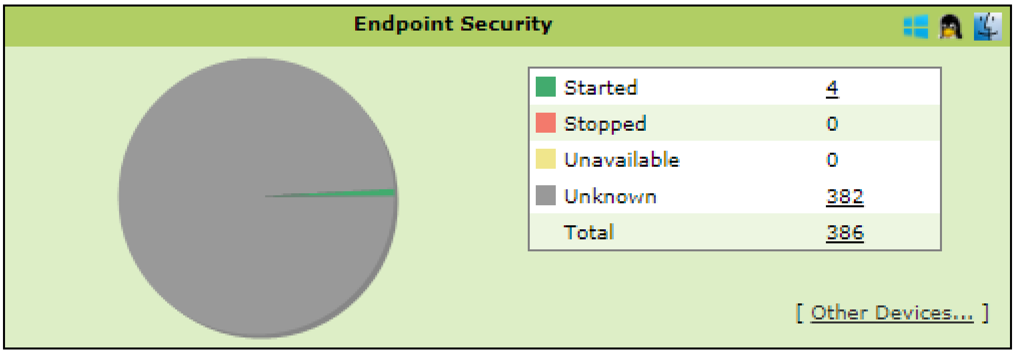


FireWall

🟩	Started	0
🟥	Stopped	4
🟨	Unavailable	0
⬛	Unknown	382
	Total	386

Started - It displays the number of computers on which the Firewall module is in Started state.
Stopped - It displays the number of computers on which the Firewall module is in Stopped state.
Unavailable - It displays the number of computers on which the Firewall module is unavailable.
Unknown - It displays the number of computers on which the Firewall module status is unknown.
Total – It displays the total number of computers connected across the network.

Endpoint Security



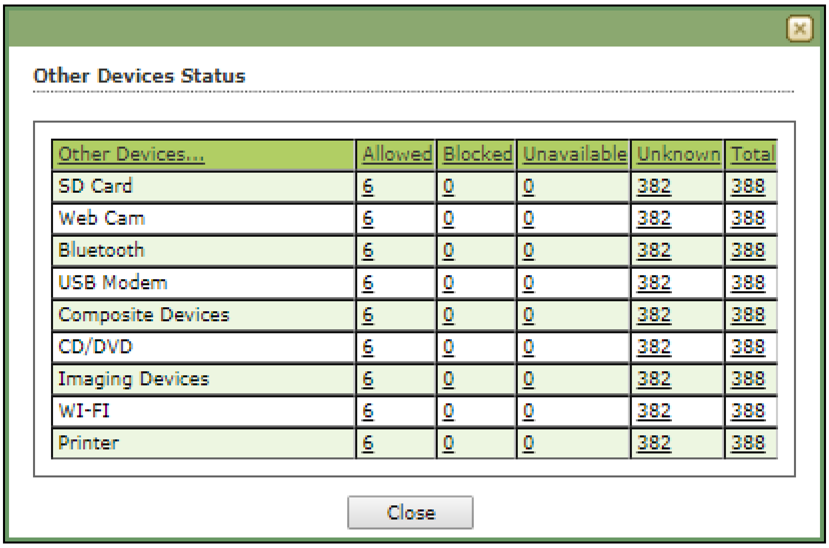
Endpoint Security

🟩	Started	4
🟥	Stopped	0
🟨	Unavailable	0
⬛	Unknown	382
	Total	386

[Other Devices...]

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.
Total – It displays the total number of computers connected across the network.

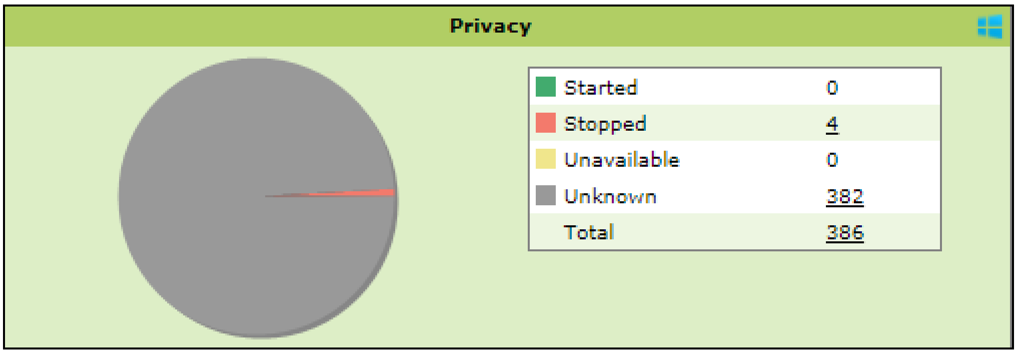
Clicking **Other Devices** displays details about other devices.



Other Devices Status

Other Devices...	Allowed	Blocked	Unavailable	Unknown	Total
SD Card	6	0	0	382	388
Web Cam	6	0	0	382	388
Bluetooth	6	0	0	382	388
USB Modem	6	0	0	382	388
Composite Devices	6	0	0	382	388
CD/DVD	6	0	0	382	388
Imaging Devices	6	0	0	382	388
WI-FI	6	0	0	382	388
Printer	6	0	0	382	388

Privacy



Privacy

🟩	Started	0
🟥	Stopped	4
🟨	Unavailable	0
⬜	Unknown	382
	Total	386

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.

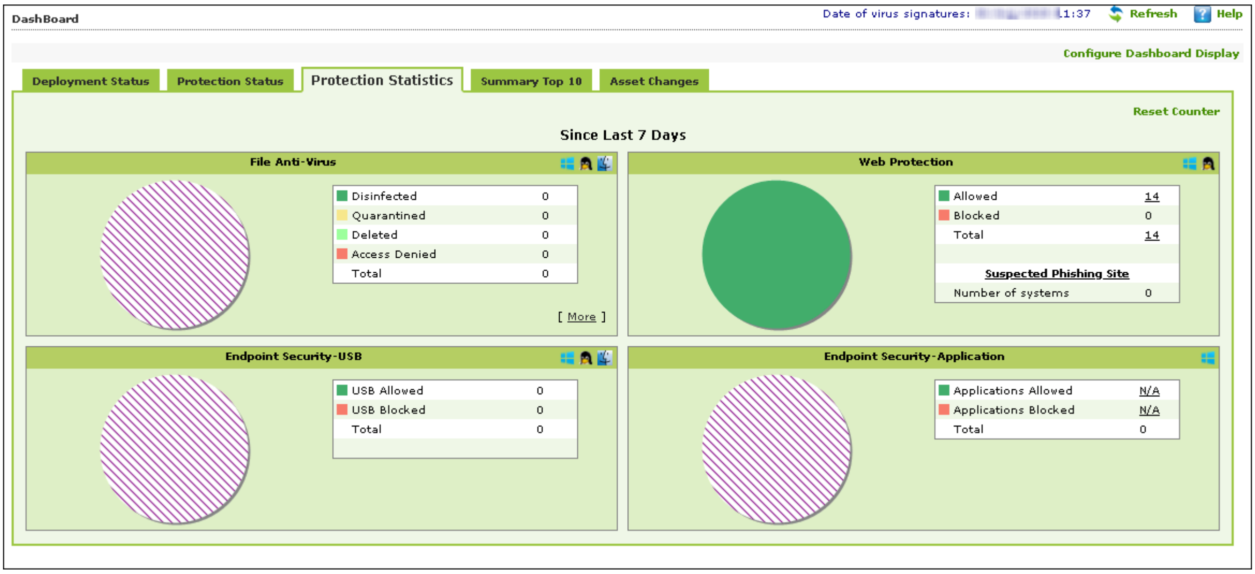
Unavailable - It displays the number of computers on which the Privacy Control module of eScan is unavailable.

Unknown - It displays the number of computers on which the Privacy Control module status is unknown.

Total – It displays the total number of computers connected across the network.

Protection Statistics

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



DashBoard

Date of virus signatures: [redacted] 11:37 Refresh Help

Configure Dashboard Display

Reset Counter

Since Last 7 Days

File Anti-Virus

🟩	Disinfected	0
🟨	Quarantined	0
🟩	Deleted	0
🟥	Access Denied	0
	Total	0

[More]

Web Protection

🟩	Allowed	14
🟥	Blocked	0
	Total	14
	Suspected Phishing Site	
	Number of systems	0

Endpoint Security-USB

🟩	USB Allowed	0
🟥	USB Blocked	0
	Total	0

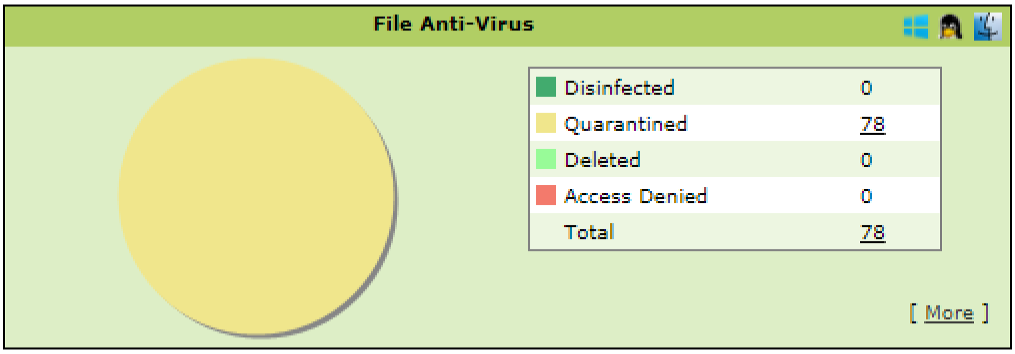
Endpoint Security-Application

🟩	Applications Allowed	N/A
🟥	Applications Blocked	N/A
	Total	0

Reset Counter

Clicking **Reset Counter** resets all the statistics to zero. This option proves useful after you have taken an action on infected files and want to scan for residual infection presence.

File Anti-Virus



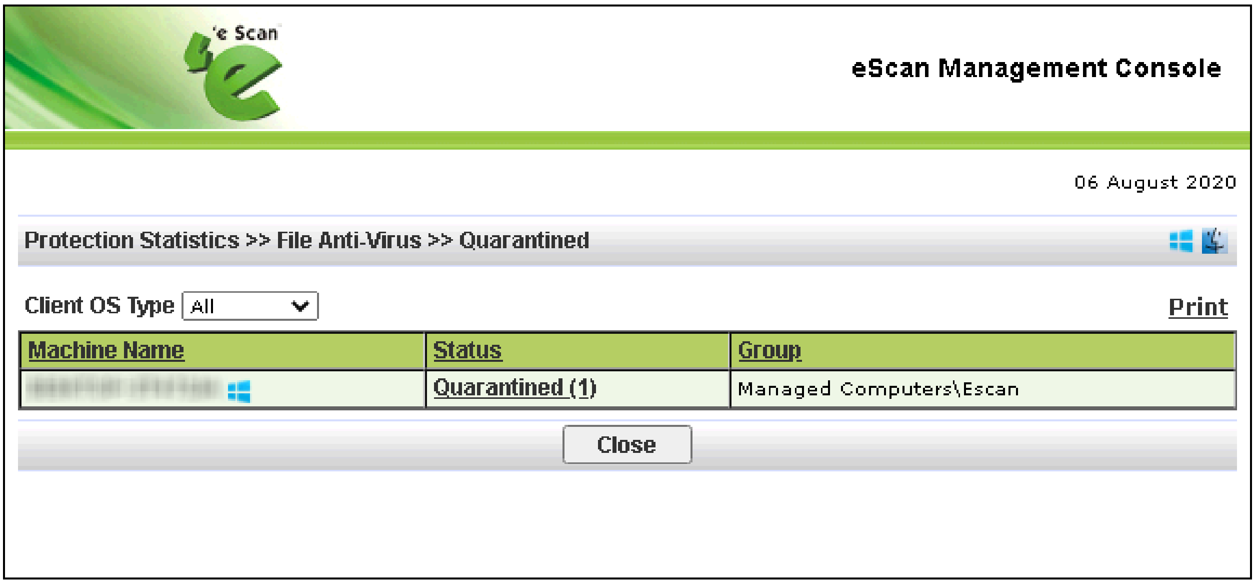
File Anti-Virus

🟩	Disinfected	0
🟨	Quarantined	78
🟩	Deleted	0
🟥	Access Denied	0
	Total	78

[More]

Disinfected – It displays the number of files disinfected by File Anti-Virus module.
Quarantined – It displays the number of files quarantined by File Anti-Virus module.
Deleted - It displays the number of files deleted by File Anti-Virus module.
Access Denied - It displays the number of files to which access was denied by File Anti-Virus module.
Total – It displays the total number of files on which File Anti-Virus module took action since last seven days.

Clicking underlined numerical displays action taken on infected files amongst different computers and the group that computer belongs to.



eScan Management Console

06 August 2020

Protection Statistics >> File Anti-Virus >> Quarantined

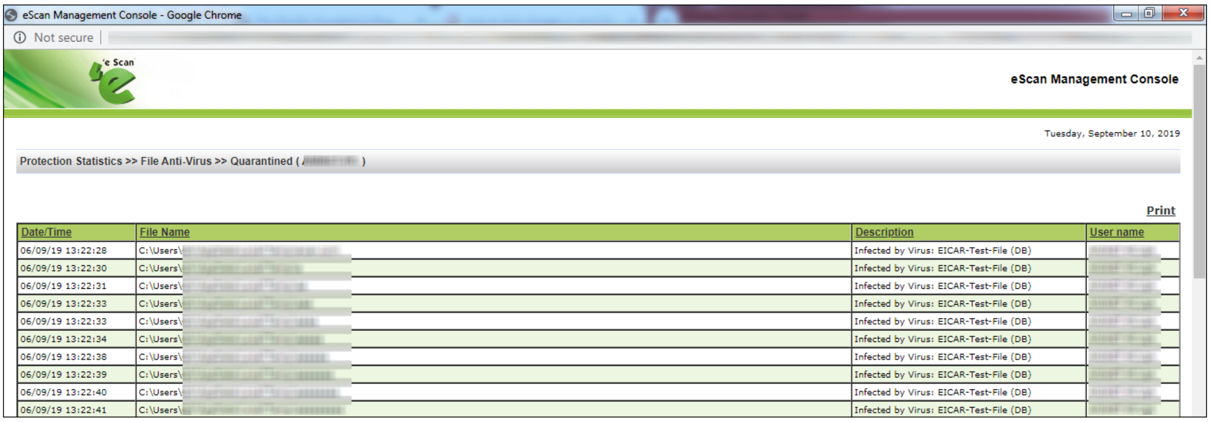
Client OS Type All

Print

Machine Name	Status	Group
[redacted]	Quarantined (1)	Managed Computers\Escan

Close

Clicking the Status link further displays the detection date and time, file path, infection description and computer's username.



eScan Management Console - Google Chrome

Not secure

eScan Management Console

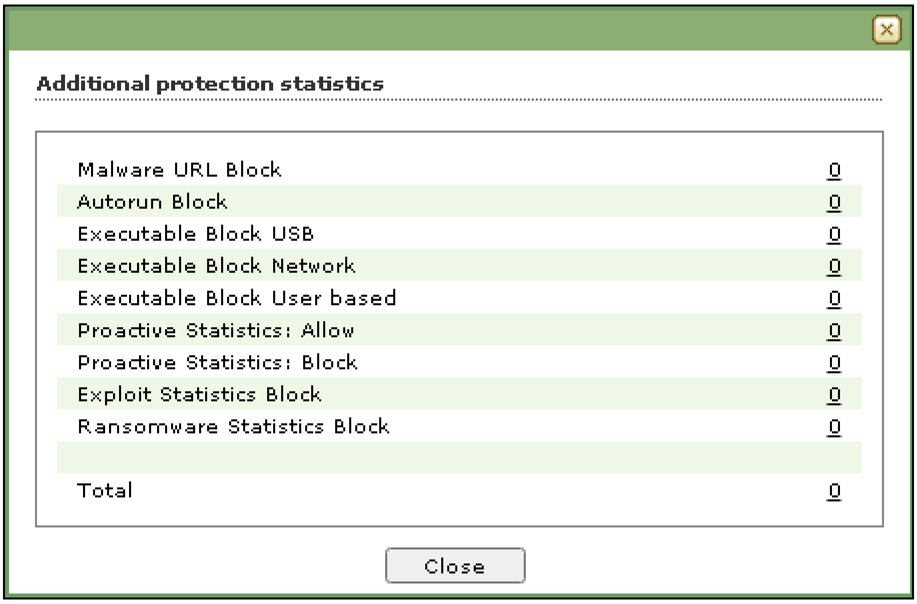
Tuesday, September 10, 2019

Protection Statistics >> File Anti-Virus >> Quarantined ([redacted])

Print

Date/Time	File Name	Description	User name
06/09/19 13:22:28	C:\Users\[redacted]	Infected by Virus: EICAR-Test-File (DB)	[redacted]
06/09/19 13:22:30	C:\Users\[redacted]	Infected by Virus: EICAR-Test-File (DB)	[redacted]
06/09/19 13:22:31	C:\Users\[redacted]	Infected by Virus: EICAR-Test-File (DB)	[redacted]
06/09/19 13:22:33	C:\Users\[redacted]	Infected by Virus: EICAR-Test-File (DB)	[redacted]
06/09/19 13:22:33	C:\Users\[redacted]	Infected by Virus: EICAR-Test-File (DB)	[redacted]
06/09/19 13:22:34	C:\Users\[redacted]	Infected by Virus: EICAR-Test-File (DB)	[redacted]
06/09/19 13:22:38	C:\Users\[redacted]	Infected by Virus: EICAR-Test-File (DB)	[redacted]
06/09/19 13:22:39	C:\Users\[redacted]	Infected by Virus: EICAR-Test-File (DB)	[redacted]
06/09/19 13:22:40	C:\Users\[redacted]	Infected by Virus: EICAR-Test-File (DB)	[redacted]
06/09/19 13:22:41	C:\Users\[redacted]	Infected by Virus: EICAR-Test-File (DB)	[redacted]

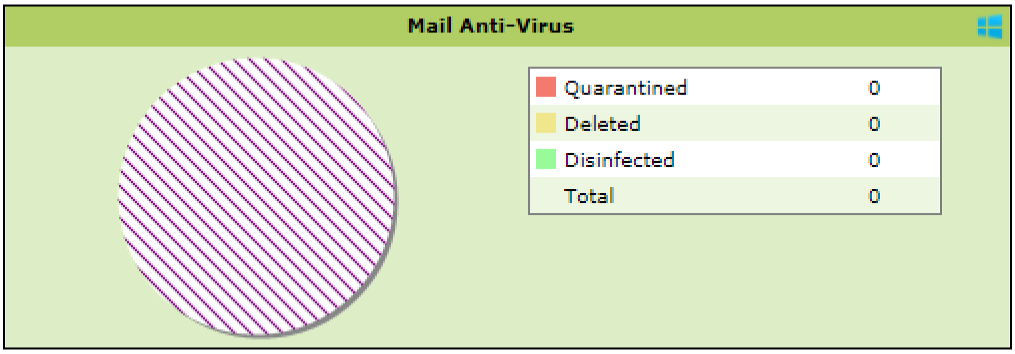
Clicking **[More]** displays additional protection statistics.



Additional protection statistics

Malware URL Block	0
Autorun Block	0
Executable Block USB	0
Executable Block Network	0
Executable Block User based	0
Proactive Statistics: Allow	0
Proactive Statistics: Block	0
Exploit Statistics Block	0
Ransomware Statistics Block	0
Total	0

Mail Anti-Virus



Mail Anti-Virus

🟥	Quarantined	0
🟨	Deleted	0
🟩	Disinfected	0
	Total	0

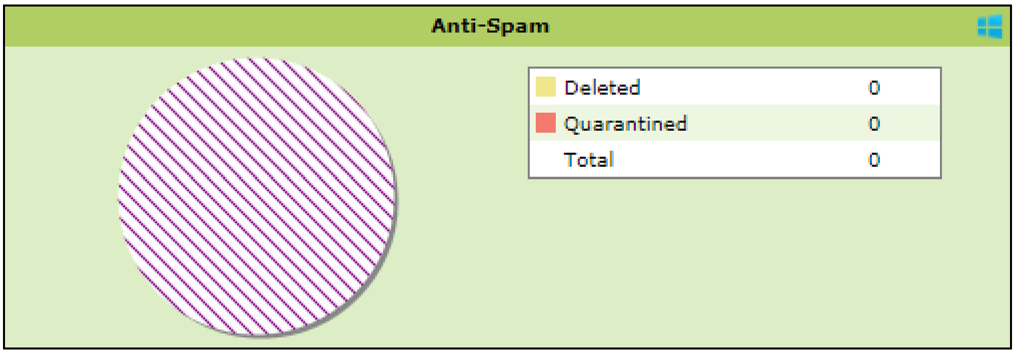
Quarantined – It displays the number of files/emails quarantined by Mail Anti-Virus module.

Deleted – It displays the number of files/emails deleted by Mail Anti-Virus module.

Disinfected – It displays the number of files/emails disinfected by Mail Anti-Virus module.

Total – It displays the total number of files/emails on which Mail Anti-Virus module took action since last seven days.

Anti-Spam

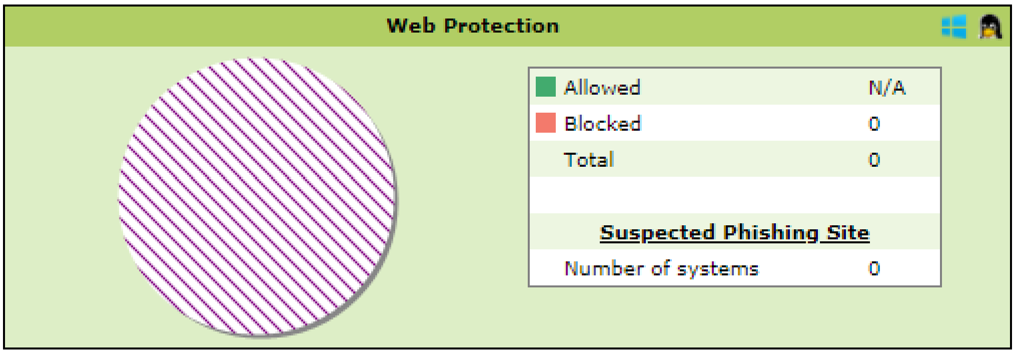


Anti-Spam

🟨	Deleted	0
🟥	Quarantined	0
	Total	0

Deleted – It displays the number of files deleted by Anti-Spam module.
Quarantined – It displays the number of files quarantined by Anti-Spam module.
Total – It displays the total number of files on which Anti-Spam module took action since last seven days.

Web Protection



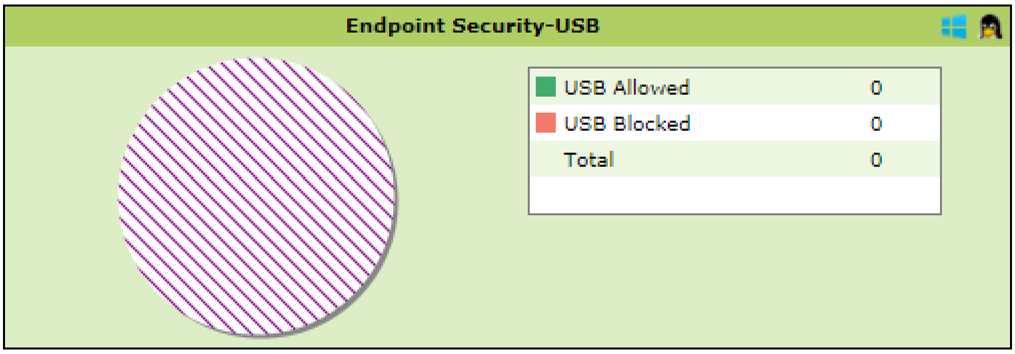
Web Protection

🟩	Allowed	N/A
🟥	Blocked	0
	Total	0
	Suspected Phishing Site	
	Number of systems	0

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.
Total – It displays the total number of websites allowed and blocked by Web Protection module since last seven days.

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

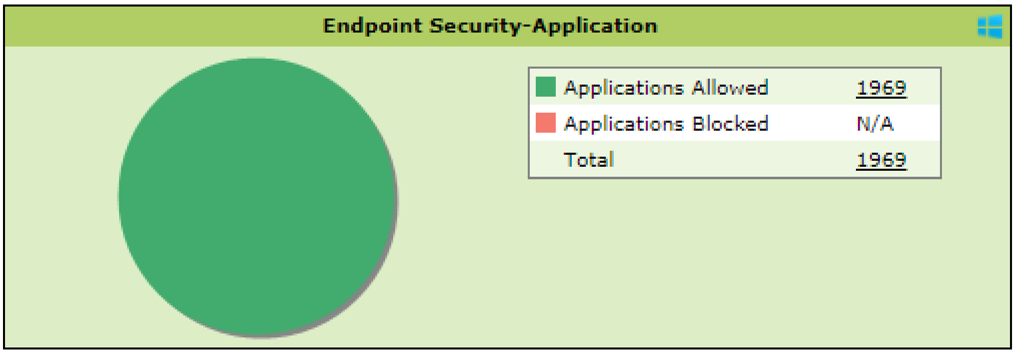


Endpoint Security-USB

🟩	USB Allowed	0
🟥	USB Blocked	0
	Total	0

USB Allowed – It displays the number of USB access allowed along with the USB details for the same by Endpoint Security-USB module.
USB Blocked – It displays the number of USB access blocked along with the USB details for the same by Endpoint Security-USB module.
Total – It displays the total number of USB connections monitored along with the USB details for the same by Endpoint Security-USB module since last seven days.

Endpoint Security-Application



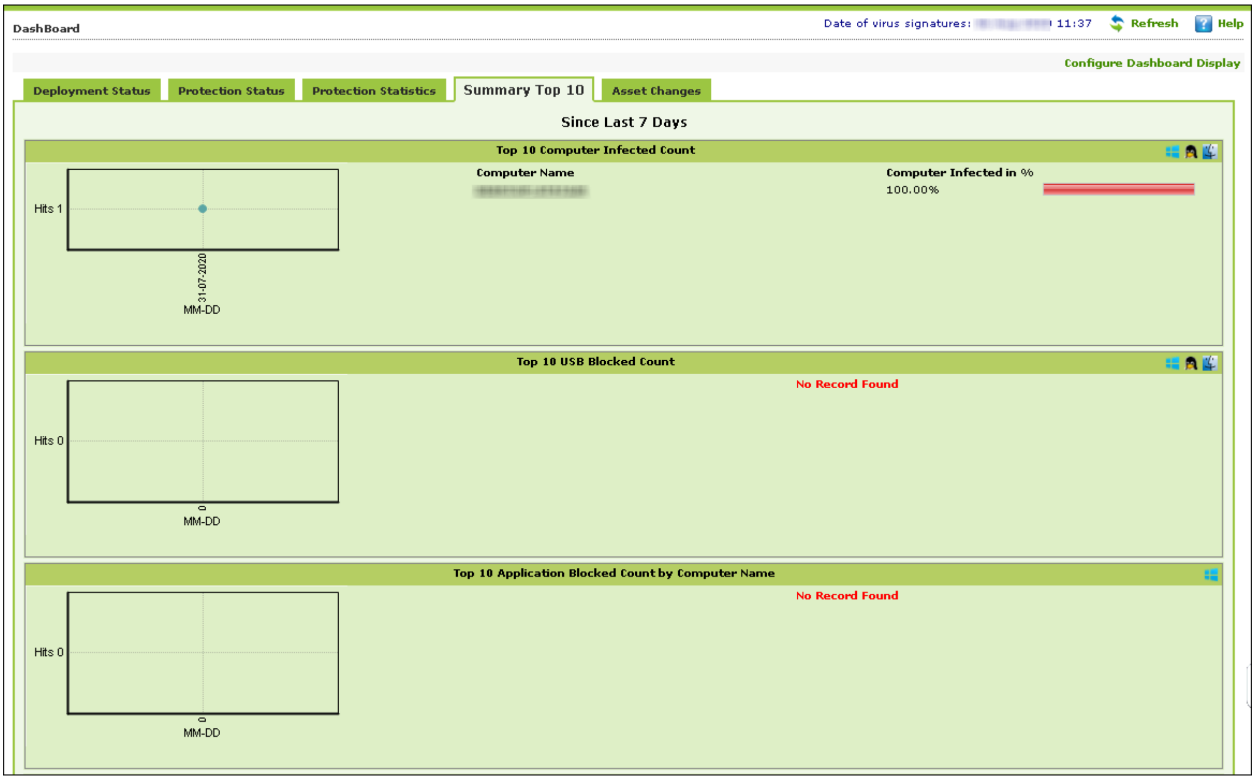
Endpoint Security-Application

🟩	Applications Allowed	1969
🟥	Applications Blocked	N/A
	Total	1969

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.
Total – It displays the total number of applications monitored by Endpoint Security-Application module since last seven days.

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**.

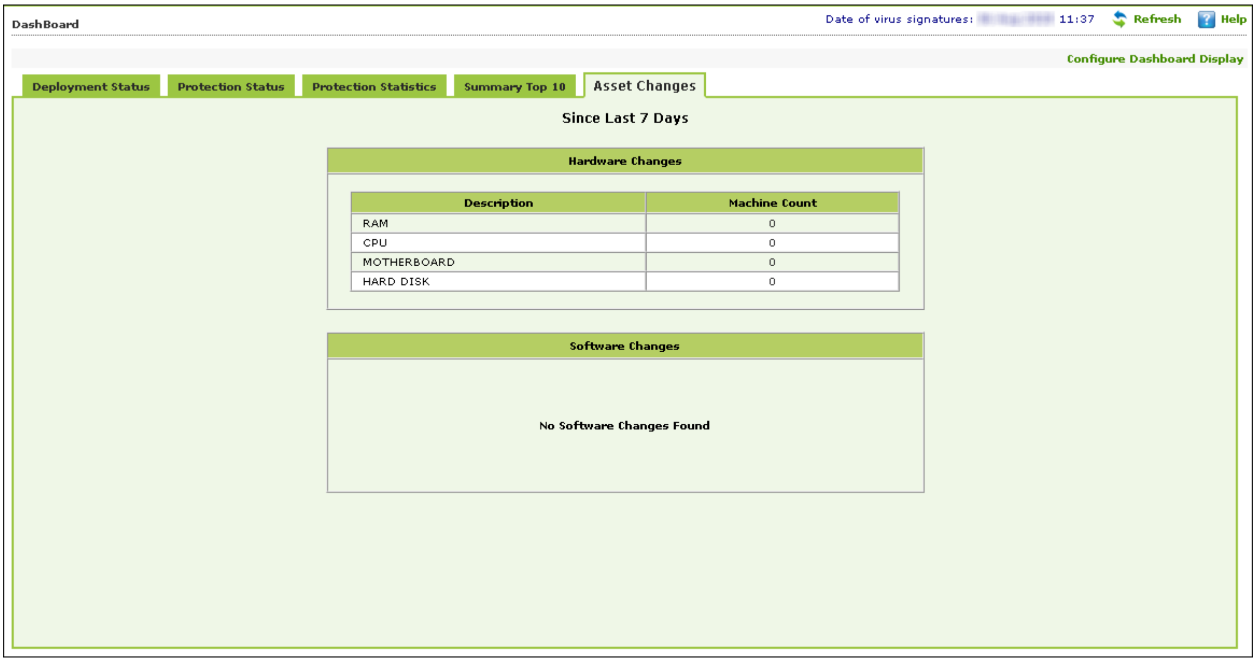


The tab displays the summary for following parameters:

- Top 10 Computer Infected Count
- Top 10 Infected Emails (Mail AV)
- Top 10 USB Blocked Count
- Top 10 Application Blocked Count by Computer Name
- Top 10 Application Allowed Count by Computer Name
- Top 10 Websites Blocked Count by Computer Name
- Top 10 Websites Allowed Count by Computer Name
- 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.



DashBoard

Date of virus signatures: [redacted] 11:37

Since Last 7 Days

Hardware Changes

Description	Machine Count
RAM	0
CPU	0
MOTHERBOARD	0
HARD DISK	0

Software Changes

No Software Changes Found

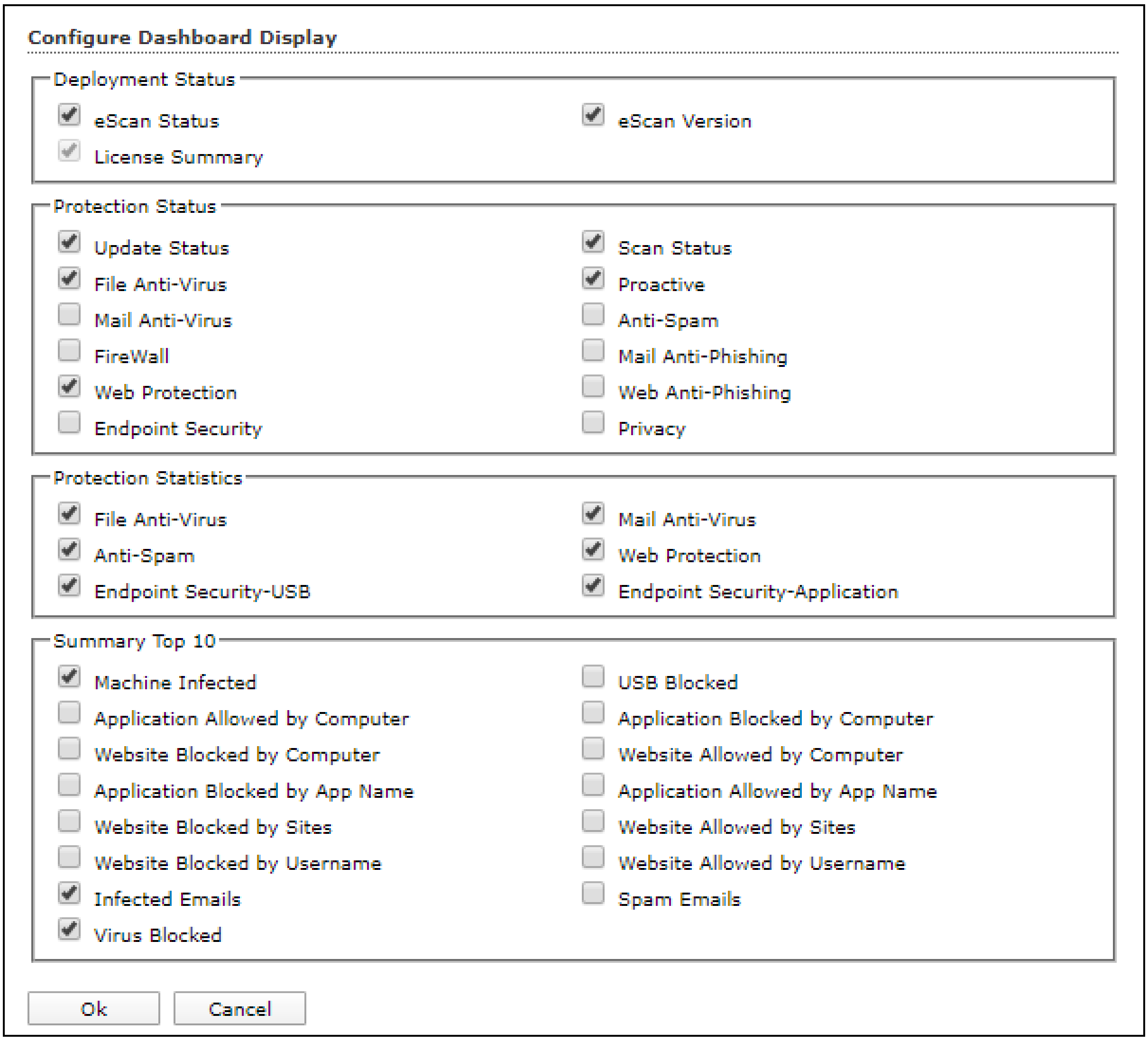
Clicking the underlined machine names displays softwares installed on the computers since last seven days. Clicking the underlined numerical displays installed / uninstalled softwares on computers since last seven days.

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

☑ Update Status ☑ Scan Status

☑ File Anti-Virus ☑ Proactive

□ Mail Anti-Virus □ Anti-Spam

□ FireWall □ Mail Anti-Phishing

☑ Web Protection □ Web Anti-Phishing

□ Endpoint Security □ Privacy

Protection Statistics

☑ File Anti-Virus ☑ Mail Anti-Virus

☑ Anti-Spam ☑ Web Protection

☑ Endpoint Security-USB ☑ Endpoint Security-Application

Summary Top 10

☑ Machine Infected □ 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

☑ Infected Emails □ Spam Emails

☑ Virus Blocked

2. Select the parameters' check boxes to be displayed in the respective tabs.
3. Click **OK**.

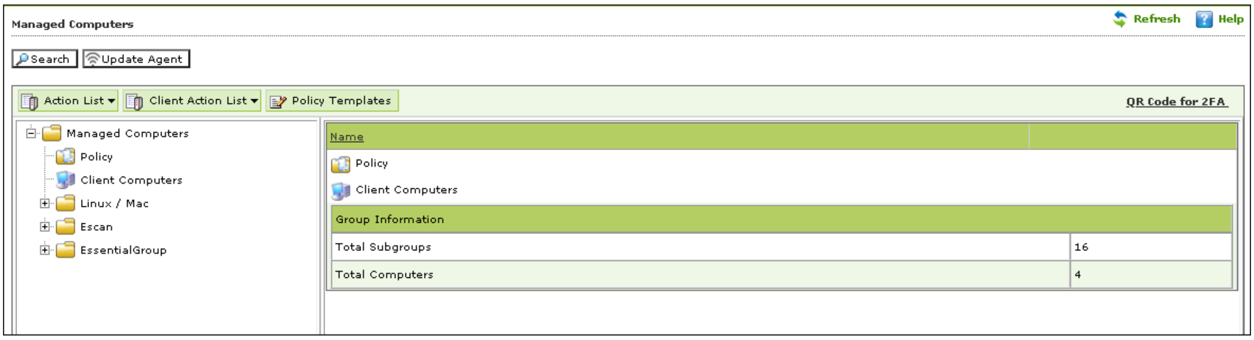
   The tabs will be updated according to the changes.

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 a group, define policy templates for the created groups and computers, create policy criteria templates and tasks for specific groups.

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.



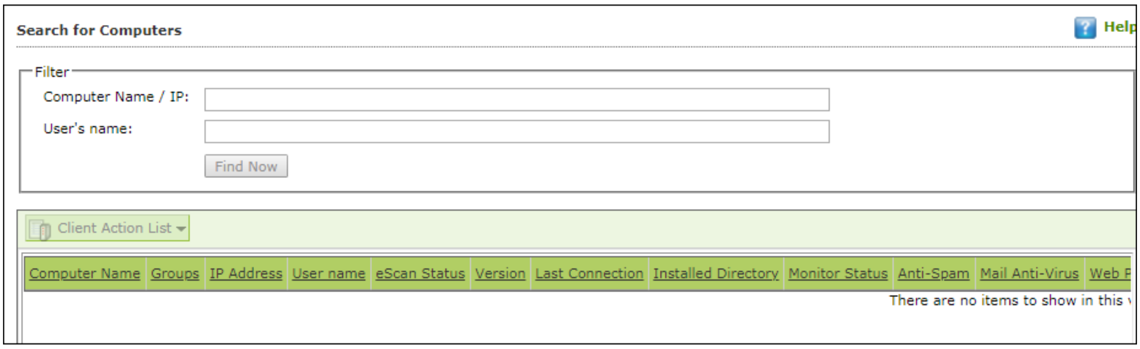
Group Information	
Total Subgroups	16
Total Computers	4

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.



Search for Computers

Filter

Computer Name / IP:

User's name:

Computer Name	Groups	IP Address	User name	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam	Mail Anti-Virus	Web F

There are no items to show in this v

The Filter section displays following fields:

Computer Name/IP

Enter a computer name or IP address. You can also search the computer using wildcard entry. For example, **admin***, this will display computers starting with name **admin**.

Username

Enter a username.

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

Update Agent

eScan lets you use a client computer as an update agent to deploy updates on groups of computers.

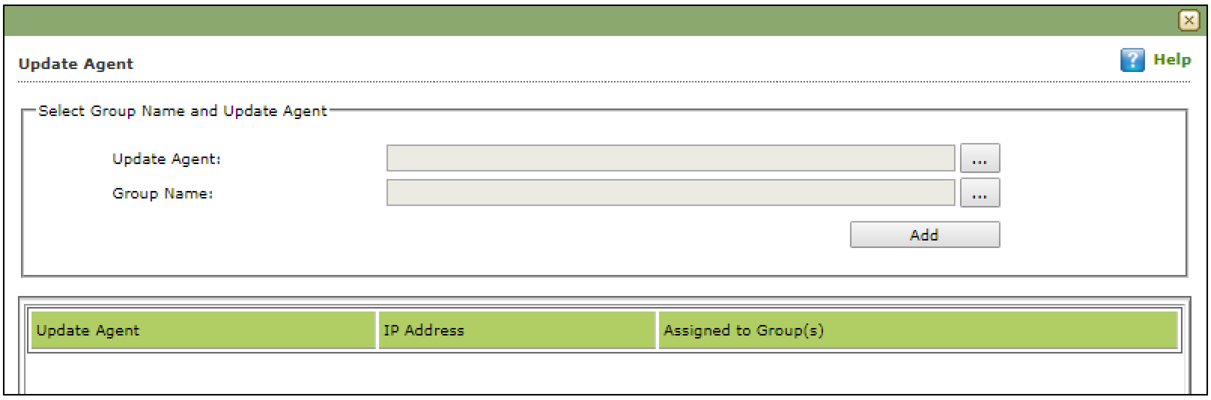
By default, eScan server distributes the virus definitions and policies to all the clients added in the web console. But, if you want to reduce server's workload, you can create an Update Agent for the respective group(s). The Update Agent will receive virus definitions and policies from server and distribute it to the assigned group(s). For more details, please see 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. The window also lets you **Add** or **Remove** Update Agents from this list. You can set an Update Agent for multiple groups.

Add an Update Agent

To add an Update Agent

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



Update Agent

Help

Select Group Name and Update Agent

Update Agent: [...]

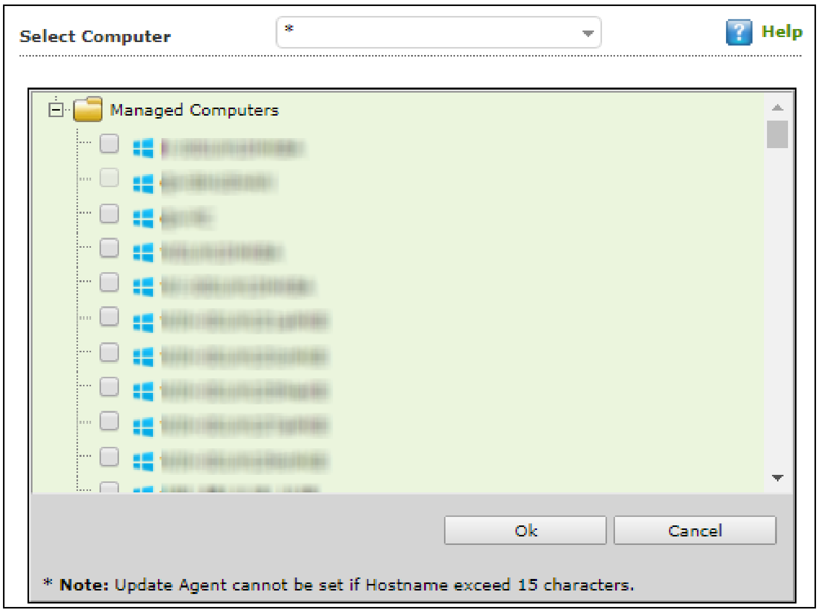
Group Name: [...]

Add

Update Agent	IP Address	Assigned to Group(s)

2. Click ... next to Update Agent box, to select the computer.

3. Select Computer widow appears.



Select Computer *

Help

Managed Computers

Ok Cancel

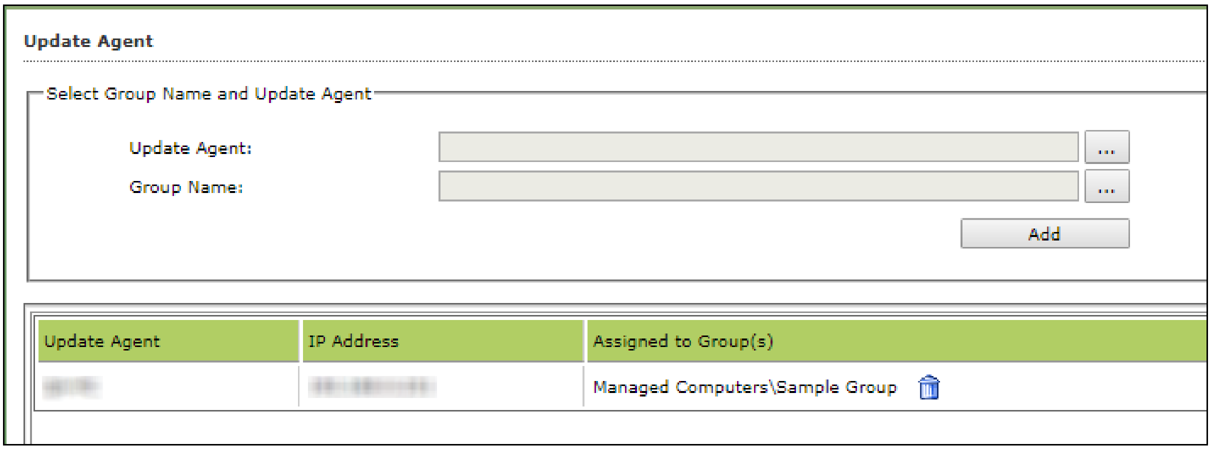
* **Note:** Update Agent cannot be set if Hostname exceed 15 characters.

3. Select a computer and then click **OK.**
4. Click ... next to Group Name box, to select the Group Name**.**
5. This is the group to which the selected computer will act as an Update Agent and provide updates.
6. Select the Group and then click **OK.**
7. Click **Add.**
   The Update Agent will be set for the selected group.

Delete an Update Agent

To delete an Update Agent

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



Update Agent

Select Group Name and Update Agent

Update Agent: [ ] ...

Group Name: [ ] ...

Add

Update Agent	IP Address	Assigned to Group(s)
[redacted]	[redacted]	Managed Computers\Sample Group 🗑

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

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

Action List

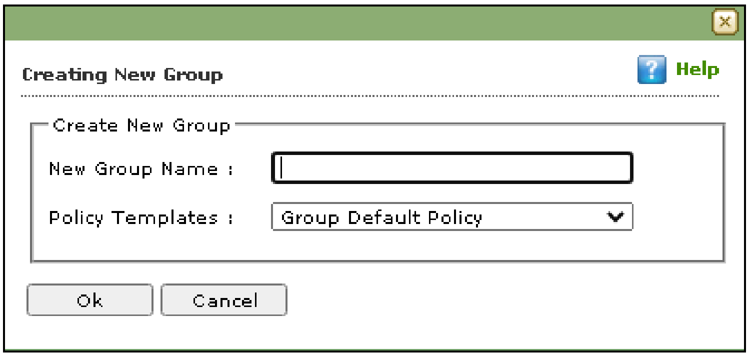
The Action List takes you action for a group. The drop-down contains following options:

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

New Subgroup

To create a Subgroup

1. In Managed Computers screen, click **Action List** > **New Subgroup**.
   Creating New Group window appears.



Creating New Group

Create New Group

New Group Name :

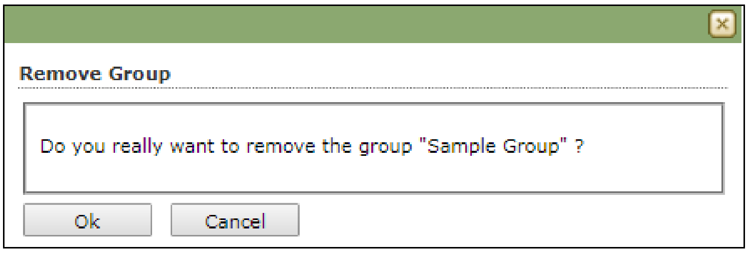
Policy Templates : Group Default Policy

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.

Remove Group

To remove a Group

1. In Managed Computers screen, select a group.
2. Click **Action List** > **Remove group**.
   A confirmation prompt appears.



Remove Group

Do you really want to remove the group "Sample Group" ?

3. Click **OK**.
4. The group gets removed.

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

Managing Installations

After grouping all computers in logical groups using eScan Management Console, you can now install eScan Client on the computers connected to your network.
This section will give you an overview on following activities:

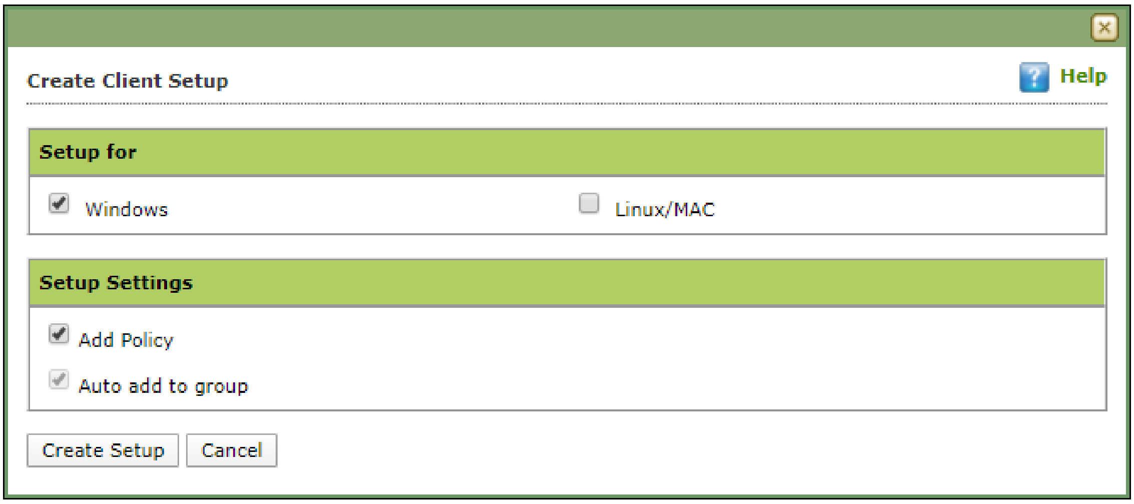
eScan Client Installation
Users will have to install eScan client manually on their computers. It does not require any remote assistance.

Viewing Installed Software List
Using Show Installed Software option you can view list of software installed on Computers connected to your network. You will find this option in **Client Action list** under **Managed Computers** when you select a computer**.**

Create Client Setup

To create a Client Setup

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

Setup for

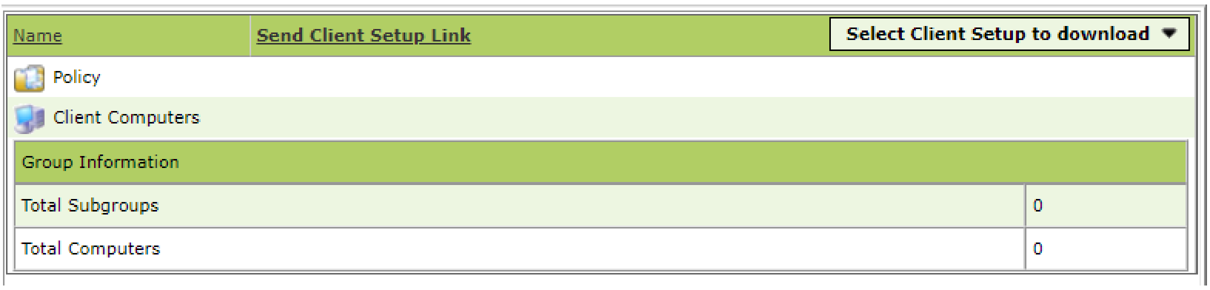
☑ Windows ☐ Linux/MAC

Setup Settings

☑ Add Policy

☑ Auto add to group

2. Select the appropriate options and then click **Create Setup**.
   The Client setup will be created and a download link will be displayed in right pane.

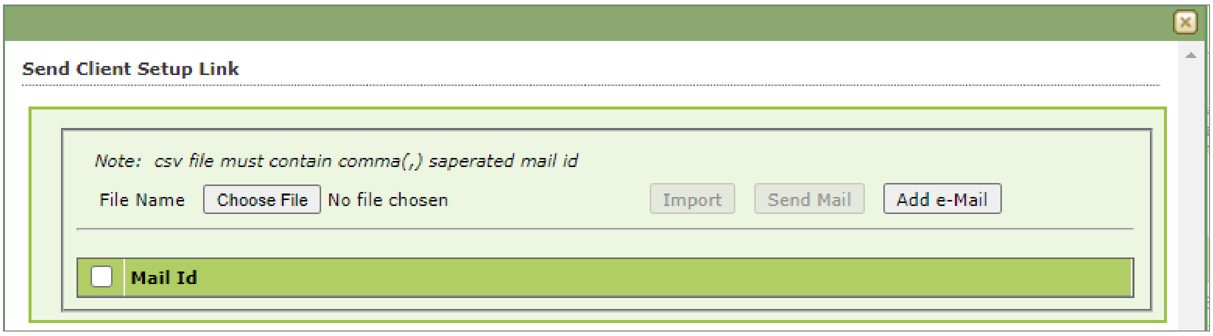


Group Information	
Total Subgroups	0
Total Computers	0

Send Client Setup Link

To send the Client Setup Link

1. Go to **Managed Computers** and select the specific group containing client computer,
2. Click **Send Client Setup Link**.
   Send Client Setup Link window appears.



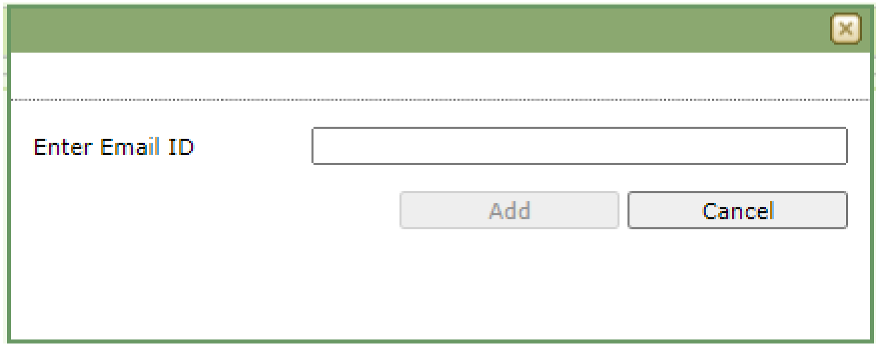
Send Client Setup Link

Note: csv file must contain comma(,) saperated mail id

File Name [Choose File] No file chosen [Import] [Send Mail] [Add e-Mail]

□ Mail Id

5. If you want to send setup link to multiple clients, click **Choose File**, select the csv file containing email IDs and then click **Import** > **Send Mail**. If you want to send setup link to a single client, click **Add email**.



Enter Email ID

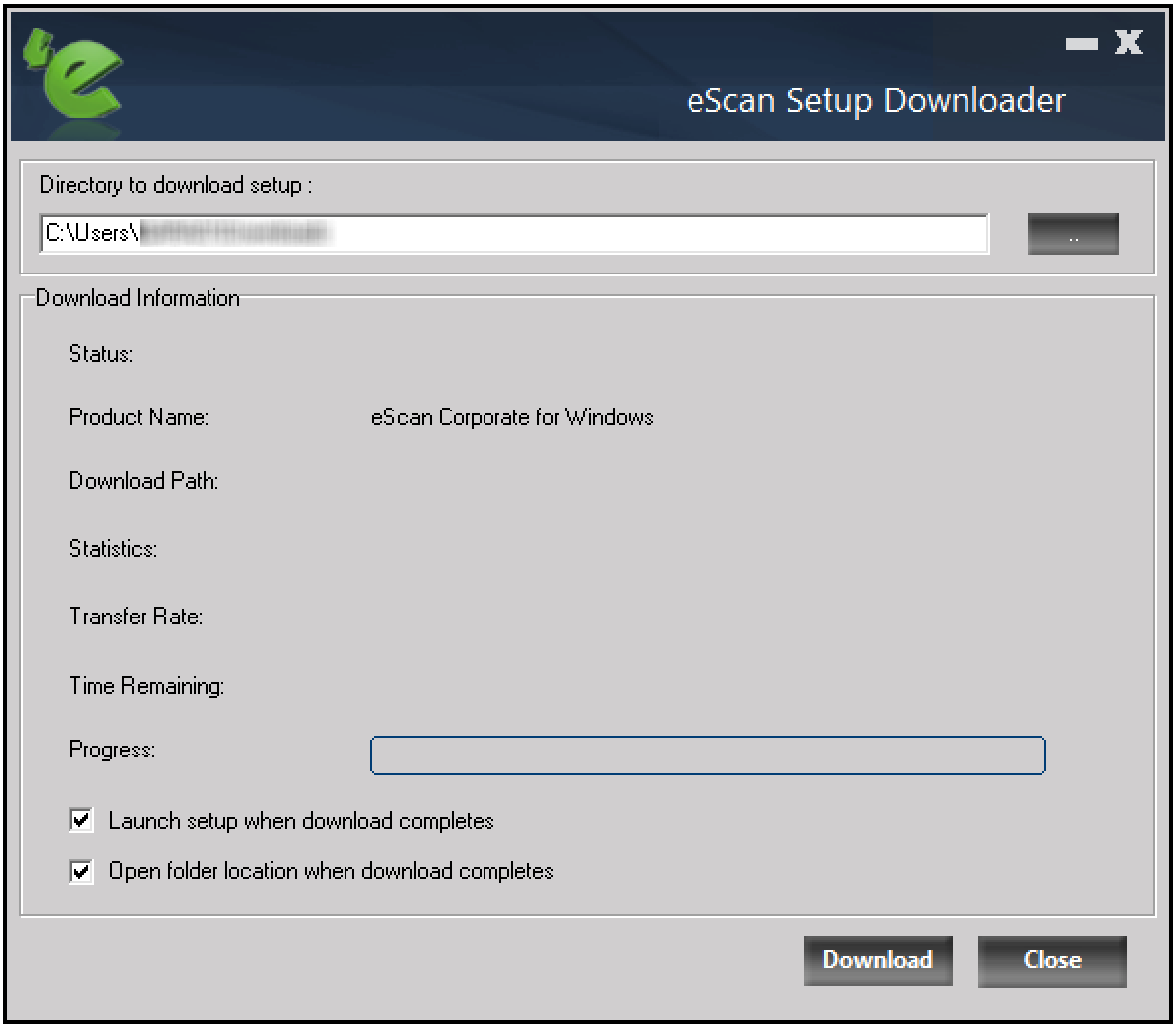
6. Enter the email ID and then click **Add**.
7. Click **Send Mail**.

The Client Setup link will be sent to the users via email.

eScan Client Installation for Windows

To install eScan Client on Windows

1. Go to the path where eScan setup file is downloaded.
2. Double-click the setup file.
   eScan Setup Downloader window appears.



eScan Setup Downloader

Directory to download setup :
C:\Users\[redacted]

Download Information

Status:
Product Name: eScan Corporate for Windows
Download Path:
Statistics:
Transfer Rate:
Time Remaining:
Progress:

☑ Launch setup when download completes
☑ Open folder location when download completes

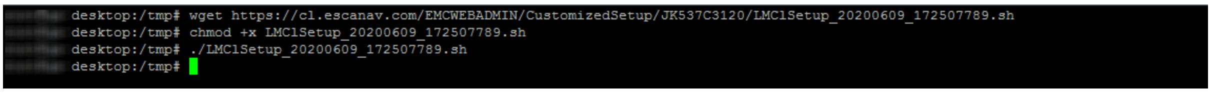
3. Enter the preferred directory to download setup file.
4. Select the checkboxes as per your preference and then click **Download**.

eScan Client Installation for Linux

To install eScan client on Linux

NOTE	Ensure that you have sudo user or root user authentication for installation.

1. Go to the path where eScan setup file is downloaded.
2. Execute the shell script by entering following commands.



```
[redacted] desktop:/tmp# wget https://cl.escanav.com/EMCWEBADMIN/CustomizedSetup/JK537C3120/LMClSetup_20200609_172507789.sh
[redacted] desktop:/tmp# chmod +x LMClSetup_20200609_172507789.sh
[redacted] desktop:/tmp# ./LMClSetup_20200609_172507789.sh
[redacted] desktop:/tmp# █
```

eScan Client Installation for Mac

To install eScan client on Mac

NOTE	Ensure that you have sudo user authentication for installation.

1. Open the Terminal.
2. Follow the Installation for Linux procedure as shown above.

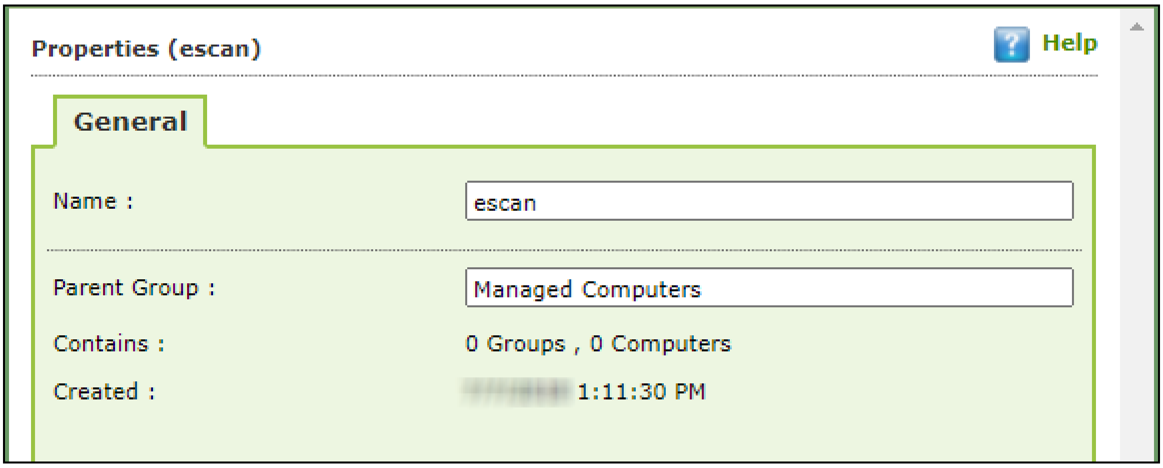
Understanding the eScan Client Protection Status

🟩 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.

Properties

To view the properties of a group:

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



Properties (escan)

Name : escan

Parent Group : Managed Computers

Contains : 0 Groups , 0 Computers

Created : [redacted] 1:11:30 PM

In Properties, General tab displays following details:

- Group Name
- Parent Group
- Sub Groups or Number of Computers in that Group
- Creation date of the Group

Client Action List

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

- **Move to Group**
- **Remove from Group**
- **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. Click **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 then click **OK**.
   The computers will be moved to the selected group.

Remove from Group

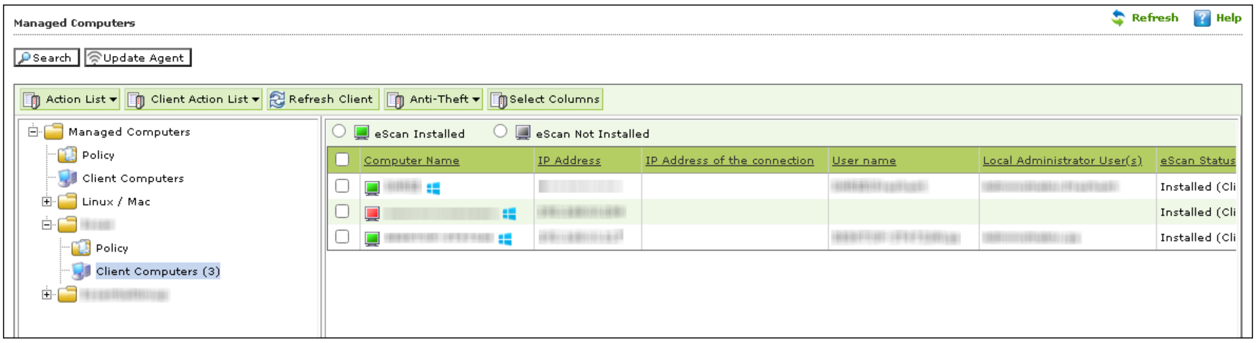
To remove computers from a group,

1. Click **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.

Export

To export a client computer's data,

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.



Managed Computers

Refresh Help

Search | Update Agent

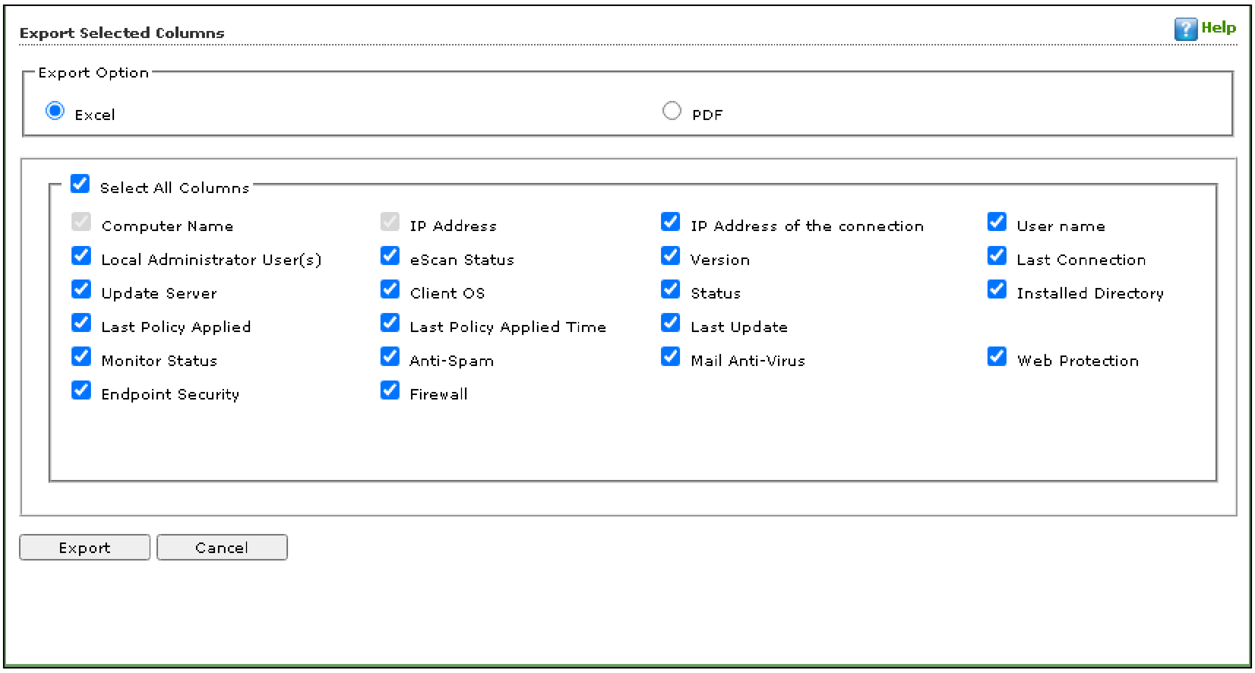
Action List ▾ | Client Action List ▾ | Refresh Client | Anti-Theft ▾ | Select Columns

- Managed Computers
  - Policy
  - Client Computers
  - Linux / Mac
  - [redacted]
    - Policy
    - Client Computers (3)
  - [redacted]

○ eScan Installed ○ eScan Not Installed

□	Computer Name	IP Address	IP Address of the connection	User name	Local Administrator User(s)	eScan Status
□	[redacted]	[redacted]		[redacted]	[redacted]	Installed (Cli
□	[redacted]	[redacted]				Installed (Cli
□	[redacted]	[redacted]		[redacted]	[redacted]	Installed (Cli

2. Select a client computer and the 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 Option

● Excel ○ PDF

☑ Select All Columns

☑ Computer Name
☑ Local Administrator User(s)
☑ Update Server
☑ Last Policy Applied
☑ Monitor Status
☑ Endpoint Security

☑ IP Address
☑ eScan Status
☑ Client OS
☑ Last Policy Applied Time
☑ Anti-Spam
☑ Firewall

☑ IP Address of the connection
☑ Version
☑ Status
☑ Last Update
☑ Mail Anti-Virus

☑ User name
☑ Last Connection
☑ Installed Directory
☑ Web Protection

Export | Cancel

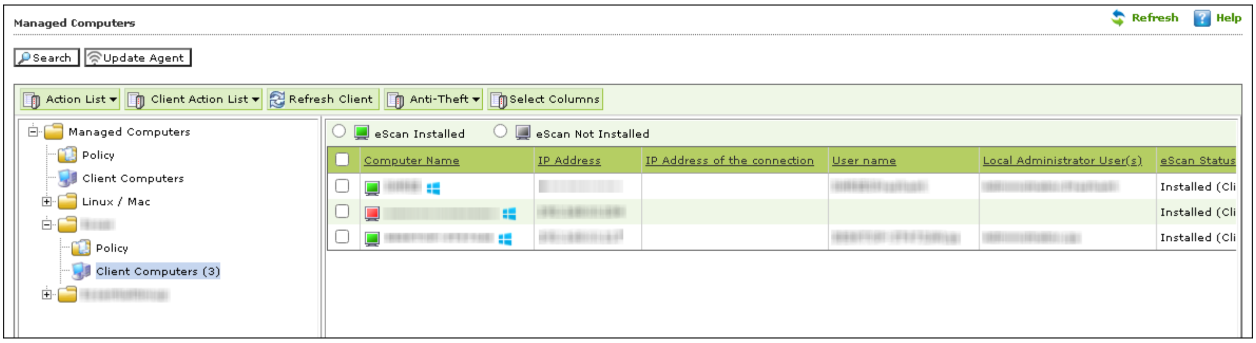
3. Select the preferred export option.
4. Select the preferred report columns.
5. Click **Export**.

The report will be exported as per your preferences.

Show Installed Softwares

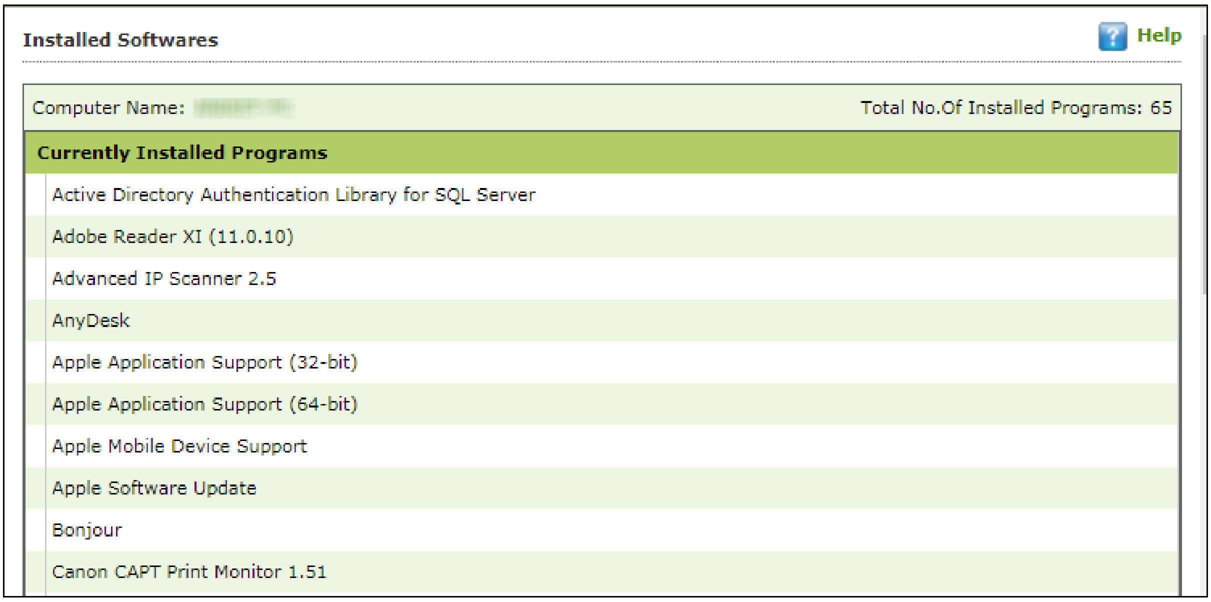
This feature displays a list of installed softwares on a computer.
To view the list of installed softwares,

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	Local Administrator User(s)	eScan Status
□	[redacted]	[redacted]		[redacted]	[redacted]	Installed (Cli
□	[redacted]	[redacted]				Installed (Cli
□	[redacted]	[redacted]		[redacted]	[redacted]	Installed (Cli

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: [redacted]   Total No.Of Installed Programs: 65

Currently Installed Programs
Active Directory Authentication Library for SQL Server
Adobe Reader XI (11.0.10)
Advanced IP Scanner 2.5
AnyDesk
Apple Application Support (32-bit)
Apple Application Support (64-bit)
Apple Mobile Device Support
Apple Software Update
Bonjour
Canon CAPT Print Monitor 1.51

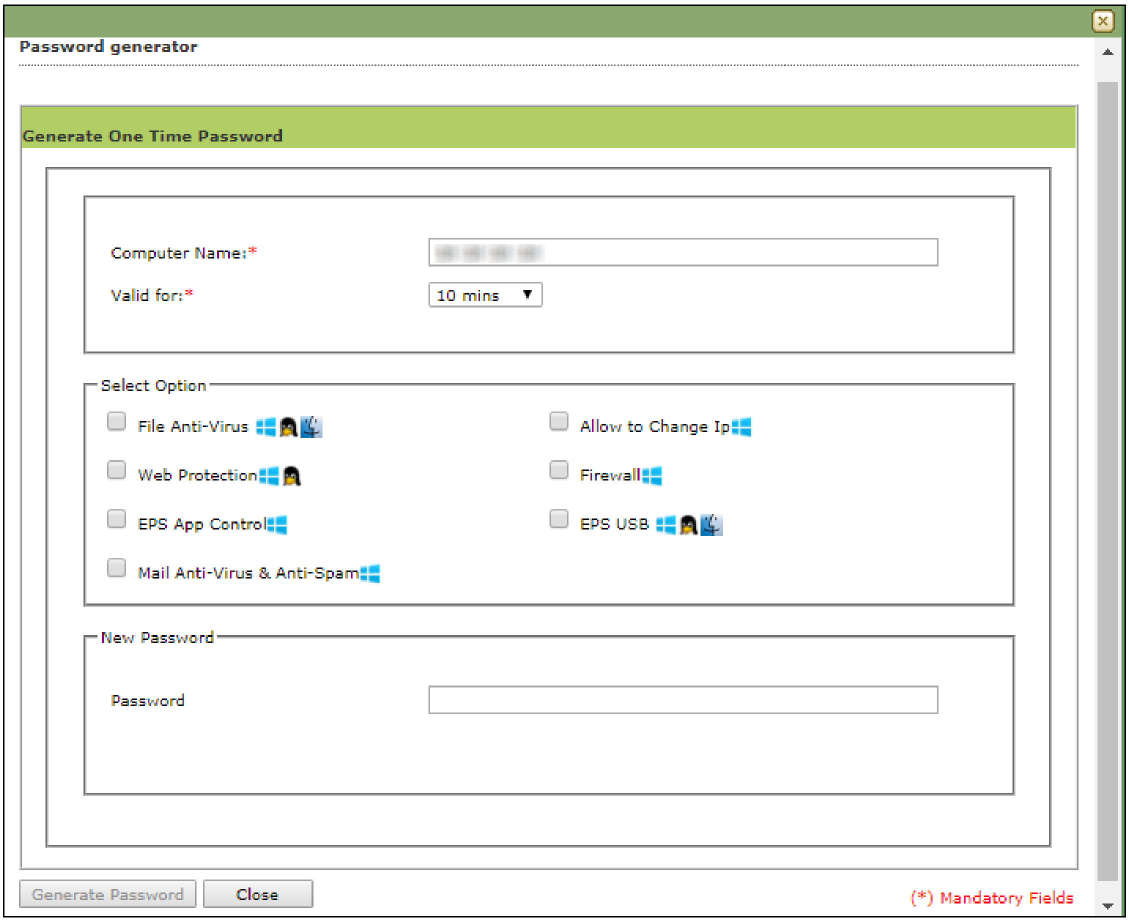
One Time Password

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 for that disables USB block policy on specific computer. The administrator can define policy disable duration ranging from 10 minutes to 26 days 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

□ File Anti-Virus
□ Allow to Change Ip
□ Web Protection
□ Firewall
□ EPS App Control
□ EPS USB
□ Mail Anti-Virus & Anti-Spam

New Password

Password

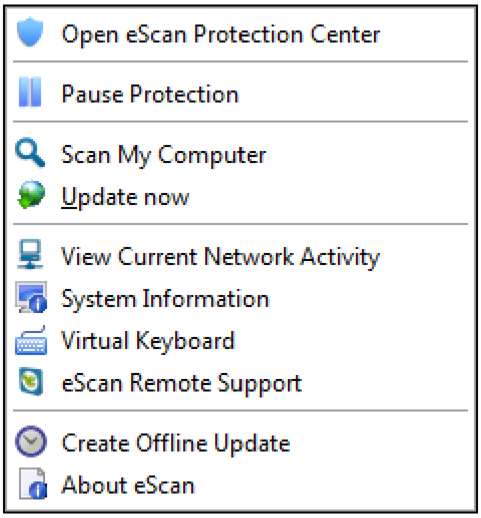
(*) Mandatory Fields

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.
1. Click **Generate Password**.
2. An OTP will be generated and displayed in **Password** field.

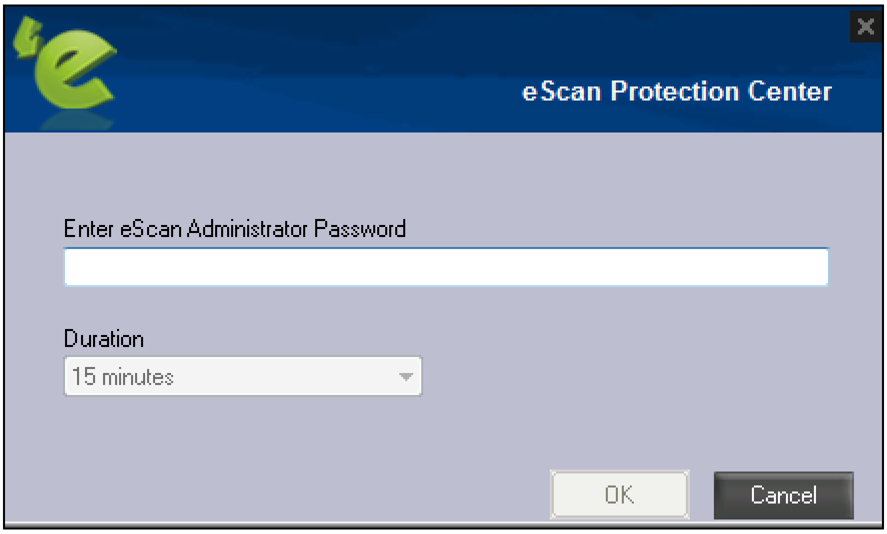
Entering an OTP

To enter an OTP, follow the steps given below:

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



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



Enter eScan Administrator Password

Duration
15 minutes

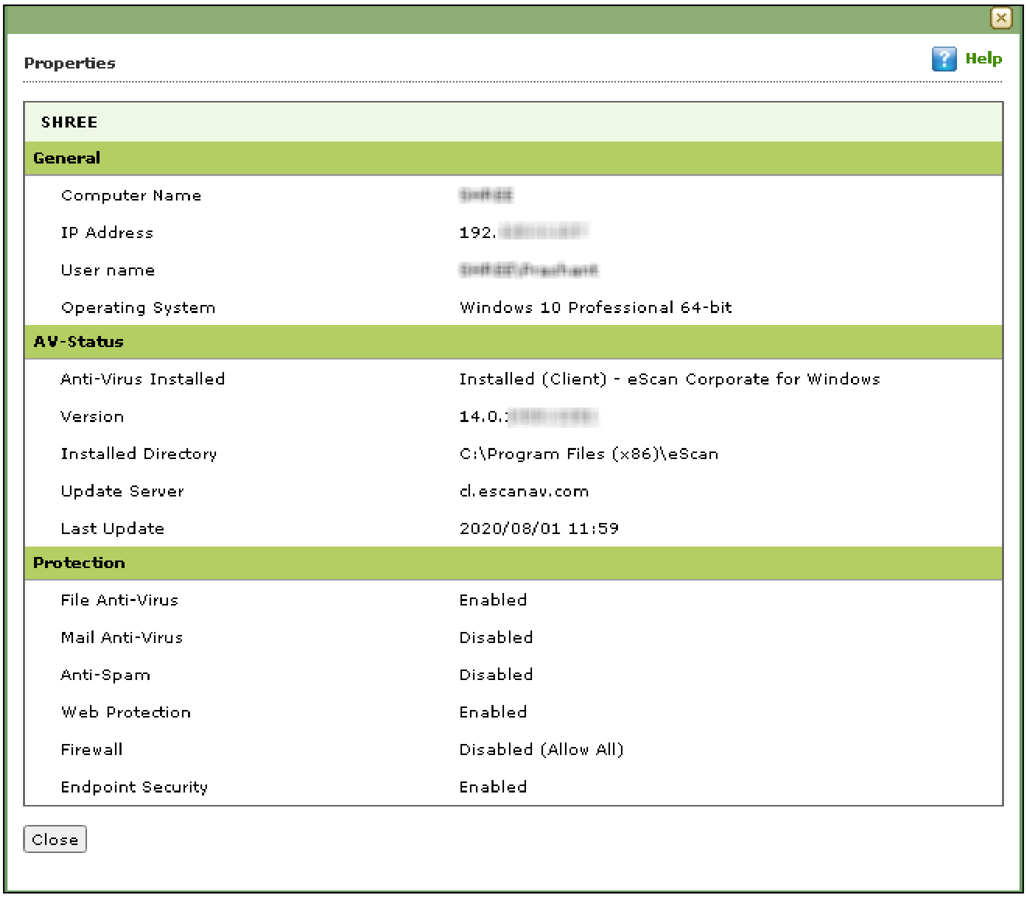
3. Enter the OTP in the field.
4. Click **OK**.
   The selected module will be disabled for set duration.

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.



Properties

SHREE

General	
Computer Name	[redacted]
IP Address	192.[redacted]
User name	[redacted]
Operating System	Windows 10 Professional 64-bit
AV-Status	
Anti-Virus Installed	Installed (Client) - eScan Corporate for Windows
Version	14.0.[redacted]
Installed Directory	C:\Program Files (x86)\eScan
Update Server	cl.escanav.com
Last Update	2020/08/01 11:59
Protection	
File Anti-Virus	Enabled
Mail Anti-Virus	Disabled
Anti-Spam	Disabled
Web Protection	Enabled
Firewall	Disabled (Allow All)
Endpoint Security	Enabled

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

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 will be refreshed with current status.

Anti-Theft

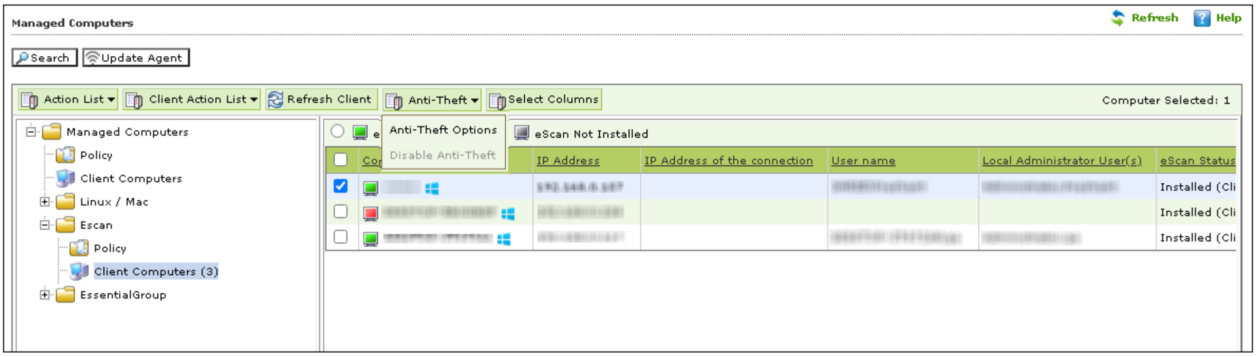
Anti-Theft portal is an online portal that can be accessed through any computer, laptop, tablet or phone at eScan Corporate Edition – Cloud (With Hybrid Network Support). From the anti-theft portal you can trace the last location of your lost or stolen system through this portal. This will help you in tracing your system in case of lost or theft. You can use the scream option to check if the device is in the vicinity, if you still can't find the system, set the system as lost / stolen on the anti-theft portal and the Locate, Scream, Camera, and Alert features will be activated and will be performed on the system.

Note: The lost/stolen system should be connected to the internet for efficient functioning of all the features.

You can remotely execute the following commands through the Anti-Theft portal on your lost Windows. For the successful execution of the commands, the laptops will have to be added to the anti-theft portal prior to the loss or theft of the device. On the anti-theft portal it will display windows device that are added to Anti-Theft.

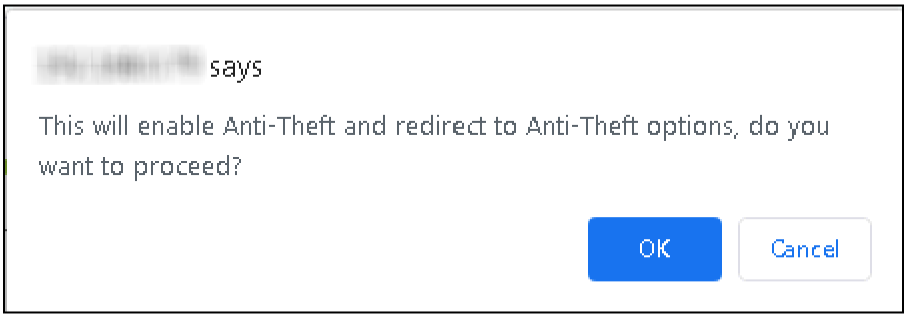
Enabling Anti-Theft for a Specific System

1. Under any group, click **Client Computers**. A list of computers appears on the right pane.
2. Select a computer.
3. Click on **Anti-Theft** option.



	Co	IP Address	IP Address of the connection	User name	Local Administrator User(s)	eScan Status
☑	[redacted]	[redacted]		[redacted]	[redacted]	Installed (Cli
☐	[redacted]	[redacted]				Installed (Cli
☐	[redacted]	[redacted]		[redacted]	[redacted]	Installed (Cli

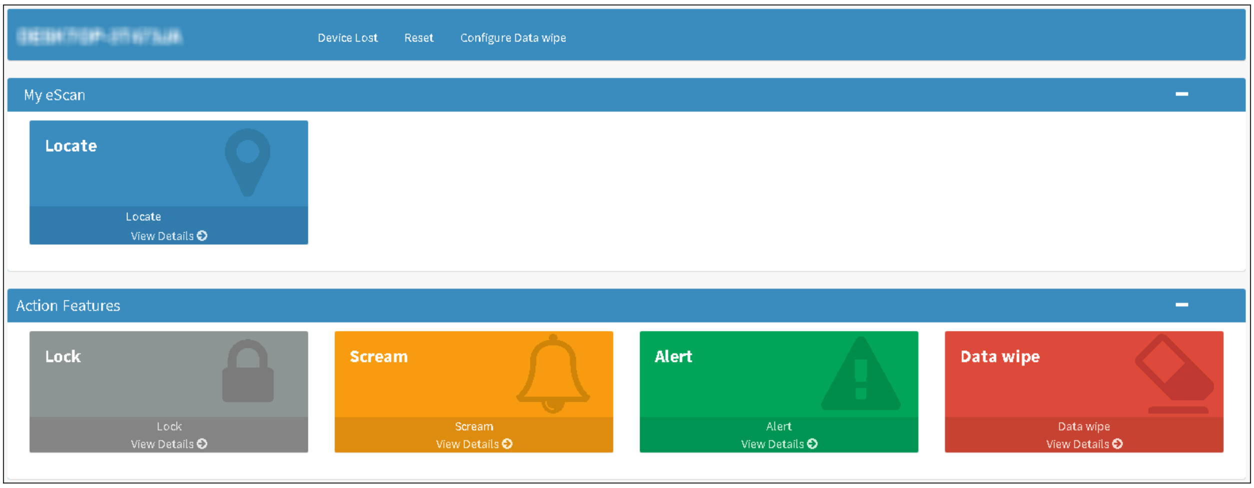
4. After clicking **Anti-Theft Options**. You will get the following pop-up:



[redacted] says

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

5. After configuring the above details, you will be redirected to the following pages:



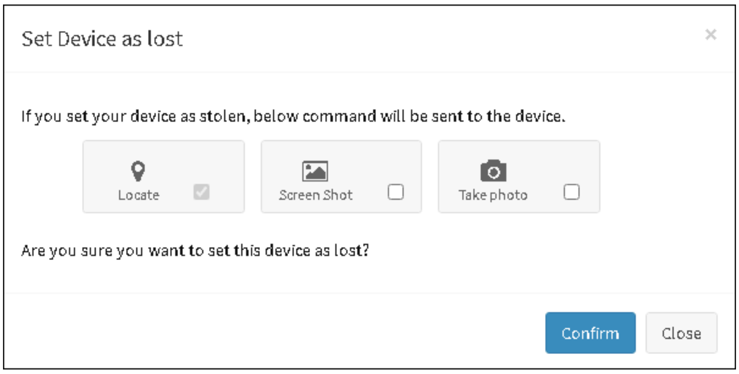
6. The user can configure various options available in the Anti-Theft portal.

Configuring Options

In case of your system is lost or stolen, you can go to Anti-Theft portal and it will display all the features that can be activated.

Device Lost

1. In case of loss or theft, click on the device name that has been lost or stolen, the status bar under it will display the system name.
2. Click **Device Lost** and this will allow you to enable the features Locate, ScreenShot, and Take photo (Camera).



Set Device as lost

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

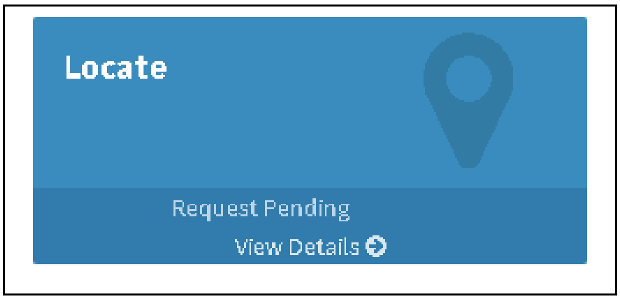
Are you sure you want to set this device as lost?

3. Select the option and click **Confirm** to confirm that your system has been lost and to execute the commands Locate, Screenshot, and Take photo.

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. The following are the steps 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.

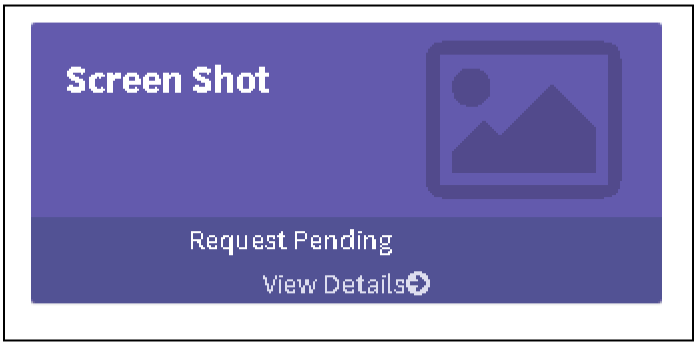


2. View Details displays the Last Location of your system on a map. It also shows details of last two successful executions of the Locate command.

Screen Shot

This option will take a screenshot of the system whenever it is synced to the eScan Corporate Edition – Cloud (With Hybrid Network Support):

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.



Screen Shot

Request Pending

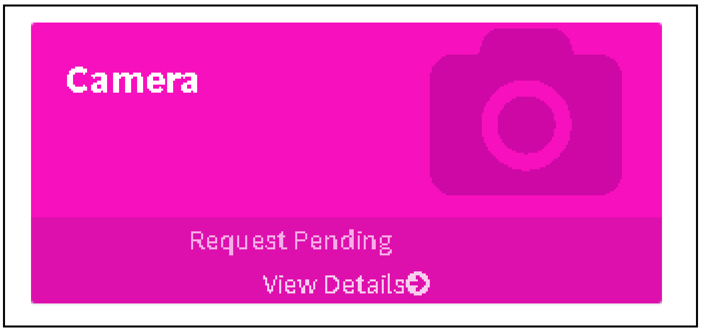
View Details

2. View Details displays the last two screenshots from the successful execution of the screenshot command.

Take Photo (Camera)

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.



Camera

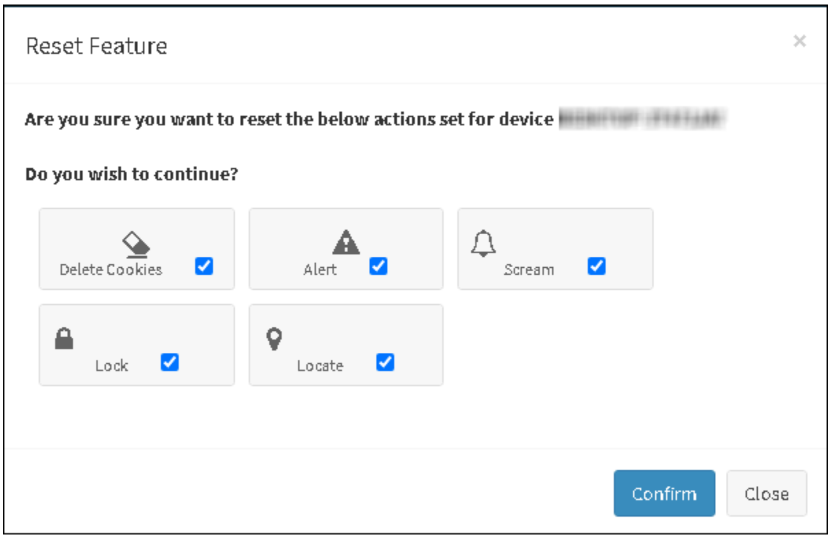
Request Pending

View Details

2. View Details displays the last two snapshots taken from your system.

Reset

To reset the action that were selected to perform on the stolen devices, click **Reset**.



Reset Feature

Are you sure you want to reset the below actions set for device [redacted]

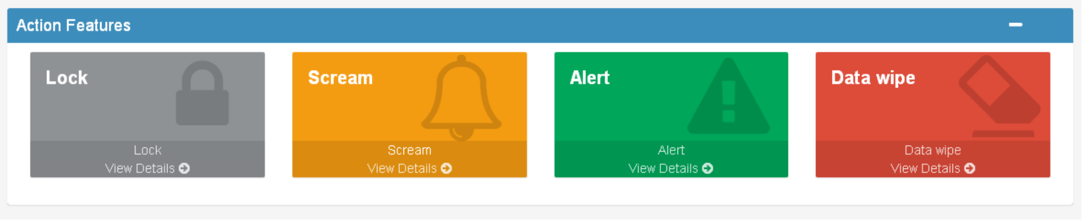
Do you wish to continue?

Delete Cookies ☑ Alert ☑ Scream ☑
Lock ☑ Locate ☑

Select the action that needed to be reset and click **Confirm** button.

Action Features

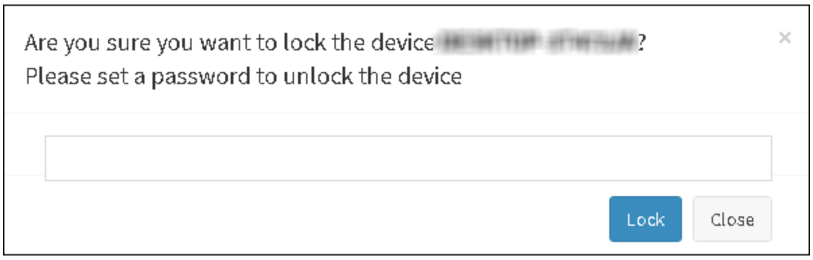
In this option, you can configure the following setting.



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.

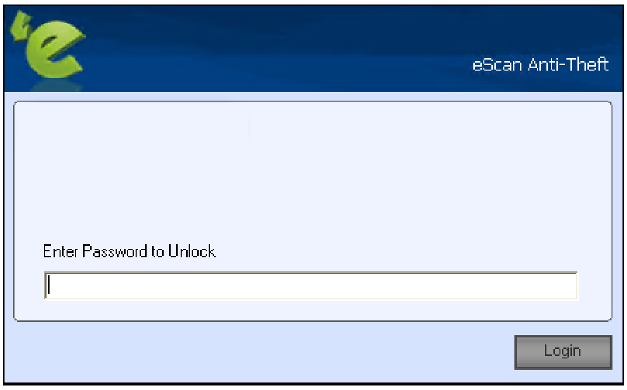
1. On the anti-theft portal, select your System Alias name and then click **Lock** to remotely lock your system, to unlock your system you will have to enter the Secret Code for executing the lock command.



Are you sure you want to lock the device [redacted]?
Please set a password to unlock the device

2. After entering the secret code, click on **Lock**.

3. In case of lost device, this option will not allow the user to login to the system. If a user tries to access your device. The user has to enter the Secret Code set by the administrator before accessing the device.



4. Click **View Details**, to know about the details about the feature lastly used.

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.
- Click **View Details**, to know about the details about the feature lastly used.

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 returned.

- Click **Alert** option to remotely send a message to your lost system. Type in your message in the send message section and click confirm.
- Click **View Details**, to know about the details about the feature lastly used.

Data Wipe

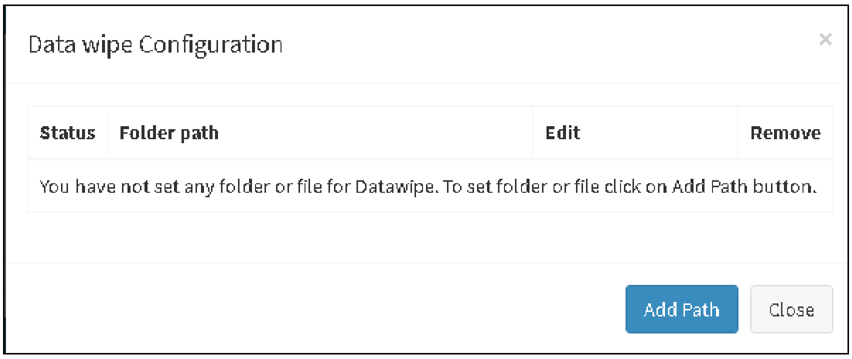
The Data Wipe feature will delete all the selected files and folders that have been added to the "**Configure Data Wipe**" option.

- Click **Data Wipe** option to remotely wipe all the selected files and folders or only delete the cookies and click confirm.
- Click **View Details**, to know about the details about the feature lastly used.

Configure Data Wipe

You can configure the path of the confidential data that can be deleted from the system, using this option:

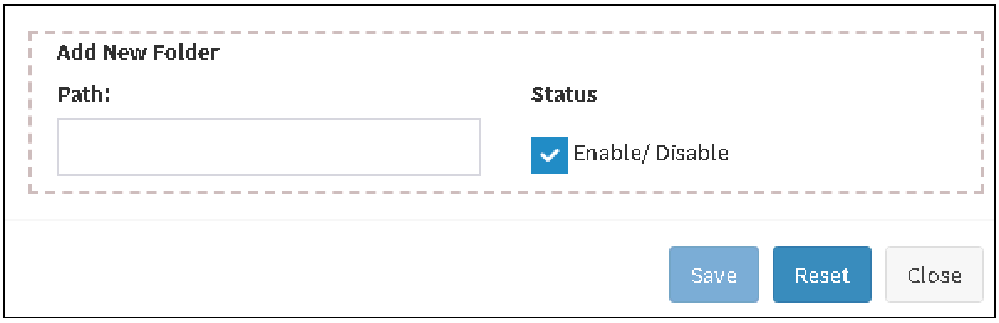
1. Click on the **Configure Data Wipe** option.
   Data wipe Configuration window pop-up.



Data wipe Configuration

Status	Folder path	Edit	Remove
You have not set any folder or file for Datawipe. To set folder or file click on Add Path button.			

2. Click **Add Path** button. You can add the path of the folder/data is present and also configure the status of the feature by enabling or disabling it.



Add New Folder

Path:

Status

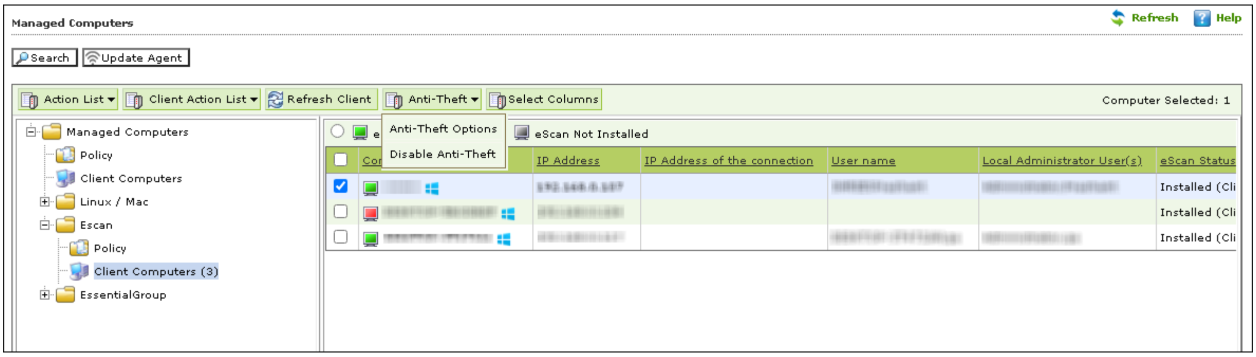
☑ Enable/ Disable

3. After providing the details click **Save** button. You can also reset the option by clicking on **Reset** button.

NOTE	• Successful execution of all the features is completely dependent on the internet connection on the lost / stolen laptop. • If the device is set as lost, the time taken for the device to sync with the anti-theft portal is five minutes. • The Status for all the features and actions will remain as "Request Pending" till the lost or stolen laptop is synced with the eScan anti-theft portal. • If the device is not set as lost, it will take ten minutes to sync with the anti-theft portal if the system is connected to internet. • The camera and Screenshot feature will save only the last two successful executions on the anti-theft portal. • Once you have recovered your system, click on "I recovered device" to deactivate all the features.

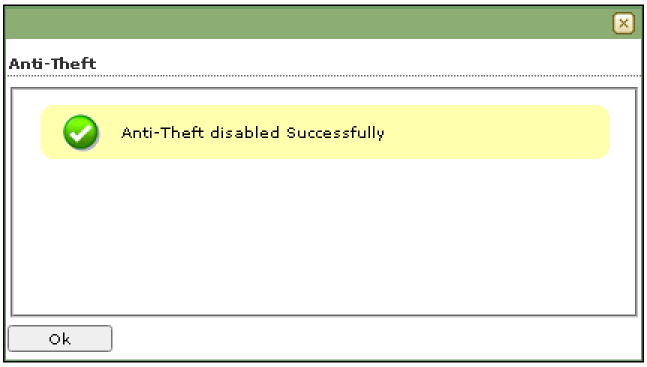
Disabling Anti-Theft for a Specific System

1. Under any group, click **Client Computers**. A list of computers appears on the right pane.
2. Select a computer.
3. Click on **Anti-Theft** option.



☐	Cor	IP Address	IP Address of the connection	User name	Local Administrator User(s)	eScan Status
☑	[redacted]	[redacted]		[redacted]	[redacted]	Installed (Cli
☐	[redacted]	[redacted]				Installed (Cli
☐	[redacted]	[redacted]		[redacted]	[redacted]	Installed (Cli

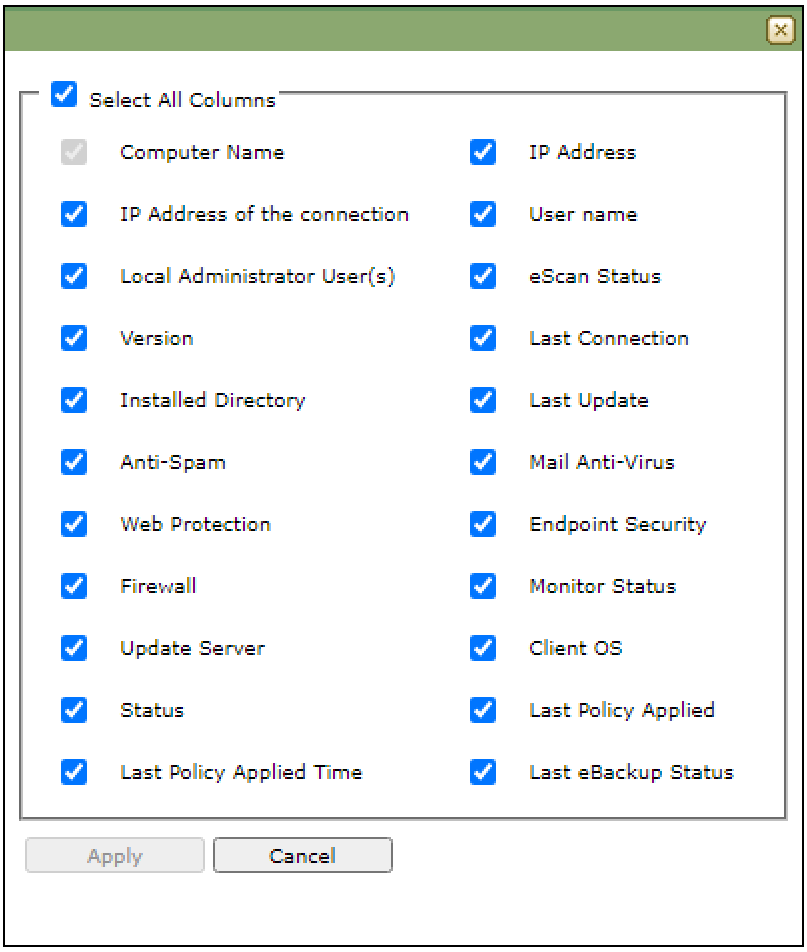
4. Select **Disable Anti-Theft** option from the dropdown menu. You will get a successful pop-up message.



Anti-Theft disabled Successfully

Select Column

This option allows administrator to filter the details of the system:



☑ Select All Columns

☑ Computer Name	☑ IP Address
☑ IP Address of the connection	☑ User name
☑ Local Administrator User(s)	☑ eScan Status
☑ Version	☑ Last Connection
☑ Installed Directory	☑ Last Update
☑ Anti-Spam	☑ Mail Anti-Virus
☑ Web Protection	☑ Endpoint Security
☑ Firewall	☑ Monitor Status
☑ Update Server	☑ Client OS
☑ Status	☑ Last Policy Applied
☑ Last Policy Applied Time	☑ Last eBackup Status

Select the option as per requirement and click **Apply** button.

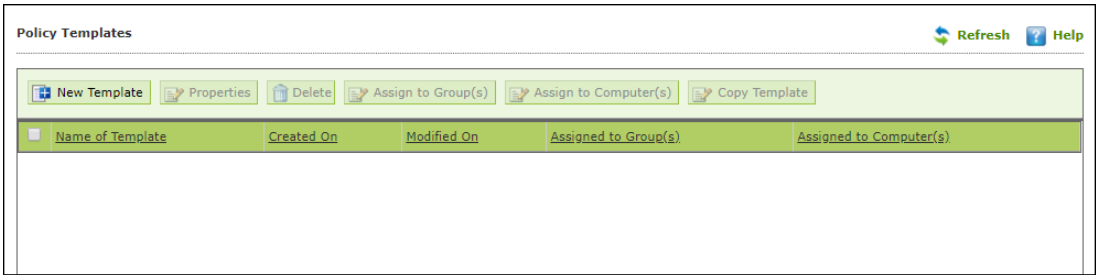
Policy Template

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

Creating a Policy Template

To create a Policy Template follow the below steps:

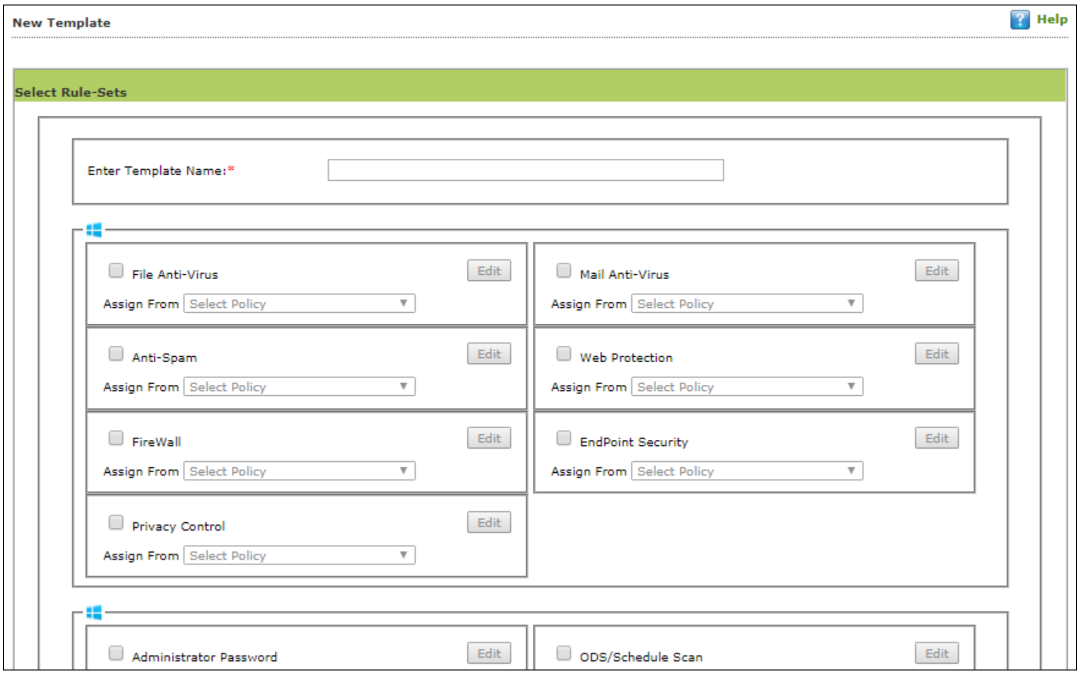
1. Go to Managed Computers.
2. Select the desired group and then click **Policy Template**.
   Policy Template window appears.



Policy Templates

□	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)

3. Click **New Template**.
   New Templates screen appears displaying modules for Windows, Linux and Mac computers.



New Template

Select Rule-Sets

Enter Template Name:*

□ File Anti-Virus
Assign From Select Policy

□ Mail Anti-Virus
Assign From Select Policy

□ Anti-Spam
Assign From Select Policy

□ Web Protection
Assign From Select Policy

□ FireWall
Assign From Select Policy

□ EndPoint Security
Assign From Select Policy

□ Privacy Control
Assign From Select Policy

□ Administrator Password

□ ODS/Schedule Scan

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

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, Mac and Linux computers connected to the network.

Defining Policies Windows computers

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

File Anti-virus
The File Anti-Virus module scans all the existing files and folders for any infection. It also lets you report/disinfect/quarantine/delete infected objects. Moreover, it saves a copy of report file for future reference, and displays attention messages.

Mail Anti-Virus
The Mail Anti-Virus module scans all the incoming and outgoing emails. It scans the emails by breaking it into three sections the header, subject and the body. After scanning, the module combines the sections and sends it to your mailbox.

Anti-Spam
The Anti-Spam module blocks spam emails by checking the content of outgoing and incoming mails and quarantines advertisement emails.

Firewall
The Firewall module lets you put up a restriction to incoming and outgoing traffic and hacking. You can define the firewall settings here. You can define the IP range, permitted applications, trusted MAC addresses and local IP addresses.

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.

Web Protection
The Web Protection module lets you block websites. You can allow/block websites on time-based access restriction.

Endpoint Security
The Endpoint Security module monitors the application on client computers. It allows/ restricts USB, Block list, White list, and defines time restrictions for applications.

Administrator Password
Administrator Password lets you create and change password for administrative login of eScan protection center. It also allows you to set 2FA login credentials.

ODS/Schedule Scan
ODS (On Demand Scanning)/Schedule Scan provides you with various options like – checking for viruses, and making settings for creating logs and receiving alerts. You can also create task in the scheduler for automatic virus scanning.

MWL Inclusion List
MWL (MicroWorld WinSock Layer) Inclusion List contains the name of all executable files which will bind itself to MWTSP.DLL. All other files are excluded.

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

Notifications & Events
Notifications & Events 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. The Events tab lets you configure settings to allow/restrict clients from sending alert for specific events.

Schedule Update
The Schedule Update lets you schedule eScan database updates.

Tools
The Tools lets you configure eBackup Settings.

Defining Policies Mac or Linux computers

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

File Anti-Virus 🐧

The File Anti-virus module scans all the existing files and folders for any infection. It also lets you report/disinfect/quarantine/delete infected objects. Moreover, it saves a copy of report file for future reference, and displays attention messages. This option is available for both Linux and Mac computers.

Endpoint Security 🐧

The Endpoint Security module monitors the application on client computers. It allows/ restricts USB, block listing, white listing, and defines time restrictions. This option is available for both Linux and Mac computers.

On Demand Scanning 🐧

The On Demand Scanning module lets you define the categories to be scanned. For example, you can scan only the mails or archives as per your requirement. This option is available for both Linux and Mac computers.

Schedule Scan 🐧

The Schedule Scan module lets you schedule the scan on the basis of time, what you want to scan and what action to be taken in case of a virus and what you want to be excluded while scanning. For example, you can create a schedule to scan the mails, sub directories and archives on a daily basis and also define the action that needs to be taken in case a virus is found; you can also exclude the scan by mask or files or folders. This option is available for both Linux and Mac computers.

Schedule Update 🐧

The Schedule Update module lets you schedule updates for Linux systems.

Administrator Password 🐧

The Administrator Password module for Linux 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.

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.

Editing Policy Template modules

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

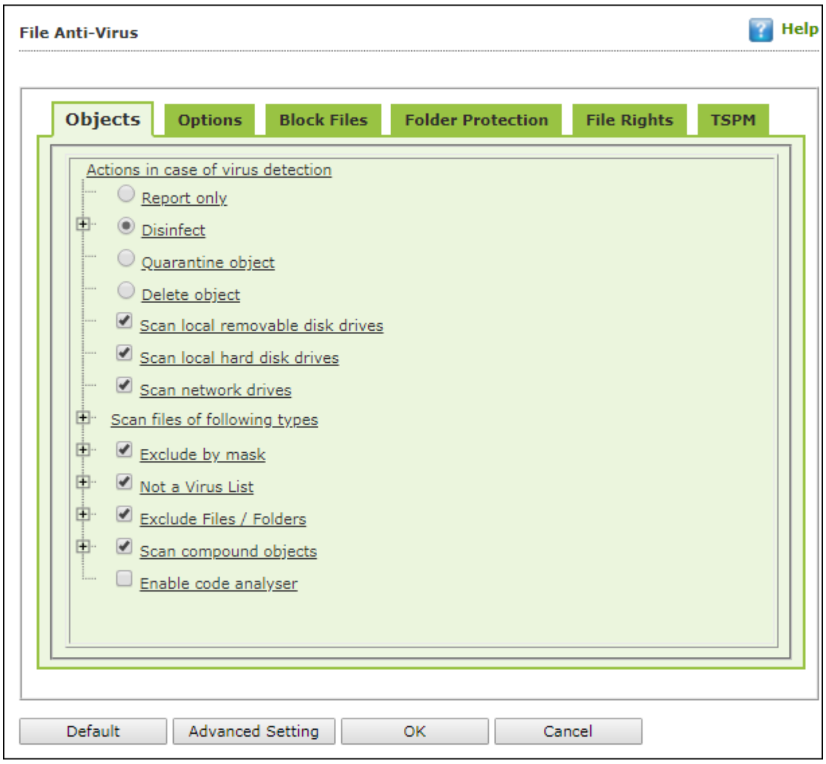
File Anti-Virus

Editing File Anti-Virus module displays following tabs:

- Objects
- Options
- Blocked Files
- Folder Protection
- File Rights
- TSPM

Objects

The Objects tab lets you configure following options.


File Anti-Virus

Actions in case of virus detection
- ○ Report only
- ● Disinfect
- ○ Quarantine object
- ○ Delete object
- ☑ Scan local removable disk drives
- ☑ Scan local hard disk drives
- ☑ Scan network drives

Scan files of following types
- ☑ Exclude by mask
- ☑ Not a Virus List
- ☑ Exclude Files / Folders
- ☑ Scan compound objects
- ☐ Enable code analyser

Actions in case of virus detection

This section lists the different actions that File Anti-Virus can perform when it detects virus infection.

Report Only

Upon virus detection, eScan will only report the virus and won't take any action.
Disinfect and **If disinfection is impossible** it will **Quarantine Object** or **Delete Object**"
Out of these, the **Disinfect** option is selected by default. By default, the quarantined files are saved in **C:\Program Files\eScan\Infected folder.** You can select the **Make**

backup file before disinfection option if you would like to make a backup of the files before they are disinfected**.**

Scan local removable disk drives [Default]
Select this option if you want eScan to scan all the local removable drives attached to the computer.

Scan local hard disk drives [Default]
Select this option if you want eScan to scan all the local hard drives installed on the computer.

Scan network drives [Default]
Select this option if you want eScan to scan all the network drives, including mapped folders and drives connected to the computer.

Scan files of following types
Select this option if you want eScan to scan all files, only infectable files, and files by extension (Scan by mask). eScan provides you a list of default files and file types that it scans by extension. You can add more items to this list or remove items as per your requirements by clicking **Add/Delete**.

Exclude by mask [Default]
Select this check box if you want File Anti-Virus monitor to exclude all the objects in the Exclude by mask list during real-time monitoring or scanning. You can add/delete a file or a particular file extension by clicking **Add/Delete**.

Not a virus list [Default]
File Anti-Virus is capable of detecting riskware. Riskware refers to software originally not intended to be malicious but somehow can pose as a security risk to critical operating system functions. You can add the names of riskware, such as remote admin software, to the riskware list in the **Not a virus list** dialog box by clicking **Add/Delete** if you are certain that they are not malicious. The riskware list is empty by default.

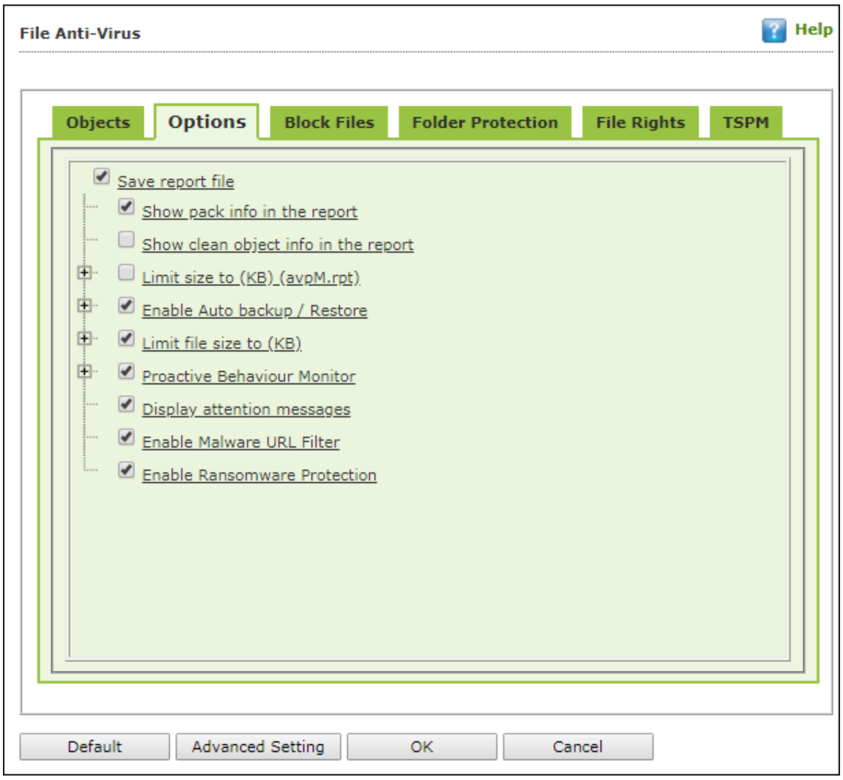
Exclude Files/Folders [Default]
Select this check box if you want File Anti-Virus to exclude all the listed files, folders, and sub folders while it is monitoring or scanning folders. The files/folders added to this list will be excluded from only real-time scan as well as on demand scan. You can add or delete files/folders from the list of by clicking **Add/Delete**.

Scan compound objects [Default]
Select this check box if you want eScan to scan archives and packed files during scan operations. By default, **Packed** is selected.

Enable code Analyzer
Select this check box if you want eScan to scan your computer for suspicious objects or unknown infections by using the heuristic analyzer. After selection, File Anti-Virus not only scans and detects infected objects, but also checks for suspicious files stored on computer.

Options

The Options tab lets you configure following options:



File Anti-Virus

- ☑ Save report file
  - ☑ Show pack info in the report
  - □ Show clean object info in the report
  - □ Limit size to (KB) (avpM.rpt)
  - ☑ Enable Auto backup / Restore
  - ☑ Limit file size to (KB)
  - ☑ Proactive Behaviour Monitor
  - ☑ Display attention messages
  - ☑ Enable Malware URL Filter
  - ☑ Enable Ransomware Protection

Save report file [Default]

Select this check box if you want eScan to save the reports generated by the File Anti-Virus module. The report file logs information about the scanned files and the action taken by File Anti-Virus when an infected file was found during the scan.

Show pack info in the report [Default]

Select this check box if you want File Anti-Virus to add information regarding scanned compressed files, such as .zip and .rar files to the Monvir.log file.

Show clean object info in the report

Select this check box if you want File Anti-Virus to add information regarding uninfected files found during a scan operation to the Monvir.log file. You can select this option to find out which files are not infected.

Limit size to (Kb) (avpM.rpt)

Select this check box if you want File Anti-Virus to limit the size of the Monvir.log file and avpM.rpt file. To modify the limit, enter the log file size in field.

Enable Auto backup/Restore [Default]

Selecting this check box lets you back up the critical files of the Windows® operating system and then automatically restores the clean files when eScan finds an infection in any of the system files that cannot be disinfected. You can do the following settings:

Do not backup files above size (KB) [Default]

This option lets you prevent File Anti-Virus from creating backup of files that are larger than the file size that you have specified.

Minimum disk space (MB) **[Default]**

The Auto-backup feature will first check for the minimum available space limit defined for a hard disk drive. If the minimum defined space is available then only the Auto-backup feature will work, if not it will stop without notifying. You can allot the Minimum disk space to be checked from this option. By default, the minimum disk space is 500 MB.

Limit file size to (KB) [Default]

This check box lets you set a limit size for the objects or files to be scanned. The default value is set to **20480 Kb**.

Proactive Behavior Monitor

Selecting this check box enables File Anti-Virus to monitor computer for suspicious applications and prompts you to block such applications when they try to execute.

Whitelist Option

Whitelisting lets you mark the files in the database that you want to exclude from being blocked. To whitelist a file/folder, click **Whitelist** and then click **Add from DB.**

Use sound effects for the following events

This check box lets you configure eScan to play a sound file and show you the details regarding the infection within a message box when any malicious software is detected by File Anti-Virus. However, you need to ensure that the computer's speakers are switched on.

Display attention messages [Default]

When this option is selected, eScan displays an alert consisting the path and name of the infected object and the action taken by the File Anti-Virus module.

Enable Malware URL Filter

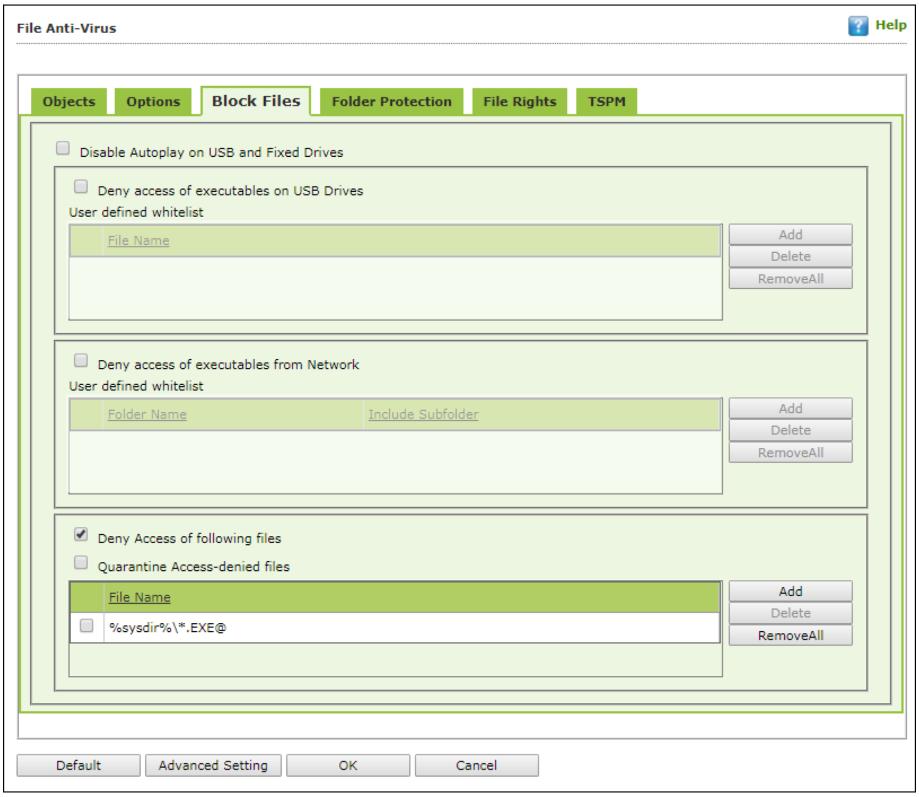
This option lets you enable a Malware URL filter where eScan blocks all URLs that are suspected to be malwares. You can exclude specific websites by whitelisting them from the eScan pop up displayed when you try to access the site.

Enable Ransomware Protection

This option lets you enable Ransomware Protection on the system where eScan blocks any suspected ransomware activities performed on system. With the technology called PBAE (Proactive Behavioral Analysis Engine) eScan monitors the activity of all processes on the local computer and when it encounters any activity or behavior that matches a ransomware, it raises a red flag and blocks the process.

Block Files

The Block Files tab lets you configure settings for preventing executables and files, such as autorun.inf, on network drives, USB drives, and fixed drives from accessing your computer.



File Anti-Virus

☐ Disable Autoplay on USB and Fixed Drives

☐ Deny access of executables on USB Drives

User defined whitelist

File Name

☐ Deny access of executables from Network

User defined whitelist

Folder Name	Include Subfolder

☑ Deny Access of following files

☐ Quarantine Access-denied files

	File Name
☐	%sysdir%*.EXE@

You can configure the following settings:

Disable AutoPlay on USB and Fixed Drives [Default]

Selecting this option will disable AutoPlay when a USB/Fixed Drive is connected.

Deny access of executables on USB Drives

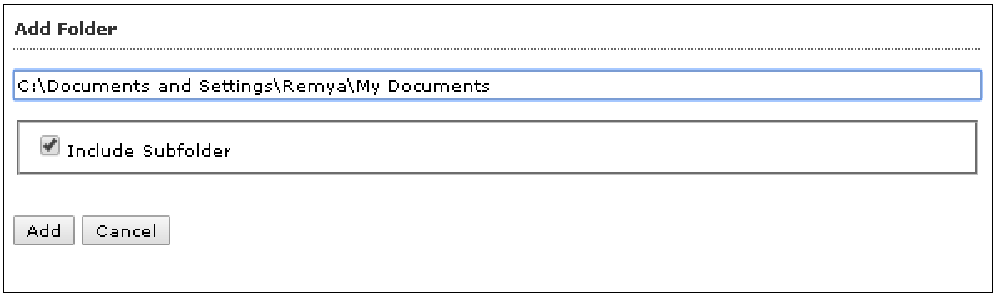
Select this check box if you want eScan to prevent executables stored on USB drives from being accessed.

Deny access of executable from Network

Select this check box if you want eScan to prevent executables on the client computer from being accessed from the network.

User defined whitelist

This option is enabled after selecting the **Deny access of executable from Network** check box. You can use this option to enter the folders that need to be whitelisted so that executables can be accessed in the network from the folders mentioned under this list. To add files, click **Add**.



Add Folder

C:\Documents and Settings\Remya\My Documents

☑ Include Subfolder

Enter the complete path of the folder to be whitelisted on the client systems. You can either whitelist the parent folder only or select the **Include subfolder** option to whitelist the subfolders as well.

Deny Access of following files [Default]

Select this check box if you want eScan to prevent the files in the list from running on the computers.

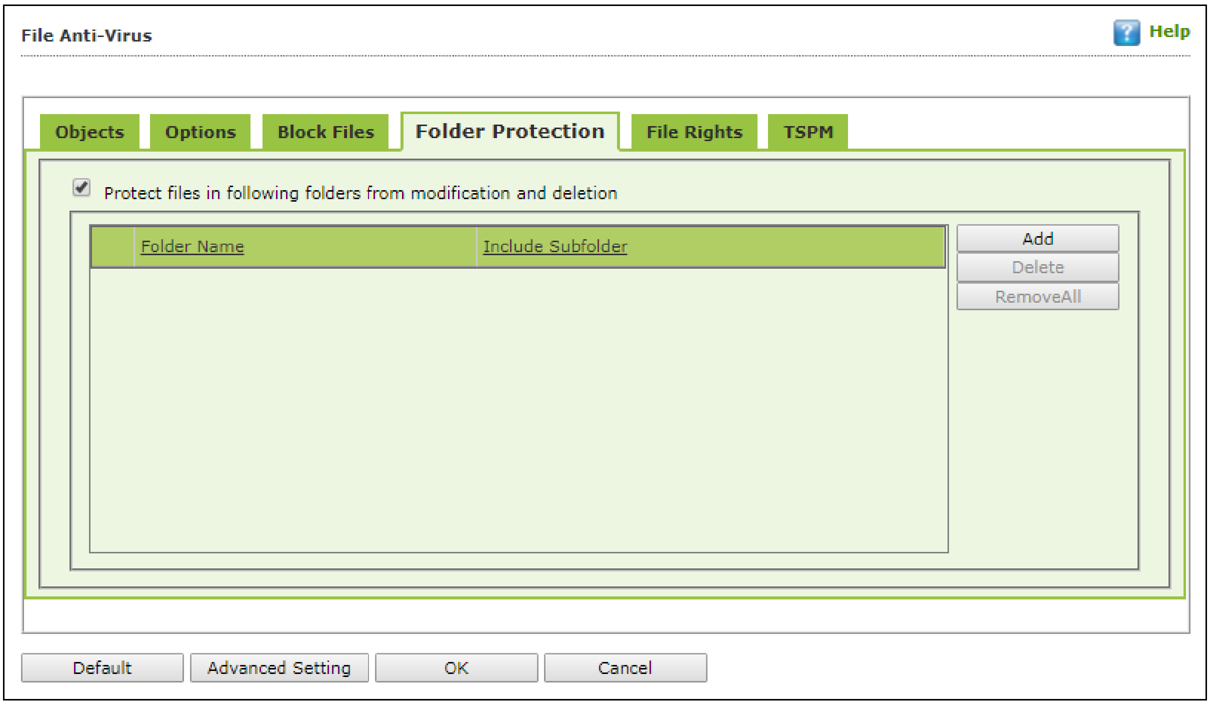
Quarantine Access-denied files

Select this check box if you want eScan to quarantine files to which access is denied.

1. You can prevent specific files from running on the eScan client computer by adding them to the Block Files list. By default, this list contains the value %sysdir%\\*.EXE@. Click **Add**.
2. Enter the full name of the file to be blocked from execution on the client systems.

Folder Protection

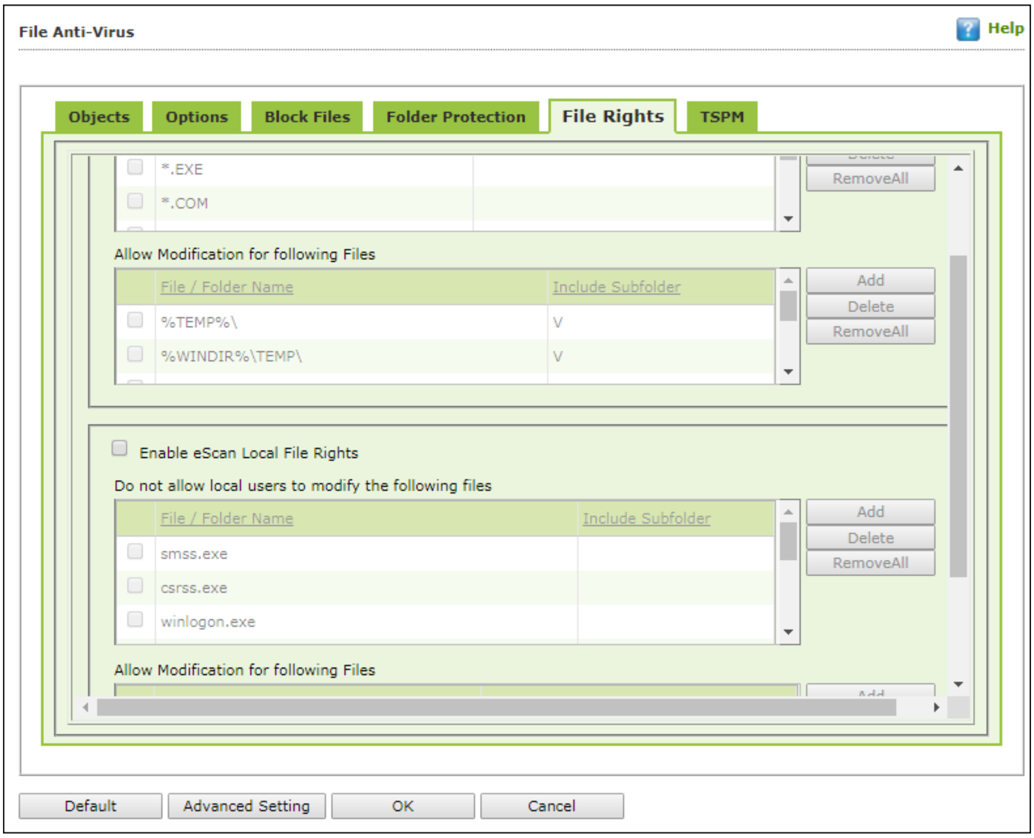
The Folder Protection tab lets you protect specific folders from being modified or deleted by adding them to the Folder Protection list. It lets you configure the following setting:



Protect files in following folders from modification and deletion [Default]
This option is selected by default.
Selecting this check box enables File Anti-Virus module to protect files in specific folders from being modified or deleted on the client systems. Click **Add**. Enter the complete path of the folder to be protected on the client systems. You can either protect the parent folder only or select the **Include subfolder** option to protect the subfolders as well.

File Rights

The File Rights tab restricts or allows for remote or local users from modifying folders, subfolders, files or files with certain extensions.



☐ *.EXE	
☐ *.COM	

Allow Modification for following Files

File / Folder Name	Include Subfolder
☐ %TEMP%\	V
☐ %WINDIR%\TEMP\	V

☐ Enable eScan Local File Rights

Do not allow local users to modify the following files

File / Folder Name	Include Subfolder
☐ smss.exe	
☐ csrss.exe	
☐ winlogon.exe	

Allow Modification for following Files

Enable eScan Remote File Rights
Select this check box to allow/restrict the remote users to make any modifications to the files and folders.

Do not allow remote users to modify the following local files
The files/folders added to this list cannot be modified by the remote users.

Allow modification for following files
The files added to this list can be modified by the remote user.

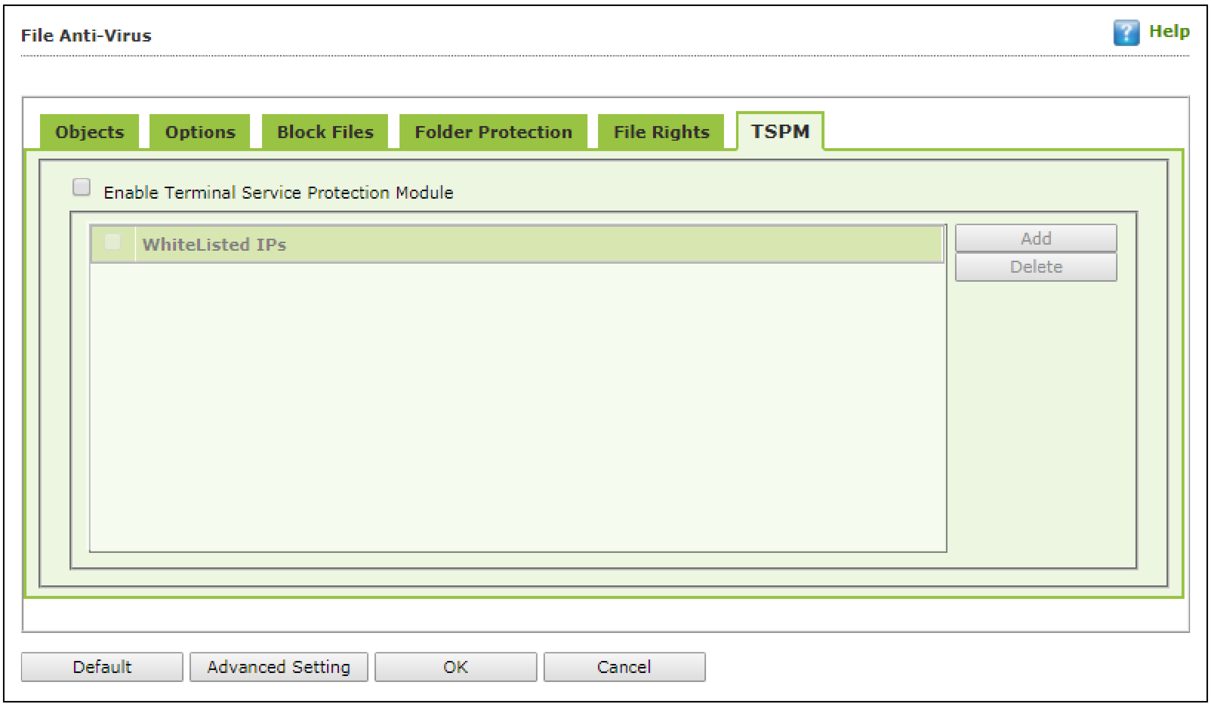
Enable eScan local file rights
Select this check box to allow/restrict the local users to make any modifications to the files/folders.

Do not allow local users to modify the following files
The files/folders added to this list cannot be modified by the local users.

Allow modification for files
The files/folders added to this list can be modified by the local users.

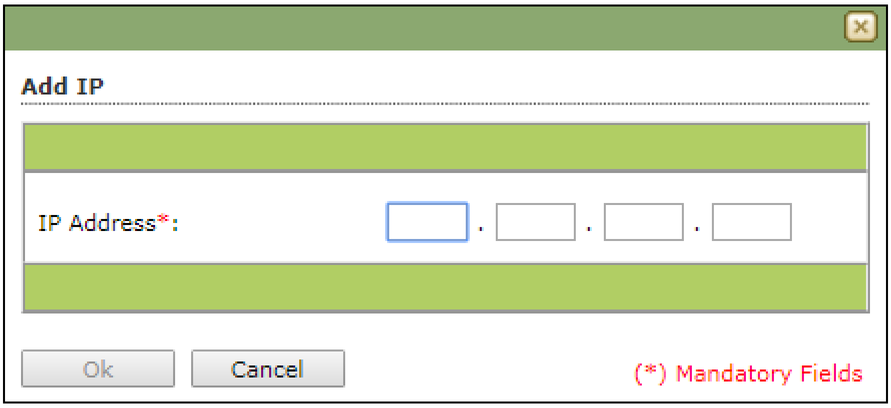
TSPM

eScan's Terminal Services Protection Module (TSPM) detects brute force attempts, identifies suspicious IP addresses/hosts and blocks any access attempts from them to prevent future attacks. The IP addresses and hosts from the attacks are banned from initiating any further connections to the system. It also detects and stops attempts of attackers who try to uninstall security applications from systems and alerts administrators about the preventive measures initiated by TSPM.



Select the check box **Enable Terminal Service Protection Module** to activate TSPM module.

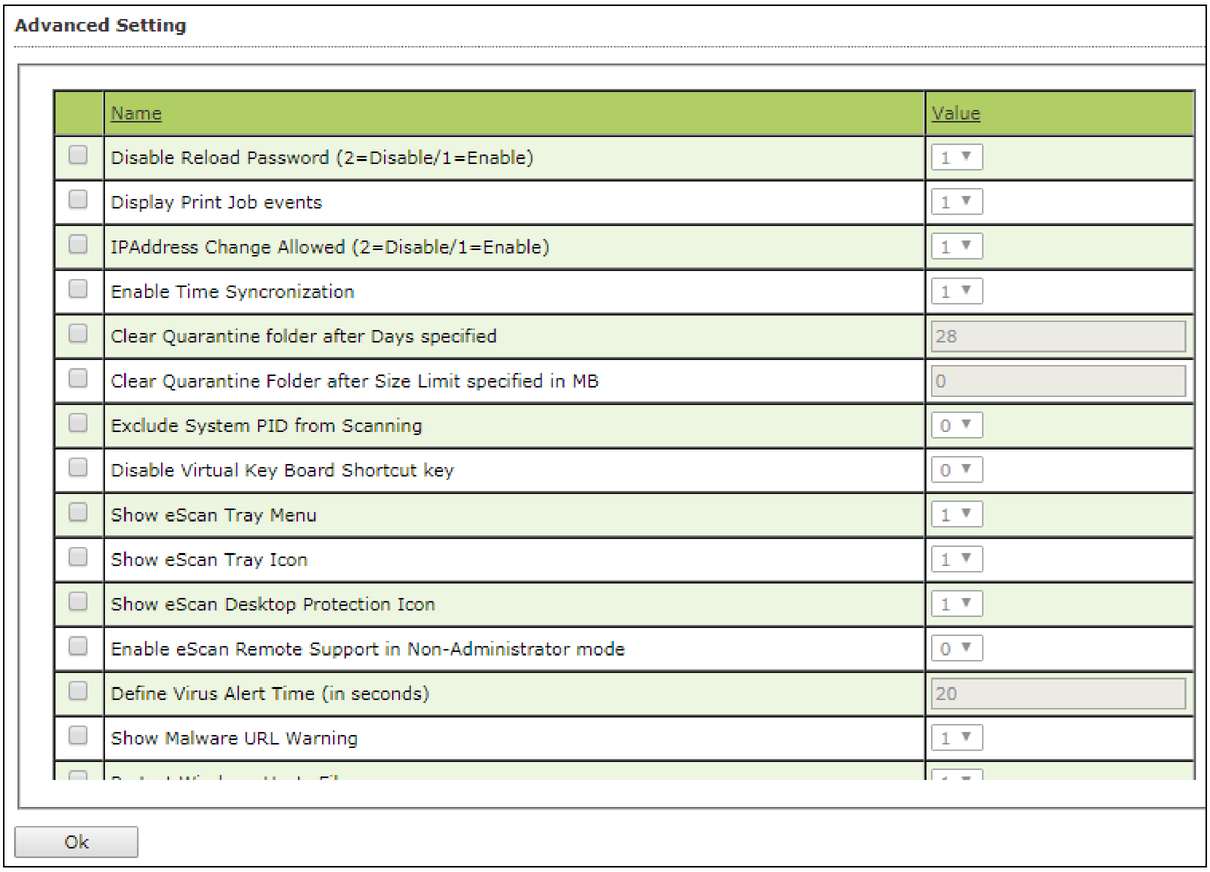
To add a list of IP addresses to be excluded from being blocked by TSPM, click **Add.** Add IP window appears.



Enter the IP address and then click **OK.**

Advanced Settings

Clicking Advanced Settings lets you configure advanced settings for console.



Advanced Setting

	Name	Value
□	Disable Reload Password (2=Disable/1=Enable)	1 ▼
□	Display Print Job events	1 ▼
□	IPAddress Change Allowed (2=Disable/1=Enable)	1 ▼
□	Enable Time Syncronization	1 ▼
□	Clear Quarantine folder after Days specified	28
□	Clear Quarantine Folder after Size Limit specified in MB	0
□	Exclude System PID from Scanning	0 ▼
□	Disable Virtual Key Board Shortcut key	0 ▼
□	Show eScan Tray Menu	1 ▼
□	Show eScan Tray Icon	1 ▼
□	Show eScan Desktop Protection Icon	1 ▼
□	Enable eScan Remote Support in Non-Administrator mode	0 ▼
□	Define Virus Alert Time (in seconds)	20
□	Show Malware URL Warning	1 ▼

Disable Reload Password (2=Disable/1=Enable)

This option lets you enable or disable password for reloading eScan. After enabling, the user will be asked to enter reload password if user attempts to reload eScan. This is the administrator password for eScan Protection Center.

Display Print Job events (1 = Enable/0 = Disable)

This option lets you capture events for the Print Jobs from Managed Computers.

IP Address Change Allowed (2 = Disable/1 = Enable)

This option lets you enable/disable IP Address Change by the user on their computer.

Enable Time Synchronization (1 = Enable/0 = Disable)

This option lets you enable/disable time synchronization with internet. Active internet connection is mandatory for this feature.

Clear Quarantine folder after Days specified

This option lets you specify number of days after which the Quarantine folder should be cleared on Managed Computers.

Clear Quarantine Folder after Size Limit specified in MB

This option lets you specify size limit for the Quarantine folder. If the defined size limit exceeds, the Quarantine folder will be cleared on Managed Computers.

Exclude System PID from Scanning (1 = Enable/0 = Disable)
This option lets you exclude system process ID (Microsoft assigned System PIDs) from scanning on Managed Computers.

Disable Virtual Key Board Shortcut key (1 = Enable/0 = Disable)
This option lets you disable shortcut for using Virtual Keyboard on Managed Computers.

Show eScan Tray Menu (1 = Show/0 = Hide)
This option lets you Hide or Show eScan Tray menu on Managed Computers.

Show eScan Tray Icon (1 = Show/0 = Hide)
This option lets you hide or show eScan Tray Icon on Managed Computers.

Show eScan Desktop Protection Icon (1 = Show/0 = Hide)
This option lets you hide or show eScan Protection icon on Managed Computers.

Enable eScan Remote Support in Non-Administrator mode (1 = Enable/0 = Disable)
This option lets you enable/disable eScan Remote Support in Non-Administrator Mode. eScan will not prompt for entering Administrator Password to start eScan Remote Support from Managed Computers.

Define Virus Alert Time (in seconds)
This option lets you define time period in seconds to display Virus Alert on Managed Computers.

Show Malware URL Warning (1 = Show/0 = Hide)
This option lets you show or hide Malware URL warning messages on Managed Computers.

Protect Windows Hosts File (1 = Allow/0 = Block)
Use this option to Allow/Block modifications to Windows Host Files.

Search for HTML Scripts (1 = Allow/0 = Block)
Use this option to Allow/Block search for html script (infection) in files. This option will have impact on system performance.

Show Network Executable block alert (1 = Show/0 = Hide)
This option lets you show/hide Network executable block alerts on Managed Computers.

Show USB Executable Block Alert (1 = Show/0 = Hide)
This option lets you show/hide USB executable block alerts on Managed Computers.

Show eScan Tray Icon on Terminal Client (1 = Show/0 = Hide)
This option lets you show/hide eScan Tray Icon on Terminal Clients on Managed Computers.

Enable eScan Self Protection (1 = Enable/0 = Disable)
This option lets you Enable/Disable eScan Self Protection on Managed Computers, if this feature is enabled, no changes or modifications can be made in any eScan File.

Enable eScan Registry Protection (1 = Enable/0 = Disable)
This option lets you Enable/Disable eScan Registry Protection. User cannot make changes in protected registry entries if it is enabled on Managed Computers.

Enable backup of DLL files (1 = Enable/0 = Disable)
This option lets you Enable/Disable backup of DLL files on Managed Computers.

Integrate Server Service dependency with Real-time monitor (1 = Enable/0 = Disable)
This option lets you Integrate Server Service dependency with real-time monitor.

Send Installed Software Events (1 = Enable/0 = Disable)
This option lets you receive Installed Software Events from Managed Computers.

Enable Winsock Protection (Require Restart) (1 = Enable/0 = Disable)
This option lets you Enable/Disable protection at the Winsock Layer.

Enable Cloud (1 = Enable/0 = Disable)
This option lets you Enable/Disable eScan Cloud Security Protection on Managed Computers.

Enable Cloud Scanning (1 = Enable/0 = Disable)
This option lets you Enable/Disable Cloud Scanning on Managed Computers.

Remove LNK (Real-Time) (1 = Enable/0 = Disable)
This option lets you Enable/Disable Removal of LNK on real-time basis.

Whitelisted AutoConfigURL
This option lets you whitelist AutoConfigURLs. Enter comma separated URLs that need to be whitelisted.

Disable Add-ons/Extension blocking (1 = Enable/0 = Disable)
Selecting this option disables Add-ons and Extension blocking.

Include files to scan for archive (Eg: abc*.exe)
This option lets you add file types that needs to be when archive scanning enabled.

Block Date-Time Modification (1 = Enable/0 = Disable)
This option lets you block the modification of the system date and time.

Allow CMD-Registry for Date-Time blocking (Depends upon Block Date-Time Modification) (1 = Enable/0 = Disable)
Selecting this option lets you block date-time modification from the CMD-Registry.

Domain list for exclusion of Host file scanning (e.g. abc.mwti)
Selecting this option lets you add the list of domains to be excluded from host file scanning.

Disable Pause Protection and Open Protection center on Right Click (Set 192 for disable)
This option disables Pause Protection and Open Protection center on Right Click if you set it to 192.

Enable Share Access Control (1 = Enable/0 = Disable)

It enables Share Access Control. Network Shares ReadOnly Access and Network Shares NoAccess options will work only if this option is selected.

NOTE	Only if it is enabled the setting "NetworkSharesReadOnlyAccess" and "NetworkSharesNoAccess" will be referred

List of comma-separated servers and/or shares and/or wildcards which needs to be given NO ACCESS e.g. \\192.168.1.1\temp or \\192.168.1.1\temp\*.doc or *.doc (Work only when "Enable Share Access Control" is set)
Selecting this option lets you add the List of comma-separated servers and/or shares and/or wildcards that should not be accessible.

List of comma-separated servers and/or shares and/or wildcards which needs to be given READ ONLY ACCESS e.g. \\192.168.1.1\temp or \\192.168.1.1\temp\*.doc or *.doc (Work only when "Enable Share Access Control" is set)
Selecting this option lets you add the List of comma-separated servers and/or shares and/or wildcards that should be given only view access and not be editable.

Include files to scan for archive (eg: abc*.exe)
Selecting this option lets you add file types that should be scanned.

Whitelist IP Address (Depends on IP Address Change Allowed) (E.G 192.168.1.* You can put comma-separated list)
Selecting this option lets you add the list of IP addresses separated by commas to whitelist them.

Block Access to Control Panel (1 = Enable/0 = Disable)
Selecting this option lets you block the user from accessing the control panel.

Disable COPY/PASTE (1 = Enable/0 = Disable)
Selecting this option lets you disable Copy/Paste actions.

Enable logging of sharing activity from suspected malware system (WSmbFilt.log on client system) (1 = Enable/0 = Disable)
Enabling this option directs eScan to log any sharing activity performed by suspected malware system. By default, this feature is enabled.

Block all RDP Session except Whitelisted under TSPM
Selecting this option lets you block all RDP sessions excluding the ones you have Whitelisted under TSPM.

Allow RDP (1=Block Foreign IP and allow Local IP/0 =Block Local & Foreign IP but allow Whitelisted IP)
This option lets you allow or block the foreign and local IP addresses excluding the whitelisted ones.

PowerShell Exclusion list
Selecting this option lets you add a PowerShell script file path manually to exclude files and folders from real-time scan.

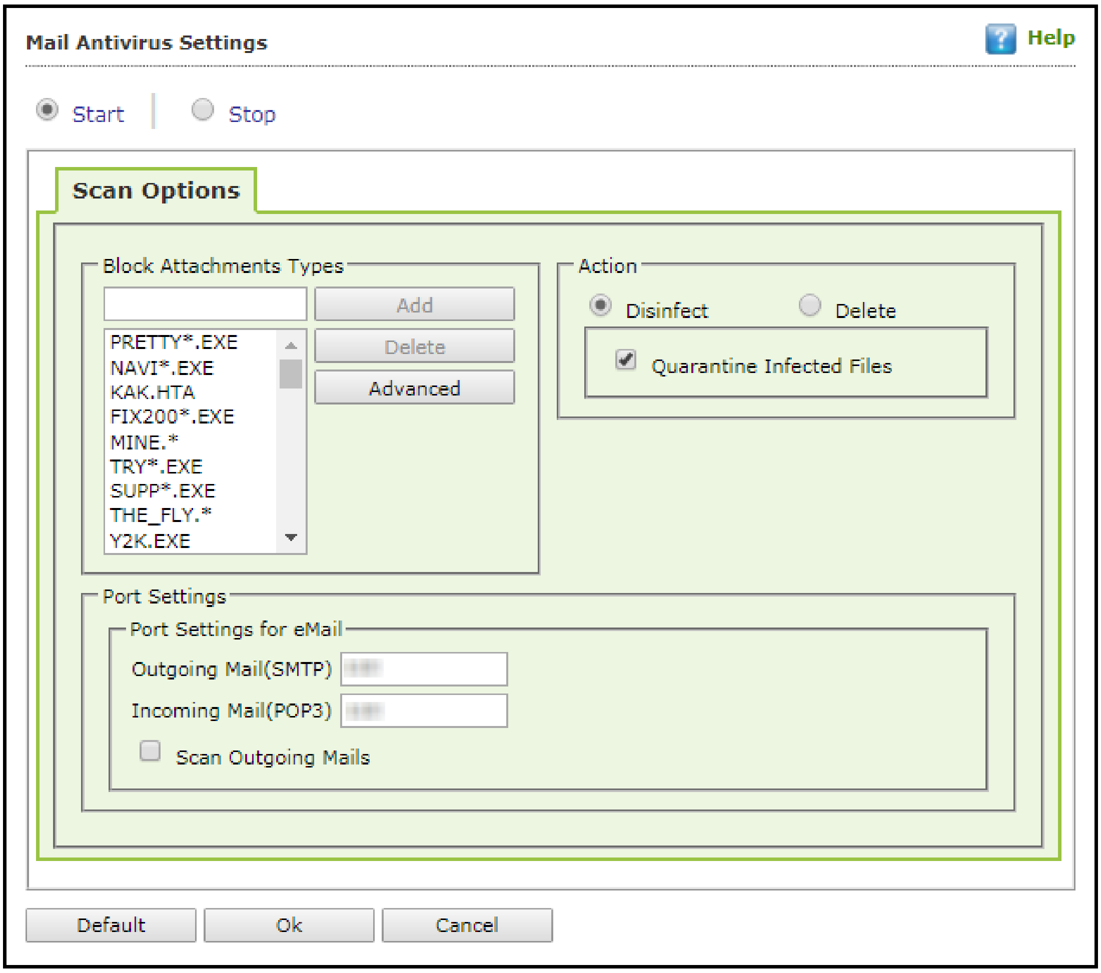
Allow Uninstallers (1 = Enable/0 = Disable)
Selecting this option lets you enable/disable use of third party uninstallers.

Block Renaming of Hostname (1 = Enable/0 = Disable)
Selecting this option lets you enable/disable block Hostname renaming.
Restricted Environment enabled (1 = Enable/0 = Disable)
Selecting this option lets you enable/disable restrict environment settings.

Block eternal blue (wannacry) exploits (1 = Enable/0 = Disable)
Selecting this option lets you block eternal blue (wannacry) exploits. By default, this option is enabled.

Mail Antivirus

Mail Anti-Virus is a part of the Protection feature of eScan. This module scans all incoming and outgoing emails for viruses, spyware, adware, and other malicious objects. It lets you send virus warnings to client computers on the Mail Anti-Virus activities. By default, Mail Anti-Virus scans only the incoming emails and attachments, but you can configure it to scan outgoing emails and attachments as well. Moreover, it lets you notify the sender or system administrator whenever you receive an infected email or attachment. This page provides you with options for configuring the module.



● Start | ○ Stop

Block Attachments Types

PRETTY*.EXE
NAVI*.EXE
KAK.HTA
FIX200*.EXE
MINE.*
TRY*.EXE
SUPP*.EXE
THE_FLY.*
Y2K.EXE

Action

● Disinfect ○ Delete

☑ Quarantine Infected Files

Port Settings

Port Settings for eMail

Outgoing Mail(SMTP) [redacted]

Incoming Mail(POP3) [redacted]

□ Scan Outgoing Mails

Scan Options

This tab lets you select the emails to be scanned and action that should be performed when a security threat is encountered during a scan operation. This tab lets you configure following settings:

Block Attachments Types

This section provides you with a predefined list of file types that are often used by virus writers to embed viruses. Any email attachment having an extension included in this list will be blocked or deleted by eScan at the gateway level. You can add file extensions to this list as per your requirements. As a best practice, you should avoid deleting the file extensions that are present in the **Block Attachments Types** list by default. You can also configure advanced settings required to scan emails for malicious code.

Action

This section lets you configure the actions to be performed on infected emails. These operations are as follows:

Disinfect [Default]

Select this option if you want Mail Anti-Virus to disinfect infected emails or attachments.

Delete

Select this option if you want Mail Anti-Virus to delete infected emails or attachments.

Quarantine Infected Files [Default]

Select this option if you want Mail Anti-Virus to quarantine infected emails or attachments. The default path for storing quarantined emails or attachments is –
C:\Program Files\eScan\QUARANT.
However, you can specify a different path for storing quarantined files, if required.

Port Settings for email

You can also specify the ports for incoming and outgoing emails so that eScan can scan the emails sent or received through those ports.

Outgoing Mail (SMTP) [Default: 25]

You need to specify a port number for SMTP.

Incoming Mail (POP3) [Default: 110]

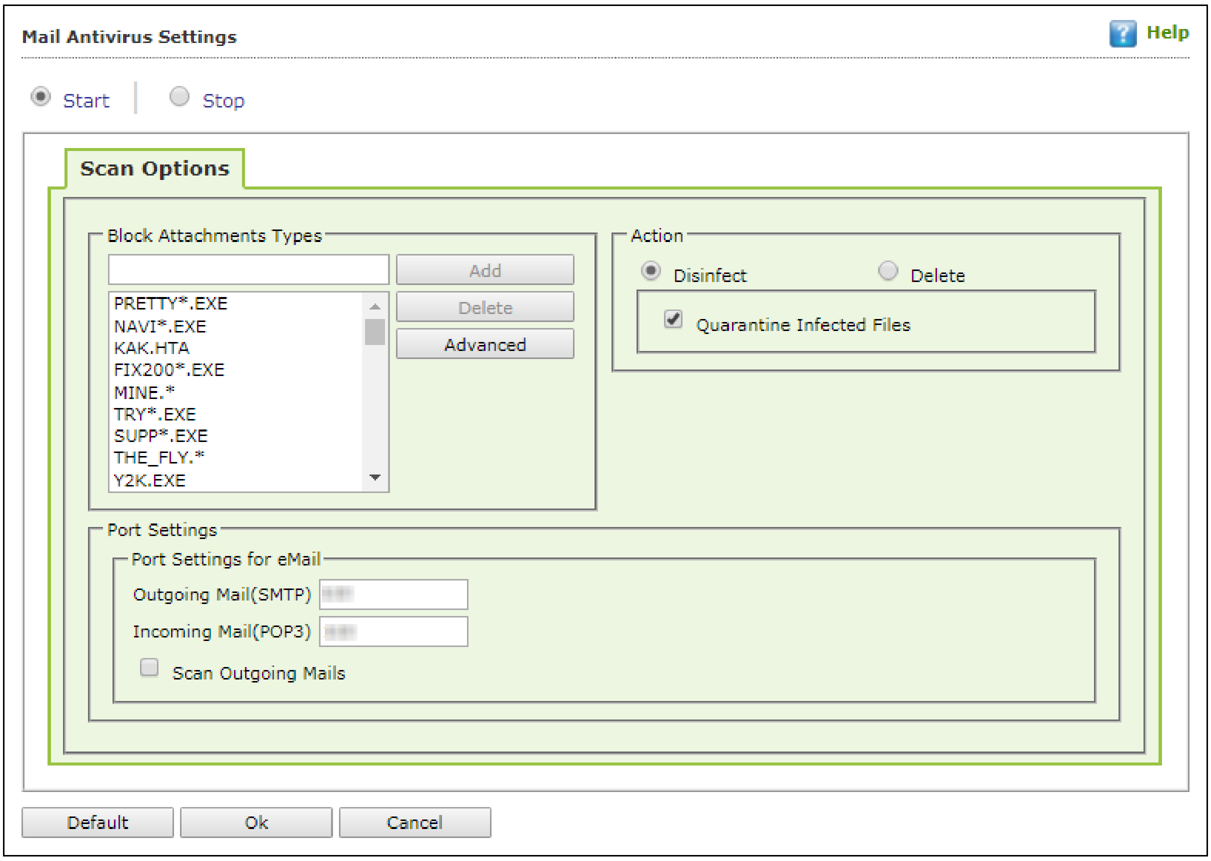
You need to specify a port number for POP3.

Scan Outgoing Mails

Select this option if you want Mail Anti-Virus to scan outgoing emails as well.

Advanced

Clicking **Advanced** displays Advanced Scan Options dialog box. This dialog box lets you configure the following advanced scanning options:



Mail Antivirus Settings

● Start | ○ Stop

Scan Options

Block Attachments Types

PRETTY*.EXE
NAVI*.EXE
KAK.HTA
FIX200*.EXE
MINE.*
TRY*.EXE
SUPP*.EXE
THE_FLY.*
Y2K.EXE

Action

● Disinfect ○ Delete

☑ Quarantine Infected Files

Port Settings

Port Settings for eMail

Outgoing Mail(SMTP) [redacted]

Incoming Mail(POP3) [redacted]

□ Scan Outgoing Mails

Delete all Attachment in email if disinfection is not possible
Select this option to delete all the email attachments that cannot be cleaned.

Delete entire email if disinfection is not possible [Default]
Select this option to delete the entire email if any attachment cannot be cleaned.

Delete entire email if any virus is found
Select this option to delete the entire email if any virus is found in the email or the attachment is infected.

Quarantine blocked Attachments [Default]
Select this option to quarantine the attachment if it bears extension blocked by eScan.

Delete entire email if any blocked attachment is found [Default]
Select this option to delete an email if it contains an attachment with an extension type blocked by eScan.

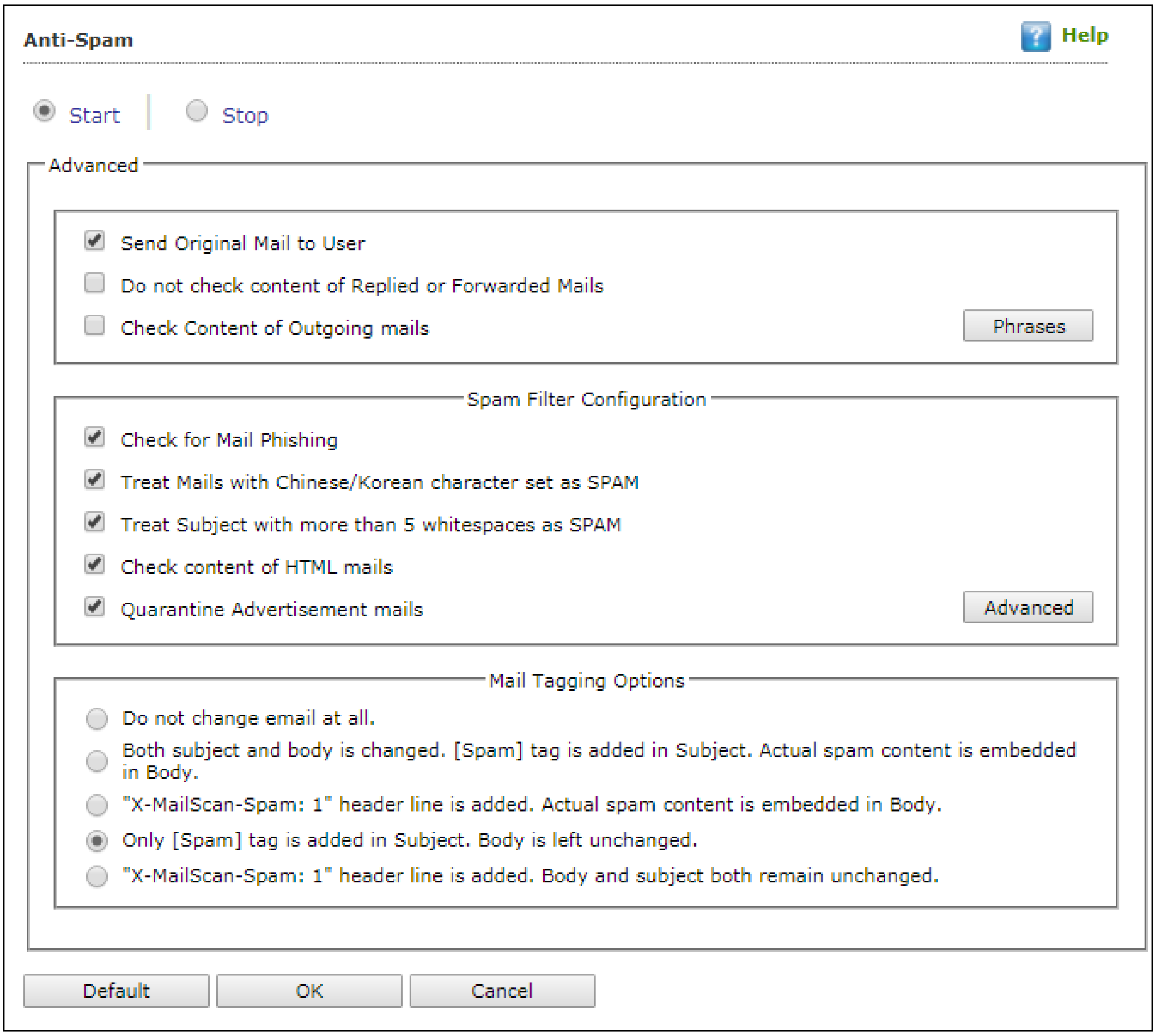
Quarantine email if attachments are not scanned
Select this check box to quarantine an entire email if it contains an attachment not scanned by Mail Anti-Virus.

Quarantine Attachments if they are scanned
Select this check box if you want eScan to quarantine attachments that are scanned by Mail Anti-Virus.

Exclude Attachments (White List)
This list is empty by default. You can add file names and file extensions that should not be blocked by eScan. You can also configure eScan to allow specific files even though if the file type is blocked. For example, if you have listed *.PIF in the list of blocked attachments and you need to allow an attachment with the name ABC, you can add abcd.pif to the Exclude Attachments list. Add D.PIFing *.PIF files in this section will allow all *.PIF to be delivered. MicroWorld recommends you to add the entire file name like ABCD.PIF.

Anti-Spam

Anti-Spam module filters junk and spam emails and sends content warnings to specified recipients. Here you can configure the following settings.



Anti-Spam

● Start | ○ Stop

Advanced

☑ Send Original Mail to User

□ Do not check content of Replied or Forwarded Mails

□ Check Content of Outgoing mails

Spam Filter Configuration

☑ Check for Mail Phishing

☑ Treat Mails with Chinese/Korean character set as SPAM

☑ Treat Subject with more than 5 whitespaces as SPAM

☑ Check content of HTML mails

☑ Quarantine Advertisement mails

Mail Tagging Options

○ Do not change email at all.

○ Both subject and body is changed. [Spam] tag is added in Subject. Actual spam content is embedded in Body.

○ "X-MailScan-Spam: 1" header line is added. Actual spam content is embedded in Body.

● Only [Spam] tag is added in Subject. Body is left unchanged.

○ "X-MailScan-Spam: 1" header line is added. Body and subject both remain unchanged.

Advanced

This section provides you with options for configuring the general email options, spam filter configuration, and tagging emails in Anti-Spam.

Send Original Mail to User [Default]

This check box is selected by default. eScan delivers spam mail to your inbox with a spam tag. When an email is tagged as SPAM, it is moved to this folder. Select this check box, if you want to send original email tagged as spam to the recipient as well.

Do not check content of Replied or Forwarded Mails

Select this check box, if you want to ensure that eScan does not check the contents of emails that you have either replied or forwarded to other recipients.

Check Content of Outgoing mails

Select this check box, if you want Anti-Spam to check outgoing emails for restricted content.

Phrases

Click **Phrases** to open the **Phrases** dialog box. This dialog box lets you configure additional email related options. In addition, it lets you specify a list of words that the user can either allow or block.

User specified whitelist of words/phrases (Color Code: **GREEN**)
This option indicates the list of words or phrases that are present in the whitelist. A phrase added to the whitelist cannot be edited, enabled, or disabled.

User specified List of Blocked words/phrases: (Color Code: **RED**)
This option indicates the list of words or phrases that are defined in block list.

User specified words/phrases disabled: (Color Code: **GRAY**)
This option indicates the list of words or phrases that are defined to be excluded during scans. The options in the **Phrases to Check** dialog box are disabled by default.

Action List

Add Phrase: Option to add phrase to quarantine or delete the mail.
Edit Phrase: To modify existing phrase added in list.
Enable Phrase: By default, it is enabled. After being disabled, you can use this option to enable it.
Disable Phrase: Disable existing phrase added in list.
Whitelist: This will allow email to deliver to inbox when phrase is found in the email.
Block list: This will delete email when it contains the phrase.
Delete: Delete the phrase added in list.

Spam Filter Configuration

This section provides you with options for configuring the spam filter. All options in this section are selected by default.

Check for Mail Phishing [Default]

Select this option if you want Anti-Spam to check for fraudulent emails and quarantine them.

Treat Mails with Chinese/Korean character set as SPAM [Default]

When this option is selected, emails are scanned for Chinese or Korean characters. This check is based on the research data conducted by MicroWorld's various spam email samples collected from around the globe. From these samples, it was observed that spammers often use Chinese or Korean characters in their emails.

Treat Subject with more than 5 whitespaces as SPAM [Default]

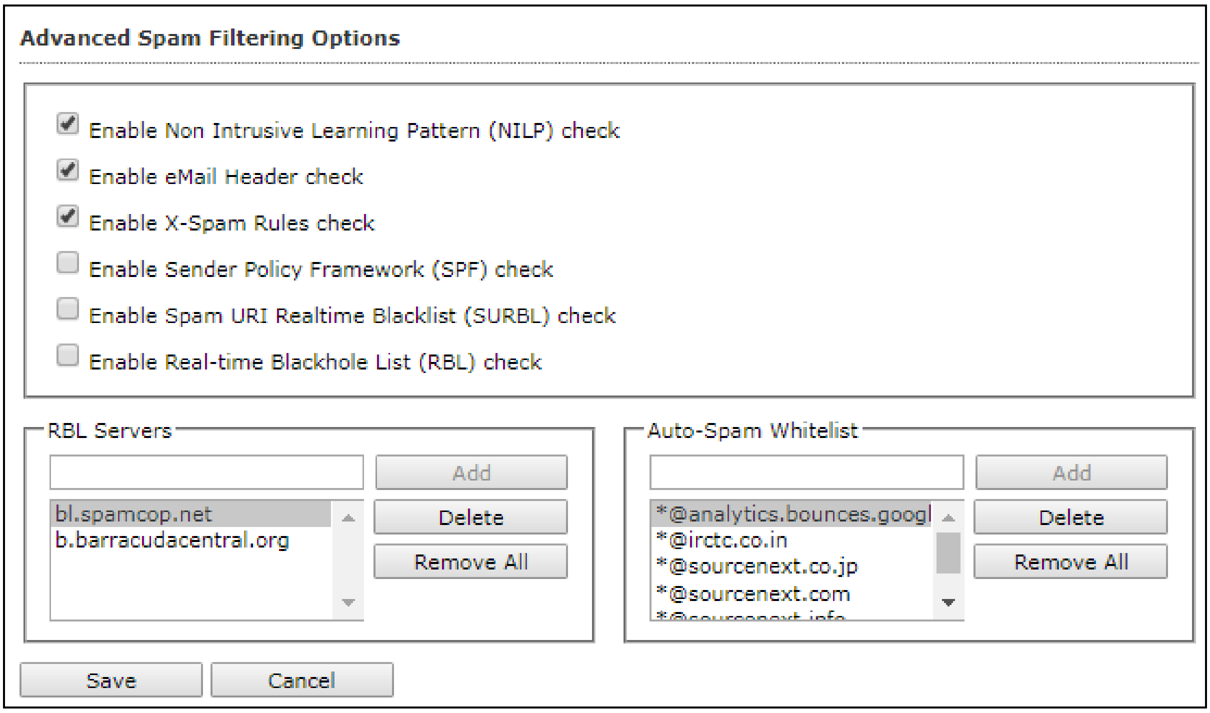
In its research, MicroWorld found that spam emails usually contain more than five consecutive white spaces. When this option is selected, Anti-Spam checks the spacing between characters or words in the subject line of emails and treats emails with more than five whitespaces in their subject lines as spam emails.

Check content of HTML mails [Default]
Select this option if you want Anti-Spam to scan emails in HTML format along with text content.

Quarantine Advertisement mails [Default]
Select this option if you want Anti-Spam to check for advertisement types of emails and quarantine them.

Advanced

Clicking **Advanced** displays Advanced Spam Filtering Options dialog box. This dialog box lets you configure the following advanced options for controlling spam.



Advanced Spam Filtering Options

☑ Enable Non Intrusive Learning Pattern (NILP) check
☑ Enable eMail Header check
☑ Enable X-Spam Rules check
☐ Enable Sender Policy Framework (SPF) check
☐ Enable Spam URI Realtime Blacklist (SURBL) check
☐ Enable Real-time Blackhole List (RBL) check

RBL Servers
bl.spamcop.net
b.barracudacentral.org

Auto-Spam Whitelist
*@analytics.bounces.googl
*@irctc.co.in
*@sourcenext.co.jp
*@sourcenext.com
*@sourcenext.info

Enable Non- Intrusive Learning Pattern (NILP) check [Default]
Non-Learning Intrusive Pattern (NILP) is MicroWorld's revolutionary technology that uses Bayesian Filtering and works on the principles of Artificial Intelligence (AI) to analyze each email and prevents spam and phishing emails from reaching your inbox. It has self-learning capabilities and it updates itself by using regular research feeds from MicroWorld servers. It uses an adaptive mechanism to analyze each email and categorize it as spam or ham based on the behavioral pattern of the user.

Enable email Header check [Default]
Select this option if you want to check the validity of certain generic fields likes From, To, and CC in an email and marks it as spam if any of the headers are invalid.

Enable X Spam Rules check [Default]
X Spam Rules are rules that describe certain characteristics of an email. It checks whether the words in the content of emails are present in eScan's database. This database contains a

list of words and phrases, each of which is assigned a score or threshold. The Spam Rules Check technology matches X Spam Rules with the mail header, body, and attachments of each email to generate a score. If the score crosses a threshold value, the mail is considered as spam. Anti-Spam refers to this database to identify emails and takes action on them.

Enable Sender Policy Framework (SPF) check
SPF is a world standard framework adopted by eScan to prevent hackers from forging sender addresses. It acts as a powerful mechanism for controlling phishing mails. Select this check box if you want Anti-Spam to check the SPF record of the sender's domain. However, your computer should be connected to the Internet for this option to work.

Enable Spam URI Real-time Blacklist (SURBL) check
Select this option if you want Anti-Spam to check the URLs in the message body of an email. If the URL is listed in the SURBL site, the email will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.

Enable Real-time Blackhole List (RBL) check
Select this option if you want Anti-Spam to check the sender's IP address in the RBL sites. If the sender IP address is blacklisted in the RBL site, the email will be blocked from being downloaded. However, your computer should be connected to the Internet for this option to work.

RBL Servers
RBL is a DNS server that lists IP addresses of known spam senders. If the IP of the sender is found in any of the blacklisted categories, the connection is terminated. The RBL Servers list contains addresses of servers and sites that maintain information regarding spammers. You can add or delete address in the list as per your requirement.

Auto Spam Whitelist
Unlike normal RBLs, SURBL scans emails for names or URLs of spam websites in the message body. It terminates the connection if the IP of the sender is found in any of the blacklisted categories. This contains a list of valid email addresses that can bypass the above Spam filtering options. It thus allows emails from the whitelist to be downloaded to the recipient's inbox. You can add or delete address in the list as per your requirement.

Mail Tagging Options
Anti-Spam also includes some mail tagging options, which are described as follows:

Do not change email at all
Select this option if you want to prevent Anti-Spam from adding the [Spam] tag to emails that have been identified as spam.

Both subject and body are changed: [Spam] tag is added in Subject: Actual spam content is embedded in Body
This option lets you identify spam emails. When you select this option, Anti-Spam adds a [Spam] tag in the subject line and the body of the email that has been identified as spam.

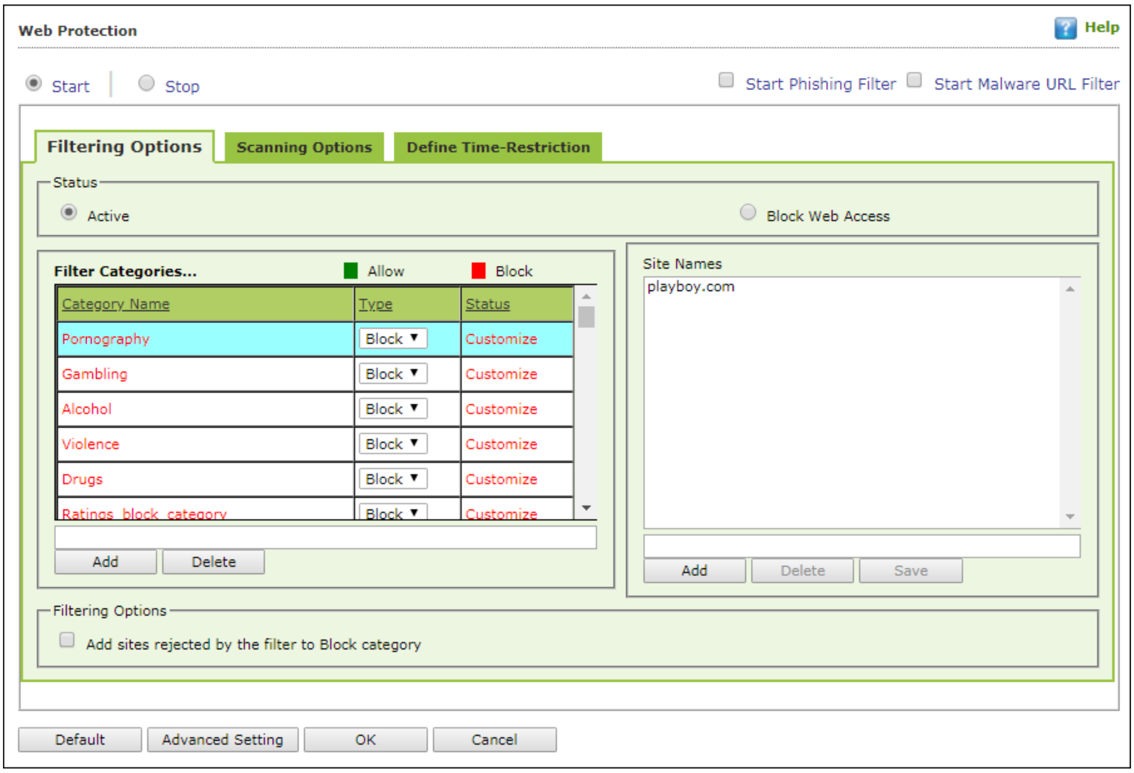
"X MailScan Spam: 1" header line is added: Actual spam content is embedded in Body
This option lets you add a [Spam] tag in the body of the email that has been identified as spam. In addition, it adds a line in the header line of the email.

Only [Spam] tag is added in Subject: Body is left unchanged [Default]
This option lets you add the [Spam] tag only in the subject of the email, which has been identified as spam.

"X MailScan Spam: 1" header line is added: Body and subject both remain unchanged
This option lets you add a header line to the email. However, it does not add any tag to the subject line or body of the email.

Web Protection

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



Web Protection

Help

● Start | ○ Stop

□ Start Phishing Filter □ Start Malware URL Filter

Filtering Options | Scanning Options | Define Time-Restriction

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

Add | Delete

Site Names

playboy.com

Add | Delete | Save

Filtering Options

□ Add sites rejected by the filter to Block category

Default | Advanced Setting | OK | Cancel

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

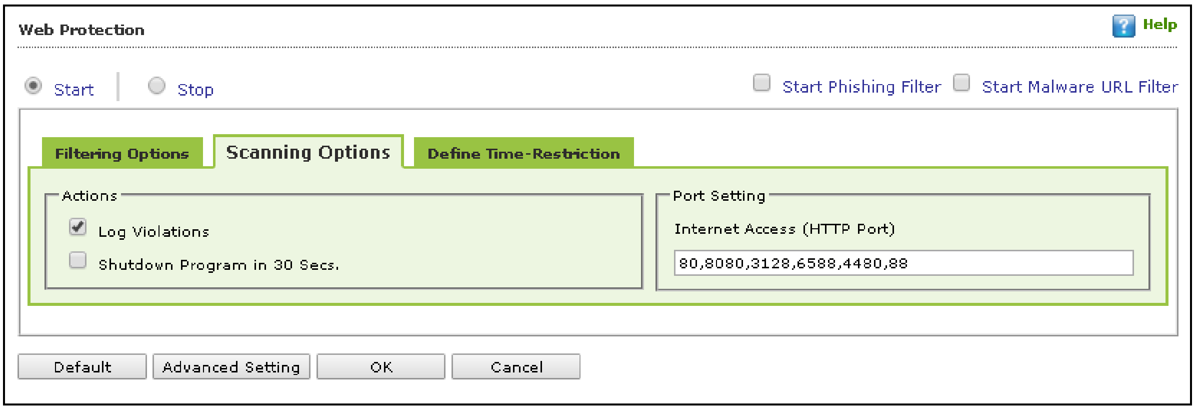
This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category. You can also add or delete filter categories depending on your requirement.

Filter Options

This section includes the **Add sites rejected by the filter to Block category check box**. Select this option 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.



Web Protection

● Start | ○ Stop

□ Start Phishing Filter □ Start Malware URL Filter

Actions

☑ Log Violations

□ Shutdown Program in 30 Secs.

Port Setting

Internet Access (HTTP Port): 80,8080,3128,6588,4480,88

Actions

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

Log Violations [Default]

This check box is selected by 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

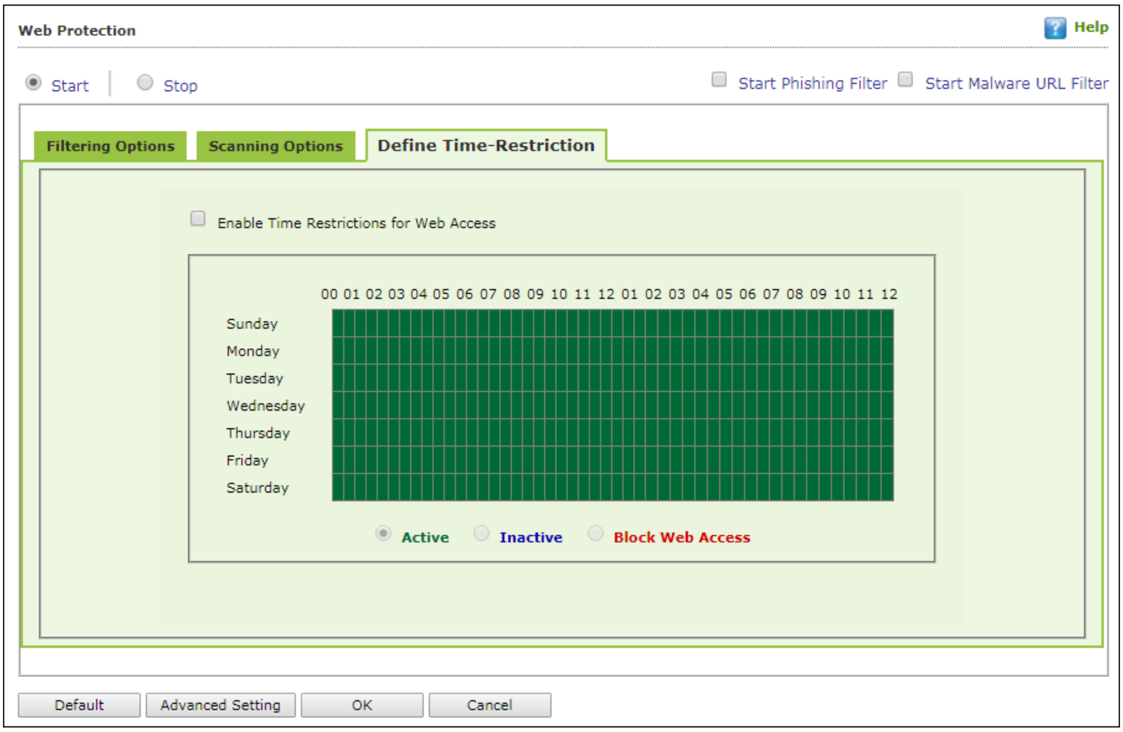
This section lets you specify the port numbers that eScan should monitor for suspicious traffic.

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.



Web Protection

● Start ○ Stop □ Start Phishing Filter □ Start Malware URL 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 the 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.

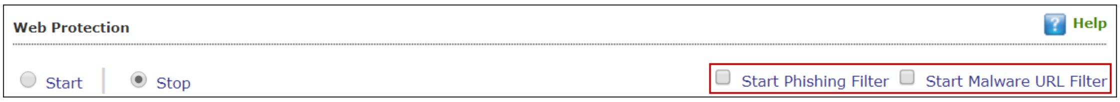
Block Web Access

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

Phishing and Malware URL Filter

Under Web Protection eScan also provides options to enable Phishing and Malware filters which will detect and prevent any phishing attempts on the system and block all malware attacks.

To enable the filters, select **Start** and then select the respective check boxes.



Web Protection

○ Start | ● Stop

□ Start Phishing Filter □ Start Malware URL Filter

Advanced Settings

Clicking **Advanced** displays Advanced Settings.

Enable HTTPS Popup (1 = Enable/0 = Disable)

Select this option to enable/disable HTTPS pop-ups.

Enable HTTP Popup (1 = Enable/0 = Disable)

Select this option to enable/disable HTTP pop-ups.

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 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)

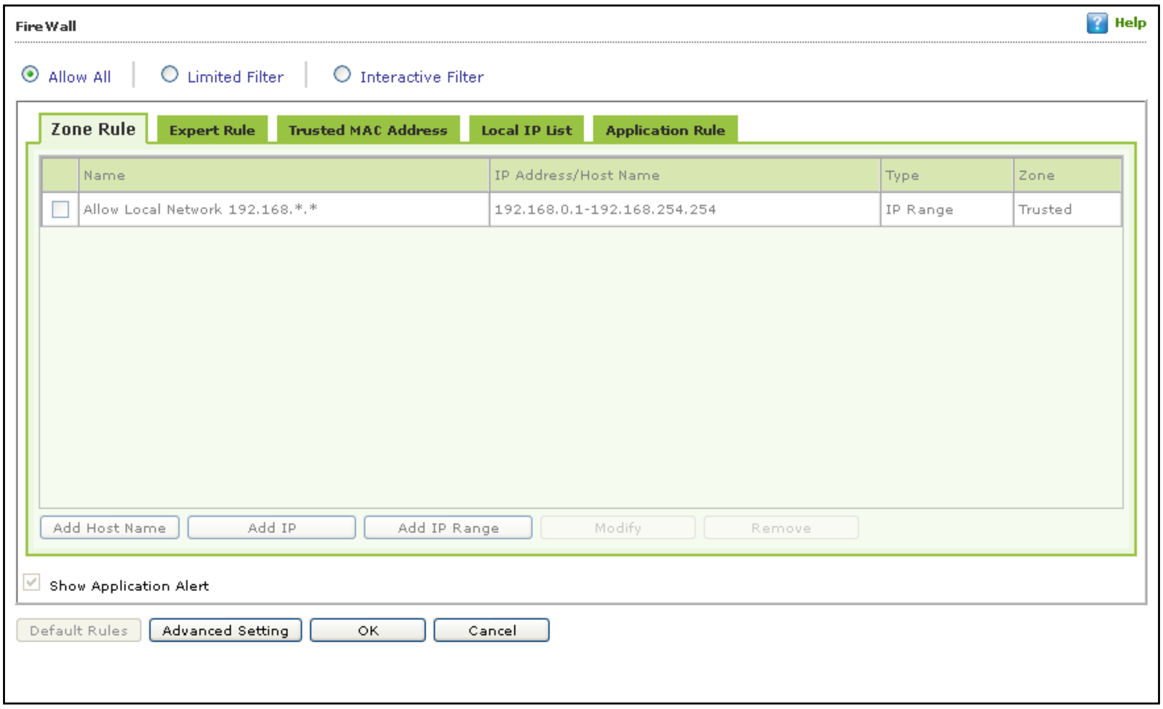
Select this option to force enable/disable web protection using filter driver.

WFP Exclude IP List (1 = Enable/0 = Disable)

Select this option to enable/disable excluding IP list from Web Filter Protection.

Firewall

Firewall module is designed to monitor all incoming and outgoing network traffic and protect your computer 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. Therefore, the Firewall feature first checks the rules, analyzes network packets, and filters them on the basis of the specified rules. When you connect to the Internet, you expose your computer to various security 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

☑ Show Application Alert

The Firewall feature of eScan protects your data when you:

- Connect to Internet Relay Chat (IRC) servers and join other people on the numerous channels on the IRC network.
- Use Telnet to connect to a server on the Internet and then execute the commands on the server.
- Use FTP to transfer files from a remote server to your computer.
- Use Network Basic Input Output System (NetBIOS) to communicate with other users on the LAN connected to the Internet.
- Use a computer that is a part of a Virtual Private Network (VPN).
- Use a computer to browse the Internet.
- Use a computer to send or receive email.

By default, the firewall operates in the **Allow All** mode. However, you can customize the firewall by using options like **Limited Filter** for filtering only incoming traffic and **Interactive Filter** to monitor incoming and outgoing traffic. The eScan Firewall also lets you specify different set of rules for allowing or blocking incoming or outgoing traffic. These rules include Zone Rules, Expert Rules, Trusted Media Access Control (MAC) Address, and Local IP list. This page provides you with options for configuring the module. 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
Application Rule

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.
Buttons (to configure a zone rule)

Add Host Name – This option lets you add a "host" in the zone rule. After clicking **Add Host Name**, enter the HOST name 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 – 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

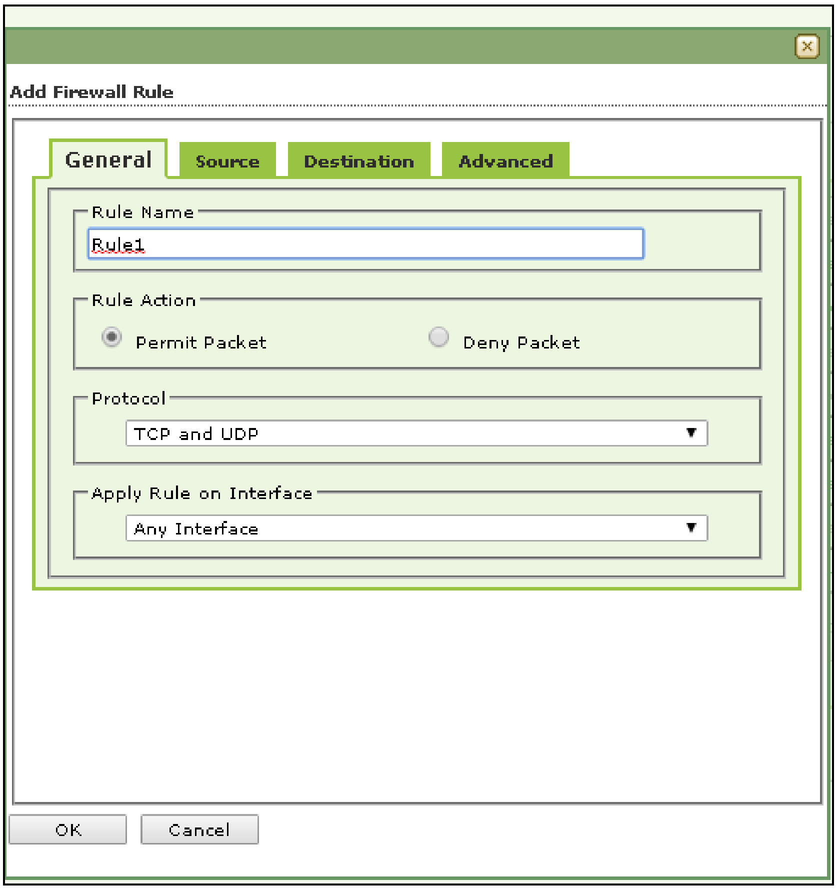
This tab lets you specify advanced rules and settings for the eScan firewall. You can configure expert rules on the basis of the various rules, protocols, source IP address and port, destination IP address and port, and ICMP types. You can create new expert rules.

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

Buttons (to configure an Expert Rule)

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



Add Firewall Rule

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.

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

Host Name – The rule will be applied for the outgoing traffic originating from the computer as per the host name specified.

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.

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 port 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.

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

Host Name – The rule will be applied for the incoming traffic to the computer as per the host name specified.

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.

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.

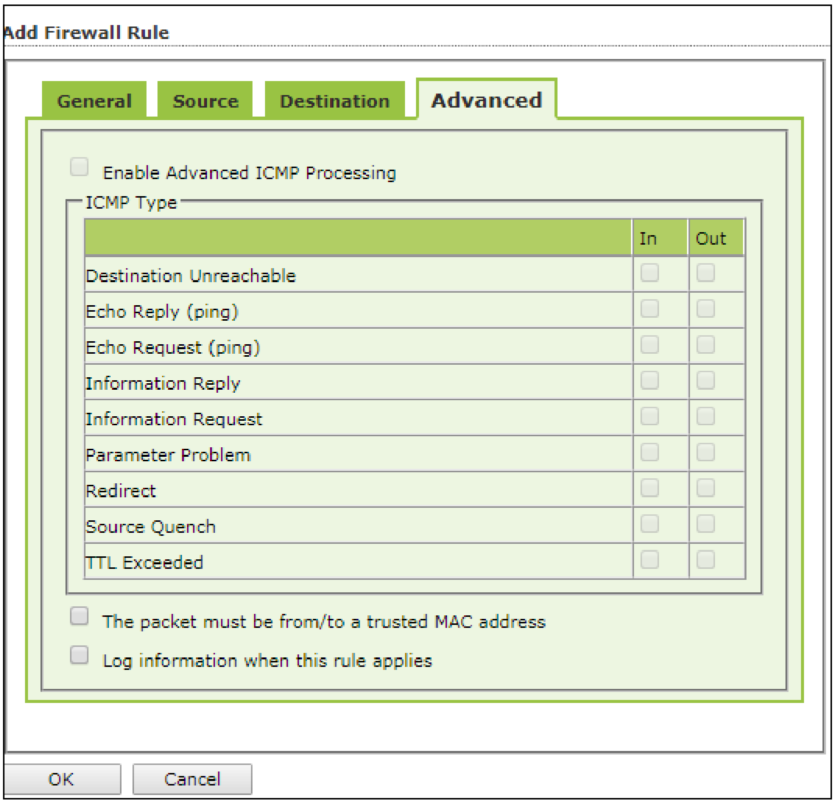
Port Range – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the incoming traffic to the port which is within the defined range of ports.

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

NOTE	The rule will be applied when the selected Destination IP Address and Destination Port 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

□ Log information when this rule applies

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.

Log information when this rule applies – This will enable to log information of the Rule when it is implied.

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).
Buttons (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. 00-13-8F-27-00-47

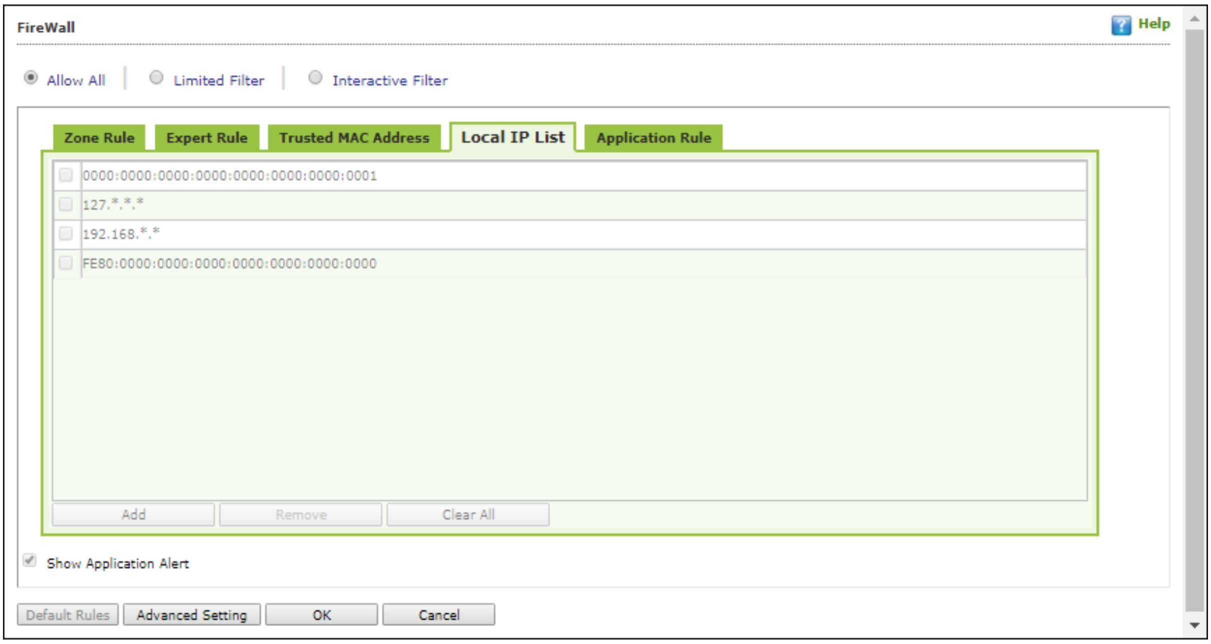
Edit – To modify/change the MAC Address, click **Edit**.

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.



FireWall

● Allow All ○ Limited Filter ○ Interactive Filter

Local IP List

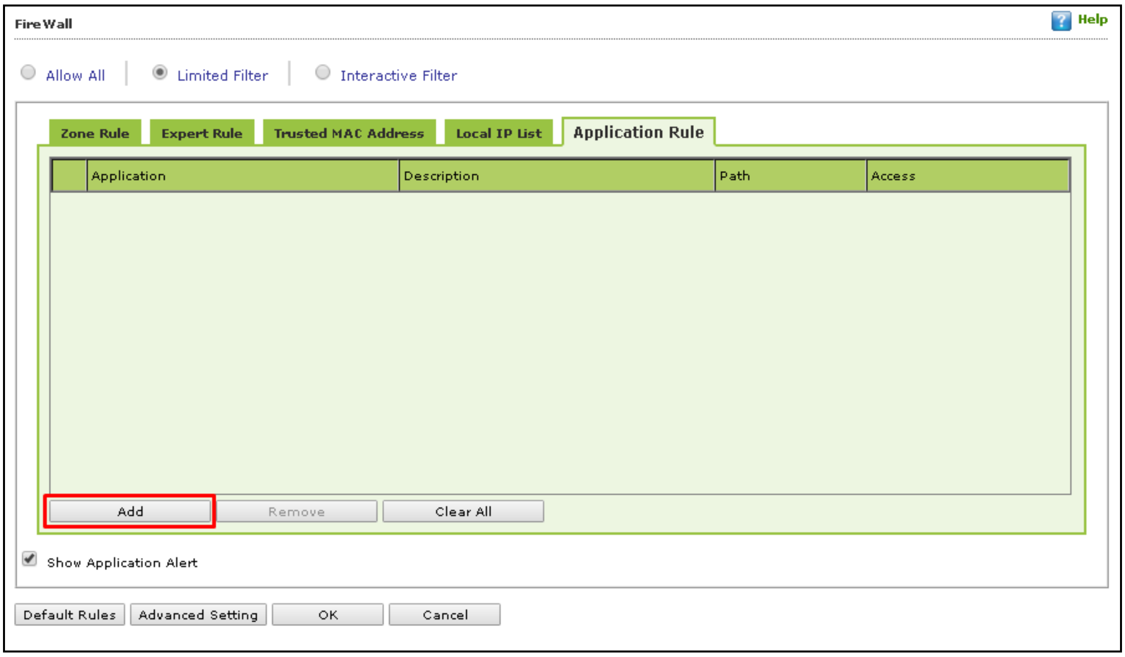
□ 0000:0000:0000:0000:0000:0000:0000:0001
□ 127.*.*.*
□ 192.168.*.*
□ FE80:0000:0000:0000:0000:0000:0000:0000

☑ Show Application Alert

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**.
Default List – To load the default list of IP addresses, click **Default List**.

Application Rule

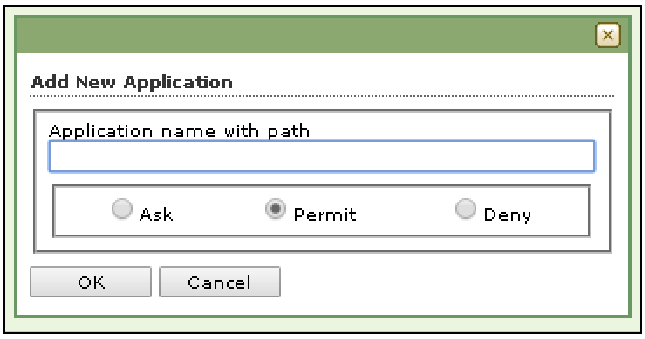
In this section you can define the permissions for different application. The application can be set to Ask, Permit or Deny mode.



Defining permission for an application

To define permission for an application,

1. Click **Add**.
2. Add New Application window appears.



3. Enter the application name with path and select a permission.
4. Click **OK**.

   The permission for the application will be defined.

Removing permission of an application

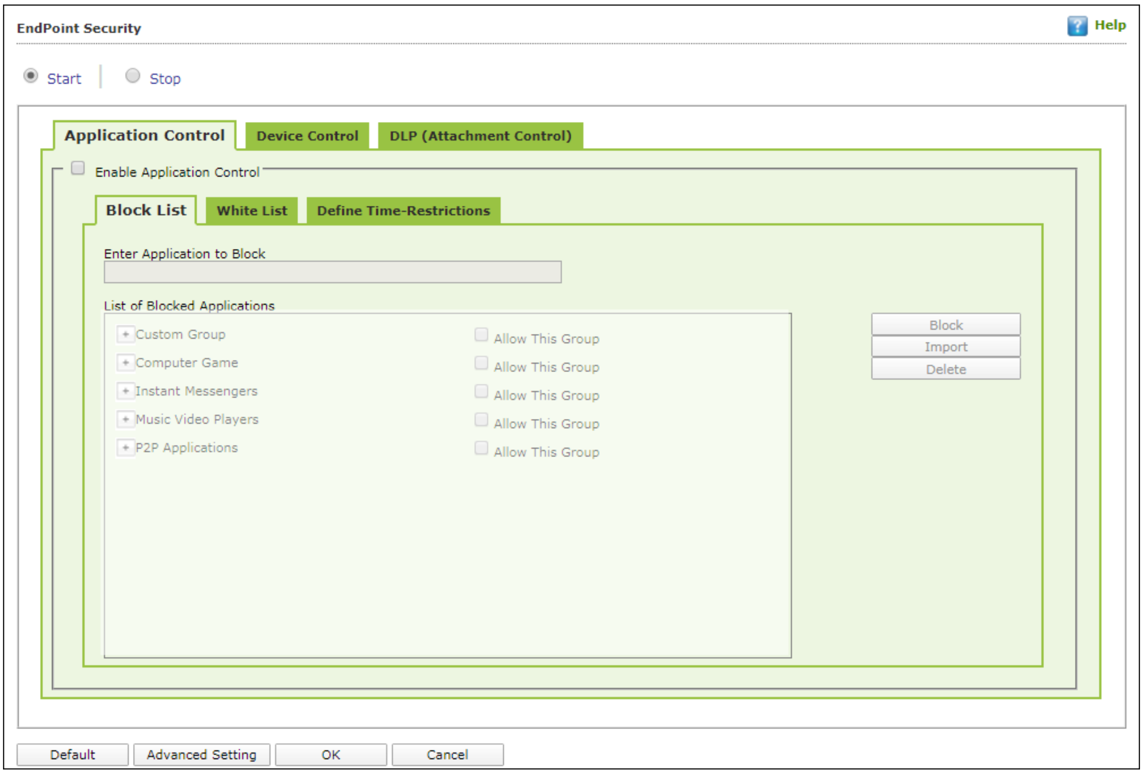
Select an application and then click **Remove**. The application will no longer have the permission.

Other Buttons

- **Clear All** - This option will clear/delete all the information stored by the Firewall cache.
- **Show Application Alert** – Selecting this option will display an eScan Firewall Alert displaying the blocking of any application as defined in the Application Rule.
- **Default Rules** - This button will load/reset the rules to the Default settings present during the installation of eScan. This will remove all the settings defined by user.

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.



EndPoint Security

Help

● Start | ○ Stop

Application Control | Device Control | DLP (Attachment Control)

□ Enable Application Control

Block List | White List | Define Time-Restrictions

Enter Application to Block

List of Blocked Applications

+ Custom Group	□ Allow This Group
+ Computer Game	□ Allow This Group
+ Instant Messengers	□ Allow This Group
+ Music Video Players	□ Allow This Group
+ P2P Applications	□ Allow This Group

This page provides you with information regarding the status of the module and options for configuring it.

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

There are two tabs – Application Control and USB Control, 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 full name of the application to be blocked.

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 to the Custom Group category. If you want, you can unblock the predefined application by clicking the **UnBlock** link. The predefined categories include computer games, instant messengers, music & video players, and P2P applications.

White List

Enable White Listing

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

Enter Application to whitelist

Enter the name of the application to be whitelisted.

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.

Define Time Restrictions

This option lets you enable/disable application control feature. 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.

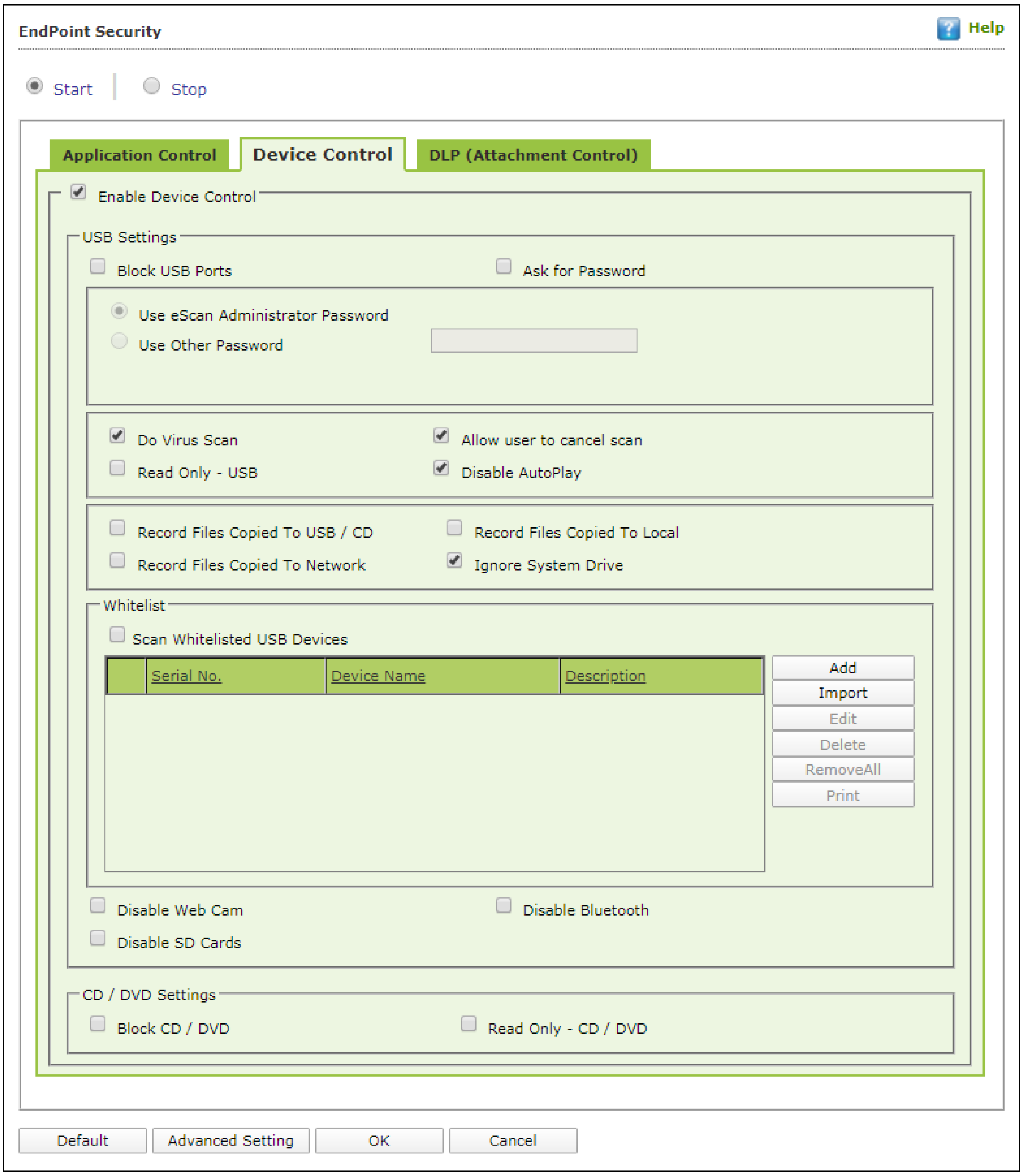
For example, the administrator can block computer games, instant messengers, for the whole day but allow during lunch hours without violating the Application Control Policies.

Datewise Restrictions

This feature 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.



EndPoint Security

● Start | ○ Stop

Application Control | Device Control | DLP (Attachment Control)

☑ Enable Device Control

USB Settings

□ Block USB Ports □ Ask for Password

● Use eScan Administrator Password

○ Use Other Password

☑ Do Virus Scan ☑ Allow user to cancel scan

□ Read Only - USB ☑ Disable AutoPlay

□ Record Files Copied To USB / CD □ Record Files Copied To Local

□ Record Files Copied To Network ☑ Ignore System Drive

Whitelist

□ Scan Whitelisted USB Devices

	Serial No.	Device Name	Description

□ Disable Web Cam □ Disable Bluetooth

□ Disable SD Cards

CD / DVD Settings

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

You can configure the following settings:

Enable Device Control [Default]

Select this option if you want to monitor all the USB storages 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 check box selected.

Use eScan Administrator

This option is available only when you select the **Ask for Password** check box. Click this option if you want to assign eScan Administrator password for accessing USB storage device.

Use Other Password

This option is available only when you select the **Ask for Password** check box. Click this option if you want assign a unique password for accessing USB storage device.

Do Virus Scan [Default]

When you select this option, the Endpoint Security module runs a virus scan if the USB storage device is connected. It is recommended that you always keep this check box selected.

Allow user to cancel scan

Select this option to allow the user to cancel the scanning process of the USB device.

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.

Read Only USB

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

Record Files Copied To USB

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

Record Files Copied To Network

Select this option if you want eScan to create a record of the files copied from managed computers to the network drive connected to it.

Record Files Copied To Local

Select this option if you want eScan to create a record of the files copied from the one drive to another drive of 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.

Ignore System Drive

Select this option in case of 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.

Whitelist

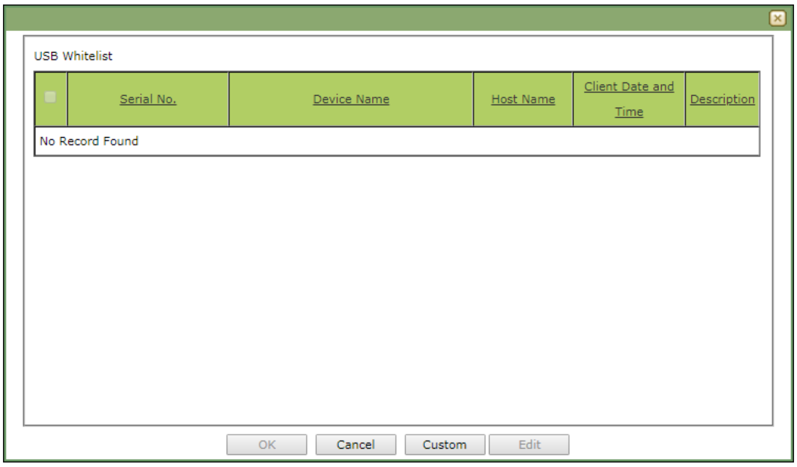
eScan provides a greater level of endpoint security by prompting you for a password whenever you connect a USB drive. To disable password protection for a specific device, you can add it along with its serial number to the whitelist. The next time you connect the device it will not ask for a password but 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 button.

Scan Whitelisted USB Devices

By default, eScan does not scan whitelisted USB devices. Select this option, if you want eScan to scan USB devices that have been added to the whitelist.

Add

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

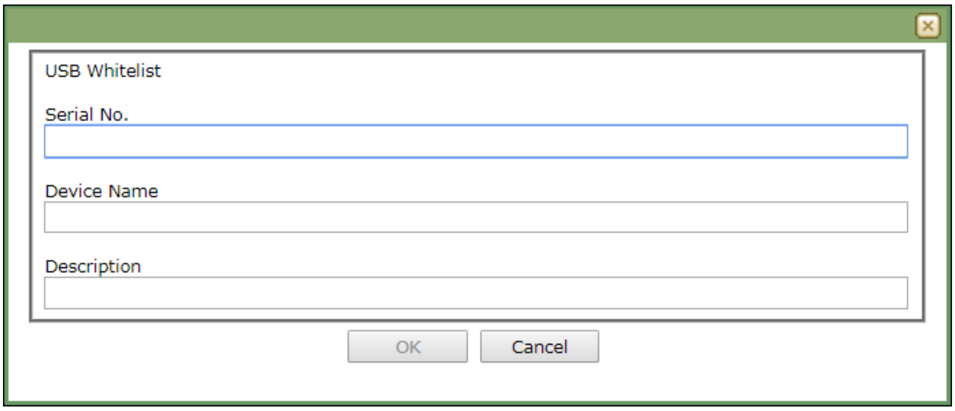


USB Whitelist

□	Serial No.	Device Name	Host Name	Client Date and Time	Description
No Record Found					

To whitelist a 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 with the list.
The list should be in following format:
Serial No 1, Device Name 1, Device Description 1(Optional)
Serial No 2, Device Name 2
Eg: SDFSD677GFQW8N6CN8CBN7CXVB, USB Drive 2.5, Whitelist by
xyzDFRGHHRS54456HGDF347OMCNAK, Flash Drive 2.2

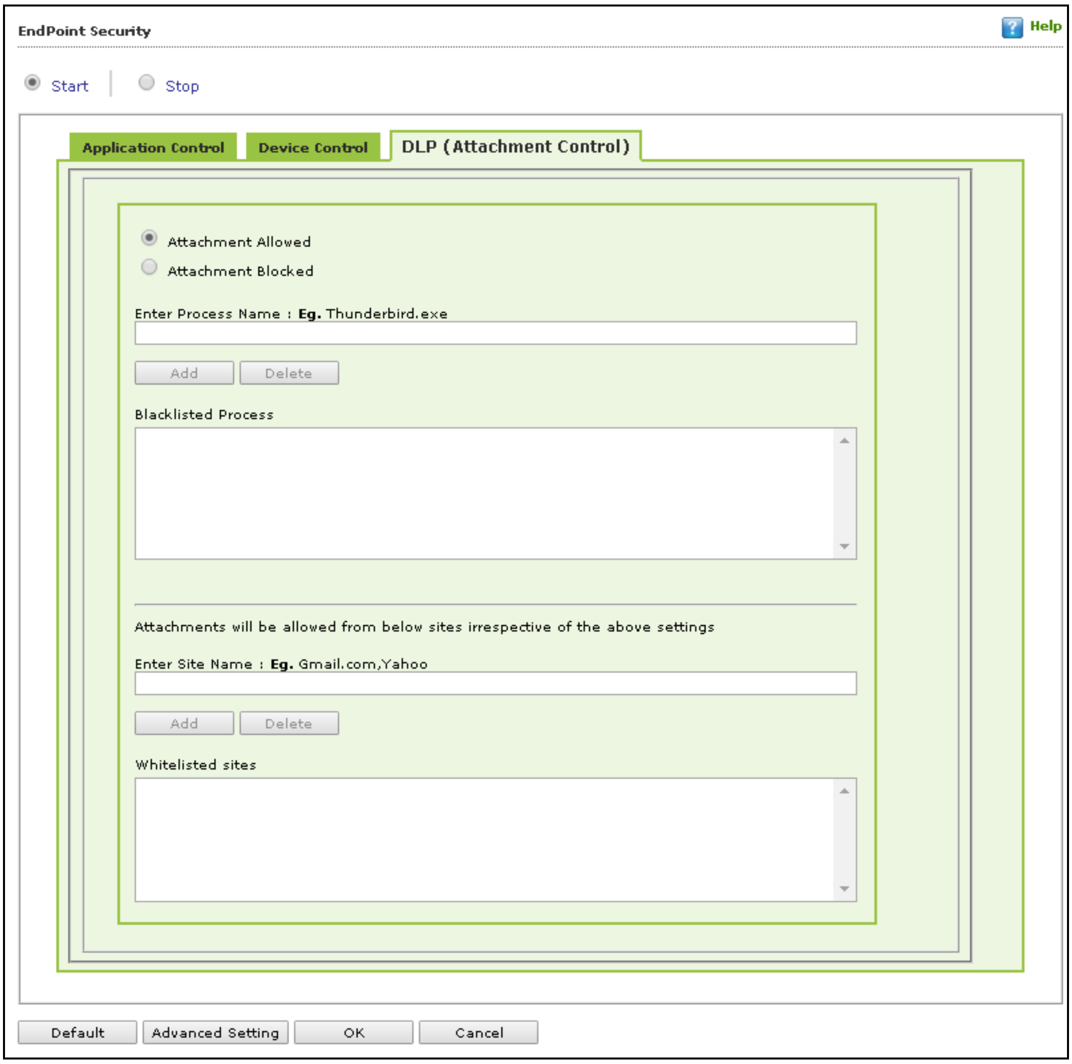
Disable Web Cam: Select this option to disable Webcams.
Disable SD Cards: Select this option to disable SD cards.
Disable Bluetooth: Select this option to disable Bluetooth.

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.

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

DLP (Attachment Control)

The DLP (Attachment Control) 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.



You can configure the following settings:

Attachment Allowed
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.

Enter Process Name
Enter the name of the processes that should be excluded from the above selection.

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.

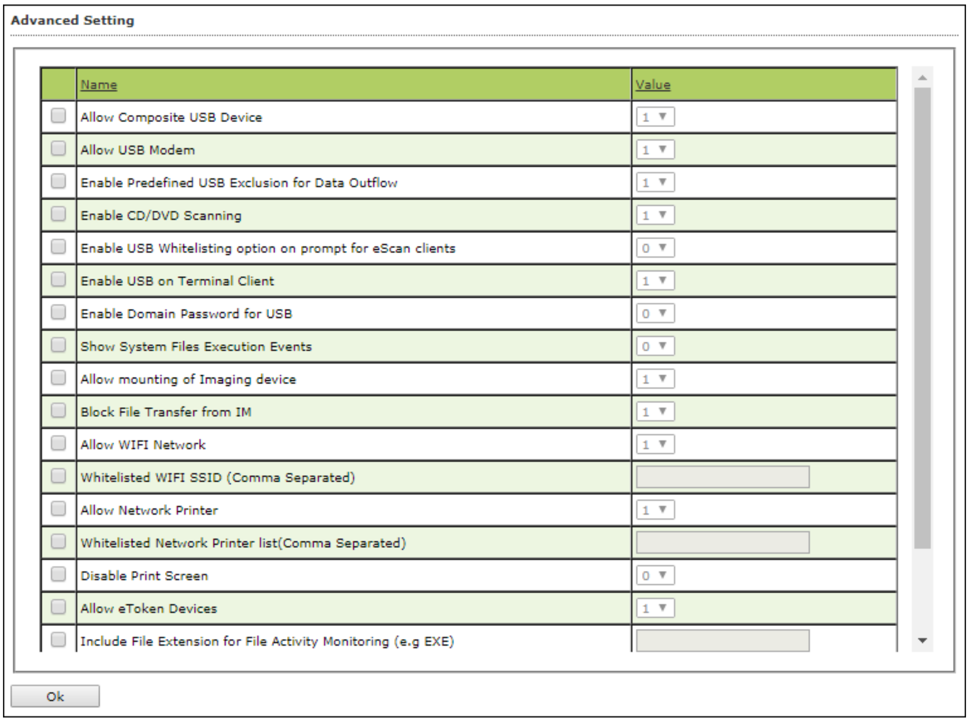
Enter Site Name

Enter the name of the websites through which attachments should be allowed irrespective of the above settings.

Whitelisted Sites

The websites added above to be whit listed are displayed in this list.

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 USB on Terminal Client (1 = Enable/0 = Disable)

Select this option to enable/disable USB on terminal client.

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.

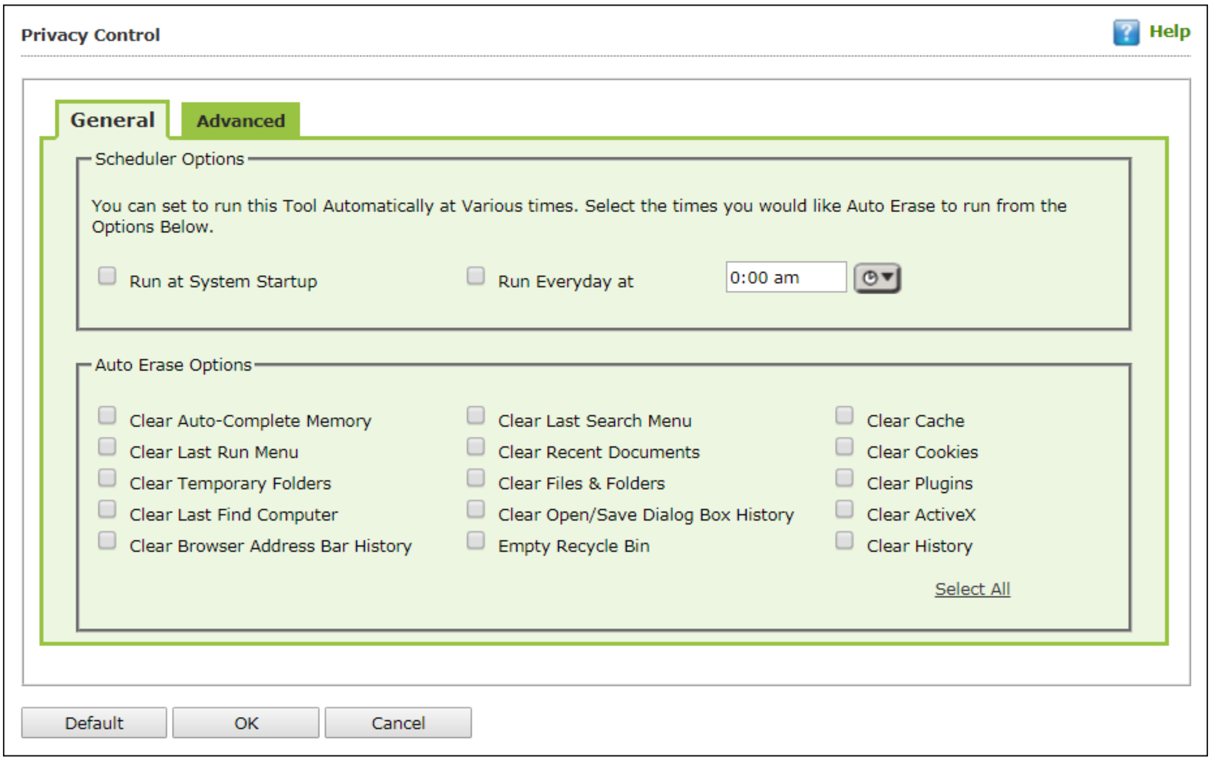
Allow Wi-Fi Network (1 = Enable/0 = Disable)
Select this option to allow/block use of Wi-Fi networks.

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

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

Privacy Control

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. This page provides you with options for configuring the module.



Privacy Control

Help

General | Advanced

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 Files & Folders
□ Clear Open/Save Dialog Box History
□ Empty Recycle Bin
□ Clear Cache
□ Clear Cookies
□ Clear Plugins
□ Clear ActiveX
□ Clear History

Select All

Default | OK | Cancel

It consists following tabs:

General
Advanced

General tab

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 Every day 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 check box, 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 check box, 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 check box, Privacy Control clears the names of the objects found in Recent Documents.

Clear Files & Folders
When you select this check box, Privacy Control deletes selected Files and Folders. Use this option with caution as it permanently deletes unwanted files and folders from the computer to free space on the computer.

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

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

Clear Cache
When you select this check box, Privacy Control clears the Temporary Internet Files.

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

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

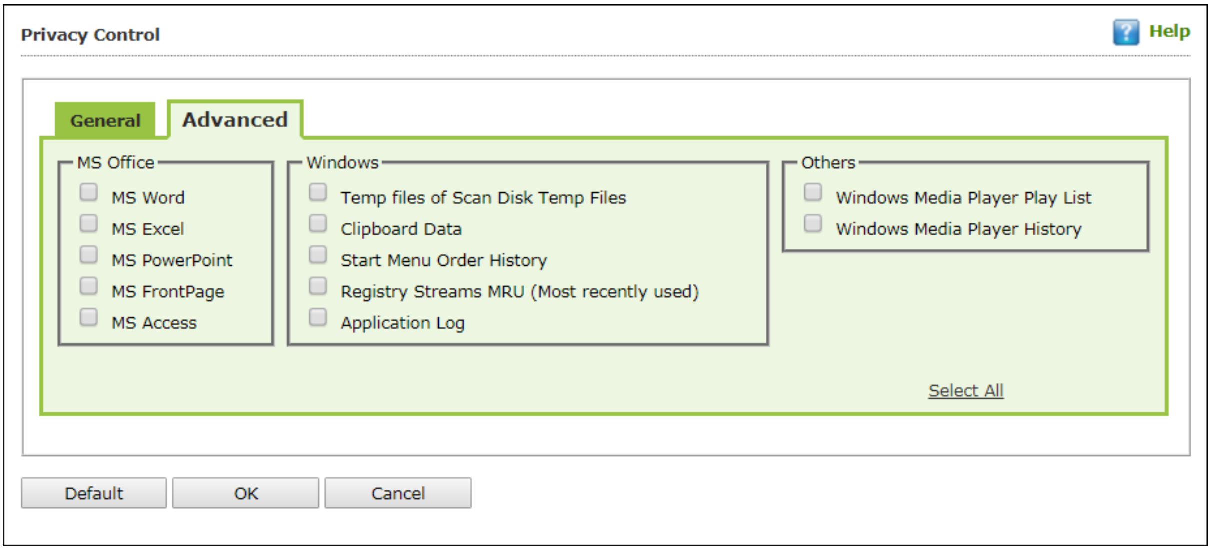
Clear ActiveX
When you select this check box, Privacy Control clears the ActiveX controls.

Clear History
When you select this check box, Privacy Control clears the history of all the websites that you have visited.
In addition to these options, the **Auto Erase Options** section has

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

Advanced tab

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

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

MS Office

The .msi extension files will be cleared if these options are selected**.**

Windows

The respective unwanted files like temp files will be cleared.

Others

The unwanted files in the Windows media player will be cleared.

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

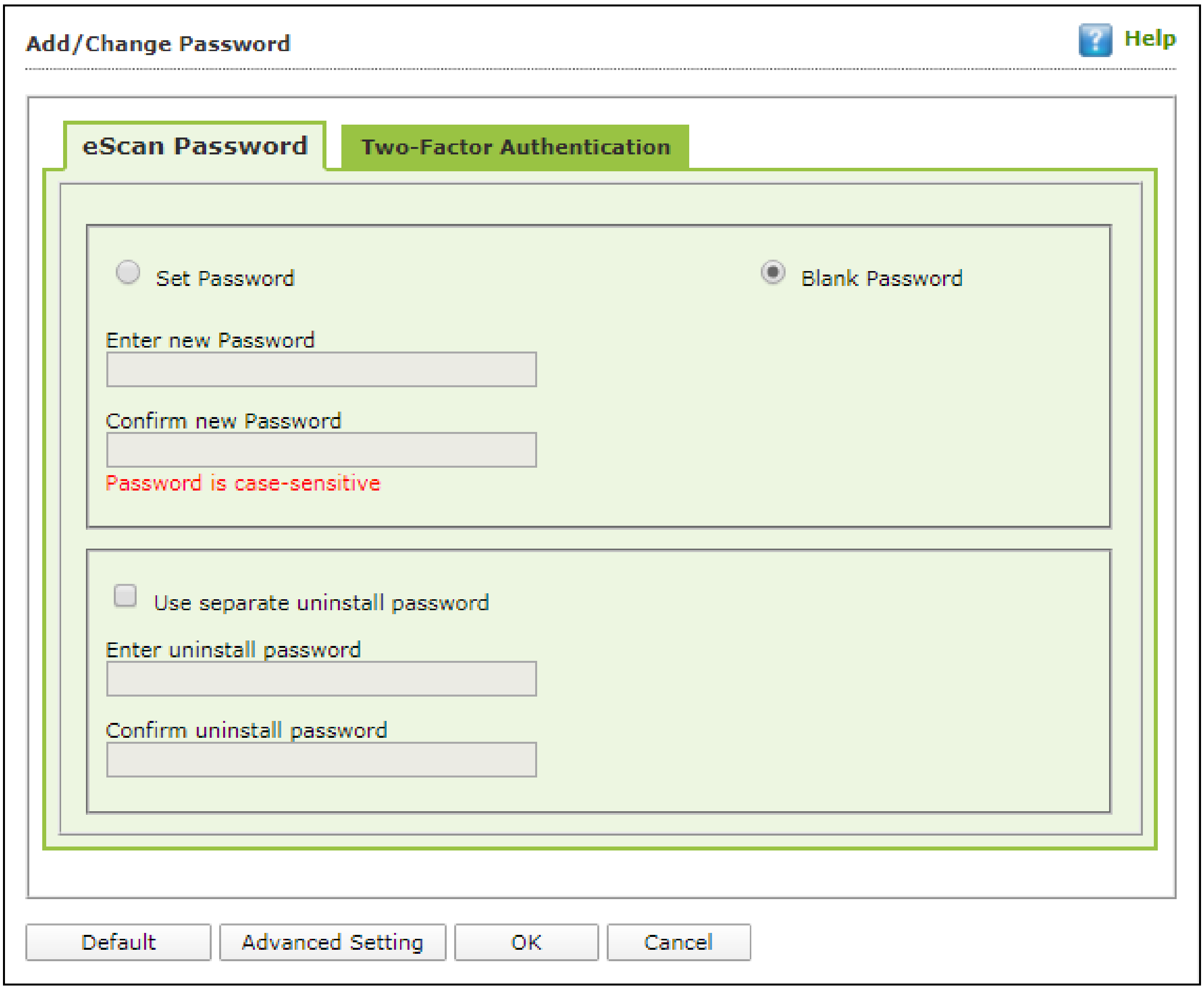
Policy Details also lets you do the following for Windows Operating System.

Administrator Password

Administrator Password lets you create and change password for administrative login of eScan protection center and Two-Factor Authentication.

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.



Add/Change Password

○ Set Password ● Blank Password

Enter new Password

Confirm new Password

Password is case-sensitive

□ Use separate uninstall password

Enter uninstall password

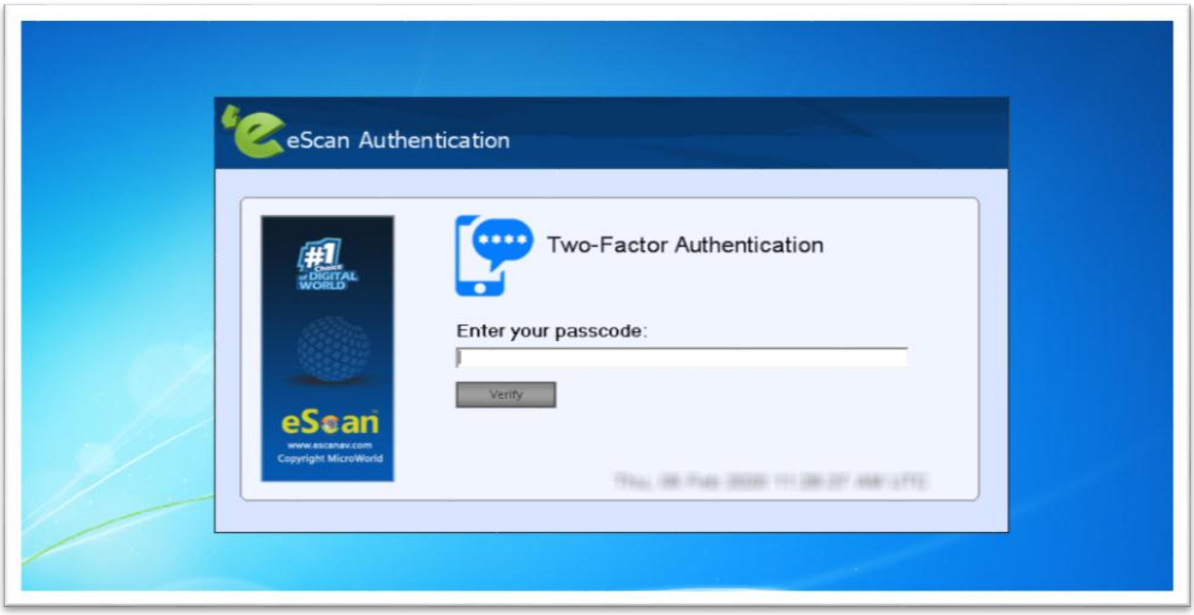
Confirm uninstall password

There is also an option to set a uninstall password. An uninstallation password prevents personnels 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**.

Two-Factor Authentication

Your default system authentication (login/password) is Single-Factor Authentication which is considered insecure 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 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 logons.

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 (as shown below) will appear. 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.



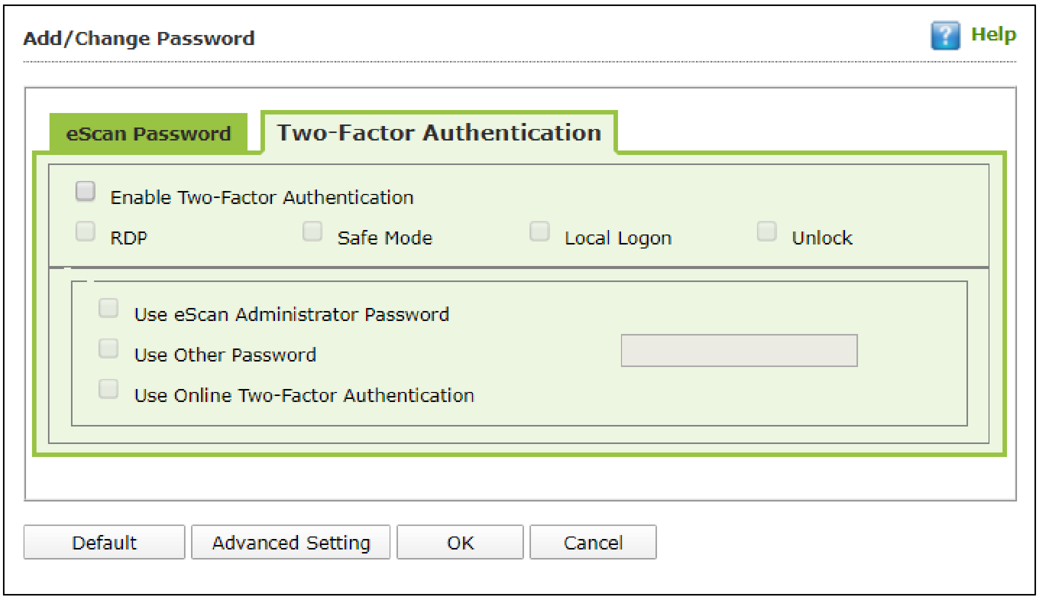
To enable the Two-Factor Authentication feature, follow the steps given below:

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** check box and then click **Edit**.

4. Click **Two-Factor Authentication** tab.
   Following window appears.



Add/Change Password

□ Enable Two-Factor Authentication

□ RDP □ Safe Mode □ Local Logon □ Unlock

□ Use eScan Administrator Password

□ Use Other Password

□ Use Online Two-Factor Authentication

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

Login Scenarios

The 2FA feature can be used for following all 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.

Local 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 combination of uppercase, lowercase, numbers, and special characters.

Use Online Two-Factor Authentication

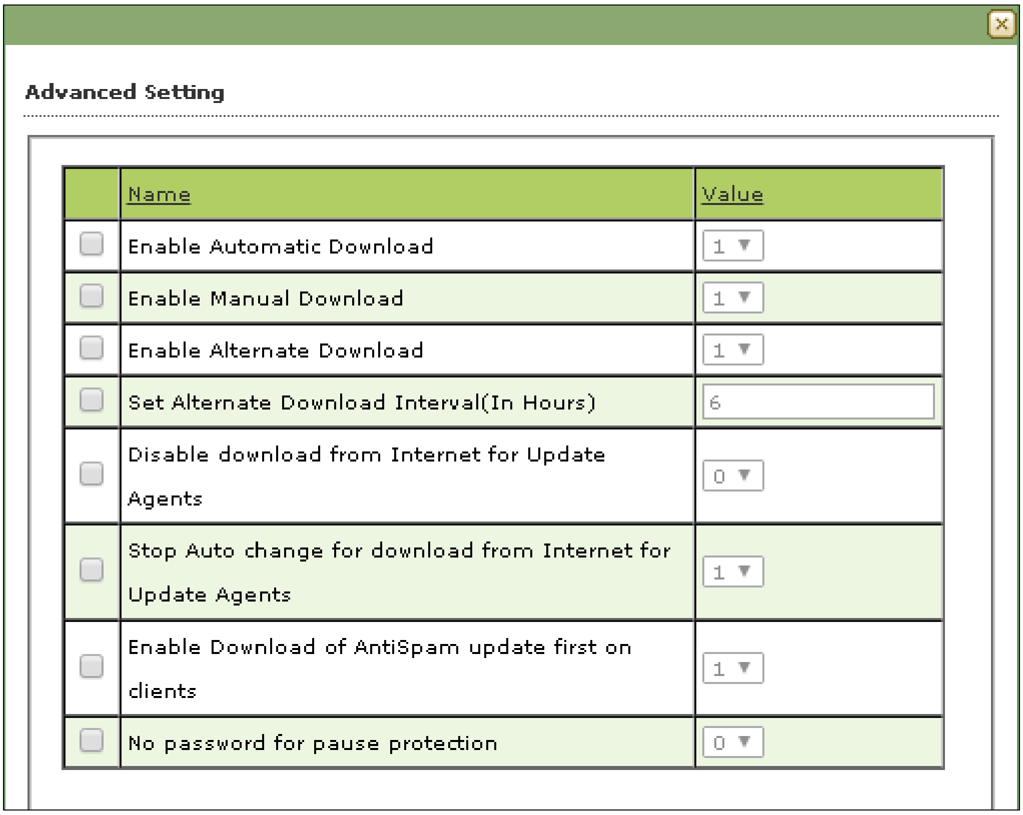
To use this feature, follow the steps given below:

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 check box **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.
6. Forward this TOTP to personnel for login.

After selecting the appropriate Login Scenarios and Password Types, click **OK**. The Policy Template gets saved/updated.

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 ▼

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 lets you pause eScan protection without entering password.

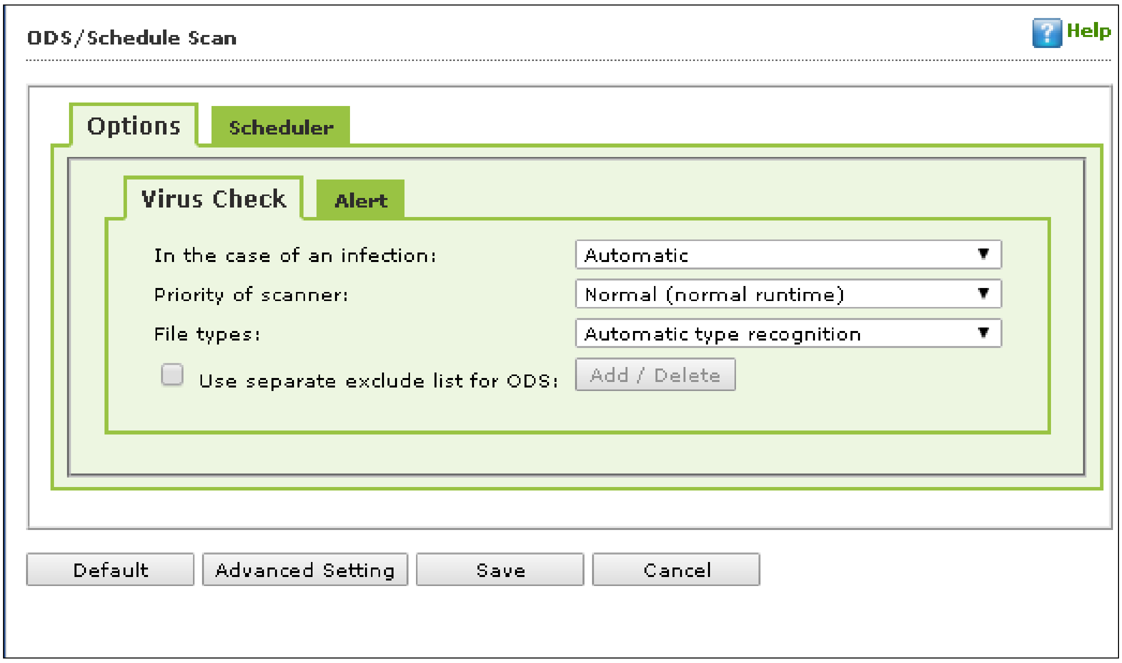
ODS/Schedule Scan

ODS (On Demand Scanning)/Schedule Scan provides you with various options like – checking for viruses, and making settings for creating logs and receiving alerts. You can also create task in the scheduler for automatic virus scanning.

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

It consists following tabs:

- **Options**
- **Scheduler**



ODS/Schedule Scan

In the case of an infection: Automatic

Priority of scanner: Normal (normal runtime)

File types: Automatic type recognition

□ Use separate exclude list for ODS:

Options

Options tab lets you make the settings for checking viruses and receiving alerts. There are two tabs – Virus Check and Alerts. You can do the following activities.

- Virus check
- Alerts

Virus Check

It lets you configure the settings for checking viruses.

To set virus check,

1. Specify the following field details.
    - **In the case of an infection**: Select an appropriate option from the drop-down list. For example, Log only, Delete infected file, and [Default] Automatic.
    - **Priority of scanner**: Select an appropriate option from the drop-down list. For example,
        - o High (short runtime)
        - o Normal (normal runtime) [Default]
        - o Low (long runtime)
    - **File types**: Select an appropriate option from the drop-down list. For example, \[Default\] Automatic type recognition and only program files.
    - **Use separate exclude list for ODS**: Select this option to add a list of file/folders that should be excluded from scan.
2. Click **Save**.

Alerts tab

It lets you configure the settings for virus alert. You can also create a log of the infected viruses.

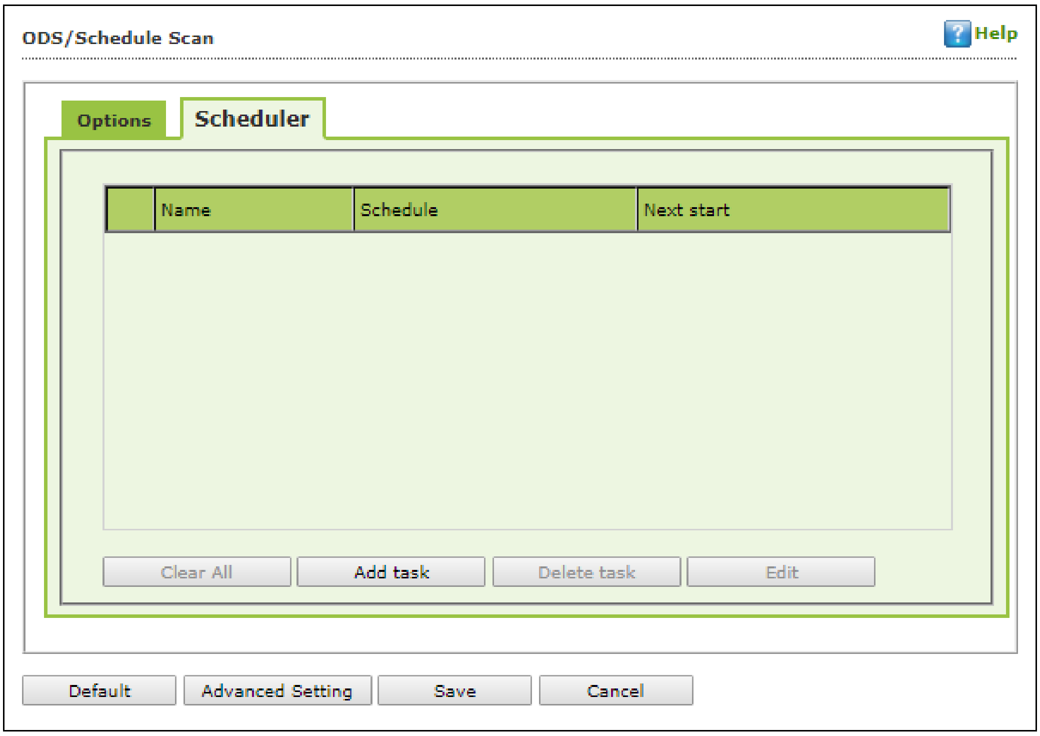
To set alerts,

1. Under **Alert** section, Select the [Default] **Warn**, if virus signature is more than x days old check box, and then enter the number of days in the x days old field, if you want to receive alerts when virus signature exceeds the specified days. By default, value 3 appears in the field.
2. Select the **Warn**, if the last computer analysis was more than x days ago check box, and then enter the number of days in the x days ago field, if you want to receive alerts when last computer analysis exceeds the specified days. By default, 3 appears in the field.
3. Under **Log Settings** section, select the [Default] **Prepare Log** check box, if you want to prepare log of the infected files, and then select an appropriate option.
4. Click **Save**.

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

Scheduler

Scheduler tab lets you create/delete various tasks in the scheduler for automatic virus scanning.



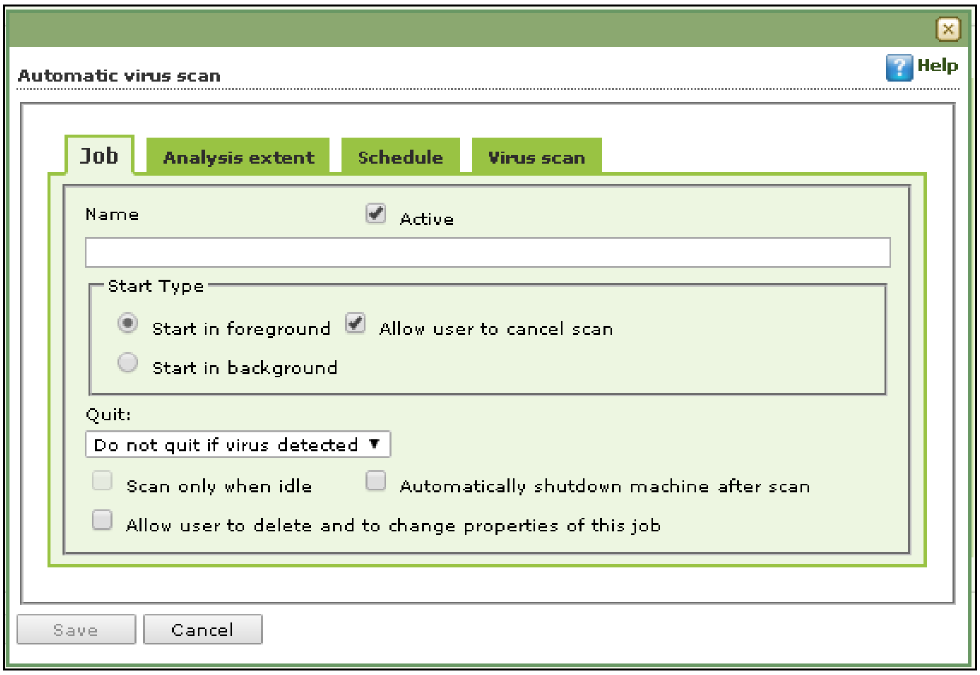
ODS/Schedule Scan

	Name	Schedule	Next start

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

Clear All - This button will clear all the listed tasks.

Add Task



Automatic virus scan

Name ☑ Active

Start Type

● Start in foreground ☑ Allow user to cancel scan

○ Start in background

Quit:

Do not quit if virus detected ▼

□ Scan only when idle □ Automatically shutdown machine after scan

□ Allow user to delete and to change properties of this job

Automatic Virus Scan lets you do following activities:

a) Creating job
b) Setting analysis extent
c) Scheduling virus execution
d) Scheduling virus scan

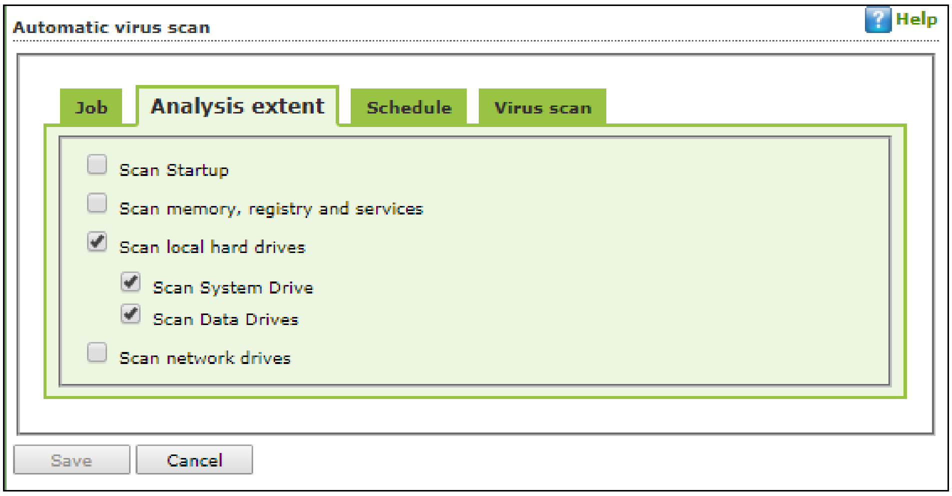
a) Job

It lets you create the job details for virus scanning.

1. Click the **Job** tab.
2. Specify the following field details.
   - **Name**: Enter a name for the task.
   - **Active [Default]**: Select this check box, if you want to allow the client to schedule the task.
   - **Start in foreground [Default]**: Click this option if you want to view scanning process running in front of you.
     When this option is selected, the **Scan only when idle** option becomes unavailable.
   - **Start in background**: Click this option if you want scanning process to run in the background. By default, Do not quit if virus is detected option is selected. When you select this option, the Quit drop-down list becomes unavailable.
3. Click **Save**.

b) Analysis Extent

It lets you configure analysis extent settings for virus scanning.



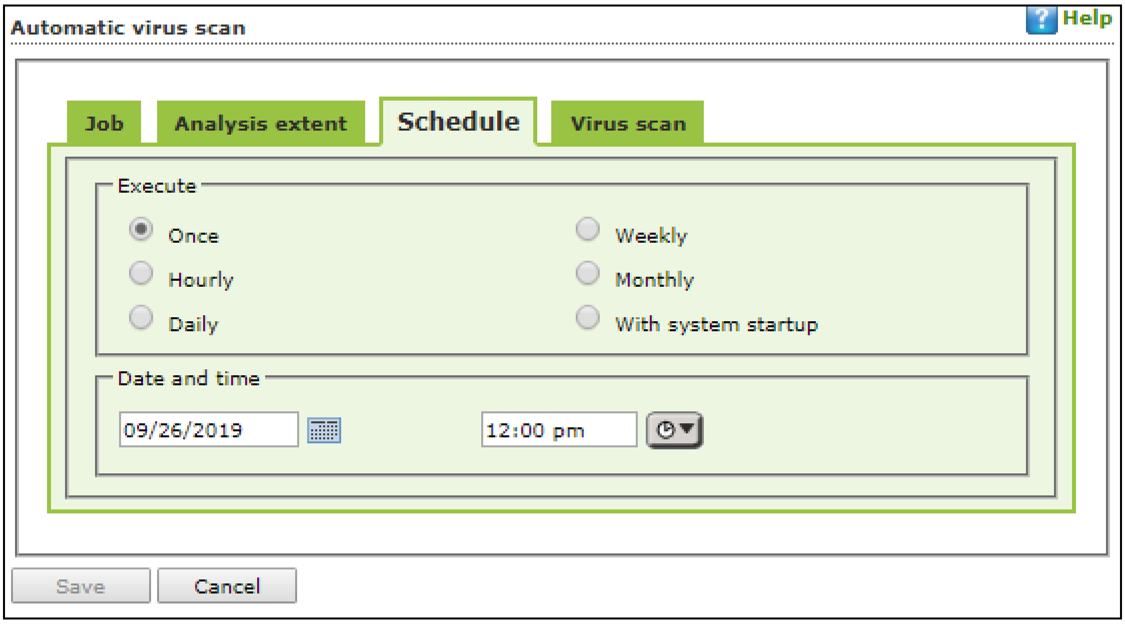
□ Scan Startup
□ Scan memory, registry and services
☑ Scan local hard drives
☑ Scan System Drive
☑ Scan Data Drives
□ Scan network drives

1. Click the **Analysis Extent** tab.
2. Select the **Scan Startup** option, if you want to scan all startup entries.
3. Select the **Scan memory, registry** and **services** option, if you want to scan memory, registry and services.
4. Select the [Default] **Scan local hard drives** option, if you want to scan local hard drives.

5. Select Scan network drives option, if you want to scan network drives. Users should note that scanning a network drive may affect system performance.
6. Click **Save**.

c) Scheduling

It lets you schedule the date and time of execution for virus scanning.



Automatic virus scan

Job | Analysis extent | Schedule | Virus scan

Execute

● Once ○ Weekly
○ Hourly ○ Monthly
○ Daily ○ With system startup

Date and time

09/26/2019 12:00 pm

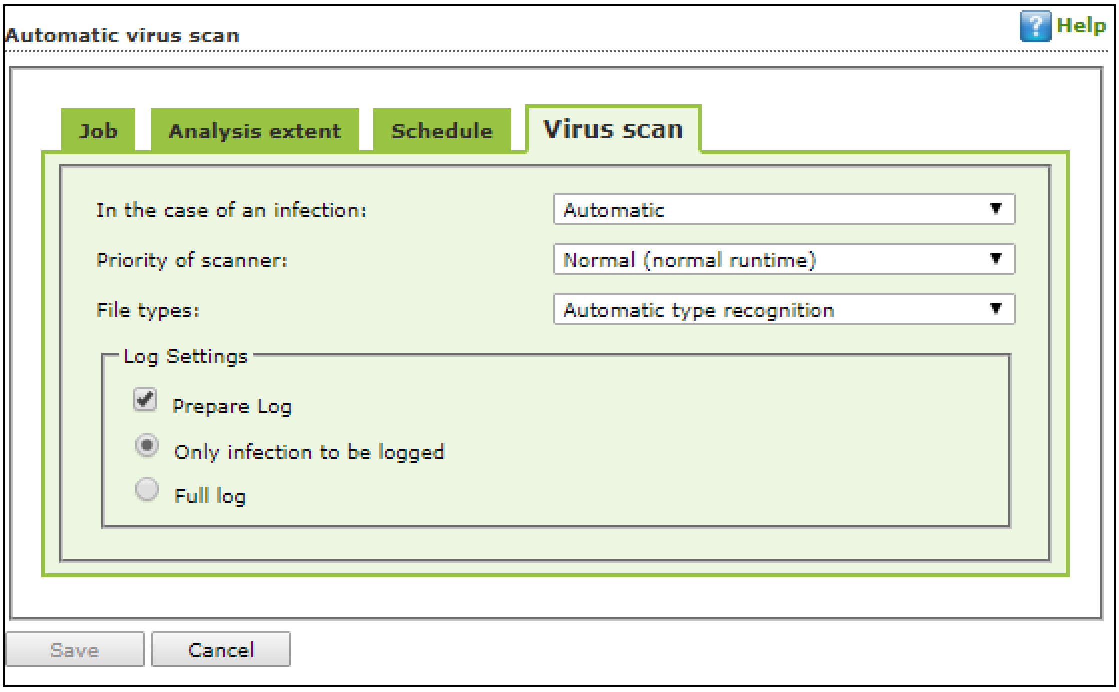
1. Click **Schedule** tab.
2. Under Execute section, select an appropriate option. For example, [Default] Once, weekly, hourly, and so on.
3. Under Date and time section, click the calendar icon. The calendar appears.
4. Select an appropriate date from the calendar.

NOTE	Click the left **<** and right **>** sign to navigate to the previous or next month and year from the calendar respectively.

5. Click the Time icon. The Timer appears.
6. Click the **AM** tab to view the before noon time and **PM** tab to view the afternoon time, and then select an appropriate time from the list.
7. Click **Save**.

d) Virus Scan

It lets you schedule virus scanning.



Automatic virus scan

In the case of an infection: Automatic

Priority of scanner: Normal (normal runtime)

File types: Automatic type recognition

Log Settings

☑ Prepare Log

● Only infection to be logged

○ Full log

1. Click the **Virus Scan** tab.
2. Specify the following field details.
   - **In the case of an infection**: Select an appropriate option from the drop-down list. For example, Log only, Delete infected file, and [Default] Automatic.
   - **Priority of scanner**: Select an appropriate priority from the drop-down list.
   - **File types**: Select an appropriate option from the drop-down list. For example, [Default] Automatic type recognition and Only program files.
3. Under Log Settings section, select the [Default] Prepare Log check box, if you want to prepare log of the infected files, and then click an appropriate option.
4. Click **Save**.

Delete Task – Clicking **Delete Task** lets you delete the particular task from the list.

Edit – Clicking **Edit** lets you edit the properties of the particular task from the list.

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.

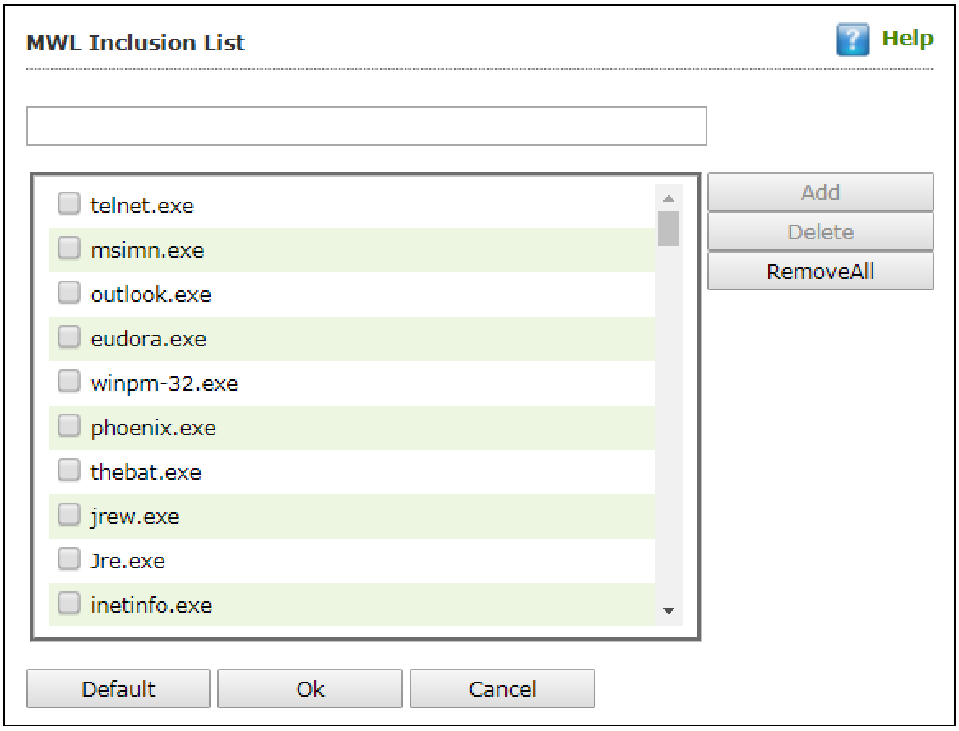
MWL Inclusion List

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

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

You can do the following activities.

- **Adding files** to Inclusion List
- **Deleting files** from Inclusion List
- **Removing all files** from Inclusion List



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,

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

Delete files from Inclusion List

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

1. Select executable files, 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,

1. Click **Remove All**.
   A confirmation prompt appears.
2. Click **OK**.
   All executable files will be removed from the Inclusion List.

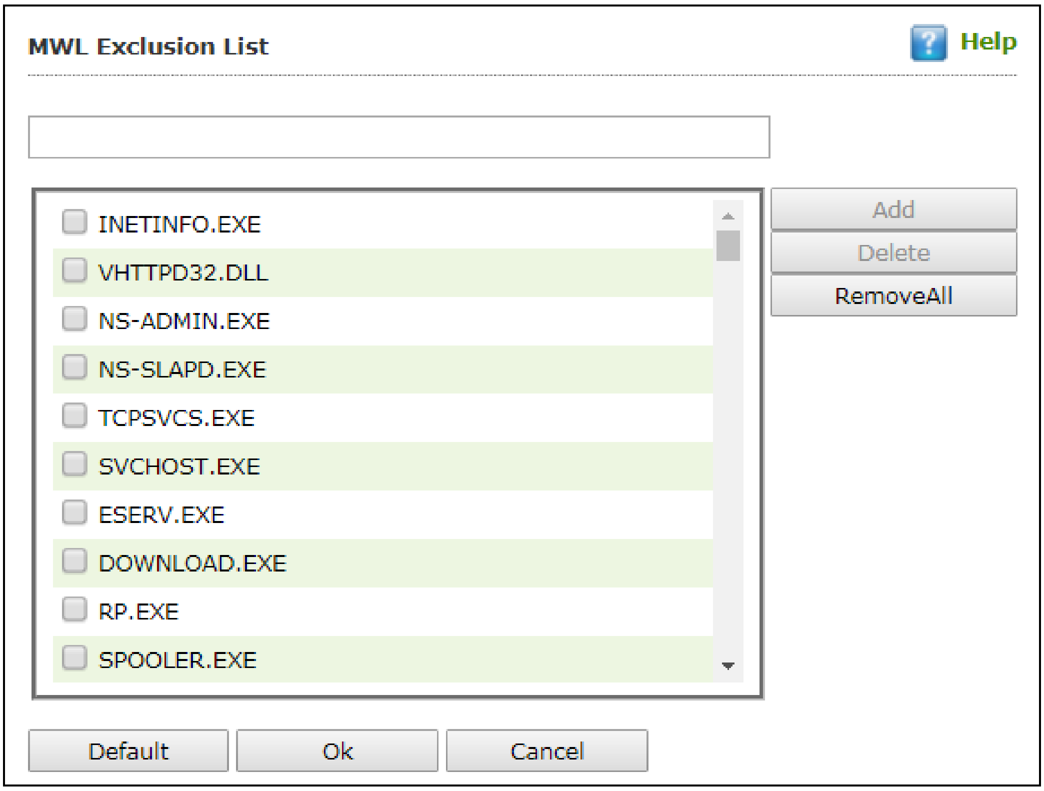
MWL Exclusion List

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

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

You can do the following activities.

- **Adding files** to Exclusion List
- **Deleting files** from Exclusion List
- **Removing all files** from Exclusion List



□ 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,

1. Enter the executable file name and then click **Add**.
   The executable file gets added to the Exclusion List.
2. Click **OK**.

Deleting files from Exclusion List

To delete executable files from the Exclusion List,

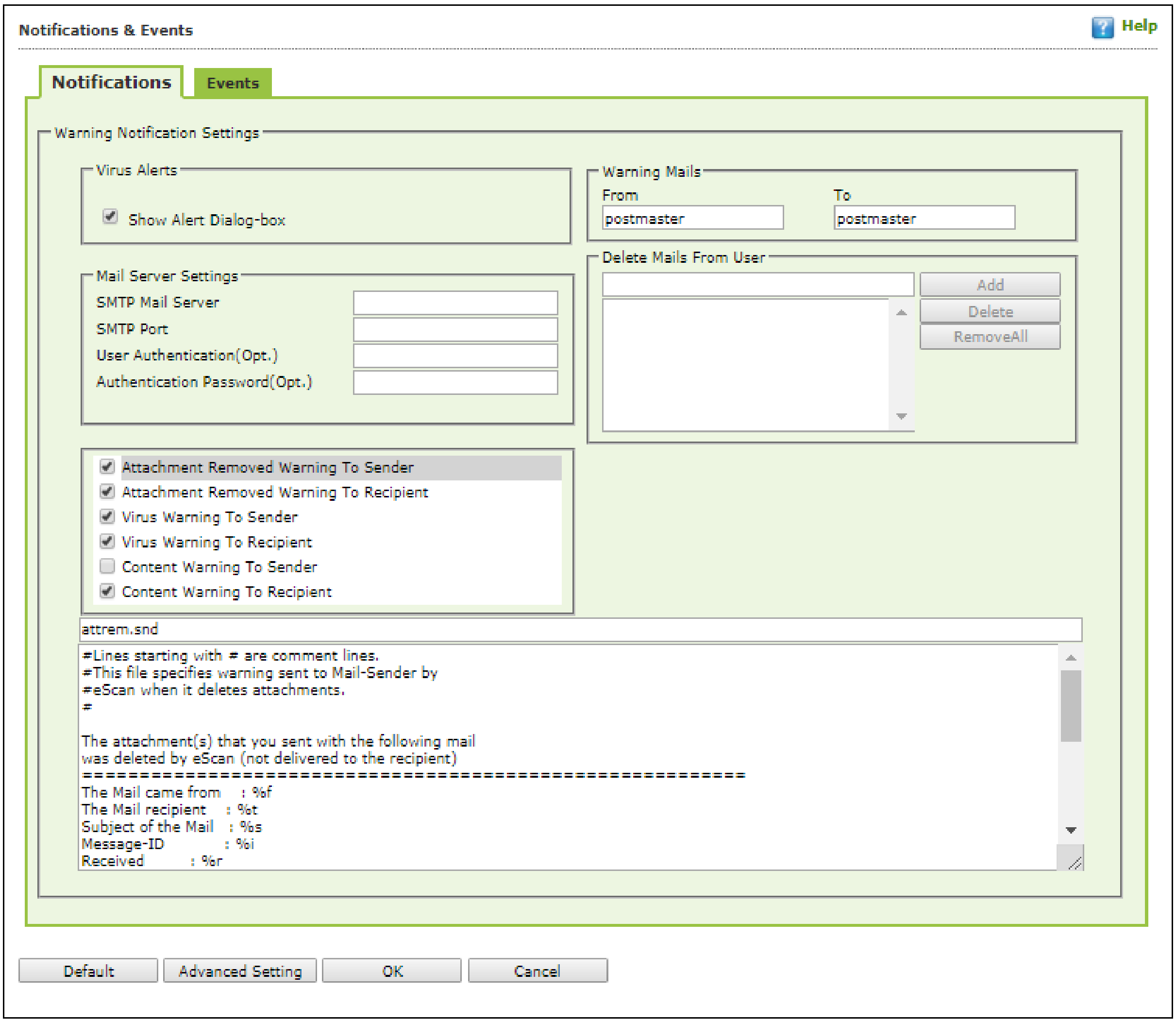
1. Select the appropriate file check box, and then click **Delete**.
   A confirmation prompt appears.
2. Click **OK**.
   The executable file gets deleted from the Exclusion List.

Removing all files from Exclusion List

To remove all executable files from the Exclusion List,

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

Notifications and Events



Notifications & Events

Warning Notification Settings

Virus Alerts

☑ Show Alert Dialog-box

Warning Mails

From: postmaster

To: postmaster

Mail Server Settings

SMTP Mail Server

SMTP Port

User Authentication(Opt.)

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 check box 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 check box 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 check box 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 check box 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 check box 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 check box if you want Mail scanner to send a content warning message to the recipient. The email content is displayed in the preview box.

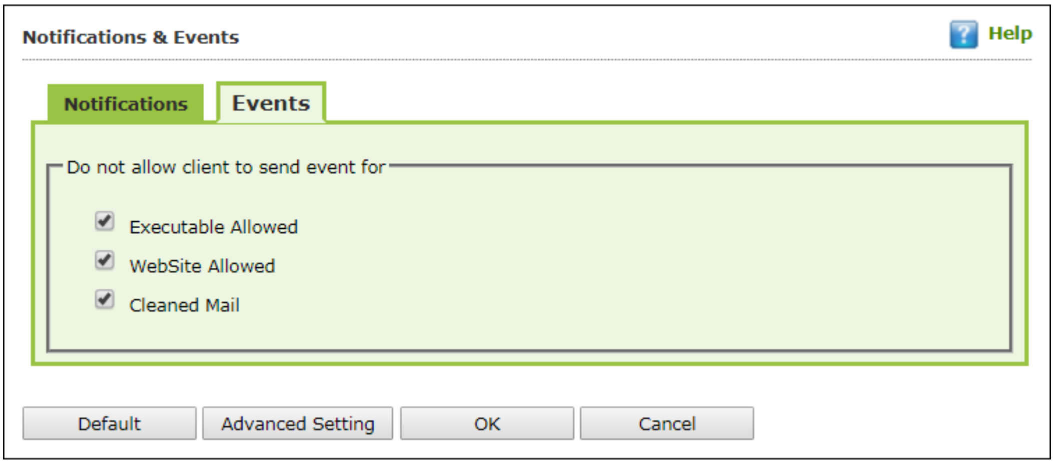
Delete Mails from User
You can configure eScan to automatically delete emails that have been sent by specific users. For this, you need to add the email addresses of such users to the **Delete Mails From User** field. The **Add**, **Delete**, and **Remove All** buttons appear as dimmed. After you enter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

Events

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

- Executable Allowed
- Website Allowed
- Cleaned Mail

By default, all events are selected.



Notifications & Events

Do not allow client to send event for

☑ Executable Allowed

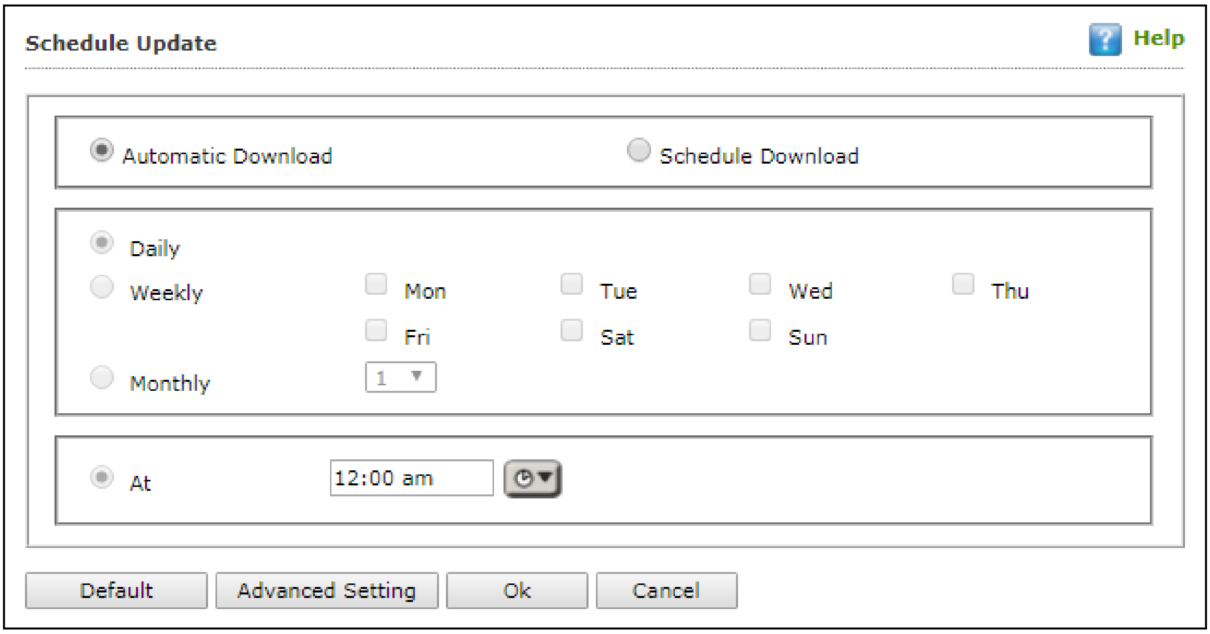
☑ WebSite Allowed

☑ Cleaned Mail

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

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

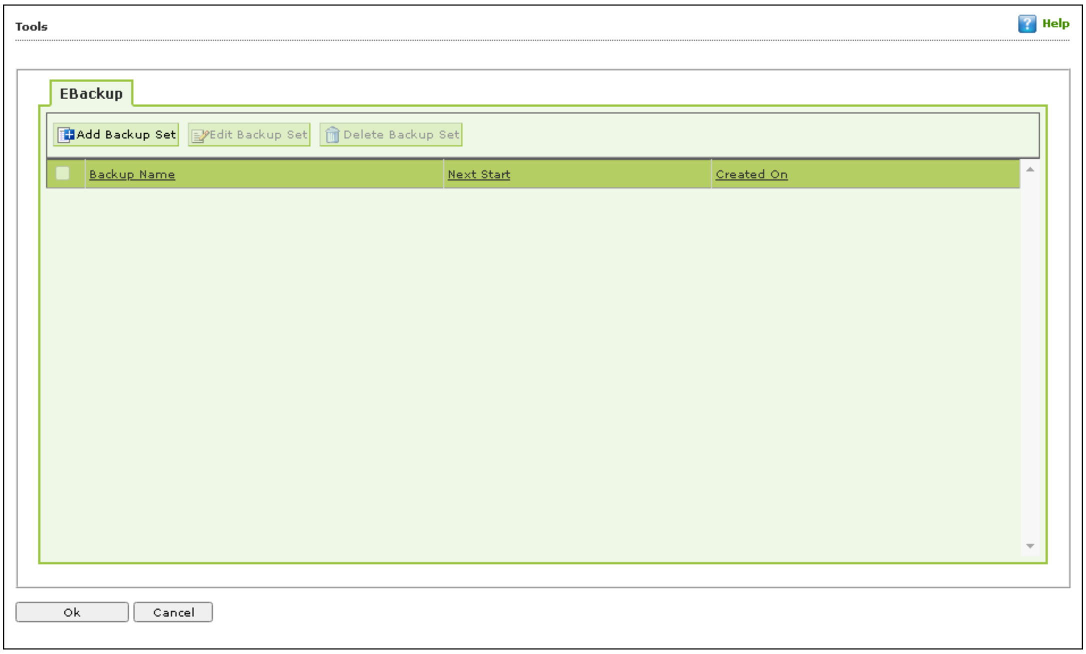
The updates can be downloaded automatically with **Automatic Download** option.

-OR-

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

Tools

The Tools lets you configure eBackup Settings.



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 feature 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.

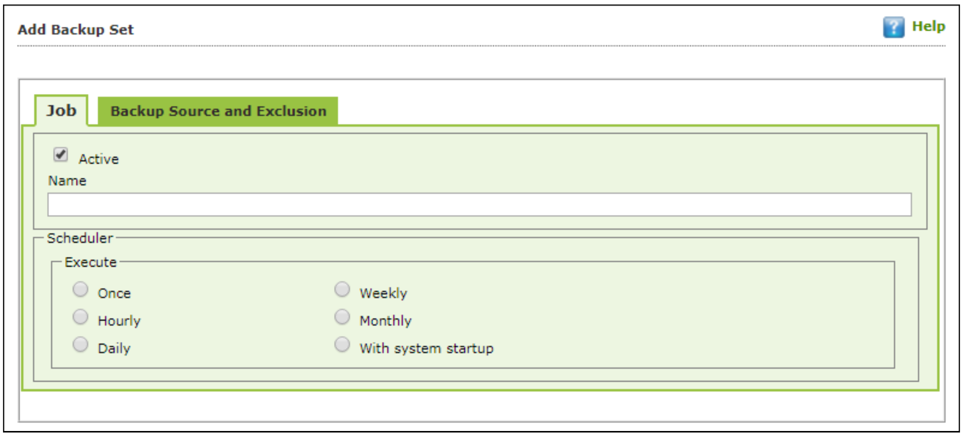
Add Backup Set

To create a Backup Set,

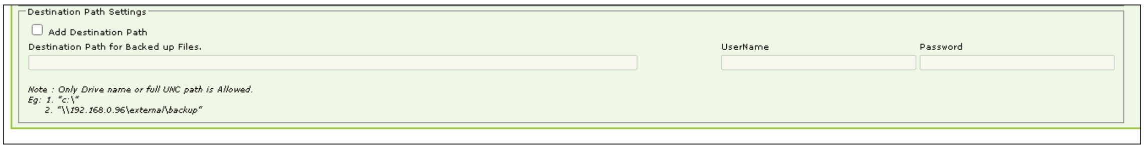
1. Go to **Managed Computers**.
2. Click **Policy Templates** > **New Template.**

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** check box and then click **Edit**.
4. Click **Add Backup Set**.
   Add Backup Set window appears.



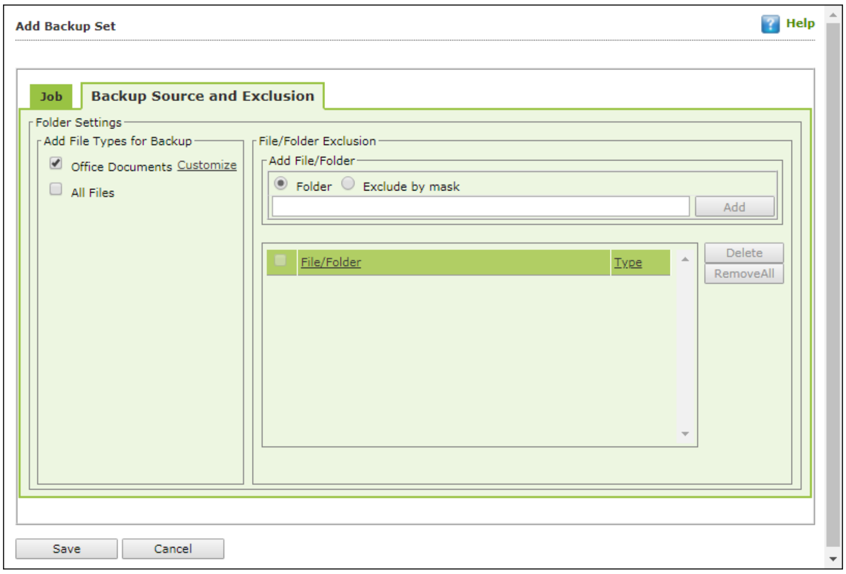
5. Enter a name.
6. In the Scheduler section, select a preferred interval for backup execution.
7. Administrator can save the backup set in the Network Drive by providing the path of the drive and Username and password for the network drive.


Destination Path Settings
☐ Add Destination Path
Destination Path for Backed up Files.
UserName
Password

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

NOTE	Network storage of 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. 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.

8. Click **Backup Source and Exclusion** tab.



Add Backup Set

Help

Job | Backup Source and Exclusion

Folder Settings

Add File Types for Backup

☑ Office Documents Customize

□ All Files

File/Folder Exclusion

Add File/Folder

● Folder ○ Exclude by mask

Add

□ File/Folder | Type

Delete

RemoveAll

Save | Cancel

9. Select the type of files for backup. By default, Office Documents option is selected.
10. Under the File/Folder Exclusion section, you can exclude a specific folder or a file format from getting backed up.
11. 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,

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.

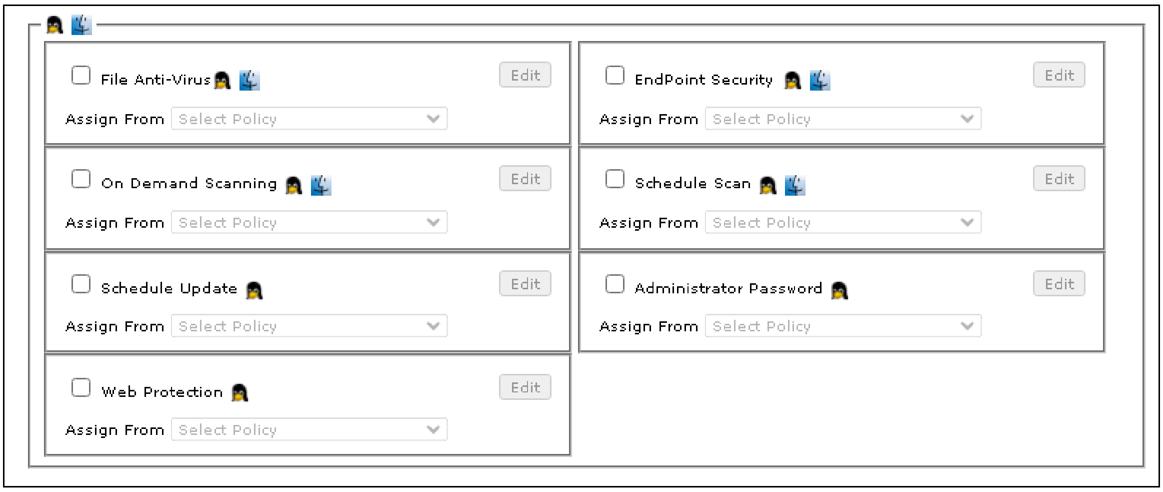
Delete Backup Set

To delete a Backup Set,

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 File Anti-Virus, Endpoint Security, On Demand scanning and Schedule Scan module for Linux and Mac computers connected to the network. Click **Edit** to configure the eScan module settings for computers with respective operating systems.



□ File Anti-Virus — Edit
Assign From: Select Policy

□ EndPoint Security — Edit
Assign From: Select Policy

□ On Demand Scanning — Edit
Assign From: Select Policy

□ Schedule Scan — Edit
Assign From: Select Policy

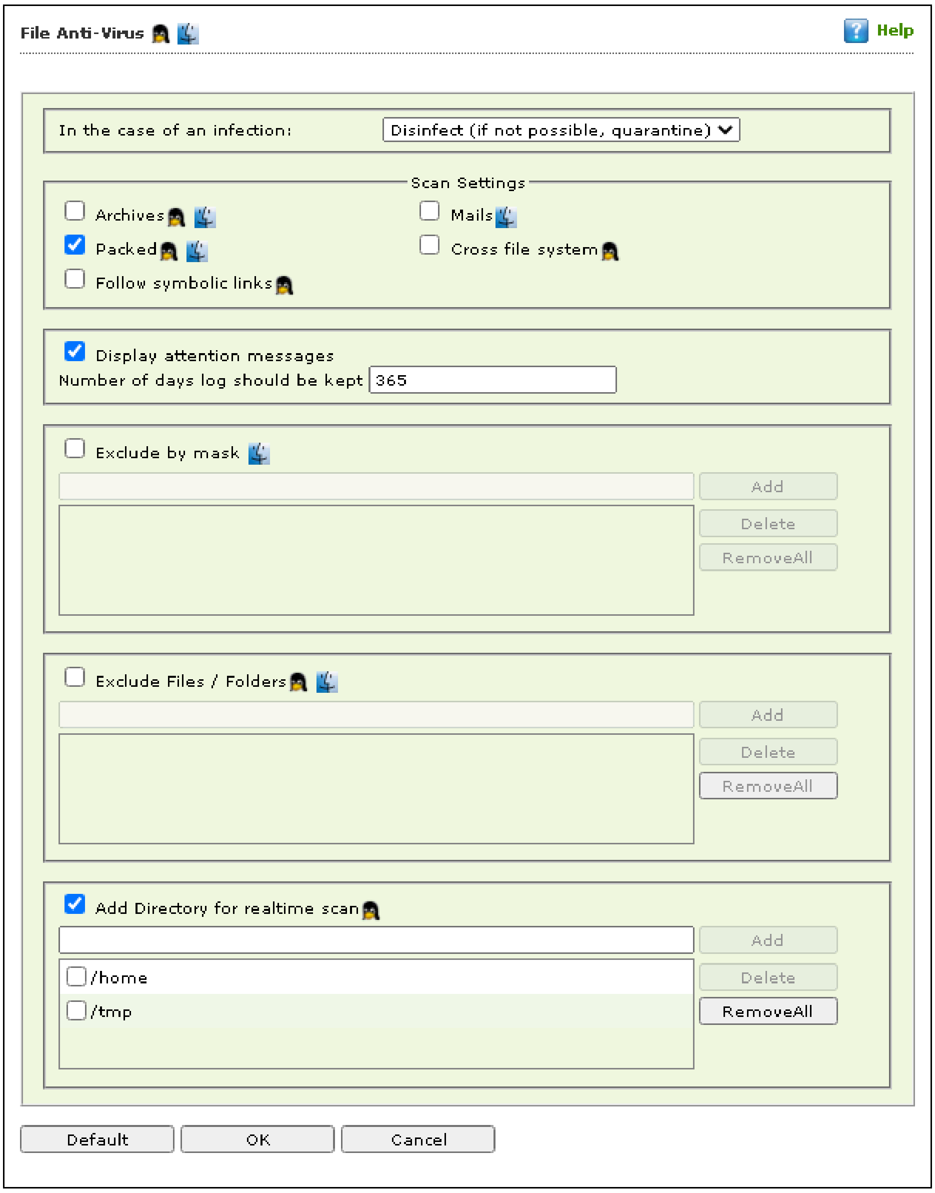
□ Schedule Update — Edit
Assign From: Select Policy

□ Administrator Password — Edit
Assign From: Select Policy

□ Web Protection — Edit
Assign From: Select Policy

NOTE	Icons next to every module displays that the settings are valid for the respective operating systems only. 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.

File Anti-Virus



File Anti-Virus

In the case of an infection: Disinfect (if not possible, quarantine)

Scan Settings

☐ Archives
☑ Packed
☐ Follow symbolic links
☐ Mails
☐ Cross file system

☑ Display attention messages

Number of days log should be kept 365

☐ Exclude by mask

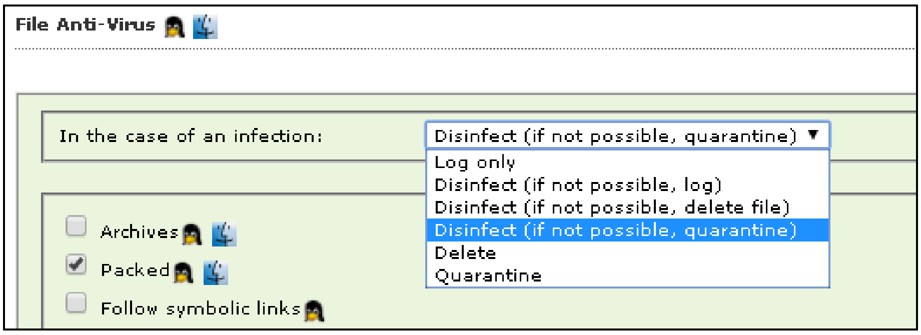
☐ Exclude Files / Folders

☑ Add Directory for realtime scan

☐ /home
☐ /tmp

Actions in case of infection [Drop-down]

It displays a list of actions eScan should take, in case of virus detection.



File Anti-Virus

In the case of an infection: Disinfect (if not possible, quarantine)

Log only
Disinfect (if not possible, log)
Disinfect (if not possible, delete file)
Disinfect (if not possible, quarantine)
Delete
Quarantine

☐ Archives
☑ Packed
☐ Follow symbolic links

By default, Disinfect (if not possible, quarantine file) option is selected. Following are the types of actions:

- **Log Only:** This option indicates or alerts the user about the infection detected (No Action is taken; only logs are maintained).
- **Disinfect (if not possible, log):** This option tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** This option tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, quarantine file):** This option tries to disinfect and if disinfection is not possible it quarantines the infected object.
- **Delete:** This option deletes the infected object.
- **Quarantine:** This option quarantines the infected object.

Scan Settings

Mails - It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.

Archives - It indicates the archived files, such as zip, rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.

Packed - It indicates the compressed executable. Select this check box if you want eScan real-time protection to scan packed files.

Cross File System that facilitates scanning of files over cross-file systems.

Follow Symbolic Links: scans the files following the symbolic links.

Exclude by Mask (file types) - Select this option if you want eScan real-time protection to exclude specific file extensions.

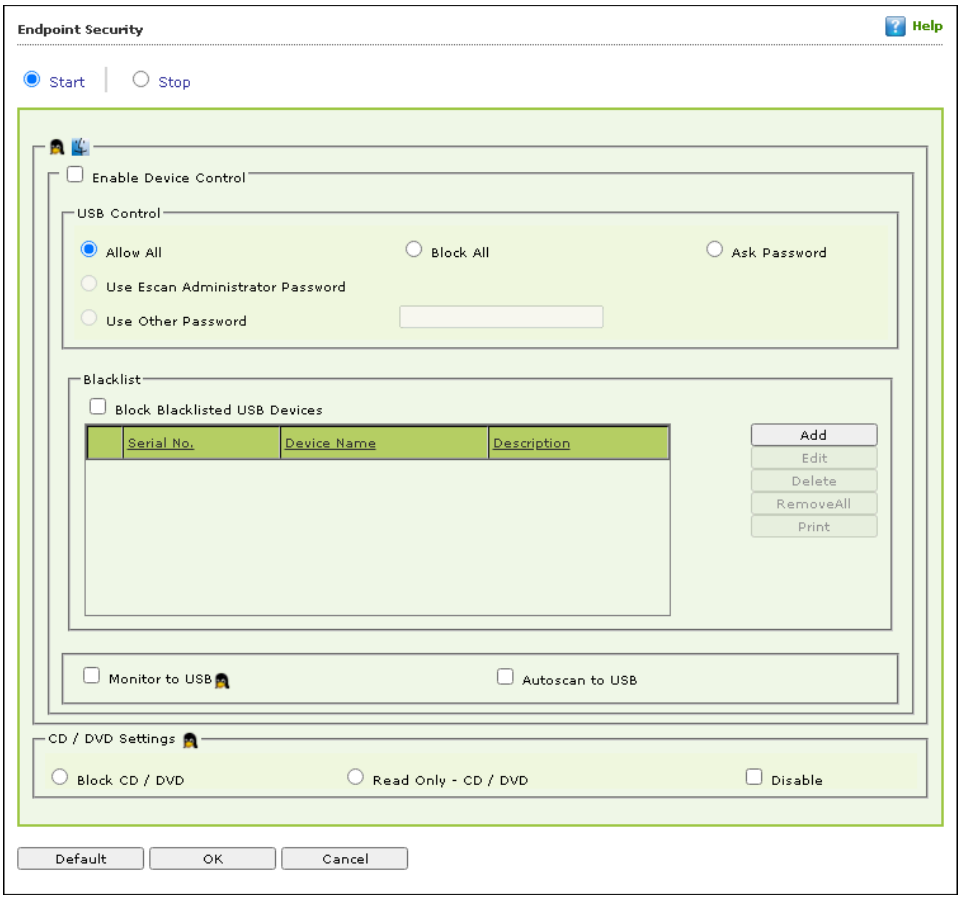
Exclude Folders and files - Select this option if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required.

Add Directory for Real-Time Scan: If you want eScan to perform real-time scan on any of the directories add them in this list.

You can restore default eScan settings by clicking **Default**.

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.



Endpoint Security

● Start | ○ Stop

☐ Enable Device Control

USB Control

● Allow All ○ Block All ○ Ask Password

○ Use Escan Administrator Password

○ Use Other Password

Blacklist

☐ Block Blacklisted USB Devices

Serial No.	Device Name	Description

☐ Monitor to USB ☐ Autoscan to USB

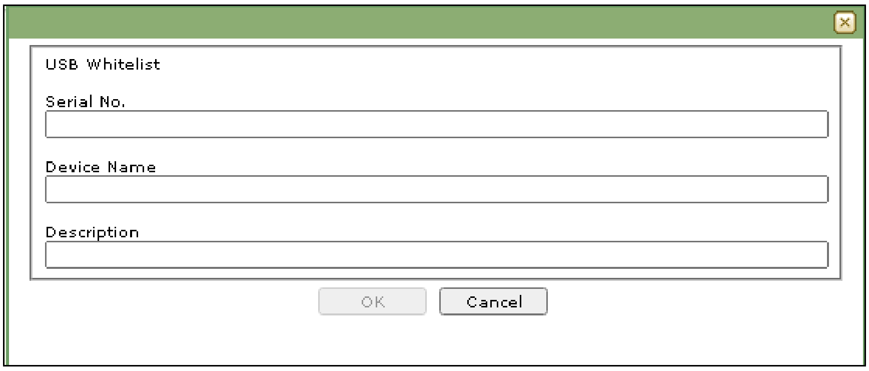
CD / DVD Settings

○ Block CD / DVD ○ Read Only - CD / DVD ☐ Disable

Enable Device Control: Select this check box 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 let's you to add USB devices to the blacklist. You can add, delete, modify using the following options:
    - **Add:** Click **Add** to add the USB serial number, name, and description of the USB devices. The USB will be added to the list.



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 check box to monitor all the connected USB devices connected to the endpoints.
- **Autoscan to USB**: Select this option to auto-scan all the USB devices connected to the endpoints.

CD/DVD Settings

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

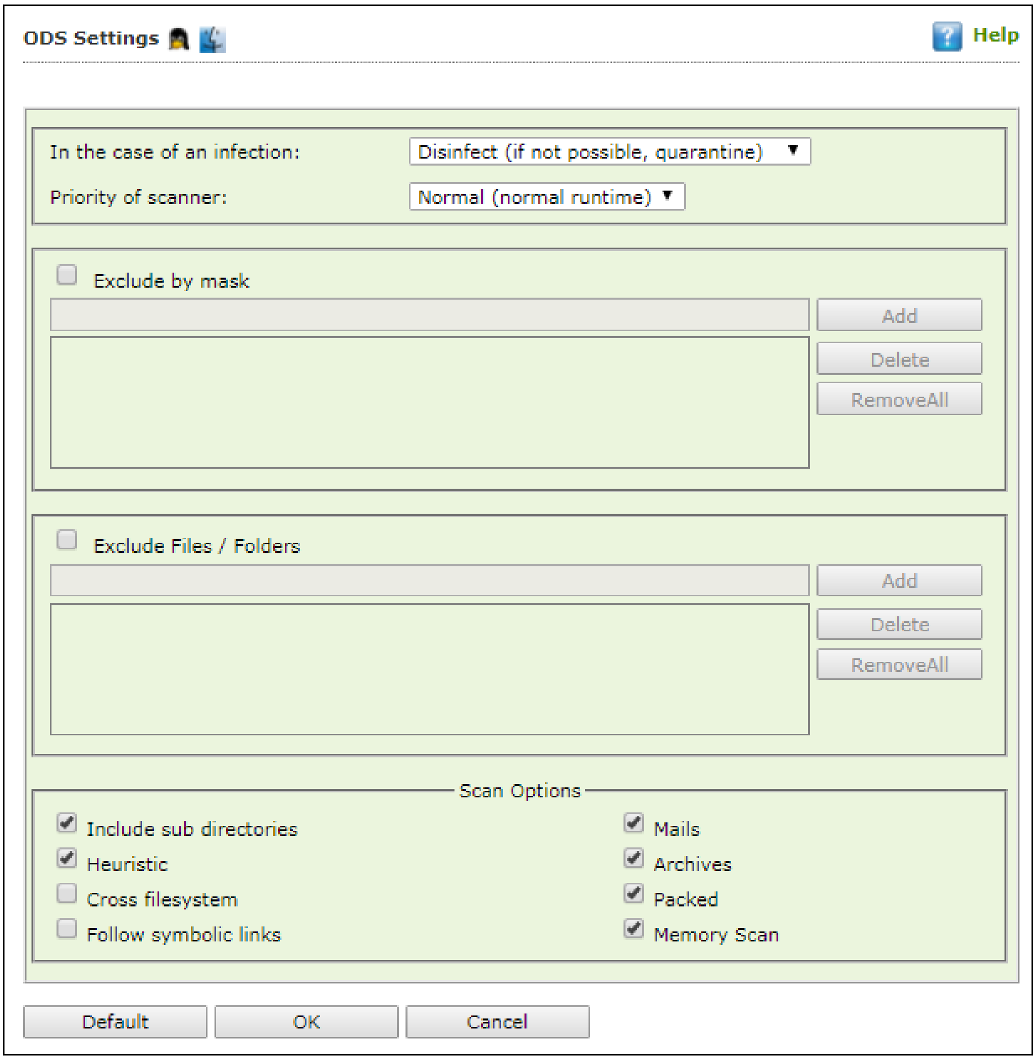
- **Block CD/DVD:** This option block all the CD and DVD.
- **Read Only CD/DVD:** This option allows user to only read the content CD and DVD.
- **Disable:** This option disables all the CD and DVD.

Default

This button resets all the setting to default.

ODS On Demand Scanning

With ODS Settings you can define actions in case of infection, you can also define list of files by mask, Files or Folders to be excluded from Scanning. It also lets you configure settings for various other Scan options like Include Sub directories, Mails, Archives Heuristic Scanning etc. by selecting respective options.



ODS Settings

In the case of an infection: Disinfect (if not possible, quarantine)

Priority of scanner: Normal (normal runtime)

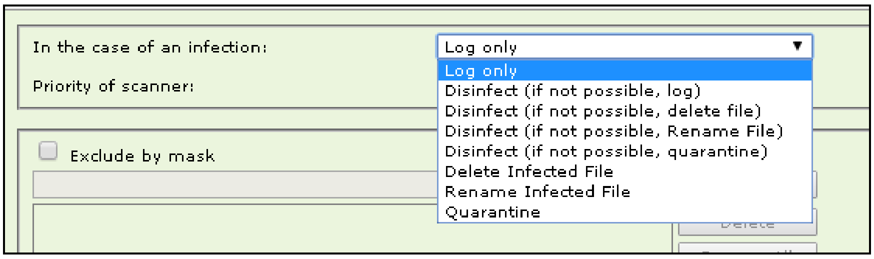
□ Exclude by mask

□ Exclude Files / Folders

Scan Options

- ☑ Include sub directories
- ☑ Heuristic
- □ Cross filesystem
- □ Follow symbolic links
- ☑ Mails
- ☑ Archives
- ☑ Packed
- ☑ Memory Scan

Actions in case of infection [Drop-down]



In the case of an infection: Log only

Priority of scanner:

□ Exclude by mask

Log only
Disinfect (if not possible, log)
Disinfect (if not possible, delete file)
Disinfect (if not possible, Rename File)
Disinfect (if not possible, quarantine)
Delete Infected File
Rename Infected File
Quarantine

It indicates a type of action which you want eScan real-time protection to take, in case of virus detection.

By default, Disinfect (if not possible, quarantine file) option is selected. Following actions can be taken:

Log Only: It indicates or alerts the user about the infection detected.

Disinfect (if not possible, log): It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.

Disinfect (if not possible, delete file): It tries to disinfect and if disinfection is not possible it deletes the infected object.

Disinfect (if not possible, Rename file): It tries to disinfect and if disinfection is not possible it renames the infected object.

Disinfect (if not possible, quarantine): It tries to disinfect and if disinfection is not possible it quarantines the infected object.

Delete Infected File: It directly deletes the infected object.

Rename Infected File: It directly renames the infected object.

Quarantine: It directly quarantines the infected object.

- **Priority of Scanner** – You can select the priority of scanning as High, Normal or Low
- **High** – Has a short runtime.
- **Normal** – Has a normal runtime.
- **Low** – Has a long runtime.
- **Exclude by Mask** – Select this check box if you want eScan real-time protection to exclude specific files, and Remove any or all Added Files whenever required.
- **Exclude Folders and Files** – Select this check box if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required during On Demand Scanning.

Scan options

Mails – It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.

Archives – It indicates the archived files, such as zip, rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.

Packed – It indicates the compressed executable.

Memory Scan – This option ensures eScan scans the system's memory for any infection from malwares.

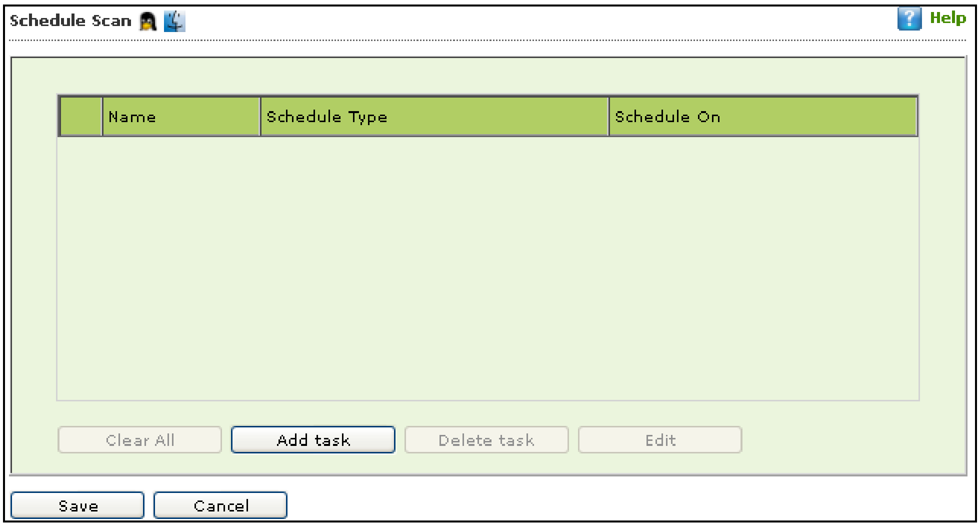
Include Sub Directories – This option ensures eScan scans all the sub directories recursively under every directory and not only the first level of directories.

Heuristic – Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application.

Cross File System that facilitates scanning of files over cross-file systems.

Follow Symbolic Links: scans the files following the symbolic links.
You can restore default eScan settings by clicking **Default**.

Schedule Scan



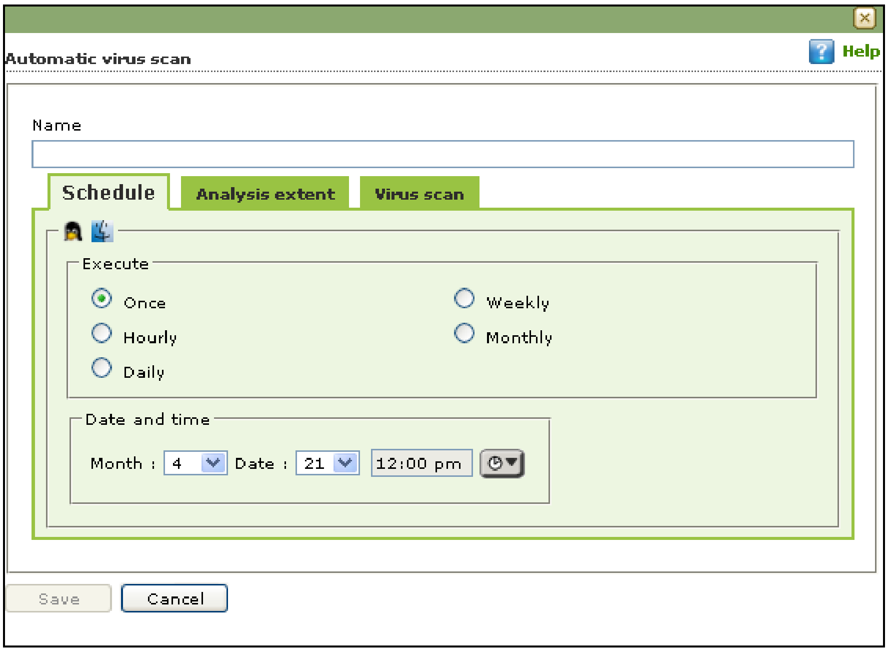
	Name	Schedule Type	Schedule On

It lets you add a task for scheduling a scan.

Adding a task - It lets you schedule and define options for Analysis extent and the files or folders to be scanned.

Automatic Virus Scan

Schedule



Name

Execute

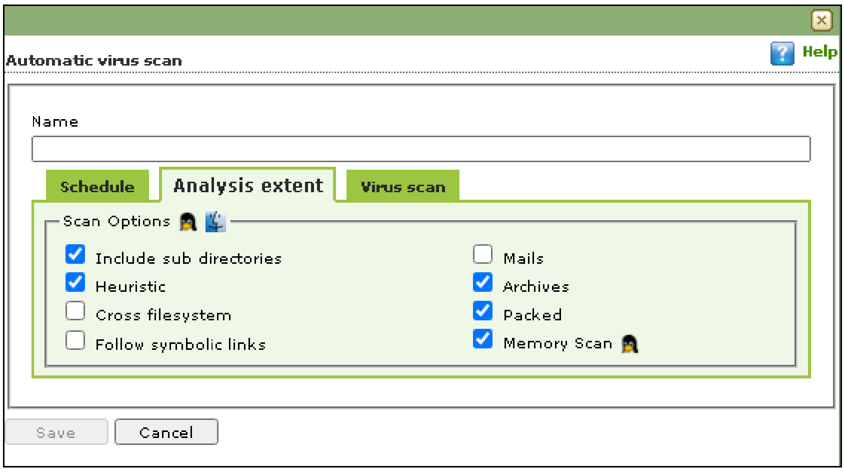
● Once
○ Hourly
○ Daily
○ Weekly
○ Monthly

Date and time

Month : 4 Date : 21 12:00 pm

Using this tab you can define the task name and schedule it as desired. You can schedule once, Weekly basis, every hour, monthly or daily. It also lets you schedule virus scan at desired date and time.

Analysis Extent



Automatic virus scan

Name

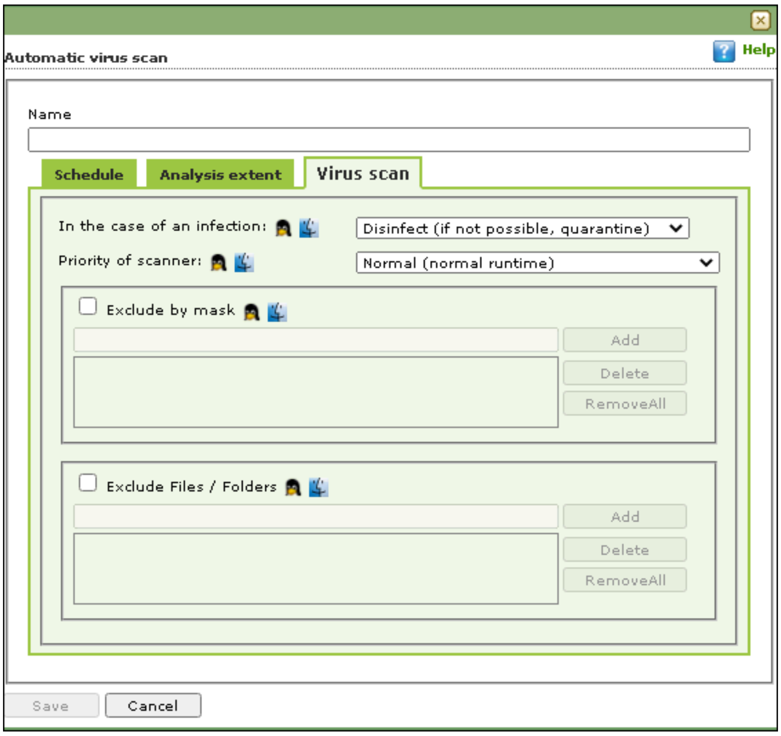
Scan Options

☑ Include sub directories
☑ Heuristic
☐ Cross filesystem
☐ Follow symbolic links
☐ Mails
☑ Archives
☑ Packed
☑ Memory Scan

Using this tab you can define the scan options for Linux and Mac computers connected to the network.

- **Include sub Directories** – This option lets you include sub directories while conducting an automatic scan.
- **Heuristic Scan** – Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application.
- **Cross File System** that facilitates scanning of files over cross-file systems.
- **Symbolic Link Scanning** scans the files following the symbolic links.
- **Mails -** It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.
- **Archives -** It indicates the archived files, such as zip, rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.
- **Packed -** It indicates the compressed executable. Select this check box if you want eScan real-time protection to scan packed files.

Virus Scan



Automatic virus scan

Name

In the case of an infection: Disinfect (if not possible, quarantine)

Priority of scanner: Normal (normal runtime)

☐ Exclude by mask

☐ Exclude Files / Folders

Actions in case of Infection [Drop-down]
It displays a list of actions eScan should take, in case of virus detection. By default, Disinfect (if not possible, quarantine file) option is selected. Following are the types of actions:

Log Only: It indicates or alerts the user about the infection detected.

Disinfect (if not possible, log): It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.

Disinfect (if not possible, delete file): It tries to disinfect and if disinfection is not possible it deletes the infected object.

Disinfect (if not possible, quarantine file): It tries to disinfect and if disinfection is not possible it quarantines the infected object.

Delete: Infected objects are deleted with this option.

Quarantine: Infected objects are quarantined with this option.

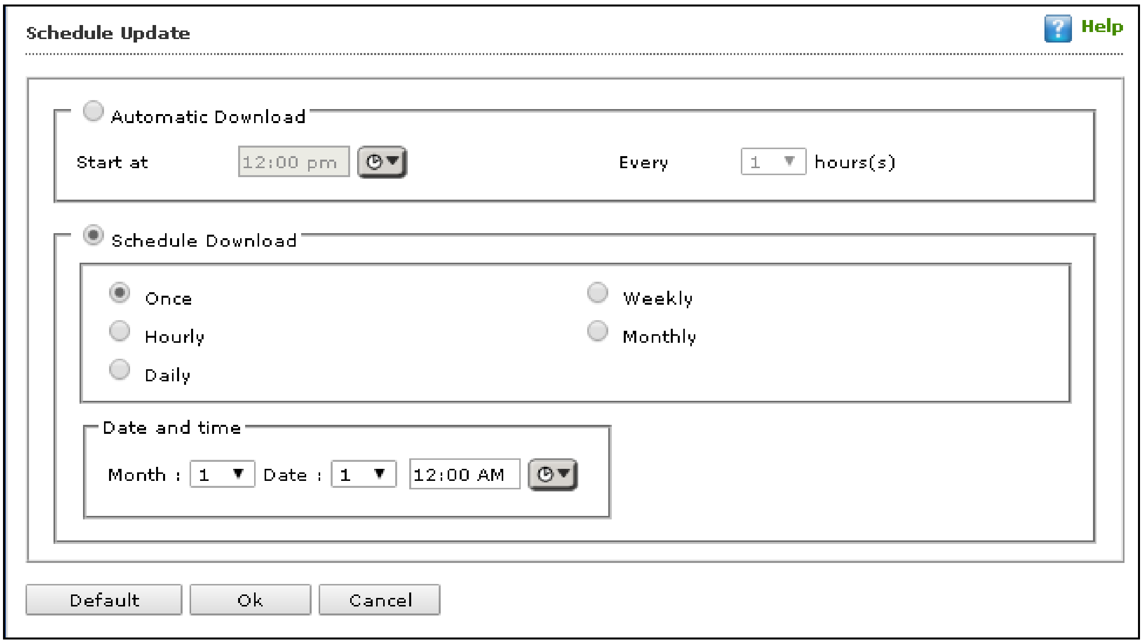
Exclude file types (Mask) - Select this check box if you want eScan real-time protection to exclude specific files, and then add the directories and files that you want to exclude by clicking **Add**. eScan lets you Remove any or all Added Files whenever required.

Exclude Folders and files - Select this check box if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required.

Schedule Update

This module lets you schedule the updates for Linux computers.

- Automatic Download
- Schedule Download



Schedule Update

○ Automatic Download

Start at 12:00 pm

Every 1 hours(s)

● Schedule Download

● Once

○ Hourly

○ Daily

○ Weekly

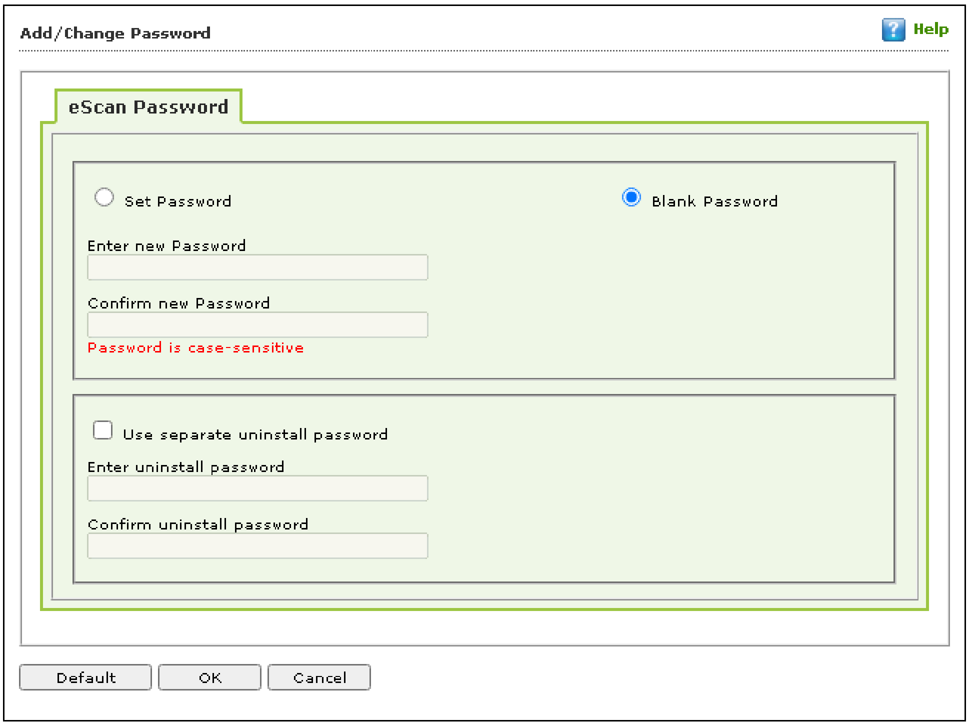
○ Monthly

Date and time

Month : 1 Date : 1 12:00 AM

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

eScan 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

To Add/Change eScan administrator 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.

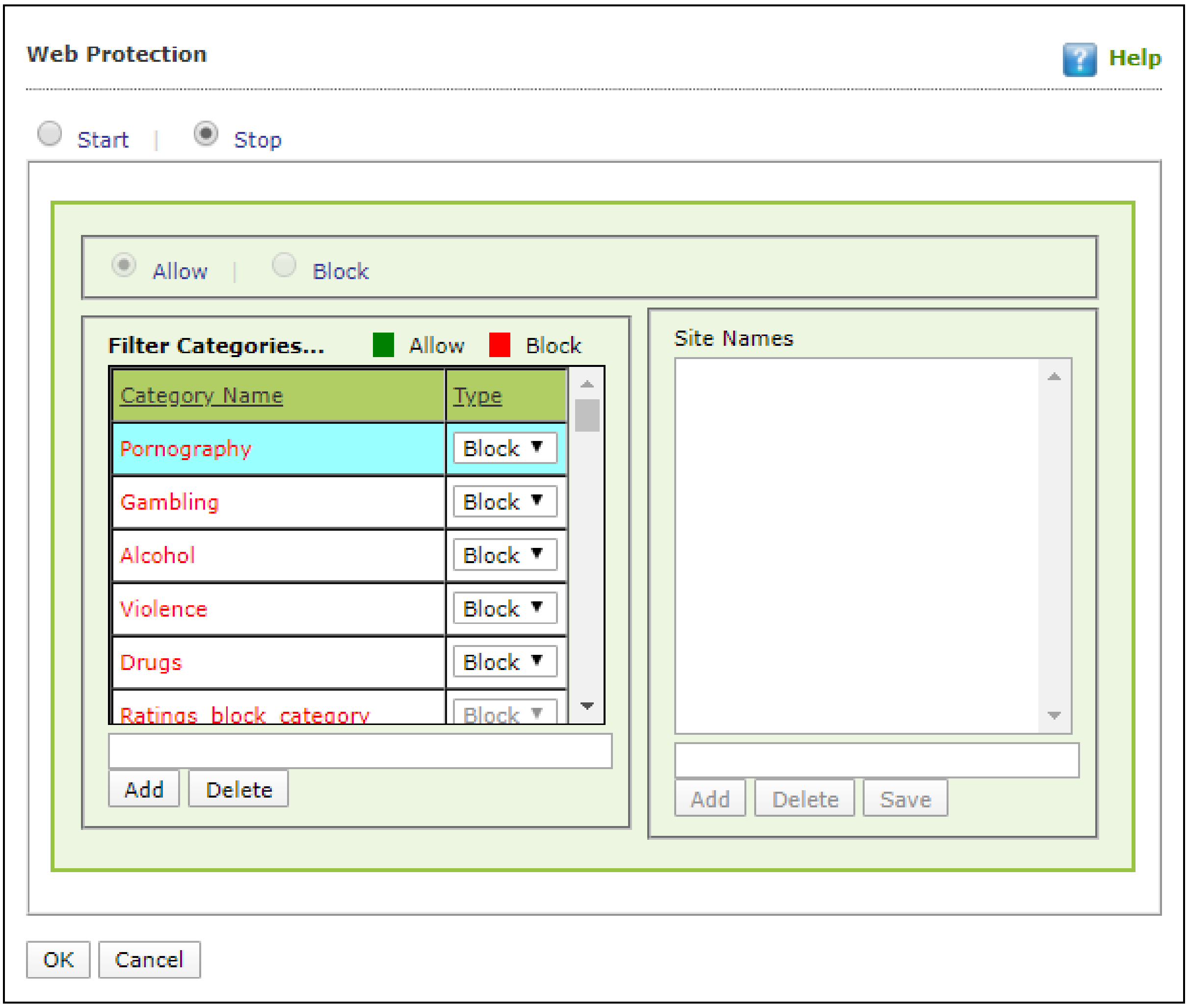
After filling all fields, click **OK**. The Password will be saved.

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.



Web Protection

○ Start | ● Stop

● Allow | ○ Block

Filter Categories... 🟩 Allow 🟥 Block

Category Name	Type
Pornography	Block
Gambling	Block
Alcohol	Block
Violence	Block
Drugs	Block
Ratings_block_category	Block

Site Names

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.

Filter Options

This section includes the **Add sites rejected by the filter to Block category check box**. Select this option if you want eScan to add websites that are denied access to the Block category database automatically.

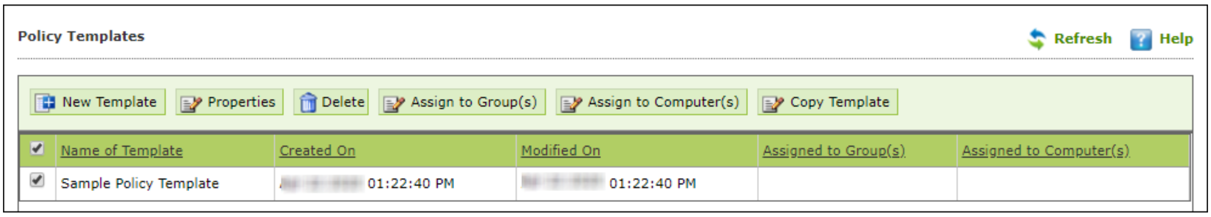
Assigning Policy Template to a group

There are two ways to assign the policy template to group.

Method 1

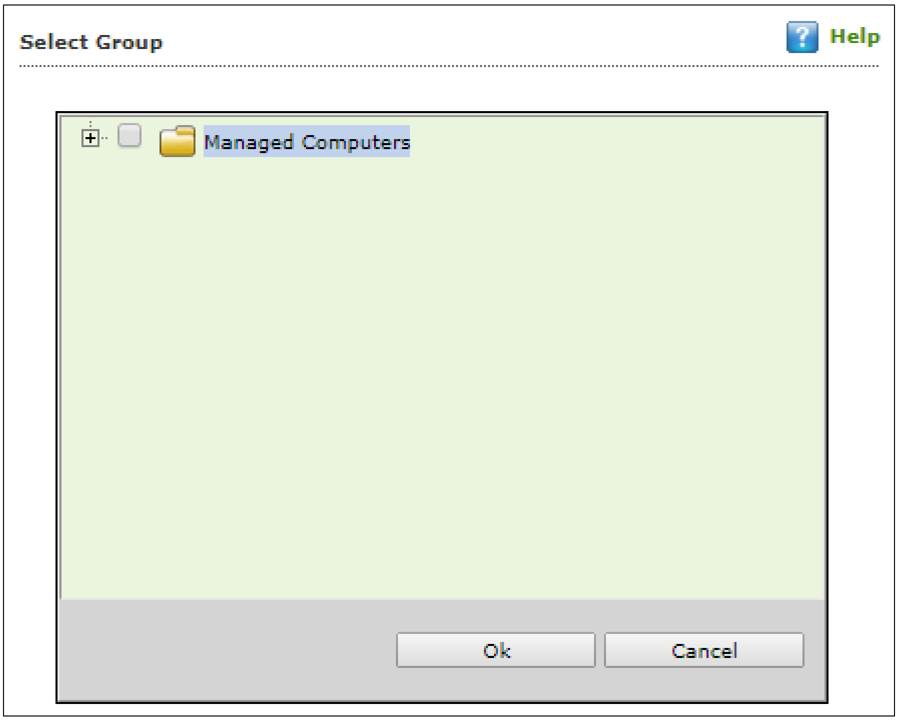
To assign a Policy to a group,

1. In the Managed Computers screen, click **Policy Templates**.
   Policy Templates window appears.
2. In the **Policy Templates** window, select a policy template.



☑	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	Sample Policy Template	[redacted] 01:22:40 PM	[redacted] 01:22:40 PM		

3. Click **Assign to Group(s)**.
   Select Group window appears.

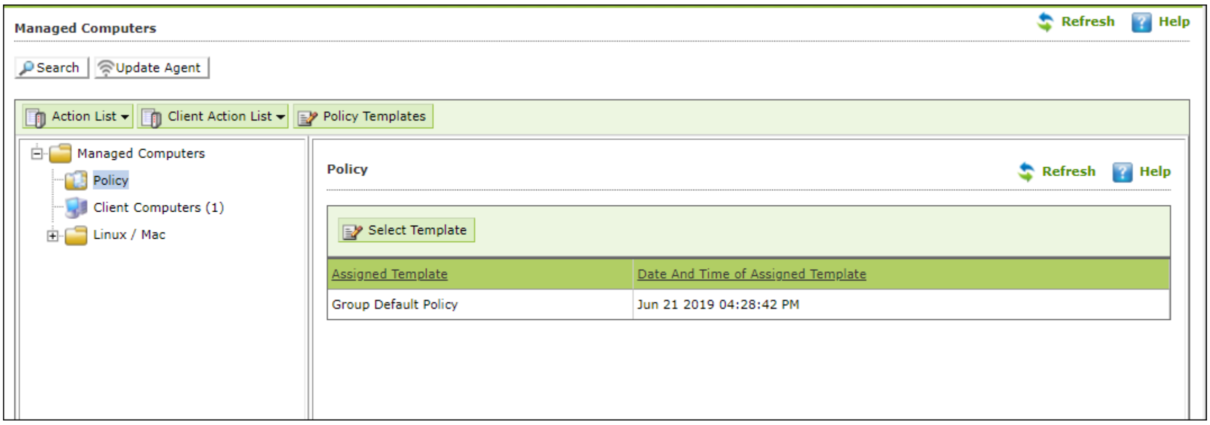


4. Select the group(s) and then click **OK**.
   The policy will be assigned to the selected group(s).

Method 2

To assign a Policy to the group:

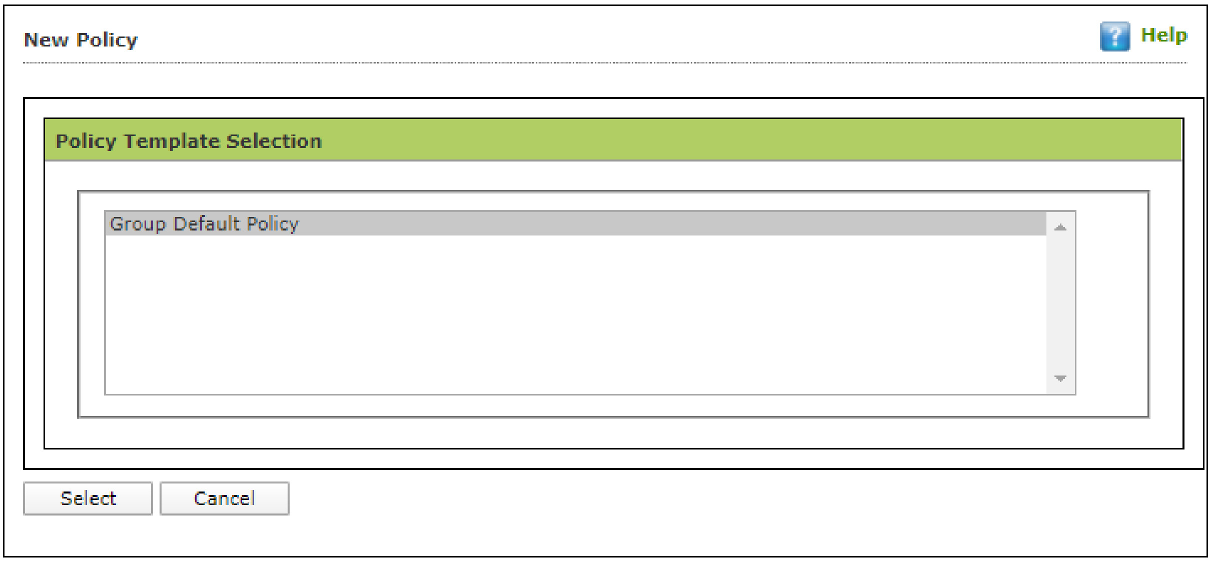
1. In the Managed Computers folder tree, select a group.
2. Under the group, click **Policy**.
   Policy pane appears on the right side.



Managed Computers

Assigned Template	Date And Time of Assigned Template
Group Default Policy	Jun 21 2019 04:28:42 PM

3. In the right pane, click **Select Template**.
   New Policy window appears.



New Policy

Policy Template Selection

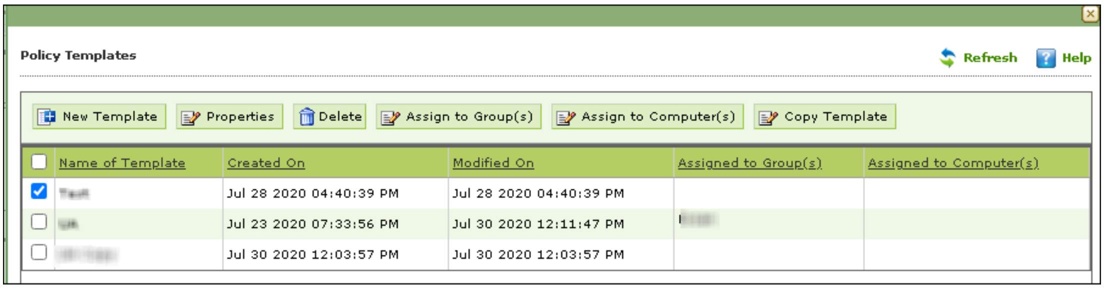
Group Default Policy

4. Select a policy template and then click **Select**.
   The default Policy Template for group will be saved and updated.

Assigning Policy Template to Computer(s)

To assign a policy template to computers,

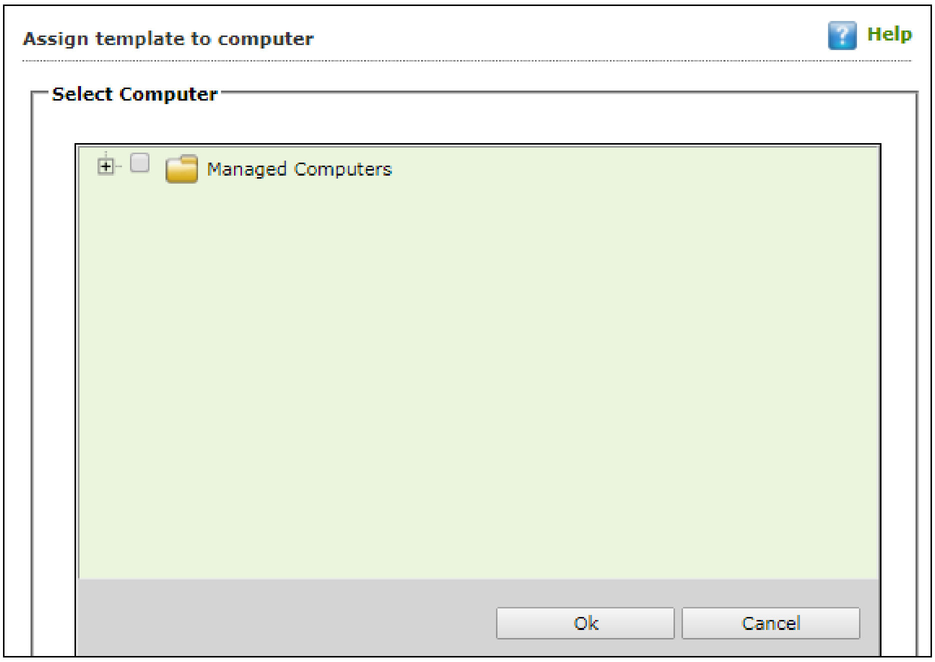
1. In the **Policy Templates** window, select a policy.



Policy Templates

□	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	Jul 28 2020 04:40:39 PM	Jul 28 2020 04:40:39 PM		
□	[redacted]	Jul 23 2020 07:33:56 PM	Jul 30 2020 12:11:47 PM	[redacted]	
□	[redacted]	Jul 30 2020 12:03:57 PM	Jul 30 2020 12:03:57 PM		

2. Click **Assign to Computer(s)**.
3. Assign Template to computer window appears.



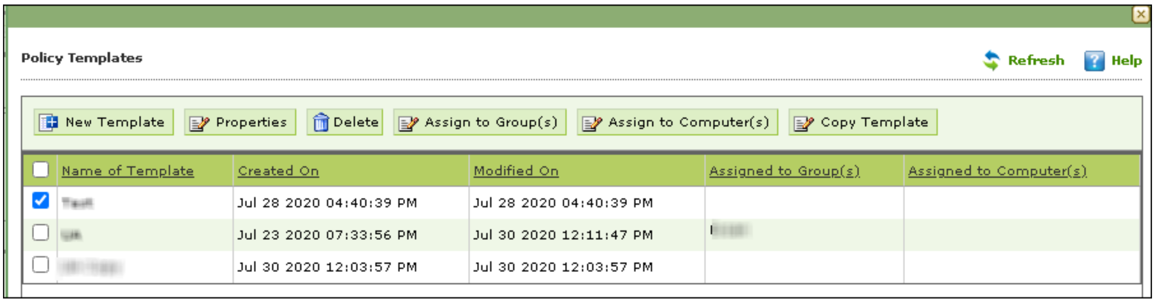
Assign template to computer

4. Click **Managed Computers**.
5. Select the computer(s) and then click **OK**.
   The policy template will be assigned to the selected computers.

Copy a Policy Template

To copy a Policy Template,

1. In the Policy Templates window, select a policy.

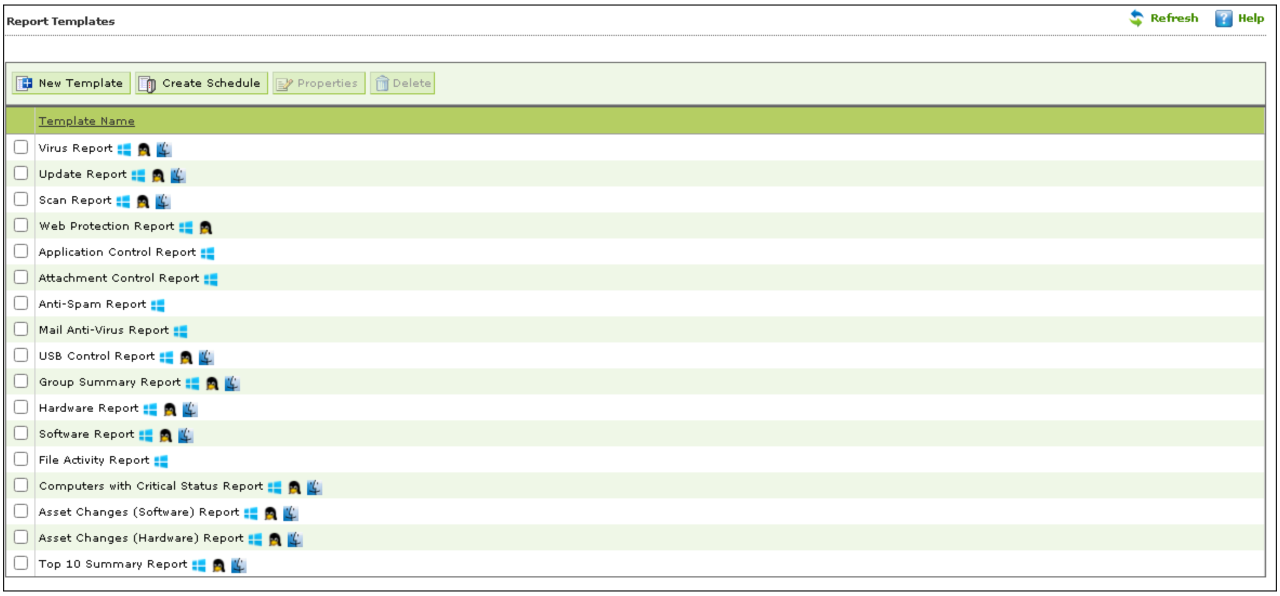


☐	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
☑	[redacted]	Jul 28 2020 04:40:39 PM	Jul 28 2020 04:40:39 PM		
☐	[redacted]	Jul 23 2020 07:33:56 PM	Jul 30 2020 12:11:47 PM	[redacted]	
☐	[redacted]	Jul 30 2020 12:03:57 PM	Jul 30 2020 12:03:57 PM		

3. Click **Copy Template**.
   New Template window appears displaying settings from the original template.
4. Enter a name for the template.
5. Make the necessary changes and then click **Save**.
   The template will be copied.

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

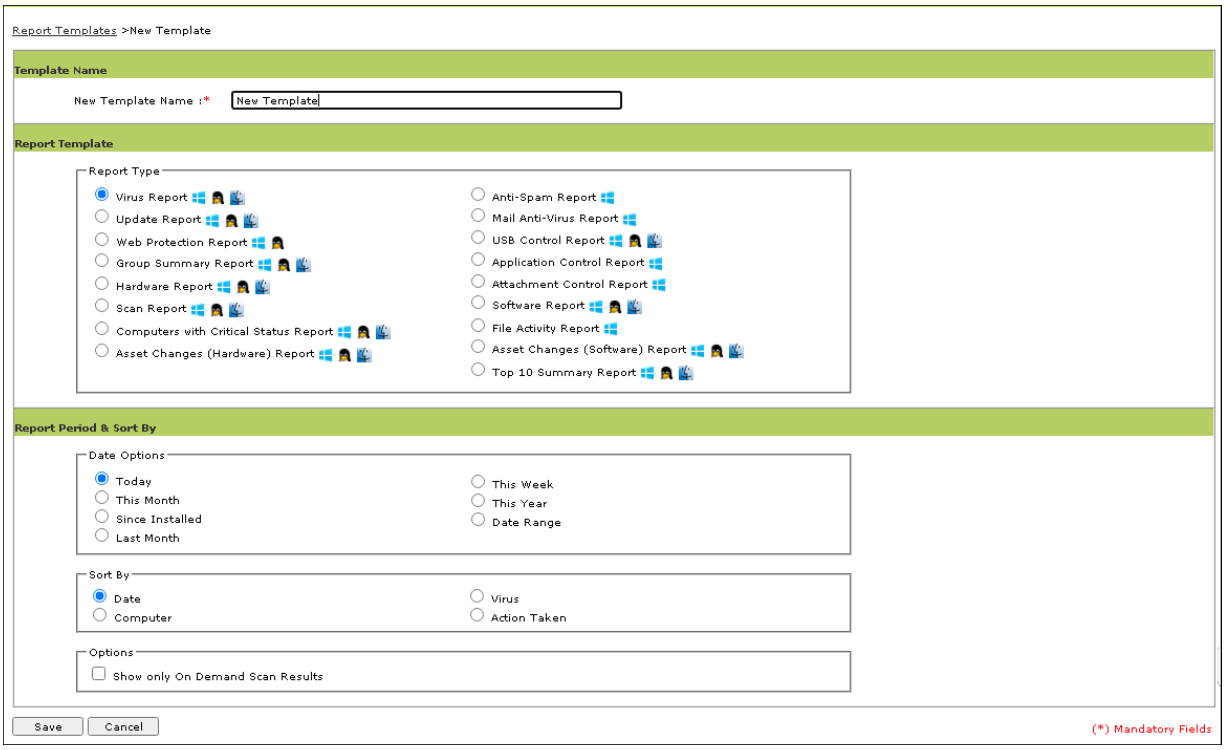
	Template Name
☐	Virus Report
☐	Update Report
☐	Scan Report
☐	Web Protection Report
☐	Application Control Report
☐	Attachment Control Report
☐	Anti-Spam Report
☐	Mail Anti-Virus Report
☐	USB Control Report
☐	Group Summary Report
☐	Hardware Report
☐	Software Report
☐	File Activity Report
☐	Computers with Critical Status Report
☐	Asset Changes (Software) Report
☐	Asset Changes (Hardware) Report
☐	Top 10 Summary 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.



Report Templates >New Template

Template Name

New Template Name :* New Template

Report Template

Report Type

● Virus Report	○ Anti-Spam Report
○ Update Report	○ Mail Anti-Virus Report
○ Web Protection Report	○ USB Control Report
○ Group Summary Report	○ Application Control Report
○ Hardware Report	○ Attachment Control Report
○ Scan Report	○ Software Report
○ Computers with Critical Status Report	○ File Activity Report
○ Asset Changes (Hardware) Report	○ Asset Changes (Software) Report
	○ Top 10 Summary Report

Report Period & Sort By

Date Options

● Today	○ This Week
○ This Month	○ This Year
○ Since Installed	○ Date Range
○ Last Month	

Sort By

● Date	○ Virus
○ Computer	○ Action Taken

Options

□ Show only On Demand Scan Results

3. Enter a name for the template.
4. Select a report enter.

   Depending upon the report enter, the additional setting varies.
5. After making the necessary selections/filling data, click **Save**.

   The template will be created according to your preferences.

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.

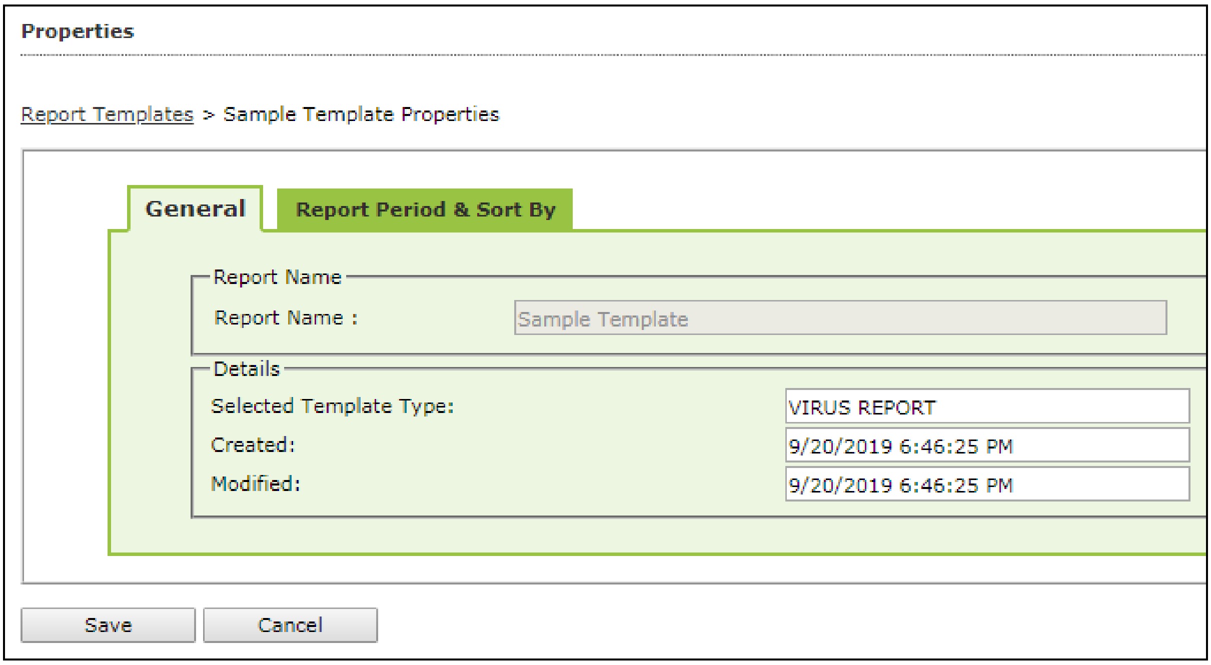
NOTE	Default Report Templates cannot be deleted.

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 > Sample Template Properties

Report Name

Report Name : Sample Template

Details

Selected Template Type: VIRUS REPORT

Created: 9/20/2019 6:46:25 PM

Modified: 9/20/2019 6:46:25 PM

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.

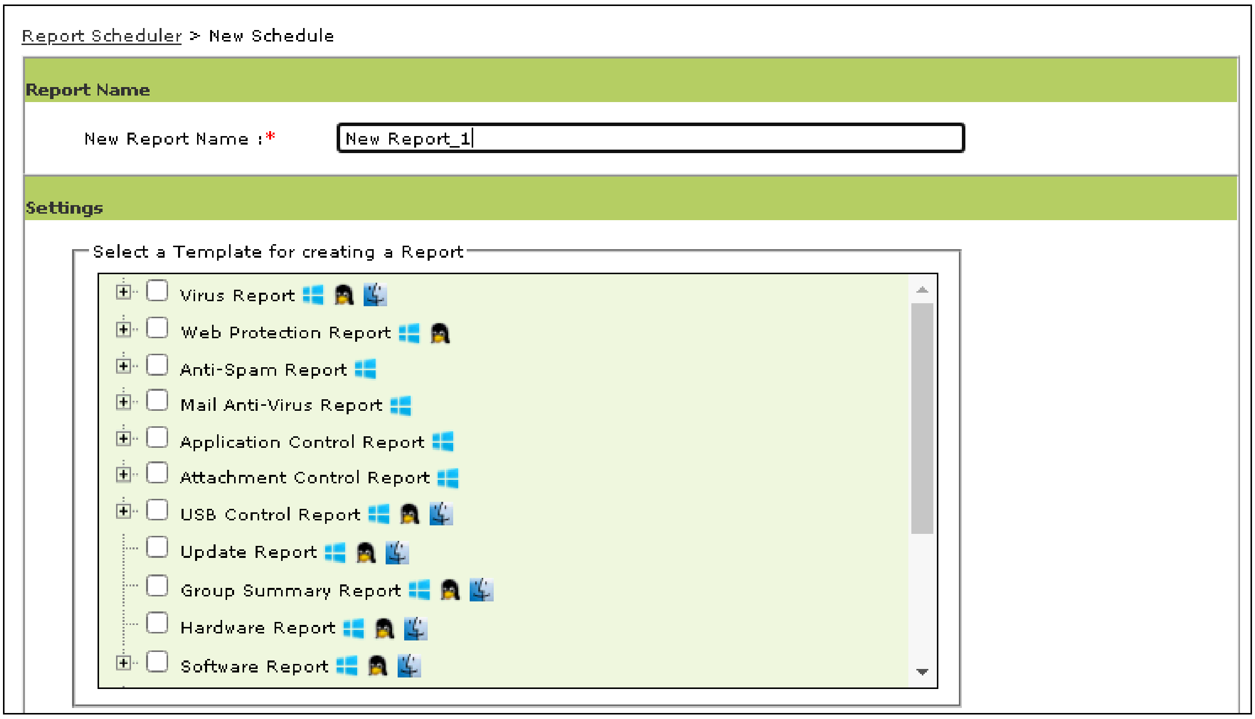
Report Scheduler

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

Create a Schedule

To create a Schedule,

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



Report Scheduler > New Schedule

Report Name

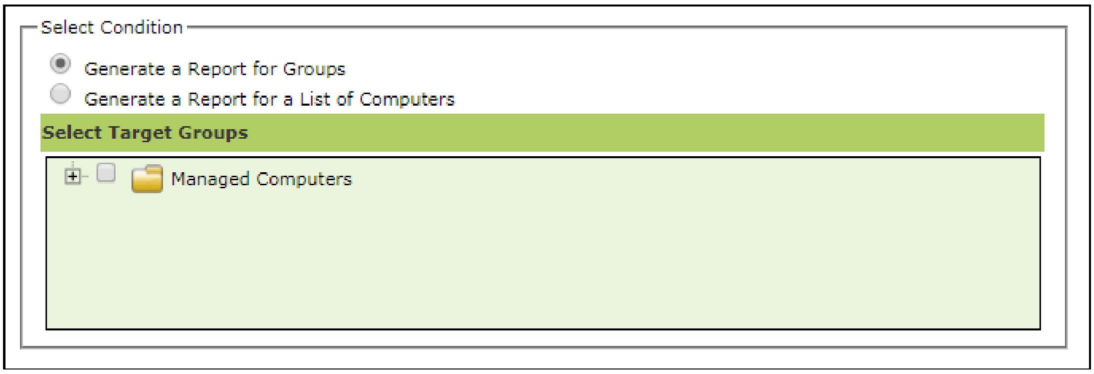
New Report Name :* New Report_1

Settings

Select a Template for creating a Report

- □ Virus Report
- □ Web Protection Report
- □ Anti-Spam Report
- □ Mail Anti-Virus Report
- □ Application Control Report
- □ Attachment Control Report
- □ USB Control Report
- □ Update Report
- □ Group Summary Report
- □ Hardware Report
- □ Software Report

2. In the Settings section, select preferred templates.
3. In the Select Condition section, select a condition for groups or specific computers.



Select Condition

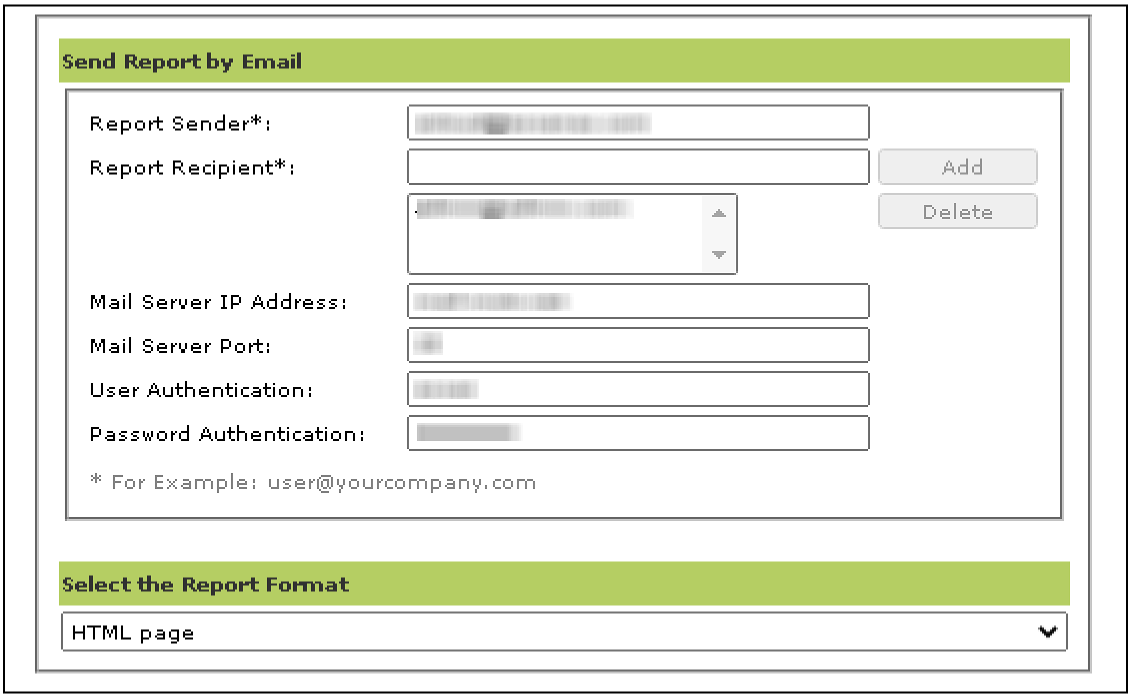
● Generate a Report for Groups

○ Generate a Report for a List of Computers

Select Target Groups

□ Managed Computers

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



Send Report by Email

Report Sender*:

Report Recipient*:

Mail Server IP Address:

Mail Server Port:

User Authentication:

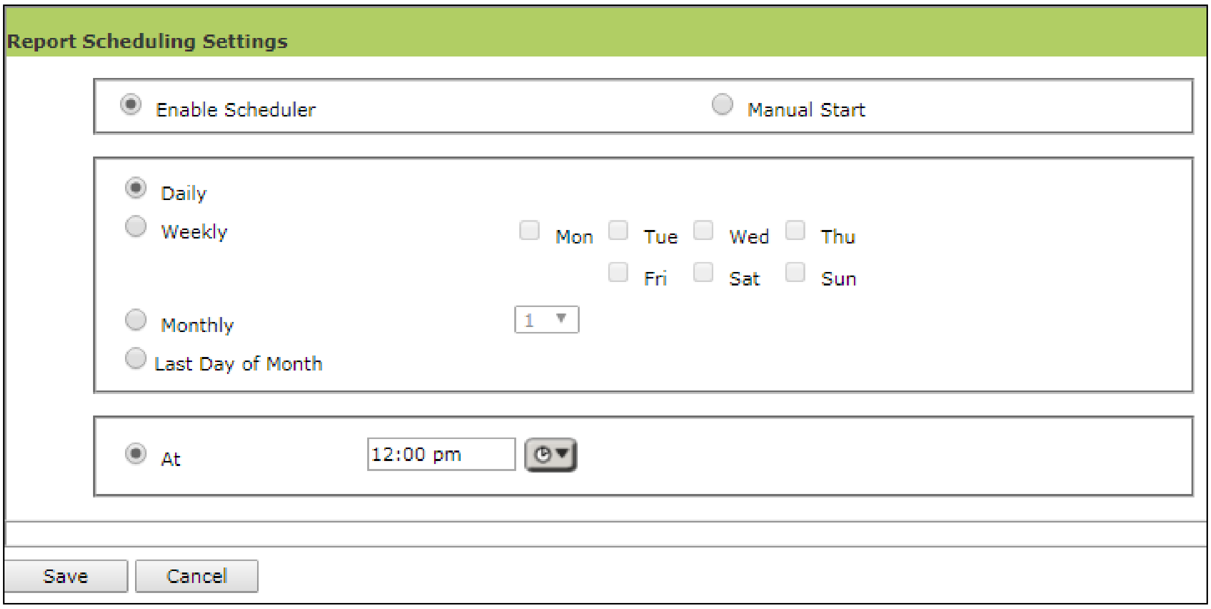
Password Authentication:

* For Example: user@yourcompany.com

Select the Report Format

HTML page

5. Select the preferred report format.
6. 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

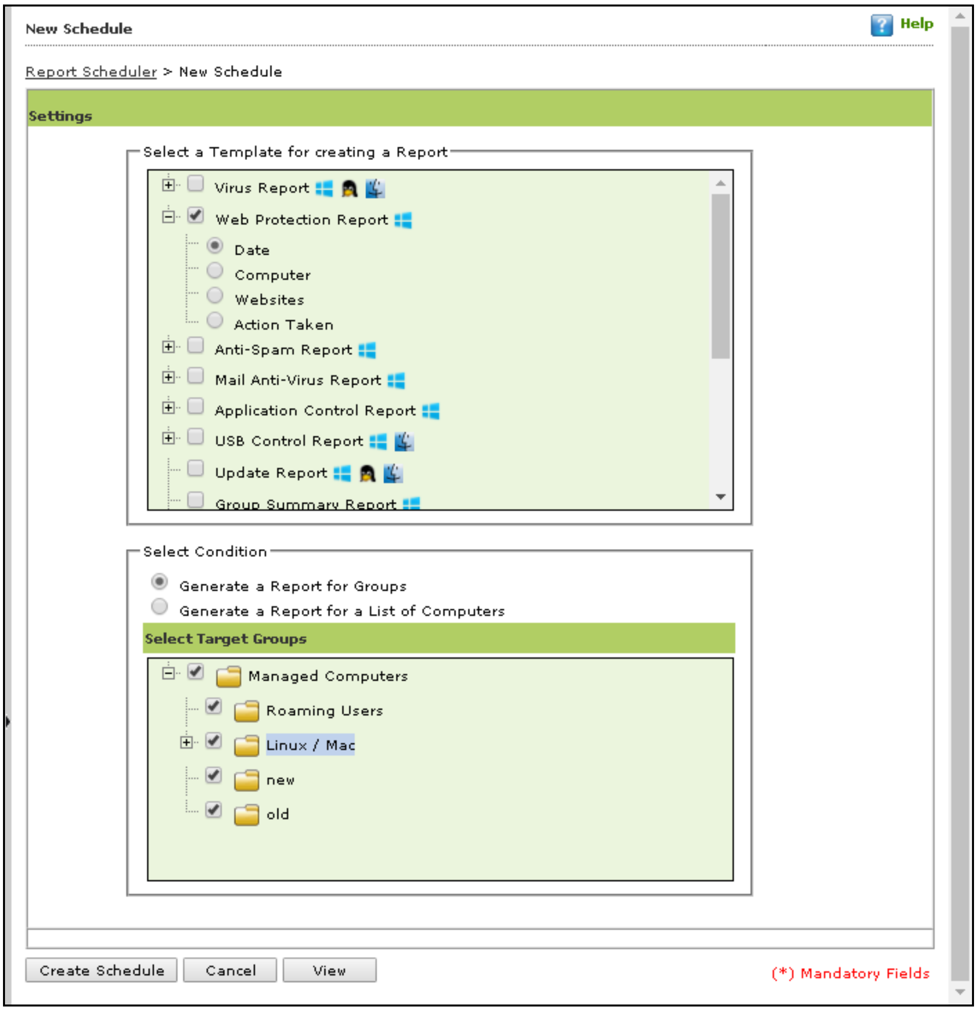
● At 12:00 pm

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

View Reports on Demand

To view a report or a set of reports immediately,

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



New Schedule

Help

Report Scheduler > New Schedule

Settings

Select a Template for creating a Report

- □ Virus Report
- ☑ Web Protection Report
  - ● Date
  - ○ Computer
  - ○ Websites
  - ○ Action Taken
- □ Anti-Spam Report
- □ Mail Anti-Virus Report
- □ Application Control Report
- □ USB Control Report
- □ Update Report
- □ Group Summary Report

Select Condition

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

Select Target Groups

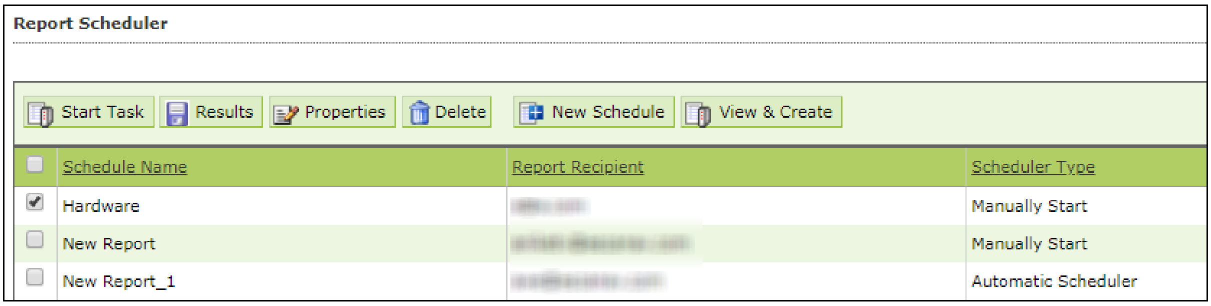
- ☑ Managed Computers
  - ☑ Roaming Users
  - ☑ Linux / Mac
  - ☑ new
  - ☑ old

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

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

Managing Existing Schedules

The Report Scheduler module lets you manage the existing schedules.



Report Scheduler

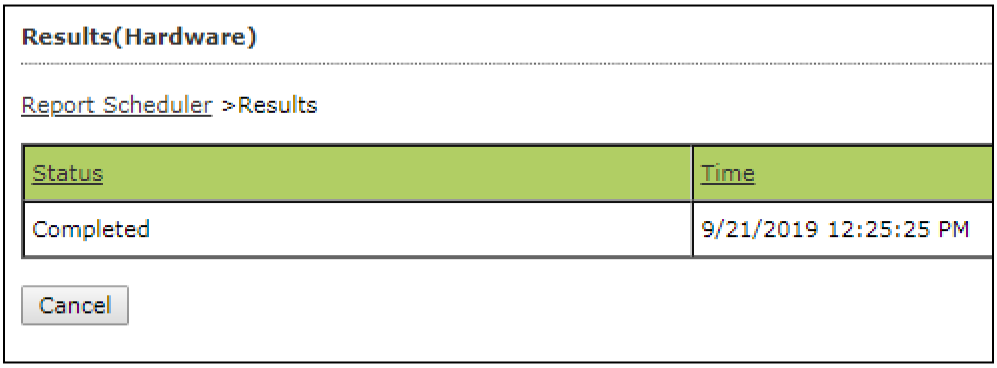
□	Schedule Name	Report Recipient	Scheduler Type
☑	Hardware	[redacted]	Manually Start
□	New Report	[redacted]	Manually Start
□	New Report_1	[redacted]	Automatic Scheduler

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.



Results(Hardware)

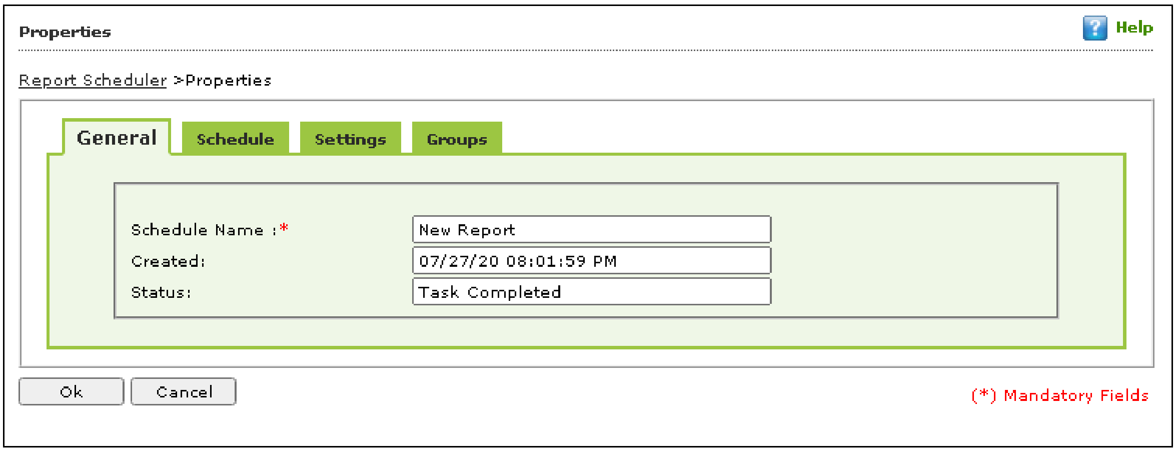
Report Scheduler >Results

Status	Time
Completed	9/21/2019 12:25:25 PM

View Properties of a Schedule

To view the properties of a schedule,

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



Schedule Name :*	New Report
Created:	07/27/20 08:01:59 PM
Status:	Task Completed

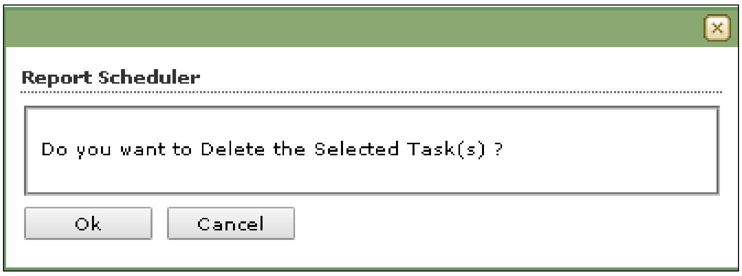
(*) Mandatory Fields

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

Delete a Schedule

To delete a report schedule

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

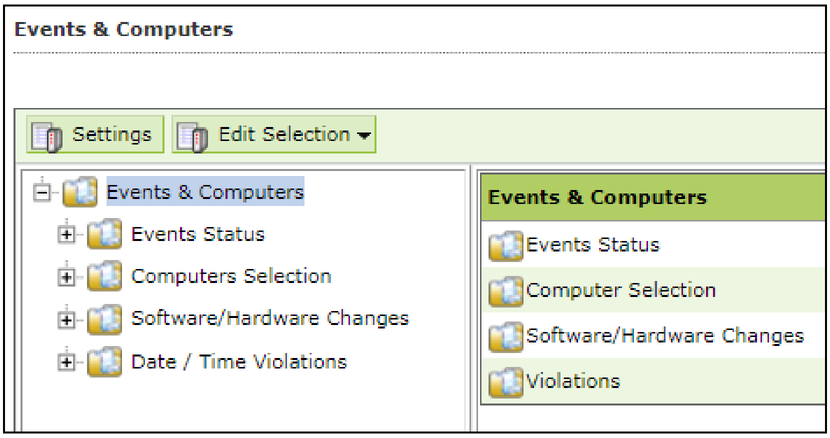


Do you want to Delete the Selected Task(s) ?

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, The module lets you sort the computer with specific properties.



Events Status

The Event Status subfolder is divided into following sections:

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

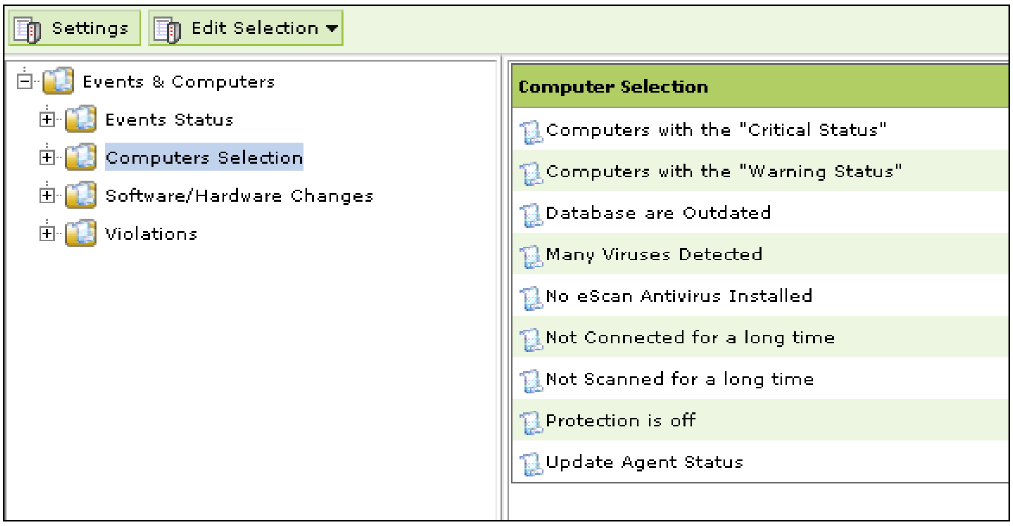
Recent
The Recent section displays both Information and Critical events.

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.



Computer Selection

- Computers with the "Critical Status"
- Computers with the "Warning Status"
- Database are Outdated
- Many Viruses Detected
- No eScan Antivirus Installed
- Not Connected for a long time
- Not Scanned for a long time
- Protection is off
- Update Agent Status

The Computer Selection subfolder consists following sections:

- **Computers with the "Critical Status"**
- **Computers with the "Warning Status"**
- **Database are Outdated**
- **Many Viruses Detected**
- **No eScan Antivirus Installed**
- **Not Connected for a long time**
- **Not Scanned for a long time**
- **Protection is off**
- **Update Agent Status**

Computers with the "Critical Status"

This section displays computers marked with Critical status.

Computers with warning status

This section displays computer with a warning status.

Database is outdated

This section displays computers whose virus database is outdated.

Many Viruses Detected

This section displays the computers whose virus count has exceeded.

No eScan 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.

Not scanned for a long time

This section displays the computers which weren’t scanned for the set duration.

Protection is off

This section displays the computers on which File Protection is disabled.

Update Agent Staus

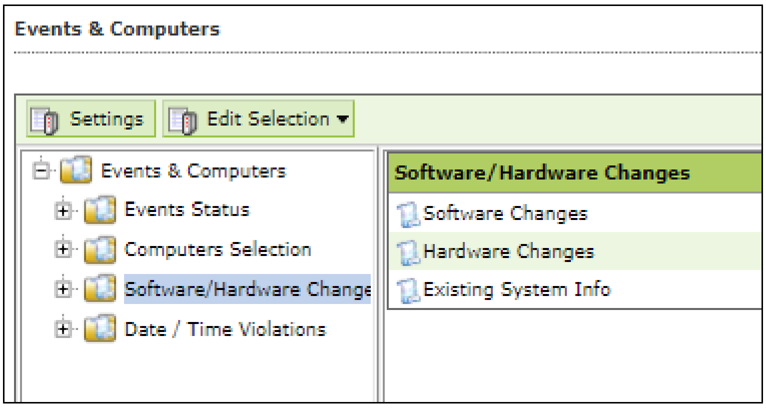
This section displays the status of computers assigned as Update Agent.

The additional settings vary depending upon the Computer Status.

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.

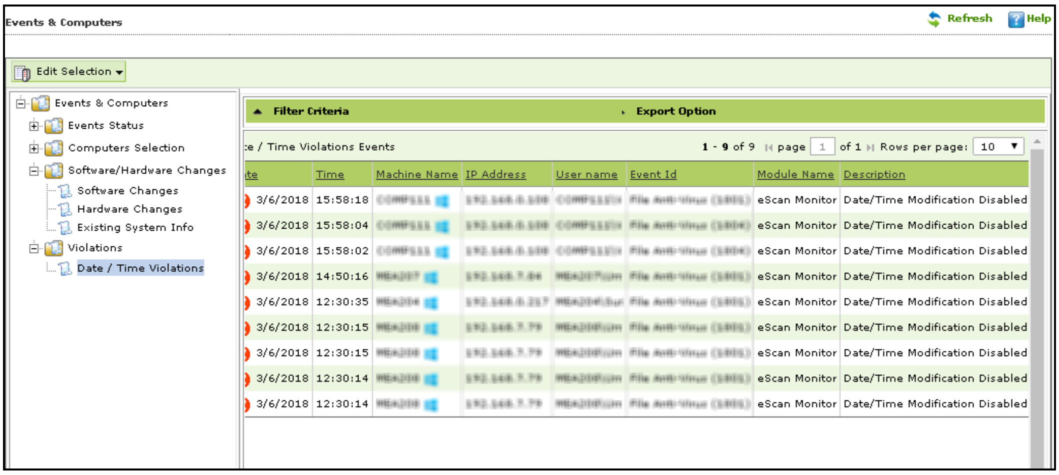
Existing System Info

This section displays a computer’s existing hardware information.

Violations

Date/Time Violations

This subfolder consists Date/Time Violations that displays client computers whose users attempted to modify date and time.



:e / Time Violations Events   1 - 9 of 9   page 1 of 1   Rows per page: 10

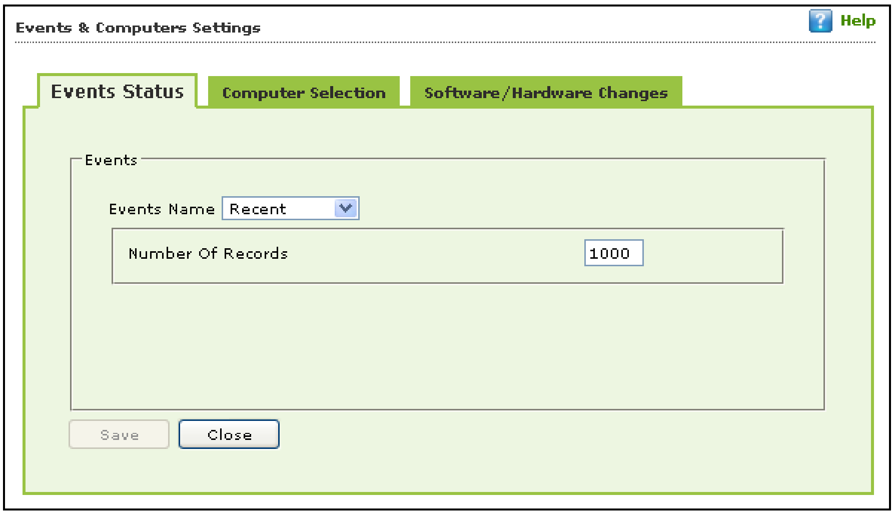
te	Time	Machine Name	IP Address	User name	Event Id	Module Name	Description
3/6/2018	15:58:18	[redacted]	[redacted]	[redacted]	[redacted]	eScan Monitor	Date/Time Modification Disabled
3/6/2018	15:58:04	[redacted]	[redacted]	[redacted]	[redacted]	eScan Monitor	Date/Time Modification Disabled
3/6/2018	15:58:02	[redacted]	[redacted]	[redacted]	[redacted]	eScan Monitor	Date/Time Modification Disabled
3/6/2018	14:50:16	[redacted]	[redacted]	[redacted]	[redacted]	eScan Monitor	Date/Time Modification Disabled
3/6/2018	12:30:35	[redacted]	[redacted]	[redacted]	[redacted]	eScan Monitor	Date/Time Modification Disabled
3/6/2018	12:30:15	[redacted]	[redacted]	[redacted]	[redacted]	eScan Monitor	Date/Time Modification Disabled
3/6/2018	12:30:15	[redacted]	[redacted]	[redacted]	[redacted]	eScan Monitor	Date/Time Modification Disabled
3/6/2018	12:30:14	[redacted]	[redacted]	[redacted]	[redacted]	eScan Monitor	Date/Time Modification Disabled
3/6/2018	12:30:14	[redacted]	[redacted]	[redacted]	[redacted]	eScan Monitor	Date/Time Modification Disabled

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 Computer settings window.

Event Status Setting

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



Events

Events Name: Recent

Number Of Records: 1000

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

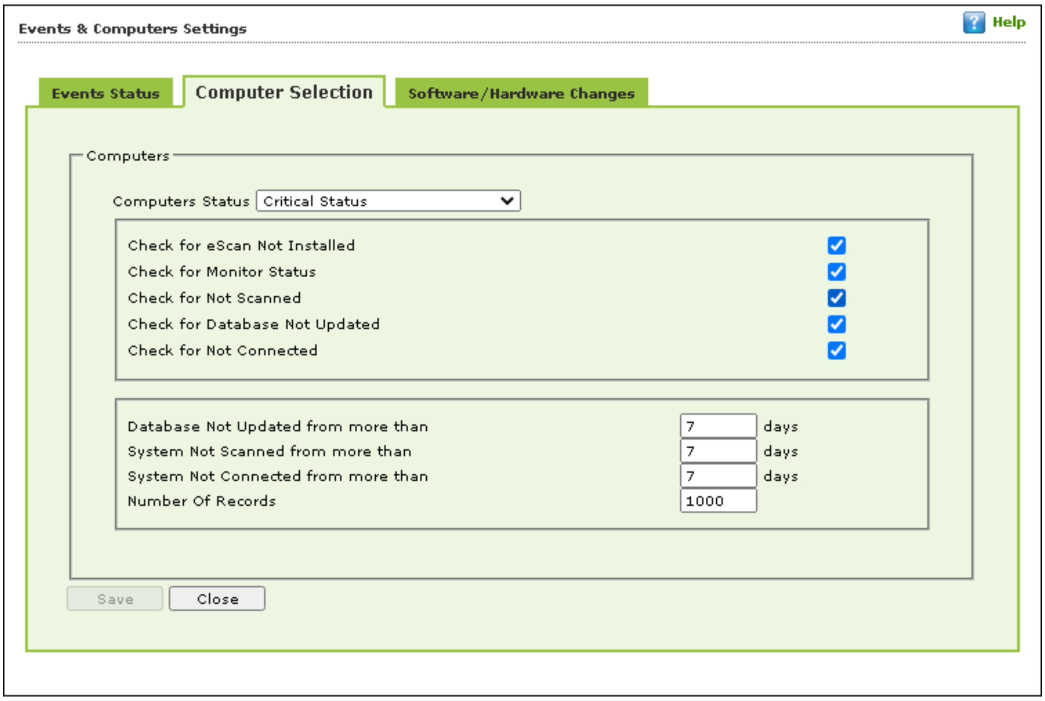
- **Recent:** It displays both critical and information events that occurred recently on managed client computers.

- **Critical:** It displays all critical events occurred on managed client computers, such as virus detection, monitor disabled status, and so on.
- **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 Monitor Status ☑
Check for Not Scanned ☑
Check for Database Not Updated ☑
Check for Not Connected ☑

Database Not Updated from more than 7 days
System Not Scanned from more than 7 days
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 Monitor Status**: Select this checkbox to view the client systems on which eScan monitor is not enabled.
- **Check for Not Scanned**: Select this checkbox to view the list of client systems which has not been scanned.
- **Check for Database Not Updated**: Select this checkbox to view the list of client systems on which database has not been updated.
- **Check for Not Connected**: Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.

- **Database Not Updated from more than**: Enter the number of days from when the database has not been updated.
- **System Not Scanned for more than**: Enter the number of days from when the system has not been scanned.
- **System Not Connected for 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 Scanned**: Select this checkbox to view the list of client systems which has not been scanned.
- **Check for Database Not Updated**: Select this checkbox to view the list of client systems on which database has not been updated.
- **Check for Not Connected**: Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **Check for Protection off**: Select this checkbox to view the list of client systems on which protection for any module is inactive.
- **Check for Many Viruses**: Select this checkbox to view the list of client systems on which maximum viruses are detected.
- **Database Not Updated from more than**: Enter the number of days from when the database has not been updated.
- **System Not Scanned for more than**: Enter the number of days from when the system has not been scanned.
- **System Not Connected for 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.

Database are Outdated: It displays a list of systems on which virus database is outdated. Specify the following field details:

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

Many viruses Detected: It displays a list of systems on which number of viruses exceeds the specified count in computer settings. Specify the following field details:

- **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 to the eScan server 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 detail:

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

Not scanned for a long time: It displays the list of systems which have not been scanned from a long time, as specified in computer settings. Specify the following field details:

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

Protection is off: It displays the list of systems on which protection is inactive for any module, as per the protection criteria's selected in computer settings. It shows the status as "Disabled" in the list. Specify the following field details.

- **Check for Monitor Status**: Select this checkbox if you want to view the client systems on which eScan monitor is not enabled.
- **Check for Mail Anti-Phishing**: Select this checkbox if you want to view the list of client systems on which **Mail Anti-Phishing** protection is inactive.
- **Check for Mail Anti-Virus**: Select this checkbox if you want to view the list of client systems on which **Mail Anti-Virus** protection is inactive.
- **Check for Mail Anti-Spam**: Select this checkbox if you want to view the list of client systems on which **Mail Anti- Spam** protection is inactive.
- **Check for Endpoint Security**: Select this checkbox if you want to view the list of client systems on which **Endpoint Security** protection is inactive.
- **Check for Firewall**: Select this checkbox if you want to view the list of client systems on which **Firewall** protection is inactive.
- **Check for Proactive**: Select this checkbox if you want to view the list of client systems on which **Proactive** protection is inactive.
- **Check for Web Protection**: Select this checkbox if you want to view the list of client systems on which protection of
- **Web Protection** module is inactive.
- **Number of Records**: Enter the number of client system that you want to view in the list.

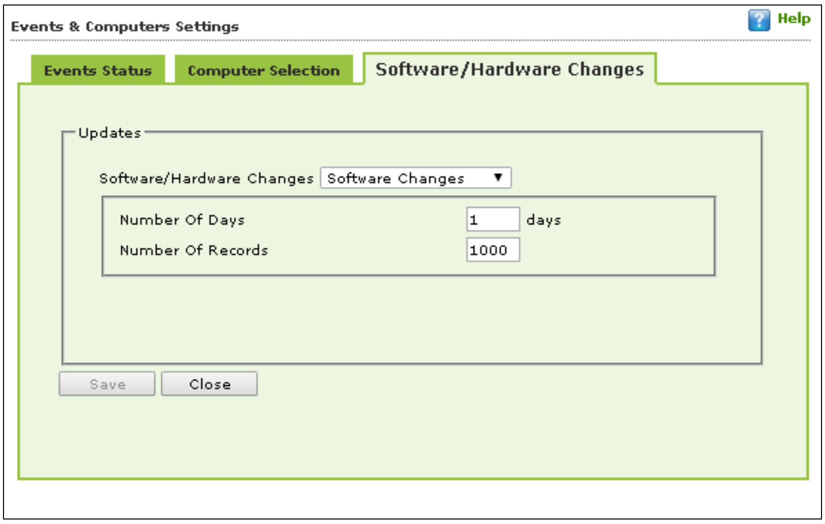
Steps to define computer settings

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.

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.
3. Click the preferred action.

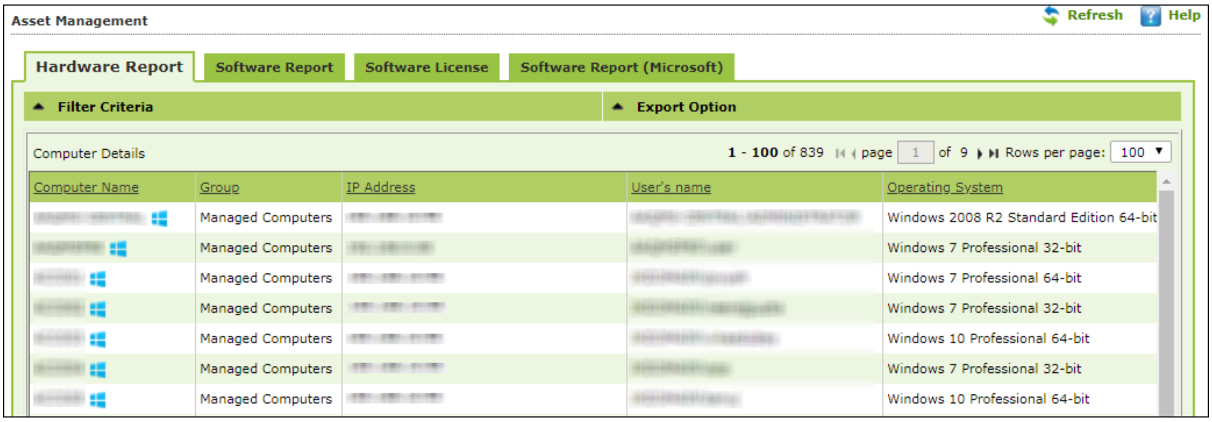
Asset Management

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 Details 1 - 100 of 839 page 1 of 9 Rows per page: 100

Computer Name	Group	IP Address	User's name	Operating System
[redacted]	Managed Computers	[redacted]	[redacted]	Windows 2008 R2 Standard Edition 64-bit
[redacted]	Managed Computers	[redacted]	[redacted]	Windows 7 Professional 32-bit
[redacted]	Managed Computers	[redacted]	[redacted]	Windows 7 Professional 64-bit
[redacted]	Managed Computers	[redacted]	[redacted]	Windows 7 Professional 32-bit
[redacted]	Managed Computers	[redacted]	[redacted]	Windows 10 Professional 64-bit
[redacted]	Managed Computers	[redacted]	[redacted]	Windows 7 Professional 32-bit
[redacted]	Managed Computers	[redacted]	[redacted]	Windows 10 Professional 64-bit

The tab displays following details of managed computers:

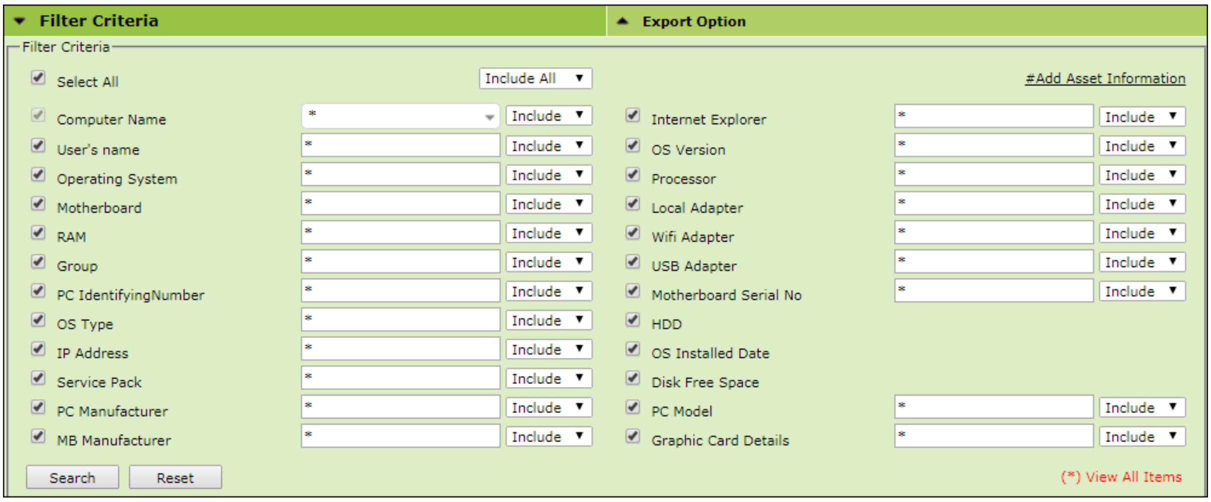
- Computer Name
- Group
- IP Address
- User name
- Operating System
- Service Pack
- OS Version
- OS Installed Date
- Internet Explorer
- Processor
- Motherboard
- RAM
- HDD
- Local MAC Adapter(s)
- Wi-Fi MAC [Adapter]
- USB MAC [Adapter]
- PC Identifying Number
- Motherboard Serial No
- Network Speed
- Disk Free Space

- PC Manufacturer
- PC Model
- MB Manufacturer
- Graphic Card Details
- Machine Type
- BitLocker Status
- Keyboard Vendor
- 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.



☑ 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 ▼

(*) View All Items

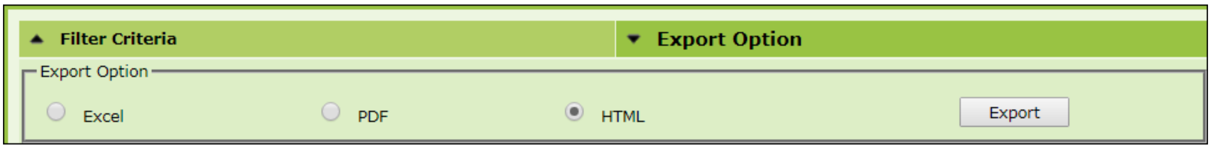
Select the parameters you want to be included in the filtered report.

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.

Exporting Hardware Report

To export the Hardware Report, click **Export Option**.
Export Option field expands.

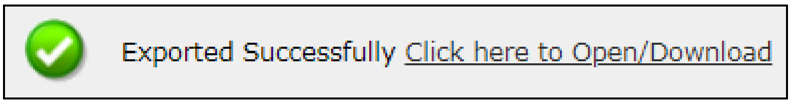


▲ Filter Criteria ▼ Export Option

Export Option

○ Excel ○ PDF ● HTML [Export]

Select the preferred option and then click **Export**. A success message appears.

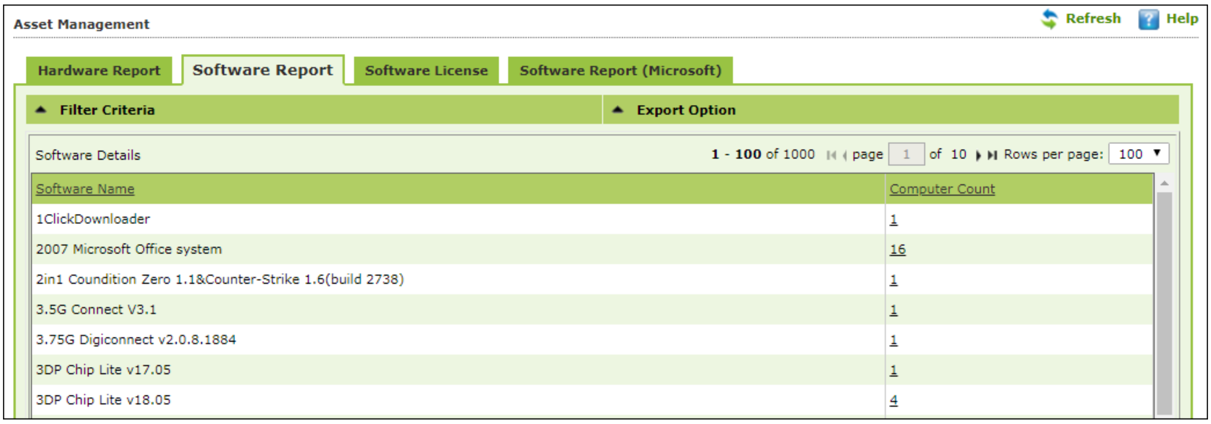


Exported Successfully Click here to Open/Download

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.



Software Details 1 - 100 of 1000 page 1 of 10 Rows per page: 100

Software Name	Computer Count
1ClickDownloader	1
2007 Microsoft Office system	16
2in1 Coundition Zero 1.1&Counter-Strike 1.6(build 2738)	1
3.5G Connect V3.1	1
3.75G Digiconnect v2.0.8.1884	1
3DP Chip Lite v17.05	1
3DP Chip Lite v18.05	4

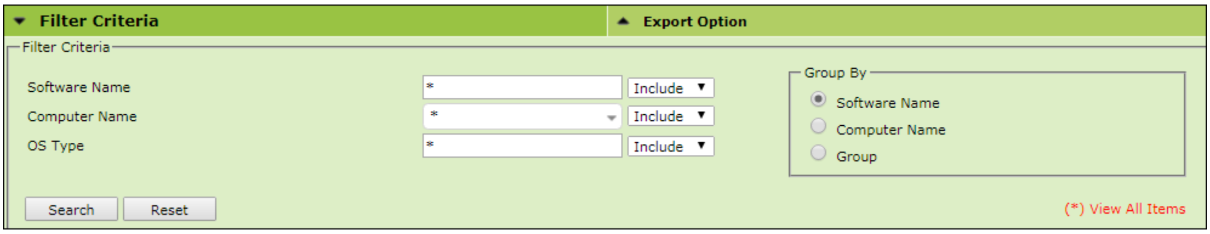
To view the computers on which the specific software is installed, click the numerical in Computer Count column.

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.



Software Name	*	Include
Computer Name	*	Include
OS Type	*	Include

Group By: ● Software Name ○ Computer Name ○ Group

(*) View All Items

The Software Report can be filtered on the basis of **Software Name** or **Computer Name**.

Software Name
Entering the Software name displays suggestions. Select the appropriate software.

Computer Name
Click the drop-down and select the preferred computer(s).

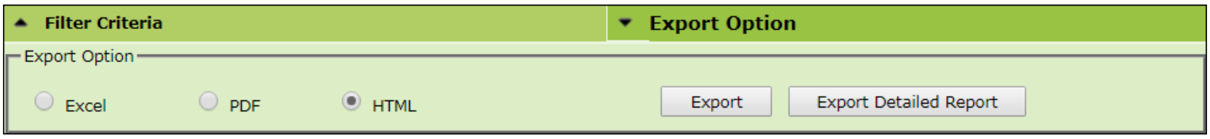
OS Type
Enter the OS type.

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.

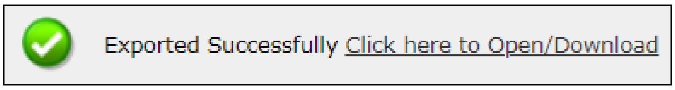
After entering data in all fields, click **Search**.
The Software Report will be filtered according to your preferences.

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.

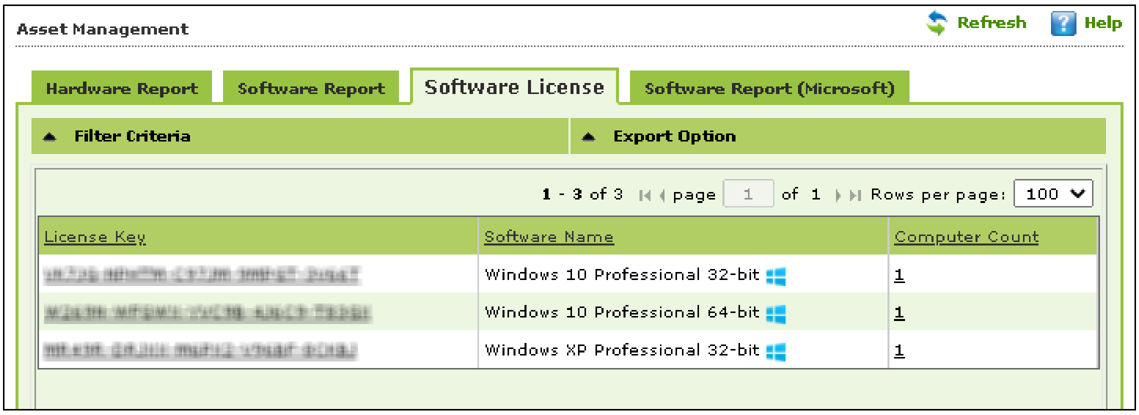


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Software License

The Software License tab displays list of Software Licenses of managed computers.

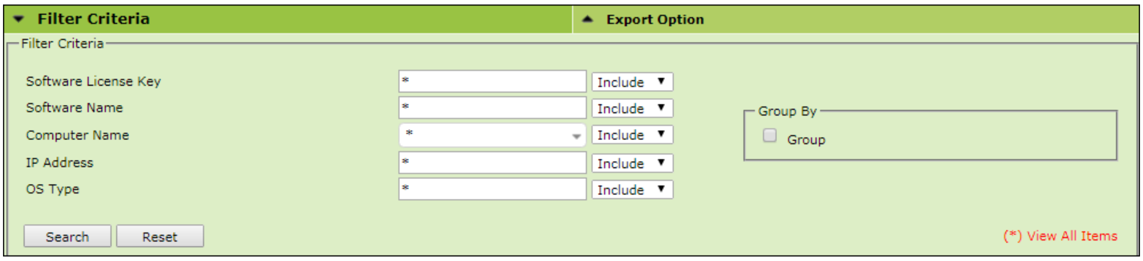


License Key	Software Name	Computer Count
[redacted]	Windows 10 Professional 32-bit	1
[redacted]	Windows 10 Professional 64-bit	1
[redacted]	Windows XP Professional 32-bit	1

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
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).

IP Address

Entering the IP address displays suggestions. Select the appropriate IP address.

OS Type

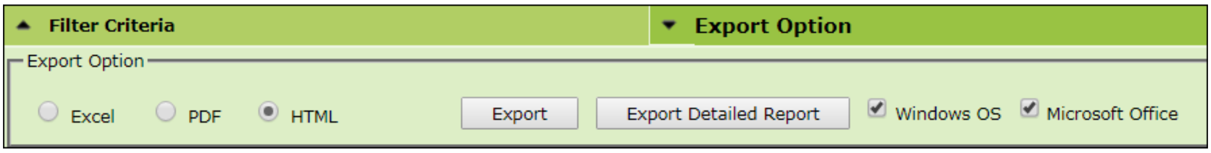
Enter the OS type.

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.

Exporting Software License Report

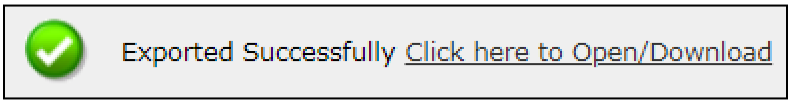
To export the Software License Report, click **Export Option**.
Export Option field expands.



○ Excel ○ PDF ● HTML ☑ Windows OS ☑ Microsoft Office

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.

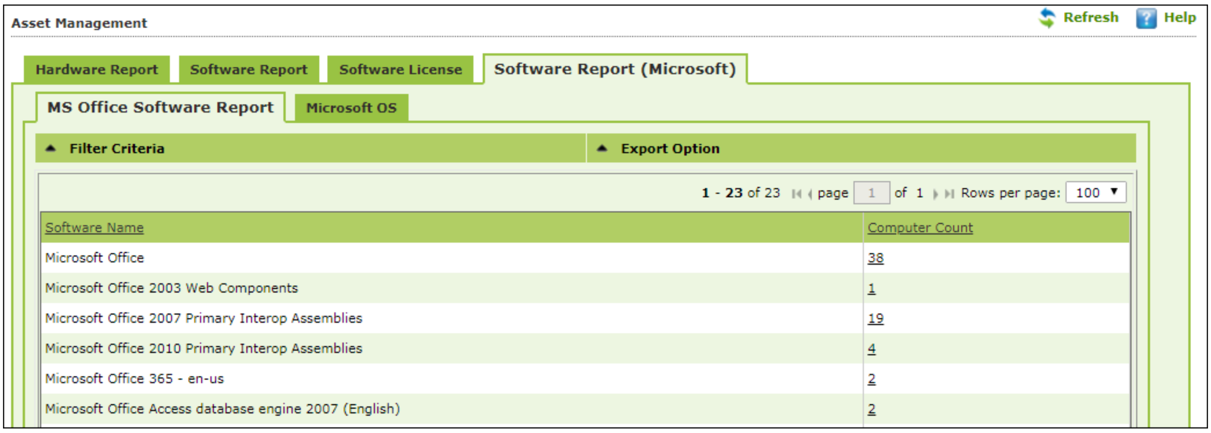


Exported Successfully Click here to Open/Download

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.



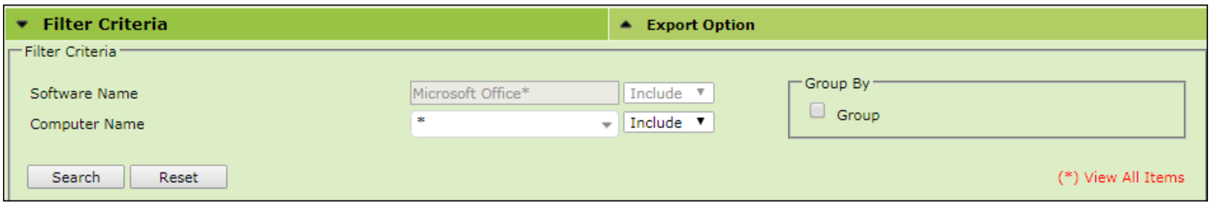
1 - 23 of 23 page 1 of 1 Rows per page: 100

Software Name	Computer Count
Microsoft Office	38
Microsoft Office 2003 Web Components	1
Microsoft Office 2007 Primary Interop Assemblies	19
Microsoft Office 2010 Primary Interop Assemblies	4
Microsoft Office 365 - en-us	2
Microsoft Office Access database engine 2007 (English)	2

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 Software Report (Microsoft)

To filter Software Report (Microsoft), click **Filter Criteria** field.
Filter Criteria field expands.



Software Name: Microsoft Office* — Include
Computer Name: * — Include
□ Group

Computer Name

Click the drop-down and select the preferred computer(s).

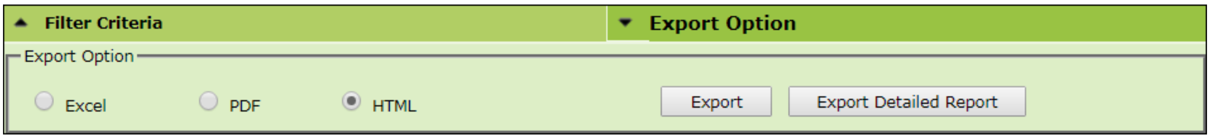
Group By

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 (Microsoft) will be filtered according to your preferences.

Exporting Software Report (Microsoft)

To export the Software Report (Microsoft), click **Export Option**.
Export Option field expands.

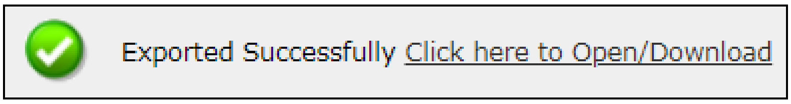


Filter Criteria | Export Option

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.

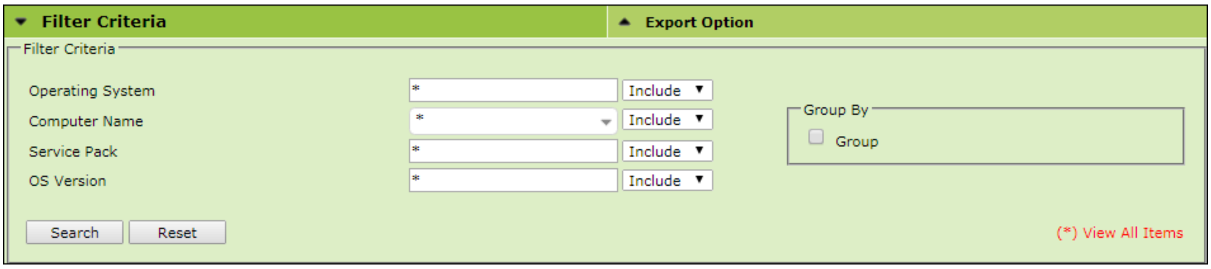


Exported Successfully Click here to Open/Download

Click the link to open/download the file.

Filtering Microsoft OS Report

To filter the Microsoft OS report, click **Filter Criteria** field.
Filter Criteria field expands.



Filter Criteria | Export Option

Filter Criteria

Operating System	*	Include
Computer Name	*	Include
Service Pack	*	Include
OS Version	*	Include

Group By

□ Group

(*) View All Items

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).

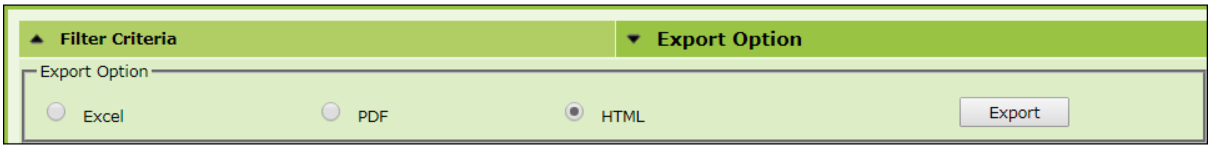
Service Pack
Entering the service pack name displays list of suggestions. Select the appropriate Service Pack.
OS Version
Entering the OS version displays list of suggestions. Select the appropriate OS version.

Include/Exclude
Selecting Include/Exclude for a parameter lets you include or exclude it from the report.

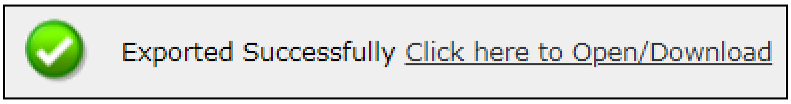
After filling all the fields, click **Search**.
The Microsoft OS report will be filtered according to your preferences.

Exporting Microsoft OS Report

To export the Microsoft OS Report, click **Export Option**.
Export Option field expands.



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.

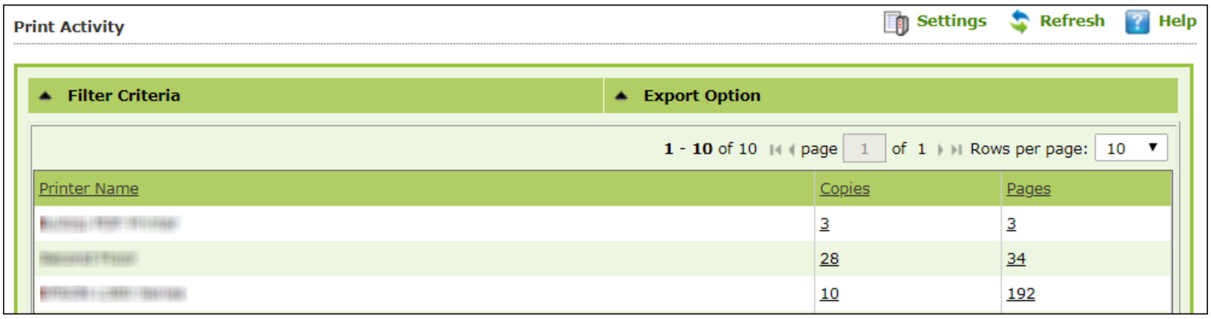
User Activity

The User Activity module lets you monitor Print, Session and File activities occurring on the client computers. It consists following submodules:

- **Print Activity**
- **Session Activity**
- **File Activity**

Print Activity

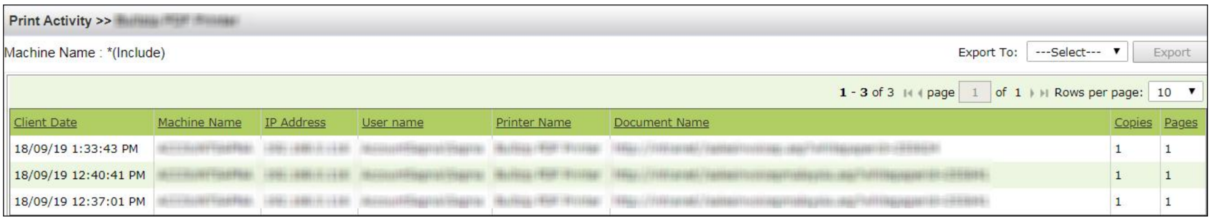
The Print Activity submodule monitors and logs print commands sent by all computers. It also lets you filter the logs on the basis of Computer name, Printer and Username. Furthermore, the module lets you export a detailed print activity report in .xls, .pdf and .html formats. The log report generated consists Print Date, Machine Name, IP Address, Username, Printer Name, Document Name along with number of Copies and Pages.



Printer Name	Copies	Pages
[redacted]	3	3
[redacted]	28	34
[redacted]	10	192

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 >> [redacted]
Export To: ---Select--- ▼
Export
1 - 3 of 3 ⏮ ◀ page 1 of 1 ▶ ⏭ Rows per page: 10 ▼

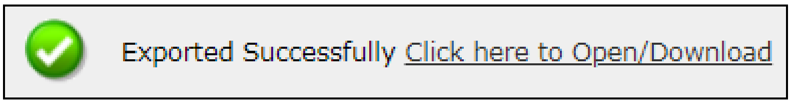
Machine Name : *(Include)

Client Date	Machine Name	IP Address	User name	Printer Name	Document Name	Copies	Pages
18/09/19 1:33:43 PM	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1	1
18/09/19 12:40:41 PM	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1	1
18/09/19 12:37:01 PM	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1	1

Exporting Print Activity Log

To export this generated log,

1. Click the **Export to** drop-down.
2. Select a preferred format.
3. Click **Export**.
   A success message appears.

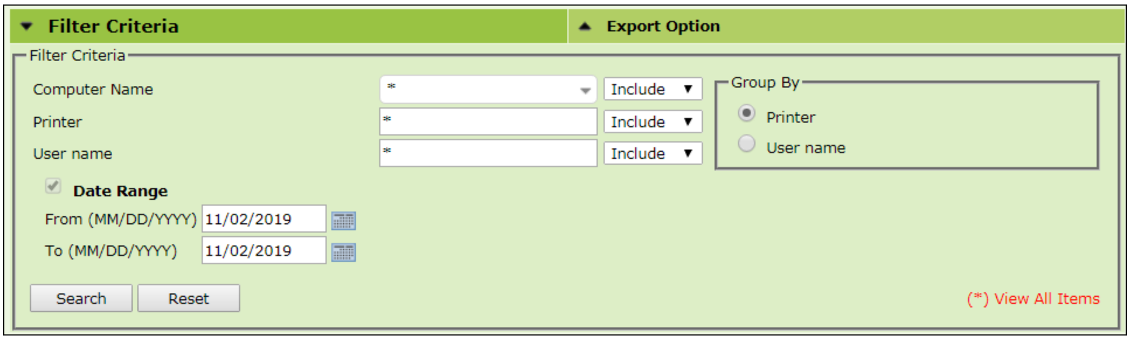


Exported Successfully Click here to Open/Download

4. 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.



Computer Name	*	Include ▼
Printer	*	Include ▼
User name	*	Include ▼

Group By
● Printer
○ User name

☑ Date Range
From (MM/DD/YYYY) 11/02/2019
To (MM/DD/YYYY) 11/02/2019

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.

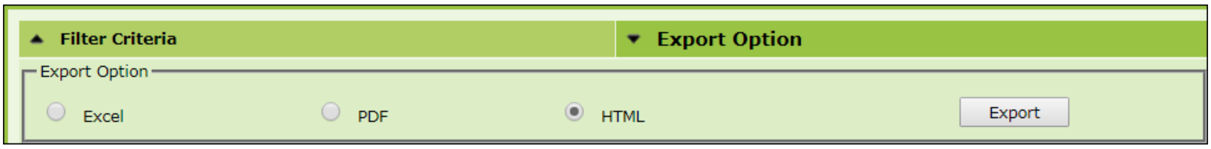
Date Range
To search the log between specific dates, select **Date Range** check box. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click **Search**.
The Print activity log will be filtered and generated according to your preferences.

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**.

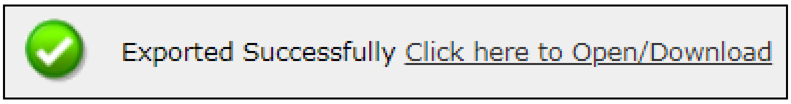
Exporting Print Activity Report

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**.
A success message appears.



Exported Successfully Click here to Open/Download

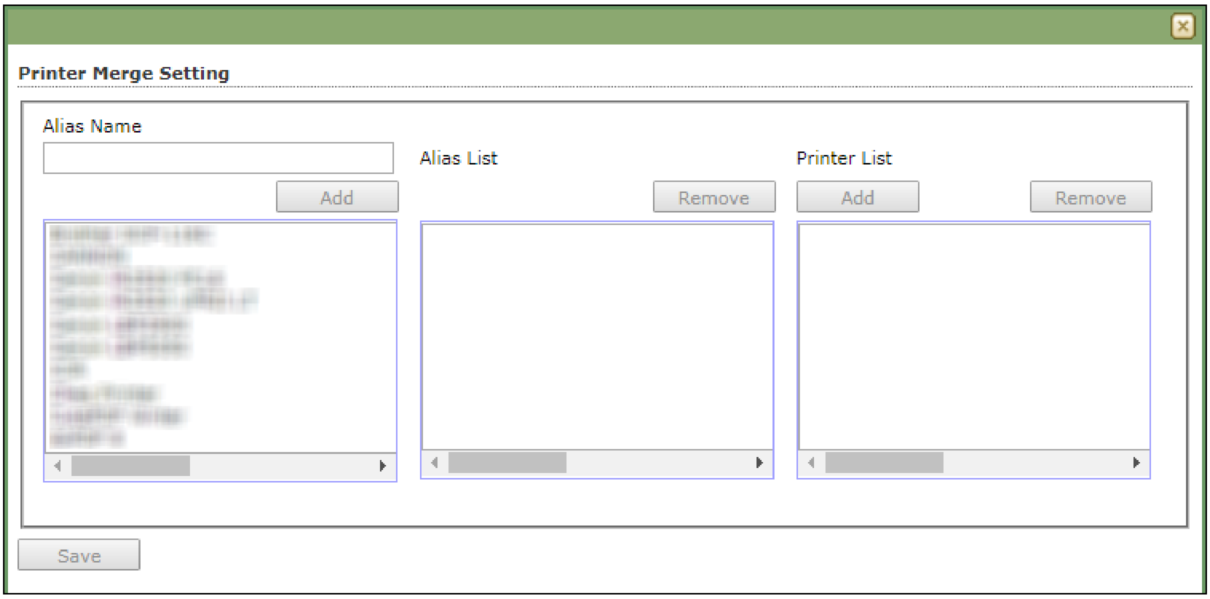
Click the link to open/download the file.

Print Activity Settings

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:

1. In the Print Activity screen, at the top right corner, click **Settings**.
   Printer Merge Setting window appears.



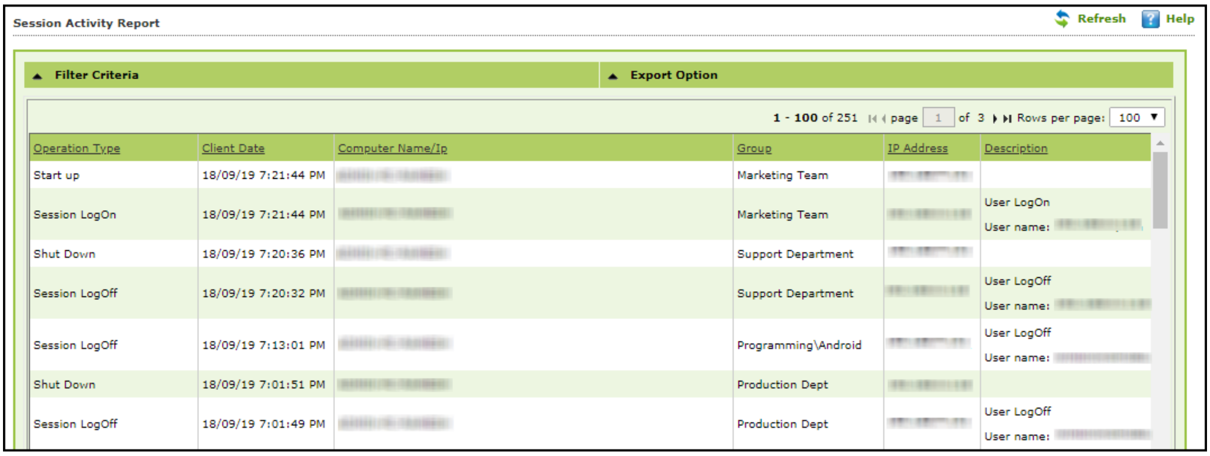
2. Enter name in Alias Name field.
3. Select printer(s) for the alias.
4. Click **Add**.
   The printer(s) will be added to the alias.
5. Click **Save**. The Print Activity Settings will be saved.

Session Activity Report

This submodule 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.

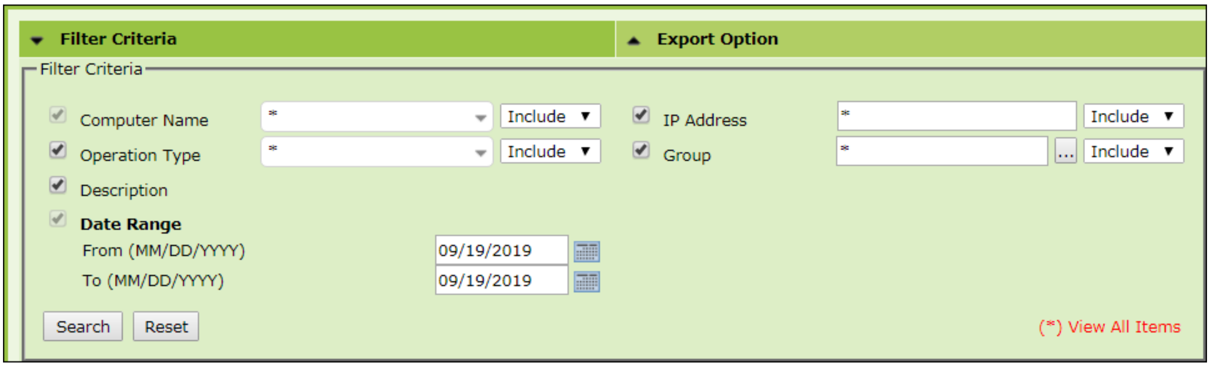


1 - 100 of 251 page 1 of 3 Rows per page: 100

Operation Type	Client Date	Computer Name/Ip	Group	IP Address	Description
Start up	18/09/19 7:21:44 PM	[redacted]	Marketing Team	[redacted]	
Session LogOn	18/09/19 7:21:44 PM	[redacted]	Marketing Team	[redacted]	User LogOn User name: [redacted]
Shut Down	18/09/19 7:20:36 PM	[redacted]	Support Department	[redacted]	
Session LogOff	18/09/19 7:20:32 PM	[redacted]	Support Department	[redacted]	User LogOff User name: [redacted]
Session LogOff	18/09/19 7:13:01 PM	[redacted]	Programming\Android	[redacted]	User LogOff User name: [redacted]
Shut Down	18/09/19 7:01:51 PM	[redacted]	Production Dept	[redacted]	
Session LogOff	18/09/19 7:01:49 PM	[redacted]	Production Dept	[redacted]	User LogOff User name: [redacted]

Filtering Session Activity Log

To filter session activities, click **Filter Criteria** field.
Filter Criteria field expands.



☑ Computer Name: * — Include
☑ Operation Type: * — Include
☑ Description
☑ Date Range
From (MM/DD/YYYY): 09/19/2019
To (MM/DD/YYYY): 09/19/2019
☑ IP Address: * — Include
☑ Group: * — Include

(*) View All Items

Filter Criteria lets you filter and generate the log according to your preferences. The check box 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.

IP Address
Enter the IP address in this field.

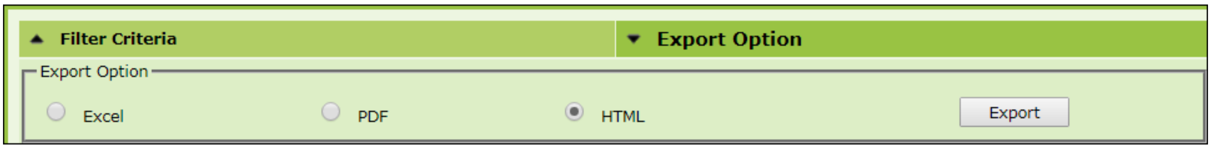
Group
Enter the group's name or click ... and select a group.

Date Range
To search the log between specific dates, select **Date Range** check box. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click **Search**.

Exporting Session Activity Report

To export the generated log, click **Export Option**.
Export Option field expands.

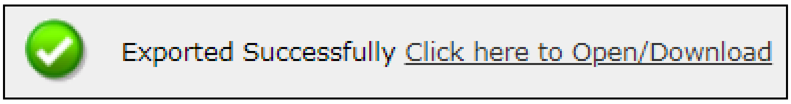


▲ Filter Criteria ▼ Export Option

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

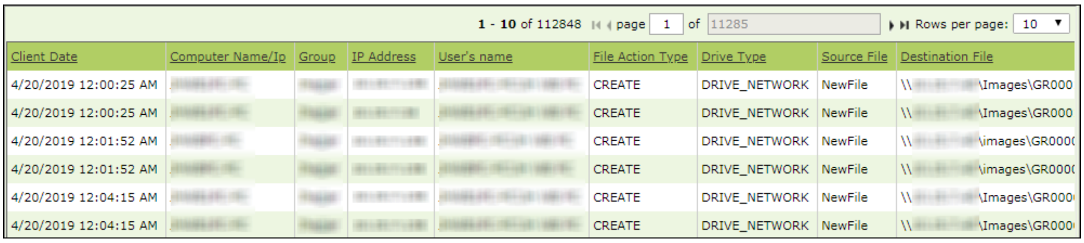
Click the link to open/download the file.

File Activity Report

The File Activity module displays a report of the files created, copied, modified, and deleted on managed computers. 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.

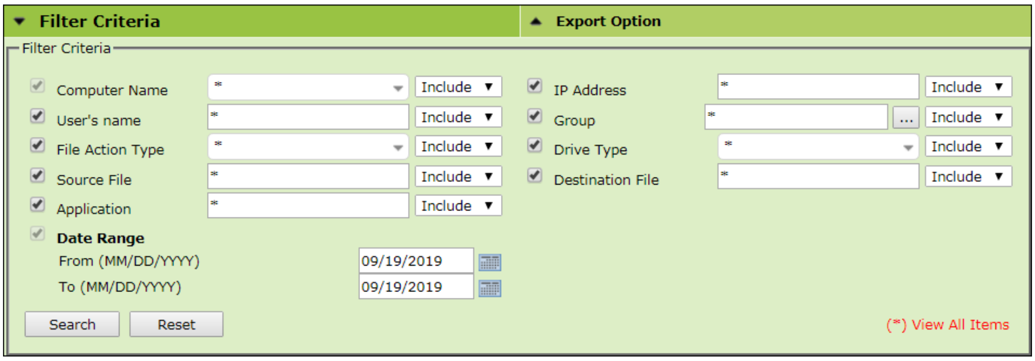


1 - 10 of 112848 | page 1 of 11285 | Rows per page: 10

Client Date	Computer Name/Ip	Group	IP Address	User's name	File Action Type	Drive Type	Source File	Destination File
4/20/2019 12:00:25 AM	[redacted]	[redacted]	[redacted]	[redacted]	CREATE	DRIVE_NETWORK	NewFile	\\[redacted]\Images\GR000
4/20/2019 12:00:25 AM	[redacted]	[redacted]	[redacted]	[redacted]	CREATE	DRIVE_NETWORK	NewFile	\\[redacted]\Images\GR000
4/20/2019 12:01:52 AM	[redacted]	[redacted]	[redacted]	[redacted]	CREATE	DRIVE_NETWORK	NewFile	\\[redacted]\images\GR000(
4/20/2019 12:01:52 AM	[redacted]	[redacted]	[redacted]	[redacted]	CREATE	DRIVE_NETWORK	NewFile	\\[redacted]\images\GR000(
4/20/2019 12:04:15 AM	[redacted]	[redacted]	[redacted]	[redacted]	CREATE	DRIVE_NETWORK	NewFile	\\[redacted]\Images\GR000
4/20/2019 12:04:15 AM	[redacted]	[redacted]	[redacted]	[redacted]	CREATE	DRIVE_NETWORK	NewFile	\\[redacted]\Images\GR000

Filtering File Activity Log

To filter file activities, click **Filter Criteria** field. Filter Criteria field expands.



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) 09/19/2019
To (MM/DD/YYYY) 09/19/2019

Filter Criteria lets you filter and generate the log according to your preferences. The check box 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.

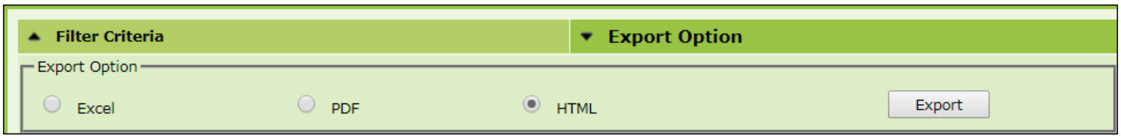
Destination File
Enter the file path.

Date Range
To search the log between specific dates, select **Date Range** check box. Afterwards, click the calendar icon and select **From** and **To** dates.

After filling all fields, click **Search**.

Exporting File activity Report

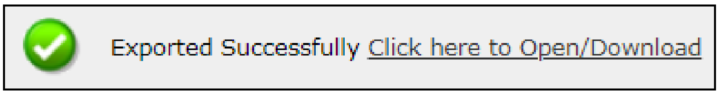
To export the generated report, click **Export Option**.
Export Option field expands.



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.

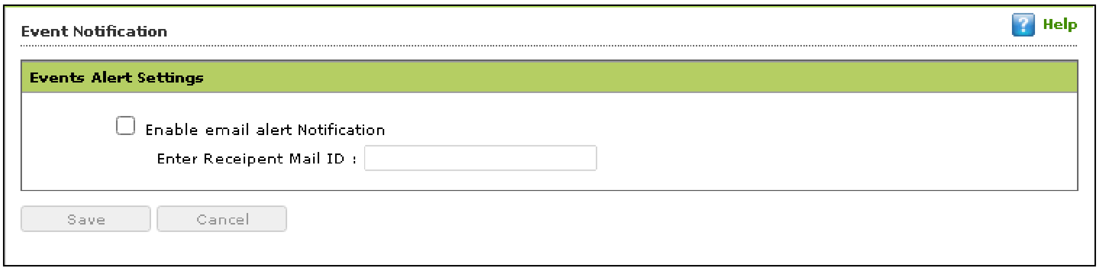
Notifications

This module lets you configure notifications for different actions/incidents that occur on the server. The Notifications module consists following submodules:

- **Event Alert**
- **Unlicensed Move Alert**

Event Alert

This submodule lets you enable email notifications about any event that occurs on the client computers connected to the server.



Event Notification

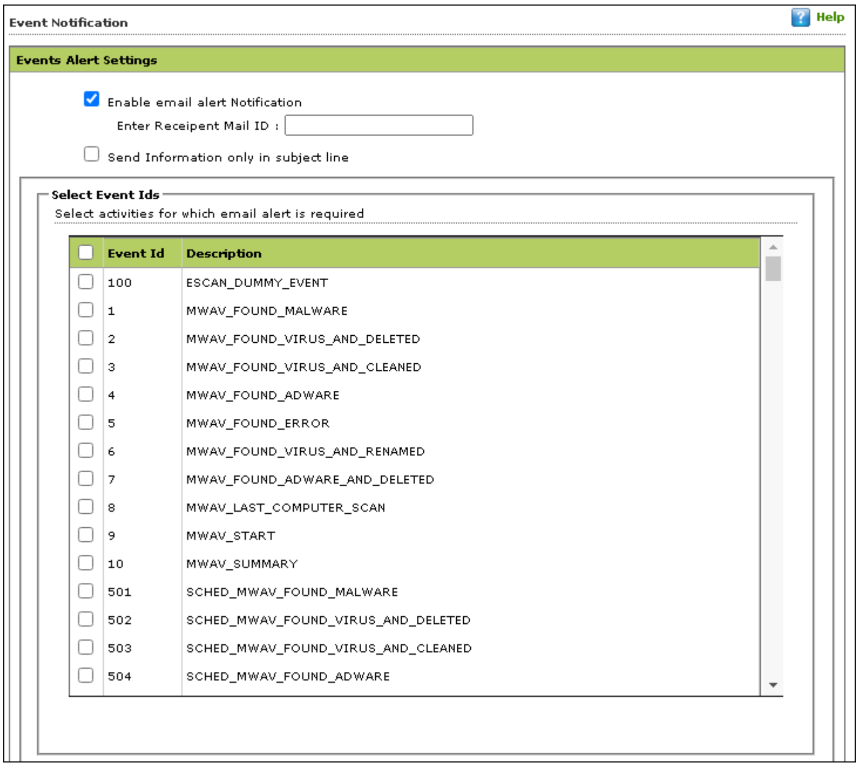
Events Alert Settings

□ Enable email alert Notification

Enter Receipent Mail ID :

To enable the event alert,

1. In the navigation panel, click **Notifications** > **Event Alert**.
2. Select the check box Enable email alert Notification.
3. Select the events from the list for which you prefer an alert.



Event Notification

Events Alert Settings

☑ Enable email alert Notification

Enter Receipent Mail ID :

□ Send Information only in subject line

Select Event Ids

Select activities for which email alert is required

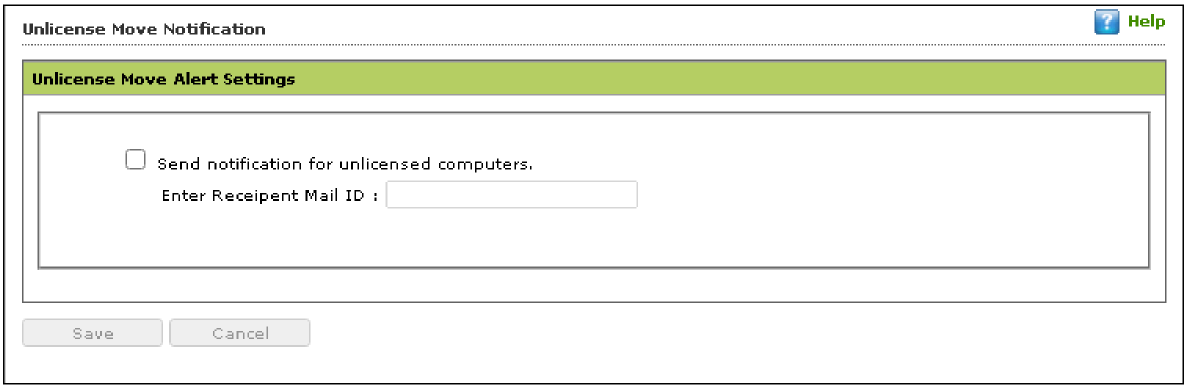
□	Event Id	Description
□	100	ESCAN_DUMMY_EVENT
□	1	MWAV_FOUND_MALWARE
□	2	MWAV_FOUND_VIRUS_AND_DELETED
□	3	MWAV_FOUND_VIRUS_AND_CLEANED
□	4	MWAV_FOUND_ADWARE
□	5	MWAV_FOUND_ERROR
□	6	MWAV_FOUND_VIRUS_AND_RENAMED
□	7	MWAV_FOUND_ADWARE_AND_DELETED
□	8	MWAV_LAST_COMPUTER_SCAN
□	9	MWAV_START
□	10	MWAV_SUMMARY
□	501	SCHED_MWAV_FOUND_MALWARE
□	502	SCHED_MWAV_FOUND_VIRUS_AND_DELETED
□	503	SCHED_MWAV_FOUND_VIRUS_AND_CLEANED
□	504	SCHED_MWAV_FOUND_ADWARE

4. Select the required hosts or group.

5. Click **Save.**
   The Event Alert Settings will be saved.

Unlicensed Move Alert

This submodule 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,

1. In the navigation panel, click **Notifications** > **Unlicensed Move Alert**.
2. Select the check box **Send notification for unlicensed computers**.
3. Click **Save**.
   The Unlicensed Move Alert Settings will be saved.

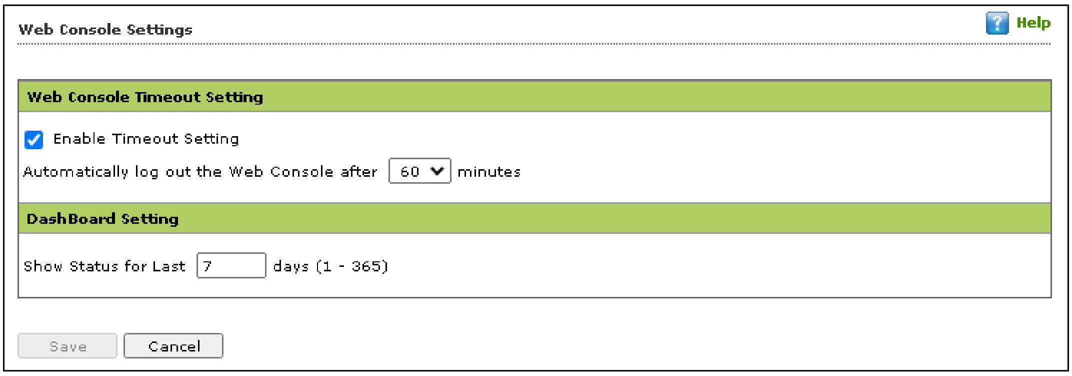
Settings

The Settings module lets you configure general settings. It contains following submodules.

- **Web Console Settings**
- **Excluded Clients**

Web Console Settings

Web Console Settings submodule lets you configure web console Timeout, Dashboard, Login Page, SQL Server Connection, SQL Database compression.



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 7 days (1 - 365)

Web Console Timeout Settings

To enable web console Timeout, select **Enable Timeout Setting** option.
After selecting the check box, click the drop-down and select the preferred duration.

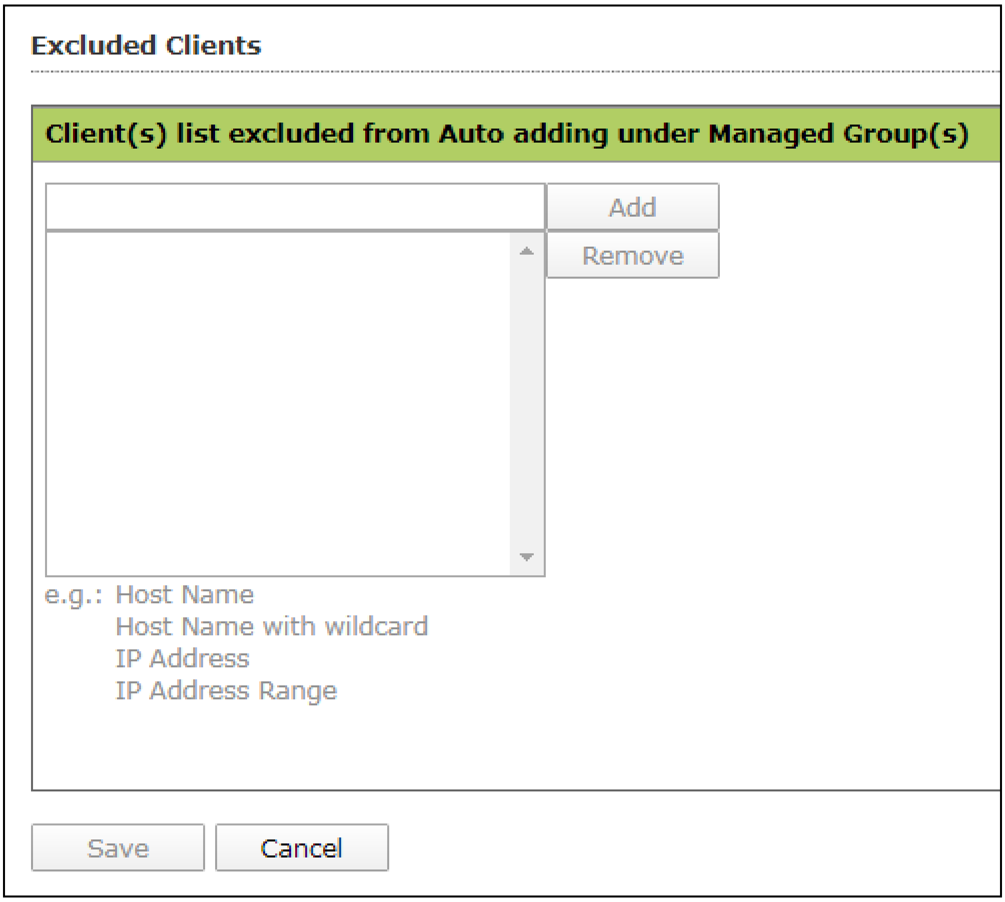
Dashboard Setting

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.

After making the necessary changes, click **Save.** The web console Settings will be updated.

Excluded Clients

The Excluded Clients settings let you exclude specific client computers from getting added under Managed Group(s).



Excluded Clients

Client(s) list excluded from Auto adding under Managed Group(s)

e.g.: Host Name
Host Name with wildcard
IP Address
IP Address Range

Exclude Clients from auto adding under Managed Group(s)

To exclude a client computer from auto adding under Managed Group(s),

1. In the box, enter the client computer's name.
2. Click **Add** > **Save**.
   The client computer gets excluded from auto adding.

Remove a client computer from excluded clients

To remove a client computer from excluded clients, select the client computer you want to remove and then click **Remove**.

The client computer gets removed from excluded clients list.

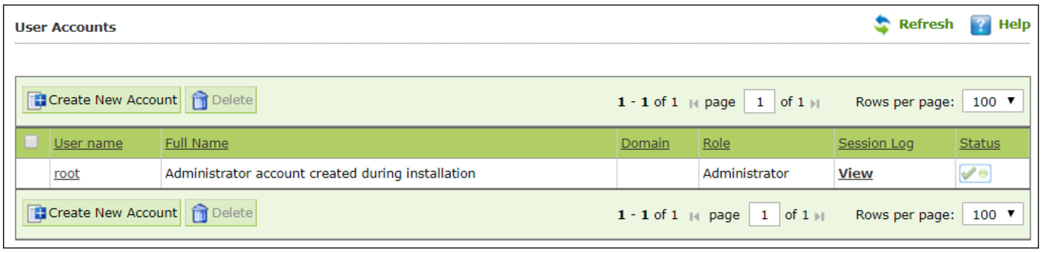
Administration

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 rights to the other employees and allow them to install eScan Client, implement Policies and Tasks. The Administration module consists following submodules:

- **User Accounts**
- **User Roles**

User Accounts

For a large organization, installing eScan Client and monitoring activities may become a difficult task. With User Accounts submodule, you can create new user accounts and assign Administrator role to added users and reduce the workload. This submodule displays a list of users and their details like Domain, Role, Session Log and Status.

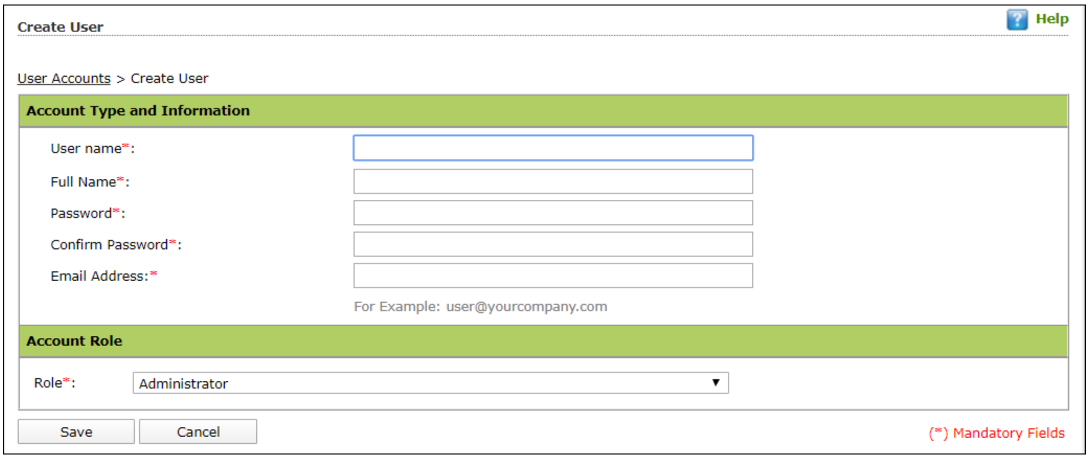


□	User name	Full Name	Domain	Role	Session Log	Status
	root	Administrator account created during installation		Administrator	View	✓

Create New Account

To create a User Account,

1. In the User Accounts screen, click **Create New Account**.
   Create User form appears.



Account Type and Information

User name*:

Full Name*:

Password*:

Confirm Password*:

Email Address:*

For Example: user@yourcompany.com

Account Role

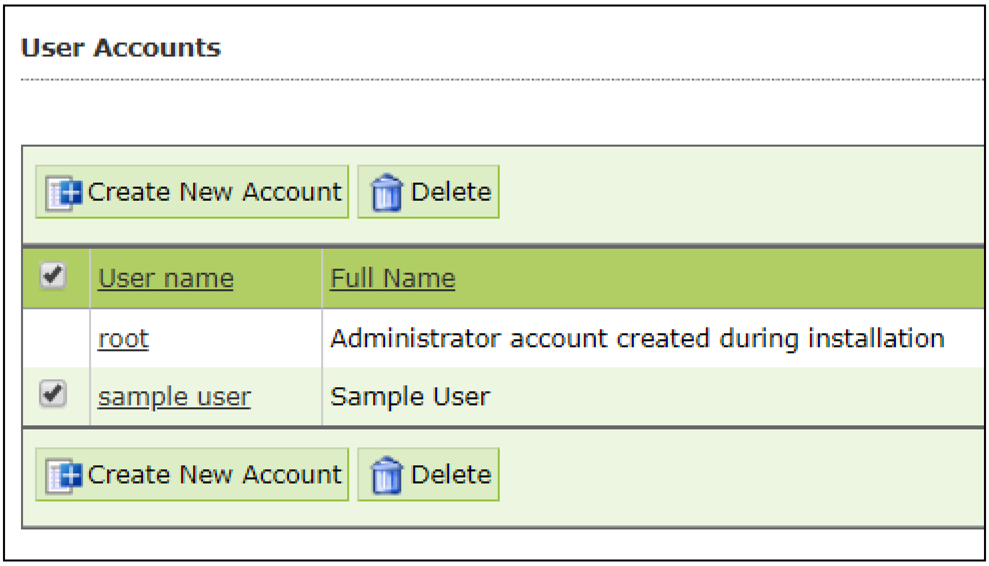
Role*: Administrator

2. 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

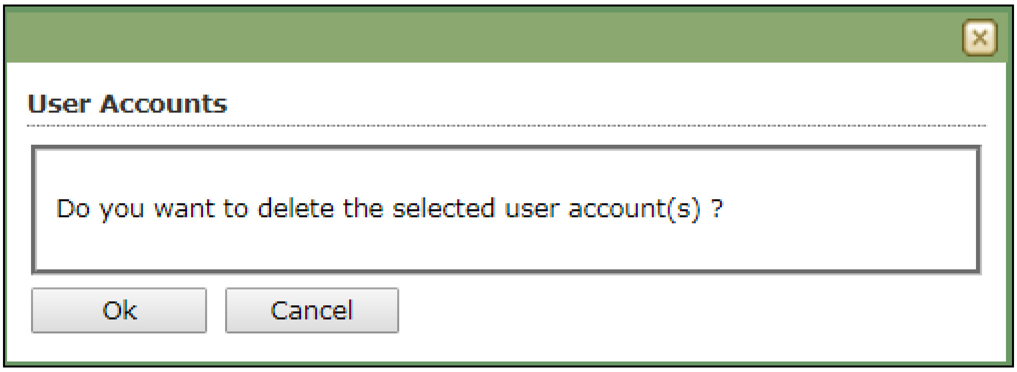
1. In the User Accounts screen, select the user you want to delete.



User Accounts

☑	User name	Full Name
	root	Administrator account created during installation
☑	sample user	Sample User

2. Click **Delete**.
   A confirmation prompt appears.



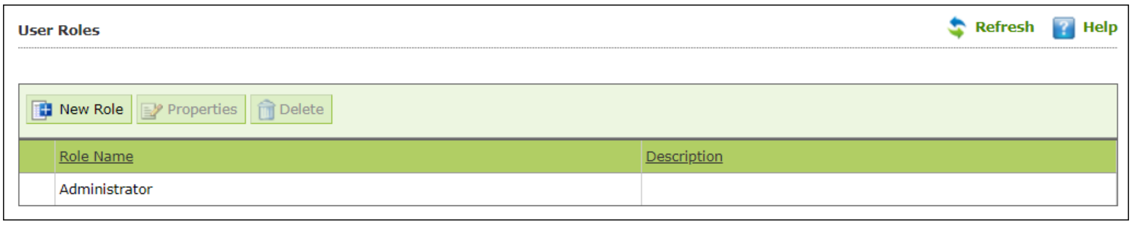
User Accounts

Do you want to delete the selected user account(s) ?

3. Click **OK**.
   The User Account will be deleted.

User Roles

The User Roles submodule 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.



User Roles

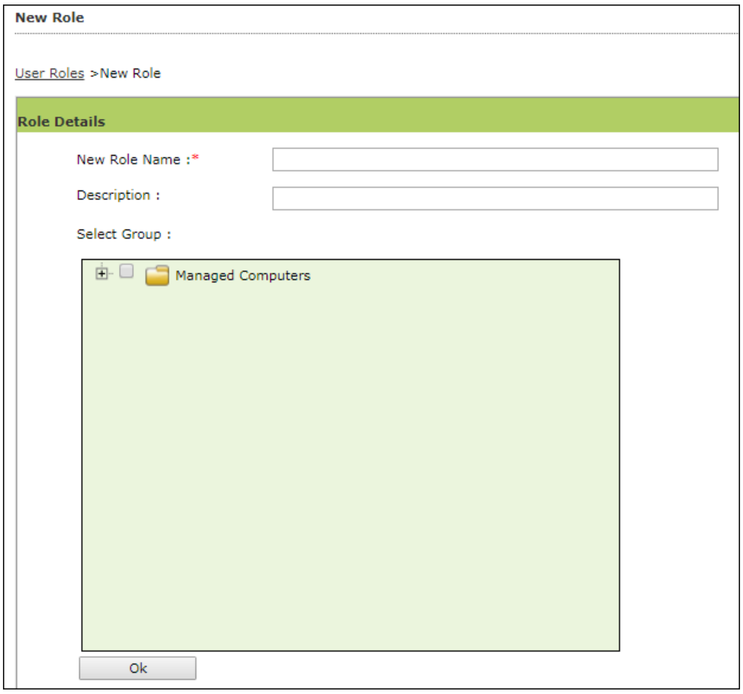
Role Name	Description
Administrator	

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,

1. In the User Roles screen, click **New Role**.
   New Role form appears.



New Role

User Roles >New Role

Role Details

New Role Name :*

Description :

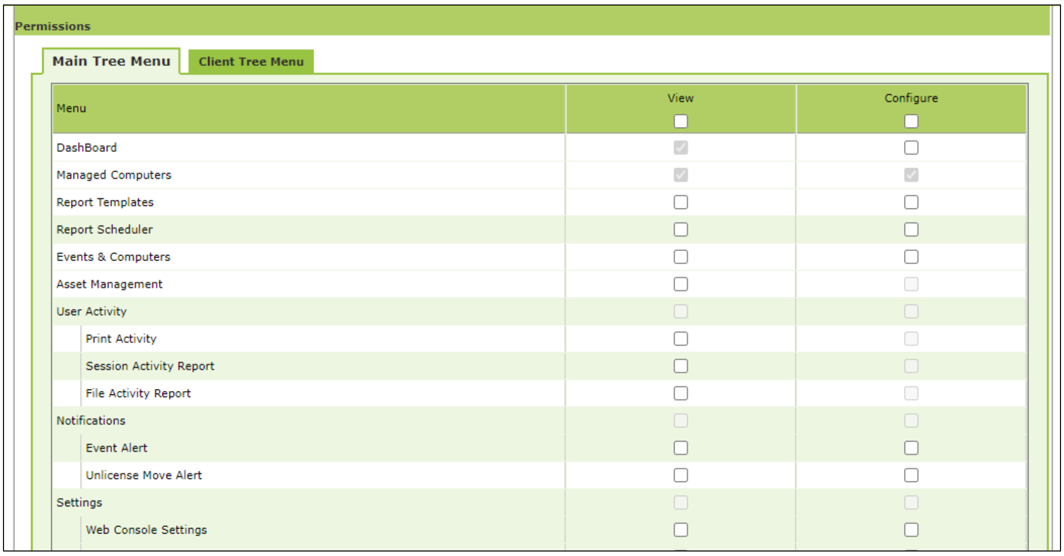
Select Group :

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.



Menu	View □	Configure □
DashBoard	☑	□
Managed Computers	☑	☑
Report Templates	□	□
Report Scheduler	□	□
Events & Computers	□	□
Asset Management	□	□
User Activity	□	□
Print Activity	□	□
Session Activity Report	□	□
File Activity Report	□	□
Notifications	□	□
Event Alert	□	□
Unlicense Move Alert	□	□
Settings	□	□
Web Console Settings	□	□

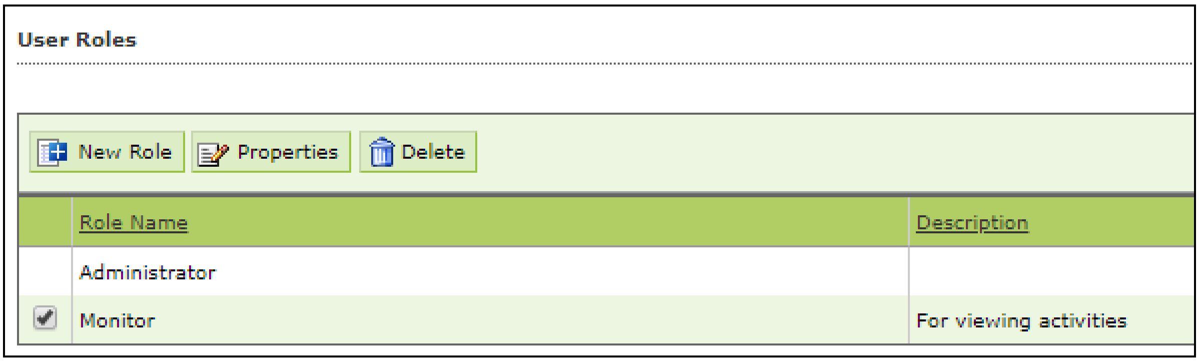
5. Select the check boxes that will allow the role to view/configure the module.
6. After selecting the necessary check boxes, click **Save**.

   The role will be added to the User Roles list.

View Role Properties

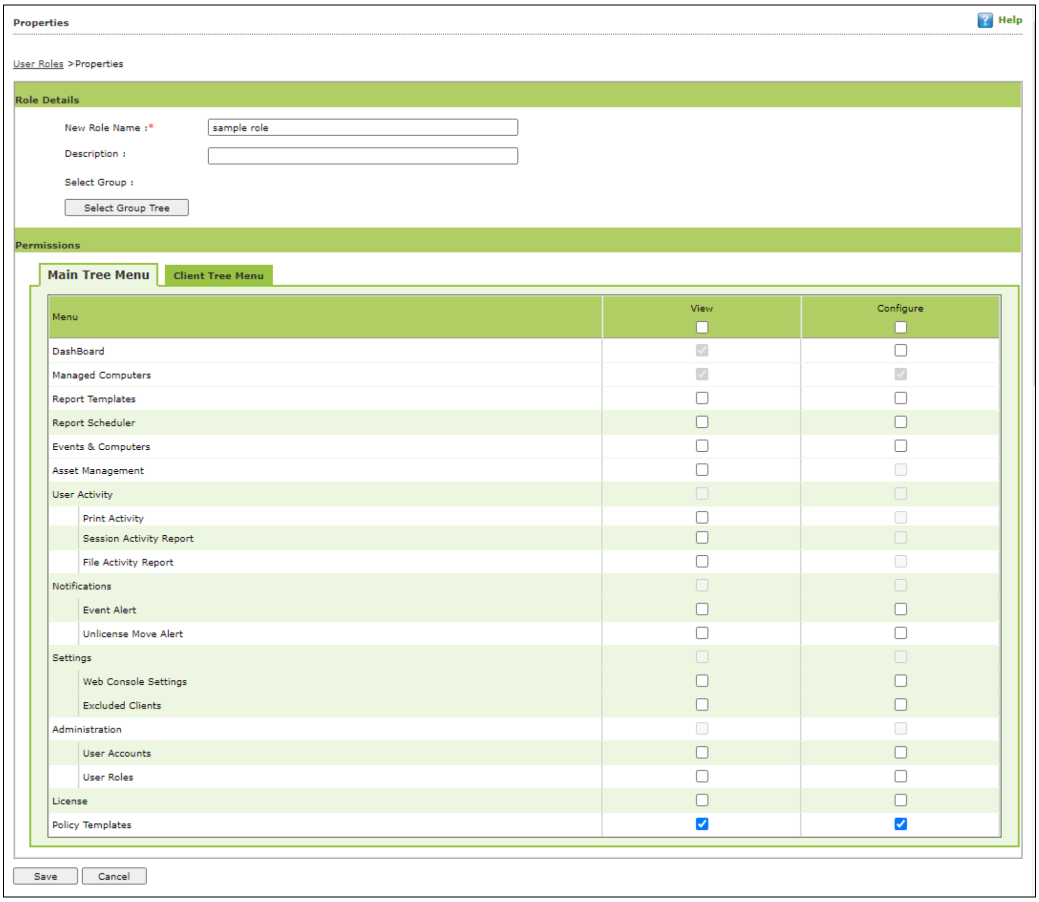
To view the properties of a role

1. In the User Roles screen, select a role.
2. This enables **Properties** and **Delete** buttons.



	Role Name	Description
	Administrator	
☑	Monitor	For viewing activities

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**.



Properties | Help

User Roles > Properties

Role Details

New Role Name :* sample role

Description :

Select Group :

[Select Group Tree]

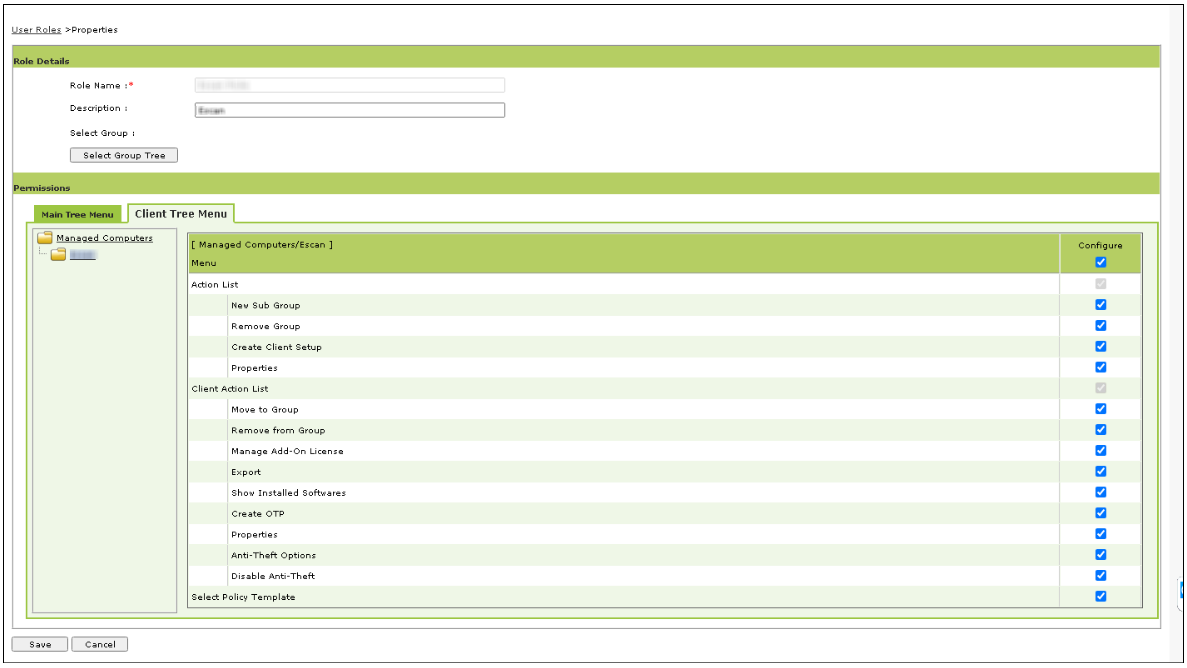
Permissions

Main Tree Menu | Client Tree Menu

Menu	View ☐	Configure ☐
DashBoard	☑	☐
Managed Computers	☑	☑
Report Templates	☐	☐
Report Scheduler	☐	☐
Events & Computers	☐	☐
Asset Management	☐	☐
User Activity	☐	☐
Print Activity	☐	☐
Session Activity Report	☐	☐
File Activity Report	☐	☐
Notifications	☐	☐
Event Alert	☐	☐
Unlicense Move Alert	☐	☐
Settings	☐	☐
Web Console Settings	☐	☐
Excluded Clients	☐	☐
Administration	☐	☐
User Accounts	☐	☐
User Roles	☐	☐
License	☐	☐
Policy Templates	☑	☑

[Save] [Cancel]

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, Select Policy Template, Policy Criteria, and Group Tasks.



User Roles >Properties

Role Details

Role Name :*

Description :

Select Group :

Permissions

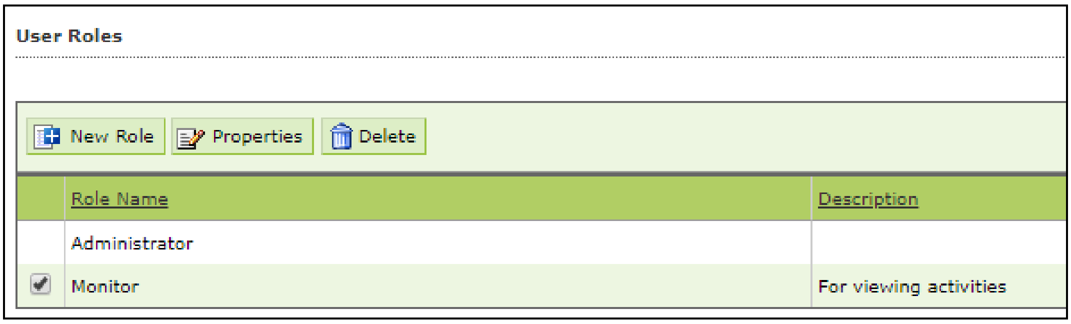
[Managed Computers/Escan] Menu	Configure ☑
Action List	☑
New Sub Group	☑
Remove Group	☑
Create Client Setup	☑
Properties	☑
Client Action List	☑
Move to Group	☑
Remove from Group	☑
Manage Add-On License	☑
Export	☑
Show Installed Softwares	☑
Create OTP	☑
Properties	☑
Anti-Theft Options	☑
Disable Anti-Theft	☑
Select Policy Template	☑

5. To let the role configure these actions, under the Configure column select the check boxes of corresponding actions.
6. Click **Save**.
   The Role Properties will be updated accordingly.

Delete a User Role

To delete a user role

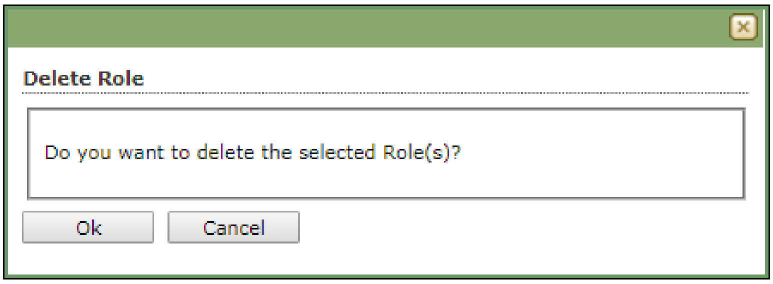
1. In the User Roles screen, select the user role you want to delete**.**



User Roles

	Role Name	Description
	Administrator	
☑	Monitor	For viewing activities

2. Click **Delete**.
   A delete confirmation prompt appears.



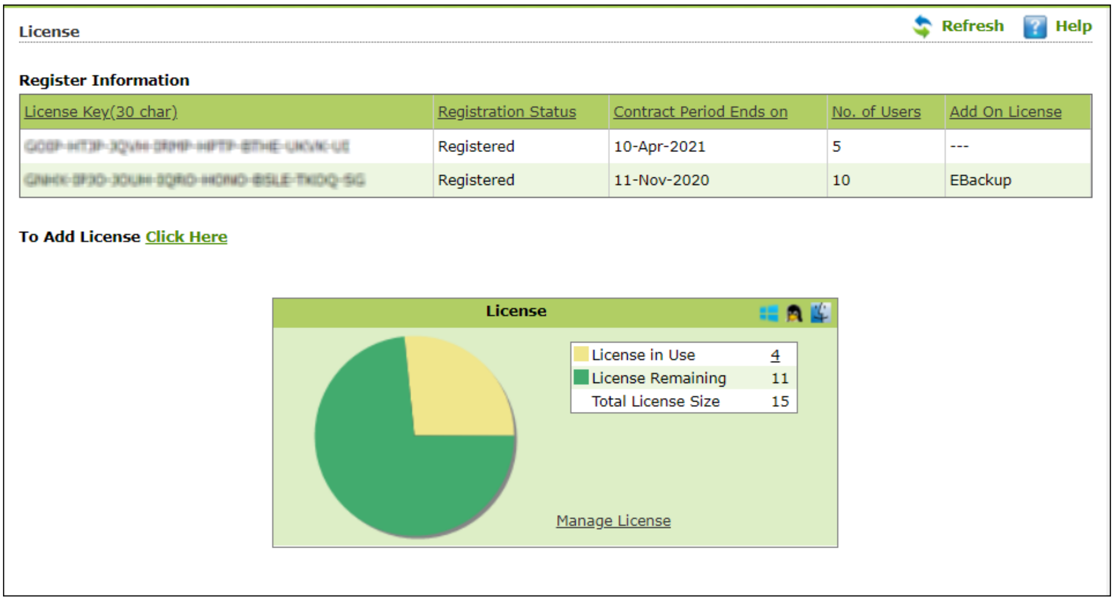
Delete Role

Do you want to delete the selected Role(s)?

3. Click **OK**.
   The User Role will be deleted.

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 eBackup, 2FA, and DLP features.



License

Register Information

License Key(30 char)	Registration Status	Contract Period Ends on	No. of Users	Add On License
[redacted]	Registered	10-Apr-2021	5	---
[redacted]	Registered	11-Nov-2020	10	EBackup

To Add License Click Here

License

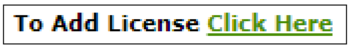
🟨	License in Use	4
🟩	License Remaining	11
	Total License Size	15

Manage License

Adding and Activating a License

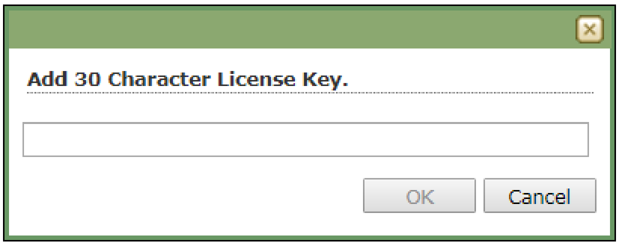
To add and activate a license

1. In the License screen, click the **Click Here** link.



To Add License Click Here

Add License Key dialog box appears.



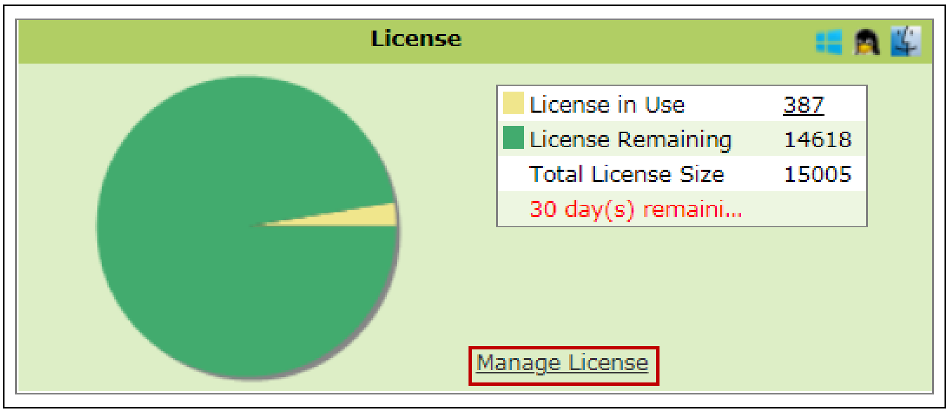
Add 30 Character License Key.

2. Enter the license key and then click **OK**.
   The license key will be added and displayed in the **Register Information** table.

Moving Licensed Computers to Non-Licensed Computers

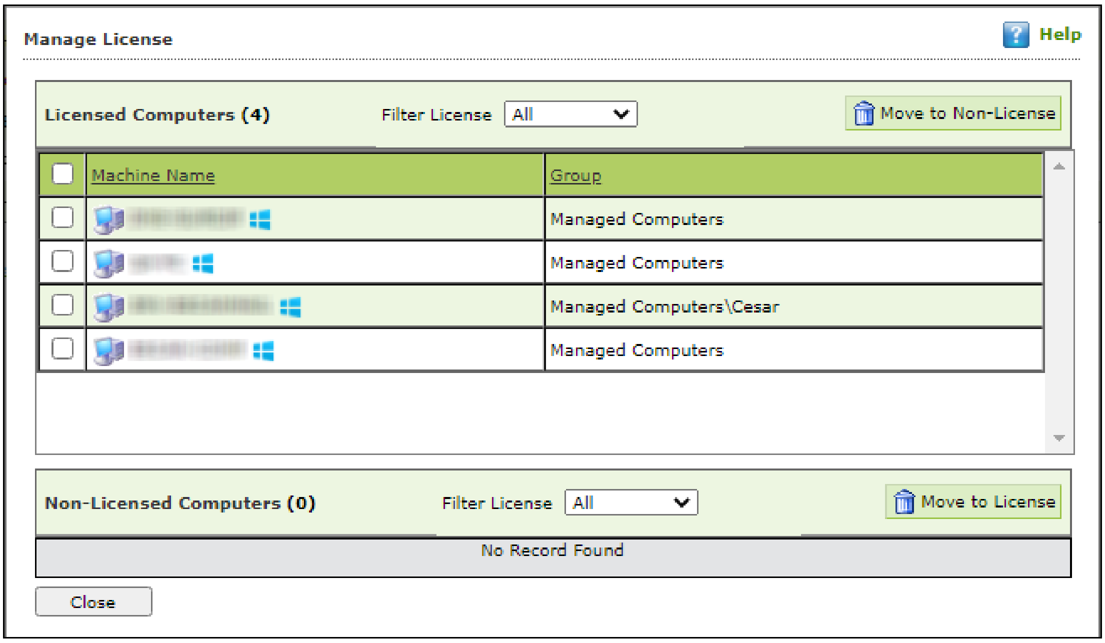
To move licensed computers to non-licensed computers,

1. In the License statistics box, click **Manage License**.



🟨	License in Use	387
🟩	License Remaining	14618
	Total License Size	15005
	30 day(s) remaini...	

Manage License window appears.



□	Machine Name	Group
□	[redacted]	Managed Computers
□	[redacted]	Managed Computers
□	[redacted]	Managed Computers\Cesar
□	[redacted]	Managed Computers

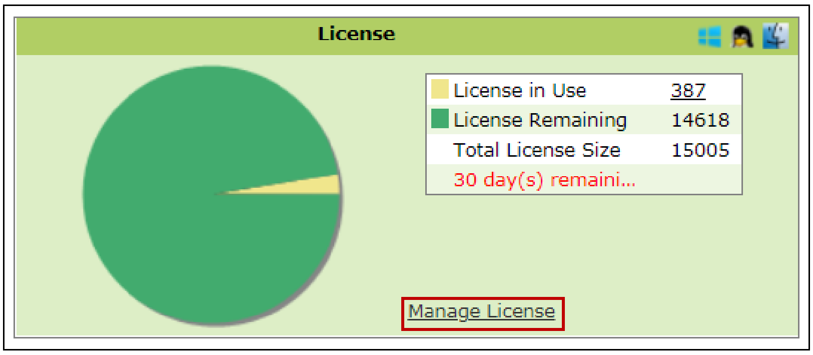
No Record Found

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**.
4. The selected computer(s) will be moved to Non-Licensed computers section.

Moving Non-Licensed Computers to Licensed Computers

To move licensed computers to non-licensed computers, follow the steps given below:

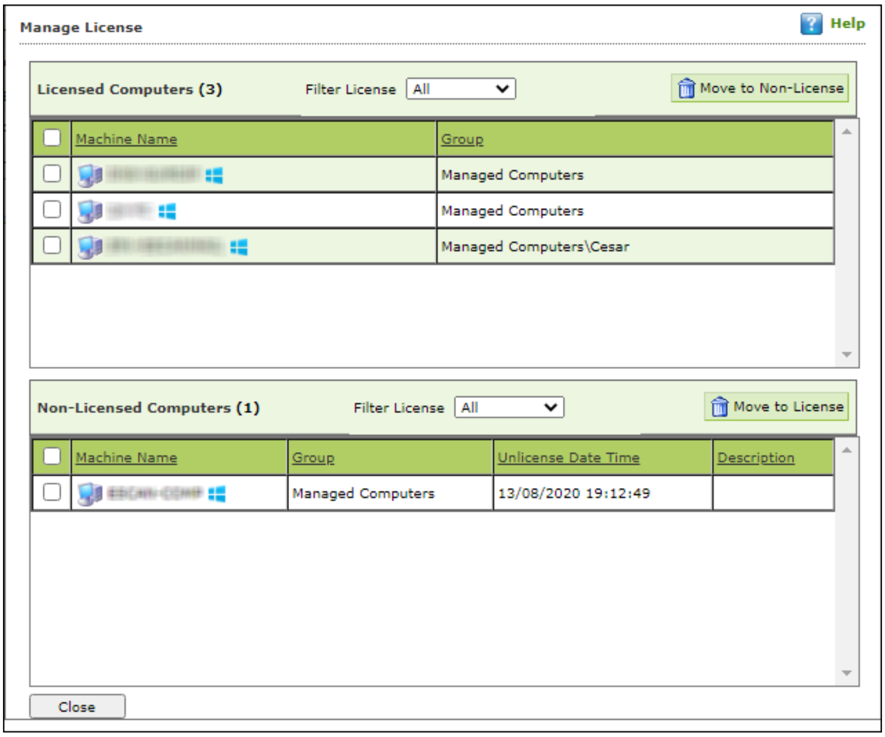
1. In the License statistics box, click **Manage License**.



License

🟨	License in Use	387
🟩	License Remaining	14618
	Total License Size	15005
	30 day(s) remaini...	

Manage License window appears.



Manage License

Licensed Computers (3)   Filter License: All

□	Machine Name	Group
□	[redacted]	Managed Computers
□	[redacted]	Managed Computers
□	[redacted]	Managed Computers\Cesar

Non-Licensed Computers (1)   Filter License: All

□	Machine Name	Group	Unlicense Date Time	Description
□	[redacted]	Managed Computers	13/08/2020 19:12:49	

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**.
4. The selected computer(s) will be moved to Licensed Computers section.

Note	Using **Filter** option in the **Manage License** section, you can view/manage the system that have add-on license activated.

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**