



CUSTOMER



MANAGEMENT
OPERATIONS



MARKETING
REPORT

eScan Enterprise EDR - Cloud User Guide

Product Version: 22.0.0000.xxxx
Document Version: 22.0.0000.xxxx

Copyright © 2021 by MicroWorld Software Services Private Limited. All rights reserved.

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

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

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

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

Document Number:	5BUG/04.08.2024/22.x
Current Software Version:	22.0.xxxx.xxxx
Technical Support:	<u>support@escanav.com</u>
Sales:	<u>sales@escanav.com</u>
Forums:	<u>https://forums.escanav.com</u>
eScan Wiki:	<u>https://wiki.escanav.com/wiki/index.php/</u>
Live Chat:	<u>https://www.escanav.com/english/livechat.asp</u>
Published by:	MicroWorld Software Services Private Limited
Date:	August, 2024

Content

Introduction.....	9
Web Console Login	10
Main Interface.....	11
Navigation Panel.....	12
Dashboard	15
Deployment Status	15
eScan Status	16
License	16
eScan version	17
Protection Status	18
Update Status	19
Scan Status	20
File Anti-Virus	20
Proactive	21
Mail Anti-Virus.....	21
Anti-Spam.....	22
Web Protection.....	22
Firewall	23
Endpoint Security.....	23
Anti – Ransomware.....	24
Protection Statistics.....	25
File Anti-Virus	26
Mail Anti-Virus.....	28
Anti-Spam.....	28
Web Protection.....	29

Endpoint Security-USB.....	29
Endpoint Security-Application	30
Summary Top 10.....	31
Asset Changes.....	32
Configure the Dashboard Display.....	33
EDR Dashboard	34
Incident - eScan.....	34
Filtering Incident – eScan Report	36
Exporting the Report.....	37
Incident-Windows.....	37
Filtering Incident – Windows Report.....	38
Exporting the Report.....	39
Incident-EDR	39
Filtering Incident – EDR Report.....	40
Exporting the Report.....	43
Endpoint Incident.....	44
Adding Specific Incident for Monitoring.....	46
Viewing the Details of the Specific Incident	47
Viewing the Details of Monitoring Incident.....	48
Deleting the Monitoring Incident.....	48
Managed Computers	49
Search.....	50
Update Agent	51
Adding an Update Agent.....	51
Delete an Update Agent	52
Action List	53
New Subgroup	53
Removing a Group.....	54

Create Client Setup	54
Properties of a group	56
Assigning a Policy to the group	57
Client Action List.....	59
Move to Group.....	60
Remove from Group	60
Refresh Client	60
Show Critical Events.....	60
Export.....	60
Show Installed Softwares.....	62
Forensic-Port/Communication	63
Create OTP.....	64
Properties of Selected Computer.....	67
Understanding the eScan Client Protection Status.....	68
Anti-Theft	69
Anti-Theft Options.....	69
Disable Anti-Theft	72
Select Columns	73
Policy Template	74
Managing Policies.....	74
Creating Policy Template for a group/specific computer	77
Configuring eScan Policies for Windows Computers	78
Configuring eScan Policies for Linux and Mac Computers	167
Assigning Policy Template to a group.....	193
Assigning Policy Template to Computer(s).....	194
Copying a Policy Template.....	195
Report Templates	196
Creating a Report Template	197

Creating Schedule for a Report Template.....	198
Viewing Properties of a Report Template.....	198
Deleting a Report Template	198
Report Scheduler.....	199
Creating a Schedule	199
Viewing Reports on Demand.....	201
Managing Existing Schedules.....	202
Generating Task Report of a Schedule	202
Viewing Results of a Schedule	202
Viewing Properties of a Schedule.....	203
Deleting a Schedule	203
Events and Computers	204
Events Status.....	204
Computer Selection.....	205
Edit Selection.....	206
Software/Hardware Changes	208
Violations.....	209
Settings.....	209
Event Status Setting.....	209
Computer Selection.....	210
Software/ Hardware Changes Setting	213
Performing an action for computer	213
Asset Management.....	214
Hardware Report.....	214
Filtering Hardware Report	215
Exporting Hardware Report.....	215
Software Report	216
Filtering Software Report.....	217

Exporting Software Report	217
Software License.....	218
Filtering Software License Report	218
Exporting Software License Report.....	219
Software Report (Microsoft).....	220
Filtering Software Report (Microsoft).....	220
Exporting Software Report (Microsoft).....	221
Filtering Microsoft OS Report	221
Exporting Microsoft OS Report.....	222
User Activity.....	223
Print Activity.....	223
Viewing Print Activity Log.....	223
Exporting Print Activity Log	223
Filtering Print Activity Log.....	224
Exporting Print Activity Report.....	225
Session Activity Report	226
Viewing Session Activity Log	226
Filtering Session Activity Log	227
Exporting Session Activity Report	227
File Activity Report	228
Viewing File Activity Log	228
Filtering File Activity Log	228
Exporting File activity Report.....	229
Application Access Report	230
Viewing Application Access Report.....	230
Filtering Application Access Report.....	231
Exporting Application Access Report.....	231
Notifications.....	232

Event Alert.....	232
Unlicensed Move Alert	234
Settings.....	235
Web Console Settings	235
Excluded Clients	237
Two-Factor Authentication (2FA)	238
Enabling 2FA login.....	239
Disabling 2FA login.....	241
Users For 2FA.....	242
Administration	244
User Accounts.....	244
Create New Account	244
Delete a User Account	245
User Roles.....	246
New Role	246
View Role Properties	248
Delete a User Role	250
Audit Trail.....	251
License	252
Adding and Activating a License.....	252
Contact Us.....	256
Forums	256
Chat Support	256
Email Support	256

Introduction

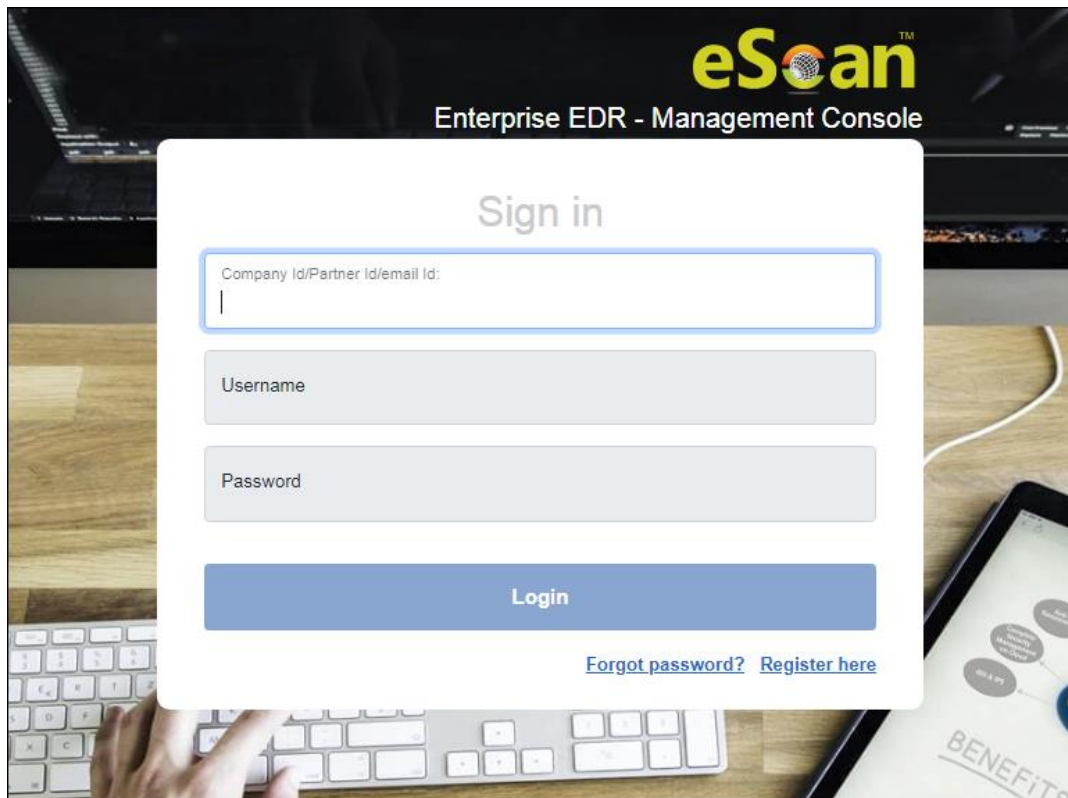
The Information Technology being the backbone of all the large corporates today, IT security is considered as a key part of business strategy by the organizations. Being aware of constantly increasing threats in the cyber-security landscape, protection of valuable intellectual property and corporate data against theft and misuse is a critical issue.

eScan Enterprise EDR (Endpoint Detection and Response)- Cloud Hosted is a comprehensive, integrated, and layered endpoint protection solution that delivers real-time visibility, analysis, protection, and remediation for endpoints. This cloud based security solution helps gaining deep insights and alerting administrators about the malicious activities in a network. This initiates fast investigation, and restricts the attacks on endpoints as soon as detected. The eScan Enterprise EDR - Cloud supports automated and manual actions to restrict the potential threats on the endpoint. It proactively reduces the attack, prevents malware infection, detects and defuses potential threats in real-time. This cloud solution is packed with cutting edge technologies that provide an ultimate protection to Windows, Mac, and Linux based endpoints in a corporate network.

Web Console Login

The web console login page can be accessed via below method:

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



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

Main Interface

The links in the top right corner are explained below:

About eScan

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

Username

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

Edit User Help

Enable this account

Account Type and Information

Custom Account

Username: root

Full Name*:

New Password:

Confirm Password:

Email Address:

For Example: user@yourcompany.com

Account Role

Role*:

(*) Mandatory Fields

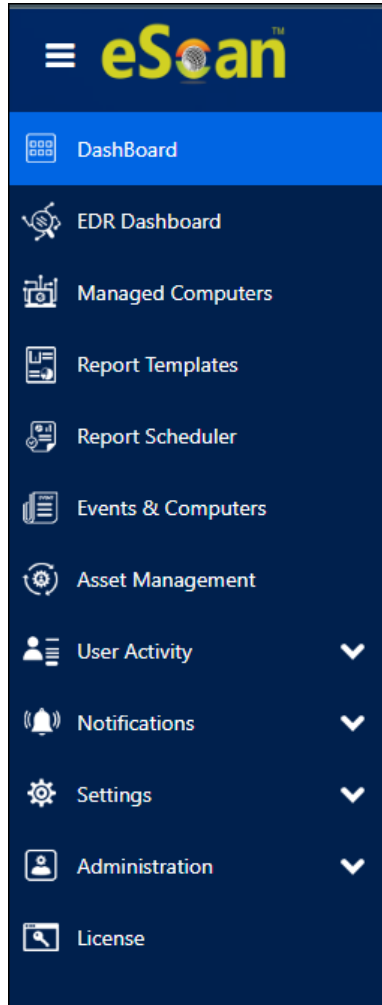
Log off

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

Company Name

This option displays user and company information.

Navigation Panel



Dashboard

The Dashboard module displays charts showing Deployment status, Protection status, Protection Statistics, Summary Top 10 and Asset Changes. The monitoring is done by Management Console of the computers for virus infections and security violations. To learn more, [click here](#).

EDR Dashboard

The EDR Dashboard provides the summary of all the malicious activities and security events gathered across the network by the eScan Server. It will provide the overview of the various incidents and the action taken on such incidents. To learn more, [click here](#).

Managed Computers

The Managed Computers module lets you define/configure Policies for computers. It provides you various options for creating groups, adding tasks, moving computers from one group to another and vice versa. To learn more, [click here](#).

Report Templates

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

Report Scheduler

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

Events and Computers

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

Asset Management

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

User Activity

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

Notifications

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

Settings

The Settings module lets you configure eScan Console timeout settings, dashboard setting, exclude client settings for eScan. To learn more, [click here](#).

Administration

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

License

The License module lets you manage licenses 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 vice-versa. To learn more, [click here](#).



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**.

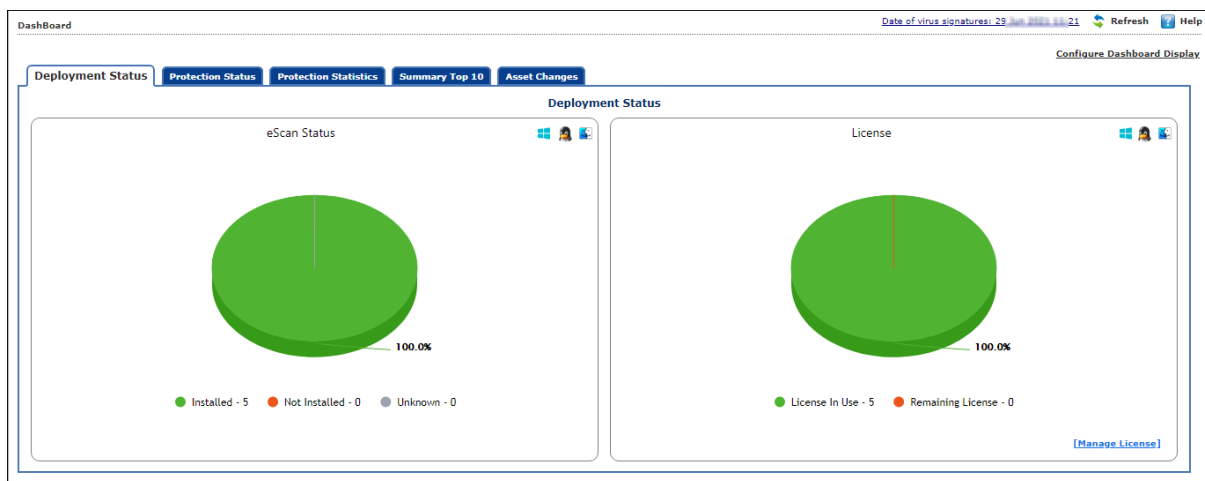
Dashboard

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

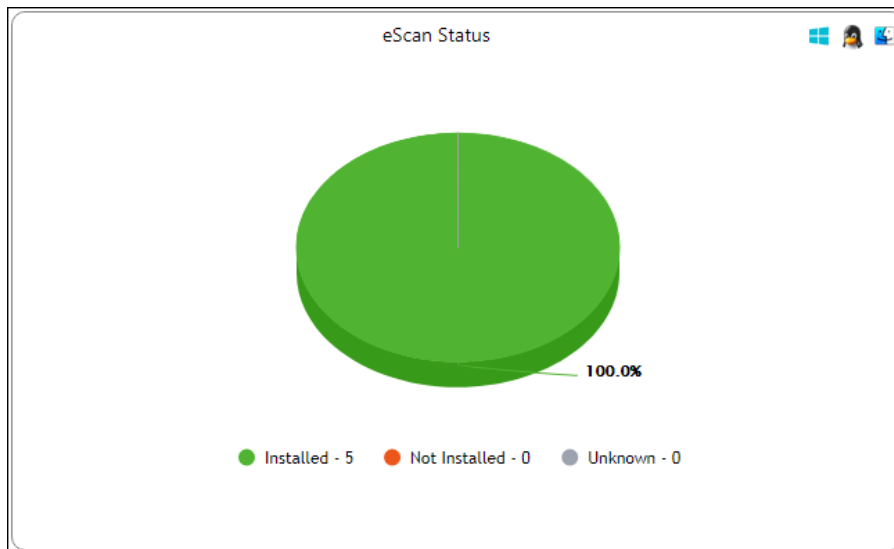
- **Deployment Status**
- **Protection Status**
- **Protection Statistics**
- **Summary Top 10**
- **Asset Changes**

Deployment Status

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



eScan Status

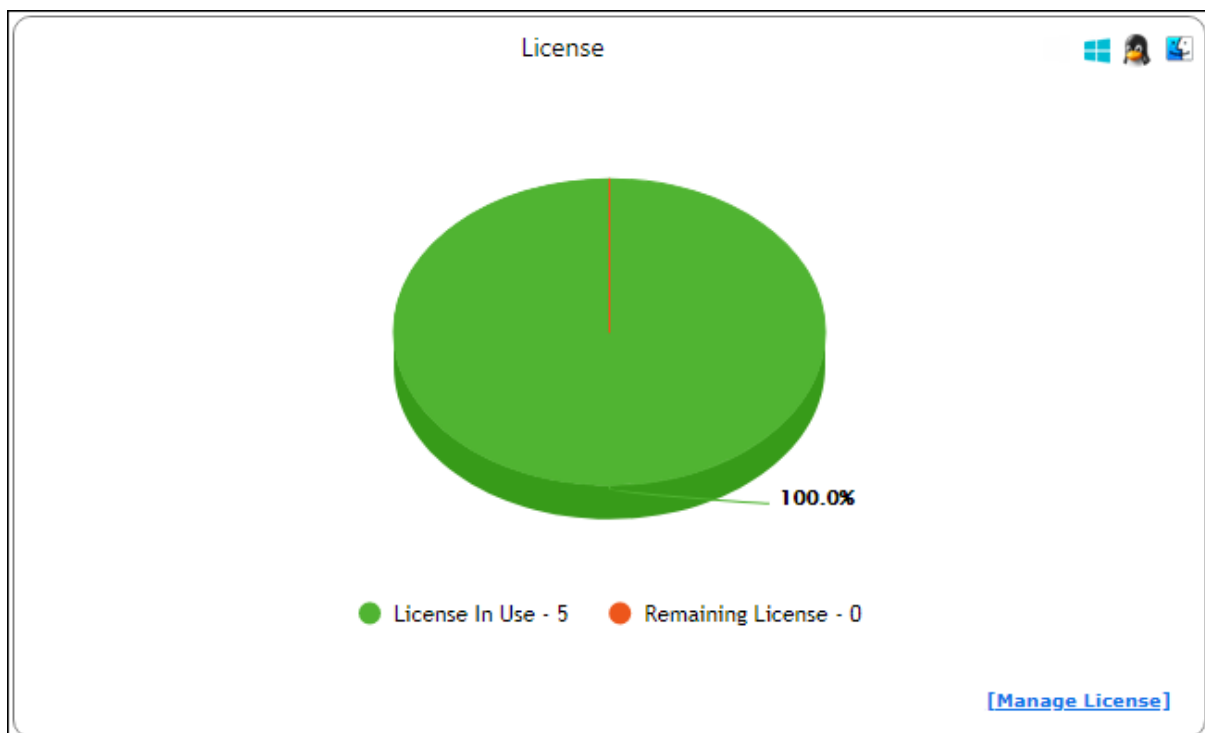


Installed – It displays the number of computers on which eScan Client is installed.

Not Installed - It displays the number of computers on which eScan Client is not installed.

Unknown - It displays the number of computers on which Client installation status is unknown.
(eScan Cloud is unable to receive information from the computers for a long time)

License

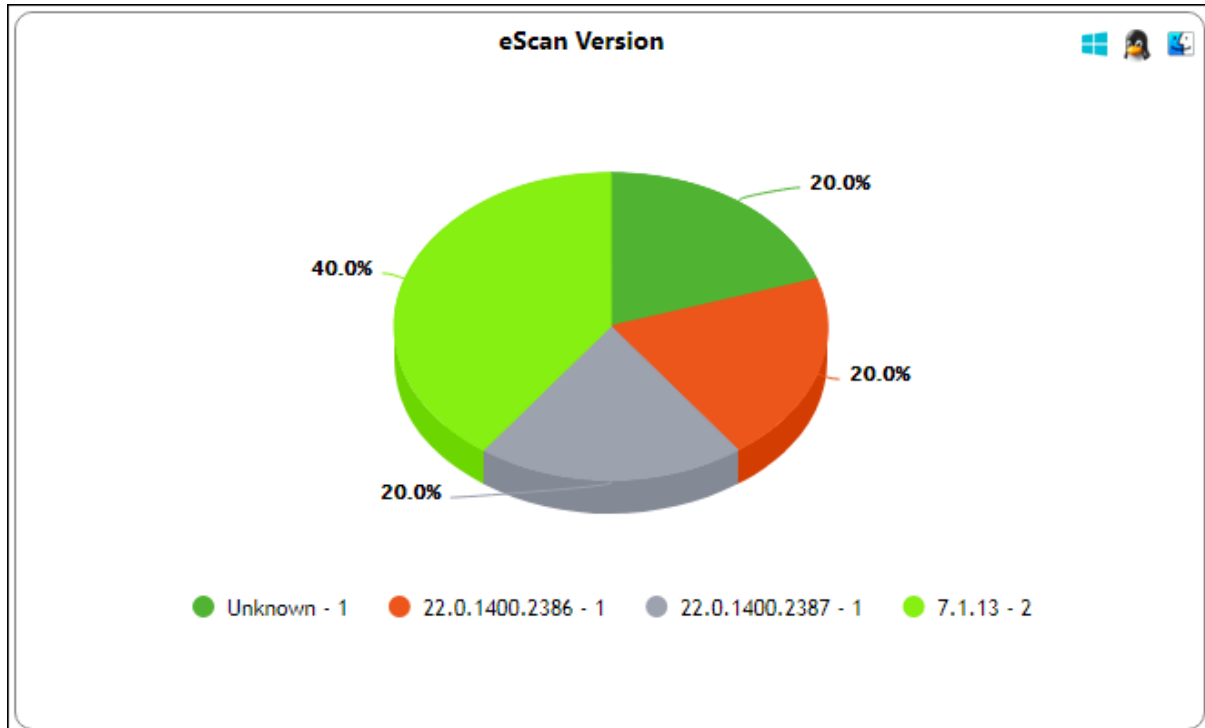


License in Use - It displays the number of licenses that are active.

Licenses Remaining - It displays the number of remaining licenses.

eScan version

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



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

Deployment Status >> eScan Version

Client OS Type: Print

Machine Name	Version	Group
SERVER	22.0.1400.2386	Managed Computers
WI...	14.0.1400.2386	Managed Computers

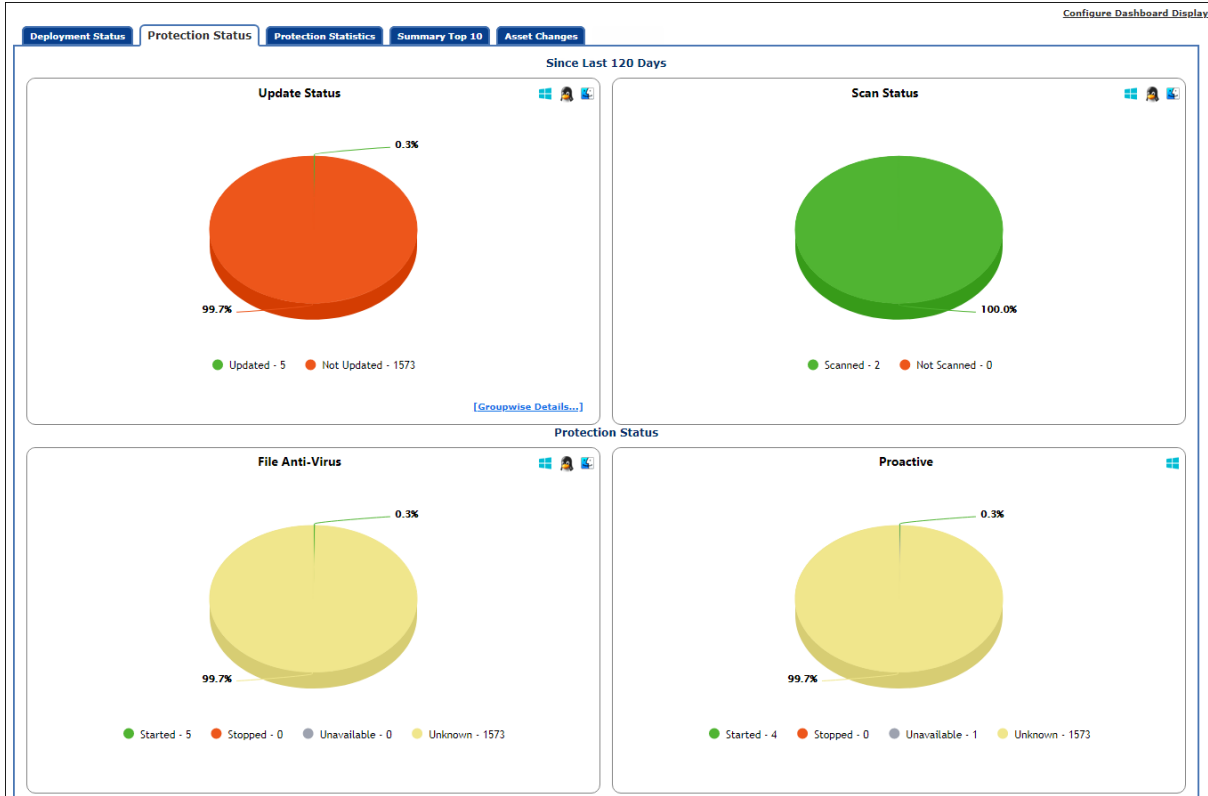
Close

NOTE Clicking underlined numerical displays detailed information for computers.

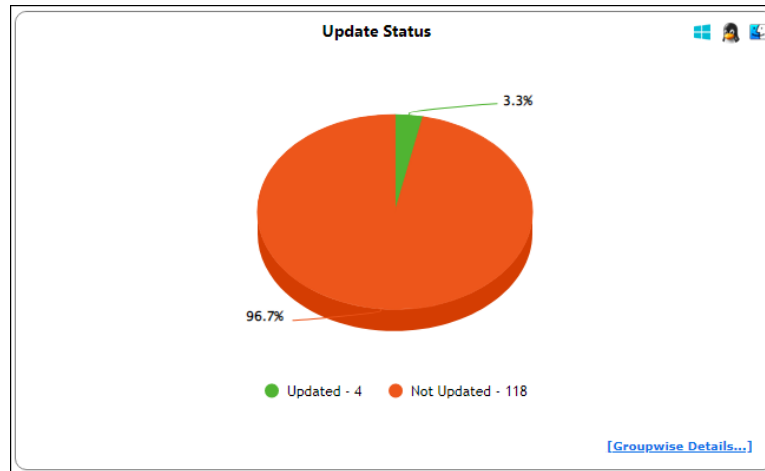
The Windows, Mac, Linux Icons at the top of every chart denote that the information is displayed for the respective Operating Systems (OS).

Protection Status

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



Update Status



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.

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

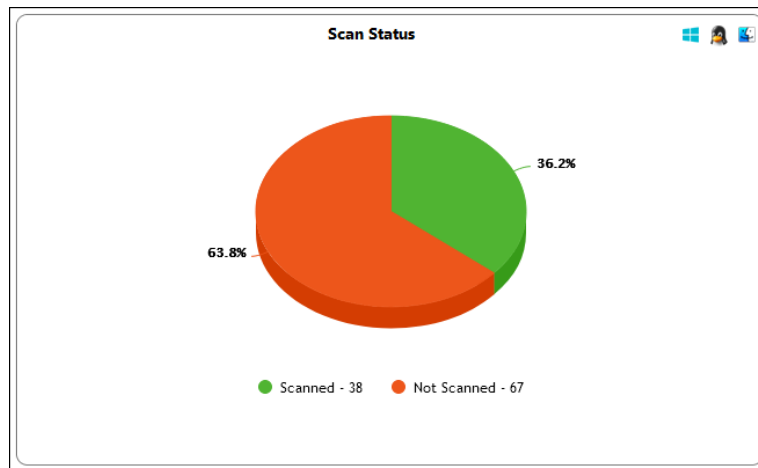
Groupwise Update Status Tuesday, June

Managed Computers Include Sub Groups Groupwise Details Print

Group: Managed Computers (Include Sub Groups)										
Group Name	Updated	Not Updated	License in Use	EP	EQ	CP	CO	IL	NA	
Managed Computers	2	0	2	1	0	1	0	0	0	
EP_TEAM	0	1	1	0	0	0	0	0	1	
TEAM	1	0	1	0	0	1	0	0	0	
Samples_Team	1	0	1	0	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** checkbox will display the subgroups containing computers.

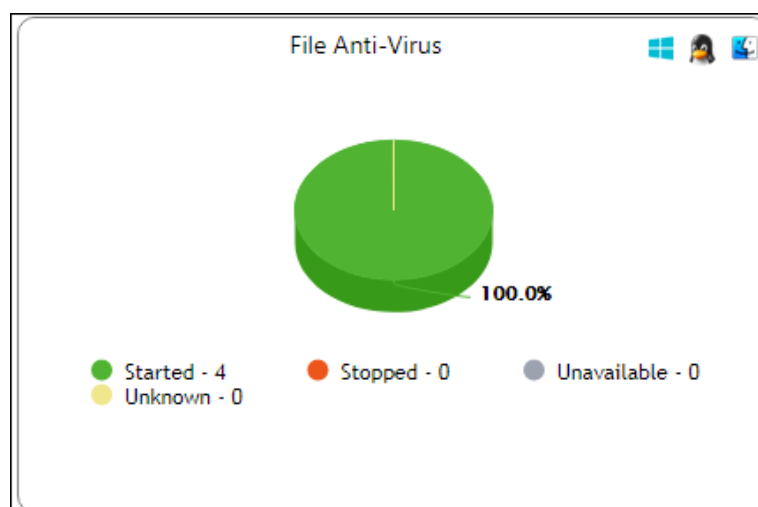
Scan Status



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.

File Anti-Virus



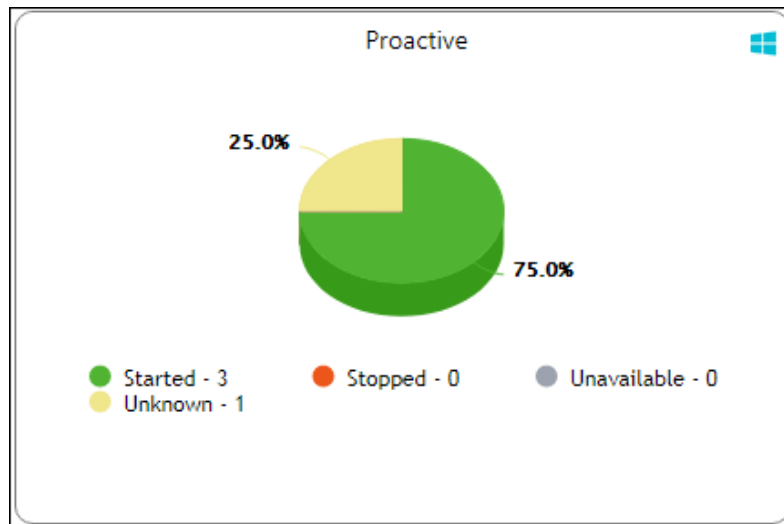
Started – It displays the number of computers on which the File Anti-Virus module is in Started state.

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.

Proactive



Started - It displays the number of computers on which Proactive scanning service is running.

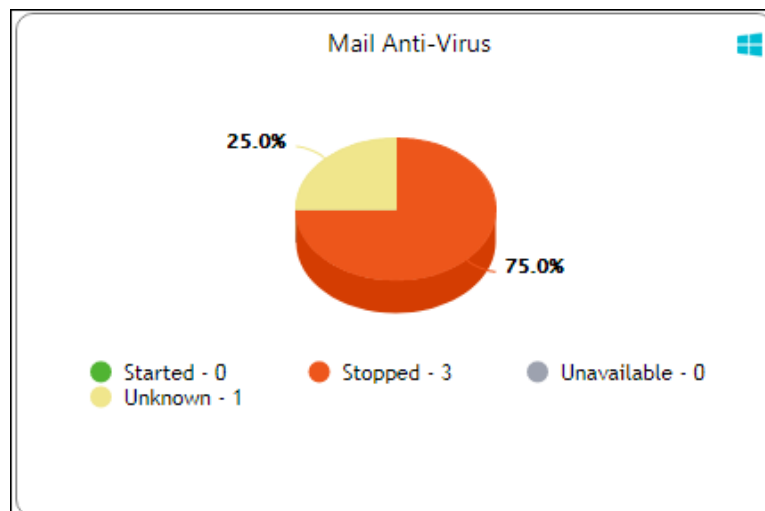
Stopped - It displays the number of computers on which Proactive scanning service is stopped.

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.

Mail Anti-Virus



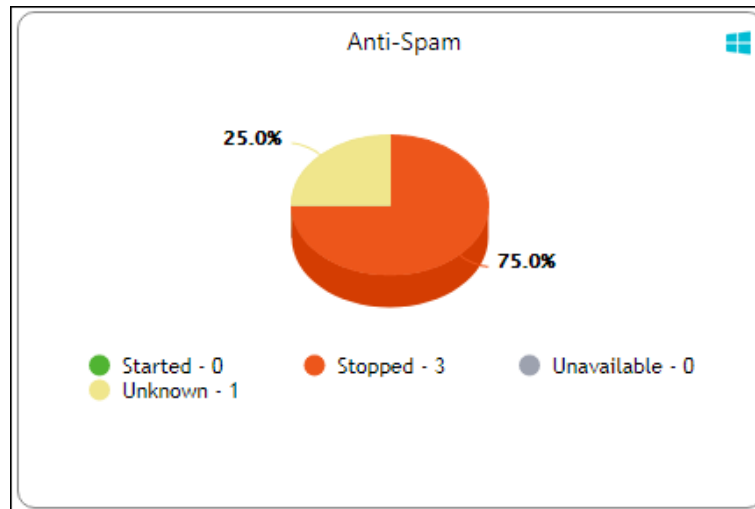
Started – It displays the number of computers on which the Mail Anti-Virus module is in Started state.

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.

Anti-Spam



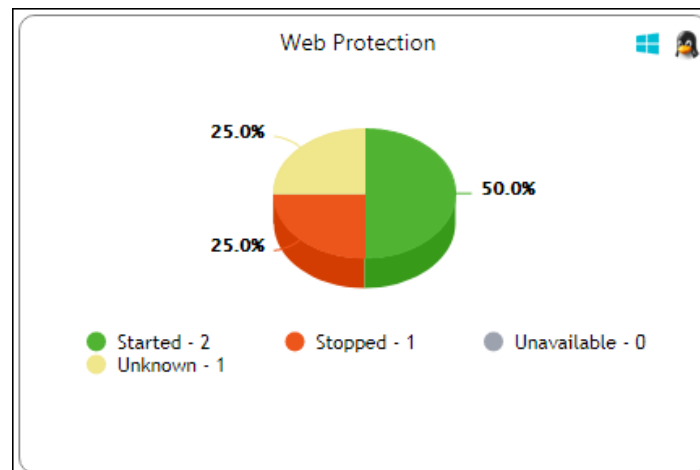
Started – It displays the number of computers on which the Anti-Spam module is in Started state.

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.

Web Protection



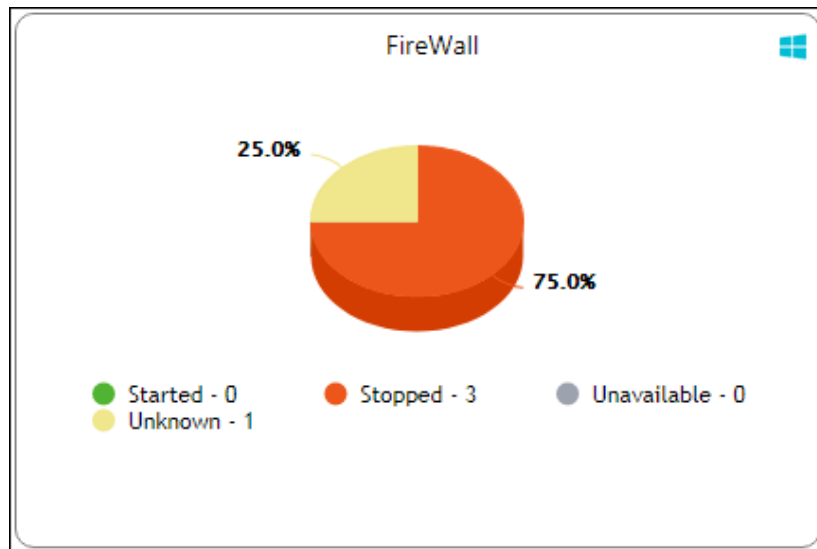
Started – It displays the number of computers on which the Web Protection module is in Started state.

Stopped – It displays the number of computers on which the Web Protection module is in Stopped state.

Unavailable – It displays the number of computers on which the Web Protection module is unavailable.

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

Firewall



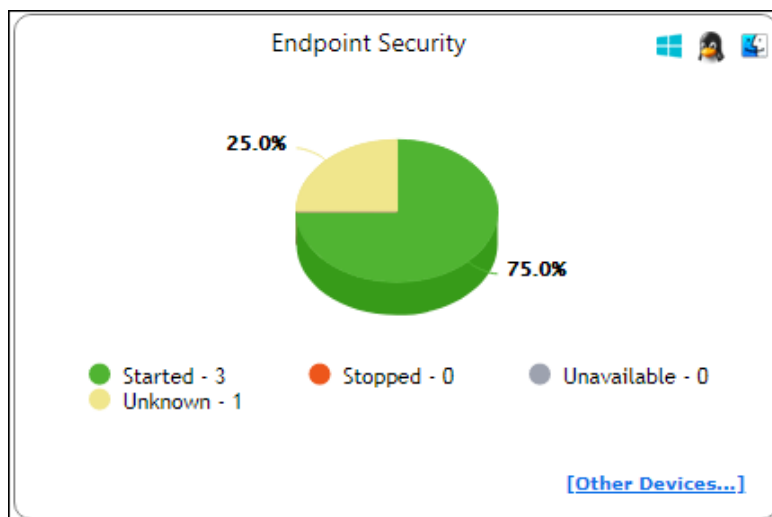
Started - It displays the number of computers on which the Firewall module is in Started state.

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.

Endpoint Security



Started - It displays the number of computers on which the Endpoint Security module is in Started state.

Stopped - It displays the number of computers on which the Endpoint Security module is in Stopped state.

Unavailable – It displays the number of computers on which the Endpoint Security module is unavailable.

Unknown - It displays the number of computers on which the Endpoint Security module status is unknown.

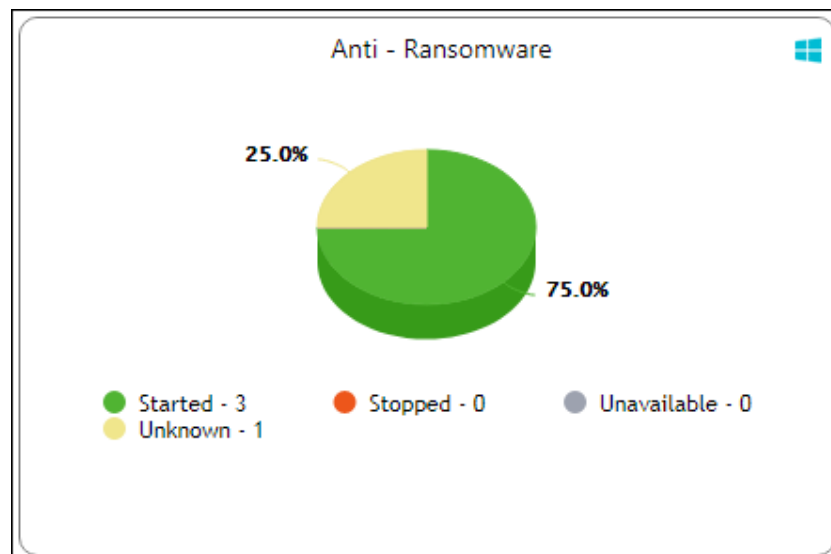
Clicking **Other Devices** displays details about other devices.

Other Devices Status

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

Close

Anti – Ransomware



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

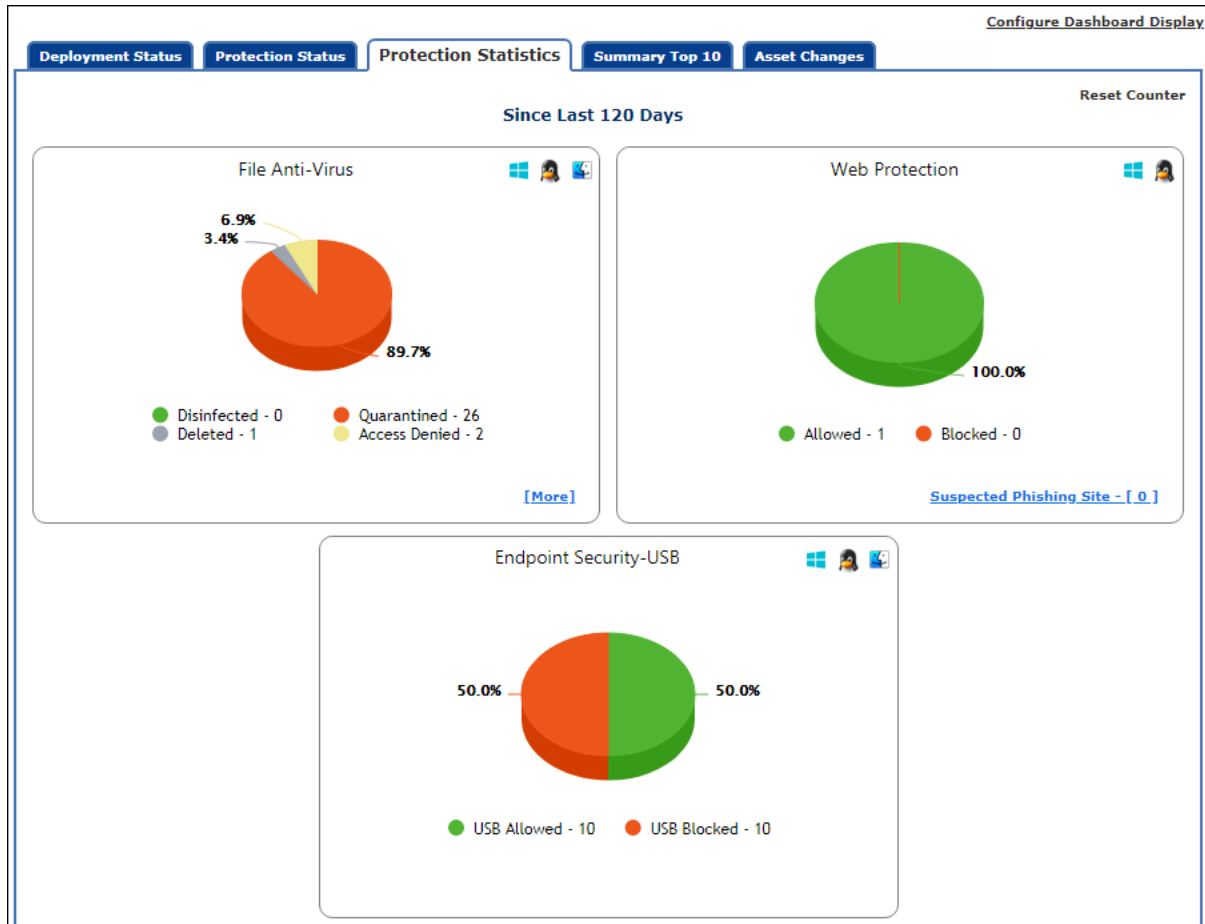
Stopped - It displays the number of computers on which the Anti – Ransomware module is in Stopped state.

Unavailable – It display the number of computers on which the Anti – Ransomware module unavailable to system.

Unknown - It displays the number of computers on which the Anti – Ransomware module status is unknown.

Protection Statistics

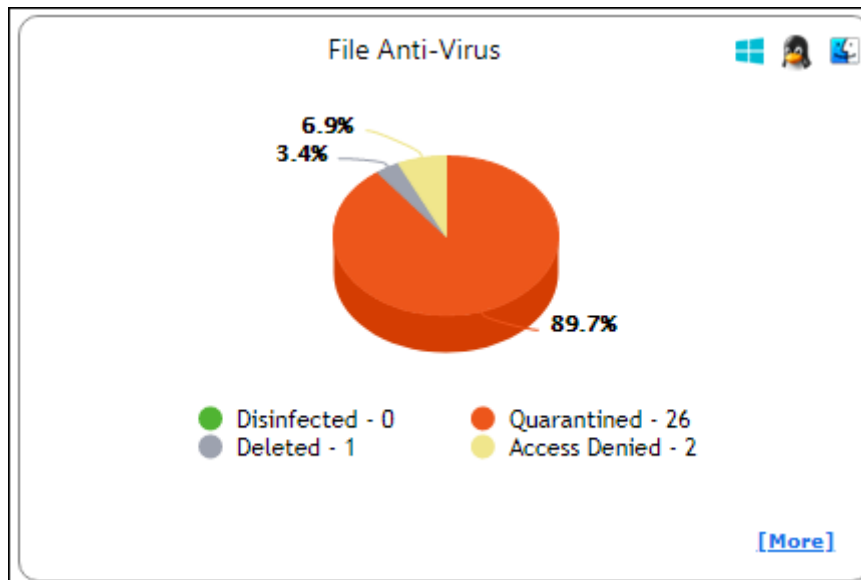
This tab displays activity statistics and action taken by all modules of eScan Client since last seven days in pie chart format.



Reset Counter

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

File Anti-Virus



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.

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

Protection Statistics >> File Anti-Virus >> Quarantined

Client OS Type: All

Machine Name	Status	Group
ESC-WK-CLIENT	Quarantined (2)	Managed Computers\Samples_Team
WIN-ESCANSERVER	Quarantined (14)	Managed Computers
WIN-QADSP	Quarantined (10)	Managed Computers\QA_TEAM

Print

Close

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

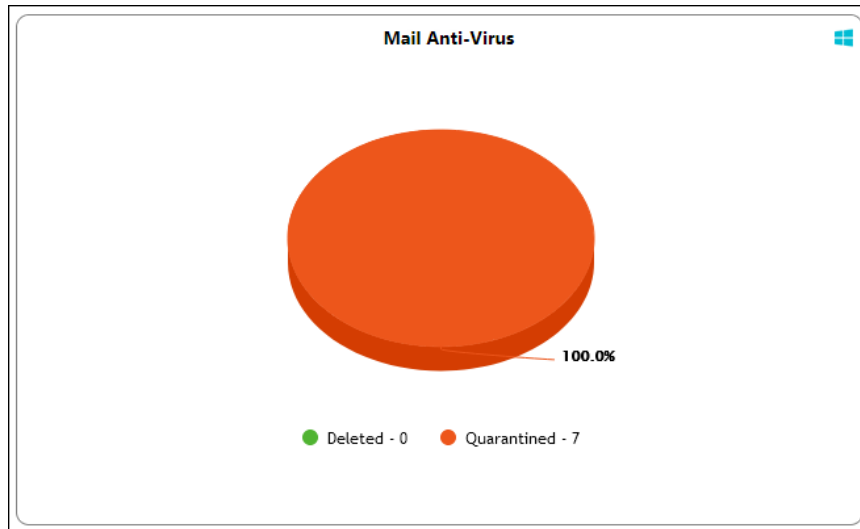
Protection Statistics >> File Anti-Virus >> Quarantined (WIN ESCANSERVER)			
Date/Time	File Name	Description	User name
23/06/21 10:53:14	\\192.168.0.30\external\temp\Prashant\samples\zdco.exe	Infected by Virus: Trojan.GeneticD.46139132 (38)	WIN- ESCANSEVER\Administrator
23/06/21 10:53:15	\\192.168.0.30\external\temp\Prashant\samples\zdfj.exe	Infected by Virus: Trojan.GeneticD.46137615 (38)	WIN- ESCANSEVER\Administrator
23/06/21 10:53:16	\\192.168.0.30\external\temp\Prashant\samples\zest.exe	Infected by Virus: Trojan.GeneticD.46136142 (38)	WIN- ESCANSEVER\Administrator
23/06/21 10:53:16	\\192.168.0.30\external\temp\Prashant\samples\znotification.exe	Infected by Virus: Trojan.AutoRun.GeneticD.46136404 (38)	WIN- ESCANSEVER\Administrator
23/06/21 10:53:16	\\192.168.0.30\external\temp\Prashant\samples\zdfh.exe	Infected by Virus: Trojan.GeneticD.46132768 (38)	WIN- ESCANSEVER\Administrator

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

Additional protection statistics	
Malware URL Block	2
Autorun Block	0
Executable Block USB	0
Executable Block Network	0
Executable Block User based	4
Proactive Statistics: Allow	0
Proactive Statistics: Block	2
Exploit Statistics Block	0
Ransomware Statistics Block	7
Total	15

Close

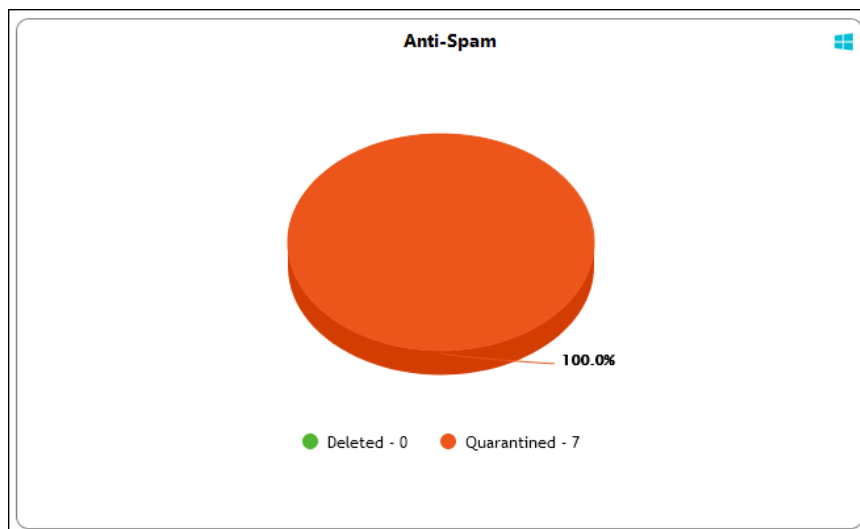
Mail Anti-Virus



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.

Anti-Spam



Deleted – It displays the number of files deleted by Anti-Spam module.

Quarantined – It displays the number of files quarantined by Anti-Spam module.

Web Protection

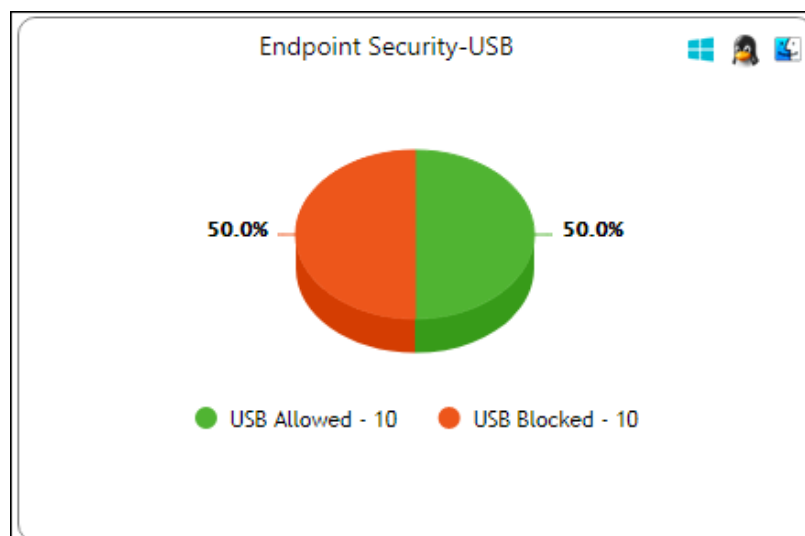


Allowed – It displays the number of websites to which access was allowed by Web Protection module.

Blocked – It displays the number of websites to which access was blocked by Web Protection module.

Suspected Phishing Site – It displays the number of systems on which suspected phishing sites were blocked. After clicking the numerical, Suspected Phishing Site window appears displaying System Name, Site Status, and Computer Group. Clicking Site Status further displays Date, Time, Website name and action taken.

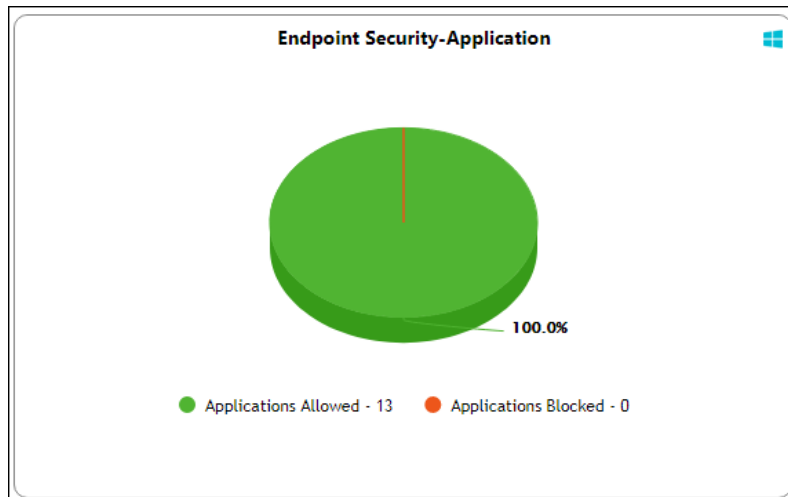
Endpoint Security-USB



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

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

Endpoint Security-Application

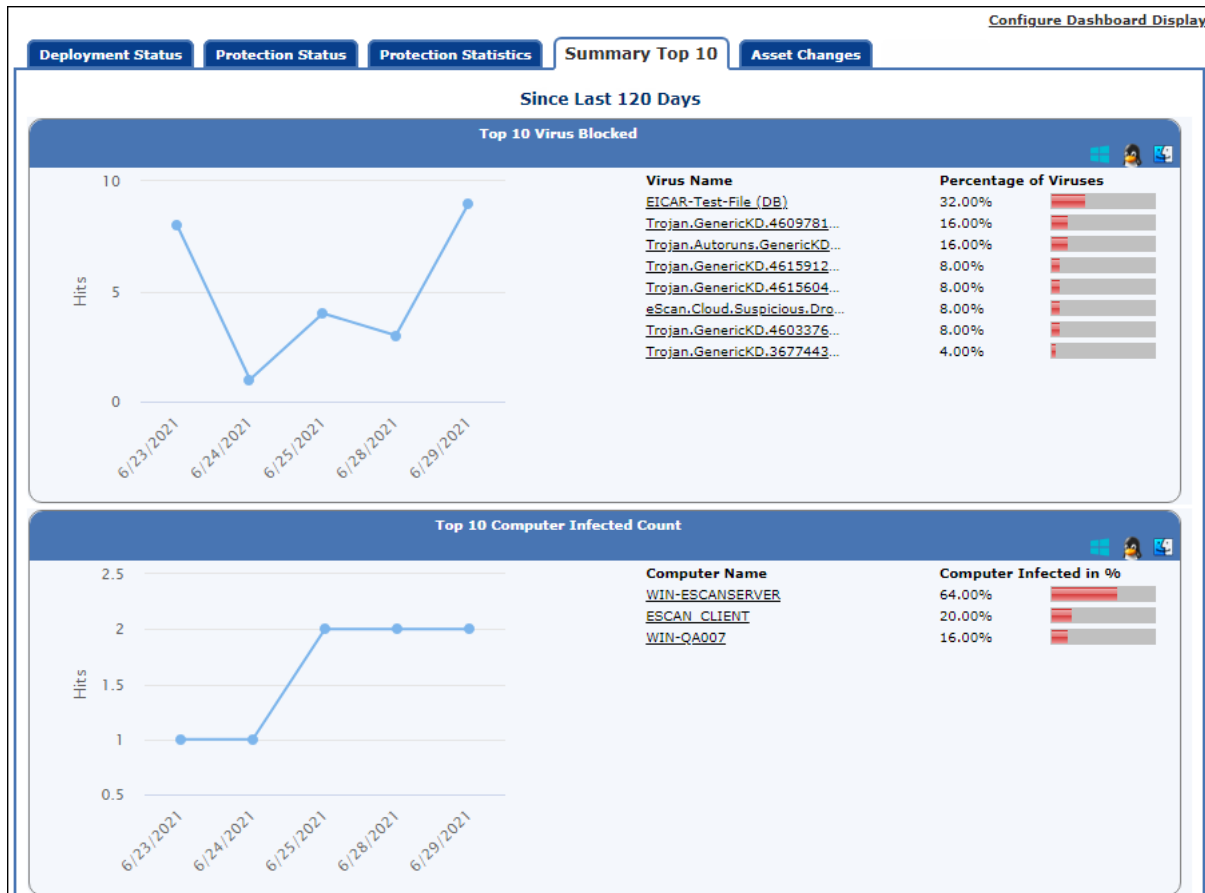


Applications Allowed – It displays the number of applications allowed by Endpoint Security-Application module.

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

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 Virus Blocked
- Top 10 Computer Infected Count
- 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 Blocked Count by Username
- Top 10 Websites Allowed Count by Username
- Top 10 Exploit Blocked Count

Asset Changes

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

[Configure Dashboard Display](#)

Deployment Status
Protection Status
Protection Statistics
Summary Top 10
Asset Changes

Since Last 120 Days

Hardware Changes

Description	Machine Count
RAM	<u>1</u>
CPU	0
MOTHERBOARD	0
HARD DISK	0

Software Changes

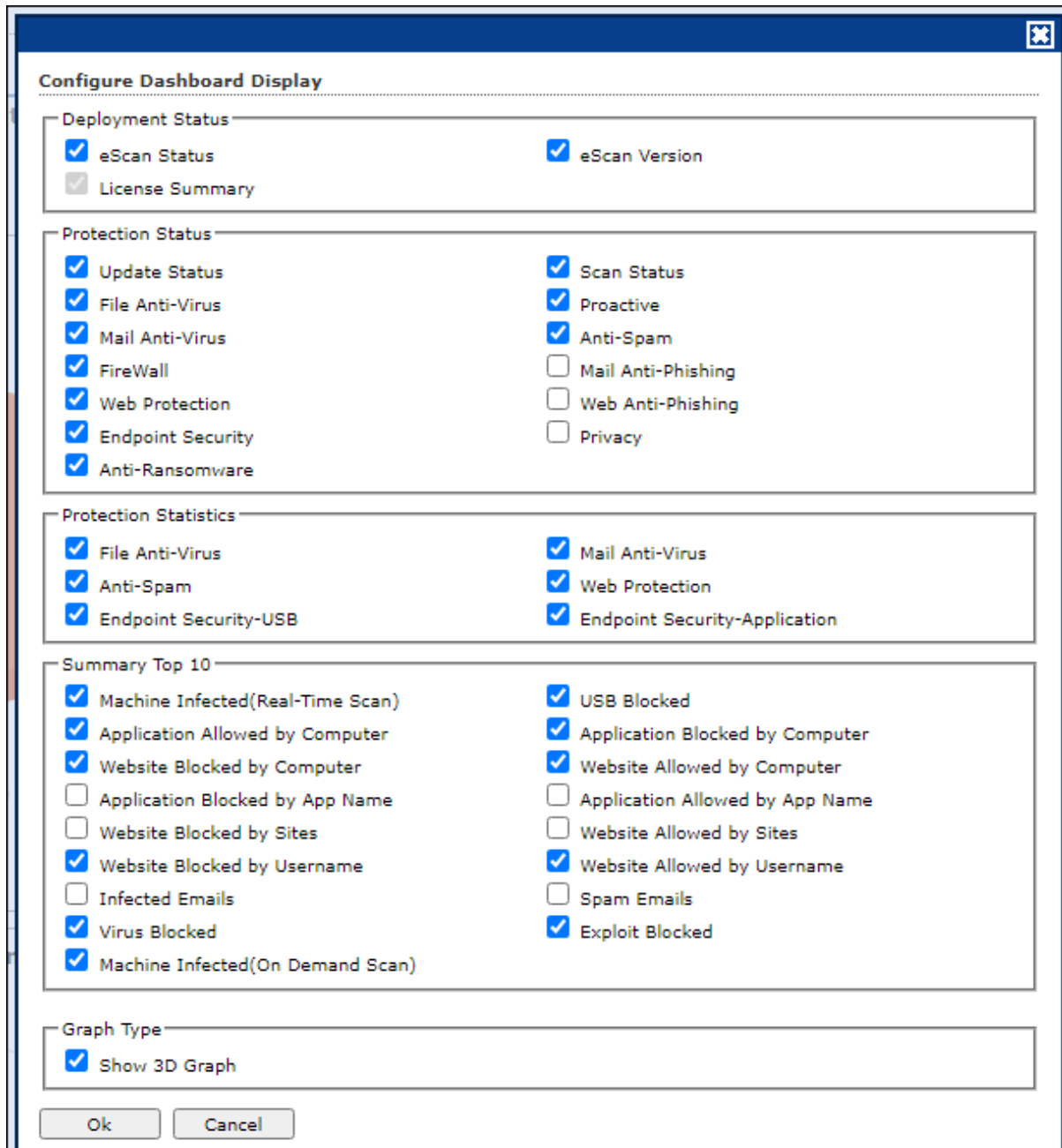
Machine Name	New Installed Softwares	Uninstalled Softwares
<u>WIN-SCANSERVER01</u>	<u>1</u>	0
<u>WIN-SCANSUP</u>	<u>2</u>	<u>1</u>

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
- License Summary
- eScan Version

Protection Status

- Update Status
- File Anti-Virus
- Mail Anti-Virus
- FireWall
- Web Protection
- Endpoint Security
- Anti-Ransomware
- Scan Status
- Proactive
- Anti-Spam
- Mail Anti-Phishing
- Web Anti-Phishing
- Privacy

Protection Statistics

- File Anti-Virus
- Anti-Spam
- Endpoint Security-USB
- Mail Anti-Virus
- Web Protection
- Endpoint Security-Application

Summary Top 10

- Machine Infected(Real-Time Scan)
- Application Allowed by Computer
- Website Blocked by Computer
- Application Blocked by App Name
- Website Blocked by Sites
- Website Blocked by Username
- Infected Emails
- Virus Blocked
- Machine Infected(On Demand Scan)
- USB Blocked
- Application Blocked by Computer
- Website Allowed by Computer
- Application Allowed by App Name
- Website Allowed by Sites
- Website Allowed by Username
- Spam Emails
- Exploit Blocked

Graph Type

- Show 3D Graph

Ok Cancel

2. Select the parameters' checkboxes to be displayed in the respective tabs.
3. Click **OK**.
The tabs will be updated according to the changes.

EDR Dashboard

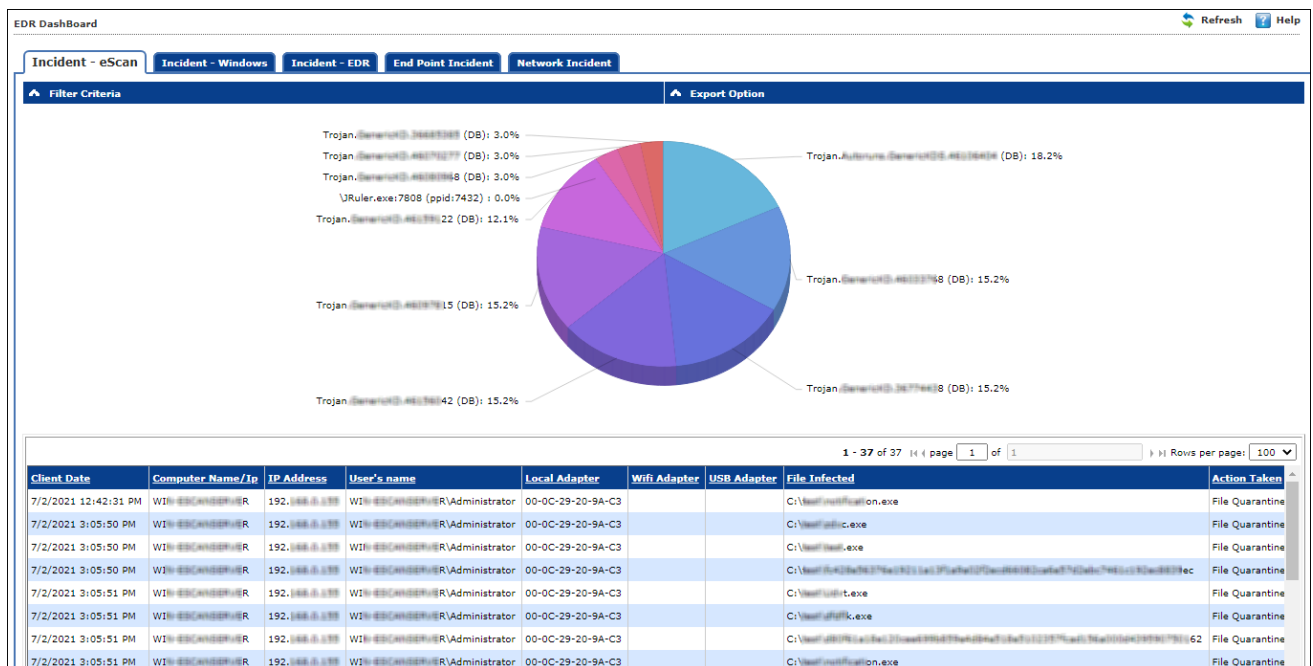
The EDR dashboard is primarily used to keep track of malicious activities and potential attacks by keeping a close eye on network. It analyses the detected threat and helps to determine the root cause of attacks. The EDR dashboard consists of different tabs having multiple summary reports that are as follows:

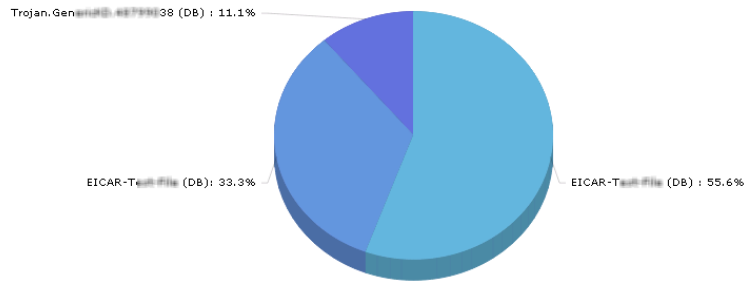
- Incident-eScan
- Incident-Windows
- Incident-EDR
- Endpoint Incidents

eScan EDR dashboard provides centralized summary of potential threats and malicious activities from all the endpoints in the network.

Incident - eScan

Incident-eScan tab displays the summary information about the different malware detected by eScan, along with action taken and graphical representation of the same.





1 - 9 of 9 (page 1 of 1) Rows per page: 10

	Action Taken	Description	Mitre
Templatus.com	File Quarantined	Infected by Virus: EICAR-Test File (DB) [0002-275af12330f64e0fa54e7509f7db4dca3fa75e2e3c0f5ba6f50d1f 52-68]	View
7307facbd99f5d7706b0d33c794	File Quarantined	Infected by Virus: Trojan.Genus#0.48799 (DB) [0002-d8bc0b7e0b52e7307facbd99f5d7706b0d33c794 52-725295]	View
ocal.Templatus.com	File Quarantined	Infected by Virus: EICAR-Test File (DB) [0002-275af12330f64e0fa54e7509f7db4dca3fa75e2e3c0f5ba6f50d1f 52-68]	View
	File Quarantined	Infected by Virus: EICAR-Test File (DB)	View
	File Quarantined	Infected by Virus: EICAR-Test File (DB)	View
	File Quarantined	Infected by Virus: EICAR-Test File (DB)	View
ocal.Templatus.com	File Quarantined	Infected by Virus: EICAR-Test File (DB) [0002-275af12330f64e0fa54e7509f7db4dca3fa75e2e3c0f5ba6f50d1f 52-68]	View
ocal.Templatus.com	File Quarantined	Infected by Virus: EICAR-Test File (DB) [0002-275af12330f64e0fa54e7509f7db4dca3fa75e2e3c0f5ba6f50d1f 52-68]	View
ocal.Templatus.com	File Quarantined	Infected by Virus: EICAR-Test File (DB) [0002-275af12330f64e0fa54e7509f7db4dca3fa75e2e3c0f5ba6f50d1f 52-68]	View

Filtering Incident – eScan Report

To filter the Incident – eScan as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

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

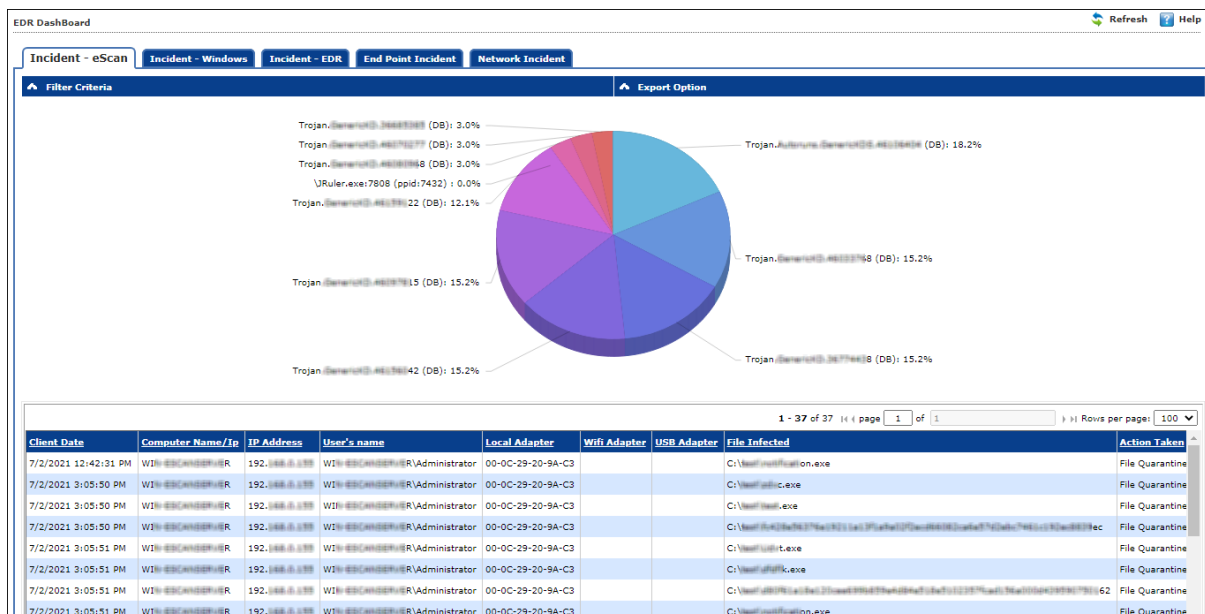
Include/Exclude

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

After making the necessary selections, click **Search**.

The Incident – eScan will be filtered according to your preferences.

In the below instance, after applying filter the following type of the summary report will be generated. It consists of general information such as Client Date, Computer Name / IP, IP Address, User Name, Event Description, Action Taken, etc.



Exporting the Report

To export the Incident – eScan Report, click **Export Option**.
Export Option field expands.

Export Option
 Excel
 PDF
 HTML
 Export

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



Click the link to open/download the file.

Incident-Windows

Incident-Windows tab provides the details of the Windows events such as RDP access, Windows logon, and more. eScan EDR monitors failed login attempts made using dictionary attacks, brute force attacks, and various other methods. It also generates the summary report of the information collected from all the eScan endpoints in the network.

EDR Dashboard
Refresh Help

Incident - eScan
Incident - Windows
Incident - EDR
End Point Incident
Network Incident

Filter Criteria
Export Option

1 - 10 of 10
1 of 1
Rows per page: 100

Client Date	Computer Name/Ip	IP Address	User's name	Event Description	Event
7/5/2021 10:34:09 AM	WIN-Q4007	192.168.0.85	WIN-Q4007\qa	The server accepted a new TCP connection from client 192.168.0.139:44626	Logged [131]
7/5/2021 10:34:15 AM	WIN-ESCANSERVER	192.168.0.139	WIN-ESCANSERVER\Administrator	A logon was attempted using explicit credentials	Logged [4648]
7/5/2021 10:34:16 AM	WIN-Q4007	192.168.0.85	WIN-Q4007\qa	The server accepted a new TCP connection from client 192.168.0.139:44627	Logged [131]
7/5/2021 10:34:17 AM	WIN-ESCANSERVER	192.168.0.139	WIN-ESCANSERVER\Administrator	A logon was attempted using explicit credentials	Logged [4648]
7/5/2021 10:34:17 AM	WIN-Q4007	192.168.0.85	WIN-Q4007\qa	The server accepted a new UDP connection from client [192.168.0.139]:43050	Logged [131]
7/5/2021 10:34:17 AM	WIN-Q4007	192.168.0.85	WIN-Q4007\qa	Remote Desktop Services: User authentication succeeded:	Logged [1149]
7/5/2021 10:34:17 AM	WIN-Q4007	192.168.0.85	WIN-Q4007\qa	The server accepted a new UDP connection from client [192.168.0.139]:43050	Logged [131]
7/5/2021 10:34:25 AM	WIN-Q4007	192.168.0.85	WIN-Q4007\qa	A logon was attempted using explicit credentials	Logged [4648]

Filtering Incident – Windows Report

To filter the Incident – Windows as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

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 Incident – Windows will be filtered according to your preferences.

In the below instance, after applying filter the following type of the summary will be generated. It displays general information such as Client Date, Computer Name / IP, IP Address, User Name, Event Description, and Event will be displayed.

Summary Data:

Event Description	Percentage
A logon was attempted using explicit credentials	40.0%
An account failed to log on	10.0%
Remote Desktop Services: User authentication succeeded	10.0%
The server accepted a new TCP connection from client 192.168.0.135	10.0%
The server accepted a new TCP connection from client 192.168.0.135	10.0%
The server accepted a new UDP connection from client :63050	10.0%
The server accepted a new UDP connection from client :63051	10.0%

Client Date	Computer Name / Ip	IP Address	User's name	Event Description	Event
7/5/2021 10:34:09 AM	WIN-Q40071qa	192.168.0.85	WIN-Q40071qa	The server accepted a new TCP connection from client 192.168.0.135-64626	Logged [131]
7/5/2021 10:34:15 AM	WIN-ESCHAMBER-ER	192.168.0.135	WIN-ESCHAMBER-ER\Administrator	A logon was attempted using explicit credentials	Logged [4648]
7/5/2021 10:34:16 AM	WIN-Q40071qa	192.168.0.85	WIN-Q40071qa	The server accepted a new TCP connection from client 192.168.0.135-64627	Logged [131]
7/5/2021 10:34:17 AM	WIN-ESCHAMBER-ER	192.168.0.135	WIN-ESCHAMBER-ER\Administrator	A logon was attempted using explicit credentials	Logged [4648]
7/5/2021 10:34:17 AM	WIN-Q40071qa	192.168.0.85	WIN-Q40071qa	The server accepted a new UDP connection from client [192.168.0.135]-43039	Logged [131]
7/5/2021 10:34:17 AM	WIN-Q40071qa	192.168.0.85	WIN-Q40071qa	Remote Desktop Services: User authentication succeeded	Logged [1149]
7/5/2021 10:34:17 AM	WIN-Q40071qa	192.168.0.85	WIN-Q40071qa	The server accepted a new UDP connection from client [192.168.0.135]-43038	Logged [131]
7/5/2021 10:34:25 AM	WIN-Q40071qa	192.168.0.85	WIN-Q40071qa	A logon was attempted using explicit credentials	Logged [4648]

Exporting the Report

To export the Incident – Windows 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.



Click the link to open/download the file.

Incident-EDR

Incident-EDR tab provides the summary report of all the events from the endpoints in the network on the basis of severity for advanced investigation and response. It blocks/remove the suspicious files and then alerts the admin for further investigation and analysis of it.

EDR Dashboard

Incident - eScan Incident - Windows Incident - EDR End Point Incident Network Incident

Filter Criteria Export Option

Report Type: select report type

Filter: * Include

Computer Name: * Include

From: 07/01/2021

To: 07/01/2021

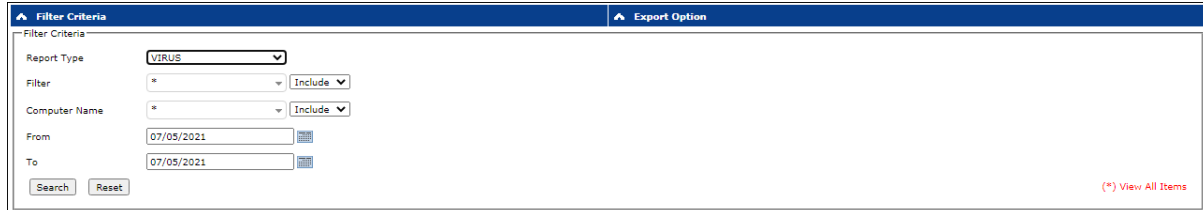
Search Reset (*) View All Items

0 - 0 of 0 rows per page: 10

Client Date and Time	Computer Name/Ip	IP Address	User's name	Event Description	Action Taken
There are no items to show in this view.					

Filtering Incident – EDR Report

To filter the Incident – EDR as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.



eScan EDR solution provides different types of report such as Virus, PowerShell, and many more based on the different types of threats and malicious activities. The admin can select the report from the drop-down menu according to the requirement and get the detailed report about the same. The types of reports are as follow:

- VIRUS
- PowerShell Blocked
- MMC Blocked
- MSHTA Blocked
- RunDLL32 Blocked
- NetCmd Blocked
- Sensitive OS-File Execution Blocked
- MSOffice Child EXE Blocked
- Unsigned USB EXE Blocked
- Adobe Child EXE Blocked
- ProgramData / Users Execution Blocked
- Unsigned Cloud EXE Blocked
- PBAE
- Ransomware Blocked
- Disconnected Bruteforcing IP
- Disconnected Prohibited IP
- Password Archive: Blocked
- User: Blocked

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

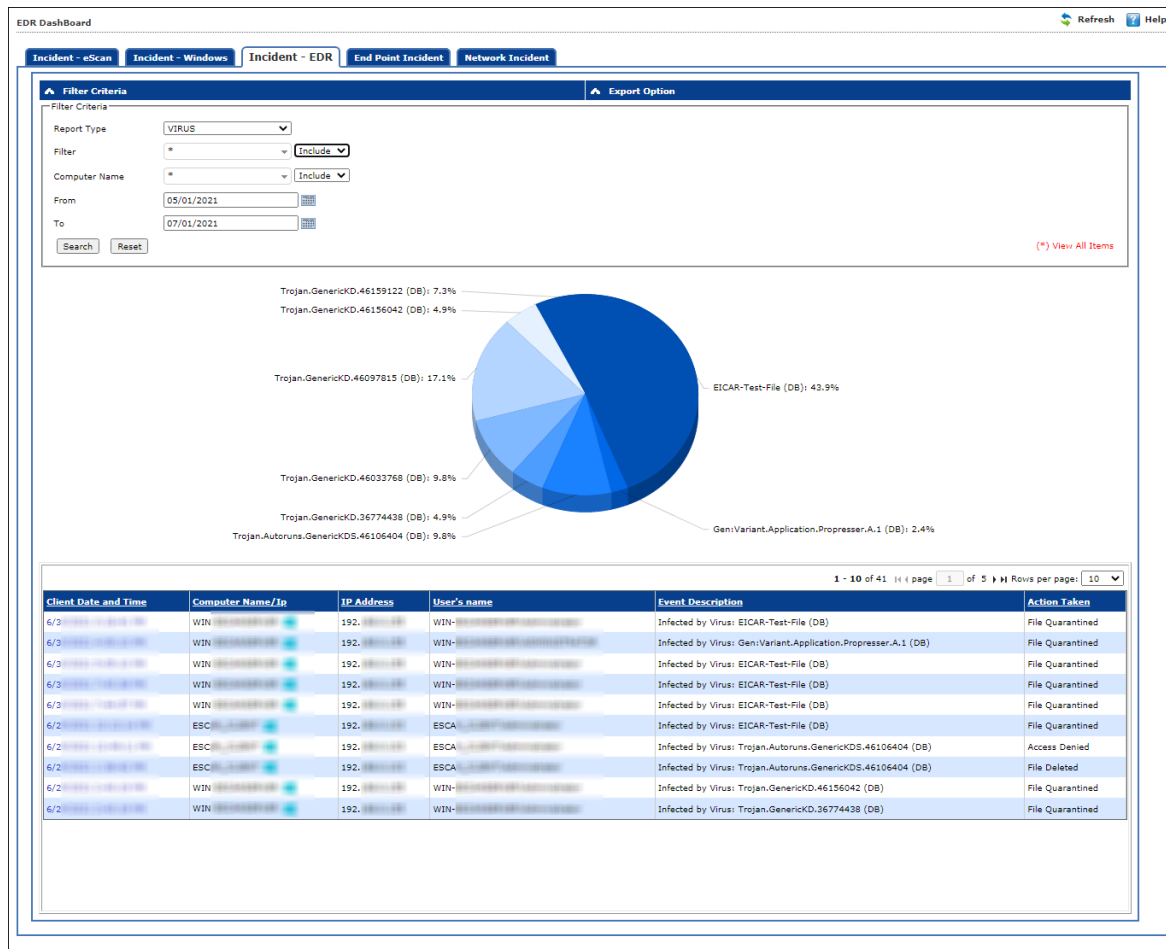
Include/Exclude

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

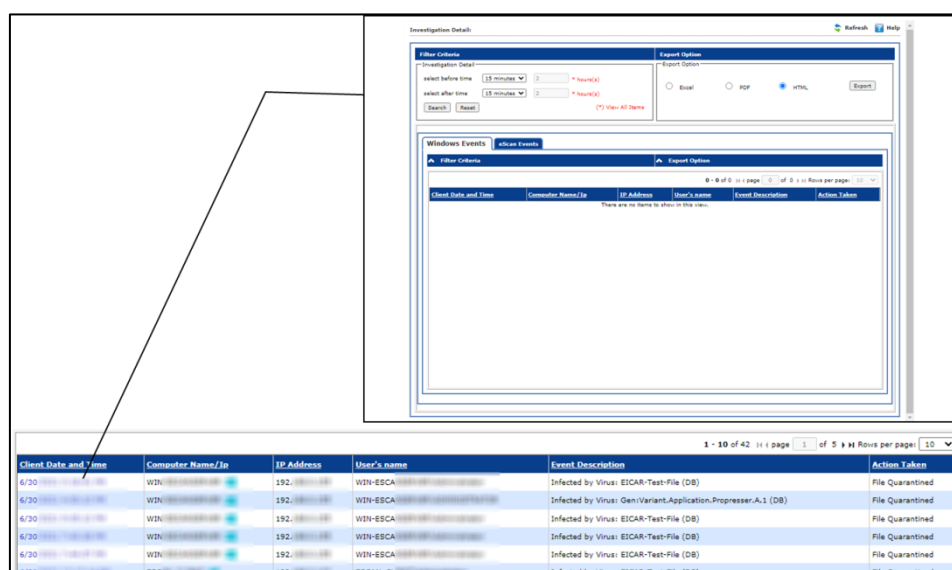
After making the necessary selections, click **Search**.

The Incident – EDR will be filtered according to your preferences.

Following figure gives the summary of the virus report:



To get the detailed investigation report for a specific incident, click the hyperlink under **Client Date and Time**, as shown below:



The detailed report will be generated.

Windows Events					
Filter Criteria			Export Option		
1 - 2 of 2 (< page 1 of 1 >) Rows per page: 100					
Client Date and Time	Computer Name/Ip	IP Address	User's name	Event Description	Action Taken
07/05/2021 10:34:17	WIN-E8C4N88P8R	192.168.0.101	WIN-E8C4N88P8R\Administrator	A logon was attempted using explicit credentials	Logged
07/05/2021 10:34:15	WIN-E8C4N88P8R	192.168.0.101	WIN-E8C4N88P8R\Administrator	A logon was attempted using explicit credentials	Logged

Windows Events: It displays the Windows event for the filtered time frame.

eScan Events: It displays the eScan events for the filtered time frame.

Network Incident: It displays the Network Incident events for the filtered time frame.

Filtering Incident – EDR Report for Specific Incident

To filter the Incident – EDR report for specific incident as per your requirements, click **Filter Criteria** field.

Filter Criteria field expands.

Filter Criteria

Investigation Detail

select before time 15 minutes ▼ 2 * hours(s)

select after time 15 minutes ▼ 2 * hours(s)

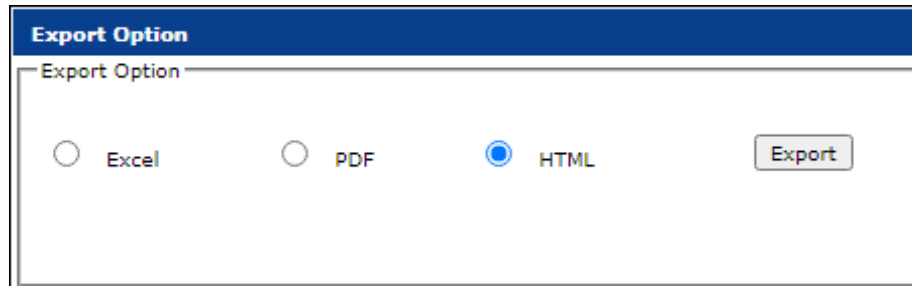
(*) View All Items

Select the before time and the after time of specific incident that has be filtered out. After making the necessary selections, click **Search**.

The Incident – EDR report for that incident will be generated according to your preferences.

Exporting Incident – EDR Report for Specific Incident

eScan EDR provides investigation details based on the Windows event and eScan events. It allows the admin to export the investigation reports in various formats such as HTML, PDF, or Excel.



Exporting the Report

To export the Incident – EDR Report, click **Export Option**.

Export Option field expands.



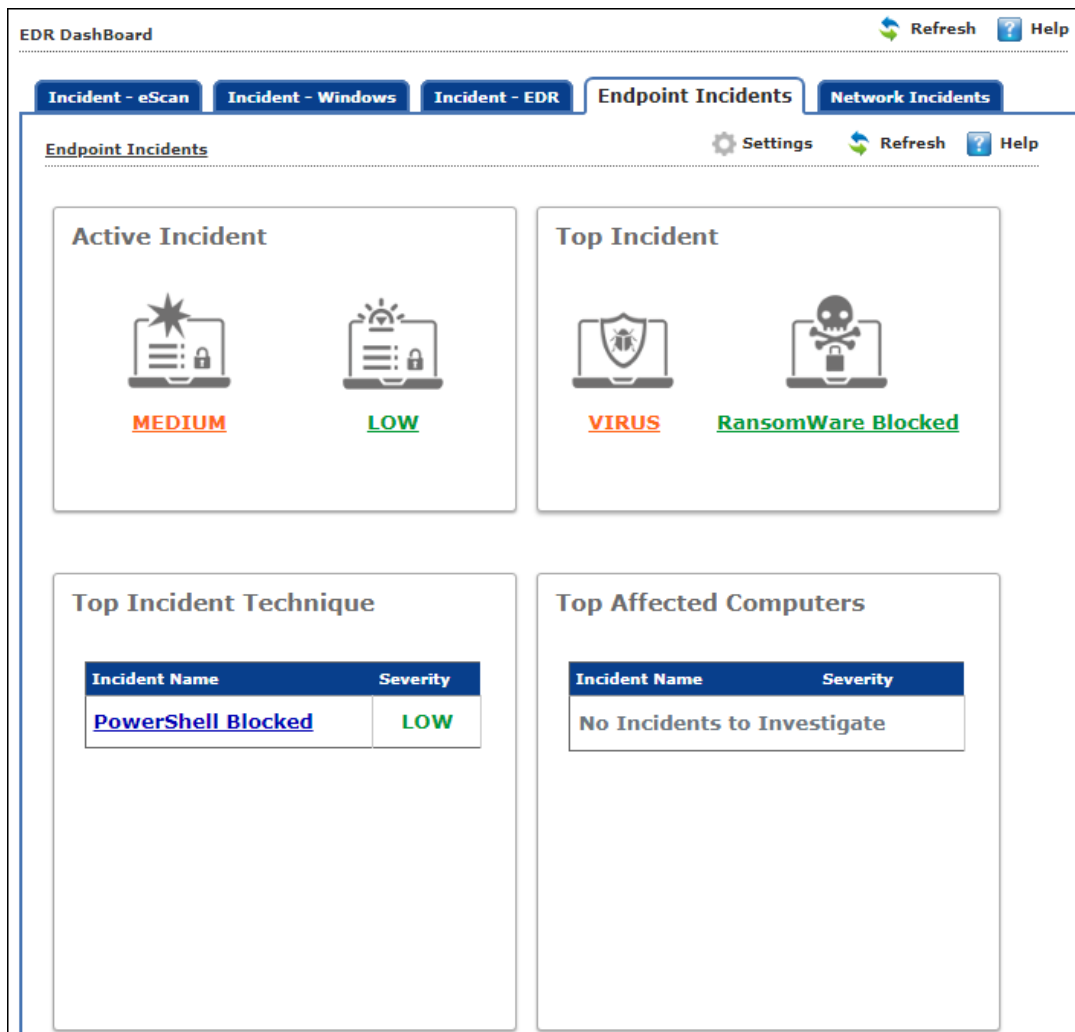
Select the preferred option and then click **Export**. A success message appears.



Click the link to open/download the file.

Endpoint Incident

In this tab, incidents from all the endpoints in the network will be displayed with categories such as Active Incidents, Top Incidents, Top Incident Techniques, and Top Affected Computers. All the incidents and incidents techniques are divided into different severity level (High, Medium, and Low) based on the defined threshold value. It displays general incident information, matches detected in the intercepted text, and details about attributes, incident history, and the violated policy.



Active Incidents

The Active Incident category displays all the current incidents within the network based on the level of severity.

Top Incident

The Top Incident category displays the malware that were detected based on different categories namely virus, Ransomware, and PBAE.

Top Incident Technique

The Top Incident Technique category displays the different techniques used for the detection for specific incident and its severity level.

Top Affected Computers

The Top Affected Computers category displays the list of the computers that are affected based on the threshold value (High, Medium, and Low).

Click on the severity level under specific category to get the details of the incident.

Index	Incident	Computer Name/Ip	User's name	IP Address	HostName	HostIp	Incident Date	Incident Count	Incident Severity
<input type="checkbox"/>	RansomWare Blocked	WI-E8CNDP7ER	WI-E8CNDP7ER\Administrator	192.168.0.139	-	-	07/05/2021	1	Low
<input type="checkbox"/>	RansomWare Blocked	WI-E8CNDP7ER	WI-E8CNDP7ER\Administrator	192.168.0.139	-	-	07/02/2021	1	Low
<input type="checkbox"/>	RansomWare Blocked	WI-E8CNDP7ER	WI-E8CNDP7ER\Administrator	192.168.0.139	-	-	06/30/2021	2	Medium
<input type="checkbox"/>	RansomWare Blocked	WI-E8CNDP7ER	WI-E8CNDP7ER\Administrator	192.168.0.139	-	-	06/30/2021	1	Low
<input type="checkbox"/>	RansomWare Blocked	WI-E8CNDP7ER	WI-E8CNDP7ER\Administrator	192.168.0.139	-	-	06/30/2021	1	Low
<input type="checkbox"/>	RansomWare Blocked	WI-Q4077G	WI-Q4077G	192.168.0.85	-	-	06/29/2021	1	Low

Adding Specific Incident for Monitoring

From the detailed list of the incident detected, admin can monitor the specific incident. Follow the below steps to do the same:

1. From the list of the detected incident, select the specific incident according to the requirement.

The screenshot shows the 'Endpoint Incidents > RansomWare Blocked' view in the eScan interface. The table below contains the following data:

Index	Incident	Computer Name/Ip	User's name	IP Address	HostName	HostIp	Incident Date	Incident Count	Incident Severity
<input type="checkbox"/>	RansomWare Blocked	WIN-ESCHN8E7R	WIN-ESCHN8E7R\Administrator	192.168.0.139	-	-	07/05/2021	1	Low
<input type="checkbox"/>	RansomWare Blocked	WIN-ESCHN8E7R	WIN-ESCHN8E7R\Administrator	192.168.0.139	-	-	07/02/2021	1	Low
<input checked="" type="checkbox"/>	RansomWare Blocked	WIN-ESCHN8E7R	WIN-ESCHN8E7R\Administrator	192.168.0.139	-	-	06/30/2021	2	Medium
<input type="checkbox"/>	RansomWare Blocked	WIN-ESCHN8E7R	WIN-ESCHN8E7R\Administrator	192.168.0.139	-	-	06/30/2021	1	Low
<input type="checkbox"/>	RansomWare Blocked	WIN-ESCHN8E7R	WIN-ESCHN8E7R\Administrator	192.168.0.139	-	-	06/30/2021	1	Low
<input type="checkbox"/>	RansomWare Blocked	WIN-Q80E7G6	WIN-Q80E7G6	192.168.0.85	-	-	06/29/2021	1	Low

At the bottom of the interface, there are two buttons: 'Add To Monitor' and 'Cancel'.

2. Click **Add To Monitor**. The specific incident will be added to the monitoring list.

Viewing the Details of the Specific Incident

A process tree contains the details from the start of the infection till the current status of the infection along with the action taken on the same. With more contextual information, extra technologies that filter out noise, prioritized incidents, guided investigation and response steps.

To view the detailed process tree follow the below steps:

1. Click the incident name under **Incident** column.

Select Incident: 7/5/2021 11:14:02 AM View Export To HTML Export Export All

Incident Report For User

Computer Name: WIN-QM8P
 User Name: WIN-QM8P\user
 IP Address: 192.168.0.88
 Date Time: 7/5/2021 11:13:58
 Session Type: Local
 Incident: PowerShell Blocked

Behavior: Chronology

Time	PID	Process Name	File Action Type	Action Object
11:13:58	4036	explorer.exe	Process Run	C:\Windows\explorer.exe
11:13:58	3252	cmd.exe	Process Run	C:\Windows\System32\cmd.exe
11:13:58	3948	powershell.exe	Process Run	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
11:13:59	3948	PowerShell Blocked	Process Run	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Behavior: Graph

```

  graph TD
    A[explorer.exe] --> B[cmd.exe]
    B --> C[powershell.exe]
    C --> D[PowerShell Blocked]
  
```

Info Files Registry Integrity

Process Name: **explorer.exe**
 PID: 4036
 Path: C:\Windows\explorer.exe
 Command Line: C:\Windows\Explorer.EXE
 url: -
 Client User Name: -
 Client HostName: -
 Client IP Address: -

2. Detailed view of the incident along with information such as process tree graph, chronology of the process, date, time, IP address, and more.

You can even filter the incident based on the different endpoints and time it was detected using **Select Incident** option.

The same report can be exported into different format such as HTML and PDF

Viewing the Details of Monitoring Incident

After adding the specific incident to the monitoring list, you can get the details of the same. You can view the details such as EDR Sensors, Date, Validity, Conditions, Status, and Result.

Index	Date	EDR Sensor	Condition1	Condition2	Condition3	Condition4	Condition5	Validity	Status	Result
<input type="checkbox"/>	07/05/2021 16:52:27	0587P12115391720	PowerShell Blocked	powershell.exe	powershell.exe -NoProfile...	-	-	1 Day	Stop Monitoring	View
<input type="checkbox"/>	07/05/2021 15:41:13	0587P1211539172	MSOffice Child EXE Blocke...	ms.exe	-	-	-	1 Day	Stop Monitoring	View
<input type="checkbox"/>	07/02/2021 15:39:50	02072021153917	Infected by Virus: Trojan...	-	G:\test\notification.exe	-	-	7 Days	Stop Monitoring	View

Click **View** option under **Result** column to get the details of the monitored incident.

Status ✕

Client Date and Time: 7/3/2021 5:11:00 PM

Computer Name/Ip: WI-E8CANSENER

User's name: WI-E8CANSENER\Administrator

IP Address: 192.168.8.155

Client Date and Time: 7/5/2021 10:35:31 AM

Computer Name/Ip: WI-E8CANSENER

User's name: WI-E8CANSENER\Administrator

This will display the details of the same incident that were detected from all the endpoints in the network.

Admin can also stop monitoring of the incident, by clicking **Stop Monitoring** option under **Status** column.

Deleting the Monitoring Incident

To delete the incident that are being monitoring, follow the below steps:

1. Select the specific incident from the list.

Index	Date	EDR Sensor	Condition1	Condition2	Condition3	Condition4	Condition5	Validity	Status	Result
<input checked="" type="checkbox"/>	07/05/2021 16:52:27	0587P12115391720	PowerShell Blocked	powershell.exe	powershell.exe -NoProfile...	-	-	1 Day	Stop Monitoring	View
<input type="checkbox"/>	07/05/2021 15:41:13	0587P1211539172	MSOffice Child EXE Blocke...	ms.exe	-	-	-	1 Day	Stop Monitoring	View

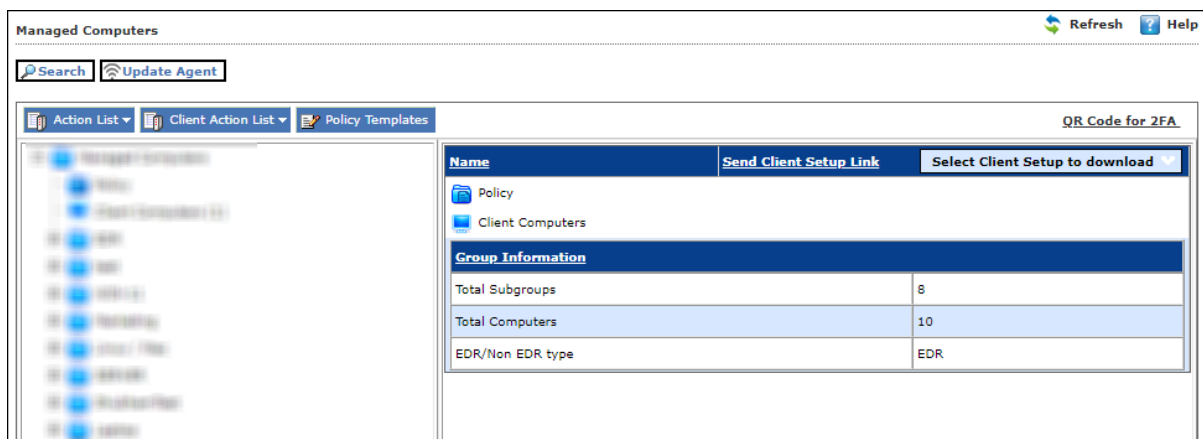
2. Click **Delete**.
The specific incident will be deleted.

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.

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.

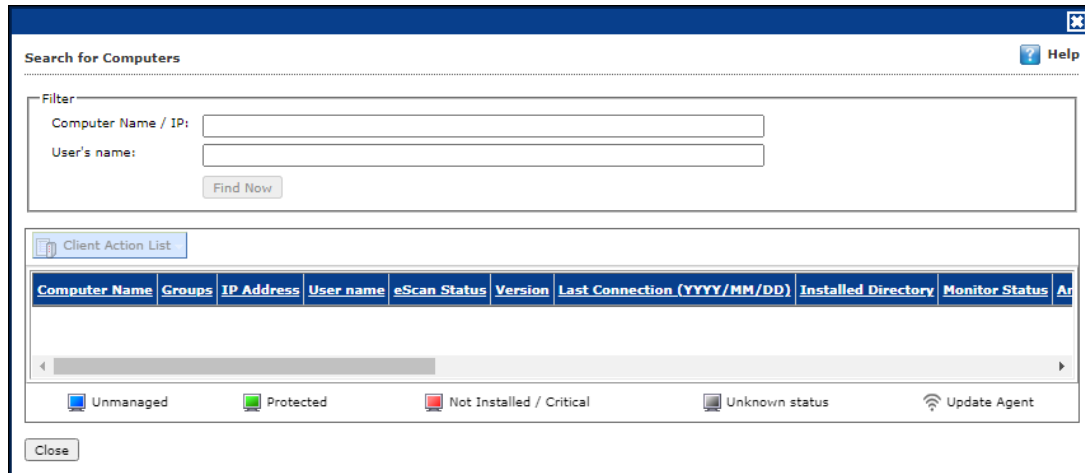


The screen consists of following buttons:

- **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.



The Filter section displays following fields:

Computer Name/IP

Enter a computer name or IP address.

Username

Enter a username.

Click **Find Now**.

The console will display the result.

Update Agent

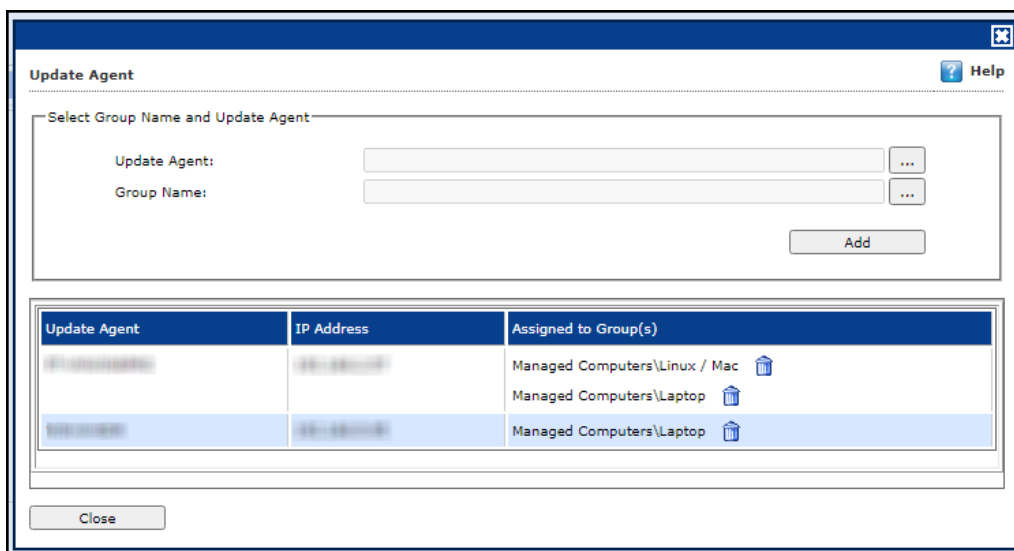
eScan lets you use a client computer as an update agent to deploy updates on groups of computers. By default, eScan server distributes the virus definitions and policies to all the clients added in the web console. But, if you want to reduce server's workload, you can create an Update Agent for the respective 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.

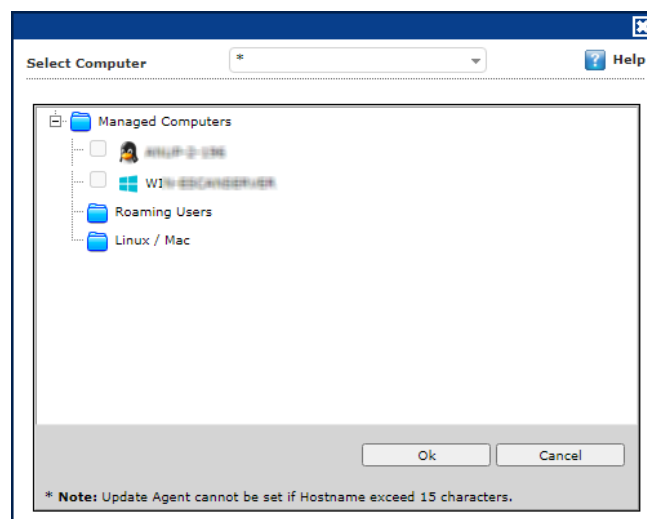
Adding an Update Agent


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

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



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

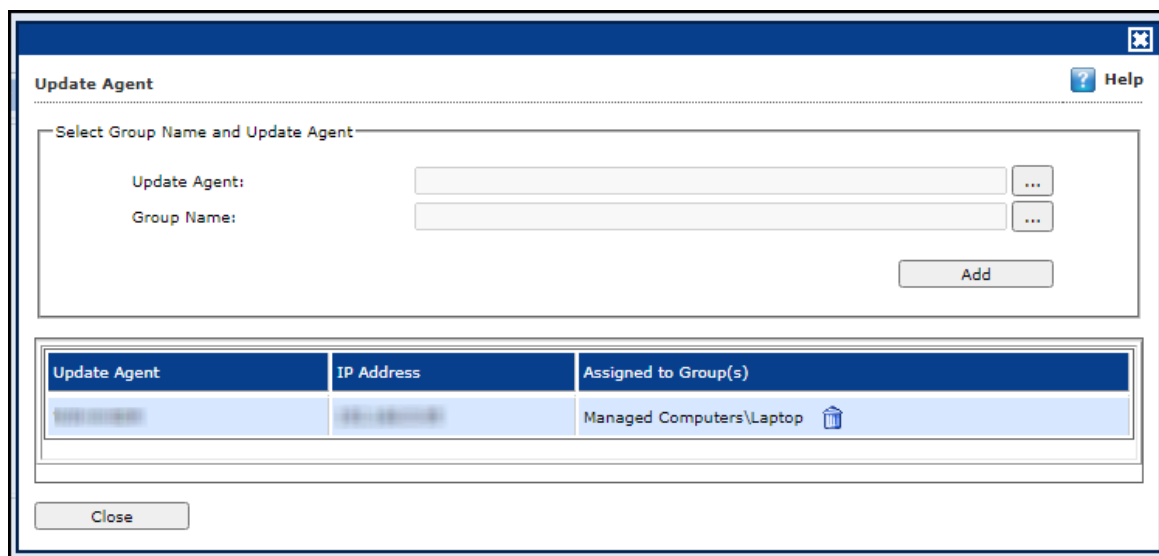


3. Select a computer and click **OK**.
4. Click  next to Group Name field, to select the Group Name. This is the group to which the selected computer will act as an Update Agent and provide updates.
5. Select the Group and click **OK**.
6. Click **Add**.
The Update Agent will be set for the selected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

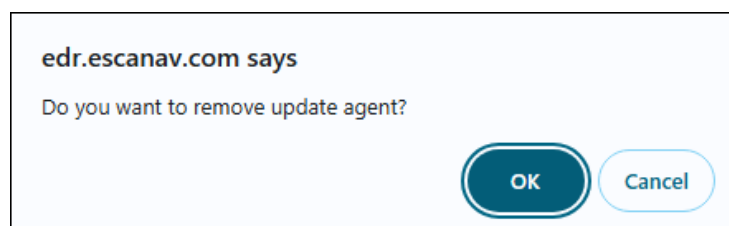
Delete an Update Agent

To delete an Update Agent:

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



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



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

Action List

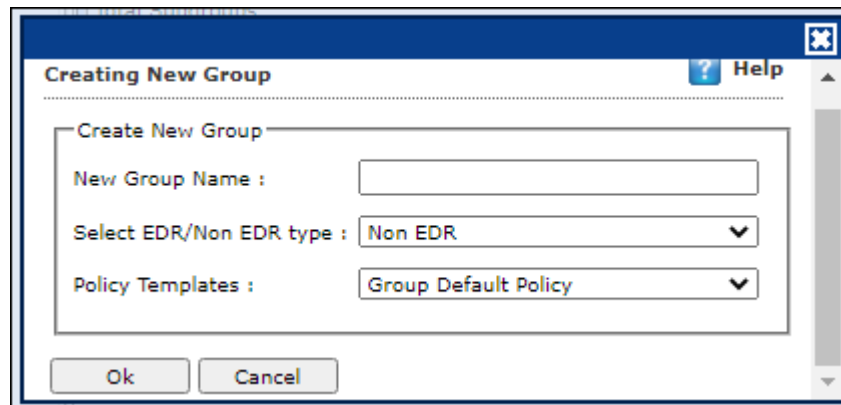
The Action List takes you action for a group. The drop-down contains following options:

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

New Subgroup

To create a group, follow the steps given below:

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

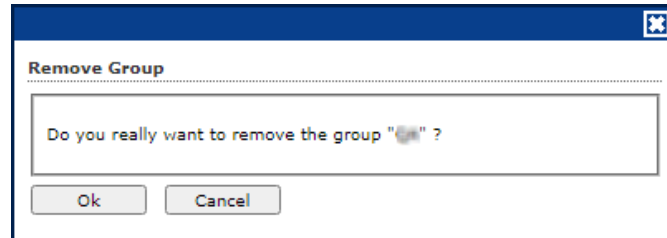


2. Enter a name for the group.
3. Click the EDR/ Non EDR drop-down and select a type.
4. Click the Policy Templates drop-down and select a policy for the group.
5. Click **OK**.
A new group will be created under the Managed Computers.

Removing a Group

To remove a group, follow the steps given below:

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



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

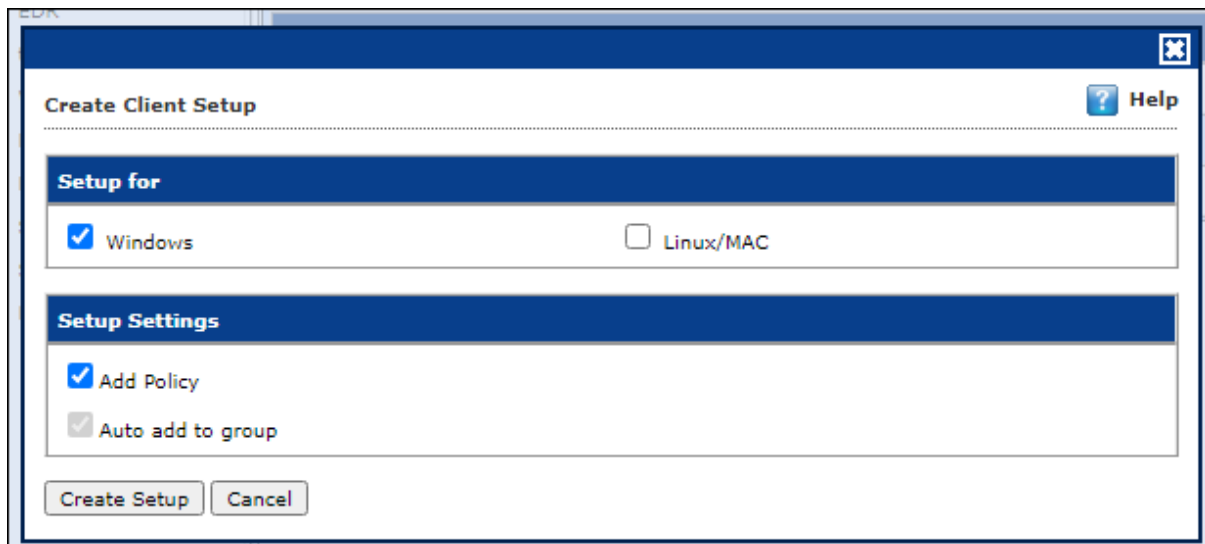
NOTE

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





Create Client Setup

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

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



2. Select the necessary settings.
3. Click **Create Setup**. The Client setup will be created and a download link will be displayed in right pane.

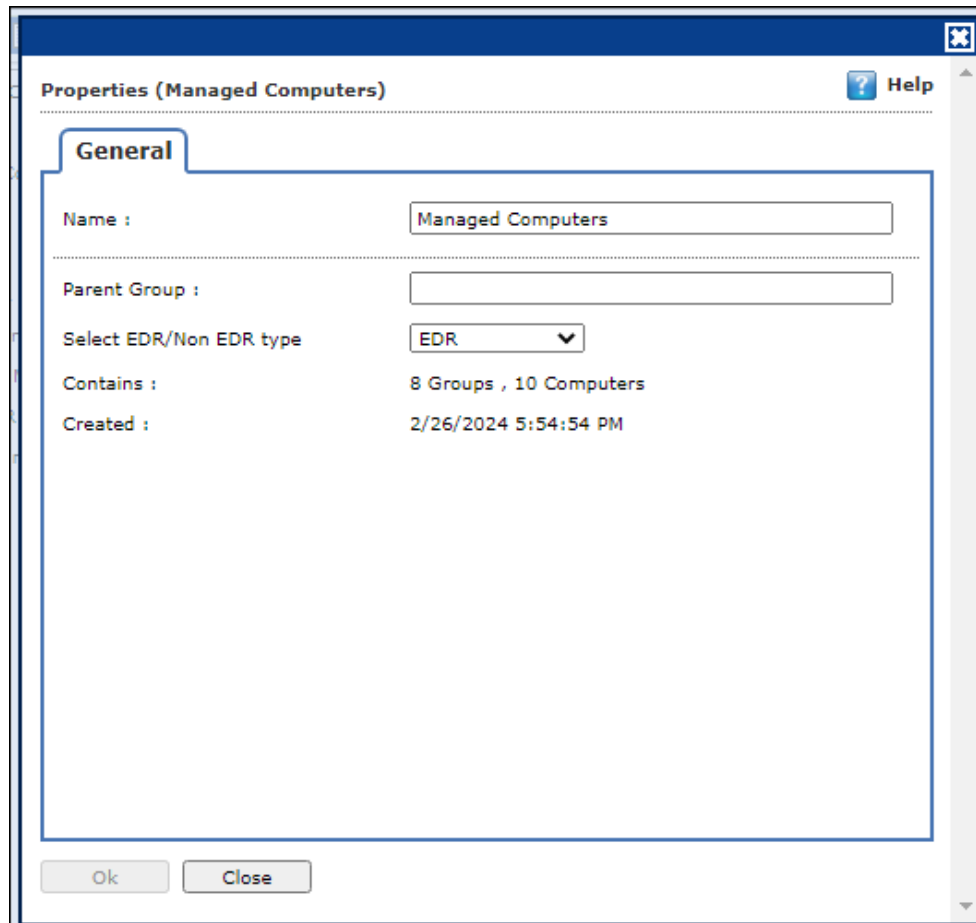
Name		Download Client Setup 
	Policy	
	Group Tasks	
	Client Computers	
Group Information		
AD Sync		Not Configured
Total Subgroups		20
Total Computers		5

Properties of a group

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

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

Properties window appears.



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

- Group Name
- Parent Group
- EDR / Non EDR Type
- Contains – Sub Groups or Number of Computers in that Group
- Creation date of the Group

Assigning a Policy to the group

To assign a Policy to the group, follow the steps given below:

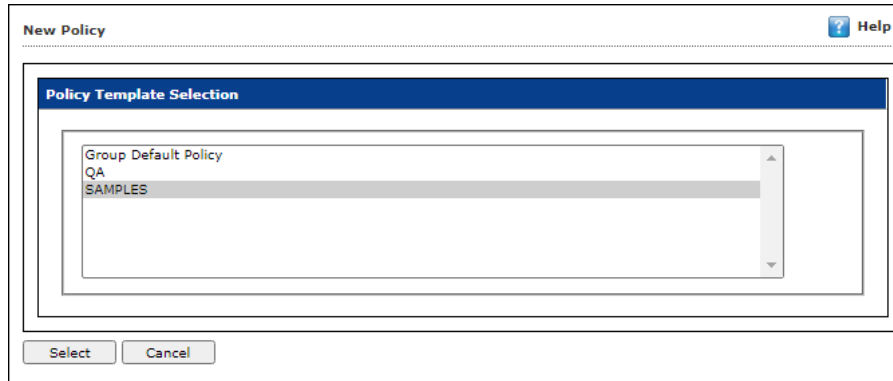
1. In the Managed Computers folder tree, select a group.
2. Under the group name, click **Policy**.

Policy pane appears on the right side.

The screenshot displays the 'Managed Computers' interface. On the left, a folder tree shows 'Client Computers' selected. The right pane shows the 'Policy' configuration for the selected group. The 'Group Information' table is as follows:

Group Information	
Total Subgroups	8
Total Computers	10
EDR/Non EDR type	EDR

3. To assign a Policy Template to group, click **Select Template**. New policy window appears.



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**
- **Refresh Client**
- **Show Critical Events**
- **Export**
- **Show Installed Softwares**
- **Forensic/Port Communication**
- **Remediation Console**
- **Search IOC**
- **Create OTP**
- **Properties**

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

Move to Group

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

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

Remove from Group

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

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

Refresh Client

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

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

Show Critical Events

To show critical events of specific computer, follow the steps given below:

1. Go to **Managed Computers**.
2. Select the client computer which you want to assign policy template.
3. Click **Client Action List > Show Critical Events**.
This will display the list of all the critical events of the computer that can also be exported as a report.

Export

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

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

Computer Name	IP Address	IP Address of the connection	User name
WIN-LL	192.168.0.100		WIN-LL\Prashant
WIN-CLP	192.168.0.61		WIN-CLP\Prashant
WIN-QAD07	192.168.0.117		

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

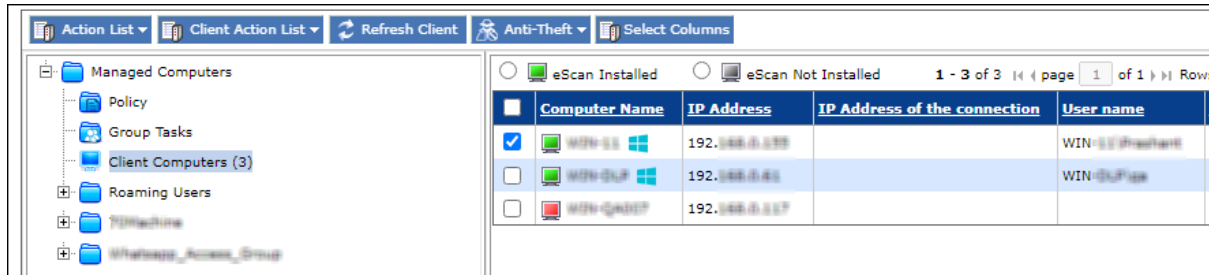
<input checked="" type="checkbox"/> Computer Name	<input checked="" type="checkbox"/> IP Address	<input checked="" type="checkbox"/> IP Address of the connection	<input checked="" type="checkbox"/> User name
<input checked="" type="checkbox"/> Local Administrator User(s)	<input checked="" type="checkbox"/>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

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

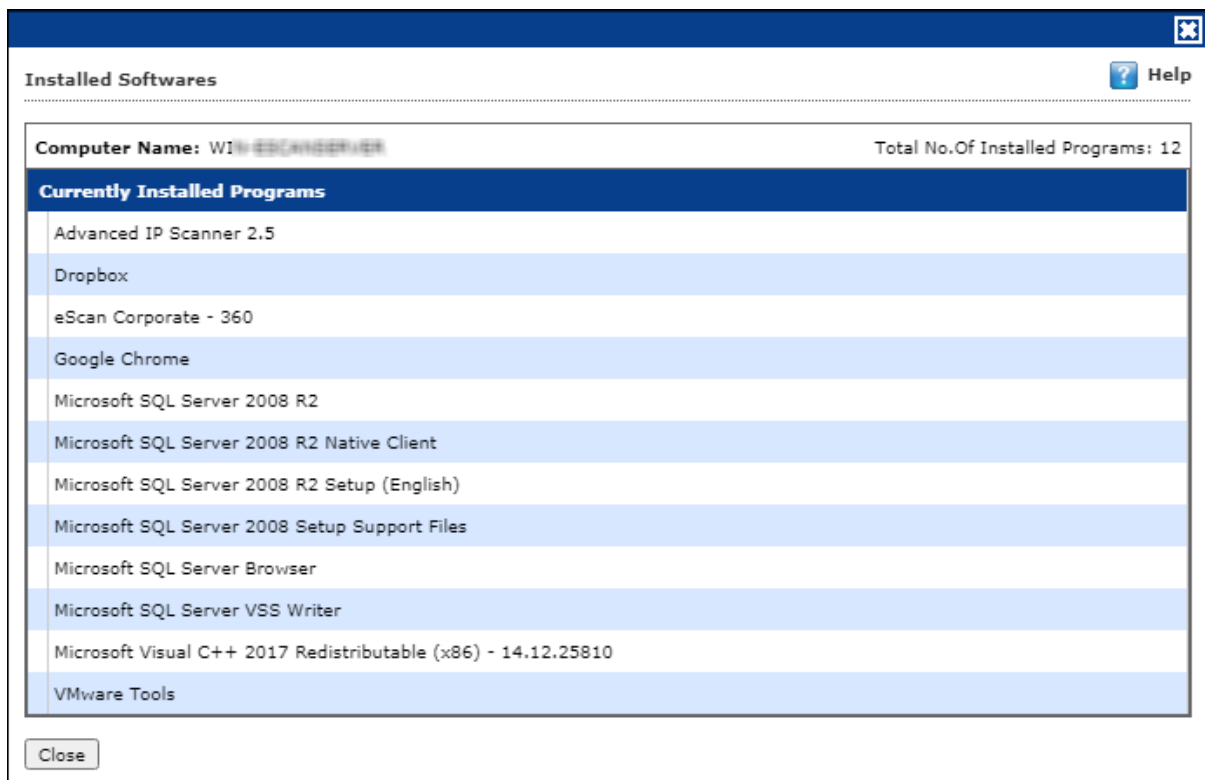
Show Installed Softwares

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

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



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.



Forensic-Port/Communication

This option generates the Forensic report of the service running on certain port during a particular period for analysis. To generate the report, select the client computer and click **Forensic Port/Communication** option.

```

Client Status
-----
7/8/2021 12:35:51 PM : Processing with group : Q:\_TEAM
7/8/2021 12:35:51 PM : Connecting to Computer... WIW-QM07
7/8/2021 12:35:52 PM : Successfully Exported Report on WIW-QM07
-----
=====
  
```

To view the forensic port, select the client machine and scroll the window to **Forensic Report**.

Computer Name	Last EBackup Status	Forensics Report
<input type="checkbox"/> WIW-QM07	Job Name:Test_Bak - Date:2021/06/06 12:07:40 -Status:Backup Finished., No files to upload on [No new files found for backup.]	View

To get the detailed report of the same or download it, click on the specific report under **File Name** column.

WIW-QM07
Refresh ? Help

Search files in selected Date Range

MM/DD/YYYY MM/DD/YYYY

From To

Report Type: Forensics - Port/Communication Report

	File Name	Created On (Date and time)	Size
<input type="checkbox"/>	eScan Forensics Anti-Malware_WIW-QM07_20210606115214.pdf	22 Jun 2021,11:52 AM	308 KB
<input type="checkbox"/>	eScan Forensics Port_WIW-QM07_20210606111901.pdf	22 Jun 2021,11:19 AM	327 KB

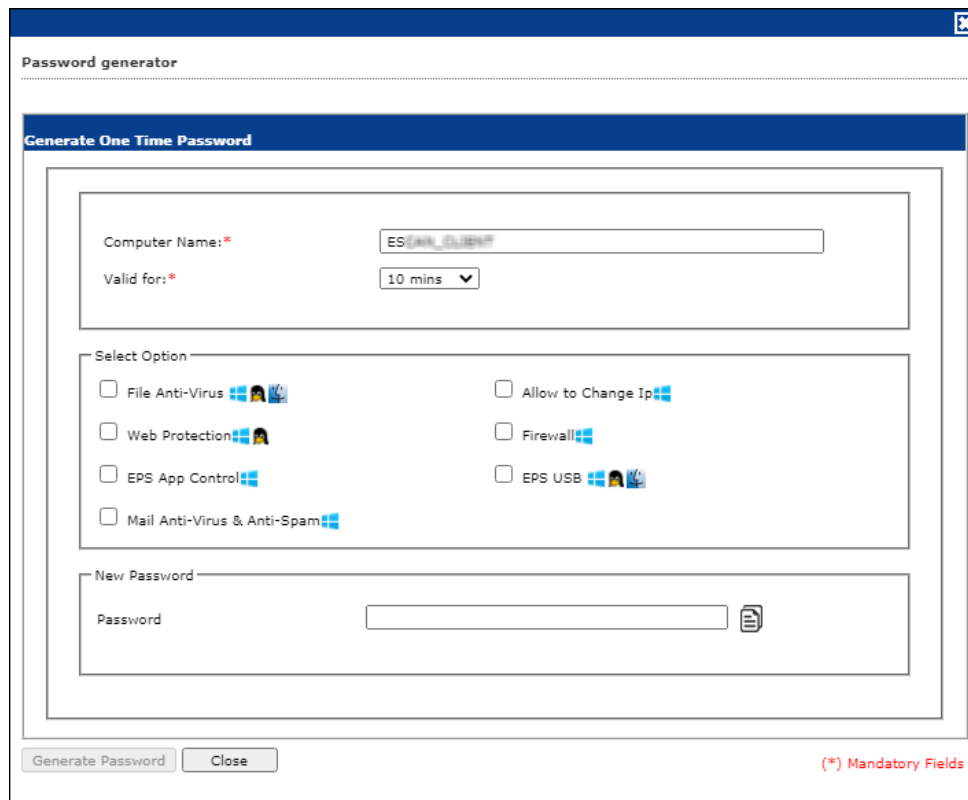
Create OTP

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

Generating an OTP

To generate an OTP, follow the steps given below:

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



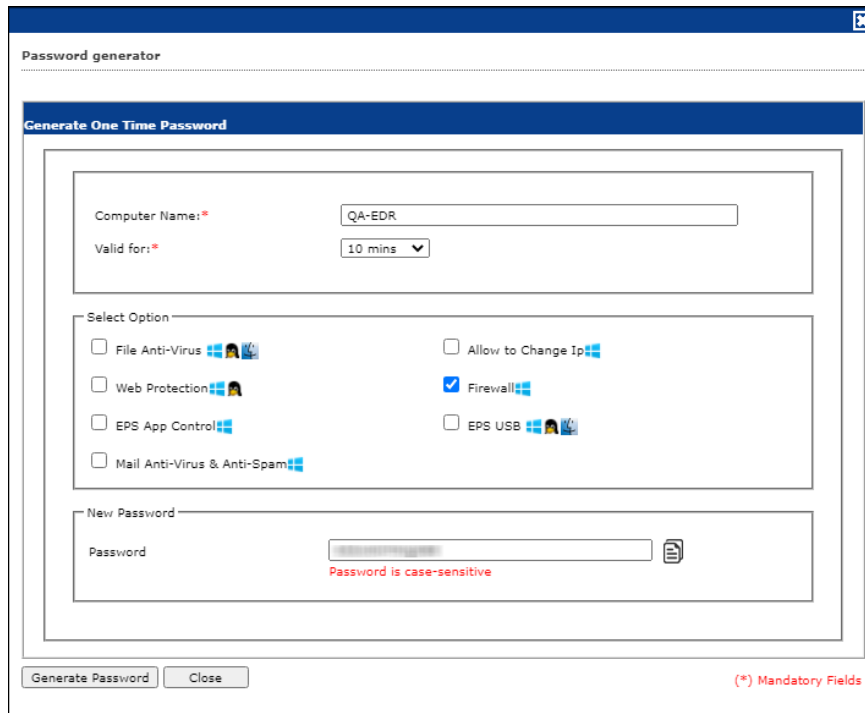
The screenshot shows a window titled "Password generator" with a sub-header "Generate One Time Password". The form contains the following fields and options:

- Computer Name:** A text box containing "ES\WIN_CLIENT".
- Valid for:** A dropdown menu set to "10 mins".
- Select Option:** A section with several checkboxes:
 - File Anti-Virus
 - Web Protection
 - EPS App Control
 - Mail Anti-Virus & Anti-Spam
 - Allow to Change Ip
 - Firewall
 - EPS USB
- New Password:** A text box labeled "Password" with a copy icon to its right.

At the bottom of the window, there are two buttons: "Generate Password" and "Close". A red note at the bottom right states "(*) Mandatory Fields".

3. In the **Valid for** drop-down, select the preferred duration to bypass the protection module.
4. In **Select Option** section, select the module you want to disable.

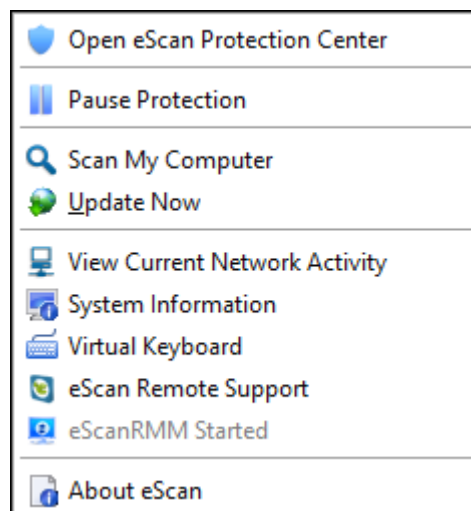
5. Click **Generate Password**. An OTP will be generated and displayed in **Password** field.



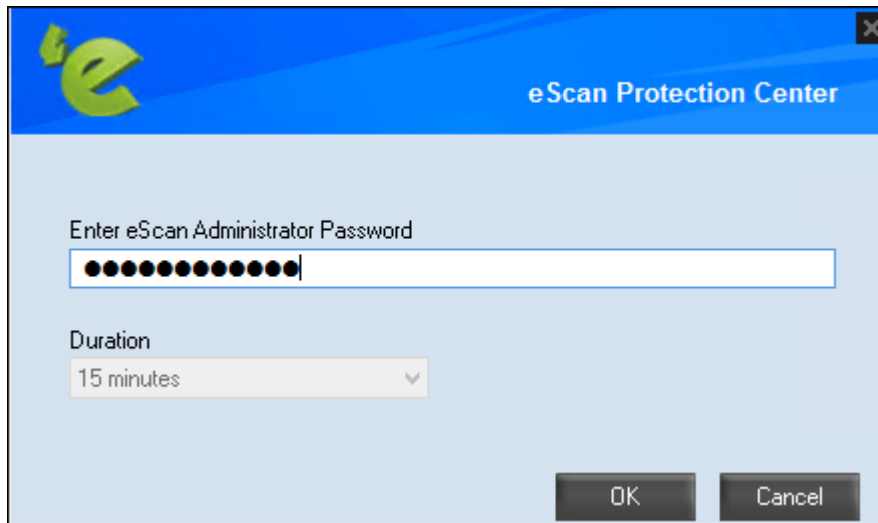
Entering an OTP

To enter an OTP, follow the steps given below:

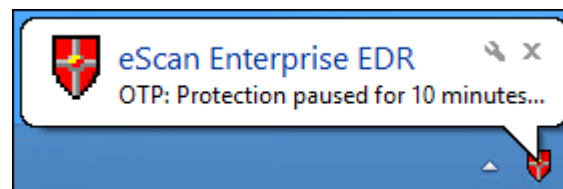
1. In the Taskbar, right-click the eScan icon . An option list appears.



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



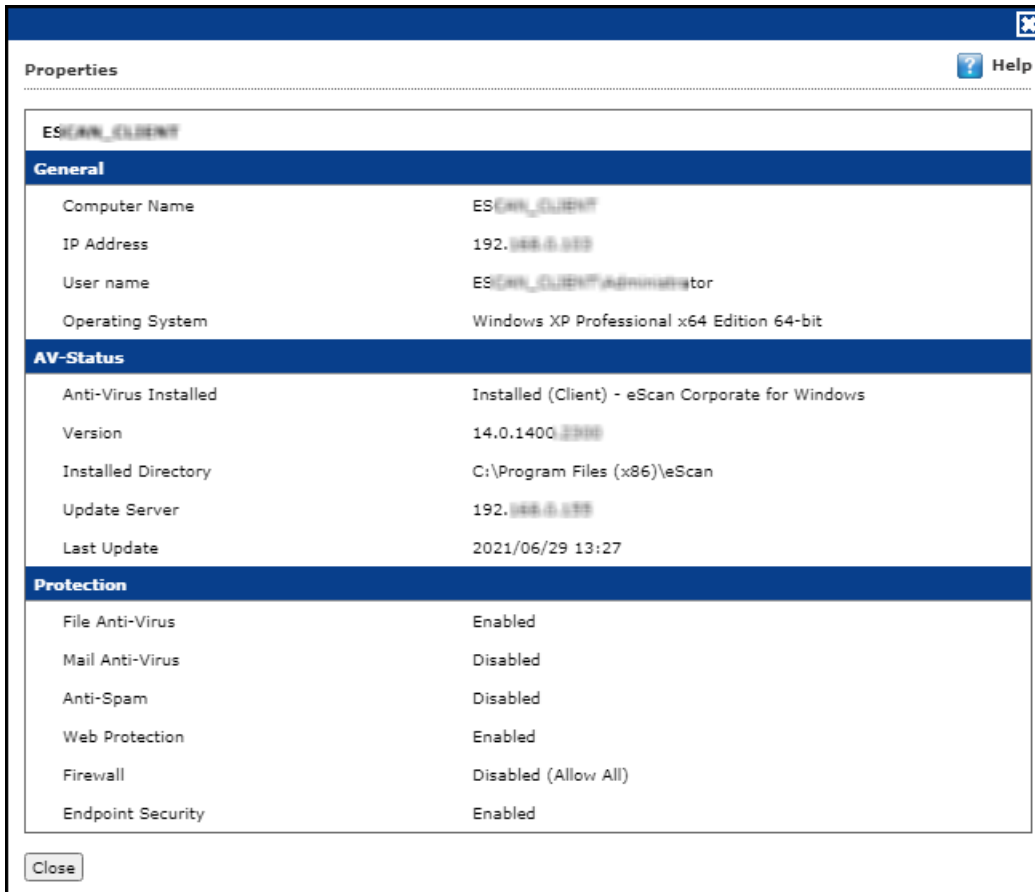
3. Enter the OTP in the field.
4. Click **OK**.
The selected module will be disabled for set duration.



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.

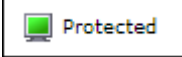
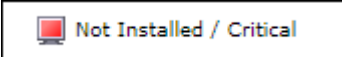
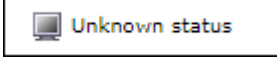
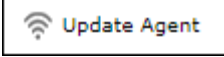
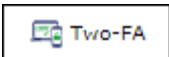
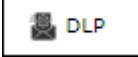
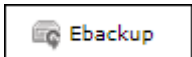
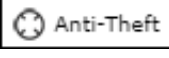


ESCAN_CLIENT	
General	
Computer Name	ESCAN_CLIENT
IP Address	192.168.0.100
User name	ESCAN_CLIENT\Administrator
Operating System	Windows XP Professional x64 Edition 64-bit
AV-Status	
Anti-Virus Installed	Installed (Client) - eScan Corporate for Windows
Version	14.0.1400.2300
Installed Directory	C:\Program Files (x86)\eScan
Update Server	192.168.0.100
Last Update	2021/06/29 13:27
Protection	
File Anti-Virus	Enabled
Mail Anti-Virus	Disabled
Anti-Spam	Disabled
Web Protection	Enabled
Firewall	Disabled (Allow All)
Endpoint Security	Enabled



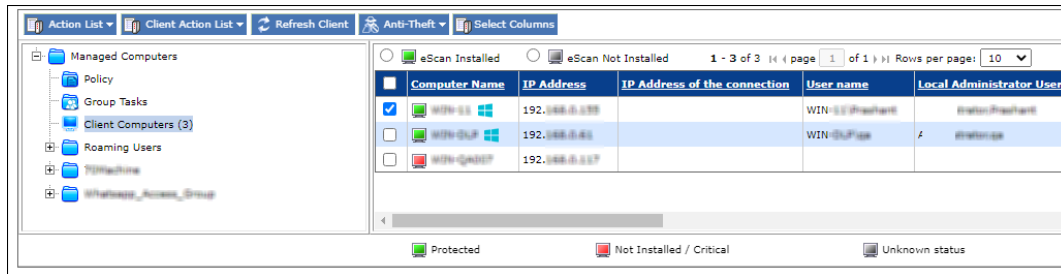
If multiple computers are selected, the **Properties** option will be disabled.

Understanding the eScan Client Protection Status

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

Anti-Theft

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

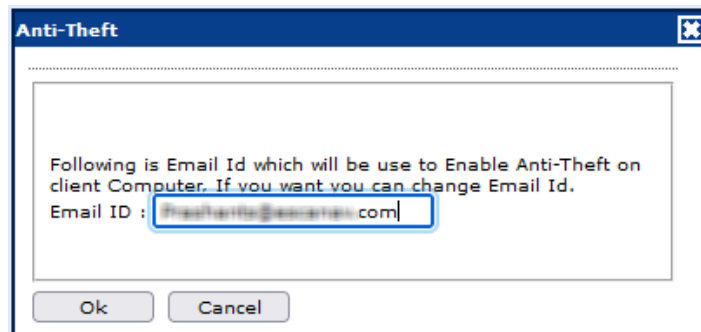


Anti-Theft Options

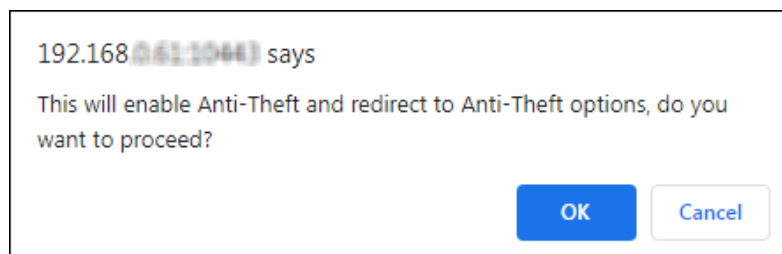
To add computers in an Anti-theft, follow the steps given below:

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

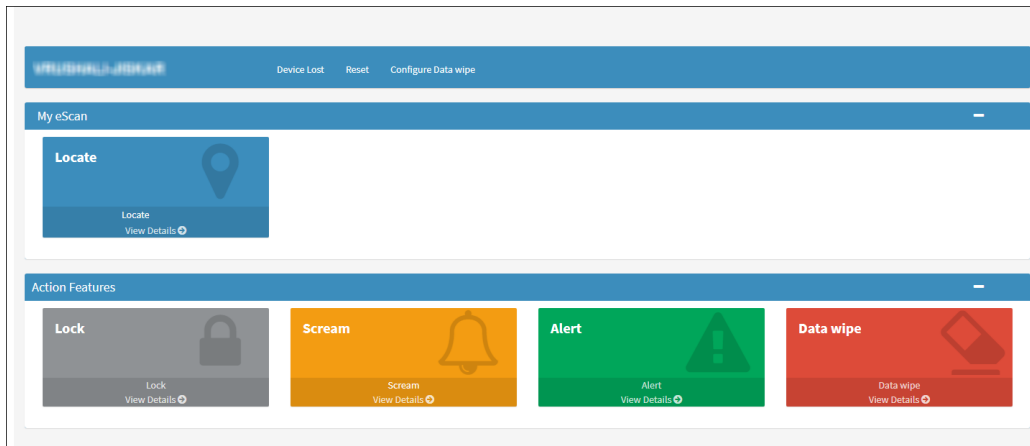
The computer will add in Anti-Theft Portal.



5. A confirmation prompt appears.

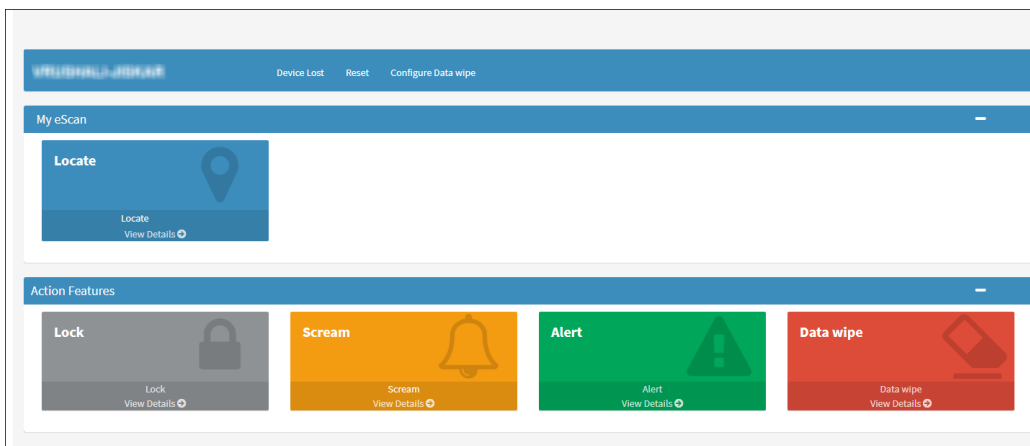


6. Click **OK**. This will redirect to Anti-Theft options.

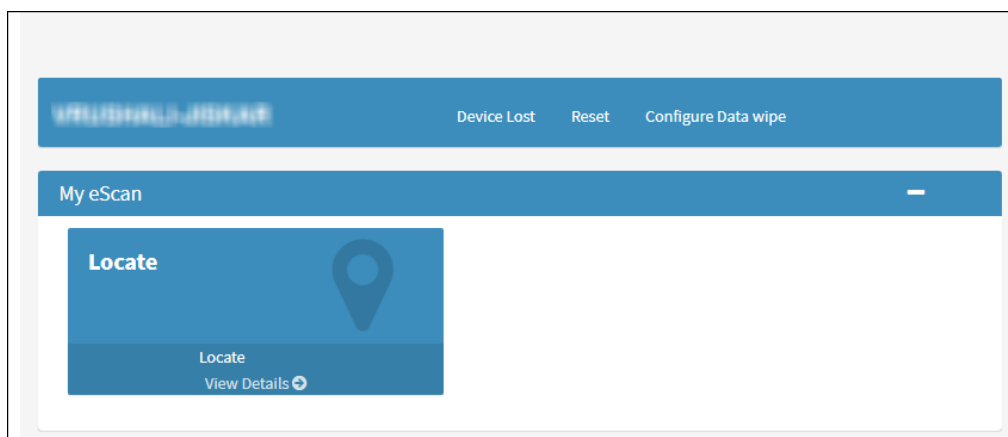


Anti-Theft Portal

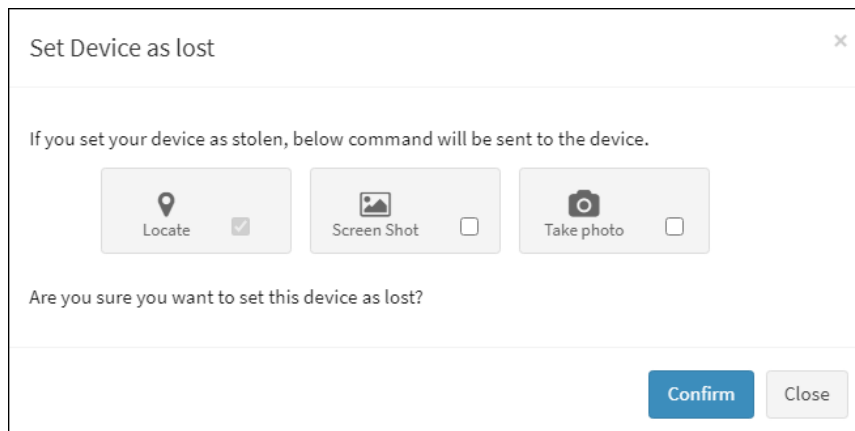
1. It will display the anti-theft features that you can activate in case your system is lost or stolen.



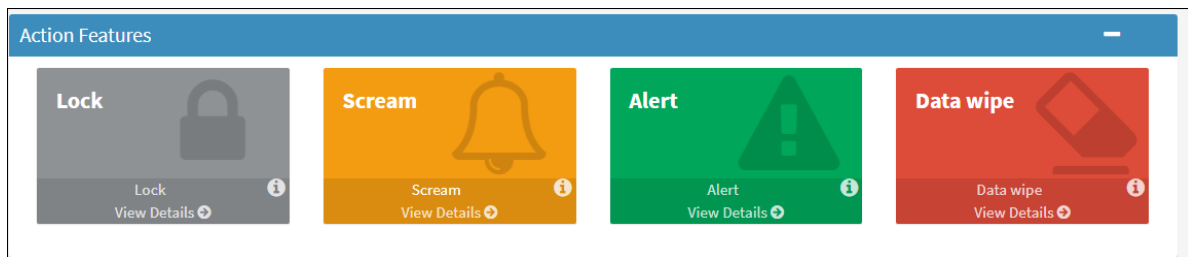
2. In case of loss or theft, click on the system name that has been lost or stolen, the status bar under it will display the system name again and when it was last seen.
3. Click **Device Lost** and this will allow you to enable the features locate, screenshot and take photo by selecting the desired options.



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



- **Locate:** This option will allow you to locate the system in case of loss/theft. Click on the **Locate** option on the anti-theft portal and the last known location of the system will be displayed on the map. Procedure to Locate the system:
 - A. 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.
 - B. **View Details** displays the Last Location of your system on a map. It also shows details of last two successful executions of the Locate command.
- **Screenshot:** This option will take a screen shot of the system whenever it is synced to the server.
 - A. 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.
 - B. **View Details** displays the last two screenshots from the successful execution of the screenshot command.
- **Take Photo:** This option will allow you to take a snapshot of the current user of the system from the webcam on clicking the camera option on the anti-theft portal.
 - A. 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.
 - B. **View Details** displays the last two snapshots taken from your system. Click **Reset** to reset the **Action Features** on the system; these actions can be performed on the system when it has been lost or stolen.



There are following action features:

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

Disable Anti-Theft

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

1. Go to Managed Computers.
2. Select the desired computers in Anti-theft Portal.
3. Click **Anti-Theft > Disable Anti-Theft**.

Select Columns

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

Select All Columns	
<input checked="" type="checkbox"/> Computer Name	<input checked="" type="checkbox"/> IP Address
<input checked="" type="checkbox"/> IP Address of the connection	<input checked="" type="checkbox"/> Mac Address
<input checked="" type="checkbox"/> User name	<input checked="" type="checkbox"/> Local Administrator User(s)
<input checked="" type="checkbox"/> eScan Status	<input checked="" type="checkbox"/> Version
<input checked="" type="checkbox"/> Last Connection	<input checked="" type="checkbox"/> Installed Directory
<input checked="" type="checkbox"/> Last Update	<input checked="" type="checkbox"/> Anti-Spam
<input checked="" type="checkbox"/> Mail Anti-Virus	<input checked="" type="checkbox"/> Web Protection
<input checked="" type="checkbox"/> Endpoint Security	<input checked="" type="checkbox"/> Firewall
<input checked="" type="checkbox"/> Monitor Status	<input checked="" type="checkbox"/> Update Server
<input checked="" type="checkbox"/> Client OS	<input checked="" type="checkbox"/> Status
<input checked="" type="checkbox"/> Installation Status	<input checked="" type="checkbox"/> Last Policy Applied
<input checked="" type="checkbox"/> Last Policy Applied Time	<input checked="" type="checkbox"/> Last eBackup Status
<input checked="" type="checkbox"/> Last Scan Date	<input checked="" type="checkbox"/> PC Model
<input checked="" type="checkbox"/> PC IdentifyingNumber	<input checked="" type="checkbox"/> Domain/Workgroup
<input checked="" type="checkbox"/> Installed Date	

Apply Cancel

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

Policy Template

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

Managing Policies

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

Defining Policies for 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 the report file for future reference, and displays attention messages. To learn more, [click here](#).

Mail Anti-Virus

The Mail Anti-Virus module scans all the incoming emails. It scans the emails by breaking them into three sections the header, the subject and the body. After scanning, the module combines the sections and sends it to your mailbox. To learn more, [click here](#).

Anti-Spam

The Anti-Spam module blocks spam emails by checking the content of outgoing and incoming mails and quarantines advertisement emails. To learn more, [click here](#).

Web Protection

The Web Protection module lets you block websites. You can allow/block websites with time-based access restrictions. To learn more, [click here](#).

Firewall

The Firewall module lets you put up a restriction on 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. To learn more, [click here](#).

Endpoint Security

The Endpoint Security module monitors the application on client computers. It allows/ restricts USB, Block lists, White lists, and defines time restrictions for applications. To learn more, [click here](#).

Privacy Control

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

Administrator Password

Administrator Password lets you create and change a password for administrative login to the eScan protection center and Two-Factor Authentication. To learn more, [click here](#).

ODS/Schedule Scan

ODS/Schedule Scan provides you with various options like – checking for viruses, and making settings for creating logs and receiving alerts. To learn more, [click here](#).

MWL Inclusion List

The inclusion list contains the names of all executable files which will bind itself to MWTSP.DLL. All other files are excluded. To learn more, [click here](#).

MWL Exclusion List

MWL Exclusion List contains the name of all executable files which will not bind itself to MWTSP.DLL. To learn more, [click here](#).

Notifications & Events

Notifications & Events allows to allow/restrict the alerts that are send to admin in case of any suspicious activity or events. To learn more, [click here](#).

Schedule Update

Schedule Update policy lets you schedule eScan database updates. To learn more, [click here](#).

Tools

Tools policy let you configure eBackup setting. To learn more, [click here](#).

Defining Policies Mac or Linux computers

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

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. To learn more, [click here](#).

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. To learn more, [click here](#).

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. To learn more, [click here](#).

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. To learn more, [click here](#).

Schedule Update



The Schedule Update module lets you schedule updates for Linux Agents. To learn more, [click here](#).

Administrator Password



The Administrator Password module for Linux lets you create and change password for administrative login of eScan protection center. It also lets you keep the password as blank, wherein you can login to eScan protection center without entering any password.

It lets you define uninstallation password which will be required before uninstalling eScan Client from managed computers manually. The user will not be able to uninstall eScan Client without entering uninstallation password. To learn more, [click here](#).


Web Protection



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

Network Security

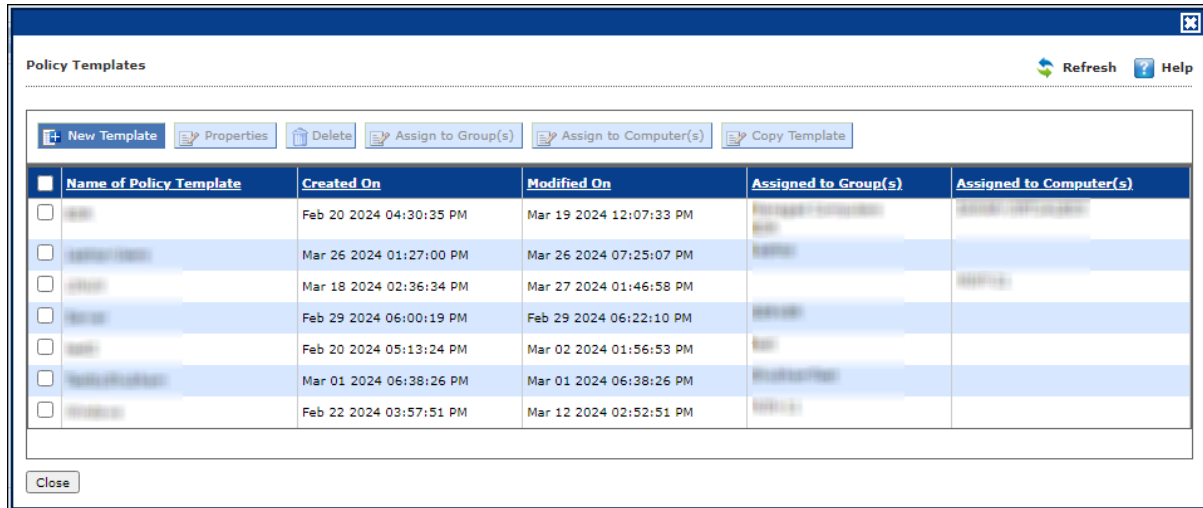
Network Security module helps to set Firewall to monitor all incoming and outgoing network traffic and protect your computer from all types of network based attacks. Enabling this features will prevents Zero-day attacks and all other cyber threats. To learn more, [click here](#).

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

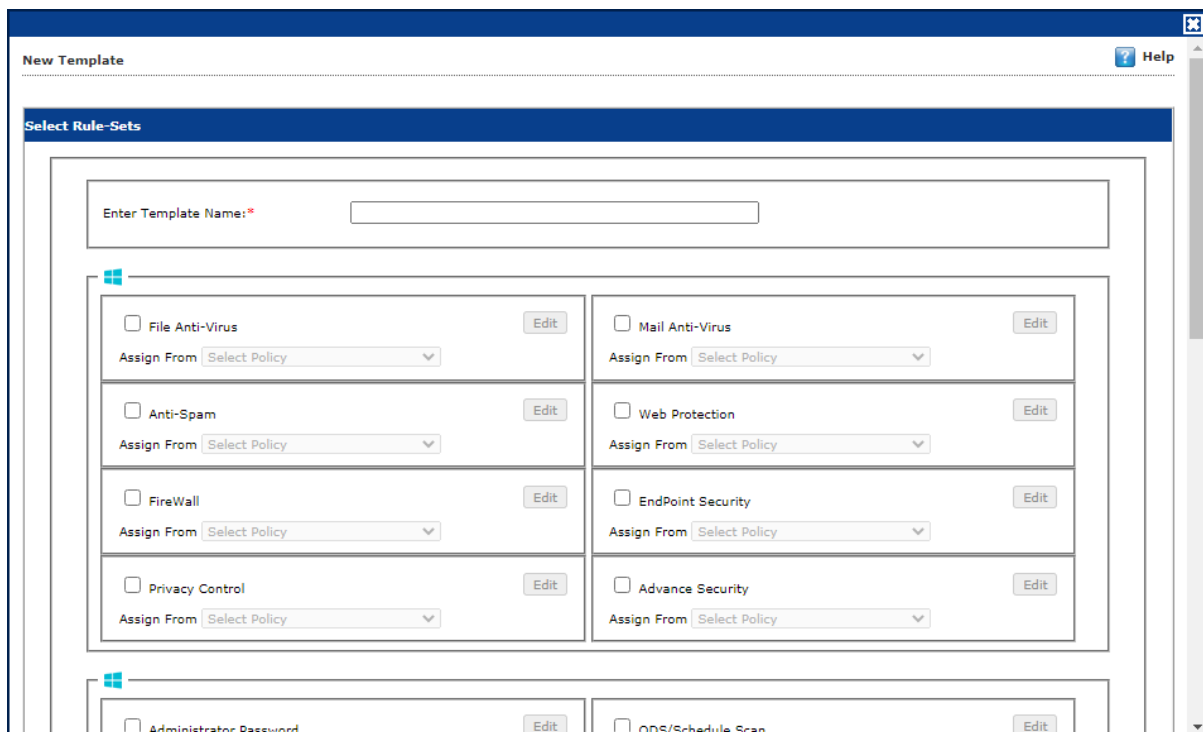
Creating Policy Template for a group/specific computer

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

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



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



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

Configuring eScan Policies for Windows Computers

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

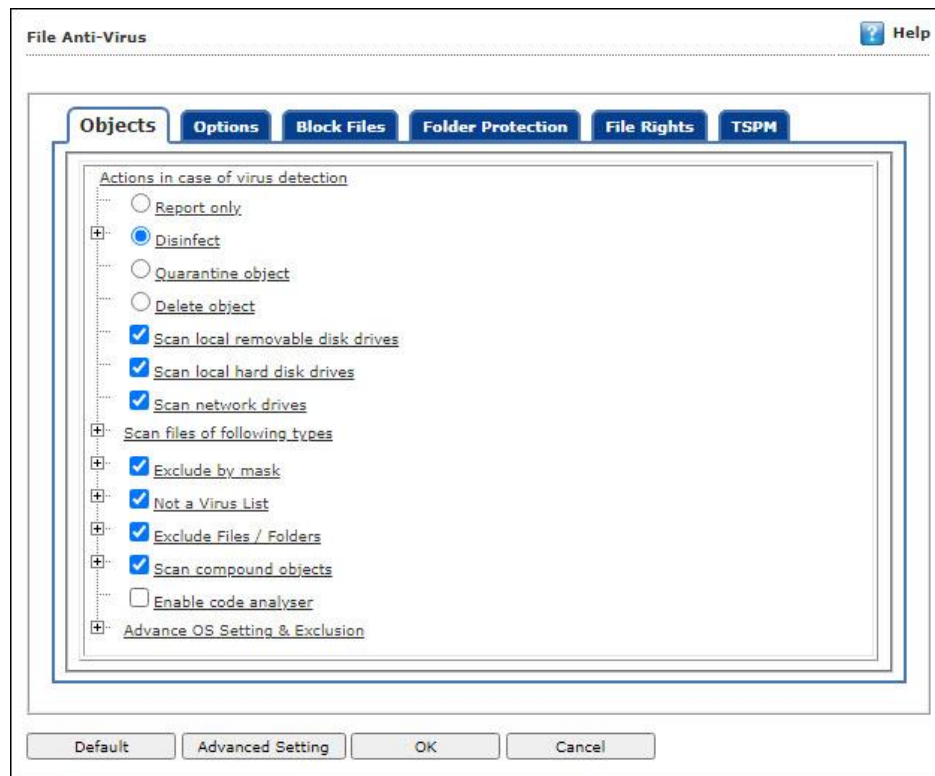
File Anti-Virus

The File Anti-Virus module displays following tabs to configure:

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

Objects

The Objects tab lets you configure following options:



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 [Default]

Upon virus detection, eScan will disinfect the object. This action has 3 additional options as below:

- **Make backup file before disinfection:** It allows you to create a backup of an object before its disinfection.
- **Report only:** If disinfection is not possible, eScan will only report the virus infection.

- **Quarantine object:** If disinfection is not possible, eScan will quarantine the object.
- **Delete object:** If disinfection is impossible, eScan will remove the object from the computer.

Quarantine object

If disinfection is impossible eScan will quarantine the object. 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.

Delete object

If disinfection is impossible, eScan will remove the object from the computer.

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 checkbox 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 checkbox 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 checkbox if you want eScan to scan archives and packed files during scan operations. By default, **Packed** is selected. All the procedures will be followed.

Enable Code Analyzer

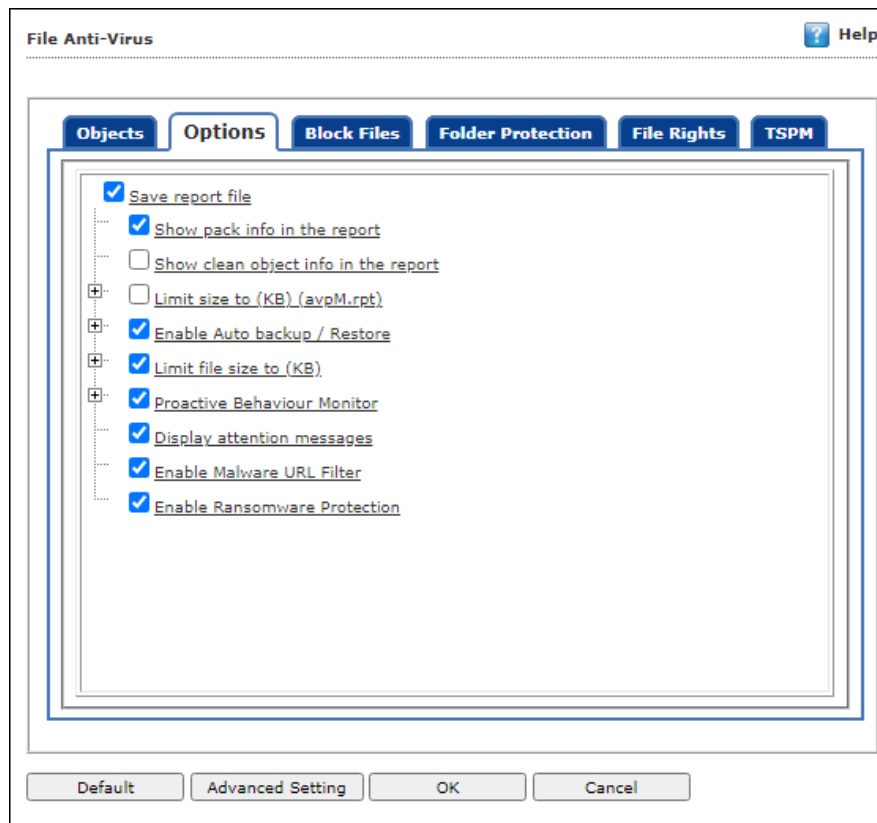
Select this checkbox if you want eScan to scan your computer for suspicious objects or unknown infections by using the heuristic analyzer. After selection, File Anti-Virus not only scans and detects infected objects, but also checks for suspicious files stored on computer.

Advance OS Settings & Exclusion

This option allows you to block the suspicious powershell scripts that can cause damage to the system. Additionally, you can exclude Program data, Valid SVC Parent, and trusted powershell scripts from getting blocked.

Options

The Options tab lets you configure following options:



Save report file [Default]

Select this checkbox 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 checkbox 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 checkbox 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 checkbox 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 checkbox 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 configure 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 checkbox 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 [Default]

Selecting this checkbox enables File Anti-Virus to monitor the computer for suspicious applications/programs and block them on a real-time basis when they try to execute. Selecting this checkbox enables below options to configure:

- **Ask user for action**
This option allows user to receive the confirmation prompt before Proactive Behavior Monitor blocks the suspicious application/program. Select **Yes**, to proceed with the blocking of application and **No** to cancel the blocking.
- **White List**
Whitelisting allows you to select the files from the database that you want to exclude from being blocked. To whitelist a file/folder, click **Whitelist** and then click **Add from DB**.

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

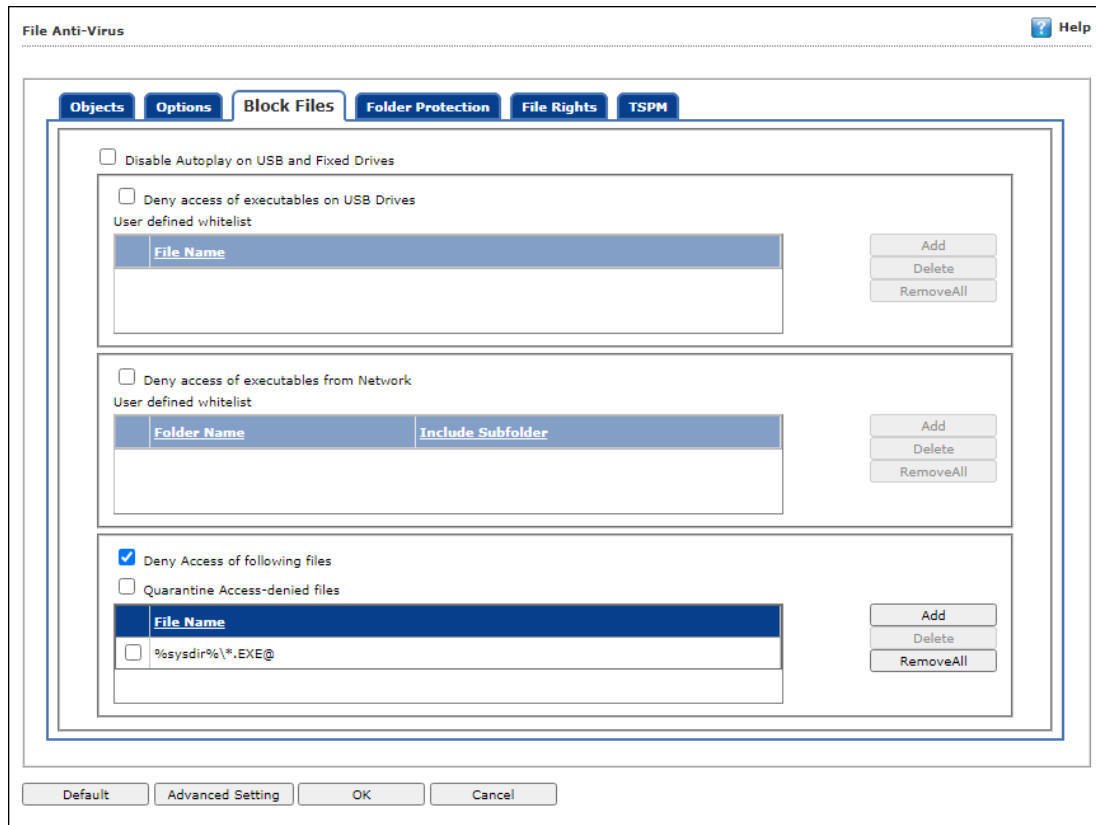
This option lets you enable a Malware URL filter where eScan blocks all URLs that are suspected to be malwares. You can exclude specific websites by whitelisting them from the eScan pop up displayed when you try to access the site.

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 Behavior 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.



You can configure the following settings:

Disable AutoPlay on USB and Fixed Drives

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

Deny access of executables on USB Drives

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

Deny access of executable from Network

Select this checkbox 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** checkbox. 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

Add Cancel

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 checkbox if you want eScan to prevent the files in the list from running on the computers.

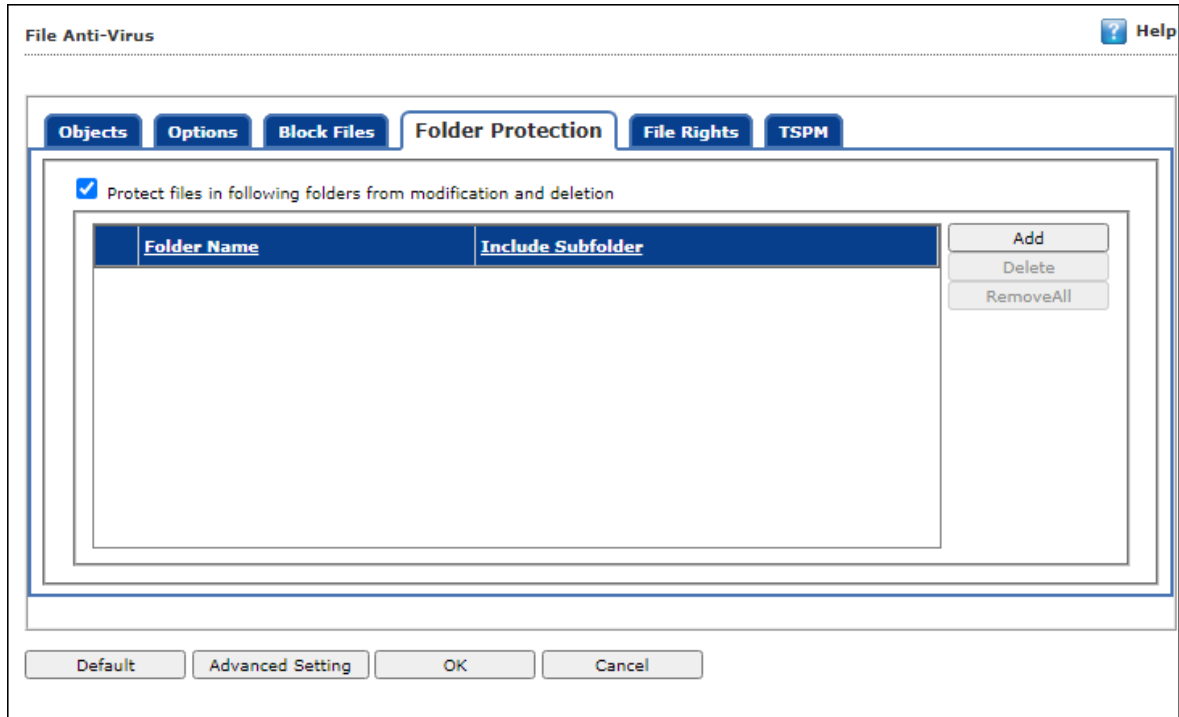
Quarantine Access-denied files

Select this checkbox 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:

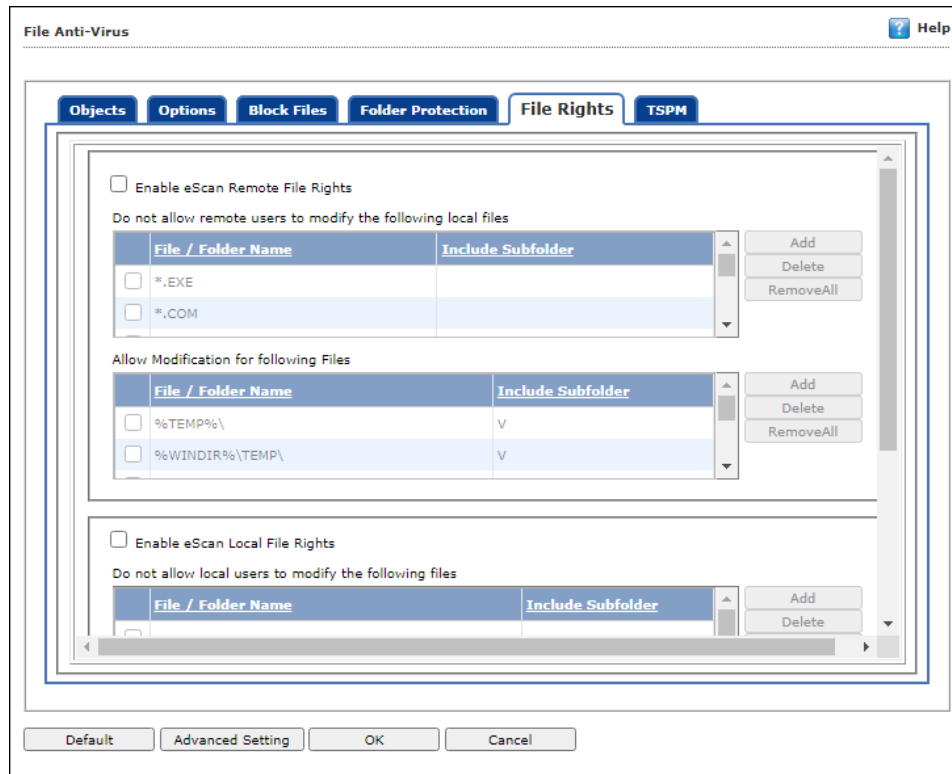


Protect files in following folders from modification and deletion [Default]

Selecting this checkbox 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.



Enable eScan Remote File Rights

Select this checkbox 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 checkbox to allow/restrict the local users to make any modifications to the files/folders.

Do not allow local users to modify the following files

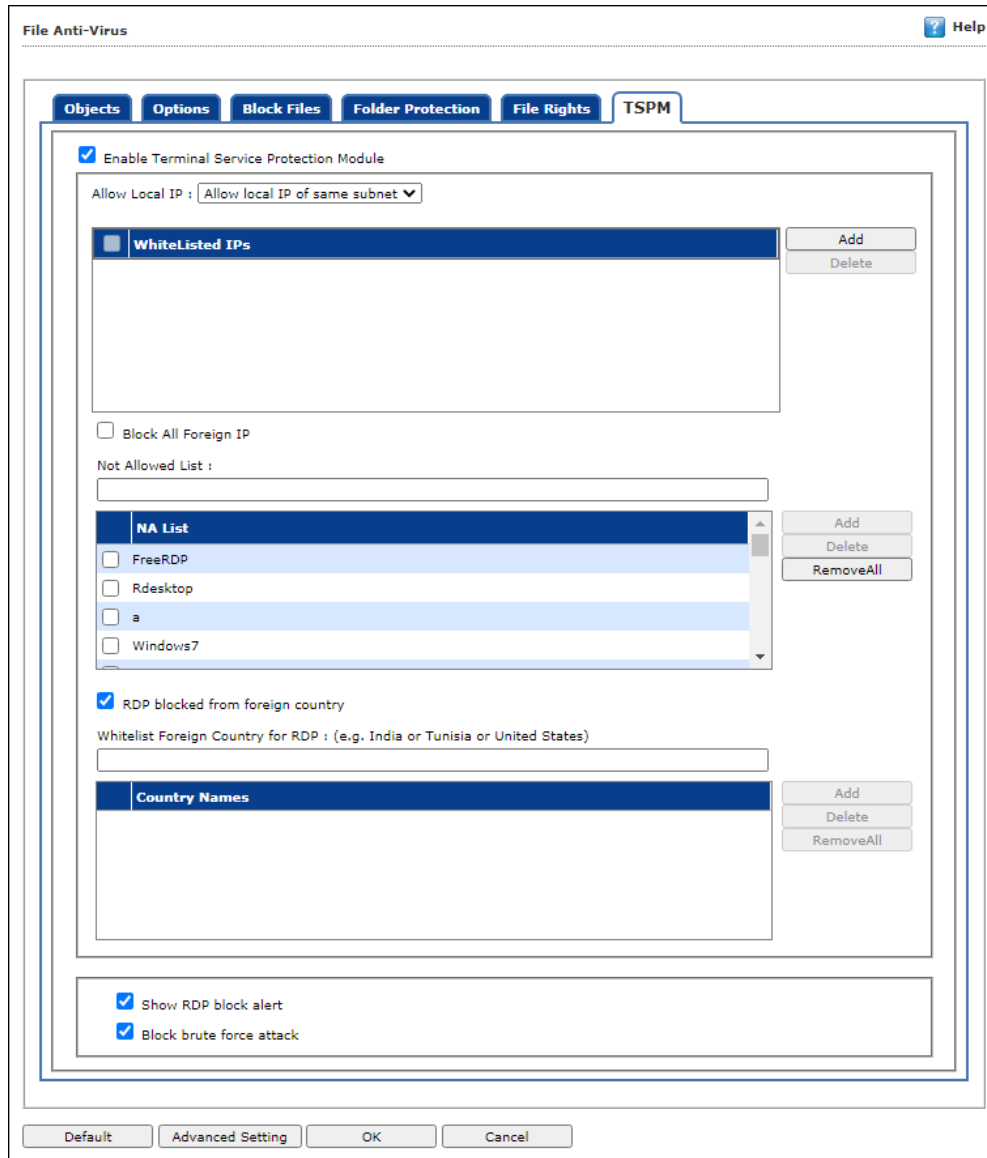
The files/folders added to this list cannot be modified by the local users.

Allow modification for files

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

TSPM

eScan's TSPM (Terminal Service Protection Module) detects brute force attacks, identifies suspicious IP addresses/hosts and blocks the 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.

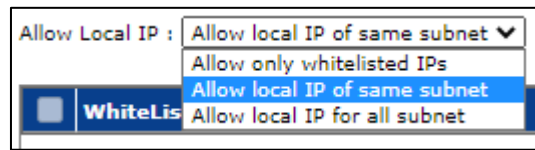


Enable Terminal Service Protection Module

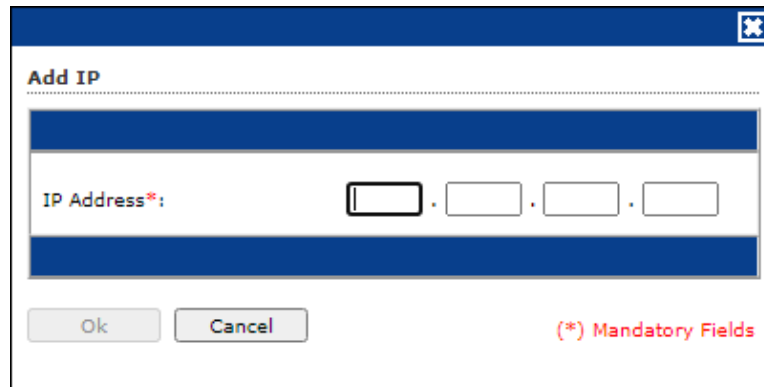
Select this checkbox to activate TSPM module.

Allow Local IP

This dropdown menu has following options:



- Allow only whitelisted IPs:** Select this option to allow only whitelisted IPs to connect to the endpoints.
 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**.

- **Block All Non Whitelisted IPs:** After selecting **Allow only whitelisted IPs** option, this will be available. Select this option to block all IPs other than the whitelisted one.
- Allow local IP of same subnet:** Select this option to allow the local IPs that belongs to same subnet. This option is selected by default.
- Allow local IP for all subnet:** Select this option to allow the local IPs of all subnet in the network.

Block All Foreign IP

Select this checkbox to block all the foreign IP addresses from communicating from the endpoint within the network.

Not Allowed List

This option has pre-defined username that are not allowed to establish connection (via RDP) with the endpoints in the network.

To add custom-defined username, Enter the username and then click **Add**.

To delete the username from pre-defined list, select the name and click **Delete**.

To remove all the usernames from list, click **Remove All**.

RDP blocked from foreign country [Default]

This checkbox blocks all the RDP connection attempts from the foreign country.

Whitelist Foreign Country for RDP: (e.g. India or Tunisia or United States)

This option allows to whitelist the country names, so that RDP connections from those countries can be allowed.

Show RDP block alert [Default]

This checkbox allows eScan to alert the user in case of any RDP connection is blocked.

Block brute force attack [Default]

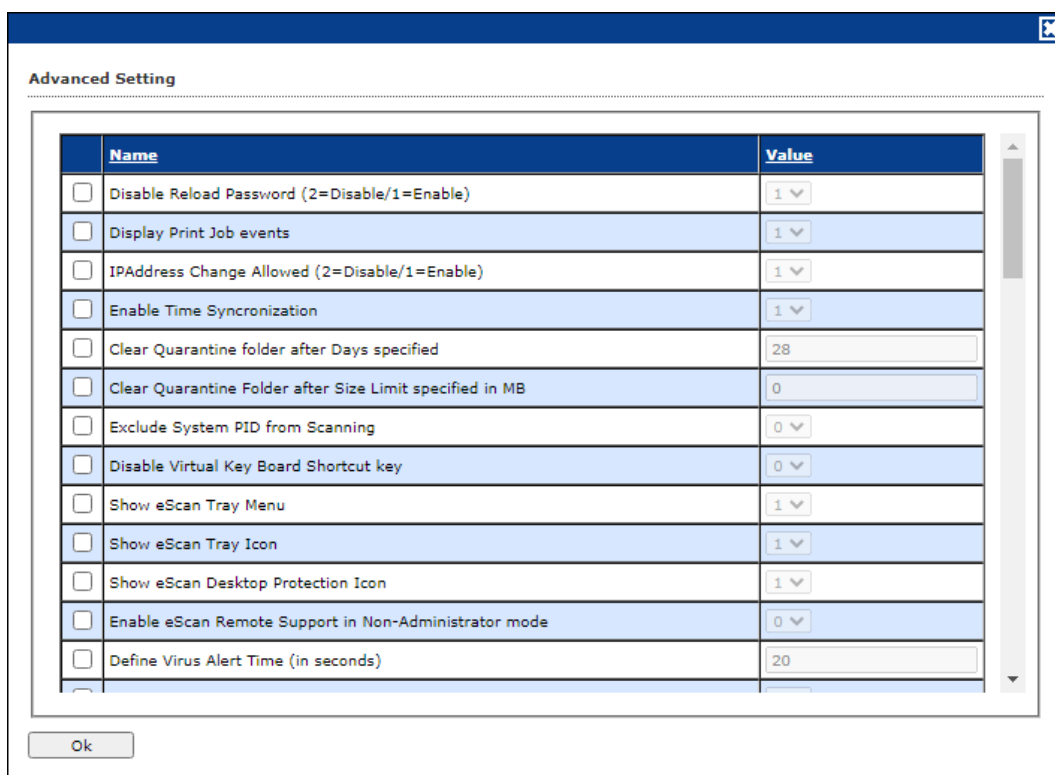
This checkbox allows you to block the connection in case of any brute force attack.

Session Activity Settings

This section provides you with multiple session activities that can be included along with the default session activities in the report to be sent to the eScan server. After policy gets applied, all the selected session activities of the client machine(s) will be captured and included in the report.

Advanced Settings

Clicking **Advanced Settings** lets you configure advanced settings for console.



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 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.

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.

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.

Allow Uninstallers (1 = Enable/0 = Disable)

Selecting this option lets you enable/disable use of third party uninstallers.

Block Renaming of Hosts files (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.

Enable Winsock Protection (Require Restart) (1 = Enable/0 = Disable)

This option lets you Enable/Disable protection at the Winsock Layer.

Disable COPY/PASTE (1 = Enable/0 = Disable)

Selecting this option lets you disable Copy/Paste actions.

PowerShell Exclusion list

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

Block Registry Editor (1 = Enable/ 0 = Disable)

This option lets you Enable/Disable block Registry Editor.

Send Windows Security Patch Events (1-KB patches;2-Security Update; 4- Hotfix; 8-Update;16-Services Pack;31-All) (1 = Enable/ 0 = Disable)

This option lets you Enable/Disable send windows Security Patch Events.

Block MS Office (1-All/2-All except Outlook) (1 = Enable/ 0 = Disable)

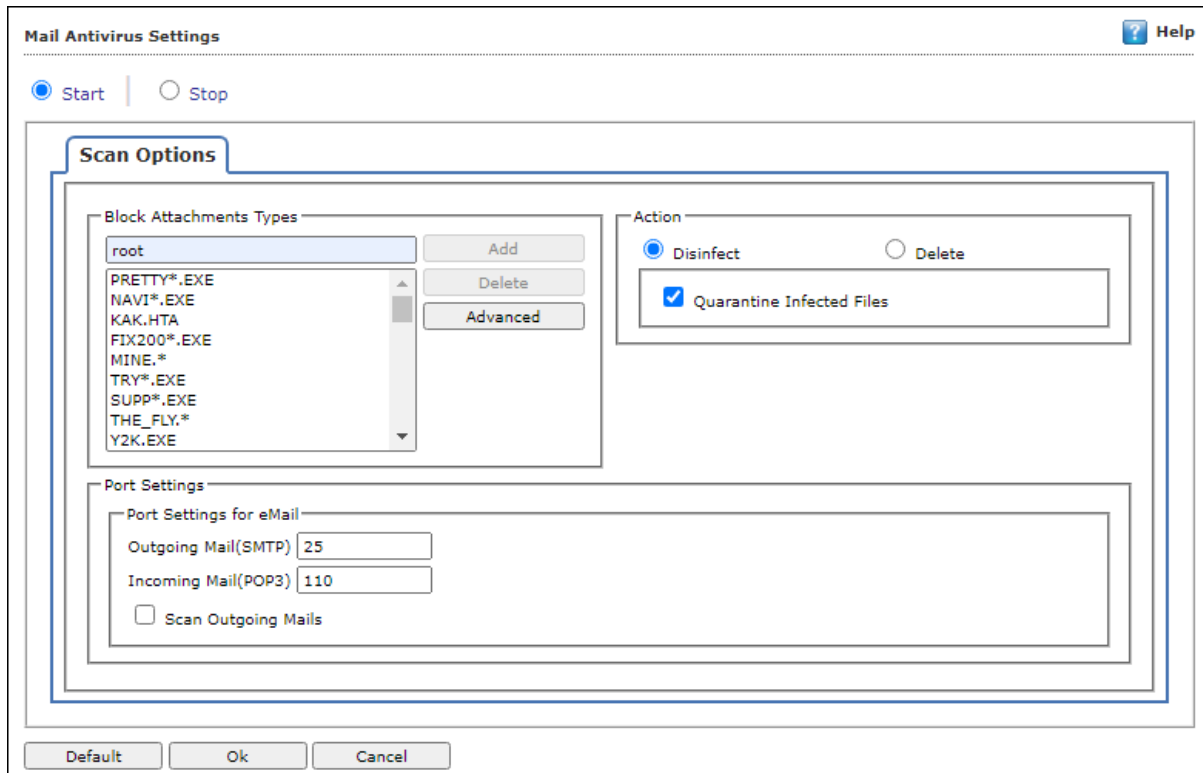
This option lets you Enable/Disable block MS Office.

Block Gmail (except corporate ones) (1 = Enable/ 0 = Disable)

This option lets you Enable/Disable block Gmail.

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.



The screenshot shows the 'Mail Antivirus Settings' dialog box. At the top, there are radio buttons for 'Start' (selected) and 'Stop'. Below this is the 'Scan Options' tab. The 'Block Attachments Types' section contains a list box with 'root' selected and a scrollable list of file extensions: PRETTY*.EXE, NAVI*.EXE, KAK.HTA, FIX200*.EXE, MINE.*, TRY*.EXE, SUPP*.EXE, THE_FLY.*, and Y2K.EXE. To the right of the list are 'Add', 'Delete', and 'Advanced' buttons. The 'Action' section has radio buttons for 'Disinfect' (selected) and 'Delete', and a checked checkbox for 'Quarantine Infected Files'. The 'Port Settings' section has input fields for 'Outgoing Mail(SMTP)' (25) and 'Incoming Mail(POP3)' (110), and an unchecked checkbox for 'Scan Outgoing Mails'. At the bottom are 'Default', 'Ok', and 'Cancel' buttons.

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:

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 checkbox to quarantine an entire email if it contains an attachment not scanned by Mail Anti-Virus.

Quarantine Attachments if they are scanned

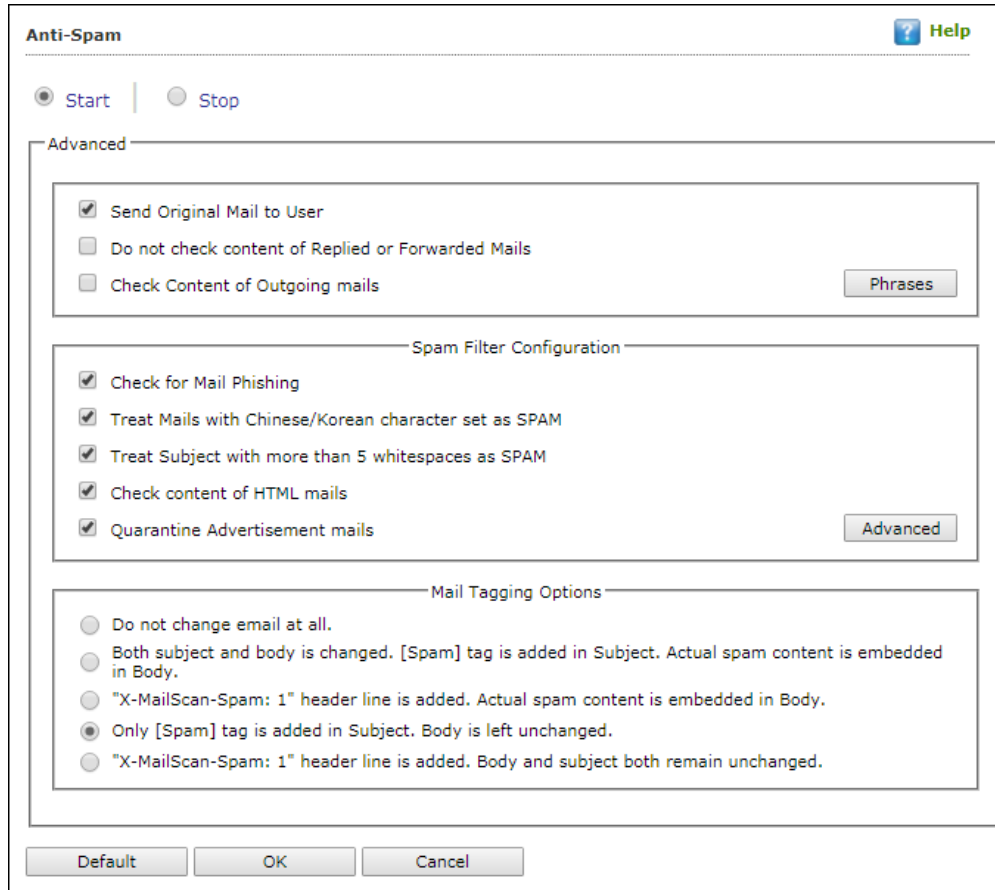
Select this checkbox if you want eScan to quarantine attachments that are scanned by Mail Anti-Virus.

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:



The screenshot shows the 'Anti-Spam' configuration window. At the top, there are radio buttons for 'Start' (selected) and 'Stop'. Below this is a 'Help' button. The main area is divided into three sections: 'Advanced', 'Spam Filter Configuration', and 'Mail Tagging Options'. The 'Advanced' section contains three checkboxes: 'Send Original Mail to User' (checked), 'Do not check content of Replied or Forwarded Mails' (unchecked), and 'Check Content of Outgoing mails' (unchecked). A 'Phrases' button is located to the right of these checkboxes. The 'Spam Filter Configuration' section contains five checkboxes: 'Check for Mail Phishing' (checked), 'Treat Mails with Chinese/Korean character set as SPAM' (checked), 'Treat Subject with more than 5 whitespaces as SPAM' (checked), 'Check content of HTML mails' (checked), and 'Quarantine Advertisement mails' (checked). An 'Advanced' button is located to the right of these checkboxes. The 'Mail Tagging Options' section contains five radio buttons: 'Do not change email at all.' (unchecked), 'Both subject and body is changed. [Spam] tag is added in Subject. Actual spam content is embedded in Body.' (unchecked), '"X-MailScan-Spam: 1" header line is added. Actual spam content is embedded in Body.' (unchecked), 'Only [Spam] tag is added in Subject. Body is left unchanged.' (checked), and '"X-MailScan-Spam: 1" header line is added. Body and subject both remain unchanged.' (unchecked). At the bottom of the window are three buttons: 'Default', 'OK', and 'Cancel'.

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 checkbox 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 checkbox, 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 checkbox, 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 checkbox, if you want Anti-Spam to check outgoing emails for restricted content.

Phrases

Click **Phrases** to open the **Phrases to Check** 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.

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 particular score. 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 checkbox 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 [Default]

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]

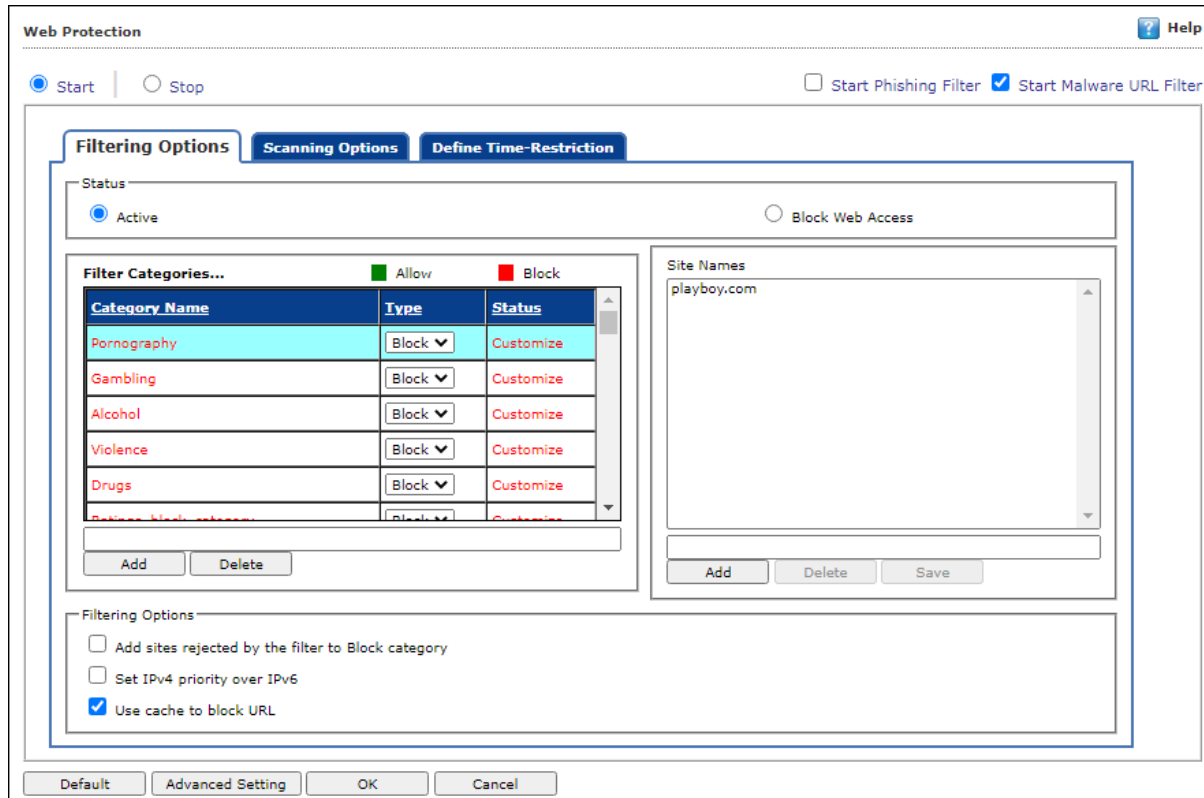
This option lets you add the [Spam] tag only in the subject of the email, which has been identified as spam.

"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.



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

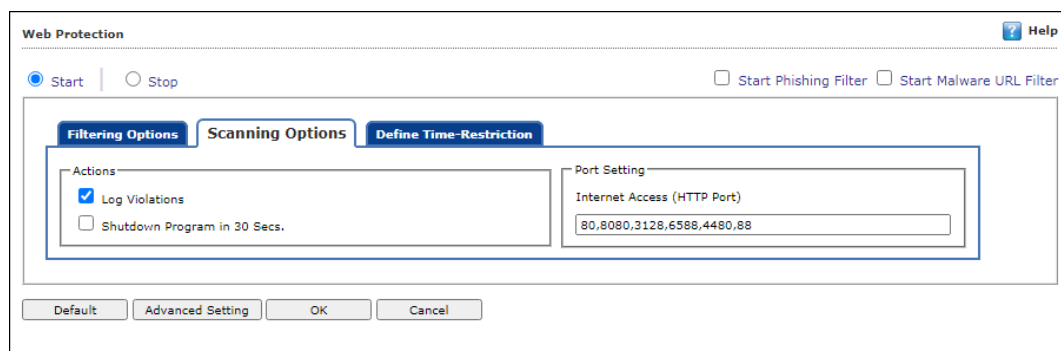
This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category. You can also add or delete filter categories depending on your requirement.

Filtering Options

This section includes the **Add sites rejected by the filter to Block category checkbox**. 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.



Actions

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

Log Violations [Default]

This checkbox 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

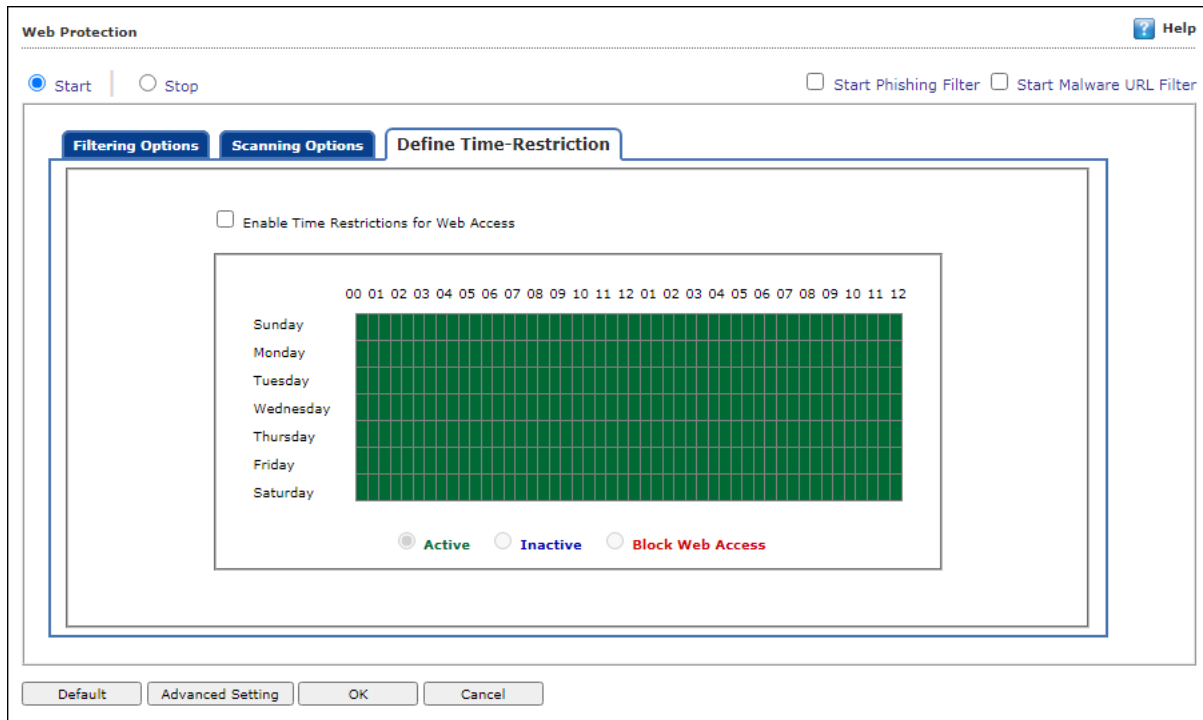
This section lets you specify the port numbers that eScan should monitor for suspicious traffic.

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.



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.

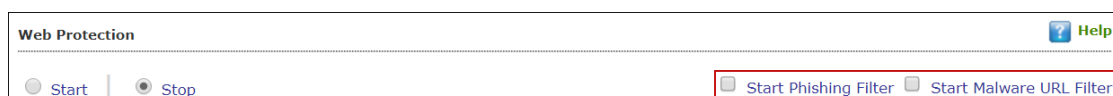
Block Web Access

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 checkboxes.



Advanced Setting

Ignore IP address from Web-scanning

Select this option to enter IP address form Web-Scanning.

Enable Unknown Browsers detection

Select this option to enable/disable unknown browser detection.

Enable allowing of WhiteListed Site during BlockTime

Select this option to enable/disable white listed site during block time.

Enable Online Web-Scanning Module

Select this option to enable/disable online web-scanning module.

Disable Web Warning Page

Select this option to enable/disable web warning page.

Enable HTTPS Popup

Select this option to enable/disable HTTPS Popup.

Show External Page for Web blocking (Page to be define under External Page)

Select this option to enable/disable external page for web blocking.

External Page Link for Web blocking (Depends on Show External Page)

Select this option to enter external page link for web blocking.

Force inclusion of Application into Layer scanning (MW Layer)

Select this option to enter Force inclusion of Application into Layer scanning.

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

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

Ignore Reference of sub-link

Select this option to enable/disable Ignore Reference of sub-link.

Allow access to SubDomain for Whitelisted sites (Only HTTP Sites)

Select this option to enable/disable access to SubDomain for Whitelisted sites.

Allow access to SubDomain for Whitelisted sites (Only HTTPS Sites)

Select this option to enable/disable access to SubDomain for Whitelisted sites.

Enable logging of visited websites

Select this option to enable/disable logging of visited websites.

Block EXE download from HTTP Sites (1 = Enable/0 = Disable)

Select this option to enable/disable block download of .exe files from HTTP websites.

Block HTTP Traffic only on Web Browser

Select these options to enable/disable block HTTP Traffic on Web Browser.

Allow website list (Depends on "Block HTTP Traffic only on Web Browser")

Select this option to enter to block HTTP Traffic on Web Browser.

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)

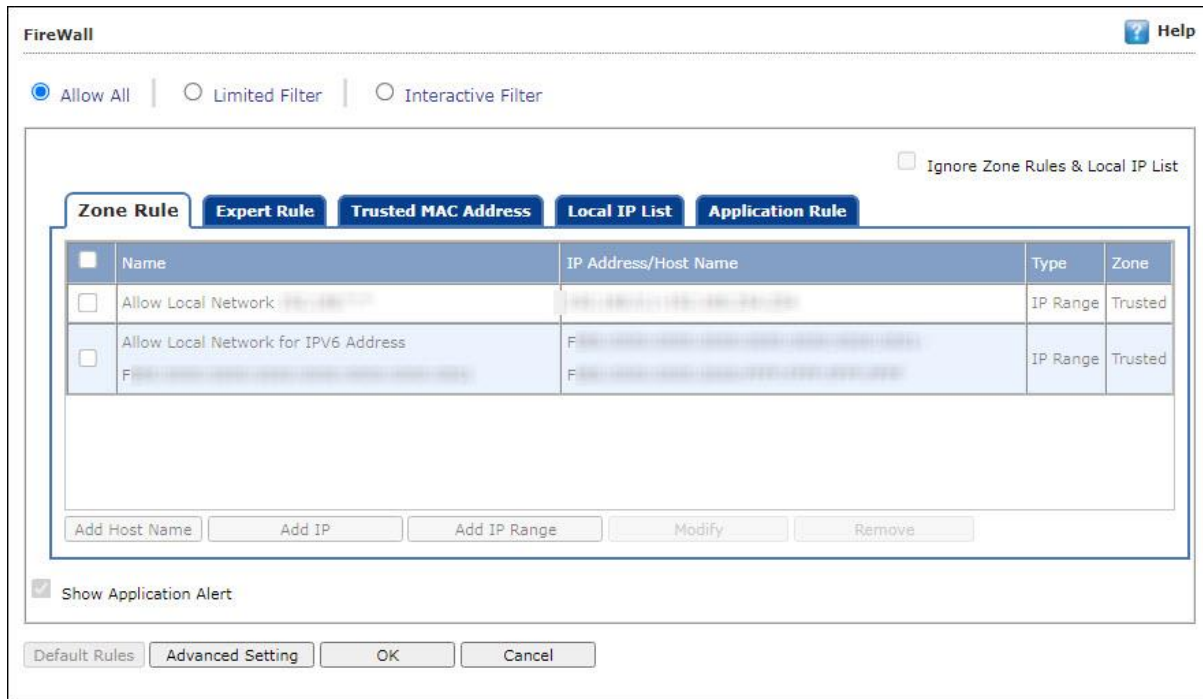
Select this option to force enable/disable web protection using filter driver.

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.



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 Filter – Clicking **Interactive Filter** 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

Ignore Zone Rules & Local IP List – This option allows you to override the Zone Rule configuration that has whitelisted IP ranges. It also overrides the Local IP list that consists of trusted local IP addresses. By selecting this checkbox, all the IP addresses listed under Zone Rule and Local IP List will be monitored by Firewall as per selected filter type.

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.

FireWall ? Help

Allow All |
 Limited Filter |
 Interactive Filter

Ignore Zone Rules & Local IP List

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

Firewall Rule	Rule Action Summary
<input type="checkbox"/> UDP Rule	Permits UDP packets on Any Interface between "My Netw
<input type="checkbox"/> ARP packet exchange - For mapping IP address to a hardware (MAC) address	Permits ARP packets on Any Interface
<input type="checkbox"/> NetBios (LAN File Sharing) - Access files and folders on other computers, from your computer	Permits TCP and UDP packets on Any Interface between "
<input type="checkbox"/> NetBios (LAN File Sharing) - Access files and folders on my computer, from other computers	Blocks TCP and UDP packets on Any Interface between "A
<input type="checkbox"/> ICMP messages	Permits ICMP packets on Any Interface between "My Netw
<input type="checkbox"/> ICMPV6 messages	Permits ICMPV6 packets on Any Interface between "My N
<input type="checkbox"/> DHCP/BOOTP packet exchange	Permits UDP packets on Any Interface between "Any Addi
<input type="checkbox"/> FTP Control - For downloading and uploading files	Permits TCP packets on Any Interface between "My Netw

Show Application Alert

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:

The screenshot shows a dialog box titled "Add Firewall Rule" with four tabs: "General", "Source", "Destination", and "Advanced". The "General" tab is selected and contains the following fields:

- Rule Name:** A text input field containing "Rule1".
- Rule Action:** Two radio buttons: "Permit Packet" (selected) and "Deny Packet".
- Protocol:** A dropdown menu showing "TCP and UDP".
- Apply Rule on Interface:** A dropdown menu showing "Any Interface".

At the bottom of the dialog box are "OK" and "Cancel" buttons.

General tab

In this section, specify the Rule settings:

Rule Name – Provide a name to the Rule.

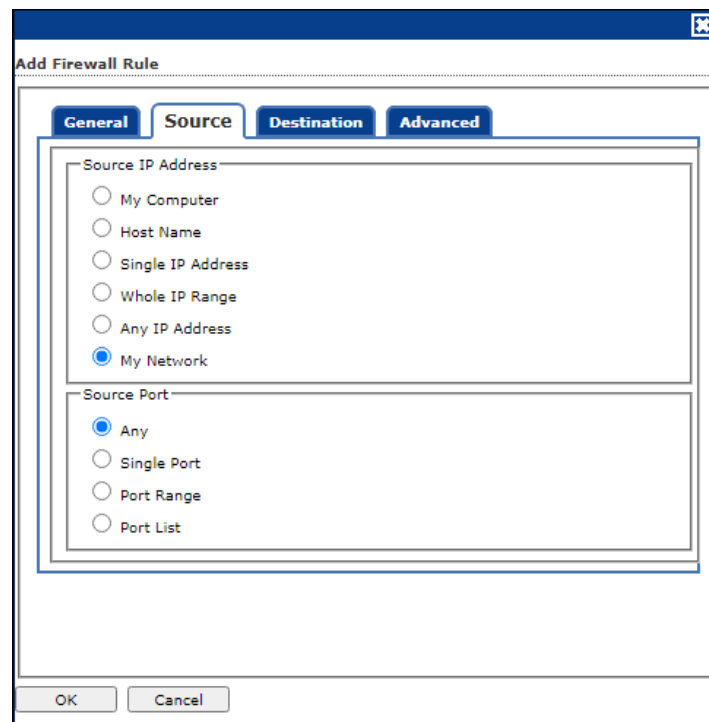
Rule Action – Action to be taken, whether to Permit Packet or Deny Packet.

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.



Source IP Address

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.

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

Source Port

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

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

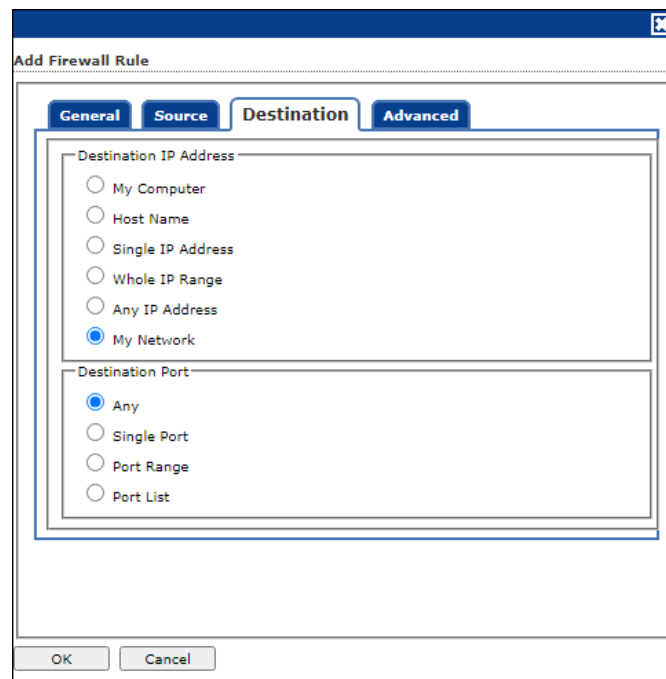
Port Range – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the outgoing traffic originating from the port which is within the defined range of ports.

Port List – A list of 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 are within the defined IP range.

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

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

Destination Port

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

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

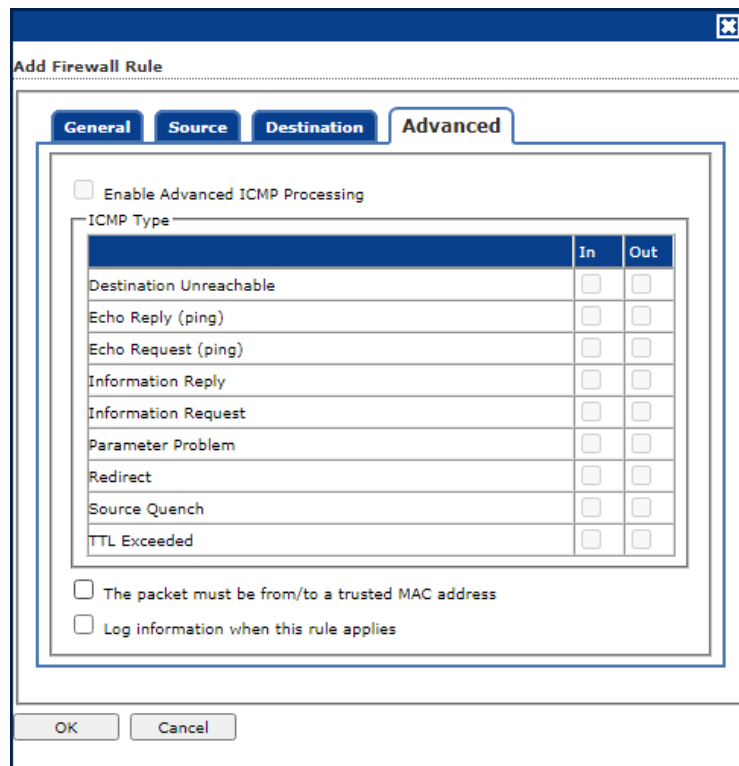
Port Range – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the incoming traffic to the port which is within the defined range of ports.

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.



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 applied.

Following are additional buttons the Expert Rule tab provides:

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 / Disable– 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-

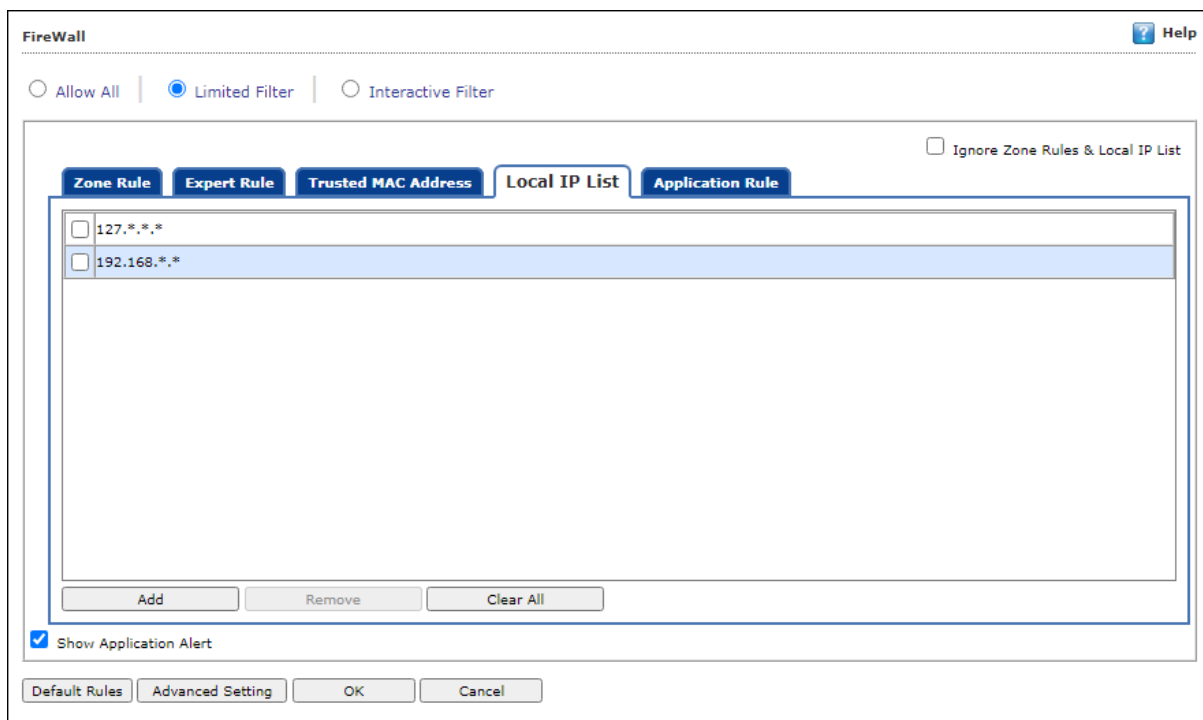
Edit – To modify/change the MAC Address, click **Edit**.

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.



The screenshot shows the 'FireWall' configuration window with the 'Local IP List' tab selected. The window has a title bar with 'FireWall' and a 'Help' icon. Below the title bar are three radio buttons: 'Allow All' (unselected), 'Limited Filter' (selected), and 'Interactive Filter' (unselected). To the right of these buttons is a checkbox labeled 'Ignore Zone Rules & Local IP List' which is also unselected. Below this is a tabbed interface with five tabs: 'Zone Rule', 'Expert Rule', 'Trusted MAC Address', 'Local IP List' (active), and 'Application Rule'. The 'Local IP List' tab contains a list with two entries: '127.*.*' and '192.168.*.*', each with a checkbox to its left. Below the list are three buttons: 'Add', 'Remove', and 'Clear All'. At the bottom left of the window is a checked checkbox labeled 'Show Application Alert'. At the very bottom are four buttons: 'Default Rules', 'Advanced Setting', 'OK', and 'Cancel'.

Add – To add a local IP address, click **Add**.

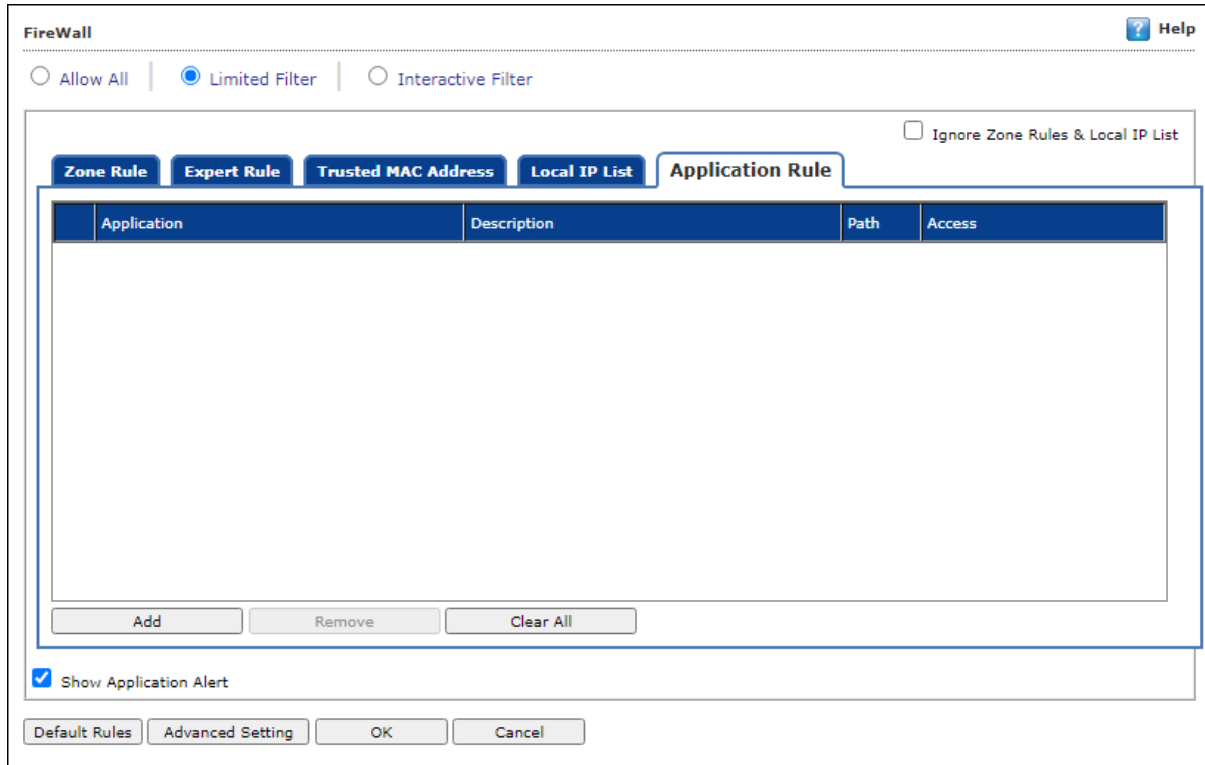
Remove – To remove a local IP address, click **Remove**.

Clear All – To clear all local IP addresses, click **Clear All**.

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

Application Rule

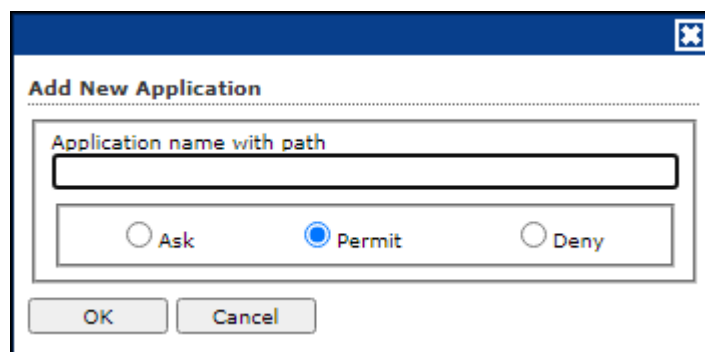
In this section you can define the permissions for different application. The application can be set to Ask, Permit or Deny mode.



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 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:

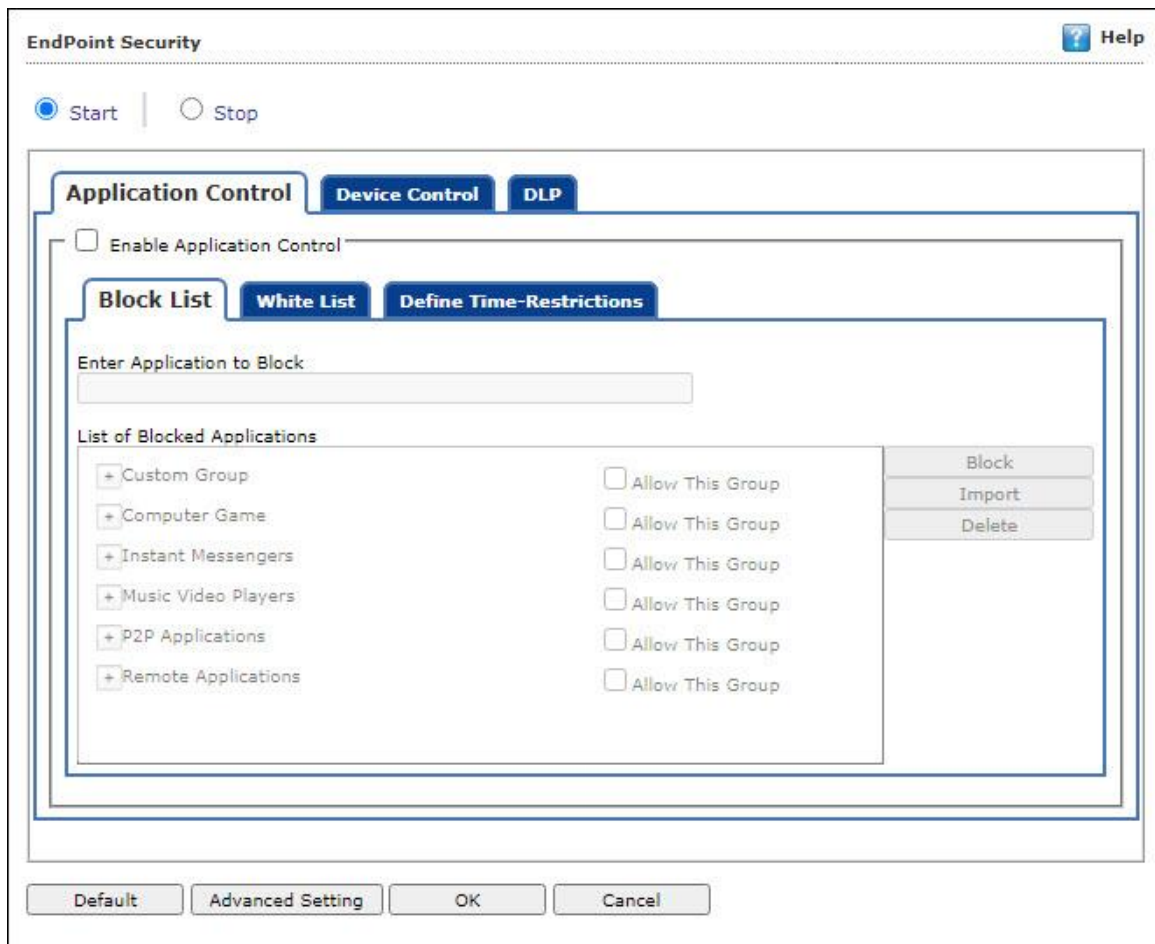
- **Clear All** - This option will clear/delete all the information stored by the Firewall cache.
- **Show Application Alert** – Selecting this option will display an eScan Firewall Alert displaying the blocking of any application as defined in the Application Rule.
- **Default Rules** - This button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

Advanced Setting	
Name	Value
<input type="checkbox"/> Disable Trojan Rule	1 ▼
<input type="checkbox"/> Block Portscan	0 ▼

- **Disable Trojan Rule:** It allows you to disable the blocking of programs that are either Trojan malware or follow Trojan rule.
- **Block Portscan:** It allows you to block the scanning of network ports.

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.



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, Device Control, and DLP which are as follows:

Application Control

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

Enable Application Control

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

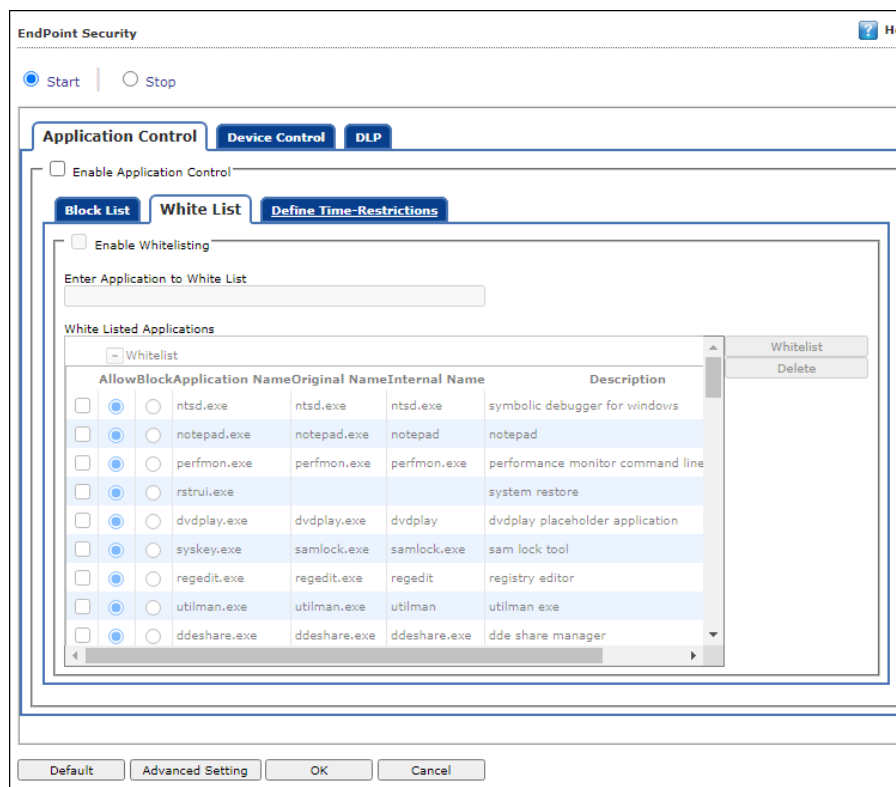
Block List

Enter Application to Block: It indicates the name of the application you want to block from execution. Enter the 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. The **Allow This Group** checkbox in front of each group allows that entire group.

White List



Enable Whitelisting

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

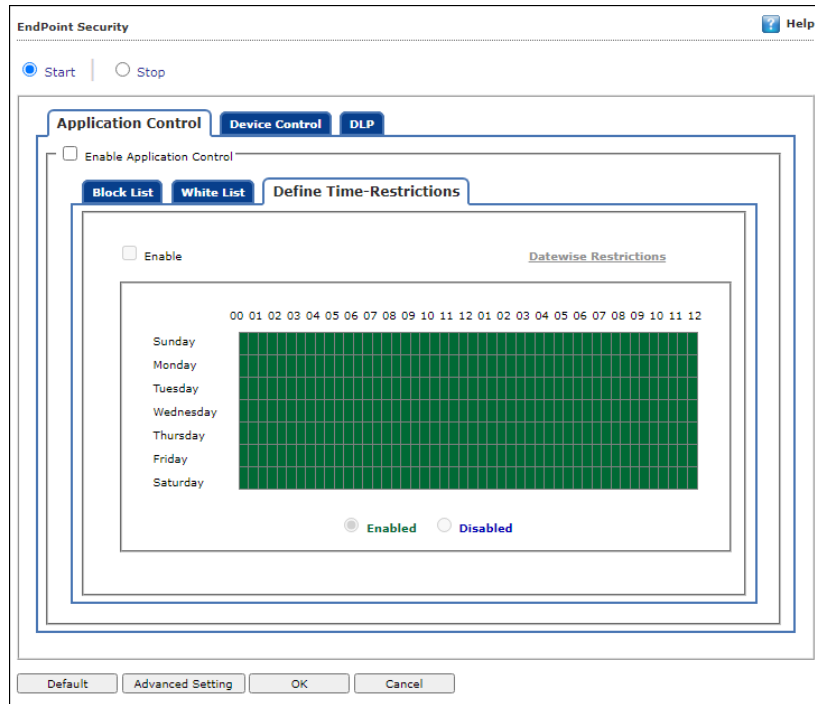
Enter Application to whitelist

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 applications, 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.

The screenshot shows the 'Device Control' configuration window. At the top, there are three tabs: 'Application Control', 'Device Control' (which is active), and 'DLP'. Below the tabs, there is a checked checkbox for 'Enable Device Control'. Underneath, there are three main sections:

- USB Settings:** Contains checkboxes for 'Block USB Ports' and 'Ask for Password'. Below these are radio buttons for 'Use eScan Administrator Password' (selected) and 'Use Other Password' with an adjacent text input field. Further down are checkboxes for 'Do Virus Scan' (checked), 'Read Only - USB', 'Allow user to cancel scan' (checked), and 'Disable AutoPlay'.
- Whitelist:** Contains checkboxes for 'Scan Whitelisted USB Devices' and 'Remove Read Only access for Whitelisted USB Device'. Below these is a table with columns 'Serial No.', 'Device Name', and 'Description'. To the right of the table are buttons for 'Add', 'Import', 'Edit', 'Delete', 'RemoveAll', and 'Print'.
- CD / DVD Settings:** Contains checkboxes for 'Block CD / DVD' and '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 storage devices connected to your endpoint. This will enable all the options in this tab.

USB Settings

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

Block USB Ports

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

Ask for Password

Select this option, if you want eScan to prompt for a password whenever a USB storage device is connected to the computer. You have to enter the correct password to access USB storage device. It is recommended that you always keep this checkbox selected.

- **Use eScan Administrator:** This option is available only when you select the **Ask for Password** checkbox. 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** checkbox. 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 checkbox selected.

Allow user to cancel scan

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

Read Only – USB

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

Disable AutoPlay [Default]

When you select this option, eScan disables the automatic execution of any program stored on a USB storage device when you connect the device.

Whitelist

eScan provides a greater level of endpoint security by prompting you for a password whenever you connect a USB drive. To disable password protection for a specific device, you can add it along with its serial number to the whitelist. The next time 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.

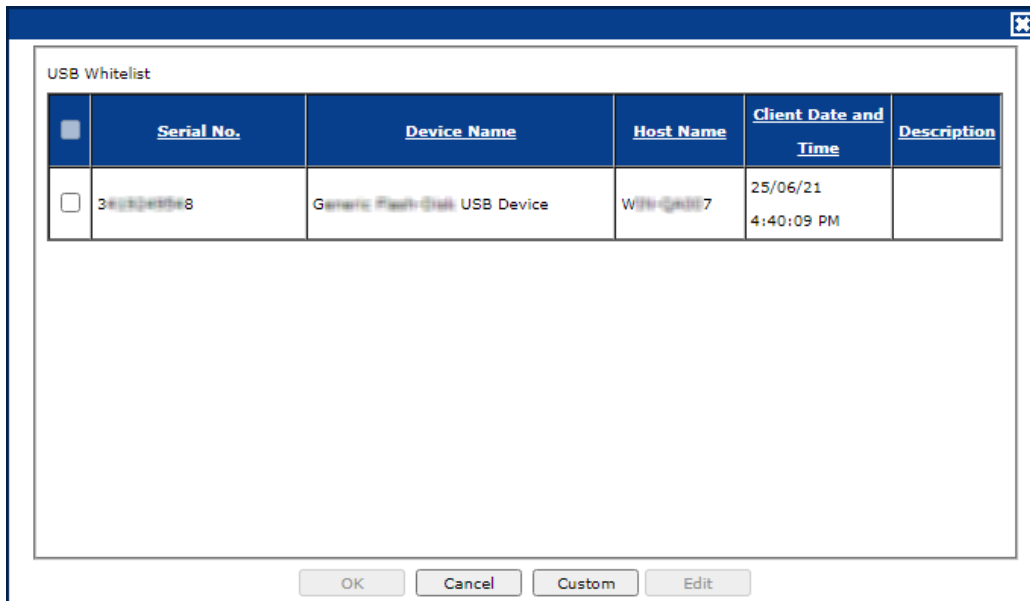
Remove Read Only access for Whitelisted USB Device

Select this option to remove the read-only access for the whitelisted USB Device.

Add

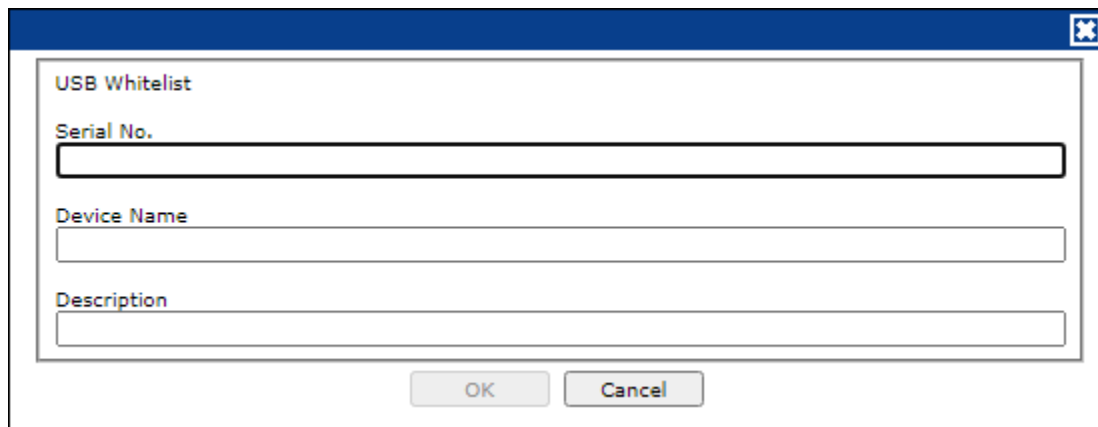
Click **Add** to whitelist USB devices.

USB Whitelist window appears.



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**.



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

E.g. SDFSD677GFQW8N6CN8CBN7CXVB, USB Drive 2.5, Whitelist by
xyzDFRGHRS54456HGDF347OMCNAK, 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.

Disable Hotspot: Select this option to disable Hotspot.

CD / DVD Settings

Block CD / DVD: Select this option to block all CD/DVD access.

Read Only - CD / DVD: Select this option to allow read-only access for CD/DVD.

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

DLP

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

EndPoint Security Help

Start | Stop

Attachment Control | Content Control | IM / Print Screen

Sensitive File/Folder Protection | Clipboard Control | File Activity Monitoring

Workspace Apps | Disk Encryption | Remote Access Software | Control sync settings

Attachment Allowed
 Attachment Blocked

Enter Process Name : Eg. Thunderbird.exe

Add Delete

Blacklisted Process Ignore Whitelisted Sites only for Blacklisted process

Process Name	Allow Only Whitelisted Site

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

Enter Site Name : Eg. Gmail.com, Yahoo

Add Delete

Whitelisted sites

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

Enable Shadow Copy for Attachment Allowed

Shadow Copy folder path :

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

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

Default | Advanced Setting | OK | Cancel

Attachment Control

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

Attachment Allowed [Default]

Select this option if you want attachments to be allowed through all processes except a user specified set of processes.

Attachment Blocked

Select this option if you want attachments to be blocked through all processes except a user specified set of processes.

Configure Extension/Group based Whitelisting

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

Enter Process Name

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

Blacklisted Process

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

Whitelisted Process

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

Ignore Whitelisted Sites only for Blacklisted process [Default]

Select this checkbox to ignore the whitelisted sites for process mentioned in Blacklist.

Enter Site Name

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

Whitelisted Sites

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

Attachment / Email report

Report for Attachment Allowed

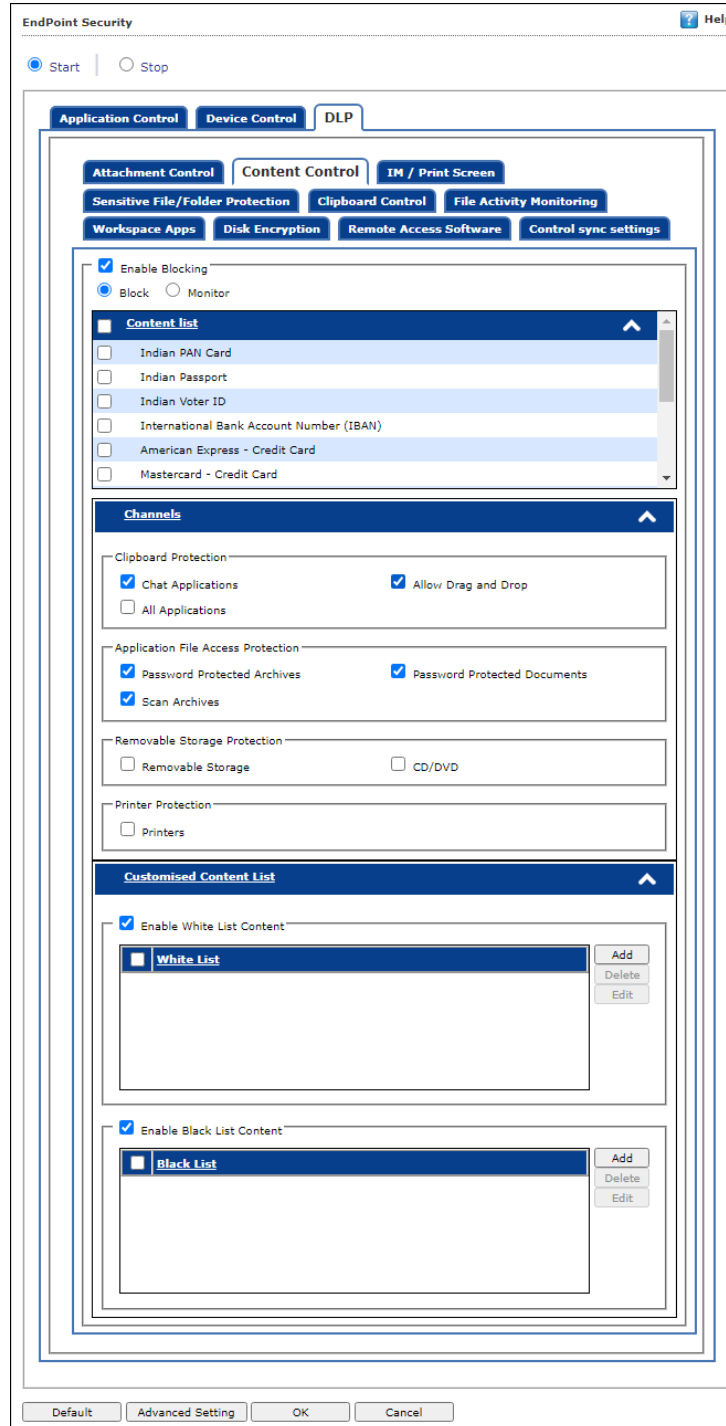
This will list all the attachment allowed along with Application used to send attachment. E.g. Chrome, Firefox, Outlook, Skype, Yahoo messenger, etc.

Report for all email (Including Attachment)

This will list all the email attachment uploaded along with Application used and subject of the email.

Content Control

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



Enable Blocking

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

Block:

Monitor:

Content List

Select this option to block sensitive information from all the listed documents like Credit/Debit Card, Passport, Pan Card, and Driving License.

Channels

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

Clipboard Protection

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

Application File Access Protection

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

Removable Storage Protection

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

Printer Protection

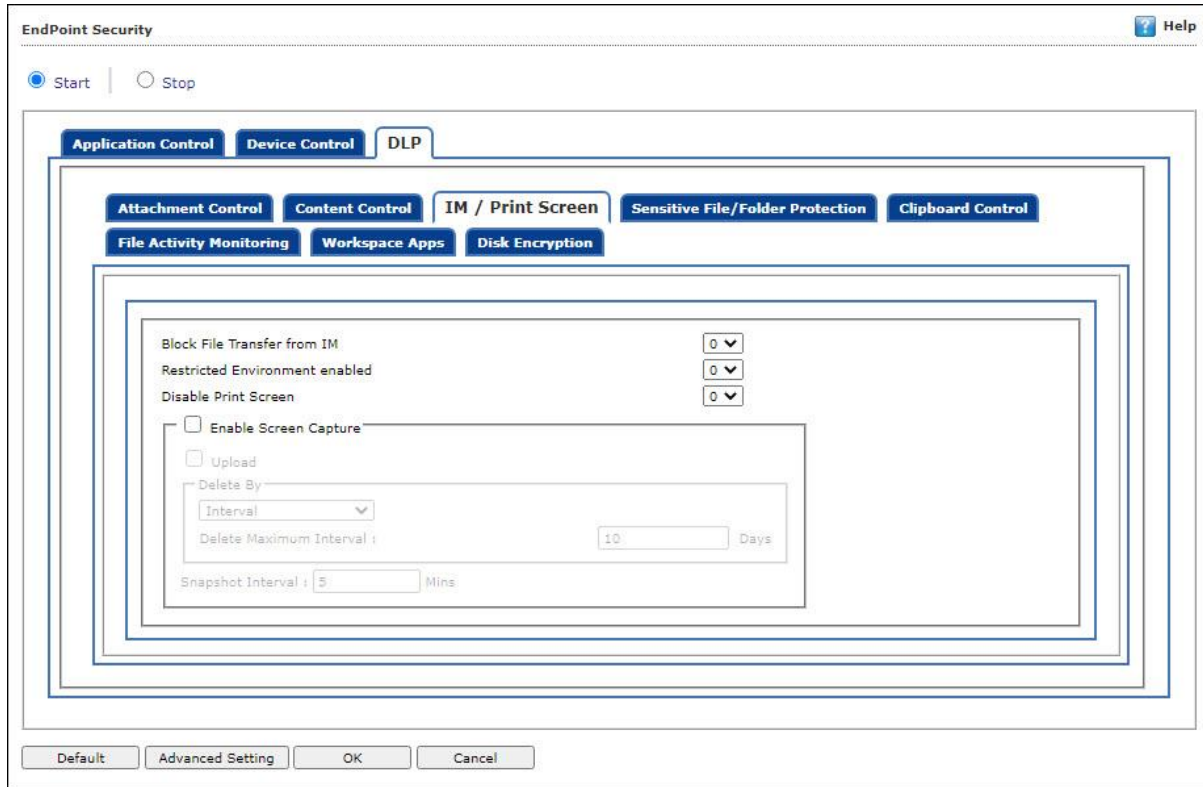
- **Printers:** Select this option to deny the use of networked printers to print the sensitive data.

Customized Content List

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

IM / Print Screen

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



Block File Transfer from IM (1 = Enable/0 = Disable)

Select this option to allow/block file transfer from Instant Messengers.

Restricted Environment enabled (1 = Enable/0 = Disable)

Selecting this option lets you enable/disable protected environment settings.

Disable Print Screen (1 = Enable/0 = Disable)

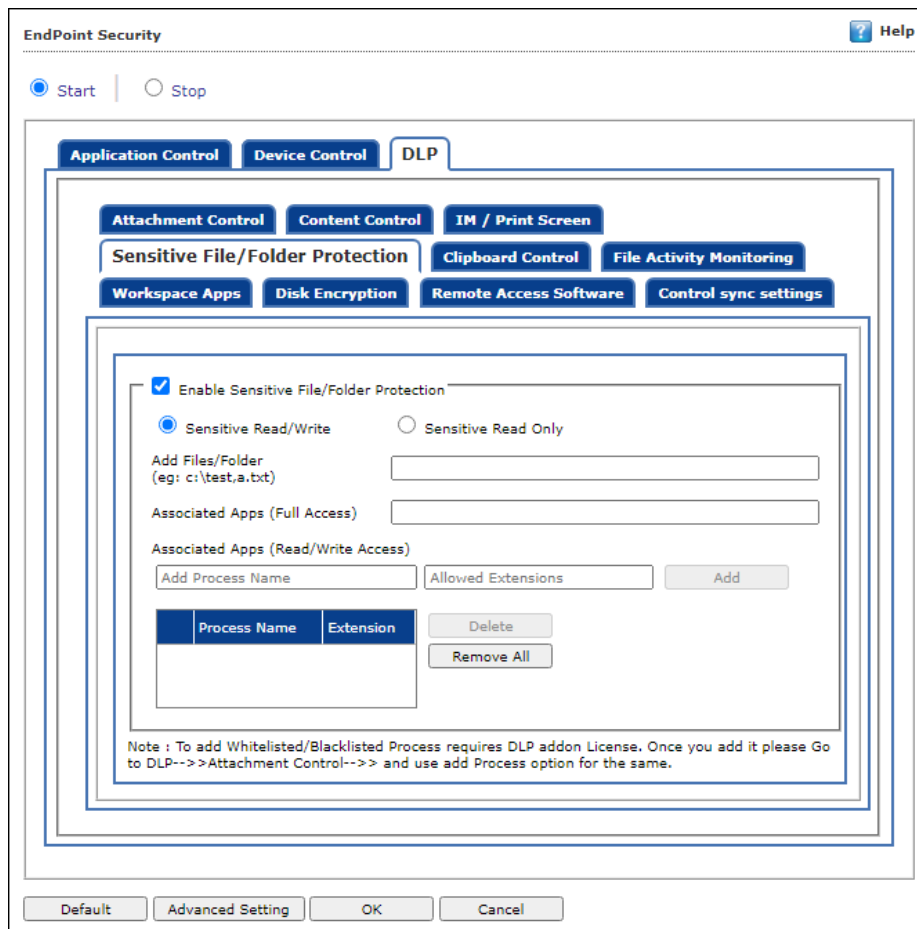
Select this option to enable/disable Print screen feature.

Snapshot Interval

This option allows you to define time interval in minutes on which the screenshots will be captured.

Sensitive File/Folder Protection

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



Enable Sensitive File/Folder Protection

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

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

Add Folder or Add Files

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

Associated Apps (Full Access)

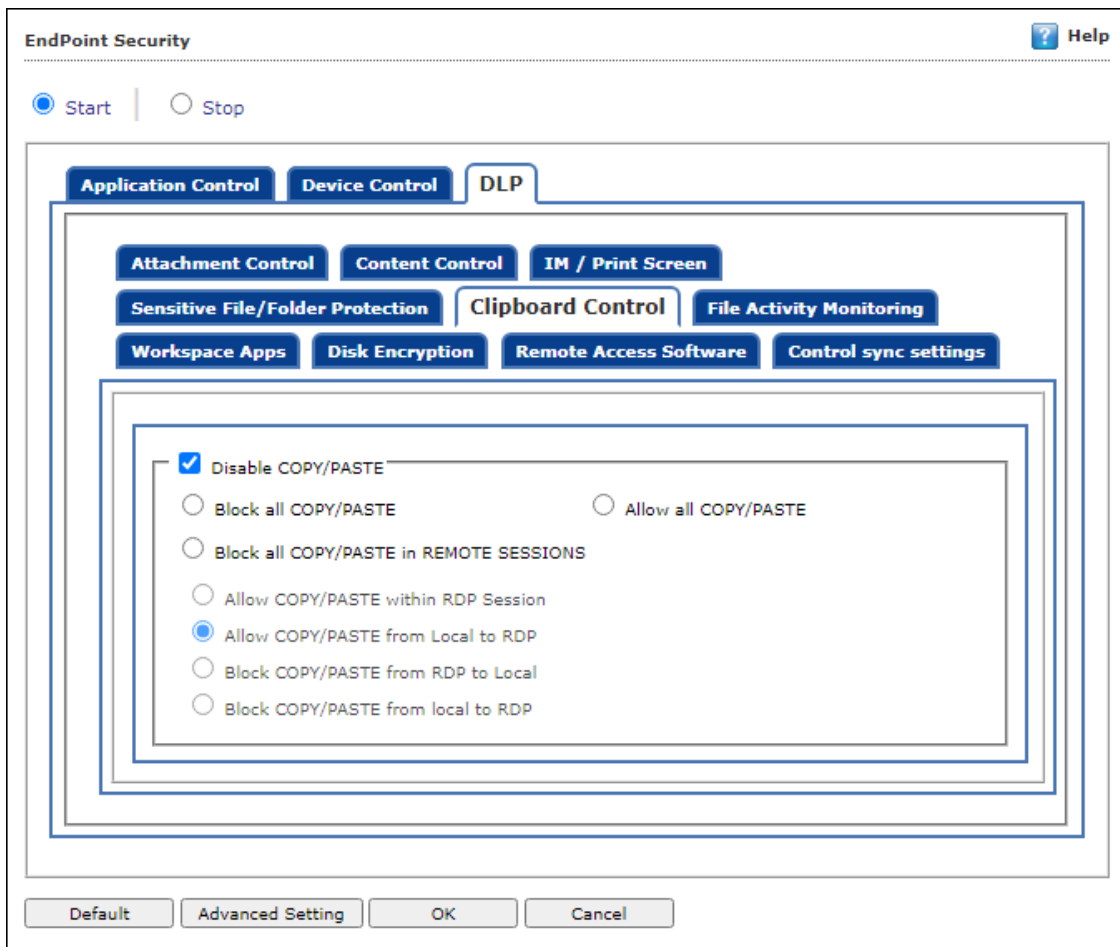
Enter the associated application name that has full access on sensitive files/folders.

Associated Apps (Read/Write Access)

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

Clipboard Control

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



Disable COPY/PASTE

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

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

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

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

Allow COPY/PASTE within RDP Session: Select this option to allow copy/paste within the RDP session.

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

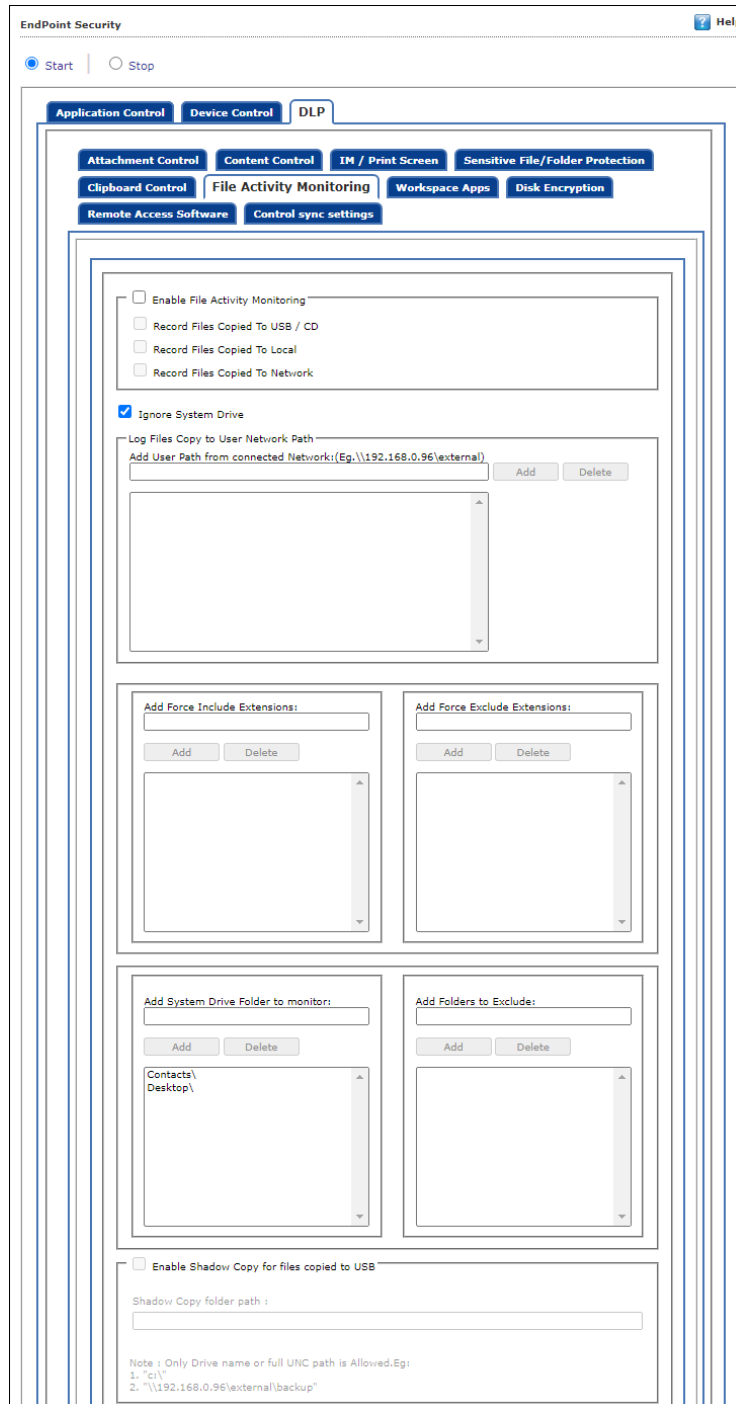
Allow COPY/PASTE for RDP to Local: Select this option to allow all copy/paste actions for RDP to local.

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

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

File Activity Monitoring

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



Enable File Activity Monitoring

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

Record Files copied To USB/CD

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

Record Files Copied To Local

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

Record Files Copied To Network

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

Ignore System Drive [Default]

Select this checkbox 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.

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

Enter the user path from connected network to monitor. You can add or delete user path from connected network from the list of by clicking **Add/Delete**.

Add Force Include Extensions

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

Add Force Exclude Extensions

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

Add System Drive Folder to monitor

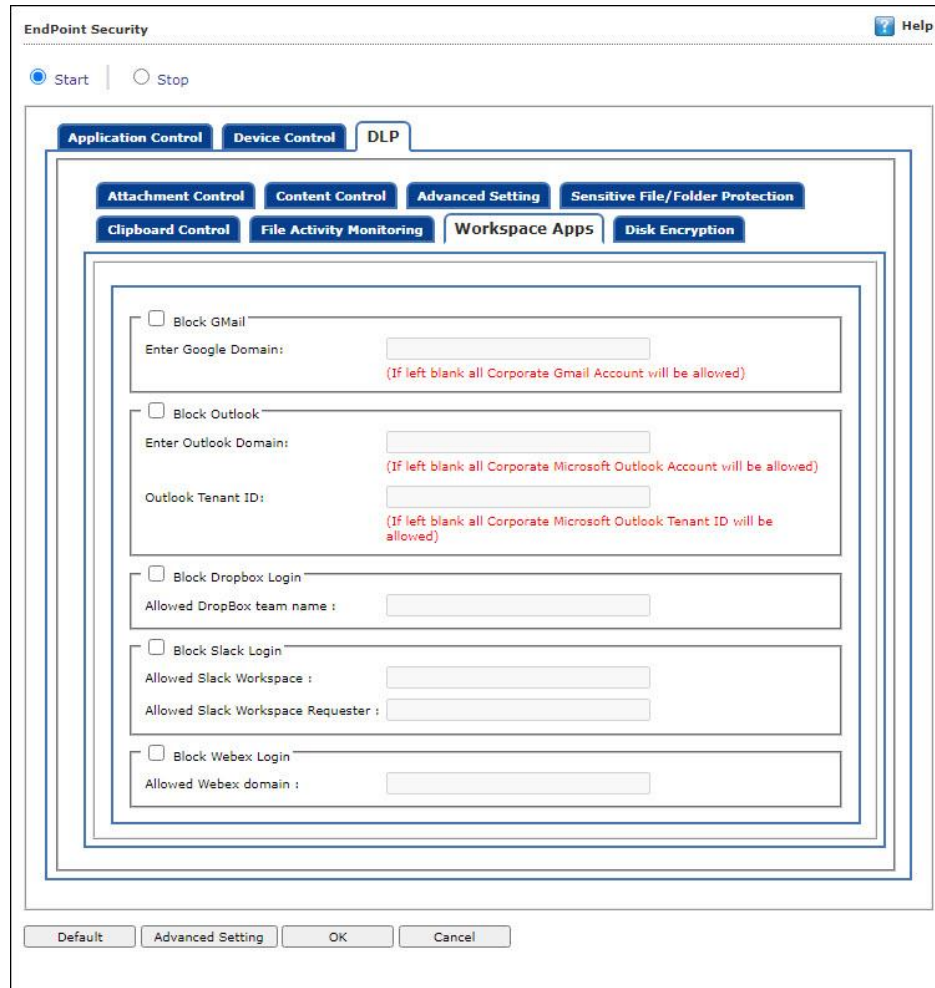
Select this option if you want eScan to monitor all the system drives installed on the computer. You can add or delete system drive folder from the list of by clicking **Add/Delete**.

Add Folder to Exclude

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

Workspace Apps

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



Block Gmail

Select this checkbox to block the personal Gmail account.

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

Block Outlook

Select this checkbox to block the personal Microsoft Outlook account.

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

Block Dropbox Login

Select this checkbox to block the Dropbox login.

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

Block Slack Login

Select this checkbox to block the Slack login.

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

Block Webex Login

Select this checkbox to block the Webex login.

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

Block Zoom Login

Select this checkbox to block the zoom login.

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

Block WeTransfer Login

Select this checkbox to block the WeTransfer Login.

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

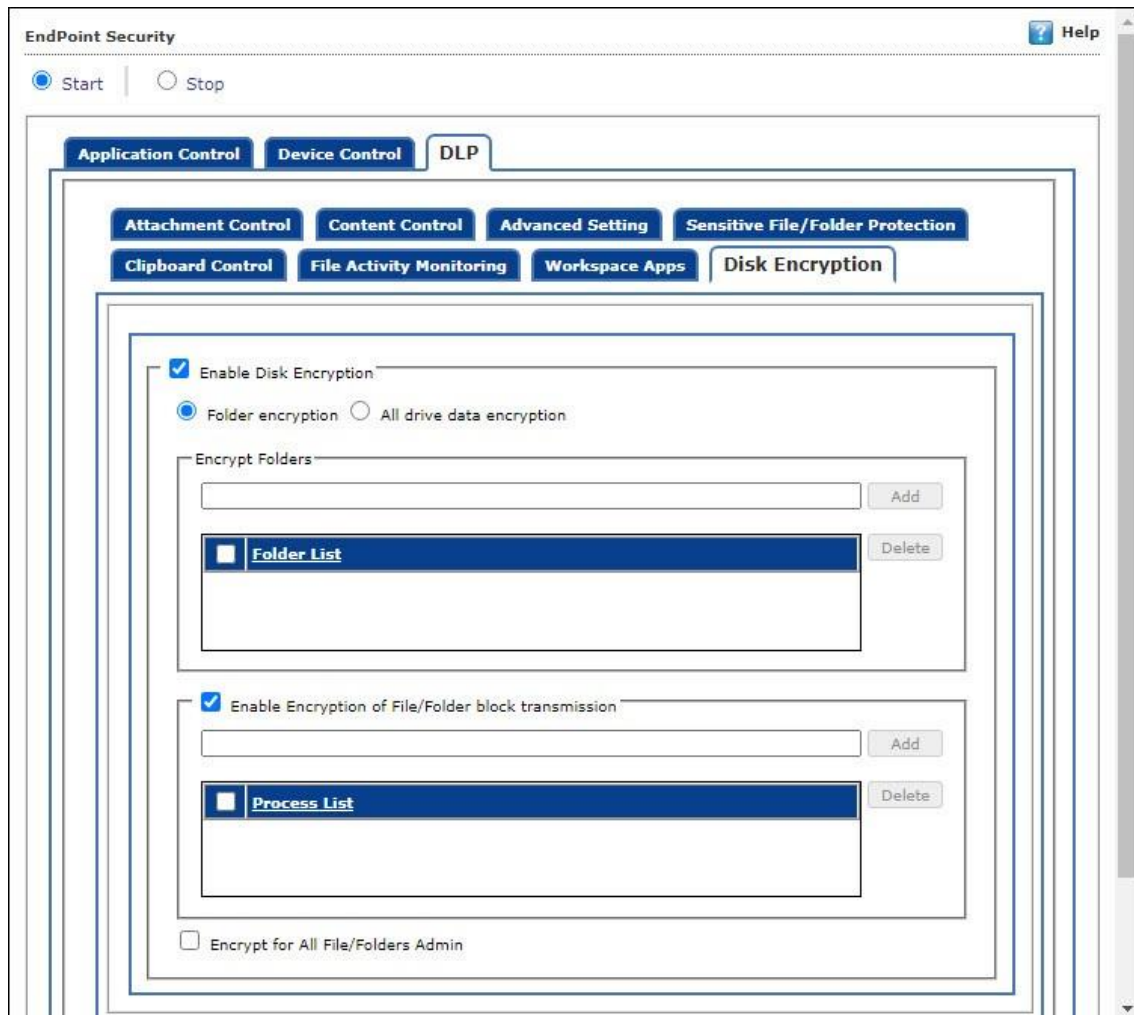
Block AutoDesk

Select this checkbox to block AutoDesk login.

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

Disk Encryption

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



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

Folder encryption

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

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

1. In the Disk Encryption window, select the checkbox **Enable Disk Encryption**.
2. Select the option **Folder encryption**.
3. Enter the folder path in the provided field in **Encrypt Folders** section.
4. Click on **Add**.

The folder will be added in the list below and will get encrypted.

All drive data encryption

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

Enable Encryption of File/Folder block transmission

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

Follow the steps mentioned below to whitelist the processes:

1. In the Disk Encryption window, select the checkbox **Enable Encryption of File/Folder block transmission**.
2. Enter the application name with extension in the provided field.
3. Click **Add**.

The process will be whitelisted for transmitting the encrypted data.

Encrypt for All File/Folders Admin

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



NOTE

- This option will encrypt only folders if **Folder encryption** option is selected.
- If the **All drive data encryption** is selected, it will encrypt folders as well as files.

Advanced Settings

Clicking **Advanced** displays Advanced Settings.

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

Ok

Allow Composite USB Device (1 = Enable/0 = Disable)

Select this option to allow/block use of composite USB devices.

Allow USB Modem (1 = Enable/0 = Disable)

Select this option to allow/block use of USB modem.

Enable Predefined USB Exclusion for Data Outflow (1 = Enable/0 = Disable)

Select this option to enable/disable use of predefined USB.

Enable CD/DVD Scanning (1 = Enable/0 = Disable)

Select this option enable/disable scanning of CD/DVD.

Enable USB Whitelisting option on prompt for eScan clients (1 = Enable/0 = Disable)

Select this option to enable/disable USB Whitelisting option on prompt for eScan clients.

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

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

Enable Domain Password for USB (1 = Enable/0 = Disable)

Select this option to enable/disable domain password for USB.

Show System Files Execution Events (1 = Enable/0 = Disable)

Select this option allow/block system files execution events.

Allow mounting of Imaging device (1 = Enable/0 = Disable)

Select this option to allow/block mounting of imaging devices.

Block File Transfer from IM (1 = Enable/0 = Disable)

Select this option to allow/block file transfer from Instant Messengers.

Allow Wi-Fi Network (1 = Enable/0 = Disable)

Select this option to allow/block use of Wi-Fi networks.

Whitelisted WIFI SSID (Comma Separated)

Select this option to whitelist WIFI SSID. Enter the WIFI SSID in comma separated format.

Allow Network Printer (1 = Enable/0 = Disable)

Select this option to allow/block use of network printers.

Whitelisted Network Printer list (Comma Separated)

Select this option to whitelist network printer list. Enter the name of printers in comma separated format.

Allow eToken Devices (1 = Enable/0 = Disable)

Select this option to allow/block use of eToken devices.

Include File Extension for File Activity Monitoring (e.g EXE)

Select this option to include File Extension for File Activity Monitoring.

Exclude File Extension for File Activity Monitoring (e.g EXE)

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

Auto Whitelist BitLocker encrypted USB Devices (1 = Enable/0 = Disable)

Select this option to allow/block auto whitelist BitLocker encrypted USB devices.

Ask Password for whitelisted Devices only (1 = Enable/0 = Disable)

Select this option to allow/block ask password for whitelisted devices.

Disable Print Screen (1 = Enable/0 = Disable)

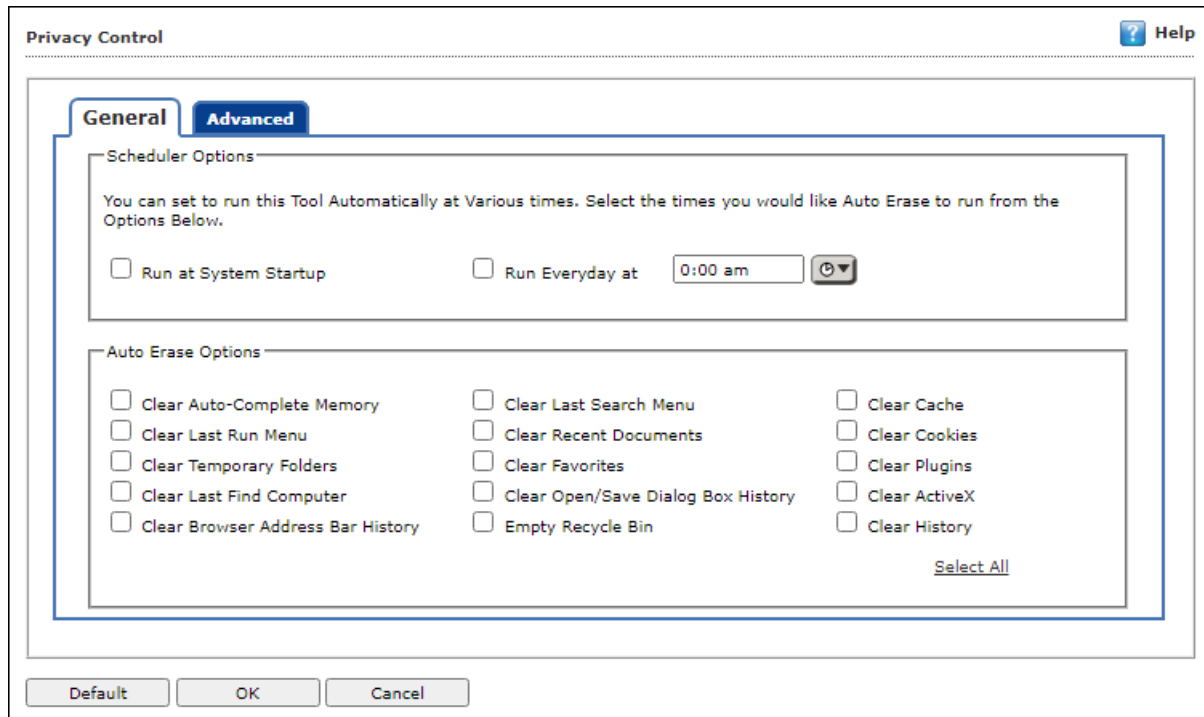
Select this option to enable/disable use of printer screen.


NOTE

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

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 the sites and web pages you have accessed while browsing. This page provides you with options for configuring the module.



It consists following tabs:

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

General tab

This tab lets you specify the unwanted files created by web browsers or other installed softwares 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 the browsing history from your computer. The following settings are available in the **Scheduler Options** section.

- **Run at System Startup:** It auto executes the Privacy Control module and performs the desired auto-erase functions when the computer starts up.
- **Run Everyday at:** It auto-executes the Privacy Control module at specified times and performs the desired auto erase functions. You can specify the time within the hours and minutes boxes.

Auto Erase Options

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

Clear Auto Complete Memory

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

Clear Last Run Menu

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

Clear Temporary Folders

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

Clear Last Find Computer

When you select this option, Privacy Control clears the name of the computer for which you searched last.

Clear Browser Address Bar History

When you select this checkbox, Privacy Control clears the websites from the browser's address bar history.

Clear Last Search Menu

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

Clear Recent Documents

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

Clear Favorites


When you select this checkbox, Privacy Control clears the names of the objects found in Favorites.

Clear Open/Save Dialog box History

When you select this checkbox, Privacy Control clears the links of all the opened and saved files.

Empty Recycle Bin

When you select this checkbox, Privacy Control clears the Recycle Bin.

 NOTE	Use this option with caution as it permanently clears the recycle bin.
--	--

Clear Cache

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

Clear Cookies

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

Clear Plugins

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

Clear ActiveX

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

Clear History

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

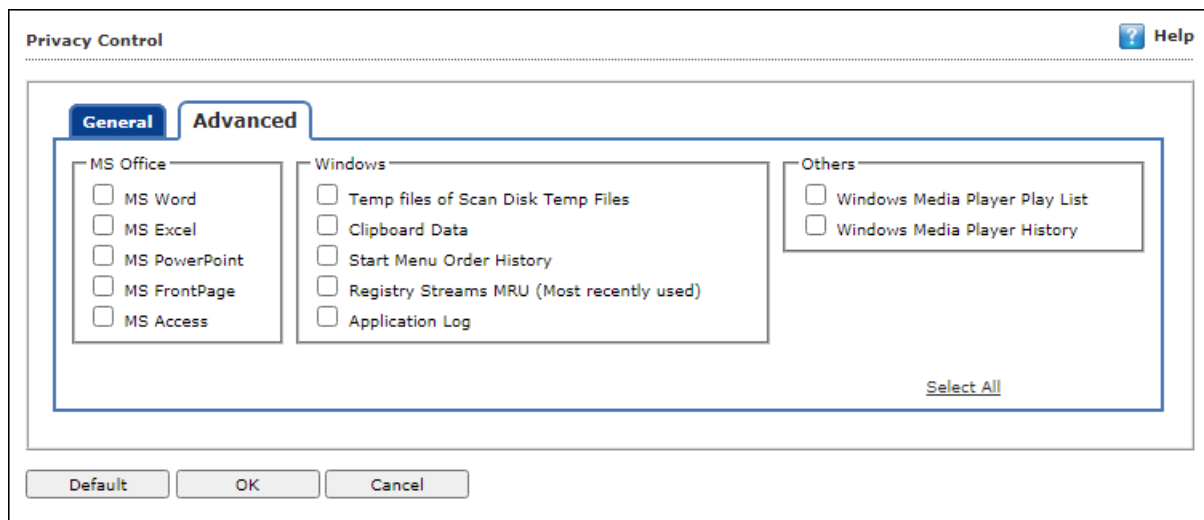
In addition to these options, the **Auto Erase Options** section has below option as well.

Select All/ Unselect All

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

Advanced 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.



MS Office

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

Windows

The respective unwanted files like temp files will be cleared.

Others

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

Select All/ Unselect All

Click this button to select/unselect all the options in Advanced tab.

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

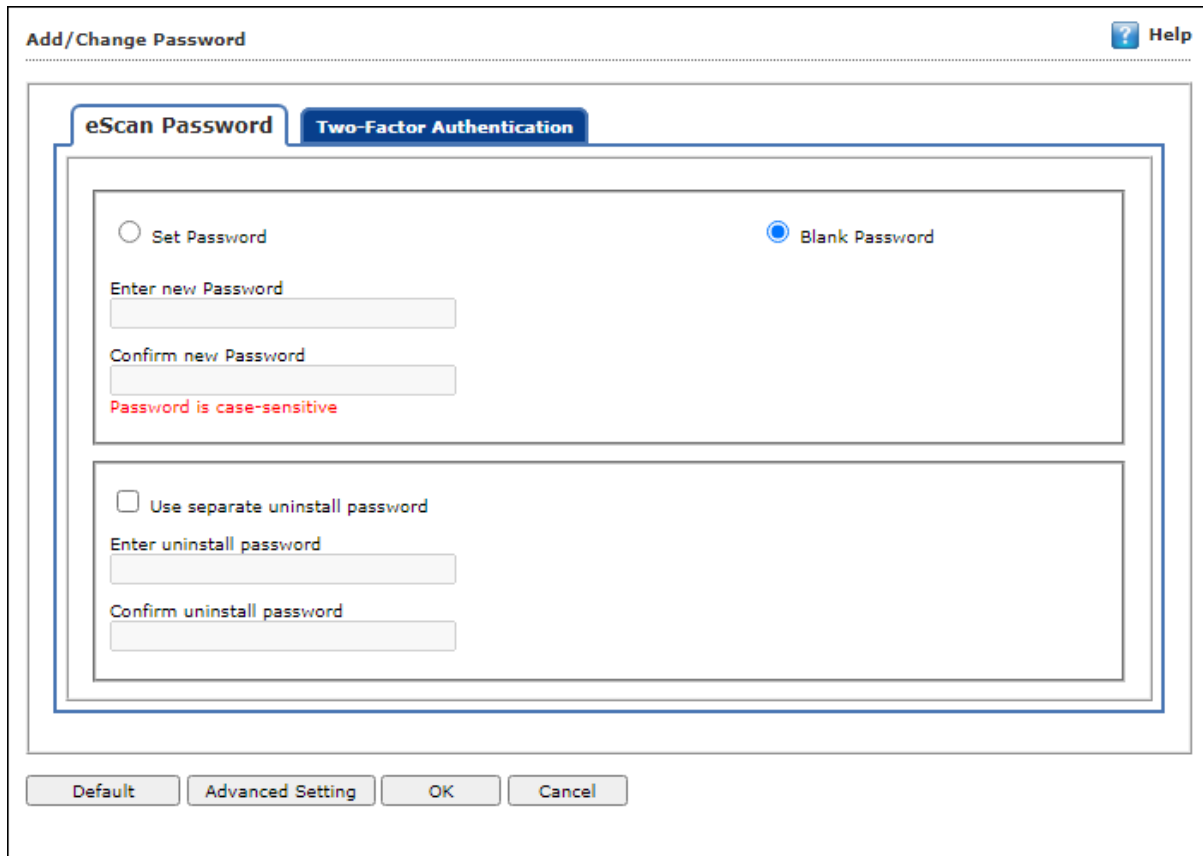
Policy Details also lets you do the following for Windows Operating System.

Administrator Password

Administrator Password policy in eScan Enterprise EDR - Cloud lets you create and change password for administrative login of eScan Protection Center and Two-Factor Authentication.

eScan Password

Select the option **Set Password** and define a password as per your choice. 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.



Below are the mandatory criteria for strong password creation:

Password length: The password length should be of minimum 8 characters.

Lowercase: The password must contain at least 1 letter in Lowercase (a-z).

Uppercase: The password must contain at least 1 letter in Uppercase (A-Z).

Numeric: The password must contain at least 1 digit (0-9).

Special character: The password must contain at least 1 special character (\$ @ ! % * # ? _ &).

Password match: Both the entered passwords should be matching.

Additionally, there is an option to set an uninstall password. An uninstall password prevents unauthorized uninstallation of eScan client from the endpoint. Upon selecting Uninstall option, eScan asks for uninstall password before proceeding further. 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 less secure as it may put your organization's data at high risk of compromise. The Two-Factor Authentication, commonly known as 2FA, adds an extra layer of protection to your basic system logon. The 2FA feature requires personnel to enter an additional passcode after entering the system login password. So, even if an unauthorized person knows your system credentials, the 2FA feature secures a system against unauthorized access.

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

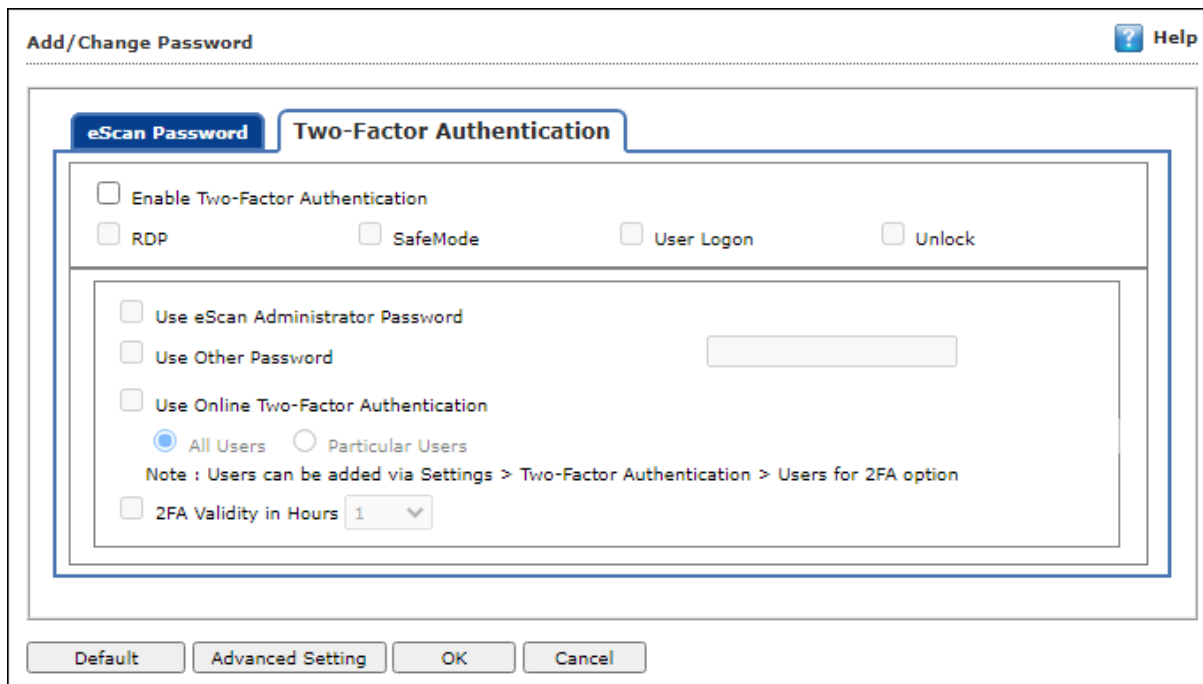


To enable the Two-Factor Authentication feature, follow the steps given below:

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

 NOTE	You can enable 2FA for existing policy templates by selecting a template > Properties . And then continue with the steps below:
--	--

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



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

Login Scenarios

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

RDP

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

Safe Mode

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

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

This option can be enabled for all users or for particular user according to the requirement.

To learn more about adding user and enabling the 2FA, [click here](#).



NOTE

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

To use this feature, follow the steps given below:

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

Advanced Setting

Clicking **Advanced Setting** displays Advance setting.

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

Ok

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 the eScan protection without entering password.

Download Signature Updates from Internet and policy from Primary Server (1= Enable/0 Disable)

Selecting this option lets you download Signature Updates from Internet and policy from Primary Server.

Change ICON to eScan (1= Enable/0=Disable)

Selecting this option will allow you to change the icon of the eScan.

Stop Patch Notification (1= Enable/ 0 = Disable)

This option allows you to enable/disable the patch notification option.

Set IPONLY (1=Enable/0=Disable)

Select enable/disable to set the IP ONLY option.

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

This option allows you to enable/ disable the HTTPS Download option.

Show Protection Center in Read Only Mode (Applicable only on icon Click)

Select enable/ disable to show Protection Center in Read Only Mode option.

Enable Policy REAPP (1=Enable/0=Disable)

Select this option to enable Policy REAPP option.

Disable Policy REAPP REG Only (1=Enable/0=Disable)

Select this option to disable the Policy REAPP REG only option.

Enable Win Patch download (1=Enable/0=Disable)

Select this option to enable Win Patch Download option.

Enable ALL Win Patch Download (1=Enable/0=Disable)

Select this option to enable ALL Win Patch Download option.

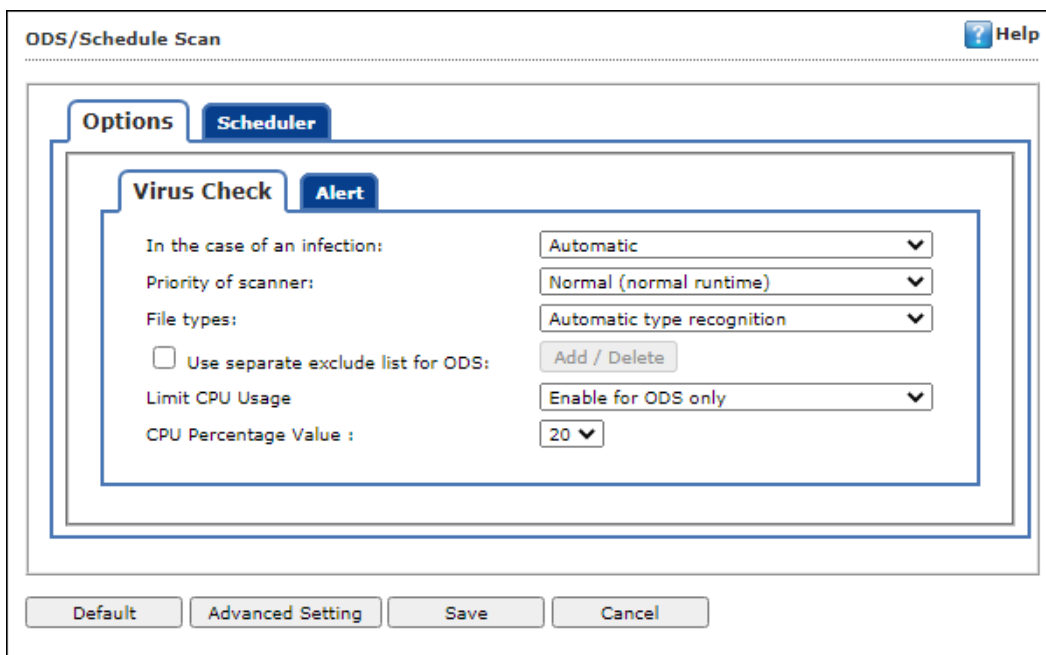
ODS/Schedule Scan

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**



The screenshot shows the 'ODS/Schedule Scan' configuration window. The 'Options' tab is selected, and the 'Virus Check' sub-tab is active. The settings are as follows:

Setting	Value
In the case of an infection:	Automatic
Priority of scanner:	Normal (normal runtime)
File types:	Automatic type recognition
Use separate exclude list for ODS:	<input type="checkbox"/> Add / Delete
Limit CPU Usage	Enable for ODS only
CPU Percentage Value :	20

Buttons at the bottom: Default, Advanced Setting, Save, Cancel.

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

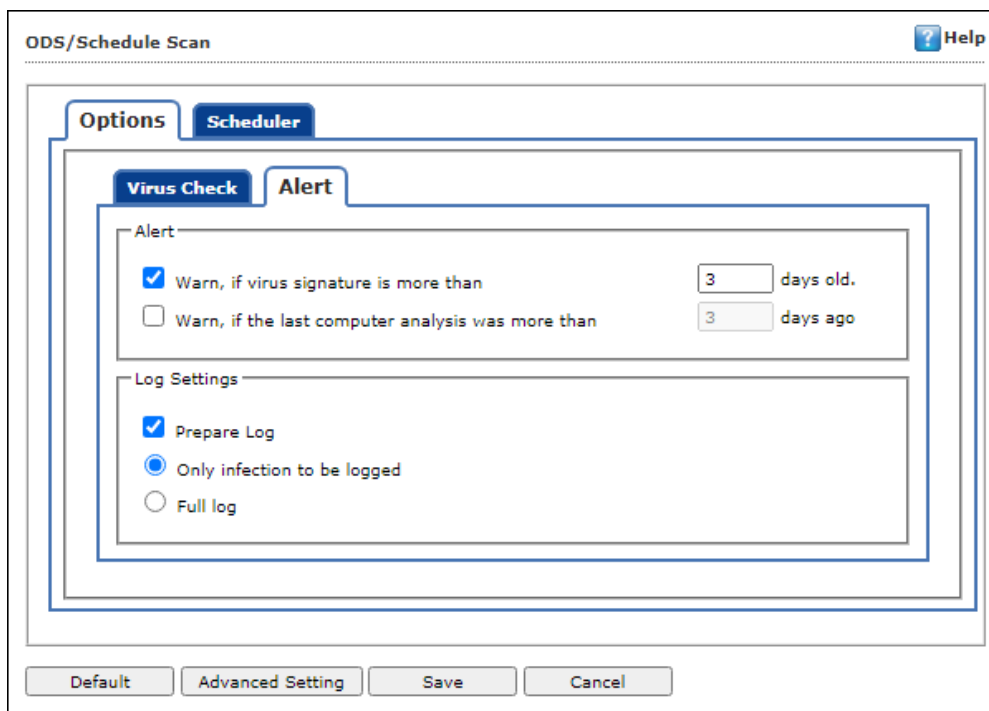
It lets you configure the settings for checking viruses.

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 Automatic [Default]. If the option Automatic is selected, eScan will quarantine the infected file. In this case, if the action Delete object is selected in File Anti-Virus module, the object will be deleted.
 - **Priority of scanner:** Select an appropriate option from the drop-down list. For example,
 - High (short runtime)
 - Normal (normal runtime) [Default]
 - 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.
 - **Limit CPU Usage:** Select an appropriate option from the drop-down list
 - **CPU Percentage Value:** Select an appropriate percentage value from the drop-down list
2. Click **Save**.

Alerts tab

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




The screenshot shows the 'Alert' tab within the 'Virus Check' section of the 'Scheduler' options. The 'Alert' section has two checkboxes: 'Warn, if virus signature is more than 3 days old.' (checked) and 'Warn, if the last computer analysis was more than 3 days ago' (unchecked). The 'Log Settings' section has three radio buttons: 'Prepare Log' (checked), 'Only infection to be logged' (selected), and 'Full log' (unchecked). At the bottom, there are buttons for 'Default', 'Advanced Setting', 'Save', and 'Cancel'.

To set alerts,

1. Under **Alert** section, Select the [Default] **Warn, if virus signature is more than** x day's old checkbox, and then enter the number of days in the x day's old field, if you want to receive

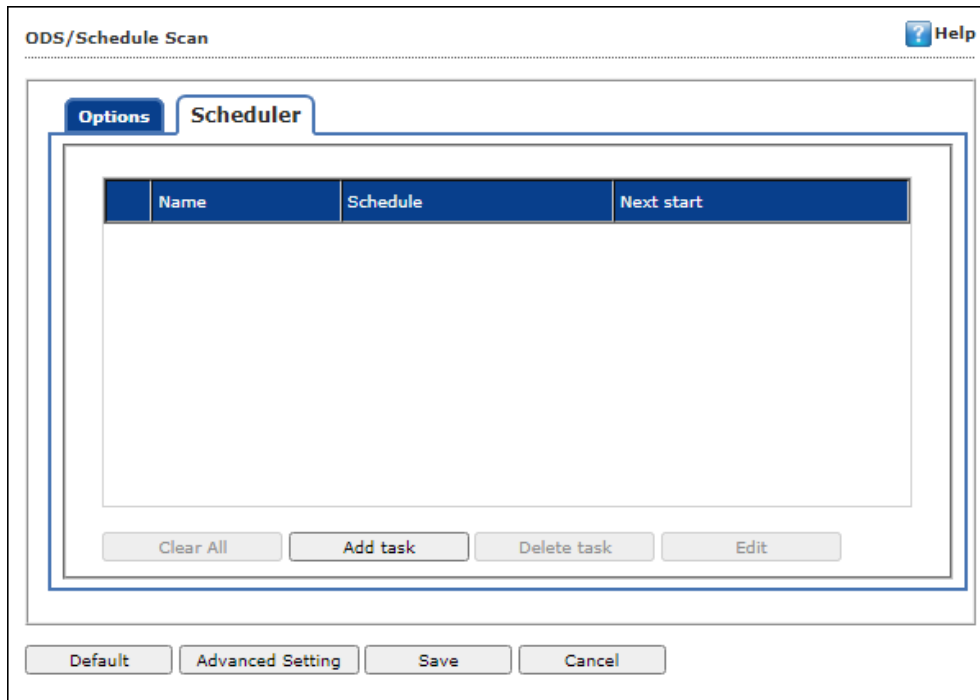
alerts when virus signature exceeds the specified days. By default, value 3 appears in the field.

2. Select the **Warn, if the last computer analysis was more than** x days ago checkbox, 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 appear in the field.
3. Under **Log Settings** section, select the [Default] **Prepare Log** checkbox, 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

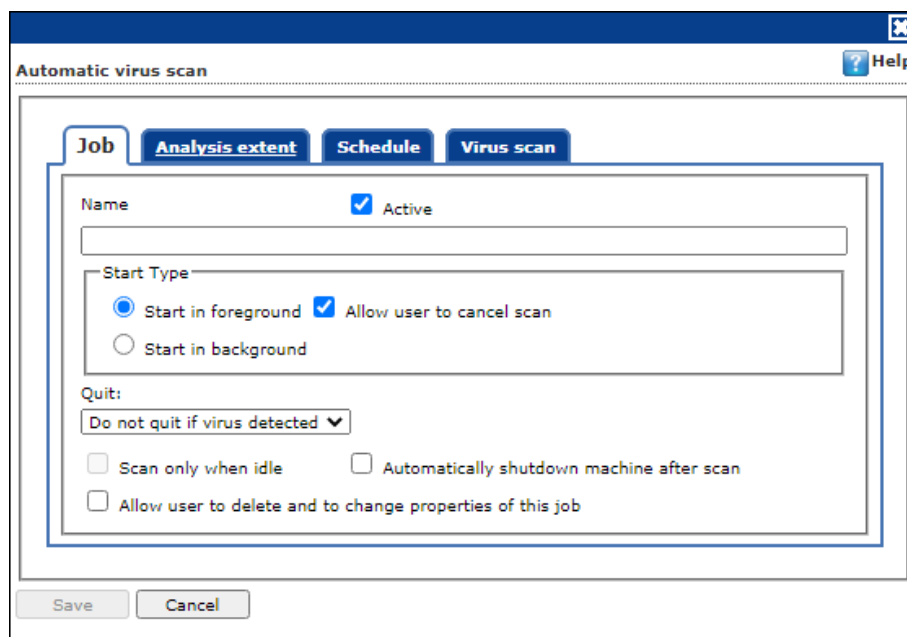
Scheduler tab lets you create/delete various tasks in the scheduler for automatic virus scanning.



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 window lets you do following activities:

- a) Creating job

- b) Setting analysis extent
- c) Scheduling virus execution
- d) Scheduling virus scan

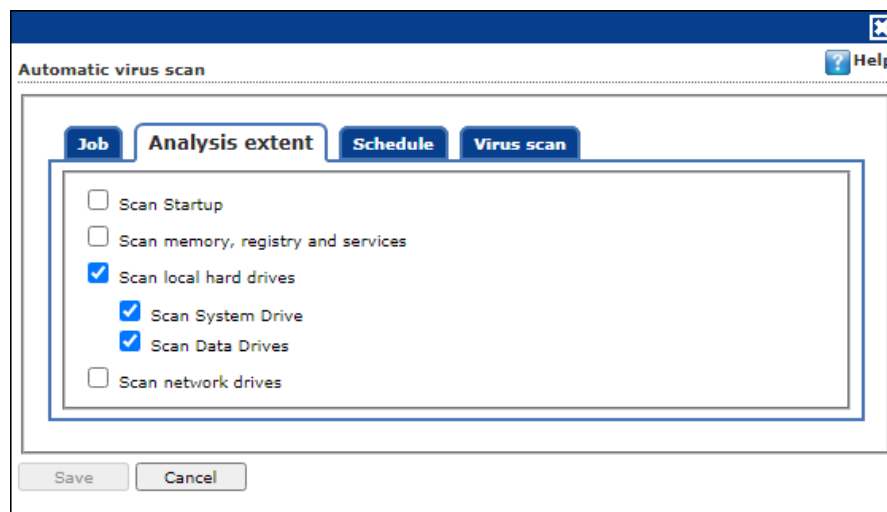
a) Job

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 checkbox, 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

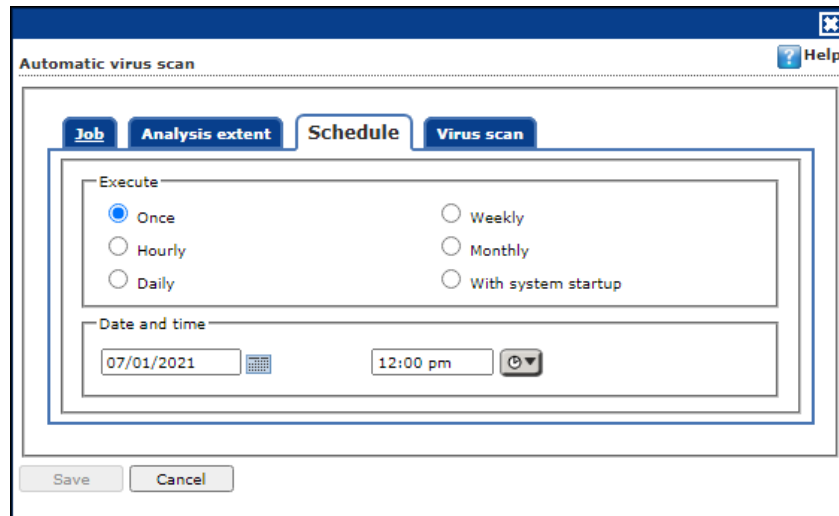
It lets you configure analysis extent settings for virus scanning.




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.



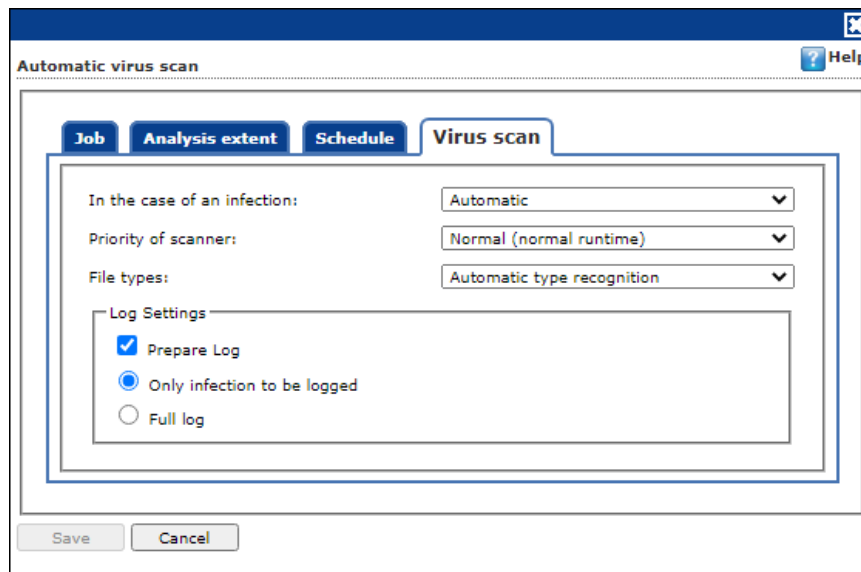
1. Click **Schedule** tab.
2. Under Execute section, select an appropriate option. For example, [Default] Once, weekly, hourly, and so on.
3. Under Date and time section, click the **calendar** icon. The calendar appears.
4. Select an appropriate date from the calendar.

 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.



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 checkbox, 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.

Advanced Settings

Autorun System Scanning if System not scanned for days defined

This option let you define days for autorun system scanning if system is not scanned.

Ignore Battery Status

Select this option to Ignore Battery Status.

Scan USB when All Drive option selected

Select this option to scan USB when all drive options are selected.

Remove LNK

This option lets you Enable/Disable Removal of LNK.

Start Background Scan in System Mode

Select this option to start background scan in system mode.

Enable Scan Caching

This option lets you Enable/Disable scanning of cache.

Check for Corrupted Files

Select this option to check for corrupted files.

Scan in low Priority Mode

It lets you Enable/Disable the scan in low priority mode on the computer.

Enable Unhiding of USB Files & Folder

This option let you enable/disable unhiding USB files & folders.

Enable Missed schedule scan JOB's to run

This option let you enable/disable missed schedule scan JOB's to run.

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.

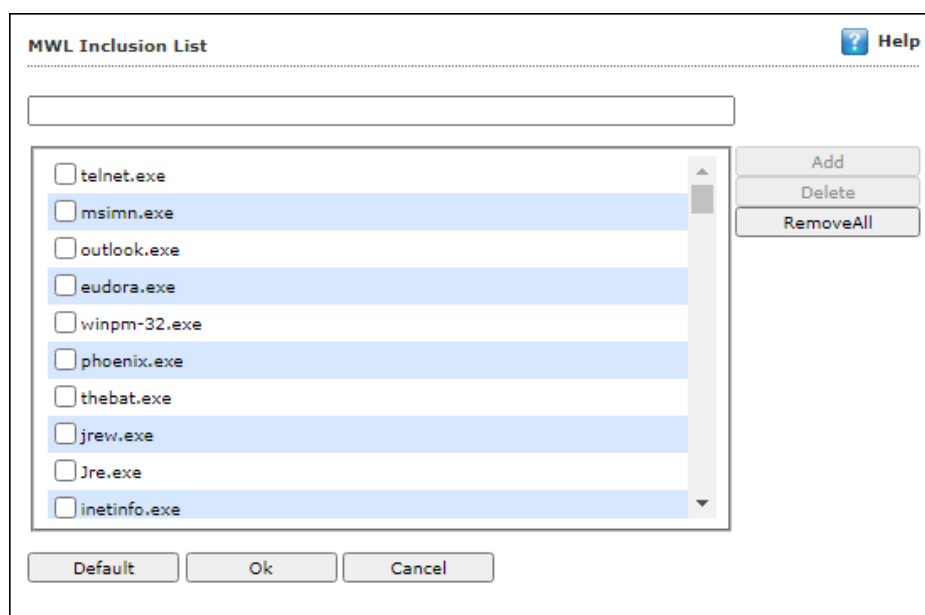
MWL Inclusion List

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



Add files to Inclusion List

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

1. Enter the executable file name and then click **Add**.
The executable file will be added to the Inclusion List.
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, follow the steps given below:

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

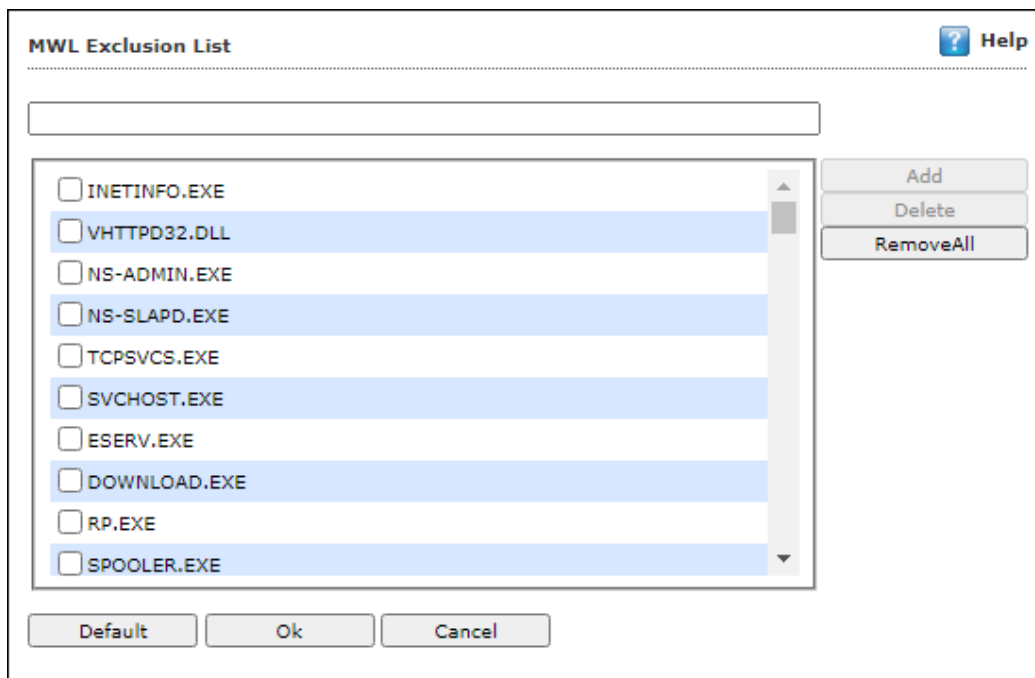
MWL Exclusion List

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



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:

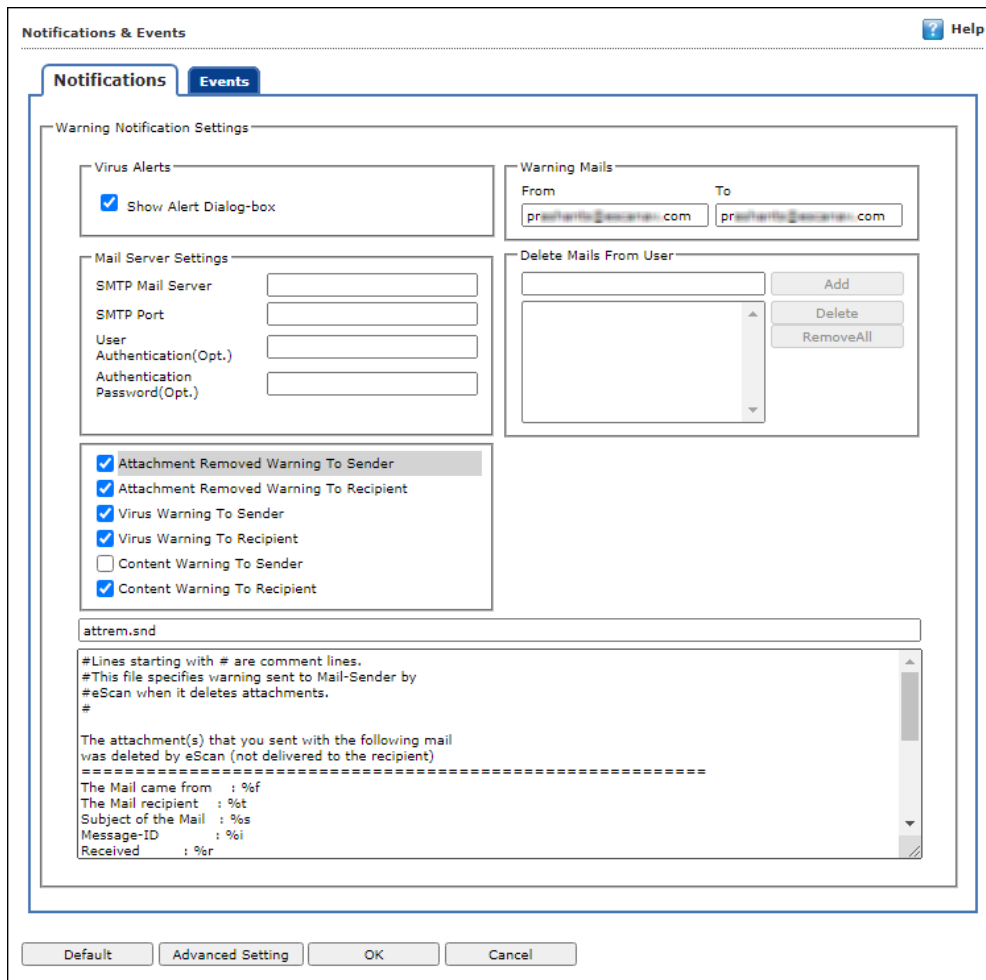
1. Select the appropriate file checkbox, and then click **Delete**.
A confirmation prompt appears.
2. Click **OK**.
The executable file gets deleted from the Exclusion List.

Removing all files from Exclusion List

To remove all executable files from the Exclusion List:

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

Notifications and Events



Notifications

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

Virus Alerts [Default]

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

Warning Mails

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

Attachment Removed Warning to Sender [Default]

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

Attachment Removed Warning to Recipient [Default]

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

Virus Warning to Sender [Default]

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

Virus Warning to Recipient [Default]

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

Content Warning to Sender

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

Content Warning to Recipient [Default]

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

Delete Mails from User

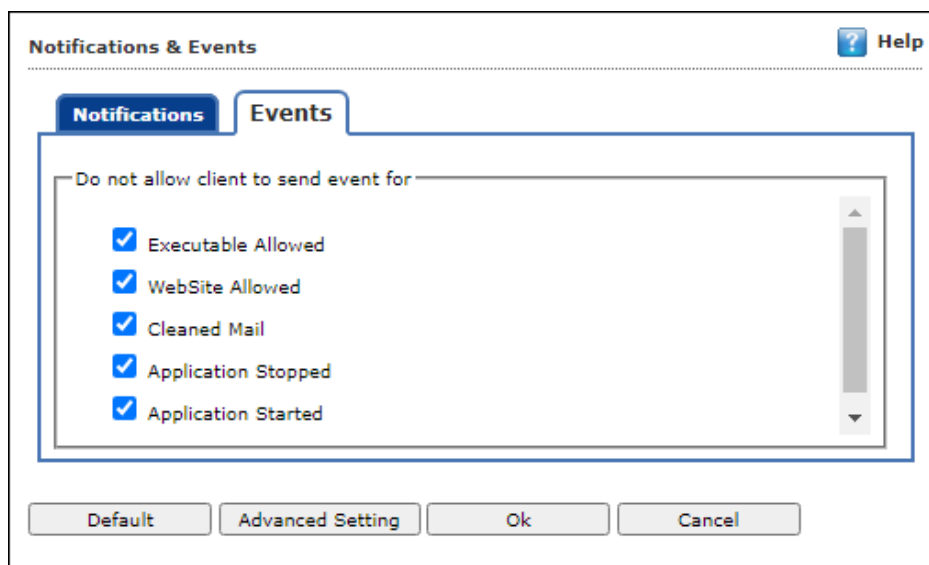
You can configure eScan to automatically delete emails that have been sent by specific users. For this, you need to add the email addresses of such users to the **Delete Mails From User** field. The **Add**, **Delete**, and **Remove All** buttons appear as dimmed. After you enter text in the **Delete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

Events

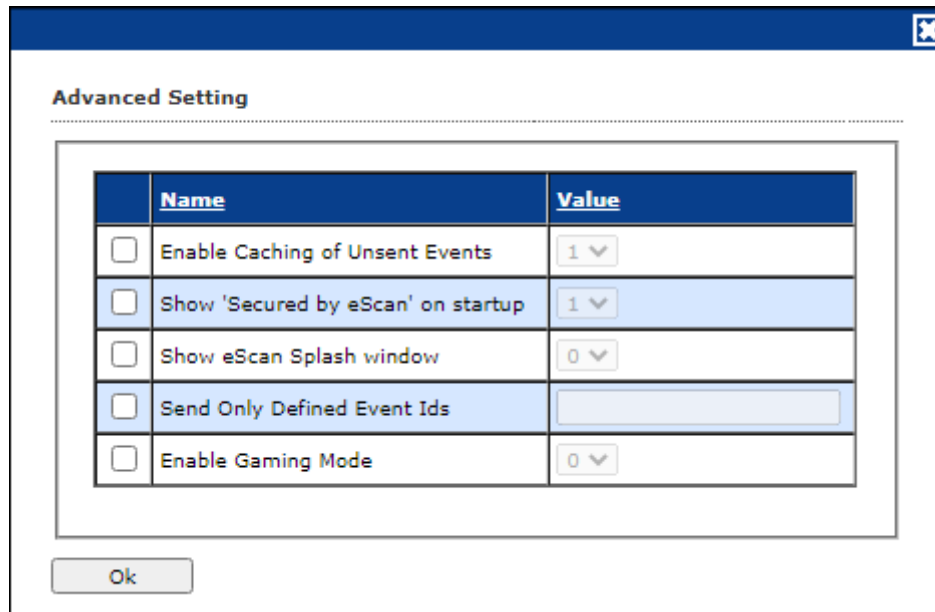
Events tab lets you define the settings to allow/restrict clients from sending alert for following events:

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

By default, all events are selected.



Advanced Settings



	Name	Value
<input type="checkbox"/>	Enable Caching of Unsent Events	1
<input type="checkbox"/>	Show 'Secured by eScan' on startup	1
<input type="checkbox"/>	Show eScan Splash window	0
<input type="checkbox"/>	Send Only Defined Event Ids	
<input type="checkbox"/>	Enable Gaming Mode	0

Ok

Enable Caching of Unseen Events (1 = Enable/0= Disable)

It lets you Enable/Disable automatic caching of unseen events.

Show 'Secured by eScan' on startup (1 = Enable/0= Disable)

It lets you Enable/Disable the display of 'Secured by eScan' at the startup of the computers.

Show eScan Splash window (1 = Enable/0= Disable)

It lets you Enable/Disable display of eScan Splash Window.

Send Only Defined Event Ids

It lets you send only the defined events such as File Antivirus IDs, Mail Antivirus IDs, and more.

Enable Gaming Mode (1 = Enable/0 = Disable)

It lets you Enable/Disable the gaming mode on the computer.

Schedule Update

The Schedule Update lets you schedule eScan database updates.

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.

Advanced Settings

Set bandwidth limit for download (in kb/sec)

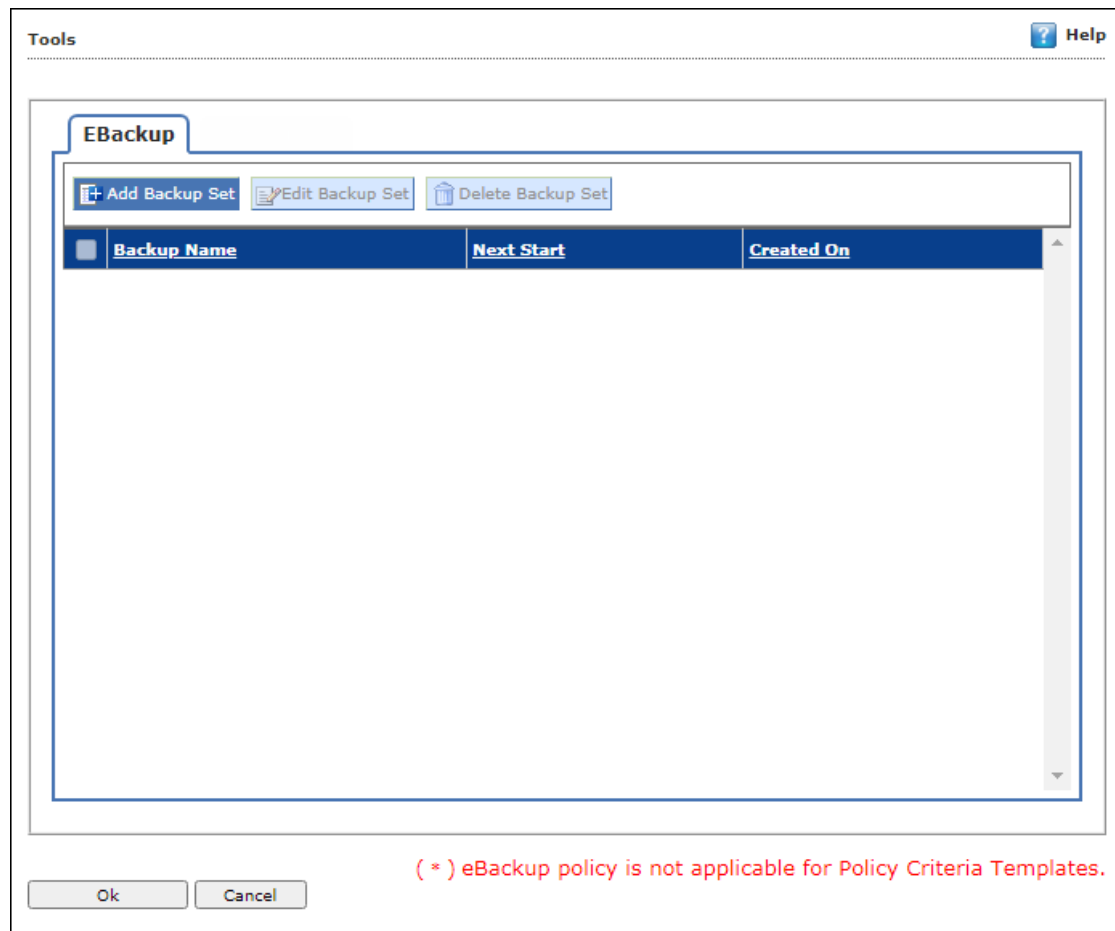
It lets you define bandwidth limit for download on managed computers, if you have limited internet connection or other network issues.

Retry schedule download (Default retry interval is 15 minutes)

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

Tools

The Tools lets you configure eBackup setting.



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.

The eBackup option has following tabs to configure:

Job

Using this tab you can schedule the eBackup task.

The screenshot shows the 'Add Backup Set' dialog box with the 'Job' tab selected. The dialog has three tabs: 'Job', 'Backup Source and Exclusion', and 'Backup location'. The 'Job' tab contains the following fields and options:

- Active
- Name:
- Scheduler:
 - Execute:
 - Once
 - Hourly
 - Daily
 - Weekly
 - Monthly
 - With system startup
- Date and time:
 - Day:
 - Date:
 - Time:
- Set Restore Password
-
- Note*: Password can be set only while adding new job.

At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Active

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

Scheduler

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

Date and time

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

Set Restore Password

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

Backup Source and Exclusion

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

Backup Source

This option allows you to add the folder path(s) on which the backup has to be performed. Apart from that you can select the document types to be backed up from these particular folders.

Folder Settings

- **Add File Type for Backup:** Select the type of files for backup. By default, Office Documents option is selected.
- **File/Folder Exclusion:** In this section, you can exclude a specific folder or a file format from getting backed up. You can add, delete, and remove the files for the same.


Backup Location

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

The screenshot shows the 'Add Backup Set' dialog box with the 'Backup location' tab selected. Underneath, the 'Local/Network' sub-tab is active. A checkbox labeled 'Store backup on Local/Network drive' is checked. Below this, there is a section for 'Local Drive Settings' containing three input fields: 'Destination Path for Backed up Files.', 'UserName', and 'Password'. A note below these fields states: 'Note : Only Drive name or full UNC path is Allowed. Eg: 1. "c:\", 2. "\\192.168.0.96\external\backup"'. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

Local/Network

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

 NOTE	<p>Network storage of backup set will be available in the trial period. To continue the use of this feature user need to avail the license for the same.</p> <p>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.</p>
--	--

Google Drive

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

The screenshot shows the 'Add Backup Set' dialog box with the 'Backup location' tab selected. Underneath, the 'Google Drive' sub-tab is active. A checkbox labeled 'Store backup on Google Drive.' is present. Below it is a section titled 'Google drive settings' containing three dropdown menus: 'Select gmail account', 'Refresh token', and 'Remove gmail account'. There are also buttons for 'Check Storage', 'Login', 'Mark for deletion', and 'Unmark'. A red note at the bottom states: 'Note: To store backup on the Google Drive, select the appropriate Google account. If you have a Google account, click "Login". Additionally, the "Login" button also lets you create an account if you want to use account other than your existing accounts.'

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

DropBox

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

The screenshot shows the 'Add Backup Set' dialog box with the 'Backup location' tab selected. Underneath, the 'DropBox' sub-tab is active. A checkbox labeled 'Store backup on DropBox.' is present. Below it, the 'DropBox settings' section contains a dropdown for 'Select DropBox account', a text field for 'Refresh token', and 'Check Storage' and 'Login' buttons. There is also a dropdown for 'Remove dropbox account' with 'Mark for deletion' and 'Unmark' buttons. A note at the bottom states: '*Note: the selected email will be permantly deleted only after saving the policy.' A red note below that says: 'Notes: To store backup on the DropBox, select the appropriate DropBox account. If you have a DropBox account, click "Login". Additionally, the "Login" button also lets you create an account if you want to use account other than your existing accounts.'



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

OneDrive

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

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

Add Backup Set

To create a Backup Set:

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

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

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

The Backup Set will be created.

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

Edit Backup Set

To edit a Backup Set:

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.

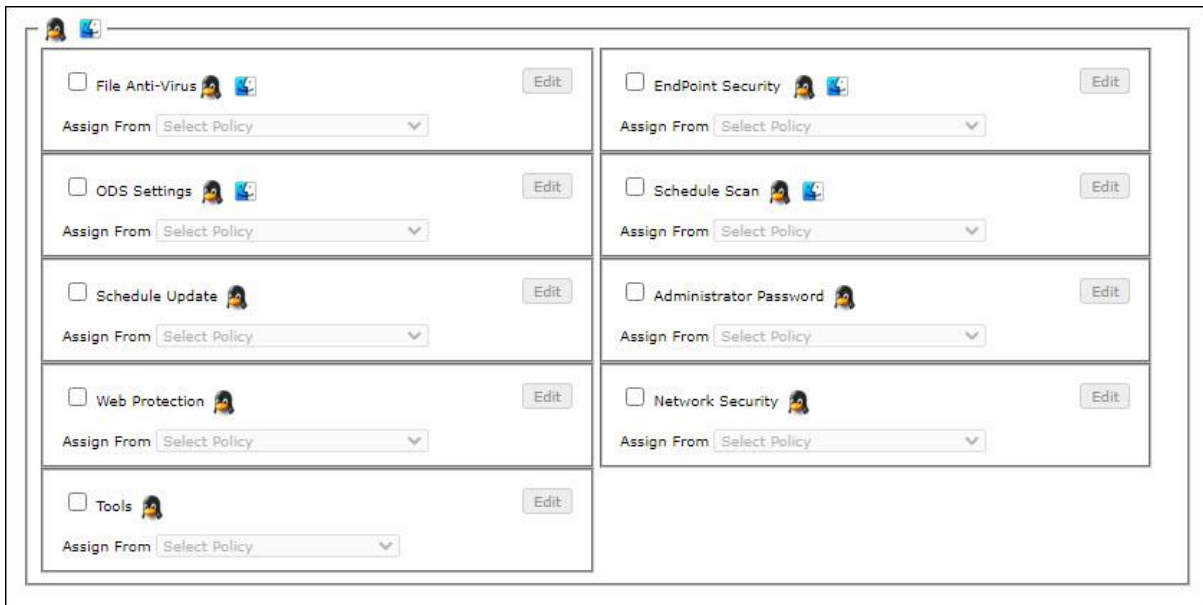
Delete Backup Set


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.



 **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
Help

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

Scan Settings

Archives

Mails

Packed

Cross file system

Follow symbolic links

Display attention messages
 Number of days log should be kept:

Exclude by mask

Add

Delete

RemoveAll

Exclude Files / Folders

Add

Delete

RemoveAll

Add Directory for realtime scan

Add

/home Delete

/tmp RemoveAll

Default
OK
Cancel

Actions in case of infection [Drop-down]

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

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

Scan Settings

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 checkbox 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 checkbox if you want eScan real-time protection to scan archived files.
- **Packed** - It indicates the compressed executable. Select this checkbox 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.


Application Control

The Application Control tab allows to block the execution of application or package.

Endpoint Security Help

Start | Stop

Application Control | Device Control | File Integrity Monitor

Enable Application Control 

Enter Application/Package to Block

List of Blocked Applications/Packages

Application/Package Name

Add
Delete
Remove All

Default OK Cancel

Enable Application Control

Select the checkbox to enable the application control feature.

Enter Application/Package to block

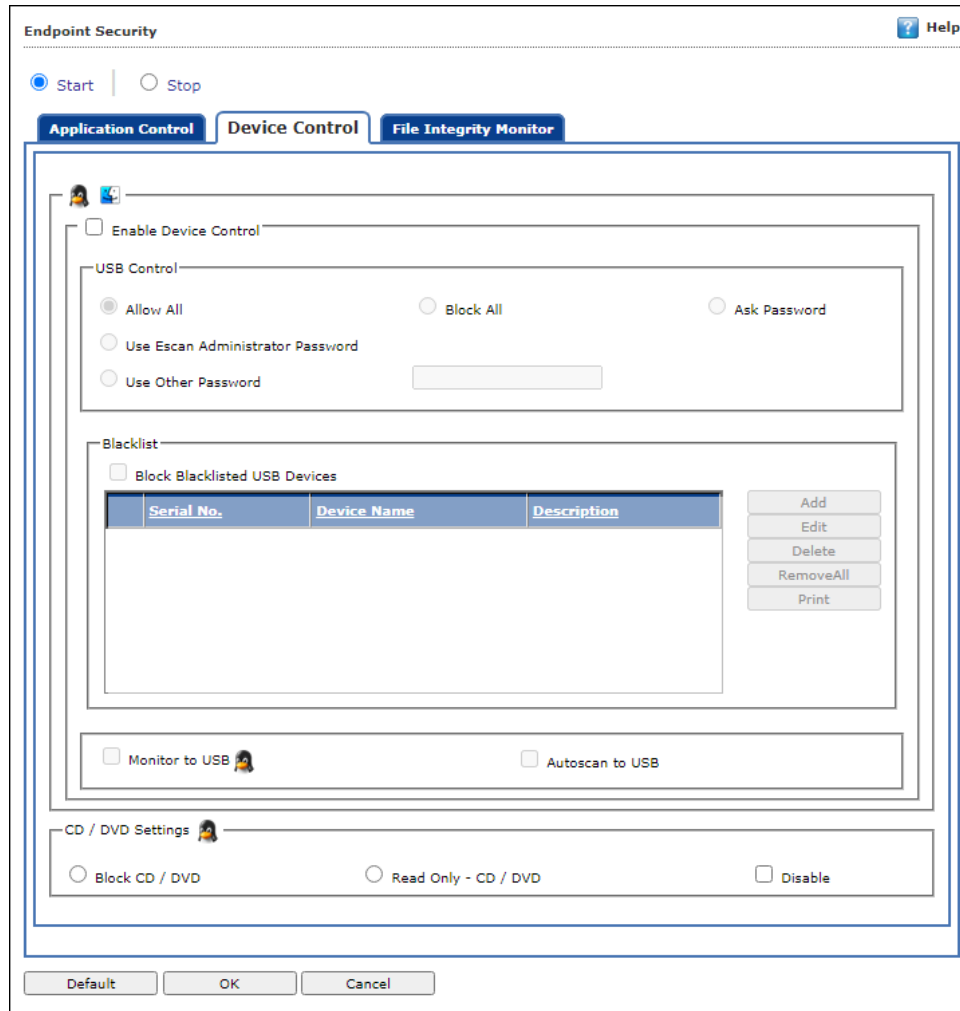
Enter the application or package name to add them in the list of application/packages blocked.

To delete the application/package, select the specific app/package and click **Delete**.

To delete all the application from the list, click **Remove All**.

Device Control

The Device Control tab enables you to allow/block the access to the USB devices and the CD/DVD in client computers.



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

- **USB Control:** This option lets you allow, block, or set 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 the options **Use Other Password** and **Use Escan Administrator Password** respectively.
- **Blacklist:** This option lets you add USB devices to the blacklist. You can add, delete, modify USB devices using the following options:

- **Add:** Use this button to enter USB serial number, name, and description of the USB devices in order to blacklist it.

- **Import:** It allows you to blacklist multiple USB devices at once using CSV file.
- **Edit:** It allows you to edit the details of the USB devices.
- **Delete:** It allows you to remove the USB device from the list.
- **Remove All:** It allows you to remove all the USB devices from the list.
- **Print:** It allows you to print the USB device list along with their details.
- **Whitelist:** This option lets you add USB devices to the whitelist. You can add, delete, modify USB devices using the following options:
 - **Add:** Use this button to enter USB serial number, name, and description of the USB devices in order to whitelist it.

- **Import:** It allows you to whitelist multiple USB devices at once using CSV file.
- **Edit:** It allows you to edit the details of the USB devices.
- **Delete:** It allows you to remove the USB device from the list.
- **Remove All:** It allows you to remove all the USB devices from the list.
- **Print:** It allows you to print the USB device list along with their details.
- **Monitor to USB:** Select this checkbox to monitor all the 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 settings. You have following options to configure:

- **Block CD/DVD:** This option blocks CD/DVD inserted in the computer.

- **Read Only CD/DVD:** This option allows limited (only reading) access to the user for the data stored in inserted CD/DVD.
- **Disable:** This option disables the configured settings for CD/DVD.

File Integrity Monitor

The screenshot shows the 'File Integrity Monitor' configuration window. At the top, there are 'Start' and 'Stop' radio buttons, with 'Start' selected. Below this are three tabs: 'Application Control', 'Device Control', and 'File Integrity Monitor'. The 'File Integrity Monitor' tab is active and contains the following elements:

- An 'Enable FIM' checkbox with a user icon, which is currently unchecked.
- A row of two checkboxes: 'File Integrity Check Alert' (checked) and 'Create New Baseline' (unchecked).
- An 'Enter Directory Name' text input field.
- An 'Add' button next to the text input field.
- A table with the following content:

Directories Name
<input type="checkbox"/> /lib
<input type="checkbox"/> /etc
<input type="checkbox"/> /bin
<input type="checkbox"/> /sbin
- 'Delete' and 'Remove All' buttons to the right of the table.
- 'Default', 'OK', and 'Cancel' buttons at the bottom of the window.

Enable FIM

Select this checkbox to enable the File Integrity Monitor option.

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

Enter Directory Name

Enter the directory name to add it to the integrity monitoring.

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

To delete a specific directory from monitoring, select the directory, and click **Delete**.

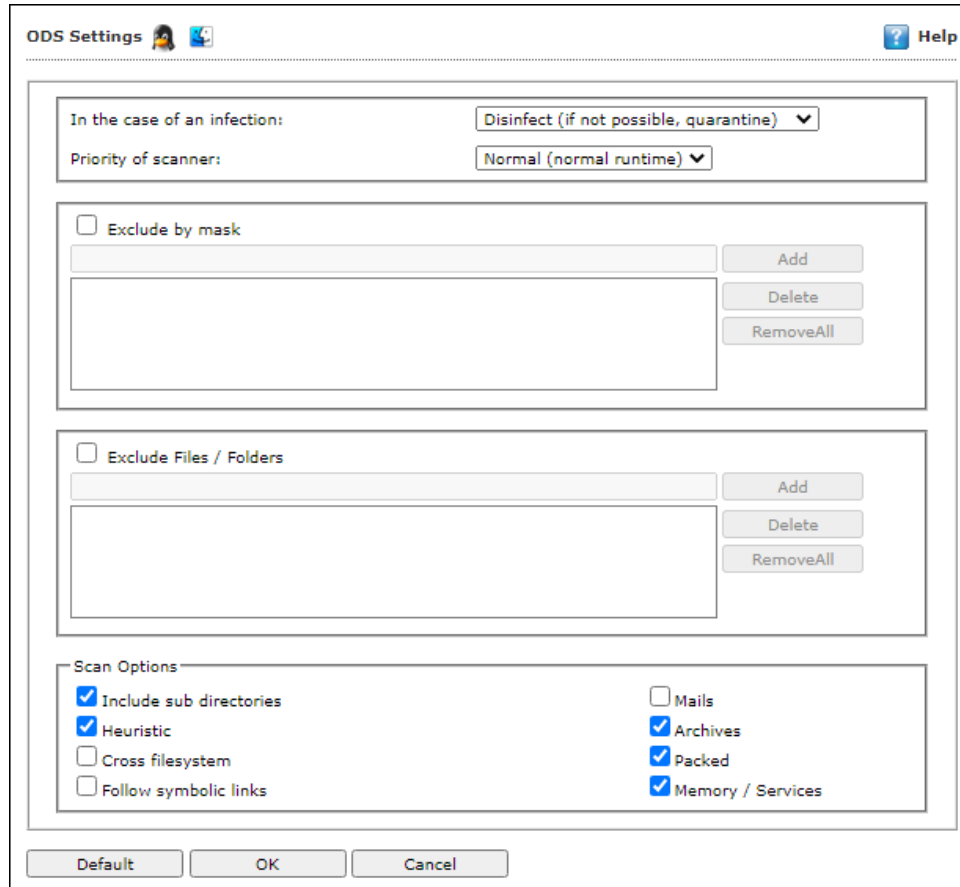
To remove all the directory from monitoring, click **Remove All**.

Default

This button will reset all the settings of the window to their default values.

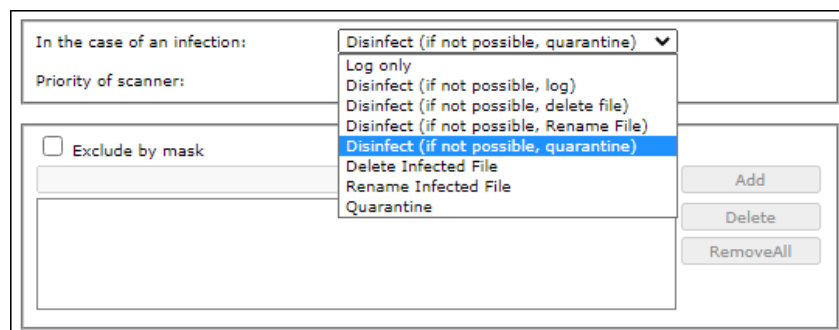
ODS Settings

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.



Actions in the case of infection [Drop-down]

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 deletes the infected object.
- **Rename Infected File:** It renames the infected object.
- **Quarantine:** It quarantines the infected object.

Priority of Scanner – You can select the priority of scanning as **High (short runtime)**, **Normal (normal runtime)**, or **Low (long runtime)**.

- **High (short runtime)** – Has a short runtime.
- **Normal (normal runtime)** – Has a normal runtime.
- **Low (long runtime)** – Has a long runtime.

Exclude by Mask – Select this checkbox if you want eScan real-time protection to exclude specific files, and Remove any or all Added Files whenever required.

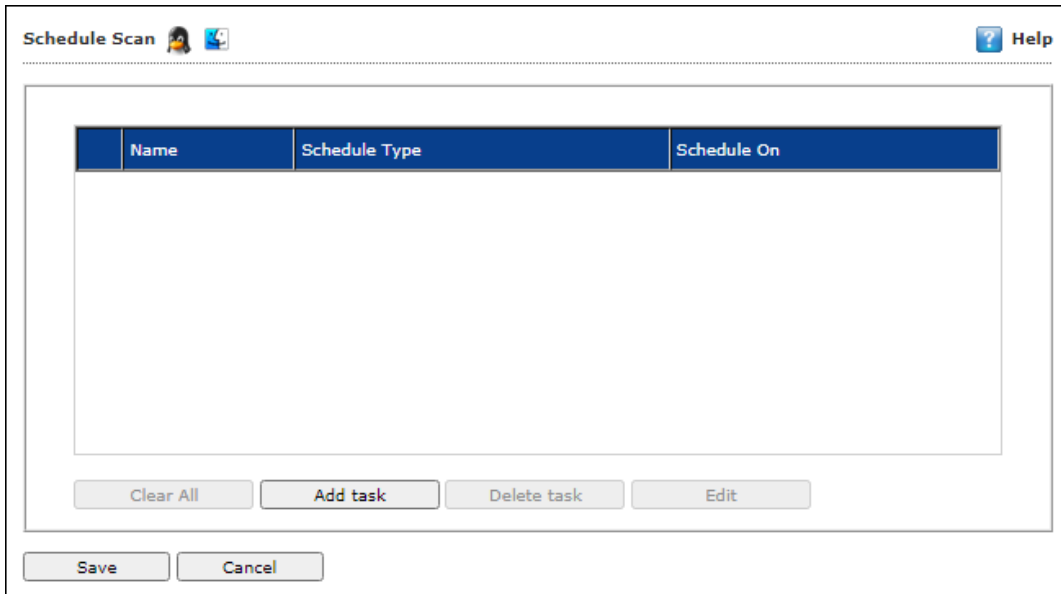
Exclude Files / Folders – Select this checkbox if you want eScan real-time protection to exclude Folders and files from scanning. eScan lets you add; Remove any or all Added Files or Folders whenever required during On Demand Scanning.

Scan options

- **Include Sub Directories [Default]** – This option ensures eScan scans all the sub directories recursively under every directory and not only the first level of directories.
- **Heuristic [Default]** – 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.
- **Mails** – It indicates scanning the mail files. Select this checkbox if you want eScan real-time protection to scan mails.
- **Archives [Default]** – It indicates the archived files, such as zip, rar, and so on. Select this checkbox if you want eScan real-time protection to scan archived files.
- **Packed [Default]** – It indicates the compressed executable.
- **Memory / Services [Default]** – This option ensures eScan scans the system's memory for any infection from malwares.

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

Schedule Scan



Name	Schedule Type	Schedule On

Clear All Add task Delete task Edit

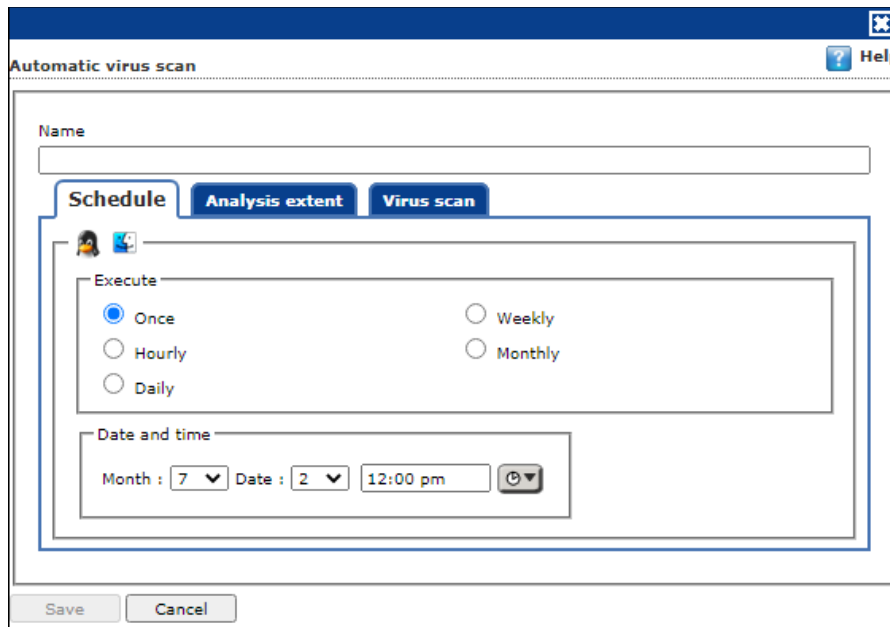
Save Cancel

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



Automatic virus scan Help

Name:

Schedule Analysis extent Virus scan


Execute:

Once Weekly

Hourly Monthly

Daily

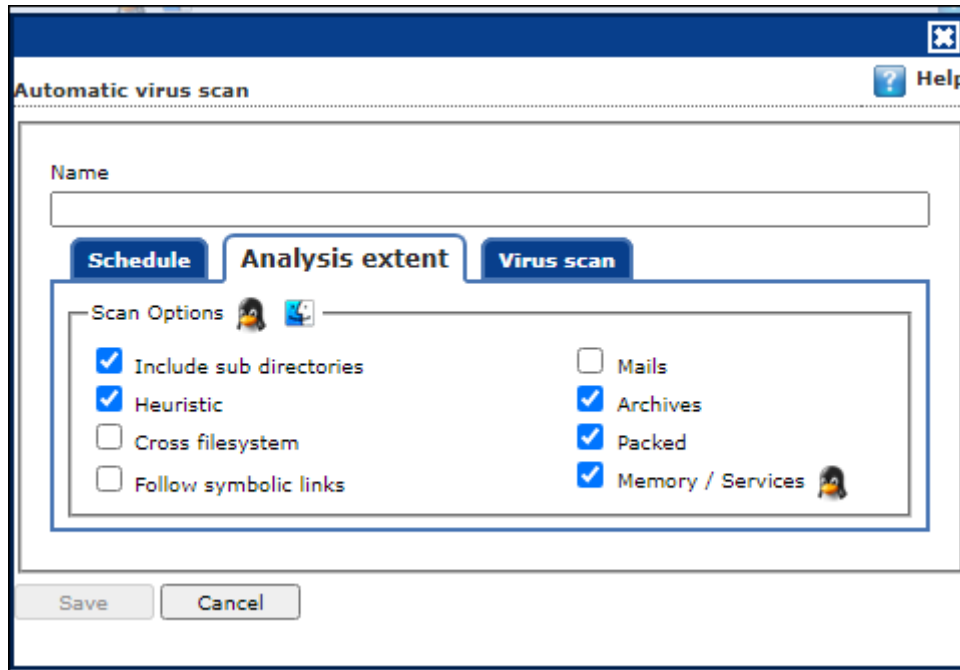
Date and time:

Month: 7 Date: 2 12:00 pm 

Save Cancel

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

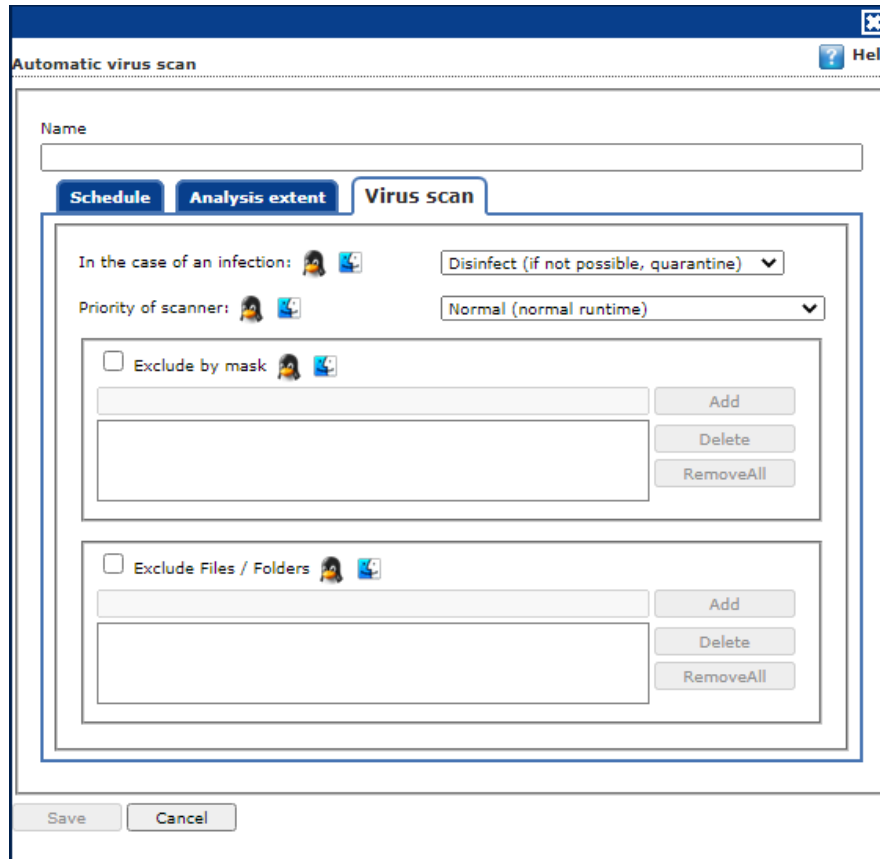
Analysis Extent



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

- **Include sub Directories [Default]** – This option lets you include sub directories while conducting an automatic scan.
- **Heuristic Scan [Default]** – 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** - facilitates scanning of files over cross-file systems.
- **Follow symbolic links** - scans the files following the symbolic links.
- **Mails** - It indicates scanning the mail files. By default, it is selected. Select this checkbox if you want eScan real-time protection to scan mails.
- **Archives [Default]** - It indicates the archived files, such as zip, rar, and so on. Select this checkbox if you want eScan real-time protection to scan archived files.
- **Packed [Default]** - It indicates the compressed executable. Select this checkbox if you want eScan real-time protection to scan packed files.
- **Memory / Services [Default]** - This option will only scan the memory of the system.

Virus Scan



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:

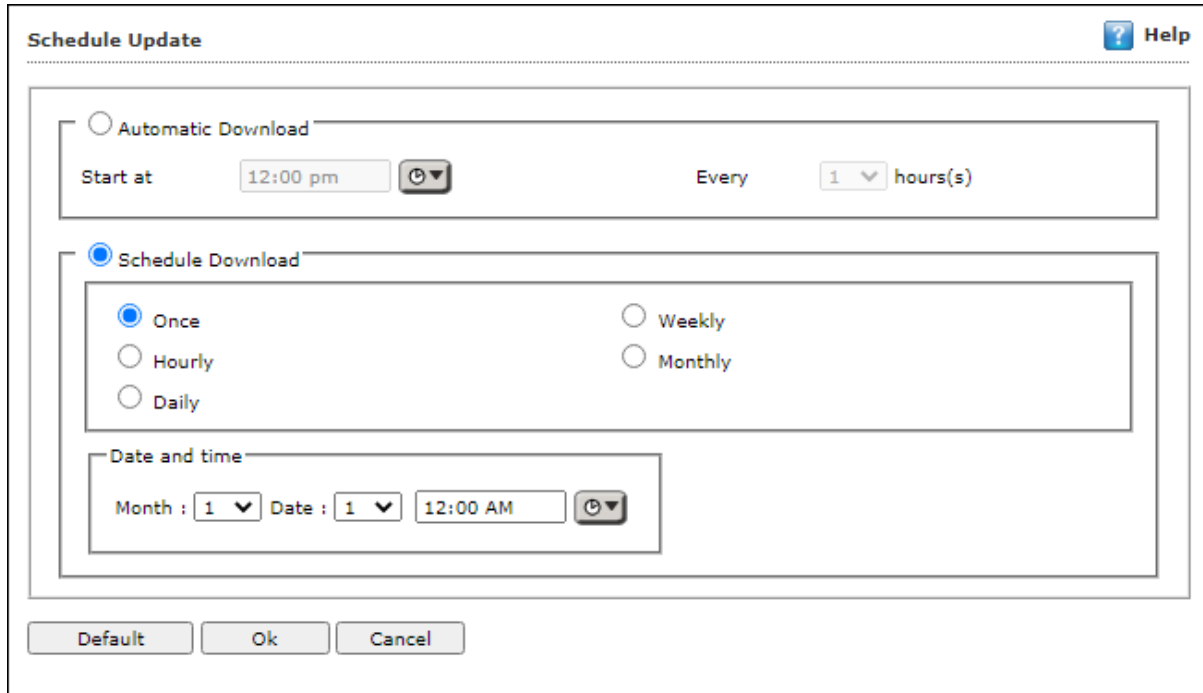
- **Log Only:** It indicates or alerts the user about the infection detected.
- **Delete Infected File:** Infected objects are deleted with this option.
- **Rename Infected File:** This option allows you to rename the infected files.
- **Quarantine:** Infected objects are quarantined with this option.
- **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):** It tries to disinfect and if disinfection is not possible it quarantines the infected object.
- **Disinfect (if not possible, Rename file):** It tries to disinfect and if disinfection is not possible it renames the infected object.

Exclude by Mask - Select this checkbox 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 Files / Folders - Select this checkbox 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.



The screenshot shows the "Schedule Update" dialog box. It has a title bar with "Schedule Update" and a "Help" button. The dialog is divided into two main sections: "Automatic Download" and "Schedule Download".

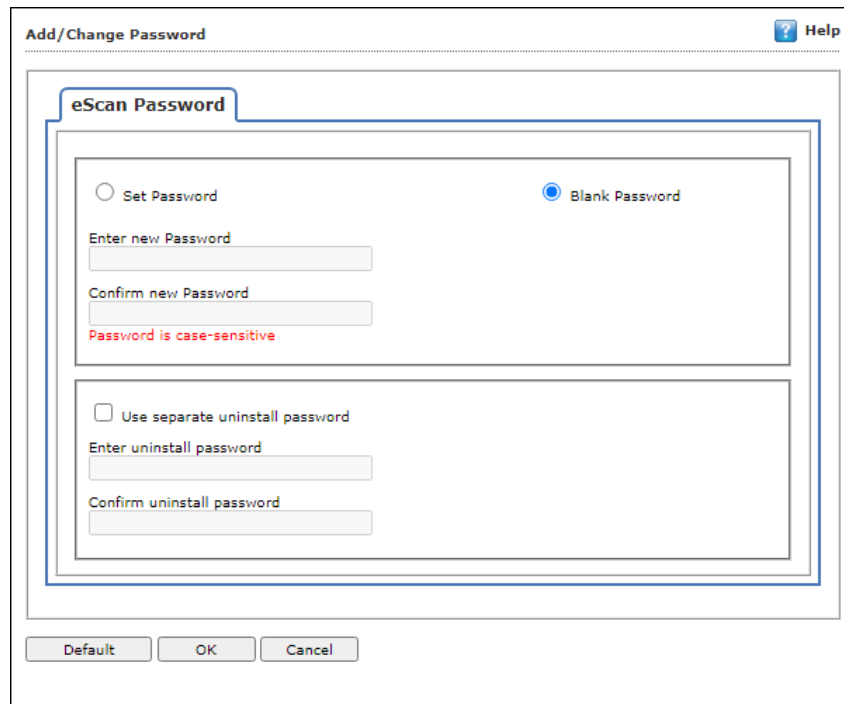
- Automatic Download:** This section is currently unselected. It contains a "Start at" field set to "12:00 pm" with a dropdown arrow, and a frequency field set to "Every 1 hours(s)".
- Schedule Download:** This section is selected. It contains five radio button options: "Once" (selected), "Hourly", "Daily", "Weekly", and "Monthly".
- Date and time:** Below the radio buttons, there is a "Date and time" section with three dropdown menus: "Month" (set to 1), "Date" (set to 1), and a time field (set to 12:00 AM) with a dropdown arrow.

At the bottom of the dialog, there are three buttons: "Default", "Ok", and "Cancel".

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

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.



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.

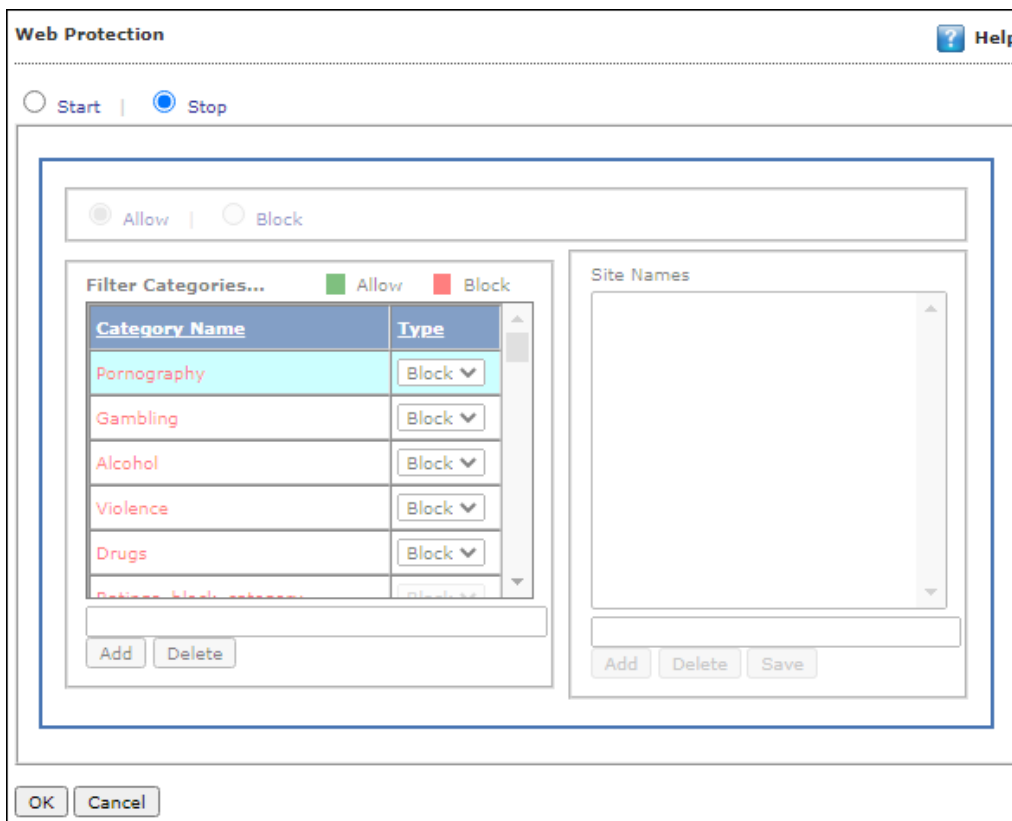
After filling all fields, click **OK**. The Password will be saved.

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.



You can configure the following settings.

Filtering Options

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

Status

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

Filter Categories

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

- **Green:** It represents an allowed websites category.
- **Red:** It represents a blocked websites category.

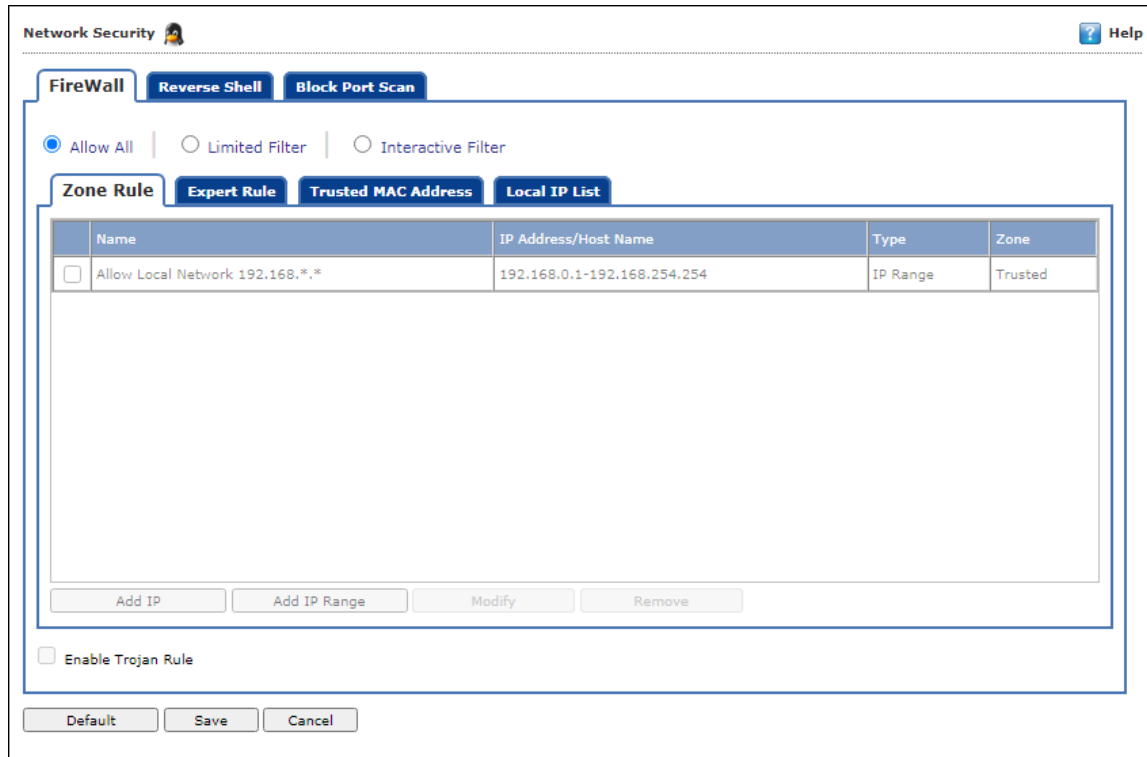
The filter categories used in this section include categories like Pornography, Gambling, Chat, Alcohol, Violence, Drugs, Ratings block category, Websites Allowed, etc. You can also add or delete filter categories depending on your requirement.


Category Name

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

Network Security

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



Network Security  ? Help

FireWall | Reverse Shell | Block Port Scan

Allow All | Limited Filter | Interactive Filter

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

	Name	IP Address/Host Name	Type	Zone
<input type="checkbox"/>	Allow Local Network 192.168.*.*	192.168.0.1-192.168.254.254	IP Range	Trusted

Enable Trojan Rule

Firewall

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

Name	IP Address/Host Name	Type	Zone
<input type="checkbox"/> Allow Local Network 192.168.0.0	192.168.0.0-192.168.255.255	IP Range	Trusted

You can configure the following settings to be deployed to the eScan client systems.

Allow All – Clicking **Allow All** disables the eScan Firewall i.e. all the incoming and outgoing network traffic will not be monitored/filtered.

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

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

Following tabs are available:

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

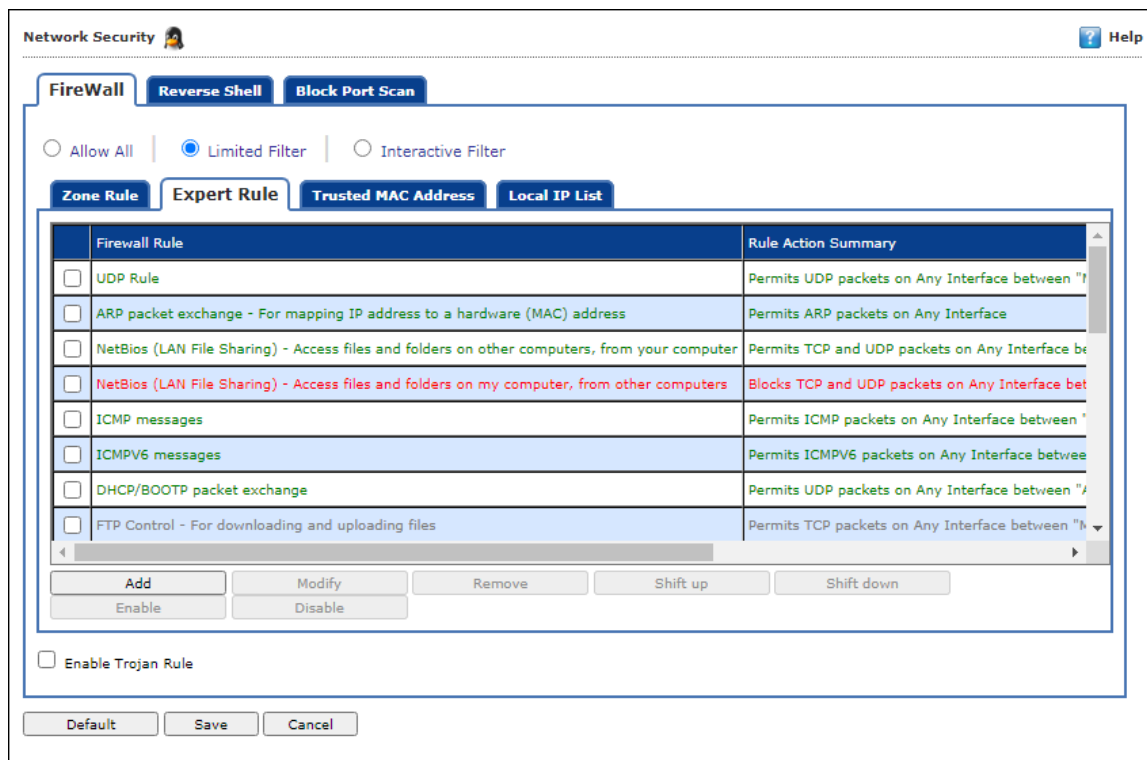
Zone Rule

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

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

Expert Rule

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



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

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

The following buttons are available to configure an Expert Rule:

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

The screenshot shows a dialog box titled "Add Firewall Rule" with four tabs: "General", "Source", "Destination", and "Advanced". The "General" tab is selected and contains the following fields:

- Rule Name:** A text input field containing "Rule1".
- Rule Action:** Two radio buttons: "Permit Packet" (selected) and "Deny Packet".
- Protocol:** A dropdown menu showing "TCP and UDP".
- Apply Rule on Interface:** A dropdown menu showing "Any Interface".

At the bottom of the dialog box are "OK" and "Cancel" buttons.

General tab

In this section, specify the Rule settings:

Rule Name – Provide a name to the Rule.

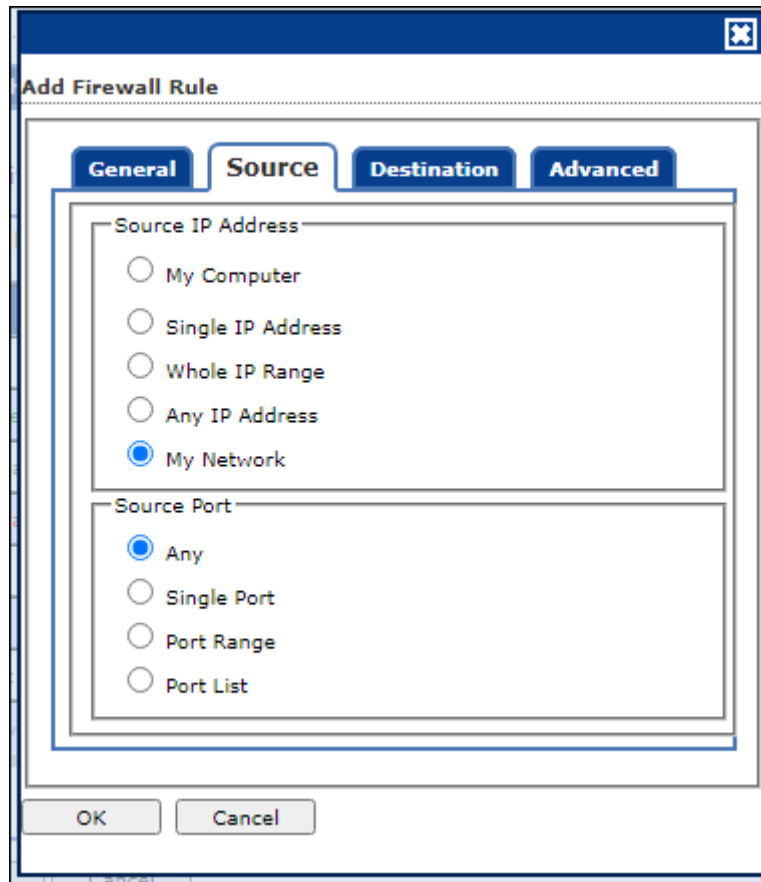
Rule Action – Action to be taken, whether to Permit Packet or Deny Packet.

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.



Source IP Address:

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

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

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

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

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

Source Port:

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

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

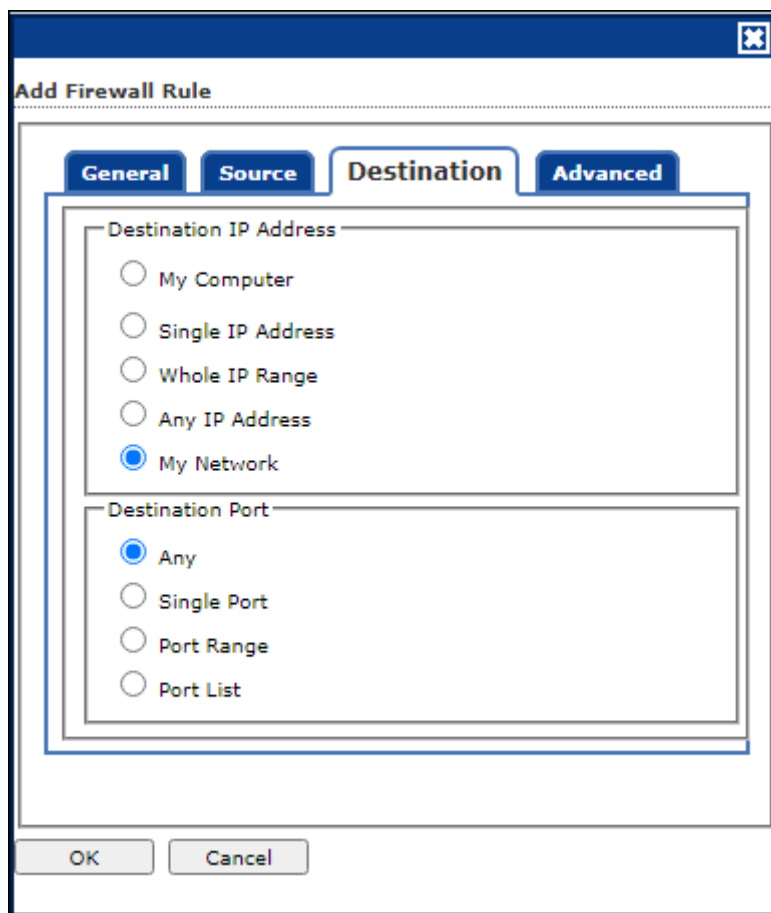
Port Range – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the outgoing traffic originating from the port which is within the defined range of ports.

Port List – A list of 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.

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

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

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

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

Destination IP Port:

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

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

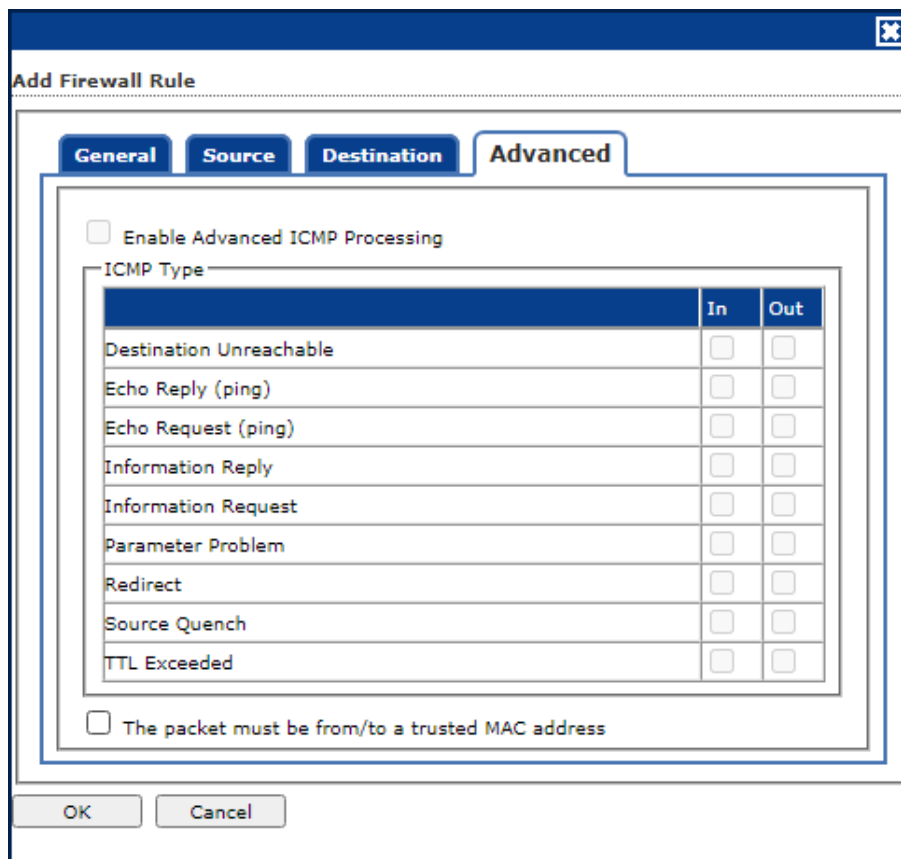
Port Range – To enable the rule on a group of ports in series, you can specify a range of ports.

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

	The rule will be applied when the selected Destination IP Address and Destination Port matches together.
--	--

Advanced tab

This tab contains advance setting for Expert Rule.



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

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

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

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

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

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

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

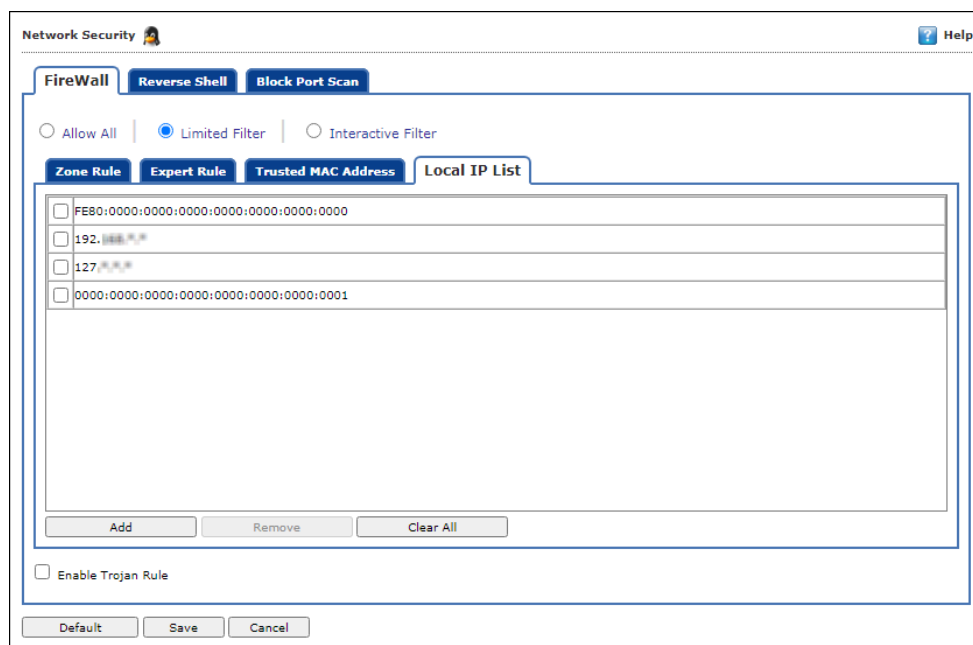
Trusted MAC Address

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

- **Add** – To add a MAC address click on this button. Enter the MAC address to be added in the list for e.g. **00-13-~~BF~~-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.



Add – To add a local IP address, click **Add**.

Remove – To remove a local IP address, click **Remove**.

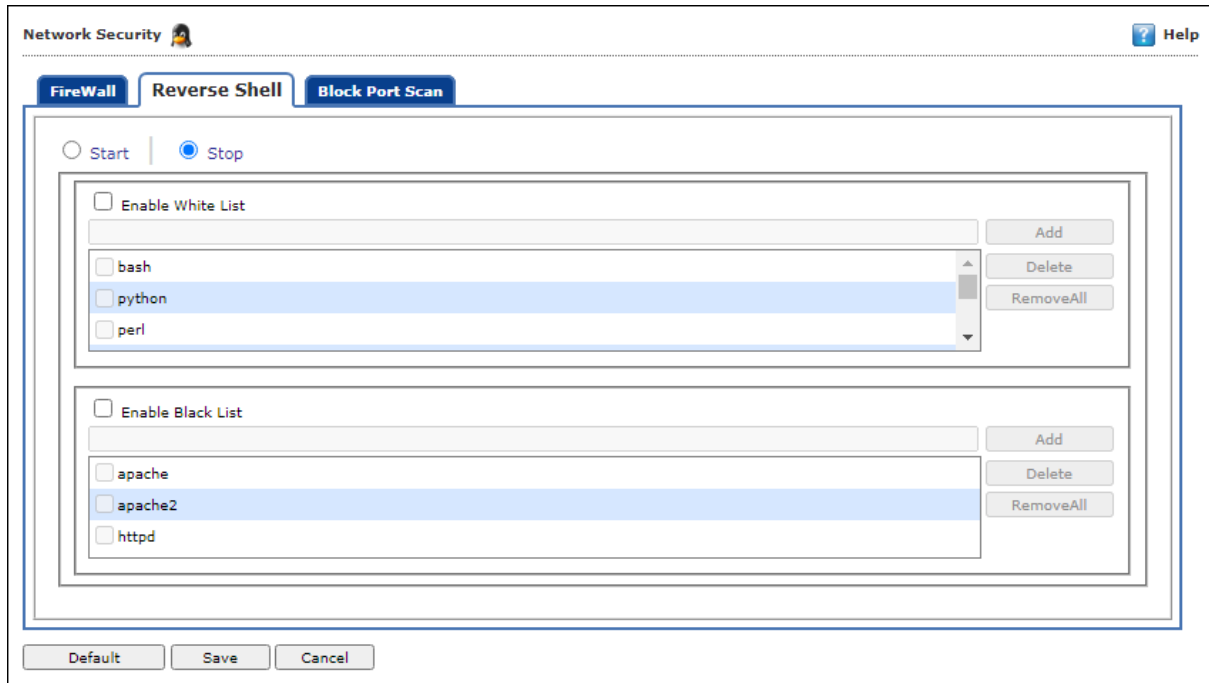
Clear All – To clear all local IP addresses, click **Clear All**.

Enable Trojan Rule

Select this checkbox, to enable the Trojan Rule.

Reverse Shell

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



Start/Stop

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

After enabling this, you can configure the following settings:

Enable White List

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

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

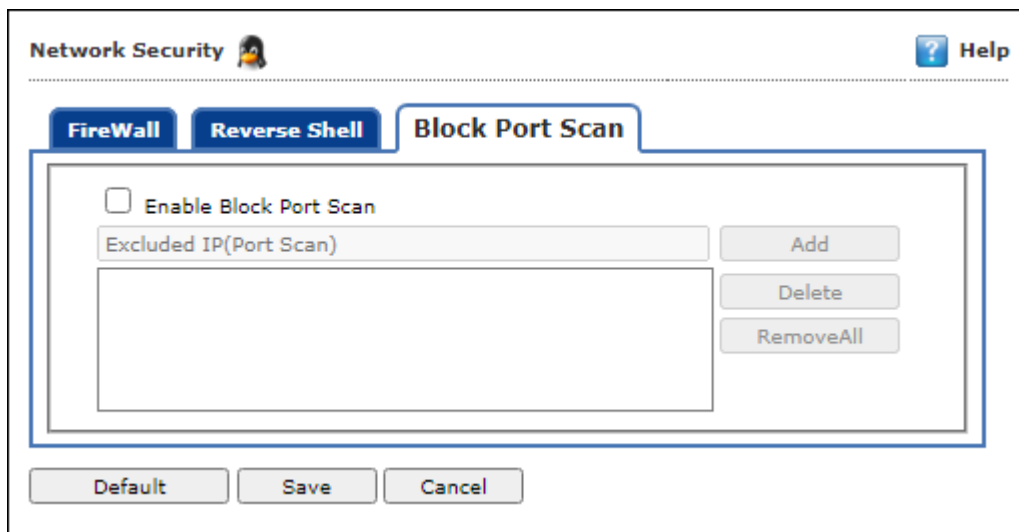
Enable Black List

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

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

Block Port Scan

This tab allows admin to configure the port scan option.



The screenshot shows the 'Network Security' configuration window with the 'Block Port Scan' tab selected. The interface includes a header with 'Network Security' and a 'Help' icon. Below the header are three tabs: 'FireWall', 'Reverse Shell', and 'Block Port Scan'. The 'Block Port Scan' tab contains a checkbox labeled 'Enable Block Port Scan'. Below this is a text input field labeled 'Excluded IP(Port Scan)' with an 'Add' button to its right. A list box is positioned below the input field, with 'Delete' and 'RemoveAll' buttons to its right. At the bottom of the window are three buttons: 'Default', 'Save', and 'Cancel'.

Enable Block Port Scan

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

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

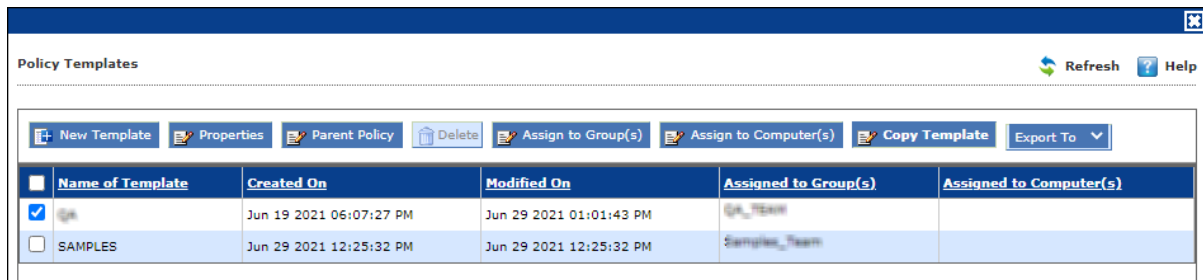
Assigning Policy Template to a group

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

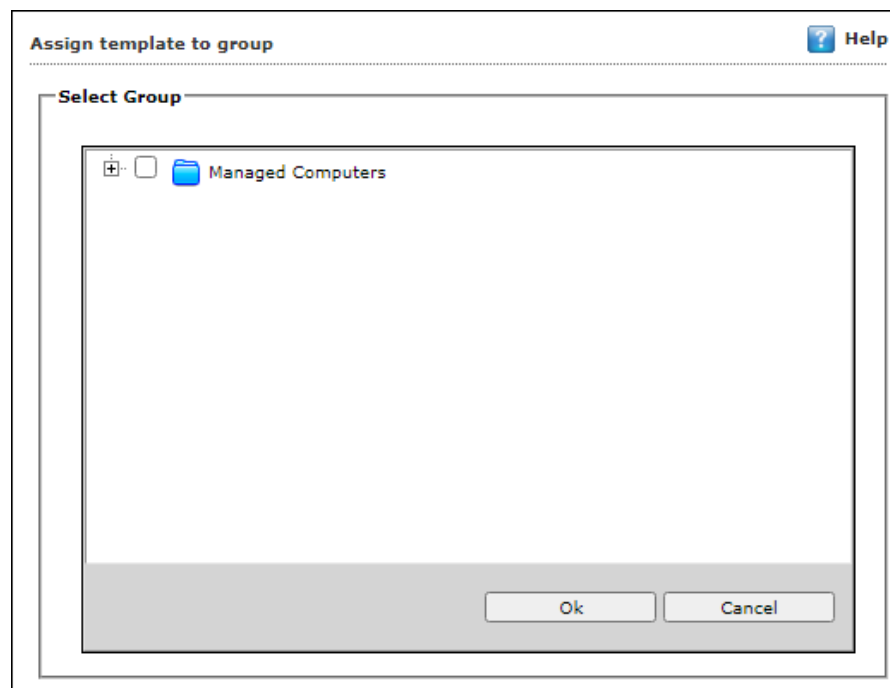
Method 1

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.



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

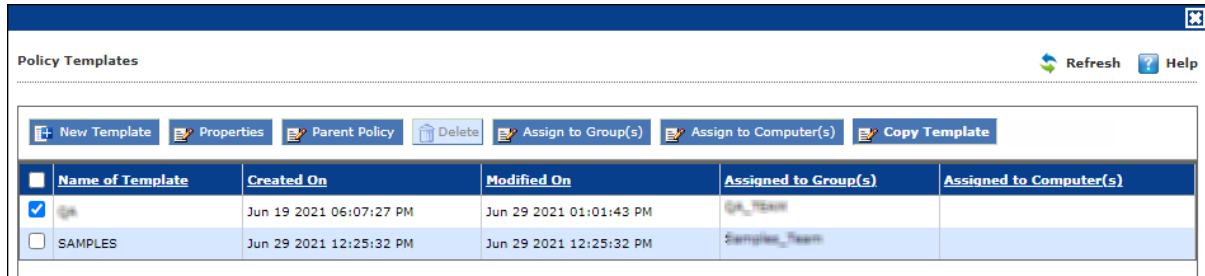


4. Select the group(s) and then click **OK**.
The policy will be assigned to the selected group(s).

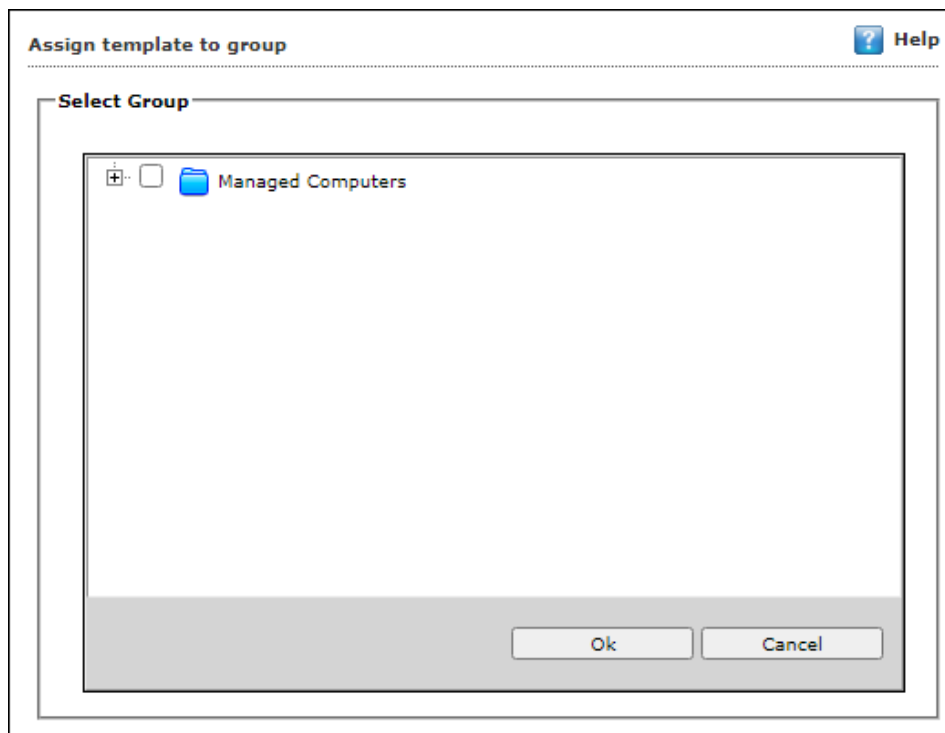
Assigning Policy Template to Computer(s)

To assign a policy template to computers:

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



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

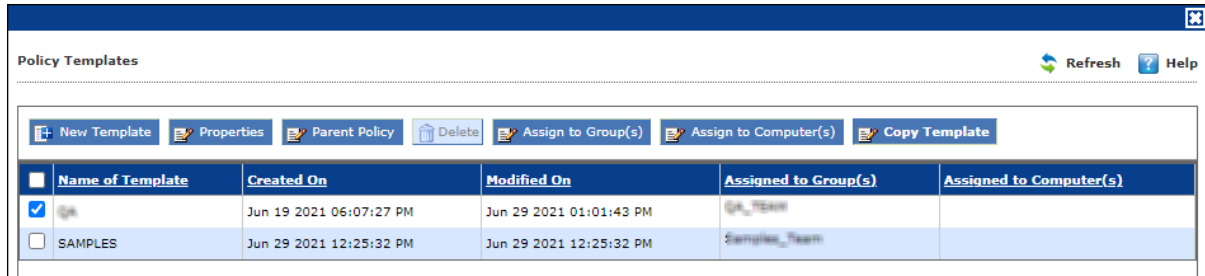


4. Click **Managed Computers**.
5. Select the computer(s) and then click **OK**.
The policy template will be assigned to the selected computers.

Copying a Policy Template

To copy a Policy Template:

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



2. Click **Copy Template**.
New Template window appears displaying settings from the original template.
3. Enter a name for the template.
4. 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

 Refresh
 Help

New Template
 Create Schedule
 Properties
 Delete

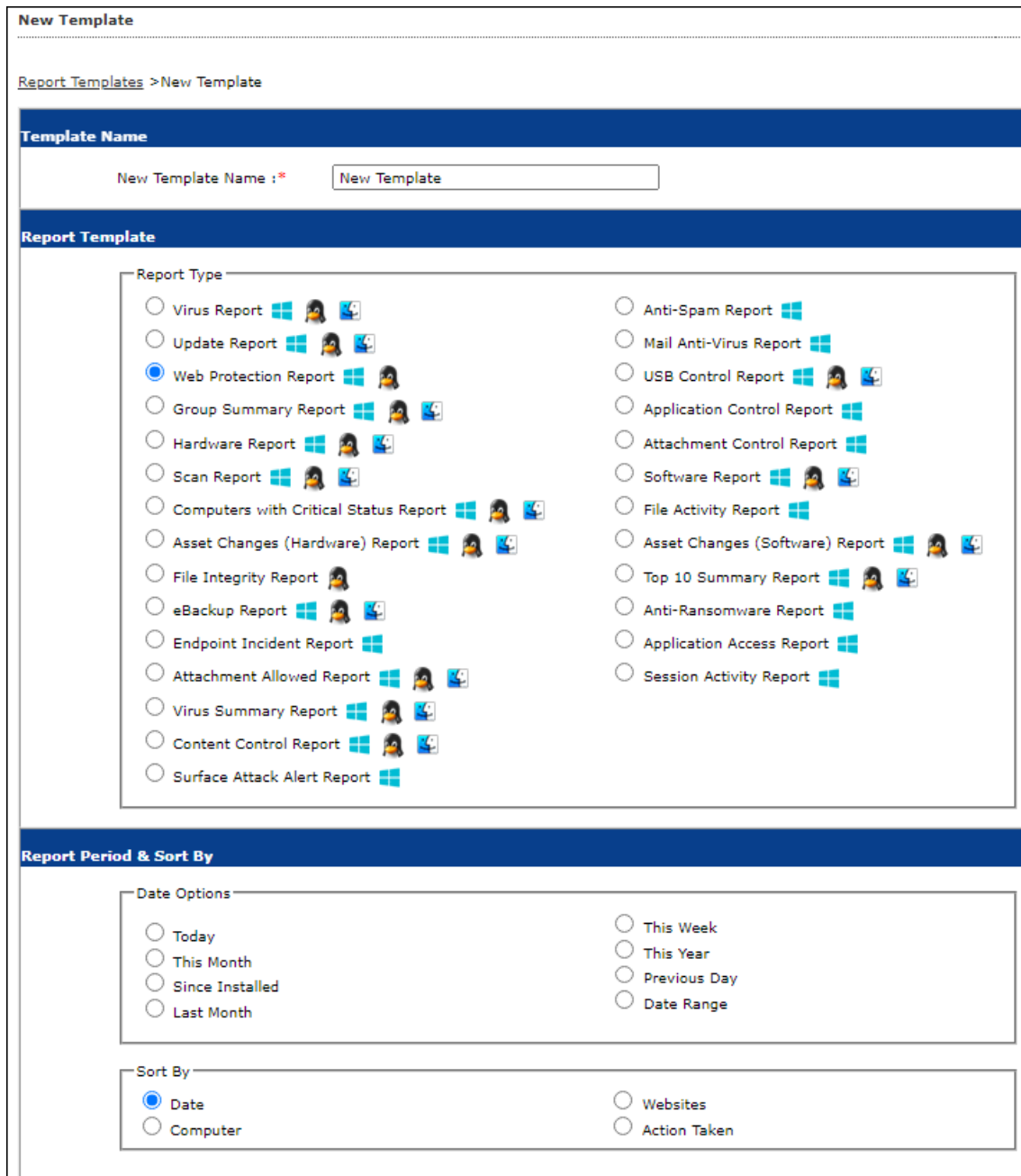
Template Name
<input type="checkbox"/> Virus Report
<input type="checkbox"/> Update Report
<input type="checkbox"/> Scan Report
<input type="checkbox"/> Web Protection Report
<input type="checkbox"/> Application Control Report
<input type="checkbox"/> Attachment Control Report
<input type="checkbox"/> Anti-Spam Report
<input type="checkbox"/> Mail Anti-Virus Report
<input type="checkbox"/> USB Control Report
<input type="checkbox"/> Group Summary Report
<input type="checkbox"/> Hardware Report
<input type="checkbox"/> Software Report
<input type="checkbox"/> File Activity Report
<input type="checkbox"/> Computers with Critical Status Report
<input type="checkbox"/> Asset Changes (Software) Report
<input type="checkbox"/> Asset Changes (Hardware) Report
<input type="checkbox"/> Top 10 Summary Report
<input type="checkbox"/> Anti-Ransomware Report
<input type="checkbox"/> Application Access Report
<input type="checkbox"/> Session Activity Report
<input type="checkbox"/> eBackup Report
<input type="checkbox"/> Endpoint Incident Report

Creating a Report Template

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

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

New Template screen appears.



New Template

[Report Templates](#) > New Template

Template Name

New Template Name :*

Report Template

Report Type

- Virus Report
- Update Report
- Web Protection Report
- Group Summary Report
- Hardware Report
- Scan Report
- Computers with Critical Status Report
- Asset Changes (Hardware) Report
- File Integrity Report
- eBackup Report
- Endpoint Incident Report
- Attachment Allowed Report
- Virus Summary Report
- Content Control Report
- Surface Attack Alert Report
- Anti-Spam Report
- Mail Anti-Virus Report
- USB Control Report
- Application Control Report
- Attachment Control Report
- Software Report
- File Activity Report
- Asset Changes (Software) Report
- Top 10 Summary Report
- Anti-Ransomware Report
- Application Access Report
- Session Activity Report

Report Period & Sort By

Date Options

- Today
- This Month
- Since Installed
- Last Month
- This Week
- This Year
- Previous Day
- Date Range

Sort By

- Date
- Computer
- Websites
- Action Taken

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

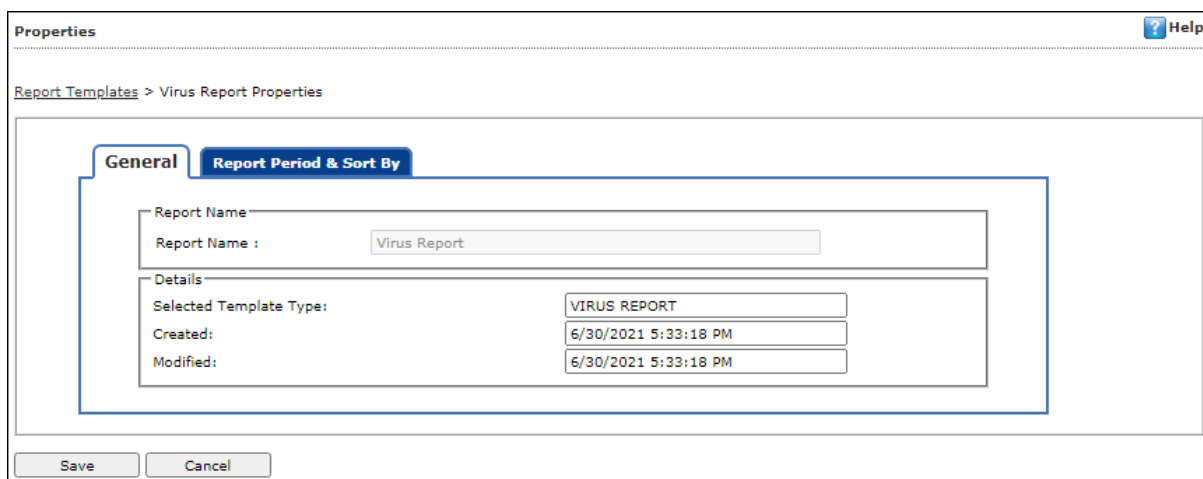
Creating Schedule for a Report Template

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

Viewing Properties of a Report Template

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

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



Properties Help

Report Templates > Virus Report Properties

General Report Period & Sort By

Report Name
Report Name : Virus Report

Details

Selected Template Type:	VIRUS REPORT
Created:	6/30/2021 5:33:18 PM
Modified:	6/30/2021 5:33:18 PM

Save Cancel

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

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

Deleting a Report Template

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

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

NOTE Default Report Templates cannot be deleted.

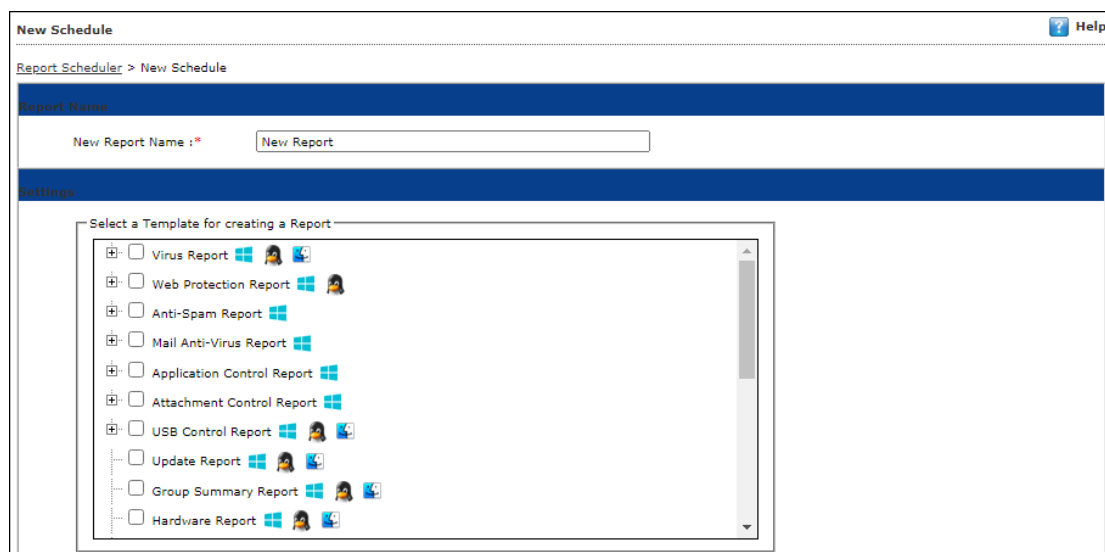
Report Scheduler

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

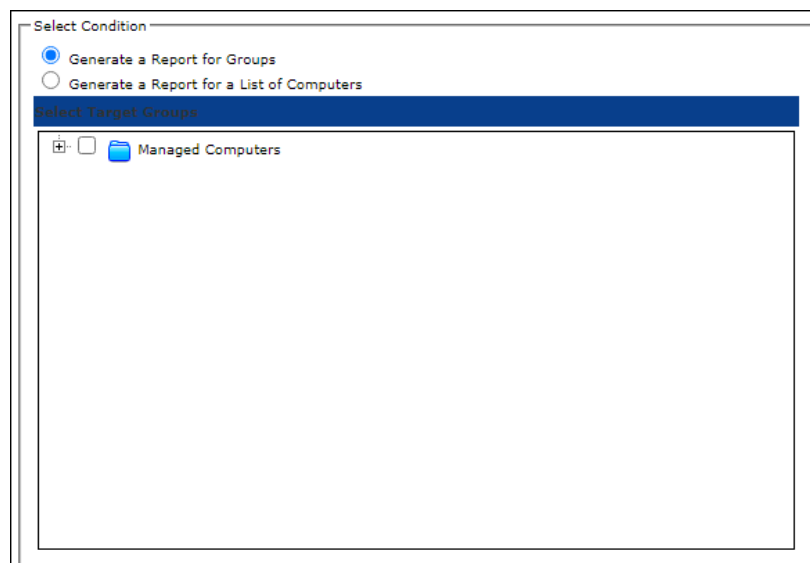
Creating a Schedule

To create a Schedule:

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



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



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

Send Report by Email

Report Sender*:	<input type="text" value="prashant@escanav.com"/>	
Report Recipient*:	<input type="text"/>	<input type="button" value="Add"/>
	<input type="text" value="prashant@escanav.com"/>	<input type="button" value="Delete"/>
Mail Server IP Address:	<input type="text" value="192.168.0.1"/>	
Mail Server Port:	<input type="text" value="25"/>	
User Authentication:	<input type="text"/>	
Password Authentication:	<input type="text"/>	

* For Example: user@yourcompany.com

Select the Report Format

HTML page
▼

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

Report Scheduling Settings

Enable Scheduler
 Manual Start

Daily
 Weekly
 Mon Tue Wed Thu
 Fri Sat Sun

Monthly
 Last Day of Month

At

(*) Mandatory Fields

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

Viewing Reports on Demand

To view a report or a set of reports immediately:

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

Report Scheduler > New Schedule

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

Select Condition

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

Select Target Groups

- Managed Computers

Create Schedule Cancel View

(*) Mandatory Fields

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.

The screenshot shows the 'Report Scheduler' interface. At the top right, there are 'Refresh' and 'Help' buttons. Below the header is a toolbar with buttons for 'Start Task', 'Results', 'Properties', 'Delete', 'New Schedule', and 'View & Create'. The main area contains a table with the following data:

	Schedule Name	Report Recipient	Scheduler Type	View
<input checked="" type="checkbox"/>	New Report	prashanta@escanav.com	Automatic Scheduler	View

Generating Task Report of a Schedule

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

Viewing Results of a Schedule

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

The screenshot shows the 'Results(EDR)' window. It has a 'Help' button at the top right. Below the header, it says 'Report Scheduler > Results'. The main area contains a table with the following data:

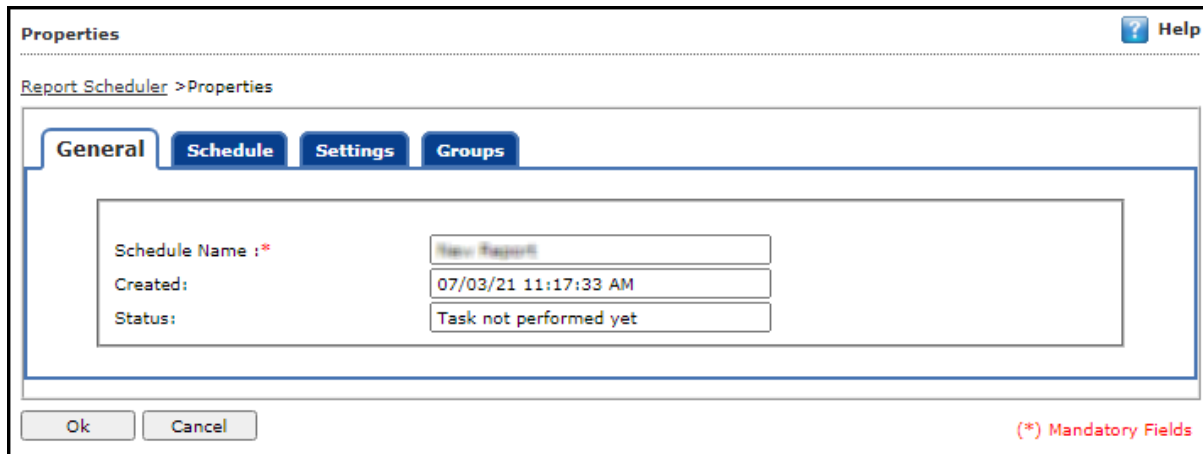
Status	Time
Completed	7/7/2021 1:35:05 PM
Completed	7/7/2021 1:21:47 PM
Completed	7/7/2021 1:17:39 PM
Completed	7/7/2021 1:12:01 PM
Completed	7/7/2021 1:08:25 PM
Completed	7/7/2021 1:02:29 PM
Completed	7/7/2021 12:53:48 PM
Completed	7/7/2021 12:37:36 PM

At the bottom left, there is a 'Cancel' button.

Viewing Properties of a Schedule

To view the properties of a schedule:

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



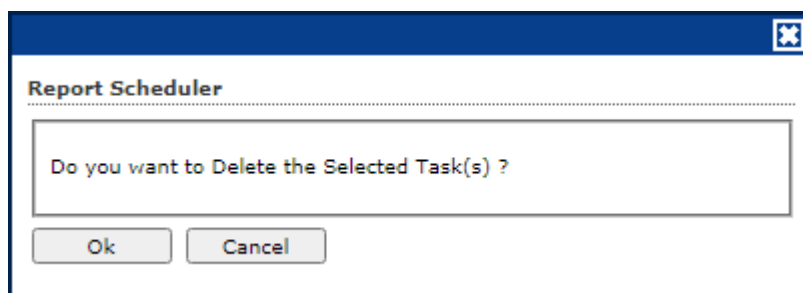
The screenshot shows a 'Properties' dialog box for a 'Report Scheduler'. The dialog has a title bar with a help icon and the text 'Properties'. Below the title bar, there is a breadcrumb 'Report Scheduler > Properties'. The main area contains four tabs: 'General', 'Schedule', 'Settings', and 'Groups'. The 'General' tab is selected. Inside the 'General' tab, there are three input fields: 'Schedule Name :*' with the value 'New Report', 'Created:' with the value '07/03/21 11:17:33 AM', and 'Status:' with the value 'Task not performed yet'. At the bottom left, there are 'Ok' and 'Cancel' buttons. At the bottom right, there is a red asterisk legend: '(*) Mandatory Fields'.

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

Deleting a Schedule

To delete a report schedule:

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

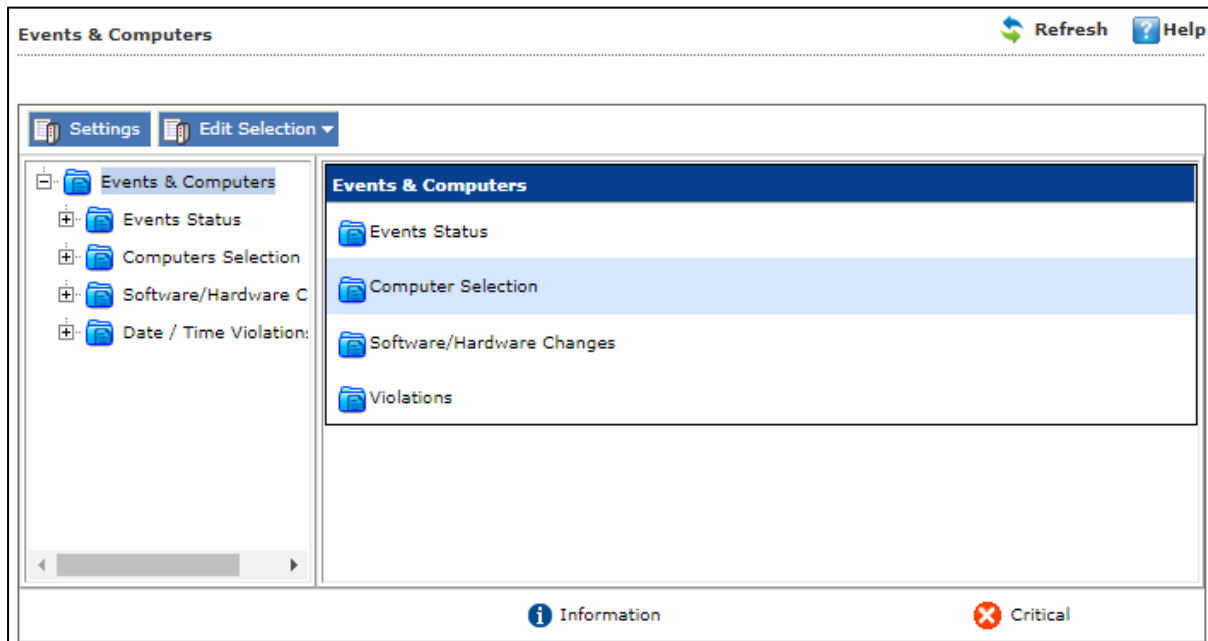


The screenshot shows a confirmation dialog box titled 'Report Scheduler'. The dialog has a title bar with a close icon. The main area contains the text 'Do you want to Delete the Selected Task(s) ?'. At the bottom, there are 'Ok' and 'Cancel' buttons.

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.

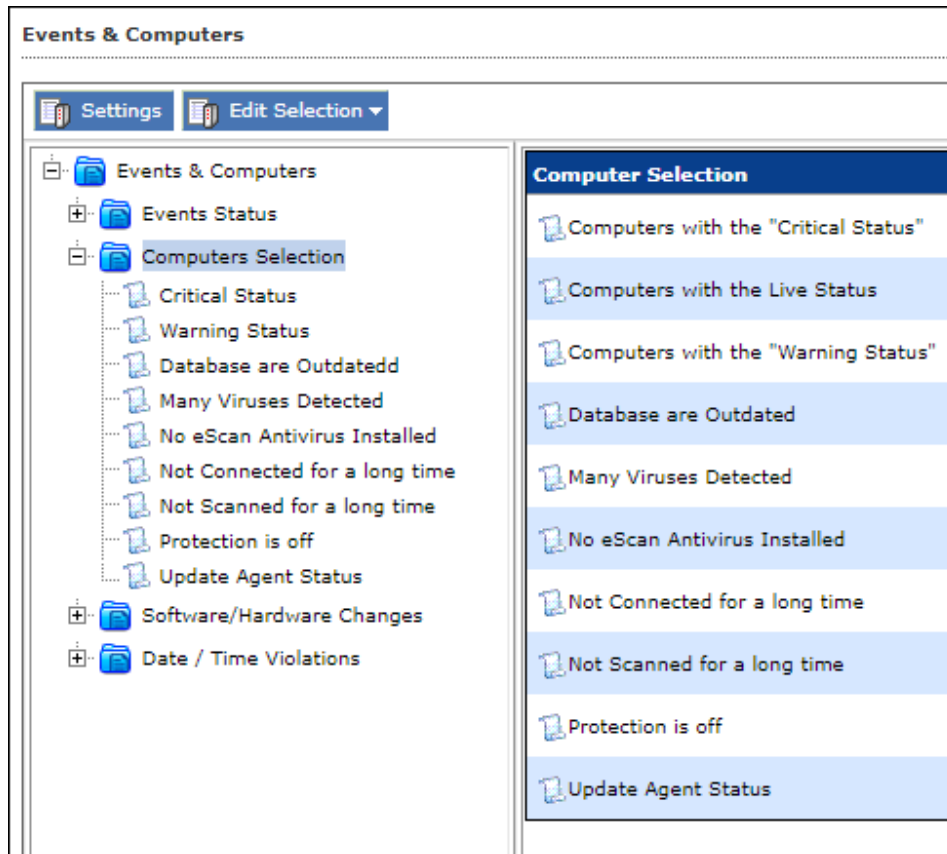
Information

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.



The Computer Selection subfolder consists following sections:

- **Computers with "Critical Status"**
- **Computers with "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**

This section displays computers marked with Critical status.

Computers with critical status

This section displays computers marked with Critical status.

Computers with warning status

This section displays computer with a warning status.

Database are 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 Antivirus Installed

This section displays computers on which eScan is not installed.

Not connected for a long time

This section displays the computers which didn't connect to the eScan server for the set duration.

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 Status

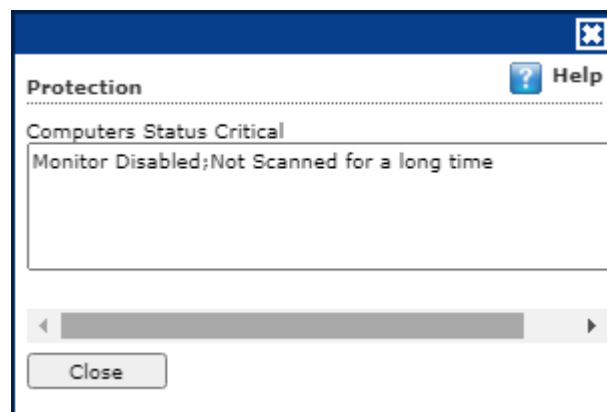
This section displays the status of computers assigned as Update Agent.

The additional settings vary depending upon the Computer Status.

Edit Selection

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

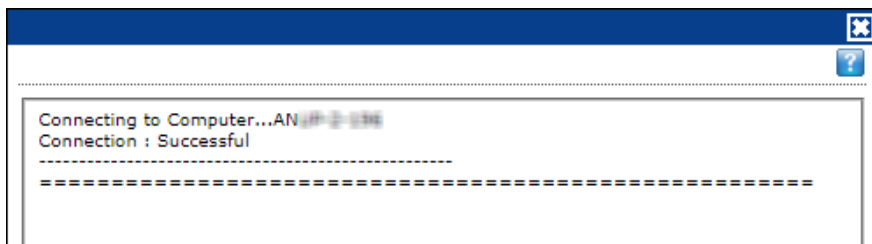
- **Protection:** This option displays the protection status of the selected computer.



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

Events & Computers Refresh Help						
Recent Events (#ANUP-2-636)						1 - 10 of 622 4 page
Date	Time	User's name	Event Id	Module Name	Description	Clie
	7/3/2021 12:52:35	root	File Anti-Virus (10154)	update	New virus database taken and applied [2021/07/03 07:52] [7.890105]	Upd
	7/3/2021 12:52:35	root	File Anti-Virus (10740)	winclient	/opt/MicroWorld/http://192.168.0.100-222/MWC/Win	eSc
	7/3/2021 12:52:34	root	File Anti-Virus (10154)	update	New virus database taken and applied [2021/07/03 07:52] [7.890105]	Upd
	7/3/2021 12:52:34	root	File Anti-Virus (10740)	winclient	/opt/MicroWorld/http://192.168.0.100-222/MWC/Win	eSc
	7/3/2021 11:30:18	root	File Anti-Virus (10154)	update	New virus database taken and applied [2021/07/03 08:08] [7.890105]	Upd
	7/3/2021 11:30:18	root	File Anti-Virus (10740)	winclient	/opt/MicroWorld/http://192.168.0.100-222/MWC/Win	eSc
	7/3/2021 11:30:18	root	File Anti-Virus (10740)	winclient	/opt/MicroWorld/http://192.168.0.100-222/MWC/Win	eSc
	7/3/2021 11:30:18	root	File Anti-Virus (10154)	update	New virus database taken and applied [2021/07/03 08:08] [7.890105]	Upd
	7/3/2021 10:30:14	root	File Anti-Virus (10740)	winclient	/opt/MicroWorld/http://192.168.0.100-222/MWC/Win	eSc
	7/3/2021 10:30:14	root	File Anti-Virus (10154)	update	New virus database taken and applied [2021/07/03 08:08] [7.890105]	Upd

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

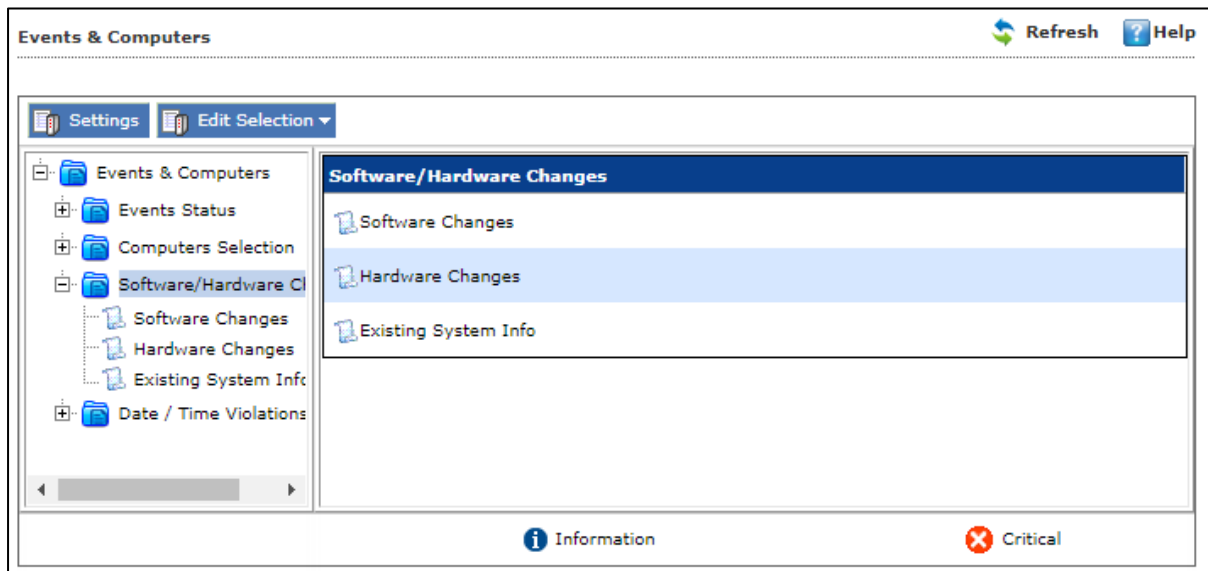


- **Remove from Group:** To learn about this option, [click here](#).
- **Force Download:** To learn about this option, [click here](#).
- **On Demand Scanning:** To learn about this option, [click here](#).
- **Send Message:** To learn about this option, [click here](#).
- **Properties:** To learn about this option, [click here](#).

Software/Hardware Changes

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

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



Software Changes

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

Hardware Changes

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

Existing System Info

This section displays a computer's existing hardware information.

Violations

Date/Time Violations

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

Date	Time	Machine Name	IP Address	User's name	Event Id	Module Name	Client Action
7/6/2021	13:05:53	WIN-QA007	192.168.0.88	WIN-QA007\pas	File Anti-Virus (1805)	eScan Monitor	Device/Computer Modif

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.

The screenshot shows the 'Events & Computers Settings' window with three tabs: 'Events Status', 'Computer Selection', and 'Software/Hardware Changes'. The 'Events Status' tab is active. Inside this tab, there is a section titled 'Events' containing an 'Events Name' dropdown menu set to 'Recent' and a 'Number Of Records' text input field set to '1000'. At the bottom of the window are 'Save' and 'Close' buttons.

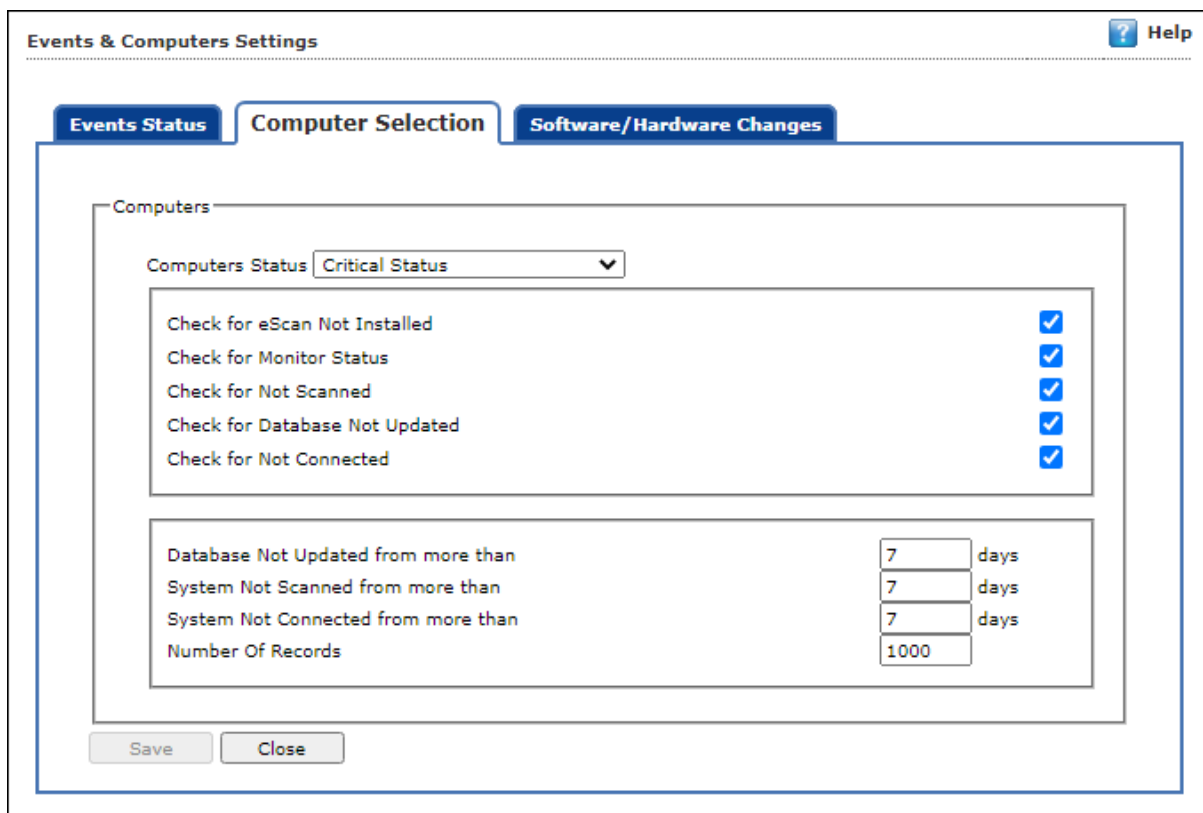
On the basis of severity, the events are categorized in to the following types:

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

Perform the following steps to define 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



The **Computer Selection** lets you select and save the computer status settings. This module lets you perform 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 details in following fields:

- **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 have 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 particular 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 systems that you want to view in the list.

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

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

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

- **System Not Connected from more than:** Enter the number of days from when the system has not been connected.
- **Number Of Record:** 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 Anti-Spam:** Select this checkbox if you want to view the list of client systems on which **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 the **Web Protection** is inactive.
- **Number of Records:** Enter the number of client system that you want to view in the list.

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

- **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 configure these settings to receive updates on any Software, Hardware, and existing system changes.

The screenshot shows a web-based configuration window titled "Events & Computers Settings". It has three tabs: "Events Status", "Computer Selection", and "Software/Hardware Changes". The "Software/Hardware Changes" tab is active. Inside this tab, there is a section labeled "Updates". Under "Updates", there is a dropdown menu labeled "Software/Hardware Changes" with "Software Changes" selected. Below this, there are two input fields: "Number Of Days" with the value "1" and the unit "days", and "Number Of Records" with the value "1000". At the bottom of the window, there are two buttons: "Save" and "Close".

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. To learn more [click here](#).
3. Click the preferred action.

Asset Management

This module displays list of hardware configuration, software installed, software version number and a Software report for Microsoft software installed on **Managed Computers**. The Asset Management module consists following tabs:

- **Hardware Report**
- **Software Report**
- **Software License**
- **Software Report (Microsoft)**

Hardware Report

The Hardware Report tab displays hardware configuration of all Managed Computers.

Computer Name	Group	IP Address	User's name	Operating System
ANUP-2-016	Managed Computers	192.168.2.136	root	Ubuntu Linux 16.10 64-bit
ESCAN_CLIENT	Sample_Team	192.168.0.133	ESCAN_CLIENT\Administrator	Windows XP Professional x64 Edition 64-bit
PRADHANT-Q1	Managed Computers	192.168.0.132	PRADHANT-Q1\Administrator	Windows 7 Home Basic Edition 32-bit
WII-ESCANDEVELOPER	Managed Computers	192.168.0.135	WII-ESCANDEVELOPER\Administrator	Windows 8 Professional 32-bit
WII-QAD07	QA_TEAM	192.168.0.85	WII-QAD07\qa	Windows 8.1 Professional 64-bit

The tab displays following details of managed computers:

- Computer Name
- Group
- IP Address
- User's name
- Operating System
- Service Pack
- OS Version
- OS Installed Date
- Internet Explorer
- Processor
- Motherboard
- RAM
- HDD
- Local MAC Adapter(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 version and 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 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.

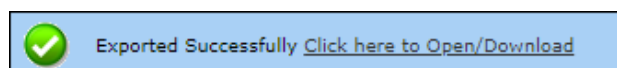
After making the necessary selections, click **Search**.

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.

Select the preferred format and then click **Export**. A success message appears with 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 Name	Computer Count
Brave	1
Client Authentication Agent	1
Dropbox	1
eScan Corporate - 360	1
eScan Corporate for Windows	2
Google Chrome	2
Microsoft SQL Server 2008 R2	1
Microsoft SQL Server 2008 R2 Native Client	1
Microsoft SQL Server 2008 R2 Setup (English)	1
Microsoft SQL Server 2008 Setup Support Files	1

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

Computer Name	Group	IP Address	Operating System	Software Version	Installed Date
1. 09L0D002703C4002N	Linux / Mac	192.168.0.209	Ubuntu Linux 18.04 32-Bit		20/10/2022
CE17020412.018	Linux / Mac	192.168.0.206	centos Linux 7 64-Bit		10/03/2022
RUB04-18-2022	Managed Computers	192.168.0.203	Ubuntu Linux 16.10 64-Bit	3.20.0-2ubuntu2	05/09/2022
VA00000000000000000000	Linux / Mac	192.168.0.207	LinuxMint Linux 19.2 32-Bit		17/10/2022

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.

Filter Criteria	Export Options
Software Name	Include
Computer Name	Include
Host Name	Include
OS Type	Include
Group By	
<input checked="" type="radio"/> Software Name	
<input type="radio"/> Computer Name	
Search Reset	
(*) 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).

Host Name

Enter the Host Name displays suggestions. Select the appropriate key.

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.

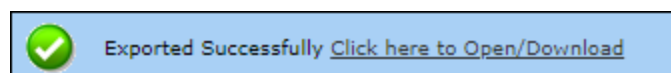
Filter Criteria	Export Option
Export Option	
<input type="radio"/> Excel <input type="radio"/> PDF <input checked="" type="radio"/> HTML	
Export Export Detailed Report	

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



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
YGPAE-GDND-3N33-FR3D-3R3V	Windows 7 Home Basic Edition 32-bit	1
NG3WV-3N3C-3R3W-3R3E-3R34	Windows 8 Professional 32-bit	1
GC3E3-3N3W3-FR3E3-GDND3-3R39	Windows 8.1 Professional 64-bit	1
VC3R3-3R3E3-3R3W3-3R3E3-3R3M	Windows XP Professional x64 Edition 64-bit	1

The log displays License Key, Software Name and Computer Count.

To see more details of the computer's license key installed, click the numerical value in License Key or Computer Count Column.

Filtering Software License Report

To filter Software Report, click **Filter Criteria** field.

Filter Criteria field expands.

Filter Criteria	Export Options
Software License Key	* <input type="text"/> Include
Software Name	* <input type="text"/> Include
Computer Name	* <input type="text"/> Include
Host Name	* <input type="text"/> Include
IP Address	* <input type="text"/> Include
OS Type	* <input type="text"/> Include

Search Reset (*) View All Items

Software License Key

Entering the license key displays suggestions. Select the appropriate key.

Software Name

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

Computer Name

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

Host Name

Enter the Host Name displays suggestions. Select the appropriate key.

IP Address

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

OS Type

Enter the OS type.

Include/Exclude

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

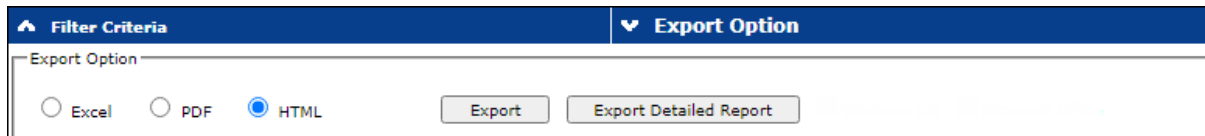
After entering data in all fields, click **Search**.

The Software License Report will be filtered according to your preferences.

Exporting Software License Report

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

Export Option field expands.



The screenshot shows a dropdown menu titled "Export Option" with three radio button options: "Excel", "PDF", and "HTML". The "HTML" option is selected. Below the options are two buttons: "Export" and "Export Detailed Report".

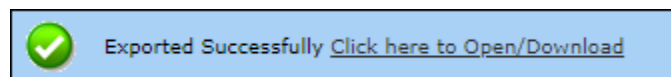
Select whether you want report for Windows OS and Microsoft Office.

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

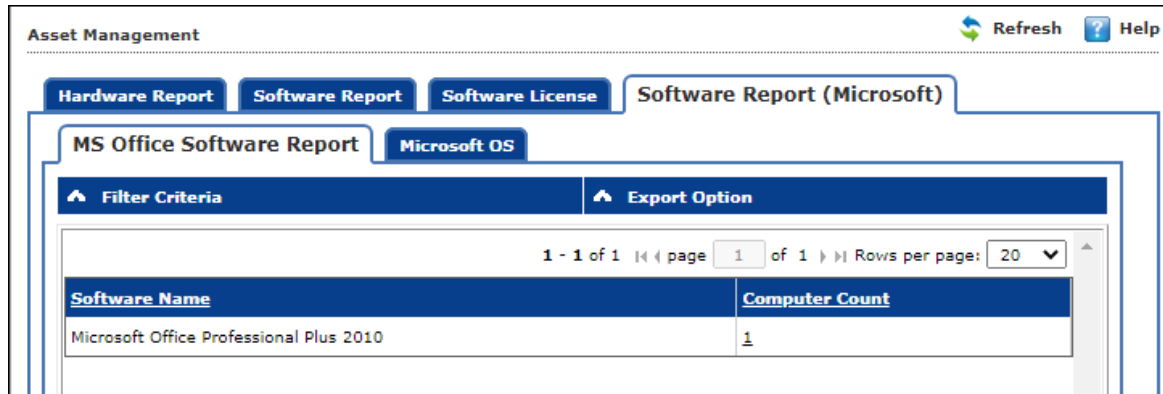
A success message appears.



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.



The tab consists following subtabs:

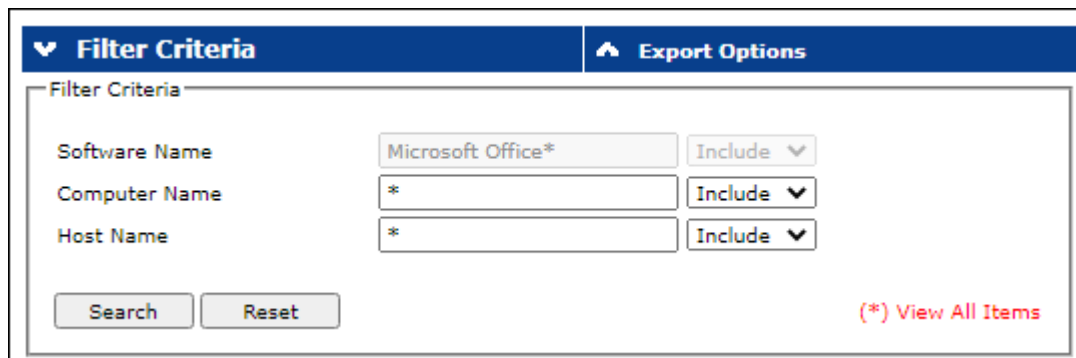
MS Office Software Report – It displays Microsoft software name and computer count.

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

Enter the preferred software name and click the drop – down.

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				
<input type="radio"/> Excel	<input type="radio"/> PDF	<input checked="" type="radio"/> HTML	<input type="button" value="Export"/>	<input type="button" value="Export Detailed Report"/>

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.
A success message appears.



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 Options
Filter Criteria	
Operating System	* <input type="text"/> Include ▼
Computer Name	* <input type="text"/> Include ▼
Host Name	* <input type="text"/> Include ▼
Service Pack	* <input type="text"/> Include ▼
OS Version	* <input type="text"/> Include ▼
<input type="button" value="Search"/> <input type="button" value="Reset"/>	
(*) 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).

Host Name

Enter the Host Name displays suggestions. Select the appropriate key.

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.



Click the link to open/download the file.

User Activity

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

- **Print Activity**
- **Session Activity Report**
- **File Activity Report**
- **Application Access Report**

Print Activity

The Print Activity 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 of Print Date, Machine Name, IP Address, Username, Printer Name, Document Name along with number of Copies and Pages.

Printer Name	Copies	Pages
NFIBBNC2B (HP LaserJet 430 WRM14)	5	5

Viewing Print Activity Log

To view the Print log of a Printer, click its numerical value under **Copies** or **Pages** column. Print Activity window appears displaying the details.

Client Date	Machine Name	IP Address	User name	Printer Name	Document Name	Copies
05/08/21 4:23:03 PM	Q#-E2R#	192.168.0.117	Q#-E2R#Administrator	NFIBBNC2B (HP LaserJet 430 WRM14)	Untitled - Notepad	1
05/08/21 4:22:40 PM	Q#-E2R#	192.168.0.117	Q#-E2R#Administrator	NFIBBNC2B (HP LaserJet 430 WRM14)	Untitled - Notepad	1
05/08/21 4:22:09 PM	Q#-E2R#	192.168.0.117	Q#-E2R#Administrator	NFIBBNC2B (HP LaserJet 430 WRM14)	Untitled - Notepad	1
05/08/21 4:21:42 PM	Q#-E2R#	192.168.0.117	Q#-E2R#Administrator	NFIBBNC2B (HP LaserJet 430 WRM14)	Untitled - Notepad	1
05/08/21 4:21:31 PM	Q#-E2R#	192.168.0.117	Q#-E2R#Administrator	NFIBBNC2B (HP LaserJet 430 WRM14)	Untitled - Notepad	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.

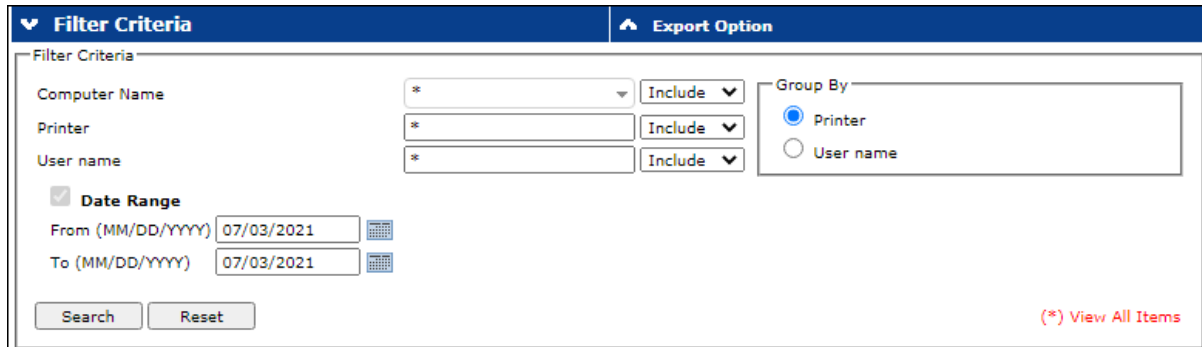
 Exported Successfully [Click here to Open/Download](#)

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.



The screenshot shows a web interface with two main sections: "Filter Criteria" and "Export Option".

- Filter Criteria:**
 - Computer Name: * (dropdown) Include (dropdown)
 - Printer: * (text input) Include (dropdown)
 - User name: * (text input) Include (dropdown)
 - Date Range**
 - From (MM/DD/YYYY): 07/03/2021
 - To (MM/DD/YYYY): 07/03/2021
 - Buttons: Search, Reset
- Export Option:**
 - Group By:
 - Printer
 - User name
 - Link: (*) View All Items

Computer Name

Click the drop-down and select the preferred computer.

Printer

Enter the printer's name.

User Name

Enter the User's name.

Include/Exclude

Selecting Include/Exclude for a Machine or Printer lets you include or exclude it from the log.

Date Range

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

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

The Print activity log will be filtered and generated according to your preferences.

Group By

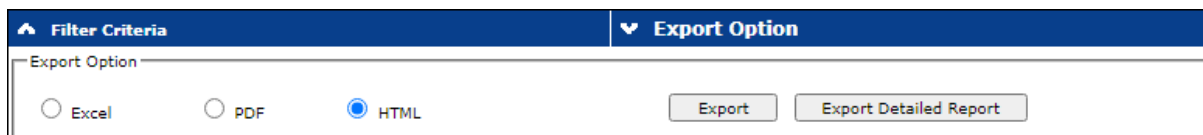
To view results by specific printer, select **Printer**, Date Range and then click **Search**.

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.

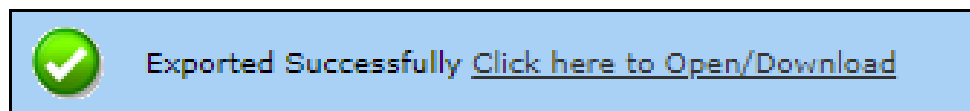


Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



Click the link to open/download the file.

Session Activity Report

This submodule monitors and logs the session activity of the managed computers. It displays a report of the Operation type, Client Date, Computer name/IP, Group, IP address and 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.

Session Activity Report					
Filter Criteria			Export Option		
Operation Type	Client Date	Computer Name /Ip	Group	IP Address	Description
Session LogOn	03/07/21 12:50:17 PM	WI\W-QAD07	QA_TEAM	192.168.0.85	User LogOn User's name: WI\W-QAD07\pax
Session LogOff	03/07/21 10:55:49 AM	WI\W-QAD07	QA_TEAM	192.168.0.85	User LogOff User's name: WI\W-QAD07\pax
Remote Session Disconnect	03/07/21 10:55:48 AM	WI\W-QAD07	QA_TEAM	192.168.0.85	Remote Session Connect User's name: WI\W-QAD07\pax Name of Remote PC: WI\ESCHANDER\ER IP of Remote PC: 192.168.0.135
Remote Session Connect	03/07/21 10:55:47 AM	WI\W-QAD07	QA_TEAM	192.168.0.85	Remote Session Connect User's name: WI\W-QAD07\pax Name of Remote PC: WI\ESCHANDER\ER IP of Remote PC: 192.168.0.135
Remote Session Disconnect	03/07/21 10:55:34 AM	WI\W-QAD07	QA_TEAM	192.168.0.85	Remote Session Connect User's name: WI\W-QAD07\pax Name of Remote PC: WI\ESCHANDER\ER IP of Remote PC: 192.168.0.135
Remote Session Connect	03/07/21 10:55:33 AM	WI\W-QAD07	QA_TEAM	192.168.0.85	Remote Session Connect User's name: WI\W-QAD07\pax Name of Remote PC: WI\ESCHANDER\ER IP of Remote PC: 192.168.0.135
Start up	03/07/21 10:43:23 AM	WI\ESCHANDER	Managed Computers	192.168.0.135	
Session LogOn	03/07/21 10:43:09 AM	WI\ESCHANDER	Managed Computers	192.168.0.135	User LogOn User's name: WI\ESCHANDER\ER\Administrator
Start up	03/07/21 10:42:13 AM	WI\W-QAD07	QA_TEAM	192.168.0.85	
Shut Down	03/07/21 10:37:44 AM	WI\ESCHANDER	Managed Computers	192.168.0.135	

Filtering Session Activity Log

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

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

Computer Name

Click the drop-down and select the preferred computers.

Operation Type

Click the drop-down and select the preferred activities.

Include/Exclude

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

IP Address

Enter the IP address in this field.

Group

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

Date Range

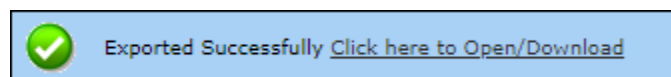
To search the log between specific dates, select **Date Range** checkbox. Afterwards, click the calendar icon and select **From** and **To** dates.

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

Exporting Session Activity Report

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

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



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.

Client Date	Computer Name/Ip	Group	IP Address	User's name	File Action Type	Drive Type	Source File	D
6/19/2021 6:11:04 PM	PRASHANT-QA	QA_TEAM	192.168.0.102	PRASHANT-QA Administrator	Copy	Fixed Drive	C:\Users\Administrator\Downloads\unconfirmed \$12948.unconfirmed	C:
6/19/2021 6:11:13 PM	PRASHANT-QA	QA_TEAM	192.168.0.102	PRASHANT-QA Administrator	Modify	Fixed Drive		C:
6/19/2021 6:11:18 PM	PRASHANT-QA	QA_TEAM	192.168.0.102	PRASHANT-QA Administrator	Delete	Fixed Drive		C:
6/21/2021 11:17:06 AM	Wjh-QA007	QA_TEAM	192.168.0.85	Wjh-QA007 user	Modify	Fixed Drive		C:
6/22/2021 11:04:10 AM	Wjh-QA007	QA_TEAM	192.168.0.85	Wjh-QA007 user	Delete	Network Drive		\\
6/22/2021 11:04:10 AM	Wjh-QA007	QA_TEAM	192.168.0.85	Wjh-QA007 user	Delete	Network Drive		\\
6/22/2021 11:04:10 AM	Wjh-QA007	QA_TEAM	192.168.0.85	Wjh-QA007 user	Delete	Network Drive		\\
6/22/2021 11:05:11 AM	Wjh-QA007	QA_TEAM	192.168.0.85	Wjh-QA007 user	Delete	Network Drive		\\
6/23/2021 11:29:58 AM	Wjh-QA007	QA_TEAM	192.168.0.85	Wjh-QA007 user	Create	Fixed Drive	NewFile	C:
6/23/2021 11:33:55 AM	Wjh-QA007	QA_TEAM	192.168.0.85	Wjh-QA007 user	Modify	Fixed Drive		C:

Filtering File Activity Log

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

Filter Criteria

Filter Criteria

Computer Name

User's name

File Action Type

Source File

Application

Date Range
 From (MM/DD/YYYY)
 To (MM/DD/YYYY)

Enable search by typing keywords on above fields (Note: By enabling this option page loading can get delayed)

Export Option

IP Address

Group

Drive Type

Destination File

(*) View All Items

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

Computer Name

Click the drop-down and select the preferred computers.

Username

Enter the username of the computer.

File Action type

Click the drop-down and select a preferred file action.

Source File

Enter the source file's name.

Application

Enter an application's name.


Include/Exclude

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

IP Address

Enter an IP address.

Group

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

Drive Type

Click the drop-down and select the drive type.

Destination File

Enter the file path.

Date Range

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

Enable search by typing keywords on above fields

Select this checkbox to filter the report as per keyword for particular field.

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

The Activity Log will be displayed.

Exporting File activity Report

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

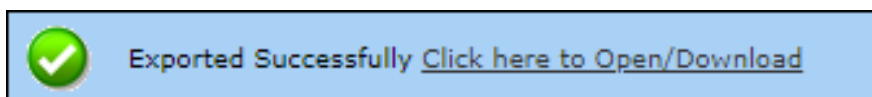
Export Option field expands.



The screenshot shows a user interface for selecting an export format. It features a blue header with 'Filter Criteria' and 'Export Option'. Below the header, there is a section titled 'Export Option' containing three radio buttons: 'Excel', 'PDF', and 'HTML'. The 'HTML' radio button is selected. To the right of the radio buttons is an 'Export' button.

Select the preferred option and then click **Export**.

A success message appears.



Click the link to open/download the file.

Application Access Report

The Application Access Report module gives the detailed view of all the applications accessed by the computers in the Managed Computers.

Viewing Application Access Report

In the navigation panel, click **User Activity > Application Access Report**.

The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

Application Name	Total Duration (DD:HH:MM:SS)
Dropbox	00:00:06:10
Google Chrome	00:04:04:12
Internet Explorer	00:04:20:22
Notepad	00:00:00:23
Qt Qtwebengineprocess	00:00:03:47
Remote Desktop Connection	00:00:00:44
Secunia PSI Tray	00:02:22:45
Windows Command Processor	00:00:21:22
WordWeb	00:02:30:56

By clicking on the duration present under **Total Duration (DD:HH:MM:SS)** column, you will get the details of the computer name accessed the app and duration.

Computer Name	Total Duration (DD:HH:MM:SS)
WI-E5CANSERVE R	00:13:50:41

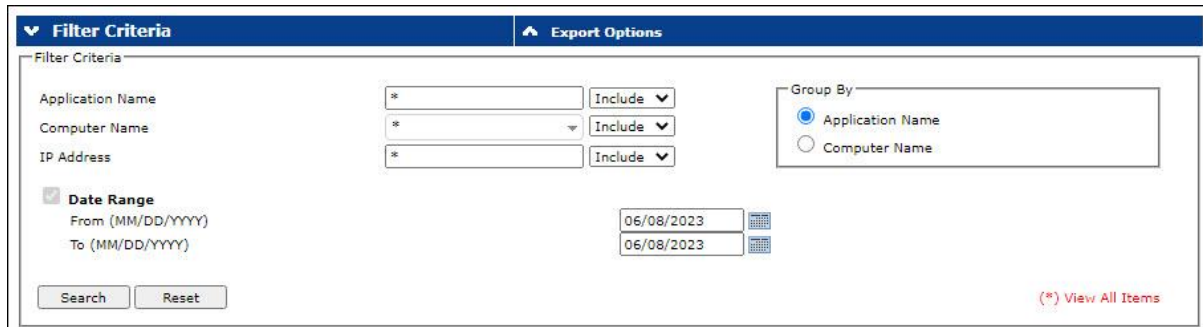
Again, if you click on the duration, you will get detailed view of the app accessed by the computer along with the date, time, and application path.

Application Name	Start Time	End Time	Total Duration (DD:HH:MM:SS)	Application Path
AruDesk.exe	09/07/21 11:51:05 AM	09/07/21 12:05:14 PM	00:00:14:08	C:\Program Files\AruDesk\AruDesk.exe

You can export this report in PDF, CSV, and HTML format.

Filtering Application Access Report

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



The screenshot shows a web interface with two main sections: "Filter Criteria" and "Export Options".

- Filter Criteria:**
 - Application Name: * [text input] [Include ▼]
 - Computer Name: * [dropdown] [Include ▼]
 - IP Address: * [text input] [Include ▼]
 - Date Range**
 - From (MM/DD/YYYY): 06/08/2023 [calendar icon]
 - To (MM/DD/YYYY): 06/08/2023 [calendar icon]
- Group By:**
 - Application Name
 - Computer Name

Buttons: Search, Reset, (*) View All Items

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

Application Name

Entering the Application name displays suggestions. Select the appropriate application.

Computer Name

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

IP Address

Click the drop-down and select the preferred IP Address.

Group By

The results can be grouped by Application name or Computer name.

Date Range

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

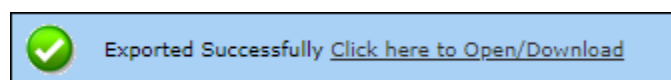
After entering data in all fields, click **Search**. The Application Access Report will be filtered according to your preferences.

Exporting Application Access Report

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

Select the preferred option and then click **Export**.

A success message appears.



Click the link to open/download the file.

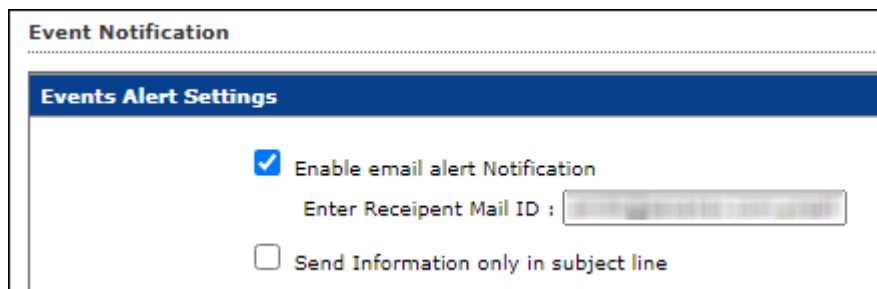
Notifications

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.



The screenshot shows a web interface for configuring event notifications. It has a title bar 'Event Notification' and a sub-header 'Events Alert Settings'. There are two main settings: a checked checkbox for 'Enable email alert Notification' with a text input field for 'Enter Receipt Mail ID' below it, and an unchecked checkbox for 'Send Information only in subject line'.

To enable the event alert:

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

Enable email alert Notification

Enter Receipt Mail ID :

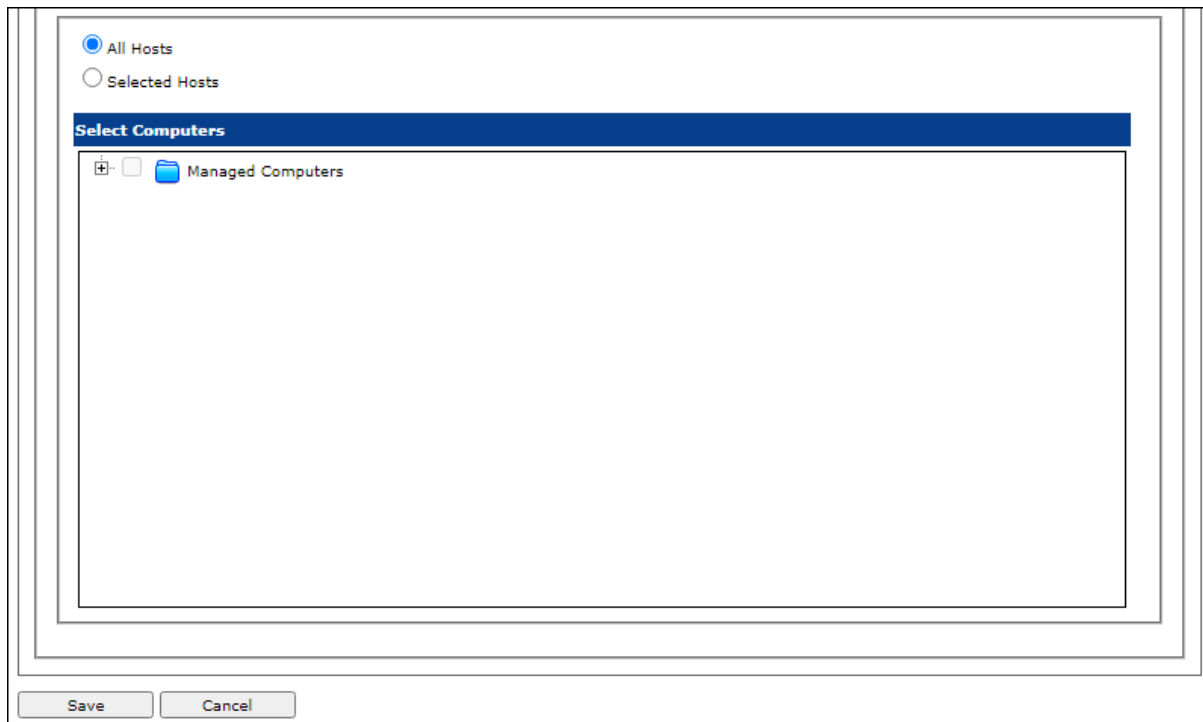
Send Information only in subject line

Select Event Ids

Select activities for which email alert is required

<input type="checkbox"/>	Event Id	Description
<input type="checkbox"/>	140	CONSCTL_USBONTERMCLNTS_ALLOWED
<input type="checkbox"/>	220	CONSCTL_USB_TETHERING_ALLOWED
<input type="checkbox"/>	221	CONSCTL_USB_TETHERING_BLOCKED
<input type="checkbox"/>	222	CONSCTL_BLUETOOTHFT_ALLOWED
<input type="checkbox"/>	223	CONSCTL_BLUETOOTHFT_BLOCKED
<input type="checkbox"/>	141	CONSCTL_COMPOSITEUSB_BLOCKED
<input type="checkbox"/>	142	CONSCTL_IMAGINGDEVICE_BLOCKED
<input type="checkbox"/>	143	CONSCTL_USBMODEM_BLOCKED
<input type="checkbox"/>	144	CONSCTL_USBONTERMCLNTS_BLOCKED
<input type="checkbox"/>	145	CONSCTL_WPD_ALLOWED
<input type="checkbox"/>	146	CONSCTL_WPD_BLOCKED
<input type="checkbox"/>	147	CONSCTL_PRINTER_ALLOWED
<input type="checkbox"/>	148	CONSCTL_PRINTER_BLOCKED
<input type="checkbox"/>	149	CONSCTL_PRINTER_NAME_BLOCKED
<input type="checkbox"/>	151	AVPMAPP_SERV_ERROR
<input type="checkbox"/>	152	AVPMAPP_MON_LOADED

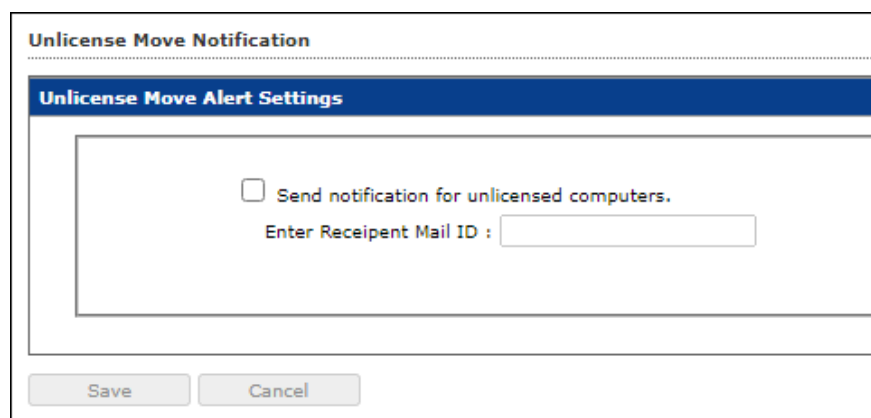
4. Select the required hosts or group.



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

Unlicensed Move Alert

This sub module lets you enable notification alert when a computer automatically moves to Unlicensed Computers category based on the setting done (under events and computers) for the computer which is not connected to the server for a long time.



To enable the unlicensed move alert:

1. In the navigation panel, click **Notifications > Unlicensed Move Alert**.
2. Select the checkbox **Send notification for unlicensed computers**.
3. After selecting the checkbox, enter the Recipients Mail ID in the textbox.
4. Click **Save**.

The Unlicensed Move Alert Settings will be saved.

Settings

The Settings module lets you to configure general settings using following submodules:

- **Web Console Settings:** This submodule lets you define settings for web console timeout, Dashboard Settings, Login Page settings, SQL Server Connection settings, SQL Database compression settings.
- **Two-Factor Authentication:** This submodule lets you to add extra layer of protection to your endpoints.
- **Excluded Clients:** This submodule lets you configure the client list to exclude it from auto isolation.

Web Console Settings

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

Web Console Settings

Web Console Timeout Setting

Enable Timeout Setting
 Automatically log out the Web Console after minutes

DashBoard Setting

Show Status for Last days (1 - 365)

Logo Settings

Logo :
The logo needs to have the size 300 x 100px, and needs to be in .png or .jpg (RGB Color) format.

Password Policy Settings

Password Age :	<input type="text" value="30"/> days (30-180 days)	0 = Password Never Expires
Password History :	<input type="text" value="3"/> (3-10 Passwords)	0 = No password history is maintained
Maximum Failed login attempts :	<input type="text" value="3"/> (3-10 times)	0 = Unlimited failed attempts allowed

Note: The above restrictions are not applicable to "Root" login.

Web Console Timeout Settings

To enable web console Timeout, select **Enable Timeout Setting** option.

After selecting the checkbox, click the drop-down and select the preferred duration.

Dashboard Setting

This setting lets you set number of days for which you wish to View the Status, Statistics and Protection Status Charts in the Dashboard. Enter the preferred number of days.

Logo Settings

This setting allows you to add the organization logo in PNG or JPEG format. So the console and reports will have the uploaded logo for customization.

To have the default eScan logo, click **Default**.

To have customized logo, click **Change**.

Password Policy Settings

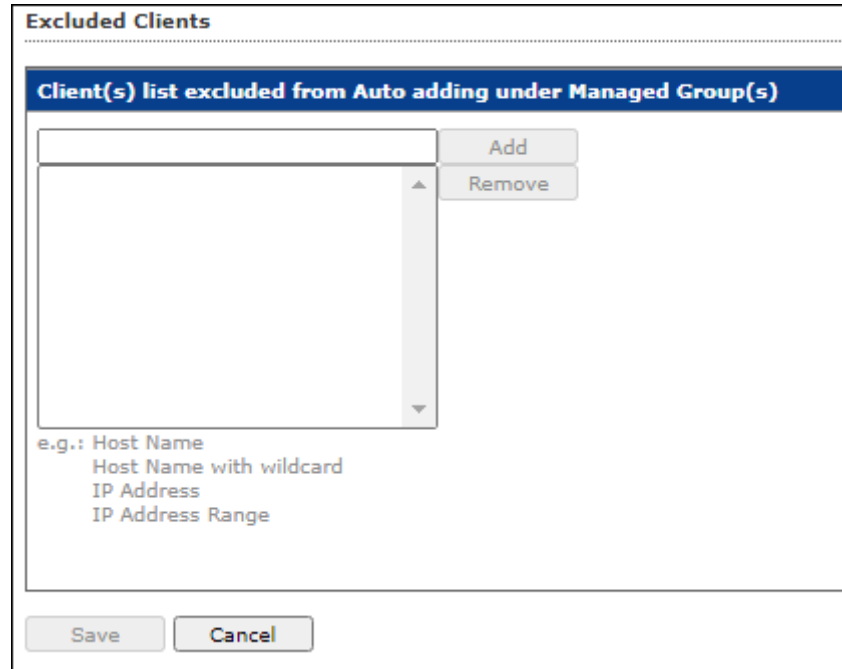
This setting allows the admin to configure the password settings for other users.

- **Password Age:** Enter the preferred value (between 30-180); this will prompt user to reset the password after specified number of days. Here, 0 indicates that password never expires.
- **Password History:** Enter the preferred value (between 3-10); this maintains the password history for specified count. Here, 0 indicates, no password history is maintained.
- **Maximum Failed login attempts:** Enter the preferred value (between 3-10); this will restrict the user from logging after specified attempts. Here, 0 indicates unlimited login attempts.

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

Excluded Clients

The Exclude Client module lets you to configure the client list to exclude it from auto isolation.



1. You can add/remove clients list to exclude it from auto isolation in the below table. To do the same, refer the following:
 - Enter the host name, IP Address, or IP address range and click **Add**.
 - To delete a particular client, select the client and click **Remove**.
2. After configuring accordingly, click **Save**. Excluded Client Settings will be saved.


Two-Factor Authentication (2FA)


The system login password is Single-Factor Authentication which is considered less secured and it may put your organization's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your eScan web console login.

The 2FA feature mandates you to enter a Time-based One-Time Password (TOTP) after entering eScan credentials. So, even if somebody knows your eScan credentials, the 2FA feature secures data against unauthorized logins. Only administrator can enable/disable the 2FA feature. It can also be enabled for added users.

To use 2FA login feature, you need to install the Authenticator app for Android devices from [Play Store](#) or for iOS devices from [App Store](#) on your smart device. The Authenticator app needs camera access for scanning a QR code. If a COD or BYOD policy restricts you from using device's camera in your organization, enter the Account Key in the Authenticator app.



 NOTE	Ensure that the smart device's date and time matches with the system's date and time or else T-OTPs generated by app won't get validated.
--	---

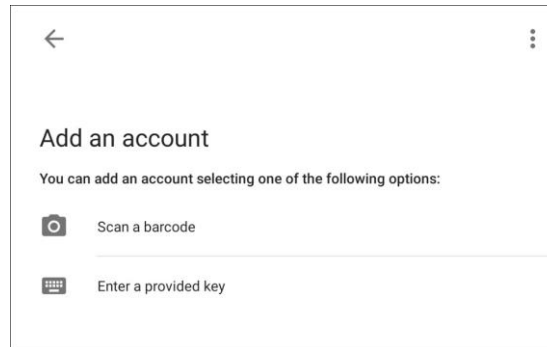
 IMPORTANT	We recommend that you save/store the Account Key in offline storage or a paperback copy, in case you lose the account access.
---	--

Enabling 2FA login

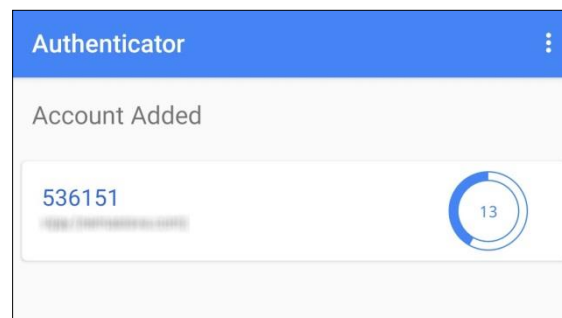
To enable 2FA login:

1. Go to **Settings > Two-Factor Authentication**.
2. Open the Authenticator app.

After basic configuration following screen appears on smart device.

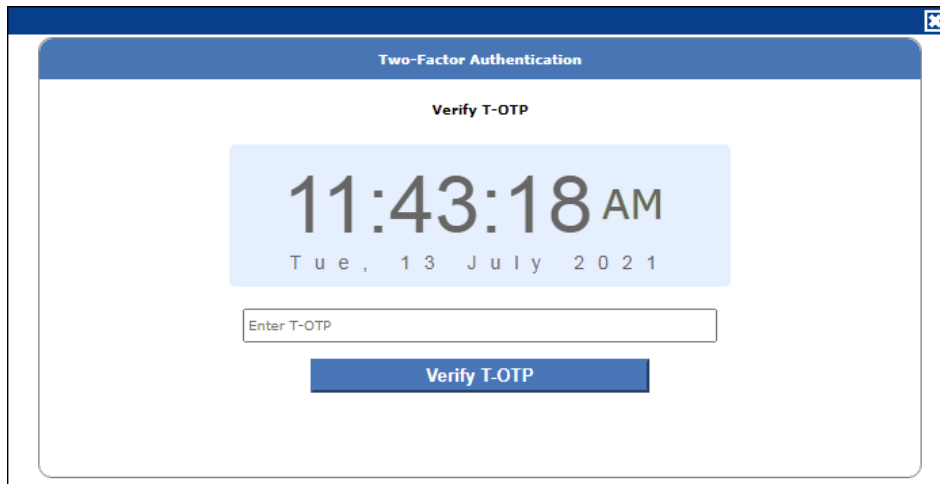


3. Select a preferred option. If you tapped **Scan a barcode**, scan the onscreen QR code via your smart device. If you tapped **Enter a provided key**, enter the Account Key and then tap **ADD**. After scanning the Account QR code or entering Account Key, the eScan server account gets added to the Authenticator app. The app then starts displaying a Time-based One-Time Password (TOTP) that is valid for 30 seconds.



4. Click **Enable Two-Factor Authentication**.

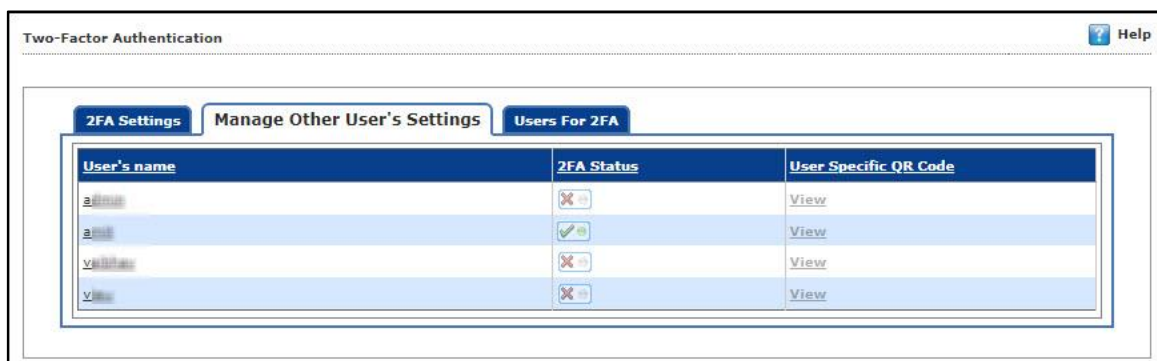
Verify T-OTP window appears.



5. Enter the TOTP displayed on smart device and then click **Verify TOTP**. The 2FA login feature gets enabled.
6. To apply the login feature for specific users, click **Manage Other User Settings** tab. The tab displays list of added users and whether 2FA status is enabled or disabled as shown below.

- 2FA Disabled

- 2FA Enabled



7. To enable 2FA login for an added user, click the button to check icon. The 2FA login for added users gets enabled. After enabling the 2FA login for users, whenever they log in to eScan web console Verify TOTP window appears.
8. To view the QR Code of specific user, click **View** option in the User Specified QR Code column.

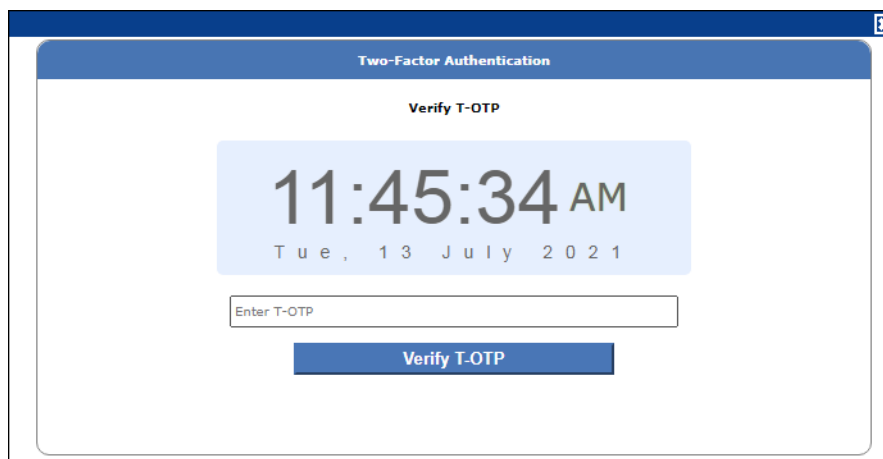
Disabling 2FA login

To disable 2FA login:

1. Go to **Settings > Two Factor Authentication**.
2. Click **Disable Two-Factor Authentication**.



Verify T-OTP window appears.



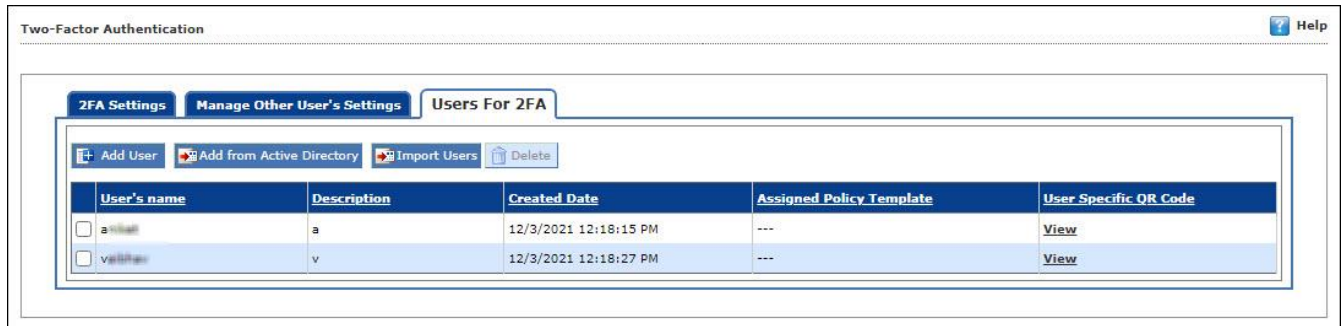
3. Enter the T-OTP and then click **Verify T-OTP**.
The 2FA feature gets disabled.

NOTE

After disabling the 2FA feature and enabling it again, the 2FA login status will be reinstated for added users.

Users For 2FA

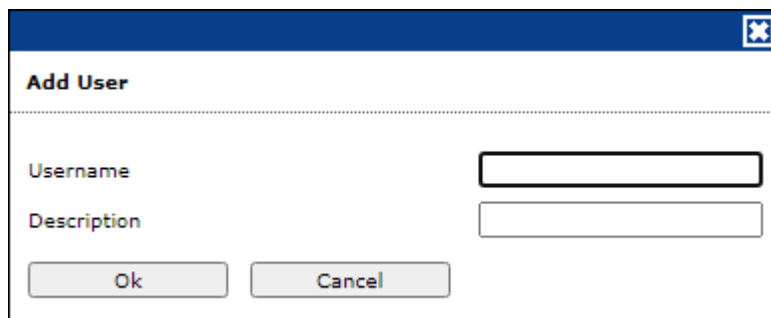
This tab helps to add the users and apply 2FA to the endpoints via policy template. The users can be added directly or from Active Directory.



Method 1: Adding user

To add users for the same, follow the below steps:

1. Go to **Settings > Two-Factor Authentication > Users For 2FA**.
2. Click **Add User**.
Add User window appears.



The 'Add User' dialog box is shown with two input fields: 'Username' and 'Description'. Below the fields are 'Ok' and 'Cancel' buttons.

3. Enter the **Username** and **Description**.
4. Click **OK**.

Method 2: Importing Users

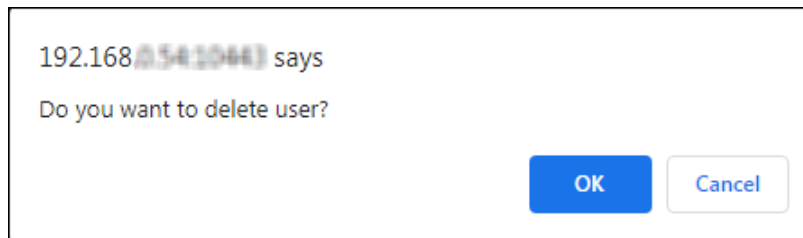
To import the users, follow the below steps:

1. Go to **Settings > Two-Factor Authentication > Users For 2FA**.
2. Click **Import Users**.
Import Users window appears.

Deleting Users

To delete the users, follow the below steps:

1. Go to **Settings > Two-Factor Authentication > Users For 2FA**.
2. Click **Delete**.
The Confirmation prompt appears.



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

Administration

The Administration module lets you create User Accounts and allocate them Admin rights for using eScan Management Console. In a large organization, installing eScan client on all computers may consume lot of time and efforts. With this option, you can allocate 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**
- **Audit Trail**

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's name	Full Name	Domain	Role	Session Log	Status
[checkbox]	[Name]		Administrator	View	[Status]
[checkbox]	[Name]		Administrator	View	[Status]
[checkbox]	[Name]		Role-A	View	[Status]

Create New Account

To create a User Account:

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

Create User

User Accounts > Create User

Account Type and Information

User's name*: [input]
 Full Name*: [input]
 Password*: [input]
 Confirm Password*: [input]
 Email Address*: [input]

For Example: user@yourcompany.com

Account Role

Role*: Administrator

Save Cancel

(*) Mandatory Fields

Password must have:

- Minimum 8 characters ✓
- Atleast 1 Lowercase letter [a-z] ✓
- Atleast 1 Uppercase letter [A-Z] ✓
- Atleast 1 digit [0-9] ✓
- Atleast 1 symbol [!@!%*#?_&] ✓
- Passwords must match. ✗

2. After filling all the details, click **Save**.
The user will be added to the User Accounts list.

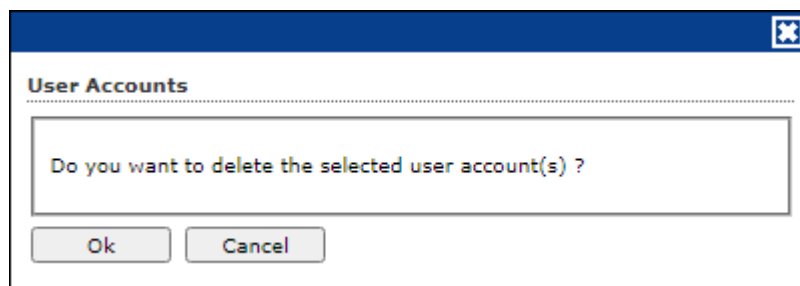
Delete a User Account

To delete a user account:

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

<input type="checkbox"/>	User's name	Full Name	Domain	Role	Session Log	Status
<input type="checkbox"/>		Administrator	View	
<input checked="" type="checkbox"/>		Administrator	View	
<input type="checkbox"/>		Role-A	View	

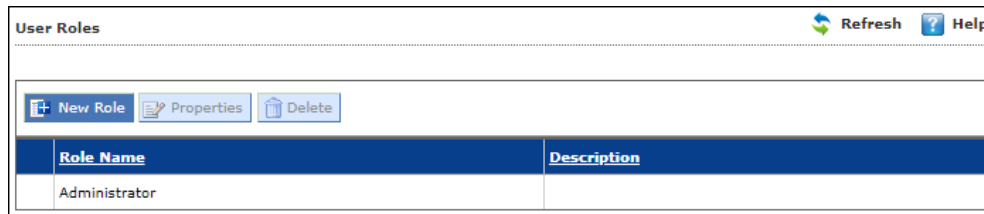
2. Click **Delete**.
A confirmation prompt appears.



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.

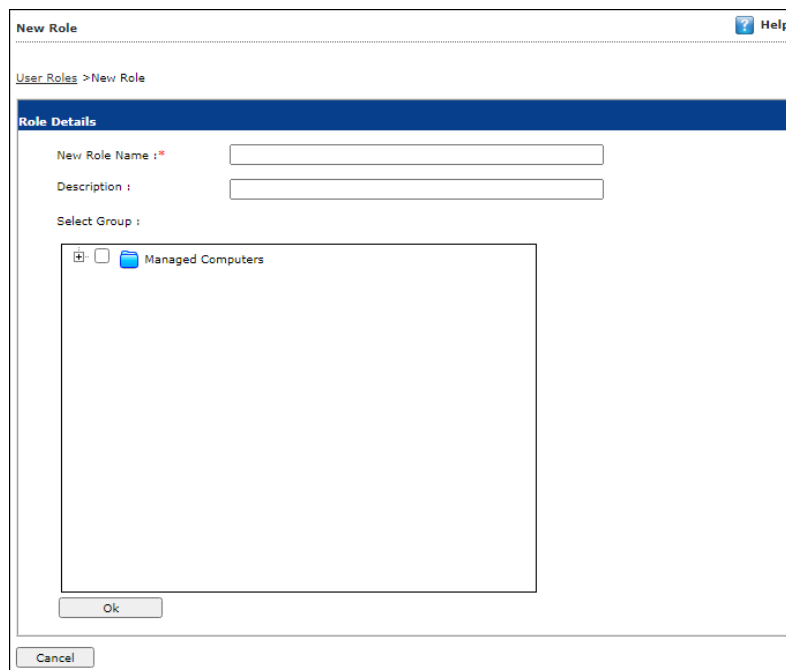


You can re-define the Properties of the created role for configuring access to various section of eScan Management Console and the networked Computers. It also lets you delete any existing role after the task is completed by them. It allows the administrator to give permission to sub administrators to 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.



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 the permissions for selected group(s) that the user is allowed to take further.

Permissions		
Main Tree Menu		
Menu	View	Configure
Dashboard	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Managed Computers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unmanaged Computers	<input type="checkbox"/>	<input type="checkbox"/>
Network Computers	<input type="checkbox"/>	<input type="checkbox"/>
IP Range	<input type="checkbox"/>	<input type="checkbox"/>
Active Directory	<input type="checkbox"/>	<input type="checkbox"/>
Report Templates	<input type="checkbox"/>	<input type="checkbox"/>
Report Scheduler	<input type="checkbox"/>	<input type="checkbox"/>
Events & Computers	<input type="checkbox"/>	<input type="checkbox"/>
System Action List	<input type="checkbox"/>	<input type="checkbox"/>
Tasks For Specific Computers	<input type="checkbox"/>	<input type="checkbox"/>
Asset Management	<input type="checkbox"/>	<input type="checkbox"/>
User Activity	<input type="checkbox"/>	<input type="checkbox"/>
Print Activity	<input type="checkbox"/>	<input type="checkbox"/>
Session Activity Report	<input type="checkbox"/>	<input type="checkbox"/>
File Activity Report	<input type="checkbox"/>	<input type="checkbox"/>
Application Access Report	<input type="checkbox"/>	<input type="checkbox"/>
Patch Report	<input type="checkbox"/>	<input type="checkbox"/>
Notifications	<input type="checkbox"/>	<input type="checkbox"/>
Outbreak Alert	<input type="checkbox"/>	<input type="checkbox"/>
Event Alert	<input type="checkbox"/>	<input type="checkbox"/>

5. Select the checkboxes that will allow the role to view/configure the module.
6. After selecting the necessary checkboxes, click **Save**.
The role will be added to the User Roles list.

View Role Properties

To view the properties of a role:

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

User Roles		Refresh	Help
<div style="display: flex; justify-content: space-between;"> + New Role Properties Delete </div>			
Role Name	Description		
Administrator			
<input checked="" type="checkbox"/> K...			

3. Click **Properties**.

Properties screen appears. It lets you modify role description, permissions for accessing and configuring modules and assign the role to other groups by clicking **Select Group Tree**.

Permissions		
Menu	View	Configure
Dashboard	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Managed Computers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unmanaged Computers	<input type="checkbox"/>	<input type="checkbox"/>
Network Computers	<input type="checkbox"/>	<input type="checkbox"/>
IP Range	<input type="checkbox"/>	<input type="checkbox"/>
Active Directory	<input type="checkbox"/>	<input type="checkbox"/>
Report Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Report Scheduler	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Events & Computers	<input type="checkbox"/>	<input type="checkbox"/>
System Action List	<input type="checkbox"/>	<input type="checkbox"/>
Tasks For Specific Computers	<input type="checkbox"/>	<input type="checkbox"/>
Asset Management	<input type="checkbox"/>	<input type="checkbox"/>
User Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Print Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Session Activity Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>
File Activity Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Application Access Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Patch Report	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Notifications	<input type="checkbox"/>	<input type="checkbox"/>

4. To modify client configuration permissions, click **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.

Permissions

Main Tree Menu Client Tree Menu

Managed Computers
Roaming Users
Linux / Mac
Samples Team

[Managed Computers/Samples_Team]

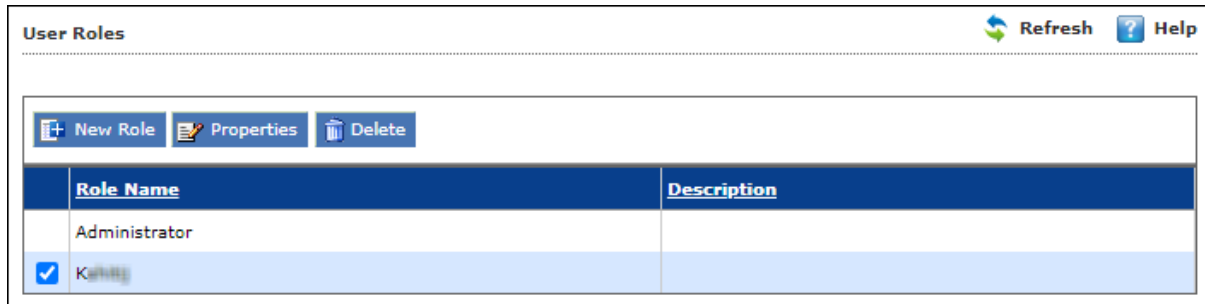
Menu	Configure
Action List	
	<input checked="" type="checkbox"/>
New Sub Group	<input type="checkbox"/>
Set Group Configuration	<input type="checkbox"/>
Deploy / Upgrade Client	<input checked="" type="checkbox"/>
Uninstall eScan Client	<input type="checkbox"/>
Remove Group	<input type="checkbox"/>
Synchronize with Active Directory	<input type="checkbox"/>
Outbreak Prevention	<input type="checkbox"/>
Create Client Setup	<input type="checkbox"/>
Properties	<input checked="" type="checkbox"/>
Client Action List	
	<input checked="" type="checkbox"/>
Set Host Configuration	<input type="checkbox"/>
Deploy / Upgrade Client	<input type="checkbox"/>
Uninstall eScan Client	<input checked="" type="checkbox"/>
Move to Group	<input type="checkbox"/>
Remove from Group	<input type="checkbox"/>
Refresh Client	<input type="checkbox"/>
Show Critical Events	<input type="checkbox"/>
Export	<input checked="" type="checkbox"/>
Show Installed Softwares	<input type="checkbox"/>

- To let the role configure these actions, under the Configure column select the checkboxes of corresponding actions.
- Click **Save**.
The Role Properties will be updated accordingly.

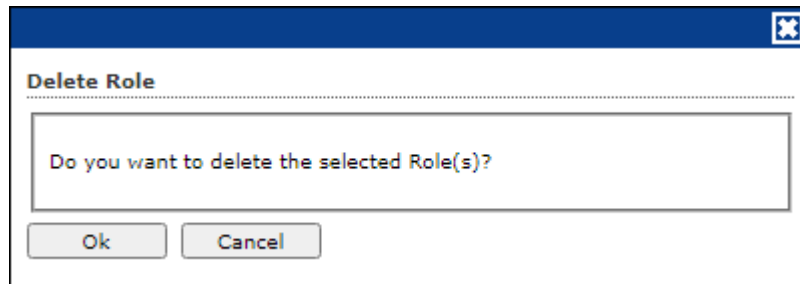
Delete a User Role

To delete a user role:

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



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



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

Audit Trail

The Audit Trail submodule lets you record the security relevant data, operation, event, Action, policy updates. Audit logs are used to track the date, time and activity of each user, including the policy/criteria that have been changed. A record of the changes that have been made to a database. You can get audit trail of user activity across all these systems.

User Name	Session Id	IP Address	Client Date	Client Time	Audit Type	Policy/Criteria Name	Module Name	Action	View Action
meat	[E510-2834379-000436]	192.168.1.101	09/09/21	12:39:56	Log Off	---	---	Console LogOut	---
meat	[DC10-2870422-000338]	192.168.1.101	09/09/21	12:39:53	Login	---	---	Console Login	---
meat	[6C1P-2844077-000335]	192.168.1.101	09/09/21	12:40:26	Login	---	---	Console Login	---
meat	[6C1P-2844077-000335]	192.168.1.101	09/09/21	12:40:47	Log Off	---	---	Console LogOut	---

Filter all Audit Trail report

To filter the Audit Trail Report as per your requirements, click **Filter Criteria** drop-down. Filter Criteria field expands.

Filter Criteria
Export Options

User Name

Audit Type

Module Name

Date Range

From (MM/DD/YYYY)

To (MM/DD/YYYY)

IP Address

Policy/Criteria Name

(*) 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

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



Click the link to open/download the file.

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 licenses and remaining licenses 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 licenses along with the names. For example, as you can see here, there are 15 add-on licenses for eBackup feature. The eBackup, 2FA, and DLP features are available through Add-On license(s).

Refresh Help

License

Register Information

License Key(30_char)	Activation Code(60_char)	Registration Status	Contract Period Ends on	No. of Users	Add On License
AKCH-8H0Q-8R0M-8L0Q-8Q0Q- AZ0B-H0R0-08	AK00UD-8R0M-8R0M-8R0R-8L0L-8R0R- 8Q0R-8R0D-8R0E-8H0F0L	Activated	05-Sep-2021	10	EBackup+ RMM+ DLP+ 2FA+ Anti-Theft

To Add License [Click Here](#)

License

70.0% 30.0%

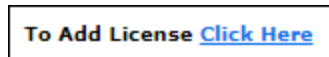
● License In Use - 3 ● Remaining License - 7

[Manage License](#)

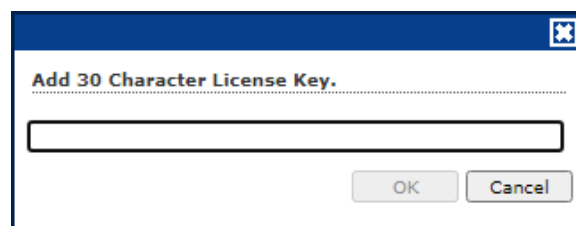
Adding and Activating a License

To add and activate a license:

1. In the License screen, click the **Click Here** link.



Add License Key dialog box appears.

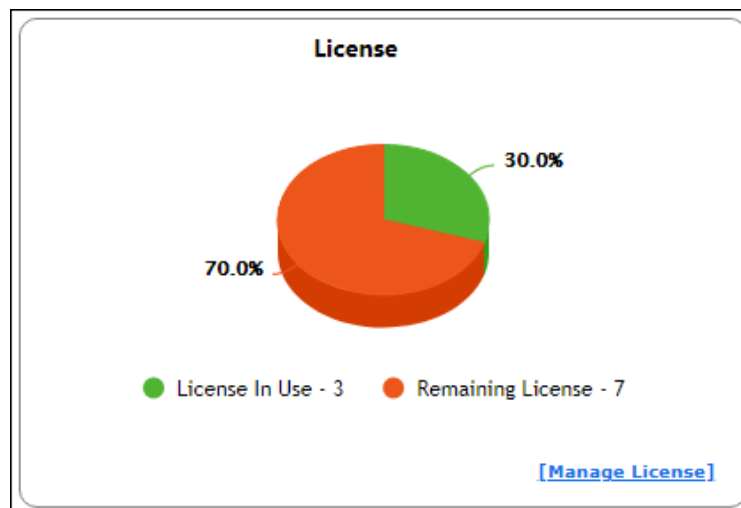


2. Enter the license key and then click **OK**.
The license key will be added and displayed in the **Register Information** table.

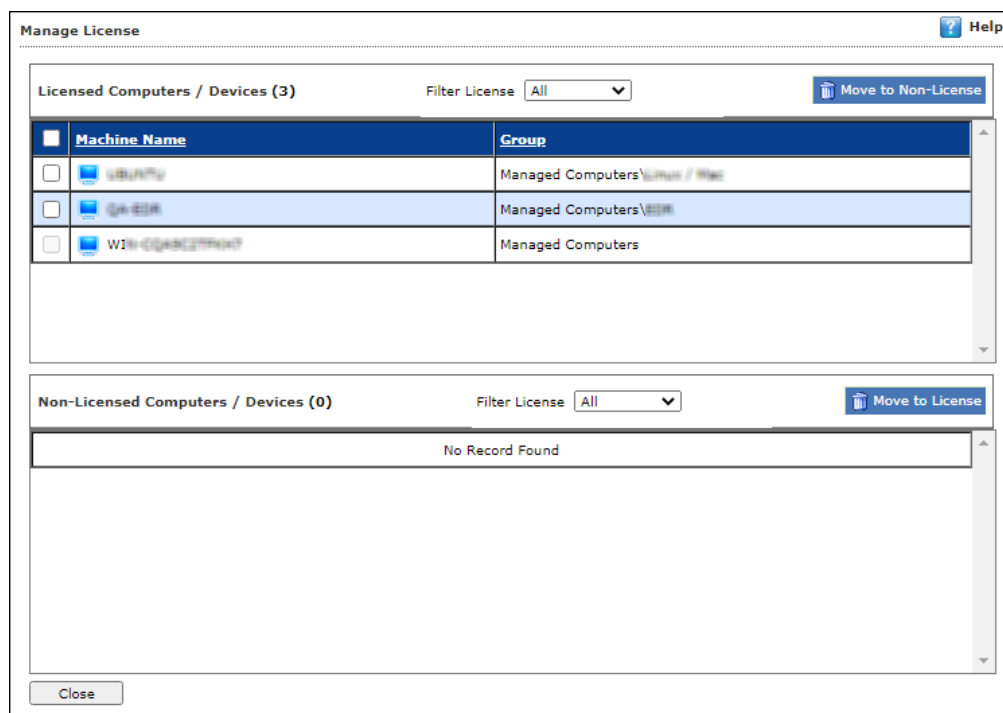
Moving Licensed Computers to Non-Licensed Computers

To move licensed computers to non-licensed computers,

1. In the License statistics box, click **Manage License**.



Manage License window appears.



2. Under the **Licensed Computers** section, select the computer(s) that you want to move to Non-Licensed Computers section.
3. Click **Move to Non-License**.
The selected computer(s) will be moved to Non-Licensed computers section.

Manage License ? Help

Licensed Computers / Devices (2) Filter License: All v Move to Non-License

	Machine Name	Group
<input type="checkbox"/>	UBUNTU	Managed Computers\ubuntu / Mac
<input type="checkbox"/>	WIN-CGKRC2THK7	Managed Computers

Non-Licensed Computers / Devices (1) Filter License: All v Move to License

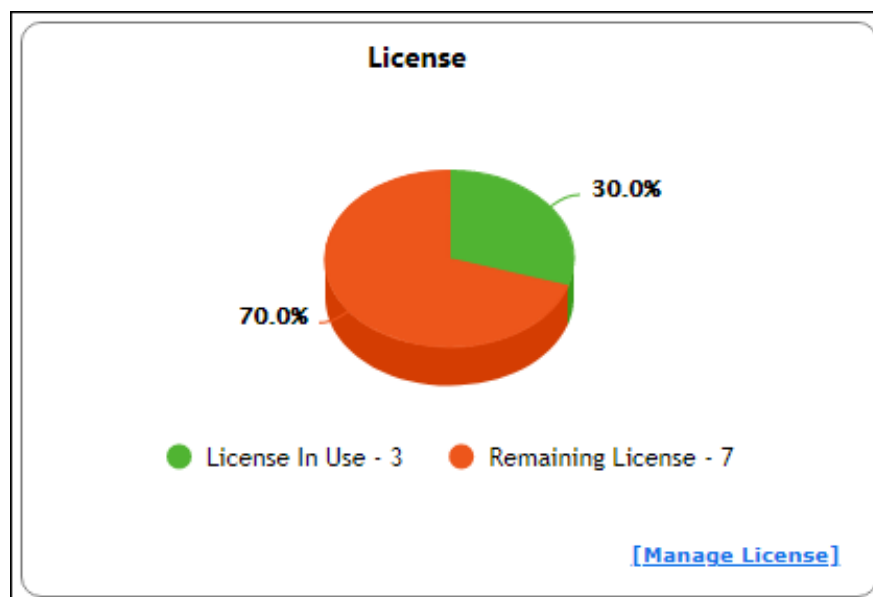
	Machine Name	Group	Unlicense Date Time	Description
<input type="checkbox"/>	QK-838	Managed Computers\QK-838	05/08/2021 16:43:00	

Close

Moving Non-Licensed Computers to Licensed Computers

To move licensed computers to non-licensed computers, follow the steps given below:

1. In the License statistics box, click **Manage License**.



Manage License window appears.

Manage License ? Help

Licensed Computers / Devices (2) Filter License All v Move to Non-License

	Machine Name	Group
<input type="checkbox"/>	UBUNTU	Managed Computers\Linux / Mac
<input type="checkbox"/>	WIN-CQANL2THX7	Managed Computers

Non-Licensed Computers / Devices (1) Filter License All v Move to License

	Machine Name	Group	Unlicense Date Time	Description
<input type="checkbox"/>	QANL2THX7	Managed Computers\QANL2THX7	05/08/2021 16:43:00	

Close

2. Under the **Non-Licensed Computers** section, select the computer(s) that you want to move to Licensed Computers section.
 3. Click **Move to License**.
- The selected computer(s) will be moved to Licensed Computers section.

Manage License ? Help

Licensed Computers / Devices (3) Filter License All v Move to Non-License

	Machine Name	Group
<input type="checkbox"/>	UBUNTU	Managed Computers\Linux / Mac
<input type="checkbox"/>	QANL2THX7	Managed Computers\QANL2THX7
<input type="checkbox"/>	WIN-CQANL2THX7	Managed Computers

Non-Licensed Computers / Devices (0) Filter License All v Move to License

No Record Found

Close

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