



Enterprise Security

**eScan Corporate Edition**  
(with Hybrid Network Support)  
**User Guide**

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

<b>Document Number:</b>	5BUG/01.06.2021/14.1
<b>Current Software Version:</b>	14.0.1400.xxxx
<b>Technical Support:</b>	<a href="mailto:support@escanav.com"><u>support@escanav.com</u></a>
<b>Sales:</b>	<a href="mailto:sales@escanav.com"><u>sales@escanav.com</u></a>
<b>Forums:</b>	<a href="http://forums.escanav.com"><u>http://forums.escanav.com</u></a>
<b>eScan Wiki:</b>	<a href="http://wiki.escanav.com/wiki/index.php/"><u>http://wiki.escanav.com/wiki/index.php/</u></a>
<b>Live Chat:</b>	<a href="http://www.escanav.com/english/livechat.asp"><u>http://www.escanav.com/english/livechat.asp</u></a>
<b>Printed by:</b>	MicroWorld Software Services Private Limited
<b>Date:</b>	June, 2021

# Content

Introduction .....	10
Pre-requisites for eScan Server .....	10
System Requirements .....	11
Installing eScan Corporate Server .....	12
Installation .....	13
Components of eScan Server .....	23
Web Console Login.....	24
Main Interface .....	28
Navigation Panel.....	29
Dashboard.....	33
Deployment Status.....	33
eScan Status .....	34
License.....	34
eScan version .....	35
Protection Status .....	37
Update Status.....	37
Scan Status .....	39
File Anti-Virus.....	40
Proactive .....	40
Mail Anti-Virus .....	41
Anti-Spam .....	41
Web Anti-Phishing .....	42
Mail Anti-Phishing .....	42
Web Protection .....	43
Firewall .....	44
Endpoint Security.....	44
Privacy .....	45
Anti – Ransomware.....	46
Protection Statistics.....	47
File Anti-Virus.....	48
Mail Anti-Virus .....	50
Anti-Spam .....	50
Web Protection .....	51
Endpoint Security-USB .....	51
Endpoint Security-Application .....	52
Summary Top 10 .....	53

Asset Changes.....	55
Live Status.....	55
Configure the Dashboard Display.....	57
Managed Computers .....	58
Search.....	59
Update Agent .....	59
Adding an Update Agent.....	60
Delete an Update Agent .....	61
Action List .....	62
Creating a Group .....	62
Removing a Group.....	64
Set Group Configuration.....	64
Managing Installations.....	65
Deploy/Upgrade Client .....	67
Refresh Client .....	70
Moving computer from one group to other .....	71
Viewing installed software (on Client computer) .....	71
Removing computers from a group.....	71
Installing eScan on Linux and MAC Computers .....	71
Manual installation of eScan Client on network computers .....	77
Installing eScan Client Using Agent.....	77
Installing other Software (Third Party Software).....	78
Uninstall eScan Client (Windows, Mac, and Linux) .....	80
Synchronize with Active Directory.....	81
Outbreak Prevention.....	82
Create Client Setup.....	85
Properties of a group .....	86
Group Tasks .....	87
Creating a Group Task .....	87
Managing a Group Task.....	90
Assigning a Policy to the group.....	91
Client Action List .....	93
Set Host Configuration.....	94
Deploy/Upgrade Client .....	95
Uninstall eScan Client.....	96
Move to Group .....	97
Remove from Group .....	97
Connect to Client (RMM).....	97

Add to RMM License.....	97
Manage Add-On License.....	98
Export .....	99
Show Installed Softwares .....	101
Force Download .....	102
On Demand Scanning .....	103
Send Message .....	104
Outbreak Prevention.....	105
Delete All Quarantine Files.....	107
Create OTP.....	107
Pause Protection.....	110
Resume Protection .....	111
Properties of Selected Computer .....	112
Policy Template.....	113
Managing Policies .....	113
Creating Policy Template for a group/specific computer .....	116
Configuring eScan Policies for Windows Computers .....	117
Configuring eScan Policies for Linux and Mac Computers.....	203
Assigning Policy Template to a group.....	222
Assigning Policy Template to Computer(s) .....	224
Copy a Policy Template.....	225
Parent Policy.....	226
Data Encryption .....	228
Policy Criteria Templates.....	235
Adding a Policy Criteria Template .....	235
Viewing Properties of a Policy Criteria template.....	241
Copying a Policy Template .....	241
Deleting a Policy Criteria template.....	242
Unmanaged Computers.....	244
Network Computers.....	244
Creating a New Group from the Select Group window .....	245
IP Range .....	246
Adding New IP Range .....	246
Moving an IP Range to a Group.....	247
Deleting an IP Range .....	247
Active Directory.....	249
Adding an Active Directory.....	249
Moving Computers from an Active Directory.....	250

New Computers Found.....	251
Filter Criteria.....	251
Action List.....	253
Report Templates.....	254
Creating a Report Template.....	255
Creating Schedule for a Report Template .....	255
Viewing Properties of a Report Template .....	256
Deleting a Report Template .....	256
Report Scheduler.....	257
Creating a Schedule .....	257
Viewing Reports on Demand .....	260
Managing Existing Schedules .....	261
Generating Task Report of a Schedule .....	261
Viewing Results of a Schedule .....	261
Viewing Properties of a Schedule.....	262
Deleting a Schedule.....	262
Events and Computers .....	263
Events Status.....	263
Computer Selection.....	264
Edit Selection.....	267
Software/Hardware Changes.....	269
Violations .....	270
Settings.....	270
Event Status Setting.....	271
Computer Selection.....	272
Software/ Hardware Changes Setting .....	275
Performing an action for computer.....	276
Tasks for Specific Computers .....	276
Creating a task for specific computers.....	276
Viewing Properties of a task .....	279
Viewing Results of a task .....	279
Deleting a task for specific computers.....	280
Asset Management .....	281
Hardware Report.....	281
Filtering Hardware Report.....	282
Exporting Hardware Report .....	283
Software Report.....	283
Filtering Software Report.....	284



Exporting Software Report.....	284
Software License.....	285
Filtering Software License Report .....	285
Exporting Software License Report.....	287
Software Report (Microsoft).....	288
Filtering Software Report (Microsoft).....	288
Exporting Software Report (Microsoft).....	289
Filtering Microsoft OS Report.....	289
Exporting Microsoft OS Report.....	290
User Activity.....	291
Print Activity .....	291
Viewing Print Activity Log.....	291
Exporting Print Activity Log .....	292
Filtering Print Activity Log .....	292
Exporting Print Activity Report.....	293
Print Activity Settings .....	294
Session Activity Report .....	295
Viewing Session Activity Log.....	295
Filtering Session Activity Log .....	295
Exporting Session Activity Report.....	296
File Activity Report.....	297
Viewing File Activity Log .....	297
Filtering File Activity Log .....	297
Exporting File activity Report .....	298
Application Access Report.....	300
Viewing Application Access Report .....	300
Filtering Application Access Report.....	301
Exporting Application Access Report.....	301
Patch Report.....	302
Patch report.....	302
Filtering Patch Report.....	302
Exporting Patch Report.....	303
All Patch Report .....	303
Filtering All Patch Report .....	305
Exporting All Patch Report .....	305
Notifications .....	306
Outbreak Alert .....	306
Event Alert .....	307

Unlicensed Move Alert.....	308
New Computer Alert .....	308
Configure SIEM .....	310
SMTP Settings.....	310
Settings .....	312
EMC Settings.....	313
Web Console Settings .....	314
Update Settings .....	317
General Config .....	317
Update Notification .....	318
Scheduling .....	319
Update Distribution.....	320
Auto-Grouping .....	322
Excluding clients from auto adding under Managed Group(s).....	323
Removing clients from the excluded list .....	323
Defining a group and client selection criteria for auto adding under managed computer(s) .....	324
Two-Factor Authentication (2FA).....	325
Enabling 2FA login .....	326
Disabling 2FA login .....	327
Administration .....	329
User Accounts .....	329
Create New Account.....	329
Delete a User Account.....	330
User Roles.....	332
New Role .....	332
View Role Properties .....	334
Delete a User Role .....	336
Export & Import.....	338
Export Settings .....	338
Import Settings.....	339
Scheduling .....	340
Customize Setup.....	342
Creating a customized setup for Windows.....	342
Creating a customized setup for Linux.....	343
Editing Setup Properties (only Windows).....	345
Deleting a Setup.....	346
License .....	347





Adding and Activating a License.....	347
Moving Licensed Computers to Non-Licensed Computers .....	348
Moving Non-Licensed Computers to Licensed Computers .....	349
Contact Us .....	351
Forums .....	351
Chat Support .....	351
Email Support.....	351

# Introduction

eScan Management Console is a web-based centralized management console that lets an administrator install and manage eScan client on the computers connected across the network. With this console, you can perform following activities:

- Install eScan client application on computers.
- Monitor the security status of computers.
- Create and manage policies or tasks for computers.
- Create and view customized reports of the security status of the computers.
- Manage notifications for alerts and warnings for computers.

## Pre-requisites for eScan Server

Before installing eScan ensure that the following pre-requisites are met:

- Access to computer as an administrator.
- Uninstall the existing anti-virus software, if any.
- Check for free space on the hard disk/partition for installing eScan.
- Static IP address for eScan server.
- IP address of the mail server to which warning messages will be sent (optional).

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

# System Requirements

Windows Server and Endpoints	Mac Endpoints	Linux Endpoints
Microsoft® Windows® 2019 / 2016 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 R2 / 2003 / 10 / 8.1 / 8 / 7 / Vista / XP SP 2 / 2000 Service Pack 4 and Rollup Pack 1 (For 32-bit and 64-bit Editions)	OS X Snow Leopard (10.6 or later) OS X Lion (10.7 or later) OS X Mountain Lion (10.8 or later) OS X Mavericks (10.9 or later) OS X Yosemite (10.10 or later) OS X El Capitan (10.11 or later) macOS Sierra (10.12 or later) macOS High Sierra (10.13 or later) macOS Mojave (10.14 or later) macOS Catalina (10.15 or later) macOS Big Sur (11.0 or later) macOS Monterey (12.0 or later)	RHEL 4 and above (32 and 64-bit) CentOS 5.10 and above (32 and 64-bit) SLES 10 SP3 and above (32 and 64-bit) Debian 4.0 and above (32 and 64-bit) openSUSE 10.1 and above (32 and 64-bit) Fedora 5.0 and above (32 and 64-bit) Ubuntu 6.06 and above (32 and 64-bit)
<b>Hardware Requirements for eScan Server</b> <b>CPU</b> - 2GHz Intel™ Core™ Duo processor or equivalent <b>Memory</b> - 4 GB and above <b>Disk Space</b> (Free) – 8 GB and above  <b>Hardware Requirements for eScan Client</b> <b>CPU</b> - 1.4 GHz minimum (2.0 GHz recommended) Intel Pentium or equivalent <b>Memory</b> - 1.0 GB and above <b>Disk Space</b> (Free) – 1 GB and above	<b>Hardware Requirements for eScan Client</b> <b>CPU</b> - Intel® Pentium or compatible or equivalent <b>Memory</b> –1 GB and above <b>Disk Space</b> – 1 GB free hard drive space for installation of the application and storage of temporary files	<b>Hardware Requirements for eScan Client</b> <b>CPU</b> - Intel based Macintosh <b>Memory</b> –1 GB and More recommended <b>Disk Space</b> – 1 GB and above

eScan Management Console can be accessed by using following browsers:

- Internet Explorer 9 and above
- Firefox 14 and above

- Google Chrome latest version

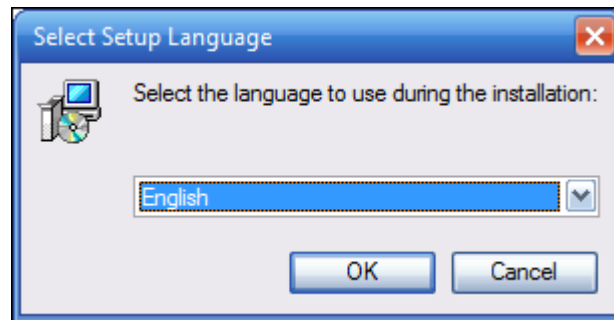
# Installing eScan Corporate Server

- **Installing eScan Corporate Server from CD/DVD**
- Installing eScan Corporate Edition (with Hybrid Network Support) from the CD/DVD is very simple, insert the CD/DVD in the ROM and wait few seconds for the Autorun to run the installation wizard. In case the installation wizard does not run automatically, locate and double-click the **cwn4k3ek.exe** on CD-ROM. This will run the installation wizard based setup of eScan Corporate Edition (with Hybrid Network Support). To complete the installation, follow the instructions on screen.
- **Downloading and installing eScan Corporate Server from internet**  
To download the setup file click [here](#). To install eScan Server from the downloaded file, double click the cwnxxxx.exe and follow the instructions on screen to complete the installation process.

# Installation

To install the eScan Corporate, follow the steps given below:

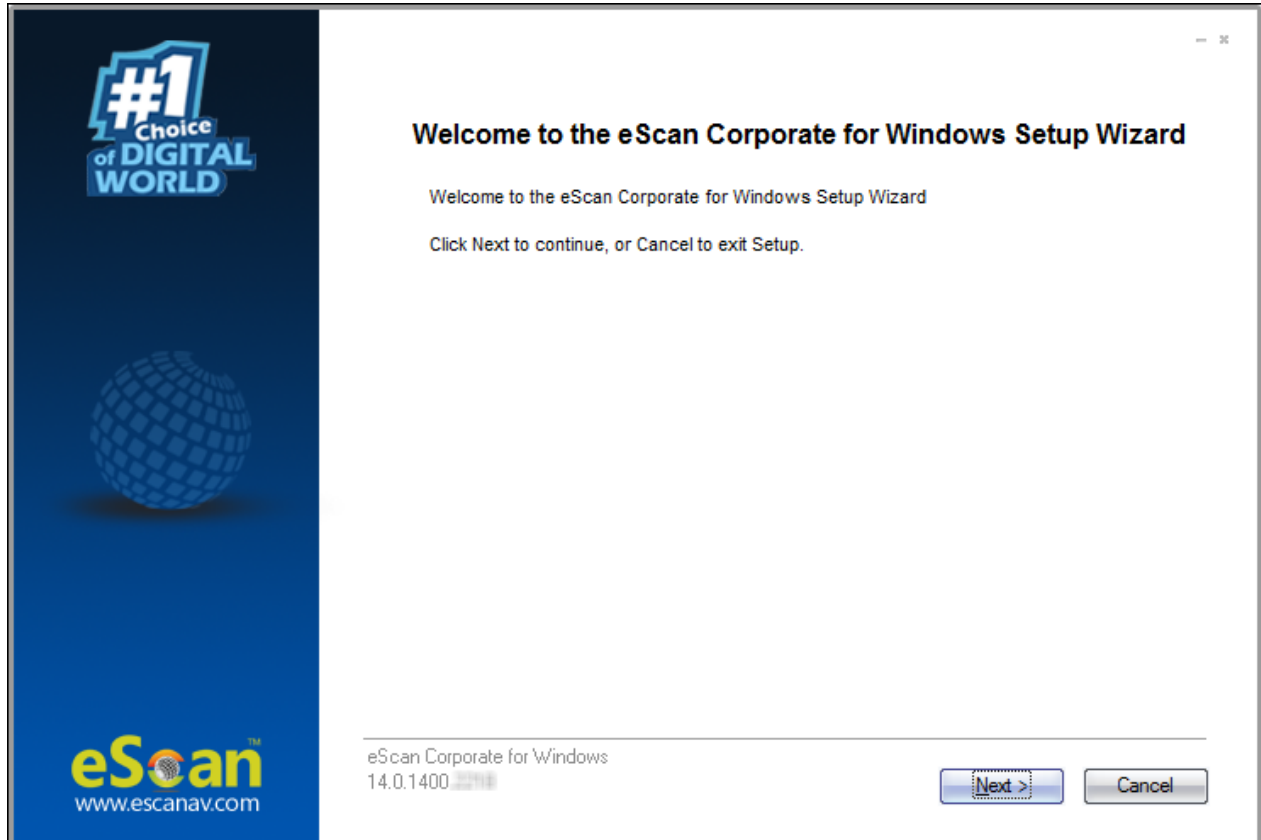
1. The installation wizard displays following window:



2. Click the drop-down and select a desired language for installation.
3. Click **OK**.

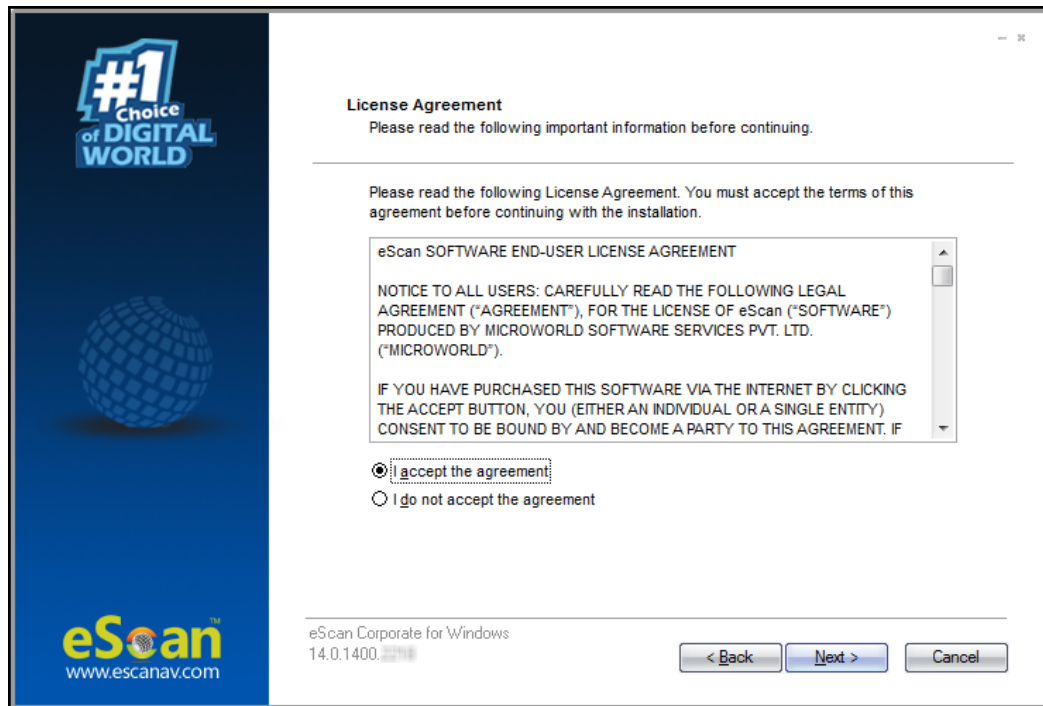
<b>Note</b>	The Default Language displayed in the drop-down menu is dependent on the Operating System's language installed on the computer.
-------------	---

The installation wizard welcomes you.

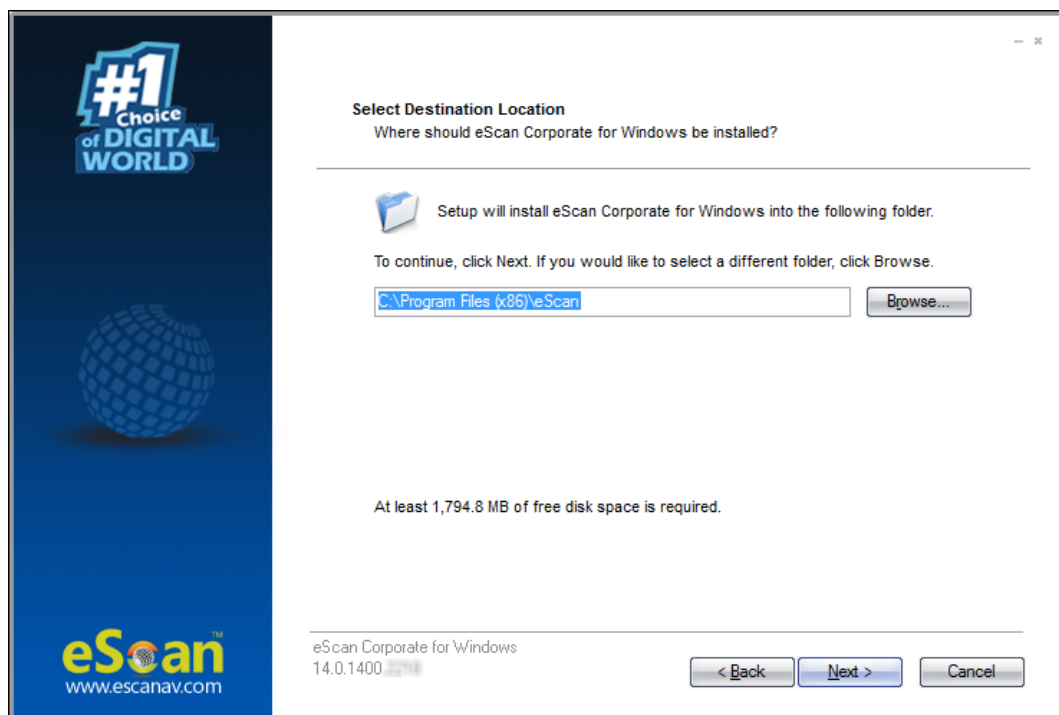


4. To proceed, click **Next**.

License Agreement screen appears.



5. Please read the License Agreement completely. To proceed with the installation, select the option **I accept the agreement** and then click **Next**.  
Select Destination Location screen appears.

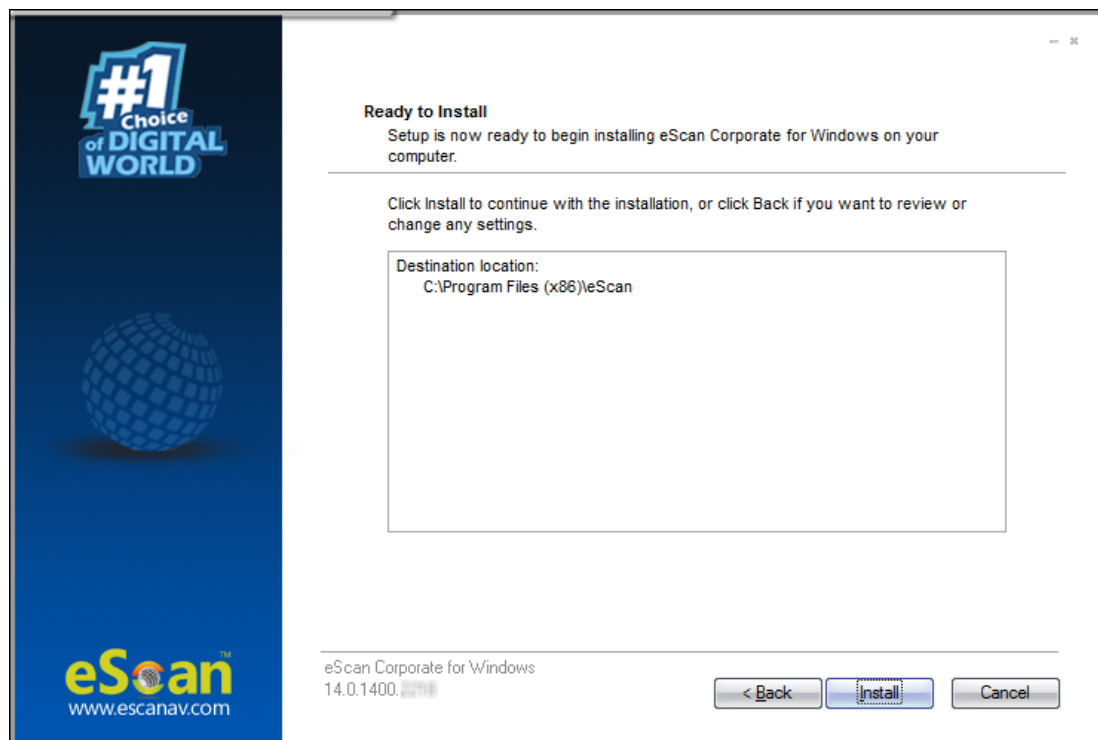


6. If you want to select a different installation location, click **Browse** and select the destination folder for installation.  
Click **Next** to proceed with the installation.

**NOTE**

Default Path for installation on a 32-bit PC – **C:\Program Files\eScan**  
Default path for installation on a 64-bit PC – **C:\Program Files (x86)\eScan**

Ready to install screen appears displaying destination location.



7. To proceed, click **Install**.  
The installation wizard initiates installation and displays the process.

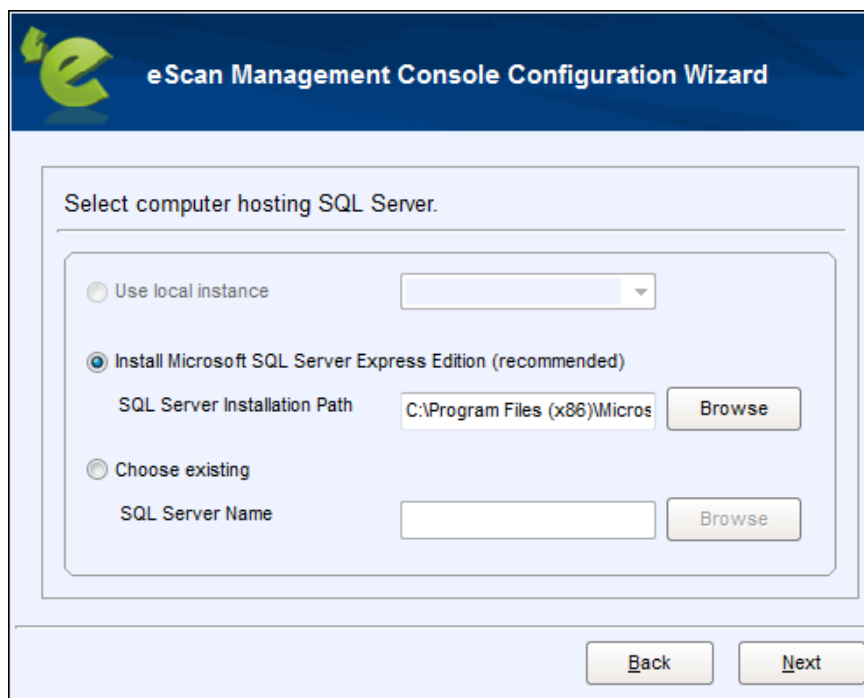




After the installation, the wizard asks you to configure the settings for SQL Server hosting and Login settings for the eScan Management console.



8. To proceed, click **Next**. The configuration wizard requests you to select a computer for hosting SQL server.



The window displays following options:

- **Use local instance**

If you already have SQL instances running locally, click the drop-down and select a desired local instance.

- **Install Microsoft SQL Server Express Edition (recommended)**

If the computer selected for eScan server installation doesn't have SQL server installed, it is recommended that you select this option. Click Browse and select an installation path for SQL server installation.

<b>NOTE</b>	Default installation path for 32-bit PC – <b>C:\Program Files\Microsoft SQL Server</b> Default installation path for 64-bit PC – <b>C:\Program Files (x86)\Microsoft SQL Server</b>
-------------	--

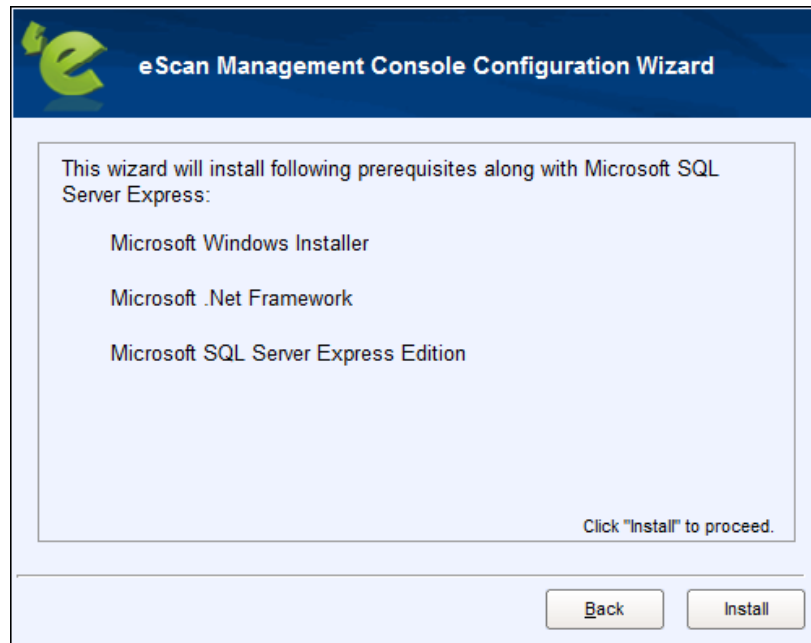
- **Choose existing**

If an SQL server hosting computer exists on your LAN, select this option. Click Browse and select the SQL server hosting computer.

Select this option if you have already created an instance for eScan Database on any SQL Server installed on any computer connected to the network. Click **Browse** to locate the server. This option is being used if you already have an instance running locally or in your local area network.

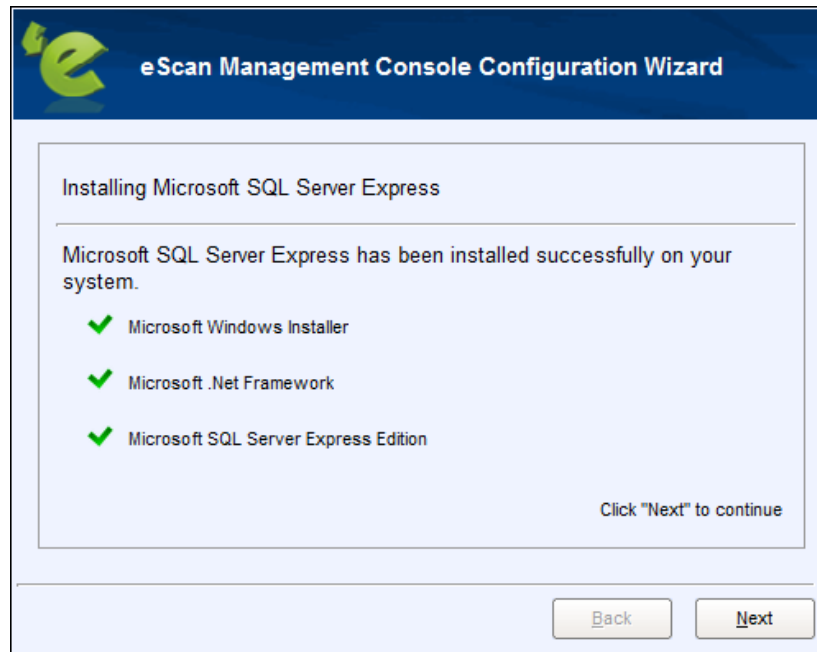
9. After selecting an option, click **Next** to proceed.

If you selected the recommended option, the configuration wizard will begin installation of the Microsoft SQL Server Express.



10. To proceed, click **Install**.

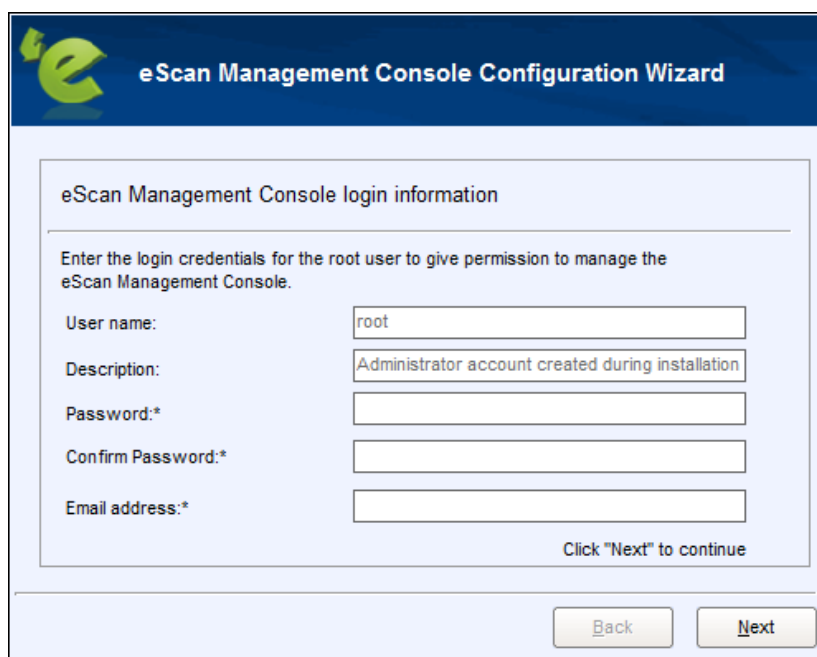
After the successful installation, the wizard displays following window.



11. To proceed, click **Next**.

The wizard requests you to enter the login credentials for the root user.

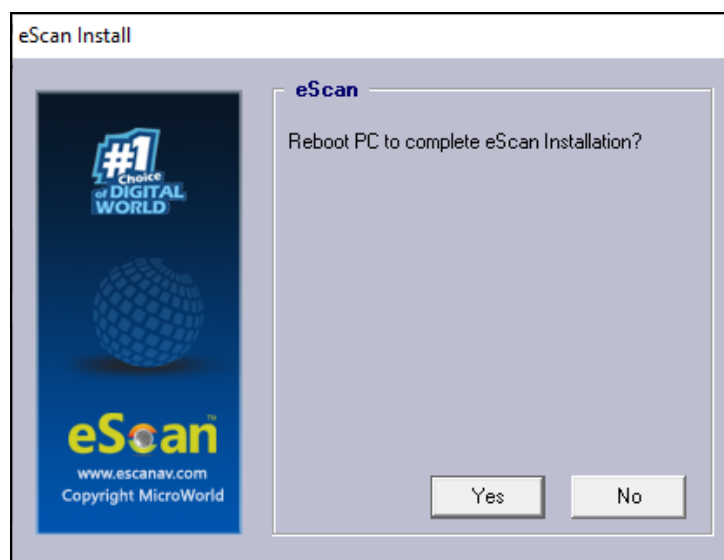
<b>NOTE</b>	The default username for web console is <b>root</b> .
-------------	---



12. After filling all the details, click **Next**. The wizard displays installation successful message.



13. To exit the installation wizard, click **Finish**.
14. Click **Finish**. The wizard asks you to restart the PC for completing the installation process.



15. To restart your PC, click **Yes**.  
After the computer restarts, launch the eScan Corporate and enter the license key for [activation](#).

<b>NOTE</b>	It is recommended that To run eScan services fully it is recommended
-------------	--



	that you restart the PC.
--	--------------------------



# Components of eScan Server

The eScan Server is comprised of following components:

- **eScan Server**  
This is the core component that lets you manage, deploy and configure eScan client on computers. It stores the configuration information and log files about the computers connected across the network. Being the core component, it communicates with the following components.
- **Agent**  
It manages the connection between the eScan server and the client computers.
- **eScan Management Console**  
It is a Web-based application hosted on the eScan Server. With this application, administrators can manage and configure eScan on computers in the network.
- **Microsoft SQL Server Express Edition**  
It is a database for storing events and logs already included in the eScan Setup file.
- **Apache**  
It is an open source, cross-platform web server software essential for running eScan Management Console. It's included in the eScan Setup file.

NOTE	For Windows 8 / 8.1 / 2008 / 2012 / 2016 / 2019 operating systems, the SQL 2008 Express edition will be installed.
	For Windows 7 and below, SQL 2005 Express edition will be installed.
	Uninstallation of eScan server won't remove SQL and APACHE from the endpoint. The user will have to uninstall these components manually.

# Web Console Login

The web console login page can be accessed via two methods.

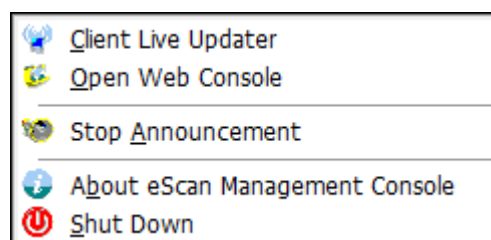
To log in to the eScan Management Console, follow the steps given below:

1. Launch a web browser.
2. Enter the following URL: <IP address of the eScan Server installed system>:10443  
Web console login page appears.

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

The second method to go to login page is as follows:

1. In the taskbar, right-click the eScan Management Console icon . A list of options appears.



2. Click **Open Web Console**.



Default browser launches and displays web console login page.

Rests of the options are explained below:

### Client Live Updater

Clicking this option displays live event feeds from all computers on your network. This feed consists of IP Address, Username of the computers, Module Names and Client actions. This Live Feed list can be exported to Excel if required.

Date	Time	Machine Na...	IP Address	User Name	Event ID	Module Name	Descri
28 May 2020	14:32:38				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:32:19				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:30:49				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:30:41				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:30:20				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:30:41				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:30:55				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:30:02				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:31:17				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:31:24				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:30:14				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:30:59				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:30:26				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:30:26				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:31:27				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:30:21				Endpoin...	[C] eScan E...	Execu
28 May 2020	14:30:34				Endpoin...	[C] eScan E...	Execu

Buttons: Export To Excel, Close

### Stop Announcement

Clicking this option stops broadcast from and towards the server.

### About eScan Management Console

Clicking this option displays Server Up Time and general information.

### Shut Down

Clicking this option shuts down the eScan Management console.

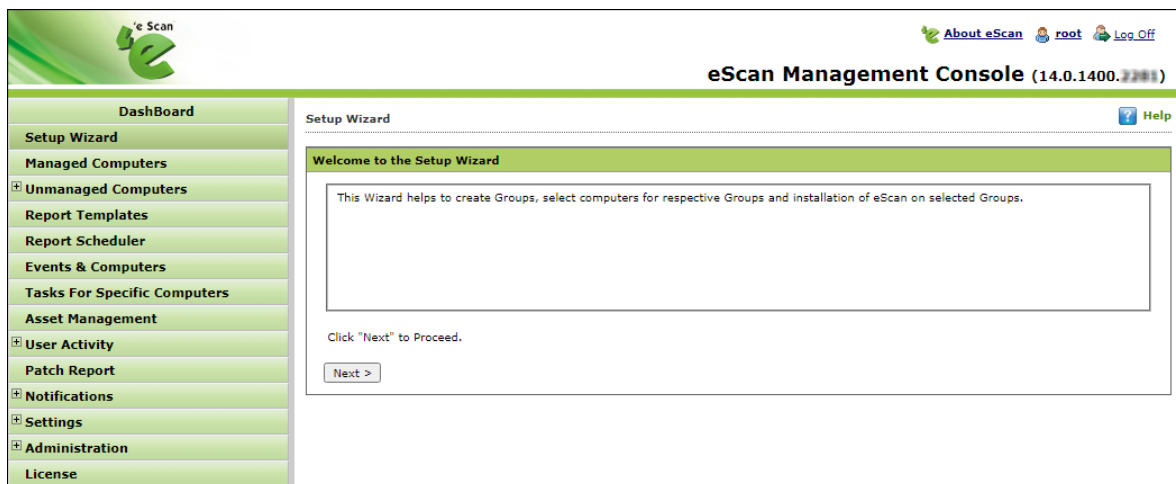
<b>NOTE</b>	<p>It is recommended that you do not shut down the server, as doing so will stop the communications between client and server.</p> <p>The "root" is the Superuser account created by eScan during Installation.</p>
-------------	---

The web console login page displays following links:

- **eScan Client Setup (Windows)**  
This link can be shared via email to the computer users where remote installation is impossible. By clicking this link users can download the eScan Client Setup and install it manually on their computers. Users can also directly access the eScan Management console from their desktop.
- **eScan Agent Setup (Windows)**  
This link can be shared via email to the computer user where you are unable to get system information or communication is breaking frequently. After the eScan Agent Setup is downloaded and installed on the Managed Computer, it establishes the connection between the server and client computers.
- **eScan Agent Setup (Linux)**  
Clicking the [+] icon displays the link for Linux Agent setup. Share this link with the Linux computer user for manual installation.
- **eScan Agent Setup (Mac)**  
Clicking the [+] icon displays the link for Mac Agent setup. Share this link with the Mac computer user for manual installation.
- **eScan AV Report**  
Clicking this link redirects you to the eScan AV Report webpage that displays Anti-Virus report for eScan installed computers. Select a group and then click **Get Details > Export**. A detailed **.xls** report will be downloaded to computer.

# Main Interface

Upon first login, console displays Setup Wizard that familiarizes you with the basic procedures. It is recommended that you follow the steps displayed, before proceeding to the other modules.



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

The links in the top right corner are explained below:

## About eScan

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

## Username

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

## Log off

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

## Date of Virus Signatures

This link displays the last date on which the Virus signatures were updated. Click it to update virus signatures.

## Navigation Panel

<b>Dashboard</b>
<b>Setup Wizard</b>
<b>Managed Computers</b>
<b>+ Unmanaged Computers</b>
<b>Report Templates</b>
<b>Report Scheduler</b>
<b>Events &amp; Computers</b>
<b>Tasks For Specific Computers</b>
<b>Asset Management</b>
<b>+ User Activity</b>
<b>Patch Report</b>
<b>+ Notifications</b>
<b>+ Settings</b>
<b>+ Administration</b>
<b>License</b>

### Dashboard

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

### Managed Computers

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

### Unmanaged Computers

The Unmanaged Computers module displays information about the computers that have not yet been assigned to any group. This section also lets you set the host configuration, move computers to a group, view the properties of a computer, or refresh the information about a client computer with Action List menu.

### Report Templates



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

### **Report Scheduler**

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

### **Events and Computers**

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

### **Tasks for Specific Computers**

The Tasks for Specific Computers module lets you create and run tasks like enable/disable protection(s) on specific computers, it also lets you schedule or modify created tasks for selected computers or groups. You can also easily re-define the settings of an already created task for a computer. It also lets you view results of the completed tasks.

### **Asset Management**

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

### **User Activity**

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

### **Patch Report**

The Patch Report module displays the number of windows security patches installed and not installed on managed computers. This will help an administrator identify the number of vulnerable systems in the network and install the critical patches quickly.

### **Notifications**



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

## Settings




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

## Administration

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

## License

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

<b>NOTE</b>	<p>Icons on every status Label denotes that the status is displayed for the computers having operating system as  <b>Windows</b>,  <b>Mac OS X</b>, or  <b>Linux</b>.</p>
-------------	--

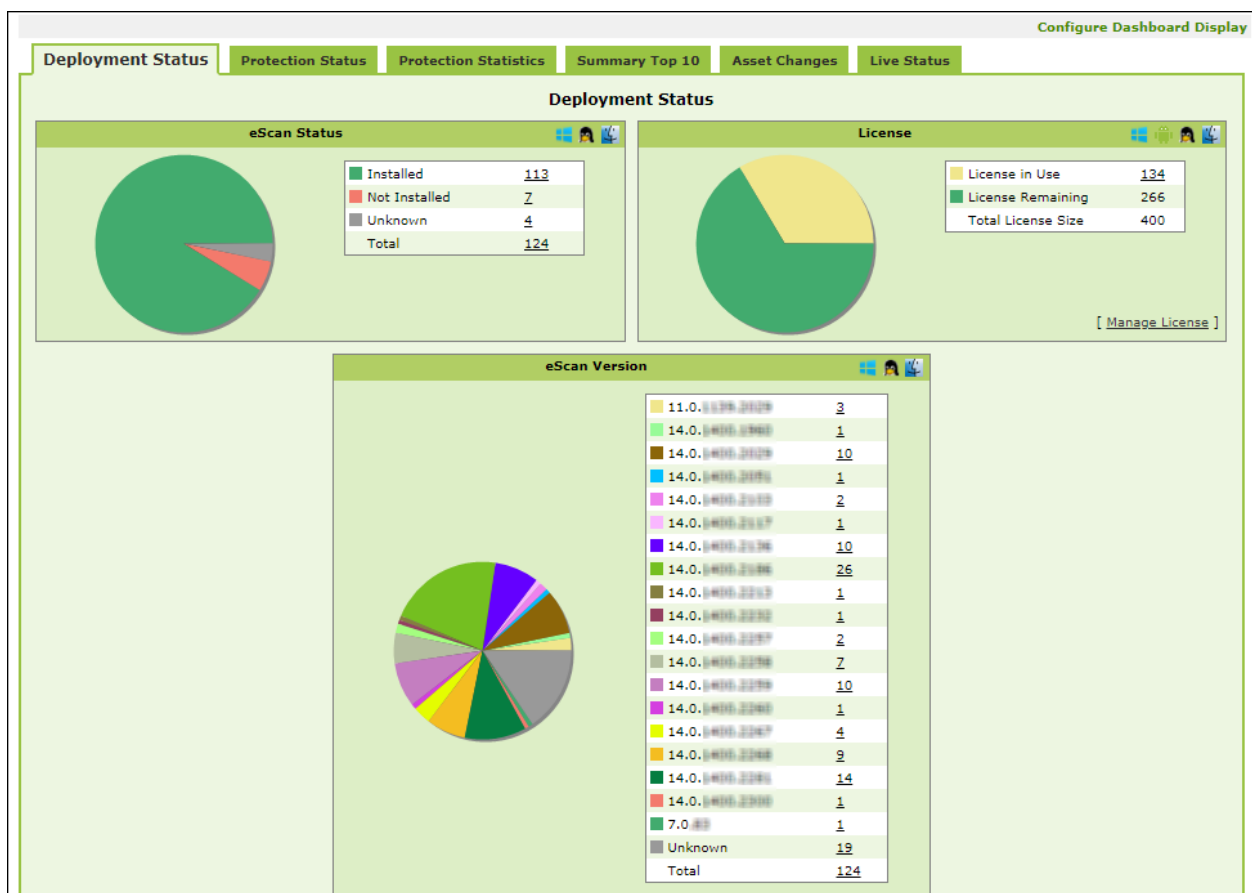
# Dashboard

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

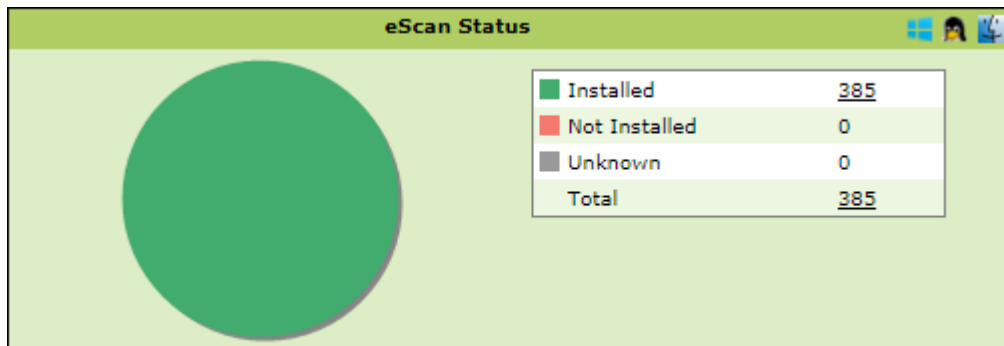
- **Deployment Status**
- **Protection Status**
- **Protection Statistics**
- **Summary Top 10**
- **Asset Changes**
- **Live Status**

## Deployment Status

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



## eScan Status



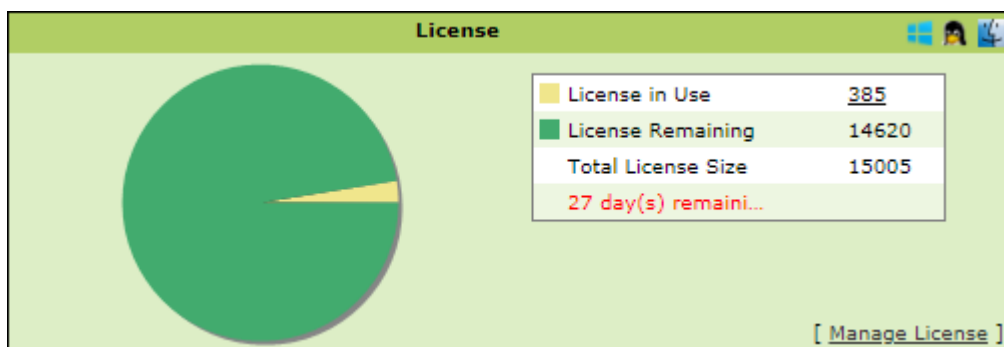
**Installed** - It displays the number of computers on which eScan Client is installed.

**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)

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

## License



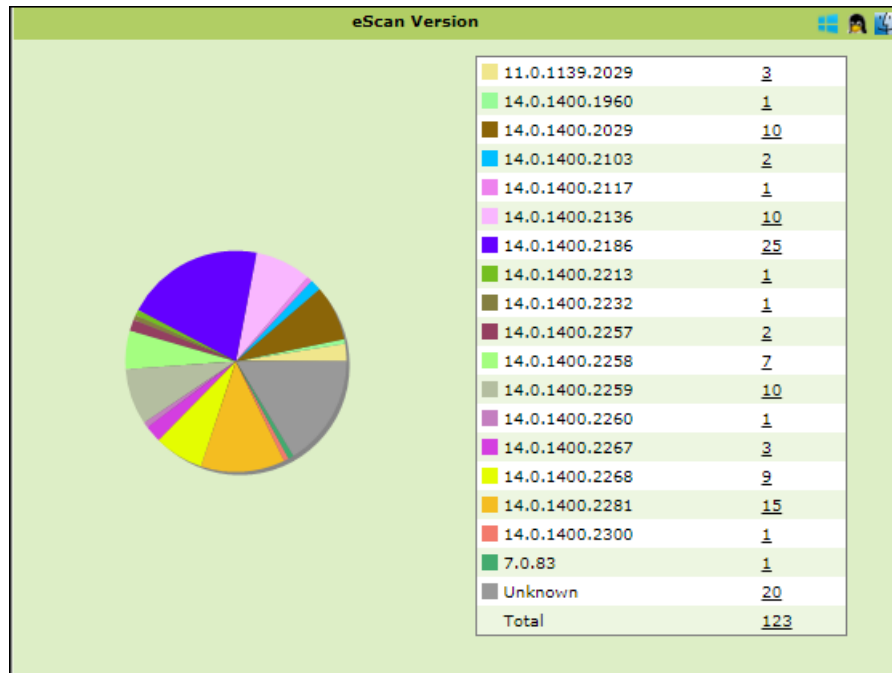
**License in Use** - It displays the number of licenses that are active.

**Licenses Remaining** - It displays the number of remaining licenses.

**Total License Size** - It displays the total number of licenses available.

## 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: All

[Print](#)

Machine Name	Version	Group
WIN-10114	14.0.1400.2258	Managed Computers\Programming\Android
WIN-10115	14.0.1400.2258	Managed Computers\Programming\Android
EU-7204	14.0.1400.2258	Managed Computers\Europe Team
EU-7205	14.0.1400.2258	Managed Computers\Europe Team
EU-7206	14.0.1400.2258	Managed Computers\Europe Team
EU-7207	14.0.1400.2258	Managed Computers\Europe Team
EU-7208	14.0.1400.2258	Managed Computers\Europe Team
US-7082	14.0.1400.2258	Managed Computers\US Team
US-7083	14.0.1400.2258	Managed Computers\US Team

Close

**Note** Clicking underlined numerical displays detailed information for computers.

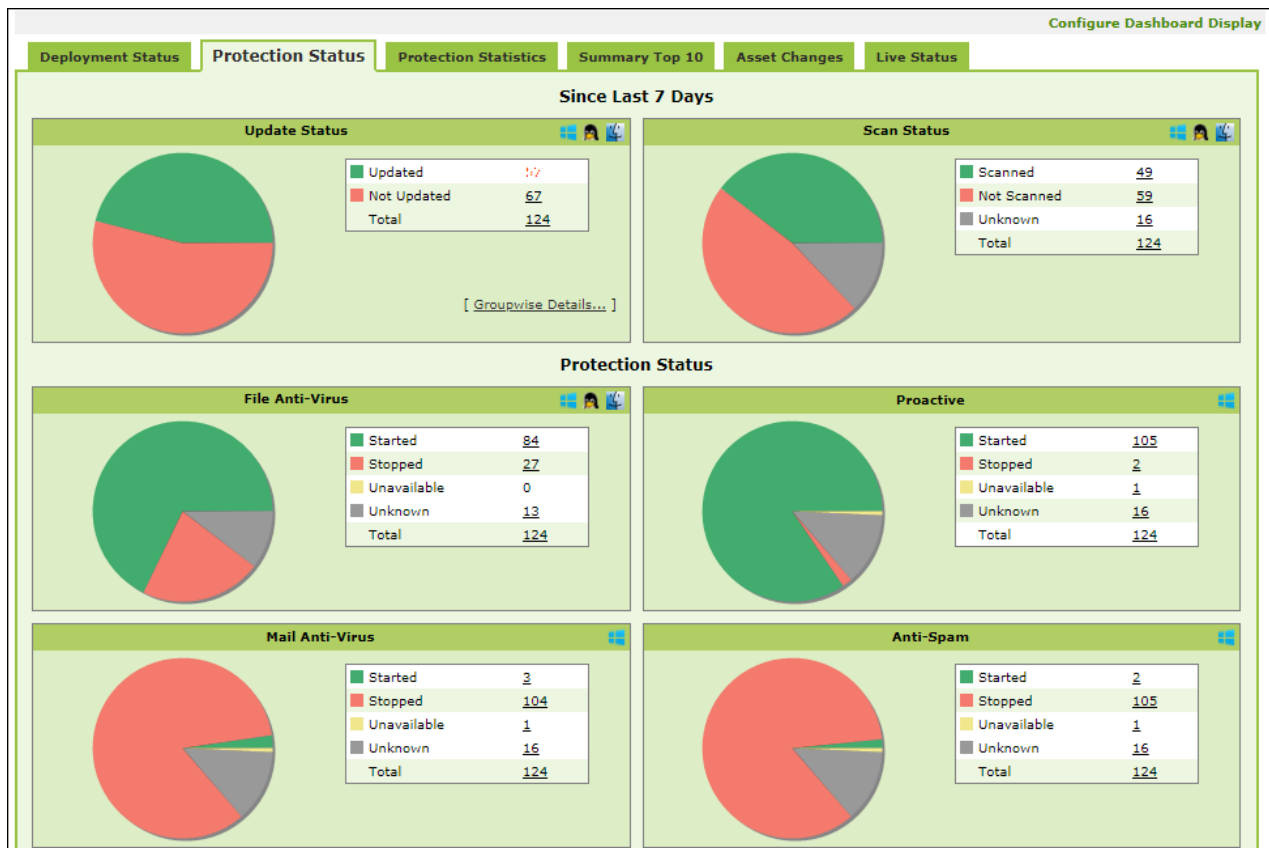
The Windows, Mac, Linux icons at the top of every chart denote that the information is displayed for the respective Operating Systems (OS).



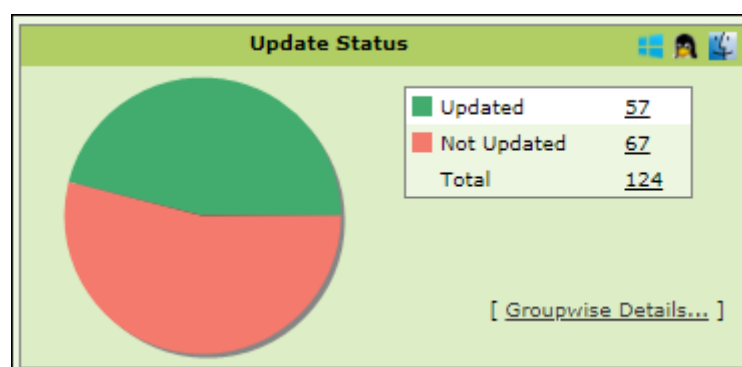


## Protection Status

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.

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

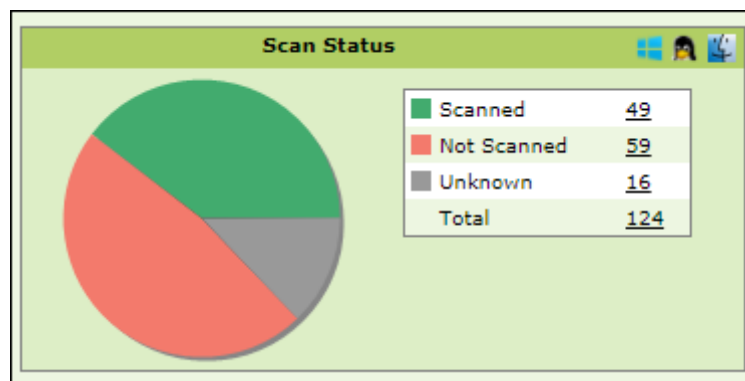
Clicking **Groupwise Details** displays Groupwise Update Status window.

The screenshot shows the 'eScan Management Console' interface. The main title is 'Groupwise Update Status' with a date 'Wednesday, October 23, 2019'. On the left, there's a tree view with 'Managed Computers' selected. On the right, there are checkboxes for 'Include Sub Groups' (unchecked) and 'Groupwise Details' (checked). A 'Print' button is in the top right. Below the checkboxes, a table titled 'Group: Managed Computers (Include Sub Groups)' displays the following data:

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

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

## Scan Status



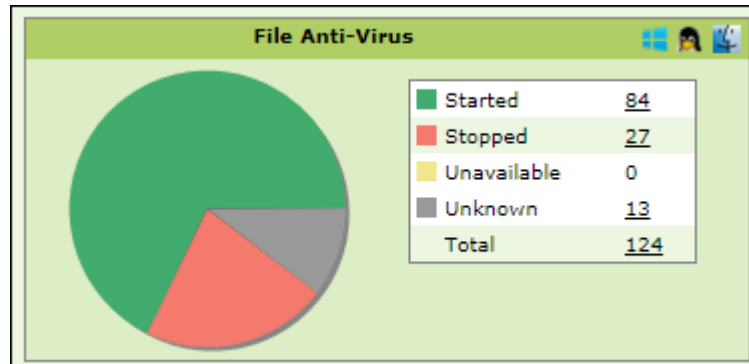
**Scanned** - It displays the number of computers that have been scanned in last 30 days for viruses and malware infections.

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

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

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

## File Anti-Virus



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

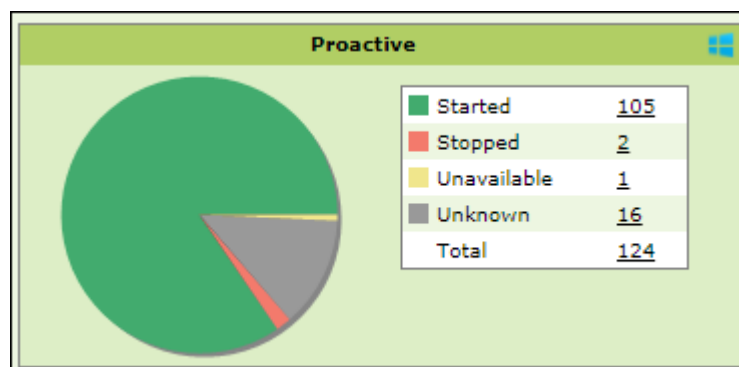
**Stopped** – It displays the number of computers on which the File Anti-Virus module is in Stopped state.

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

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

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

## Proactive



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

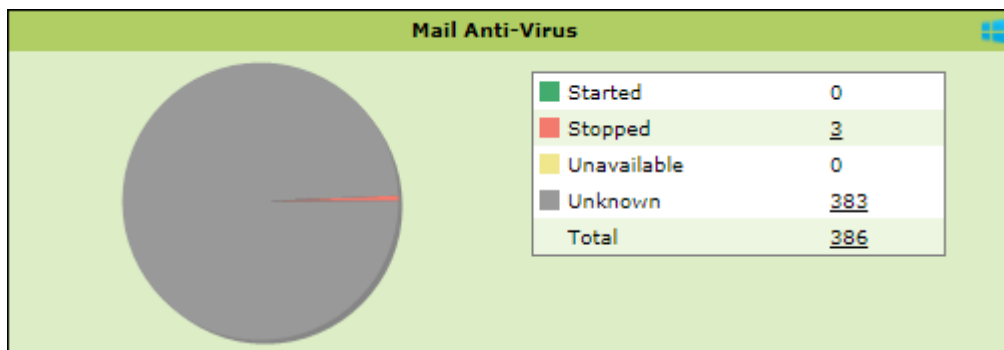
**Stopped** - It displays the number of computers on which Proactive scanning service is stopped.

**Unavailable** – It displays the number of computers where Proactive scanning service is unavailable. This module is available only in computers with Windows OS.

**Unknown** - It displays the number of computers on which the Proactive scanning service status is unknown.

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

## Mail Anti-Virus



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

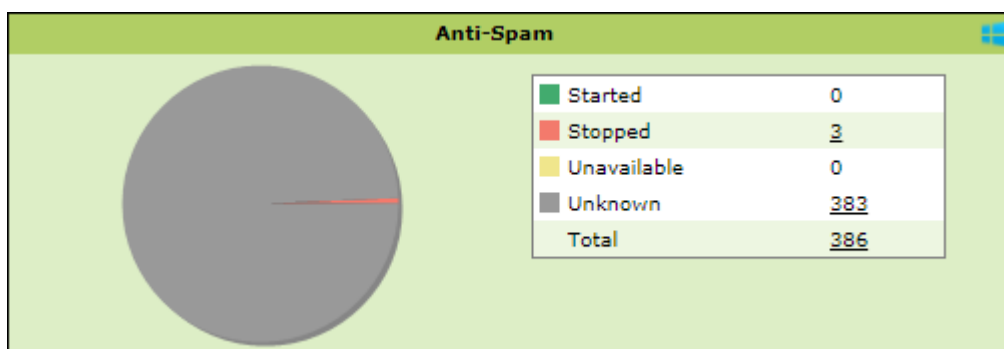
**Stopped** – It displays the number of computers on which the Mail Anti-Virus module is in Stopped state.

**Unavailable** – It displays the number of computers on which the Mail Anti-Virus module is unavailable.

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

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

## Anti-Spam



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

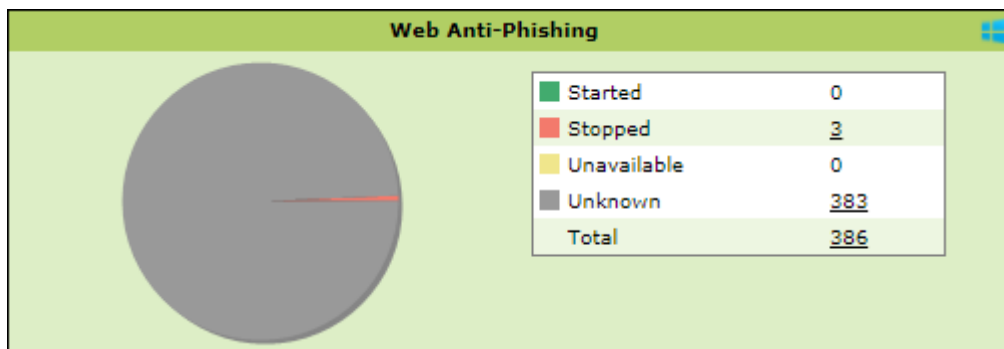
**Stopped** – It displays the number of computers on which the Anti-Spam module is in Stopped state.

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

**Unavailable** – It displays the number of computers on which the Anti-Spam module is unavailable.

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

## Web Anti-Phishing



**Started** – It displays the number of computers on which the web Anti-Phishing service is started.

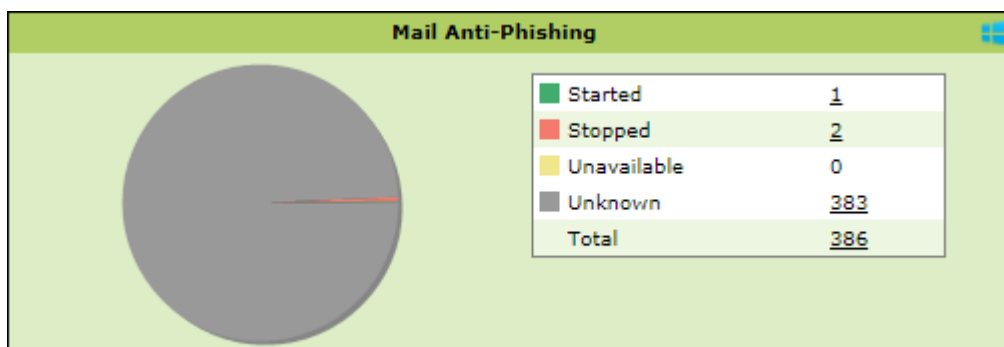
**Stopped** – It displays the number of computers on which the web Anti-Phishing service is stopped.

**Unknown** – It displays the number of computers on which the web Anti-Phishing service status is unknown.

**Unavailable** - It displays the number of computers on which the web Anti-Phishing service is unavailable.

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

## Mail Anti-Phishing



**Started** – It displays the number of computers on which the Mail Anti-Phishing service is enabled.

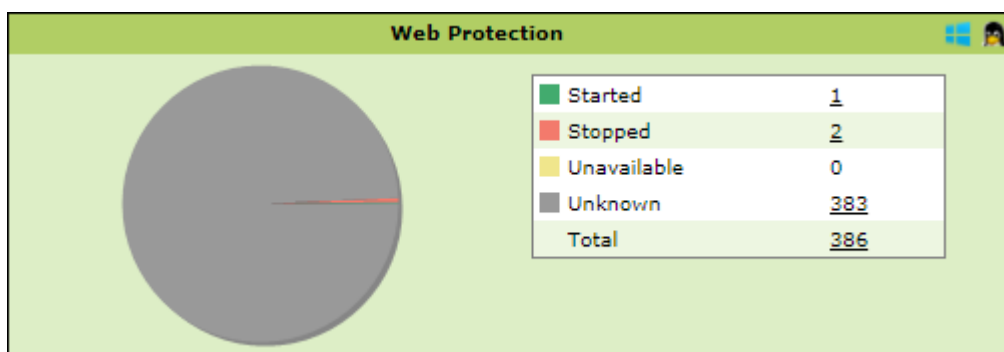
**Stopped** – It displays the number of computers on which the Mail Anti-Phishing service is disabled.

**Unknown** – It displays the number of computers on which the Mail Anti-Phishing service status is unknown.

**Unavailable** – It displays the number of computers on which the Mail Anti-Phishing service is unavailable.

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

## Web Protection



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

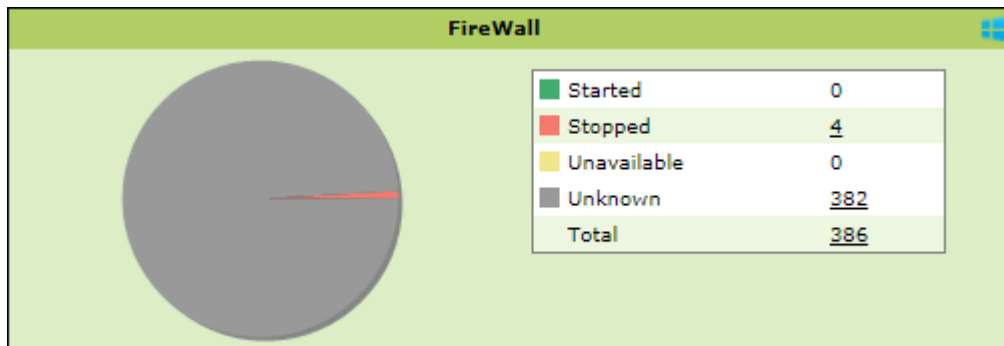
**Stopped** – It displays the number of computers on which the Web Protection module is in Stopped state.

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

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

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

## Firewall



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

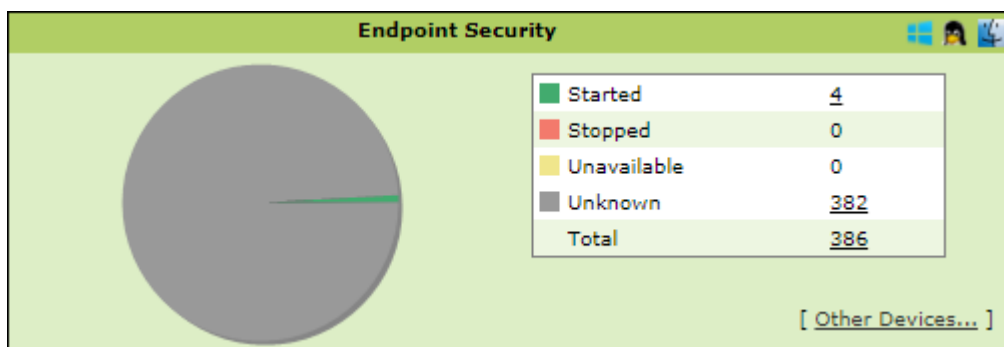
**Stopped** - It displays the number of computers on which the Firewall module is in Stopped state.

**Unavailable** - It displays the number of computers on which the Firewall module is unavailable.

**Unknown** - It displays the number of computers on which the Firewall module status is unknown.

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

## Endpoint Security



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

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

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



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

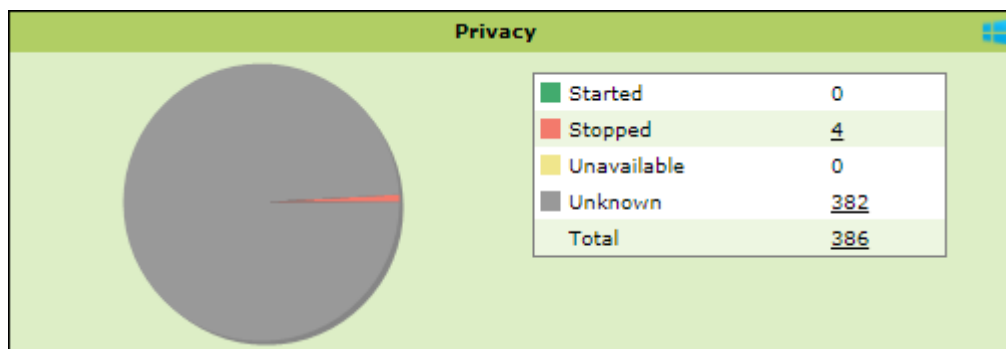
**Total** - It displays the total number of computers connected across the network.

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

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

Close

## Privacy



**Started** - It displays the number of computers on which the Privacy Control module is in Started state.

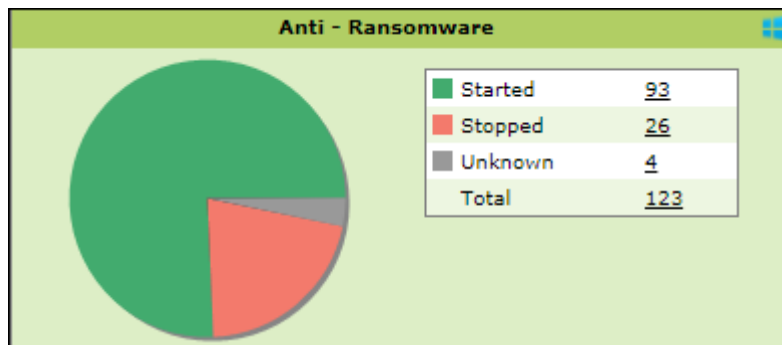
**Stopped** - It displays the number of computers on which the Privacy Control module is in Stopped state.

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

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

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

## Anti – Ransomware



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

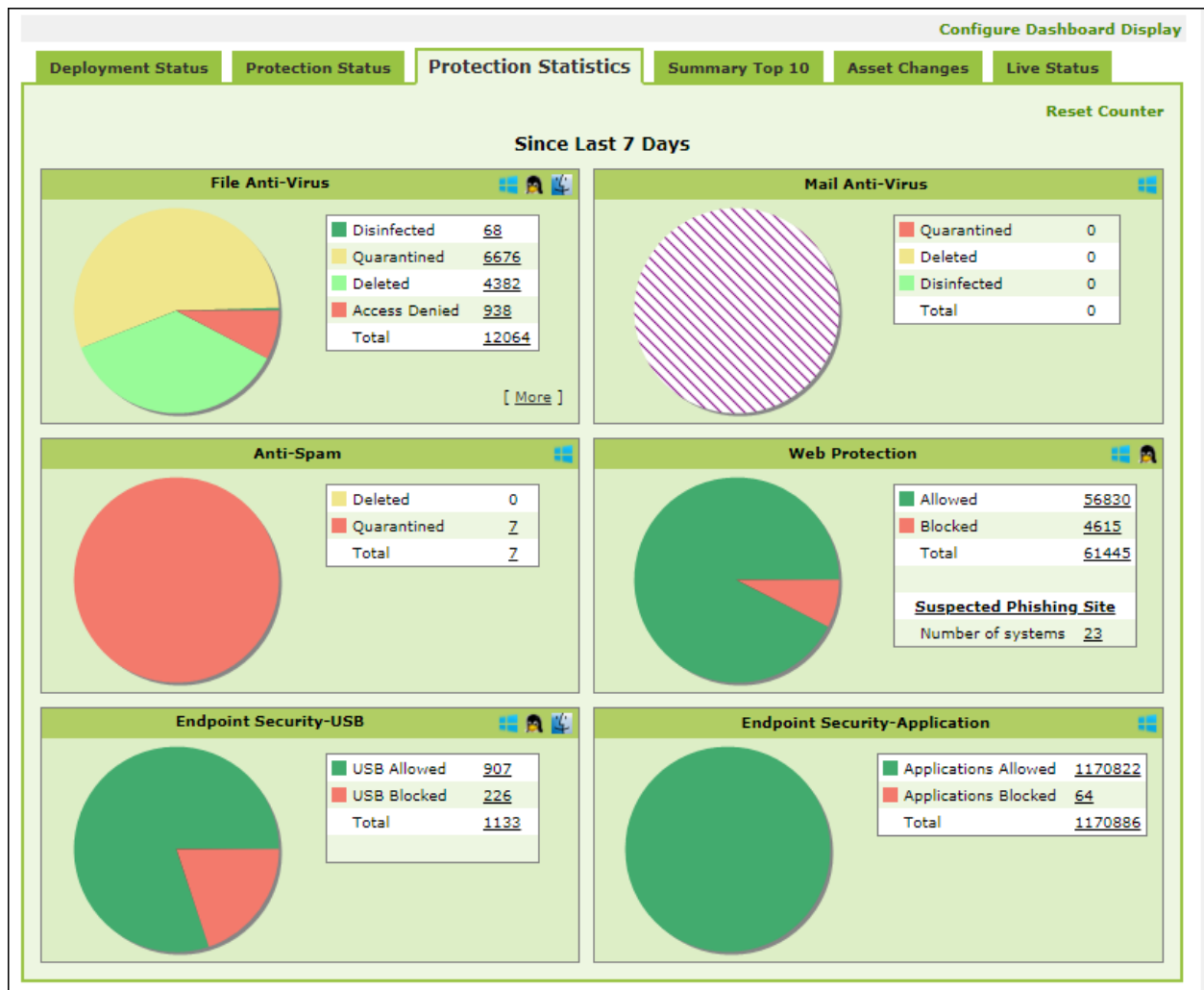
**Stopped** - It displays the number of computers on which the Anti – Ransomware module is in Stopped state.

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

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

# Protection Statistics

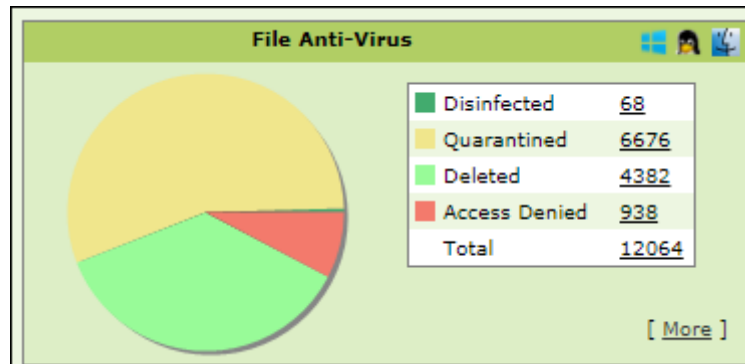
This tab displays activity statistics and action taken by all modules of eScan Client since last seven days in pie chart format.



## 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.

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

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

**eScan Management Console**

06 August 2020

Protection Statistics >> File Anti-Virus >> Quarantined

Client OS Type All Print

Machine Name	Status	Group
ESCAN-001	<u>Quarantined (1)</u>	Managed Computers\EScan

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 ( 1/10/2019 )

Tuesday, September 10, 2019

Print

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

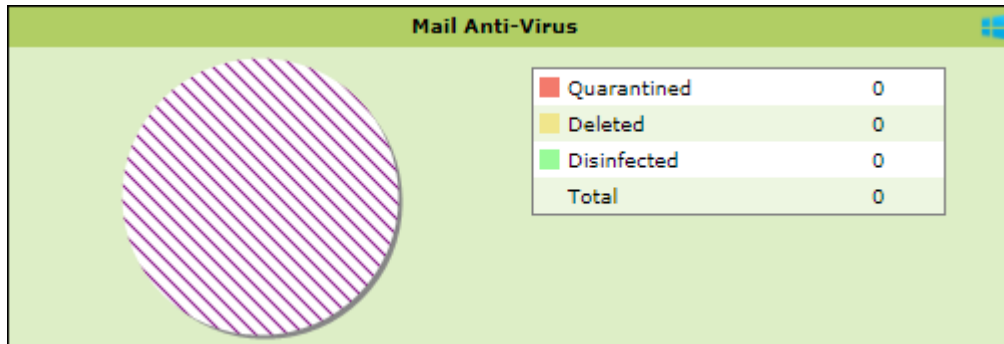
Clicking **[More]** displays additional protection statistics.

**Additional protection statistics**

Malware URL Block	12665
Autorun Block	0
Executable Block USB	27548
Executable Block Network	37427
Executable Block User based	380
Proactive Statistics: Allow	0
Proactive Statistics: Block	137
Exploit Statistics Block	6
Ransomware Statistics Block	86
<b>Total</b>	<b>78249</b>

Close

## Mail Anti-Virus



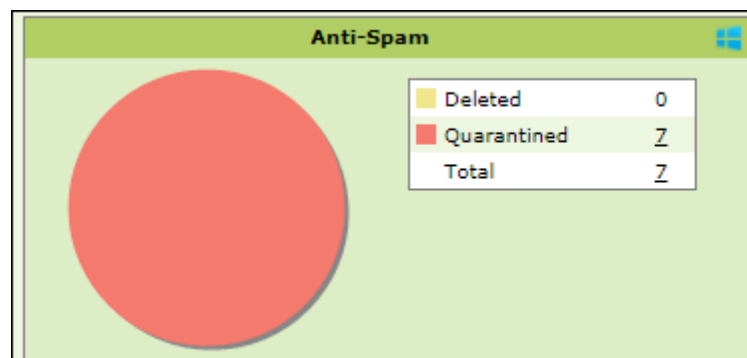
**Quarantined** – It displays the number of files/emails quarantined by Mail Anti-Virus module.

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

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

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

## Anti-Spam

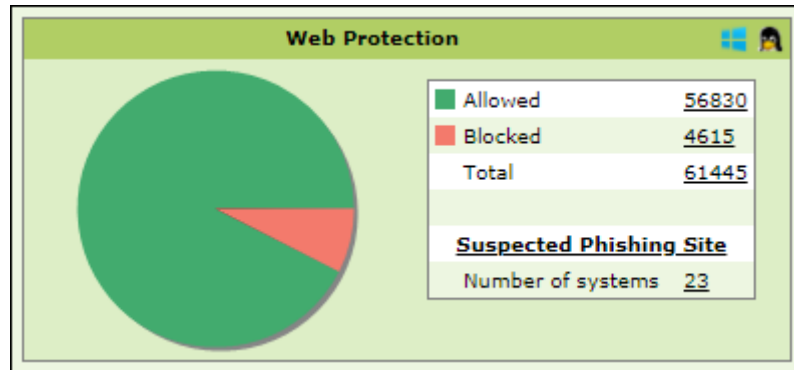


**Deleted** – It displays the number of files deleted by Anti-Spam module.

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

**Total** – It displays the total number of files on which Anti-Spam module took action since last seven days.

## Web Protection



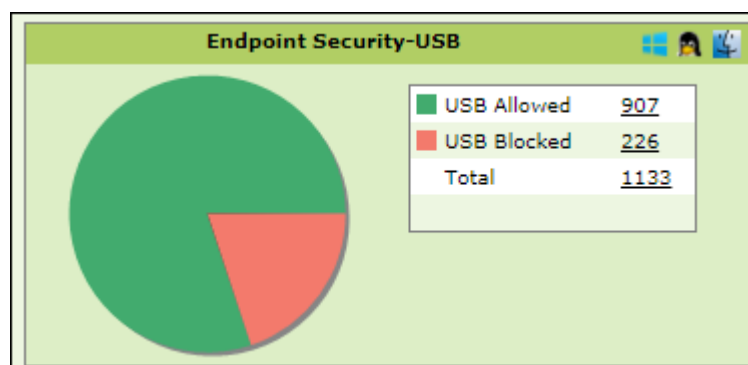
**Allowed** – It displays the number of websites to which access was allowed by Web Protection module.

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

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

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

## Endpoint Security-USB

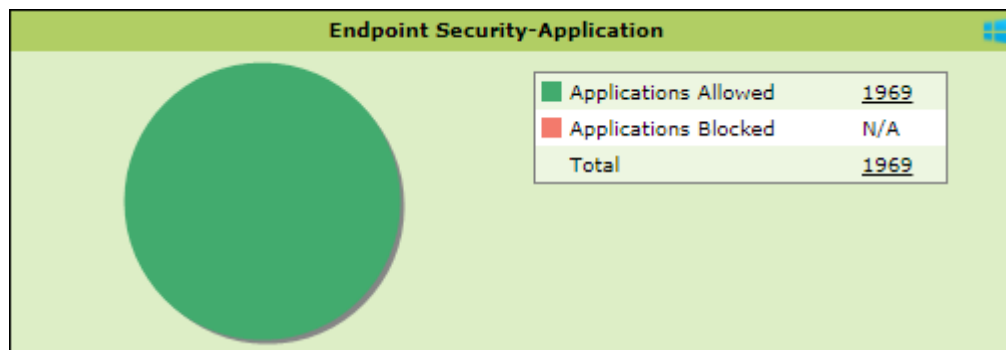


**USB Allowed** – It displays the number of USB access allowed along with the details for the same by Endpoint Security-USB module.

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

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

## Endpoint Security-Application



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

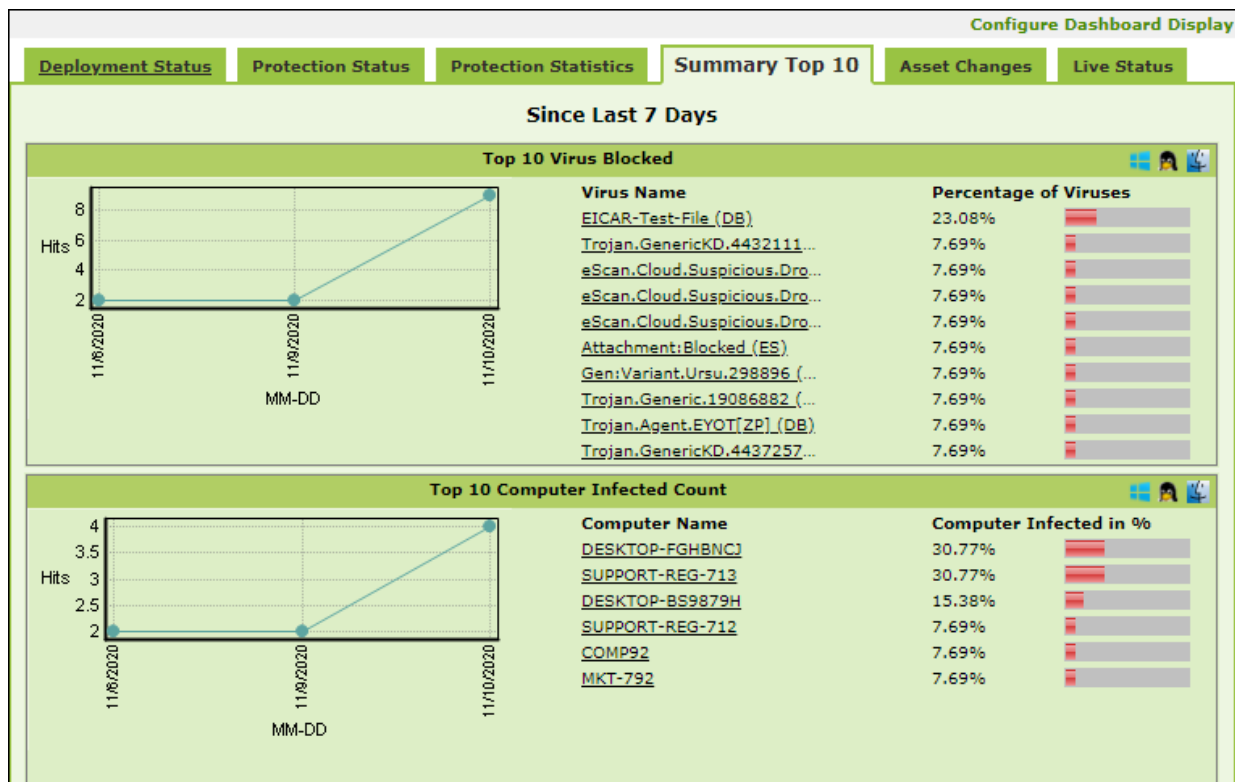
**Applications Blocked** – It displays the number of applications blocked by Endpoint Security-Application module.

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



# Summary Top 10

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



The tab displays the summary for following parameters:

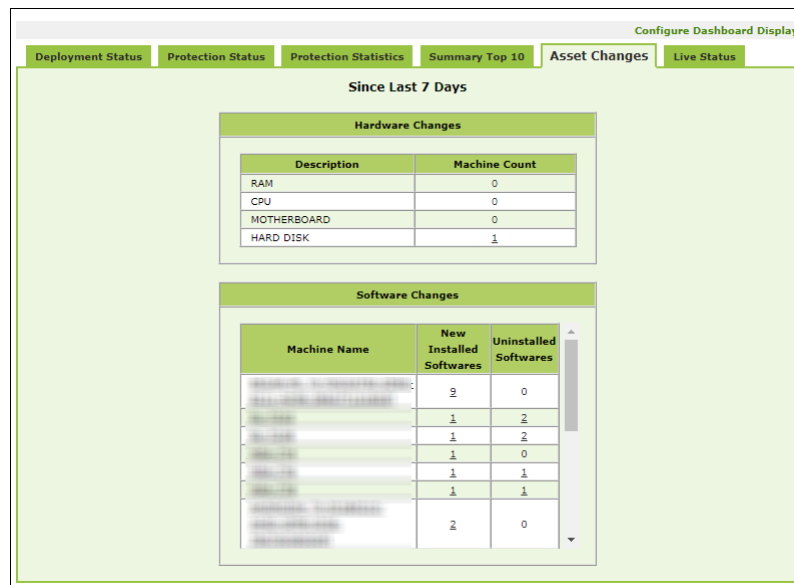
- Top 10 Virus Blocked
- Top 10 Computer Infected Count
- Top 10 USB Blocked Count
- Top 10 Application Blocked Count by Application Name
- Top 10 Application Allowed Count by Application Name
- Top 10 Application Blocked Count by Computer Name
- Top 10 Application Allowed Count by Computer Name
- Top 10 Websites Blocked Count by Website Name
- Top 10 Websites Allowed Count by Website Name
- Top 10 Websites Blocked Count by Computer Name
- Top 10 Websites Allowed Count by Computer Name
- Top 10 Infected Emails(Mail AV)
- Top 10 Spam Emails(AntiSpam) from
- Top 10 Websites Blocked Count by Username
- Top 10 Websites Allowed Count by Username



- Top 10 Exploit Blocked Count

## Asset Changes

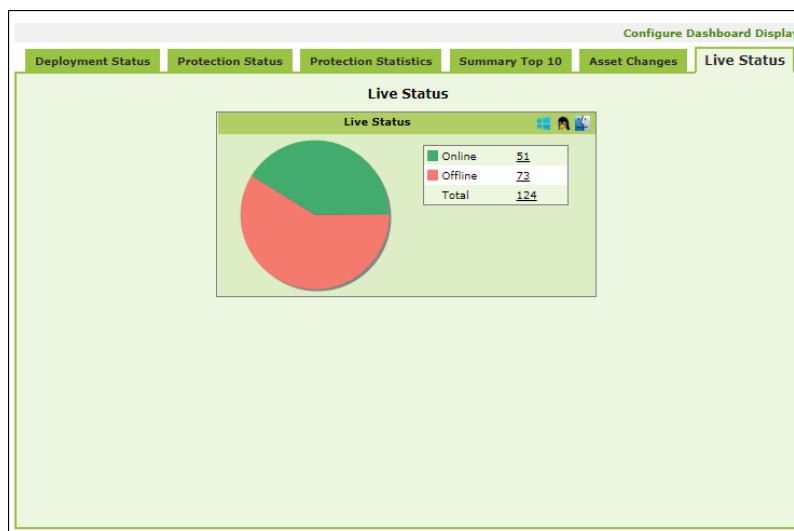
This tab displays all hardware and software changes carried out on the endpoints since last seven days.



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.

## Live Status

This tab displays the number of computers that are online and offline in a network.





Clicking the numerical displays the computer's username, status, eScan Client version number and the group under which it is categorized.

# 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.

The screenshot shows the 'Configure Dashboard Display' window with the following sections and options:

- 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
  - ☒ 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
  - ☒ 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
- Live Status**
  - ☒ Live Status

At the bottom, there are 'Ok' and 'Cancel' buttons.

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

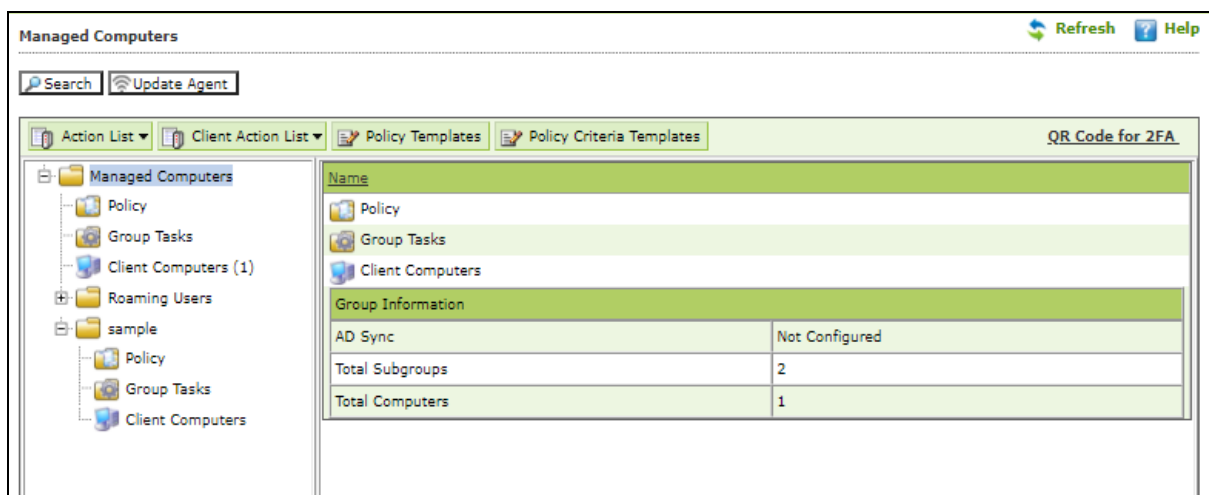
The tabs will be updated according to the changes.

# Managed Computers

To secure, manage, and monitor computers, it is necessary to add them in a group. The **Managed Computers** module lets you create computer groups, add computers to a group, define policy templates for the created groups and computers, create policy criteria templates and tasks for specific groups.

Based on the departments, user roles and designations, you can create multiple groups and assign them different policies. This lets you secure and manage computers in a better way.

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



The screen consists of following buttons:

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

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

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

2. Click  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.

Update Agent	IP Address	Assigned to Group(s)
		Managed Computers\Sample Group

2. In the Assigned to Group(s) column, click .

A confirmation prompt appears.

:10443 says

Do you want to remove update agent?

OK Cancel

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**
- **Set group Configuration**
- **Deploy/Upgrade Client**
- **Uninstall eScan Client**
- **Remove Group**
- **Synchronize with Active Directory**
- **Outbreak Prevention**
- **Create Client Setup**
- **Properties**

## Creating a Group

To create a group, follow the steps given below:

1. Click **Action List > New Subgroup**.

Creating New Group window appears.

2. Enter a name for the group.
3. Click the Group Type 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.

<b>NOTE</b>	<p>If the Group type is set to <b>Normal User</b>, then server will try to connect to the client computer using the hostname.</p> <p>If the Group type is set to <b>Roaming User</b>, then server will try to connect to the</p>
-------------	--

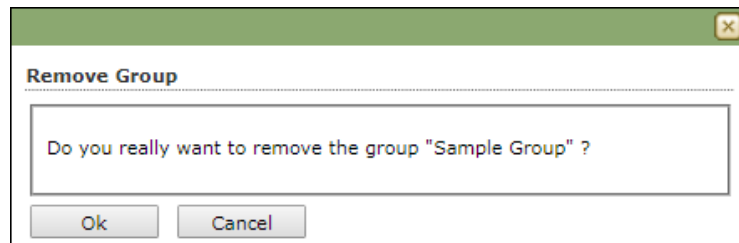


	client computer using the IP address. Multiple groups can be created within a group.
--	---

## Removing a Group

To remove a group, follow the steps given below:

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



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

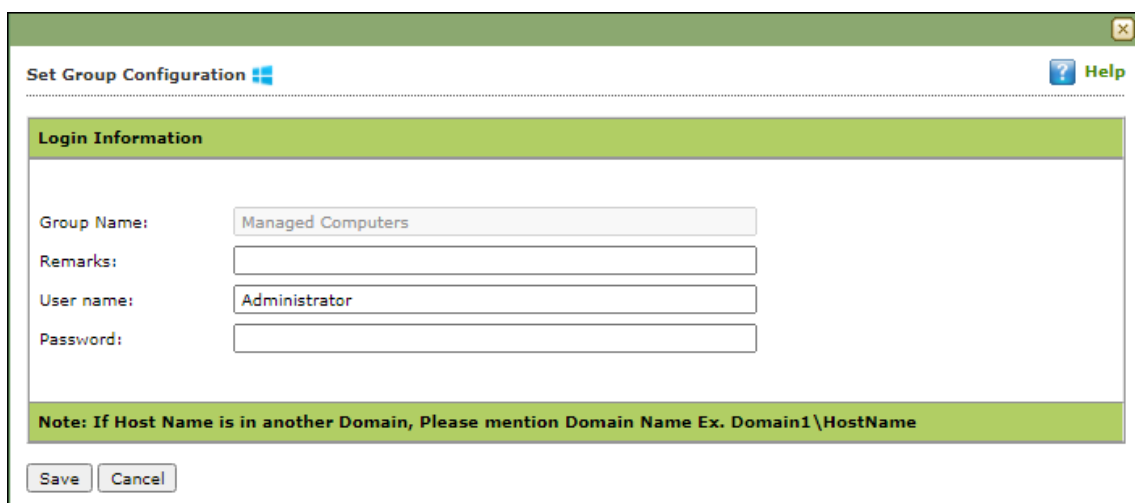
**NOTE** A group will be removed only if it contains no computers.

## Set Group Configuration

With this option you can define single Username and Password to login for all the computers in the group.

To set a group configuration, follow the steps given below:

1. Select the group you want to configure.
2. Click **Action List** > **Set Group Configuration**. Set Group Configuration window appears.

A screenshot of the 'Set Group Configuration' window. The title bar is green with a close button. The main area has a white background with a green header 'Set Group Configuration'. Below the header is a green bar with the text 'Login Information'. Under this bar are four input fields: 'Group Name' (containing 'Managed Computers'), 'Remarks' (empty), 'User name' (containing 'Administrator'), and 'Password' (empty). At the bottom is a green bar with the text 'Note: If Host Name is in another Domain, Please mention Domain Name Ex. Domain1\HostName'. Below the note are two buttons: 'Save' and 'Cancel'.

3. Enter Remarks and define Login credentials.
4. Click **Save**. The group configuration will be saved.

## Managing Installations

After grouping all computers in logical groups using eScan Management Console, you can now install eScan Client as well as other third party software on the computers connected to your network. [Conditions Apply]

This section will give you an overview on following activities:

### Installing eScan Client

eScan client can be installed on computers connected to the network in the following ways:

- **Remote Installation:** It lets you install eScan Client on all the computers in a selected group at once. You can initiate and monitor eScan Client installation using eScan Management Console. [For more click here](#)
- **Manual Installation:** In case remote installation fails, you can allow computer users to install eScan client manually on their computers. It does not require any remote assistance. [For more click here](#)
- **Installing eScan using agent:** Installation of agent ensures that you have Administrator rights on the computer and you can now remotely install eScan Client on that computer. [For more click here](#)
- **Installing other Software (3<sup>rd</sup> Party software):** eScan Management Console lets you install third party software on network computers remotely. [For more click here](#).
- **Viewing Installed Software List:** Using Show Installed Software option you can view list of software installed on Computers connected to your network. You will find this option in **Client Action list** under **Managed Computers** when you select a computer.
- **Force Download:** This option is present under Client Action List in Managed Computers. You can update eScan client on any network computer by using this option. It is required in cases where client has not been updated on the computer for many days.

To initiate Force download, in the **Managed Computers** module, select the client computer and click **Client Action list > Force Download**.

It will initiate the forced download process on selected Client computers.

<b>NOTE</b>	<p>Conditions for third party software installation:</p> <p>After starting the installation from eScan Management Console, no manual intervention should be required to complete the installation on Client computer. Only automated installations can be done through eScan Management Console.</p> <p>Care should be taken that the installation file is not huge as it may impact internal network speed of your organization.</p>
-------------	---

## Remote Installation of eScan Client

### Pre-Installation

To prepare a client computer for the remote deployment of eScan Corporate Edition (with Hybrid Network Support); begin with checking if the basic system requirements are in place.

Configure the settings on the client computer according to the OS installed on it

- **Windows XP Professional systems**
- **Windows XP Home**
- **Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10**

### Configuring the settings on Windows XP Professional systems (Windows XP, 2000, 2003, all editions)

1. Click **Start > Control Panel**.
2. Double-click the **Administrative Tools** icon.
3. Double-click the **LocalSecurityPolicy** icon.
4. On the navigation pane, click **Local Policies** folder, and then click **Security Options** folder.
5. Double-click Network Access: Sharing and Security Model for Local accounts policy.
6. Select Classic - Local user authenticate as themselves option from the drop-down list.
7. Click **Apply**, and then click **OK**.
8. Double-click the **Accounts: Limit local account use of blank passwords to console logon only policy**. The Accounts: Limit local account use of blank passwords to console logon only dialog box appears.
9. Click **Disabled** option.
10. Click **Apply**, and then click **OK**.

If Windows firewall is enabled on all locations, select **File and Printer Sharing** checkbox, under **Exceptions** tab (**Control Panel >> Windows Firewall >> Exception**).

### For Windows XP Home

Since Windows XP Home has limitations with regards to remote deployment, MWAgent should be installed on your system. You can download MWAgent from the eScan web console.

### For Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10

1. Launch **Run**.
2. Enter **secpol.msc**, and then click **OK**. Local Security Settings window appears.
3. On the navigation pane, click **Local Policies** folder, and then double-click **Security Options** folder. The security policy appears.

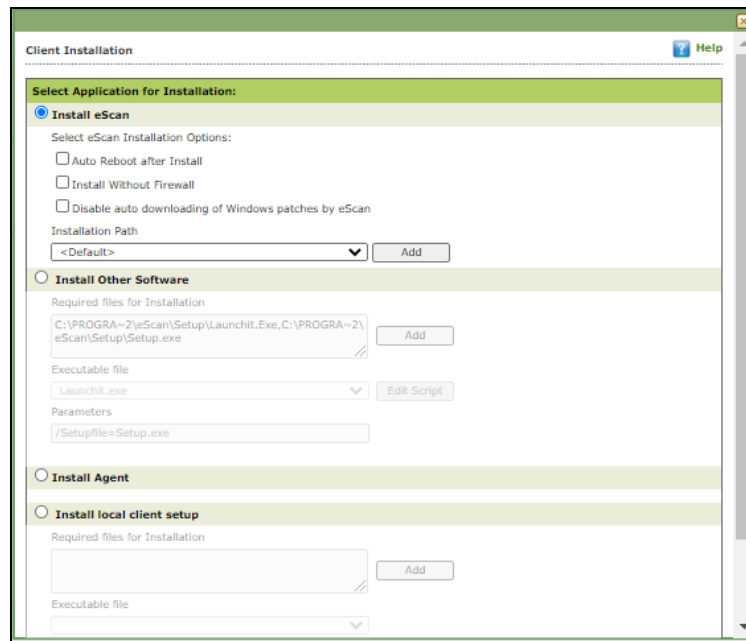
4. Double-click **Network access: Sharing and security model for local accounts** policy.
5. Select Classic - Local users authenticate as themselves option present in the drop-down.
6. Click **Apply** > **OK**.
7. Double-click **Accounts: Limit local account use of blank passwords to console logon only** policy.
8. Select **Disabled** option.
9. Click **Apply** > **OK**.
10. If the firewall is enabled, select **File and Printer Sharing** checkbox, under **Exceptions** tab.
11. On desktop, click **Start**, and right-click **My Computer**, click **Manage**. Computer Management window appears.
12. On the navigation pane, click **Local Users and Groups** option, and then click **Users** folder, and double-click **Administrator**. Administrator Properties window appears.
13. Check **Password never expires** and uncheck **Account is disabled** checkbox.
14. Click **Apply** > **OK**.

## Deploy/Upgrade Client

To Deploy/Upgrade eScan client on all computers in a group or an individual computer, follow the steps given below:

### Installing eScan Client on a Group

1. Select the group on which you want to install eScan client.
2. Click **Action List** > **Deploy/Upgrade Client**. Client Installation window appears.

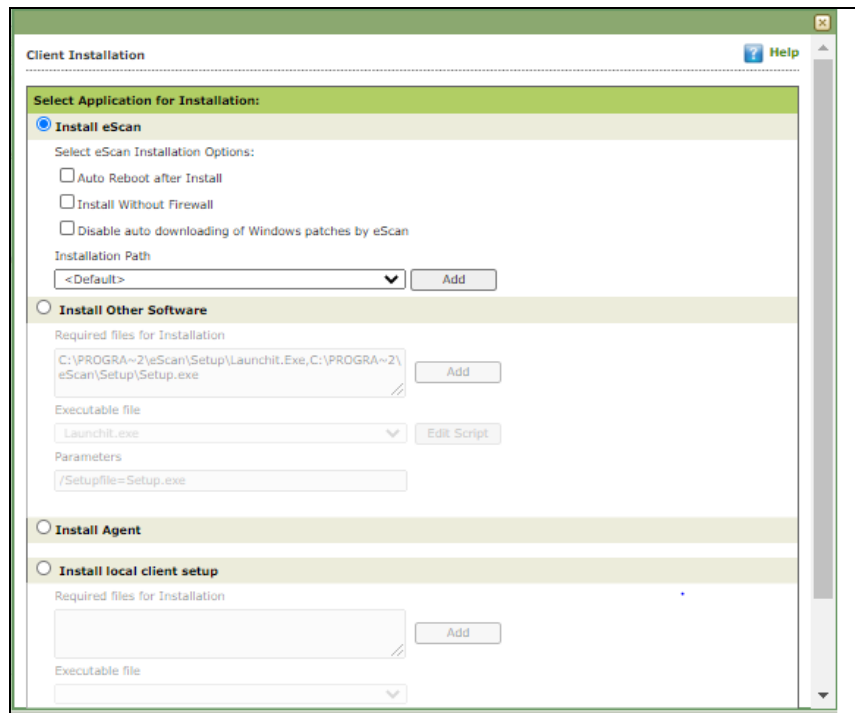


3. Select **Install eScan** option.  
By Default eScan is installed at the following Path on a Client computer.  
**C:\Program Files\eScan** (default path for 32-bit computer)  
OR  
**C:\Program Files (x86)\eScan** (default path for 64-bit computers).
4. To define a different installation path, click **Add**. (Skip this step if default path chosen).
5. Click **Install**. A window displays File transfer progress. After Installation, the eScan status will be updated in Managed Computers list.

## Installing eScan Client on an Individual Computer in a Group

1. Select a group.
2. Under the group, click **Client Computers**.
3. Select a computer.
4. Click **Client Action List > Deploy/Upgrade Client**. Client Installation window appears.






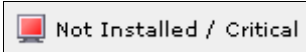
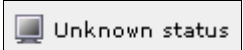

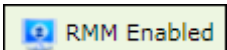
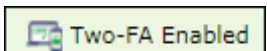

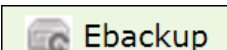
5. Select **Install eScan** option.  
By default eScan is installed at the following path on a Client computer.  
C:\Program Files\eScan (default path for 32-bit computer)  
OR  
C:\Program Files (x86)\eScan (default path for 64-bit computers).
6. To define a different installation path, click **Add**. (Skip this step if default path chosen).
7. Click **Install**. A window displays File transfer progress. After eScan installation, the eScan status will be updated in Managed Computers list.

## 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.

## Understanding the eScan Client Protection Status

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

## Moving computer from one group to other

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

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

The computers will be moved to the selected group.

## Viewing installed software (on Client computer)

To view the installed software, follow the steps given below:

1. In folder tree, click **Managed Computers**.
2. Select the desired computer.
3. Click **Client Action List > Show Installed Software**.

A list of all the Software installed on that computer will be displayed on pop up window in an instant.

## Removing computers from a group

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

1. Click **Managed Computers**.
2. Select the desired computers for removal.
3. Click **Client Action List > Remove from Group**.

A confirmation prompt appears.

4. Click **OK**.

The computers will be removed from the group.

## Installing eScan on Linux and MAC Computers

In order to install eScan on Linux or Mac computers, install eScan Agent first and then proceed for eScan installation.

### Installing Agent on Linux (Debian based Operating System) –

1. Download agent from the link sent on mail and save it at the desired path on the computer where you wish to install eScan Client.
2. Open the terminal for installing Agent.
3. Installation of Agent requires root or sudo user authentication. After Login as **root** or **sudo user**, go to the path where the **Agent\_setup.deb** file has been saved.

4. Install the agent from the path using the following command – ***dpkg -i*** ( for RPM based setup – Rpm-ivh) –

```
root@qa-ubu-208: /tmp
root@qa-ubu-208:/tmp# ls
kde-kdm          mwagent-7.0.2.amd64.i386.deb  ssh-cfUVtY0r2282
keyring-DE44sx  pulse-2DrPL76K1sLw          unity_support_test.1
ksocket-kdm     pulse-PKdhtXMr18n
root@qa-ubu-208:/tmp# dpkg -i mwagent-7.0.2.amd64.i386.deb
Selecting previously unselected package mwagent.
(Reading database ... 162068 files and directories currently installed.)
Unpacking mwagent (from mwagent-7.0.2.amd64.i386.deb) ...
Setting up mwagent (7.0.2) ...
Architecture = i386
Adding system startup for mwagent ...
Adding system startup for winclient ...
Starting MicroWorld Mwagent:
[ OK ]
root@qa-ubu-208:/tmp#
```

Agent installation will begin. After completion you will be informed via a message and the Agent will run on your computer.

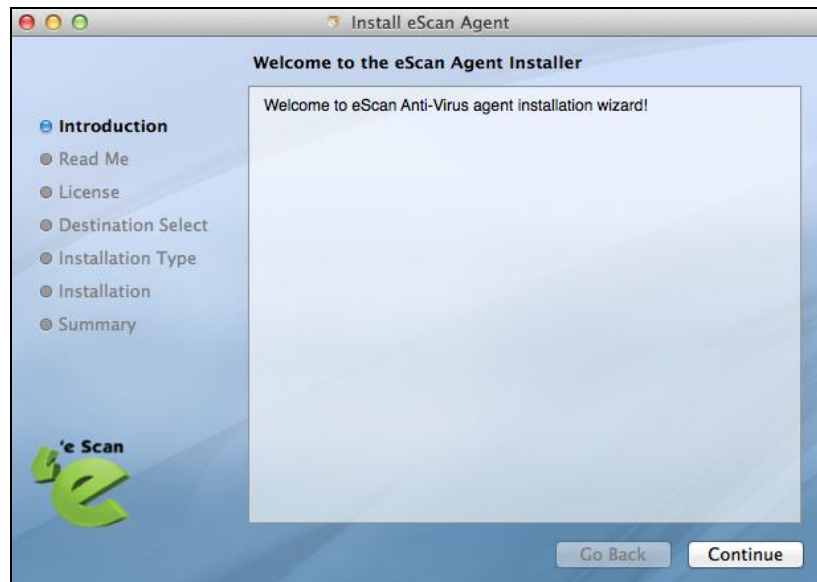
## Installing eScan Agent on Mac Computers

To install eScan Agent on Mac computers follow the steps given below:

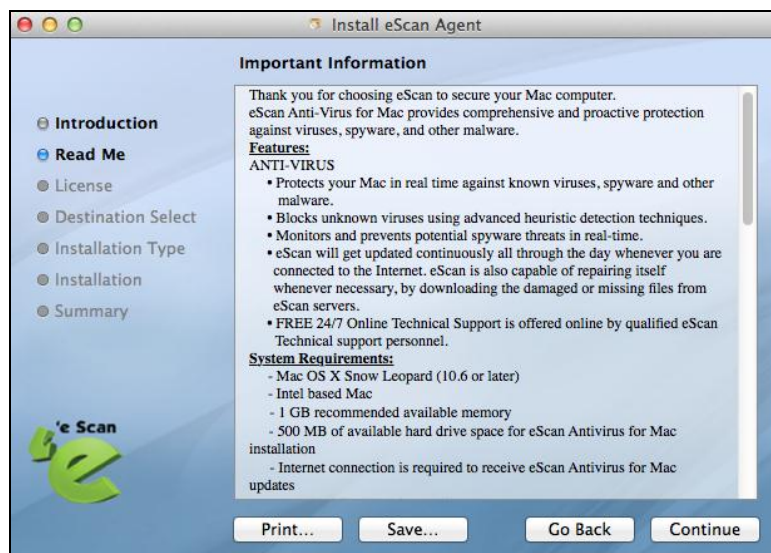
1. Download agent from the link received via mail and save it at the desired path on the computer where you wish to install eScan Client.
  2. Go to the path where Agent is saved.
  3. Double-click **Agent\_Setup.dmg** file to run the installation wizard.
- Agent Installation Wizard will run.



4. Double-click **eScan Agent**. This will start the installation process. Introduction window appears.
5. To proceed, click **Continue**.

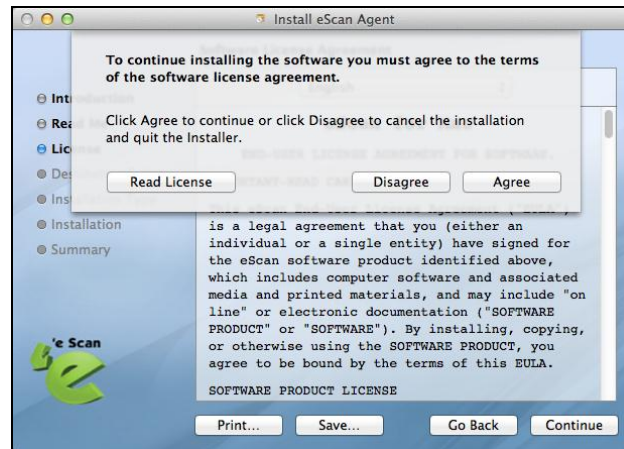


- The installation wizard displays Read Me window.
6. Please read the system requirements and click **Continue**. License window appears.

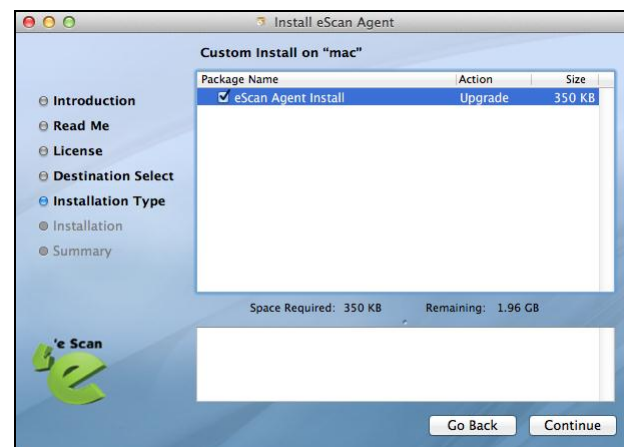


7. Please read the agreement completely and then click **Continue**.

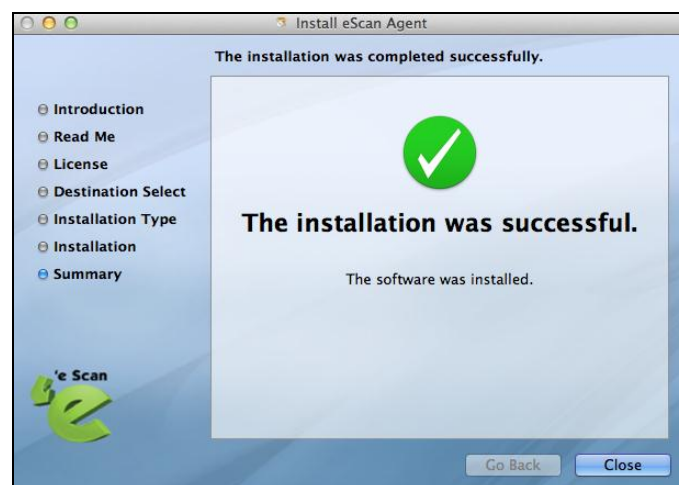
8. Agree to terms and conditions by clicking **Agree**.



9. Select **eScan Agent Install** checkbox and click **Continue**.



10. Select the destination folder by clicking **Change install Location** and click **Install**.

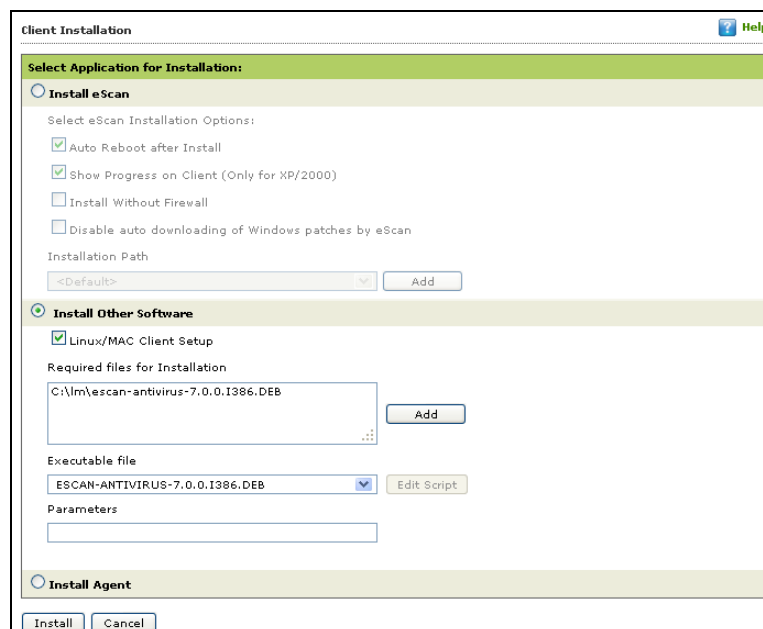


11. To exit the installation wizard, click **Close**.

## Installing eScan Client on Linux or Mac computers

To install eScan Client on Linux or Mac computers, follow the steps given below:

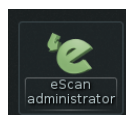
1. Select the desired computer.
2. Refresh the Client by clicking **Refresh Client**.  
A link will be created for downloading the setup file of eScan Client for that computer; you will be redirected to escanav.com from where you can download the setup file.
3. Download the Client setup from the link on eScan Corporate server.
4. To deploy the setup, click **Client Action List > Deploy/ Upgrade Client**.
5. Click **Install Other Software** and select **Linux/MAC Client setup** option.



6. Click **Install** to initiate the installation process. A notification will be displayed after successful installation.

### In Linux

- eScan Administrator Icon will be displayed on desktop.



### In Mac

- An Icon of eScan will be displayed in the **Dock**. Double-click it to launch eScan.

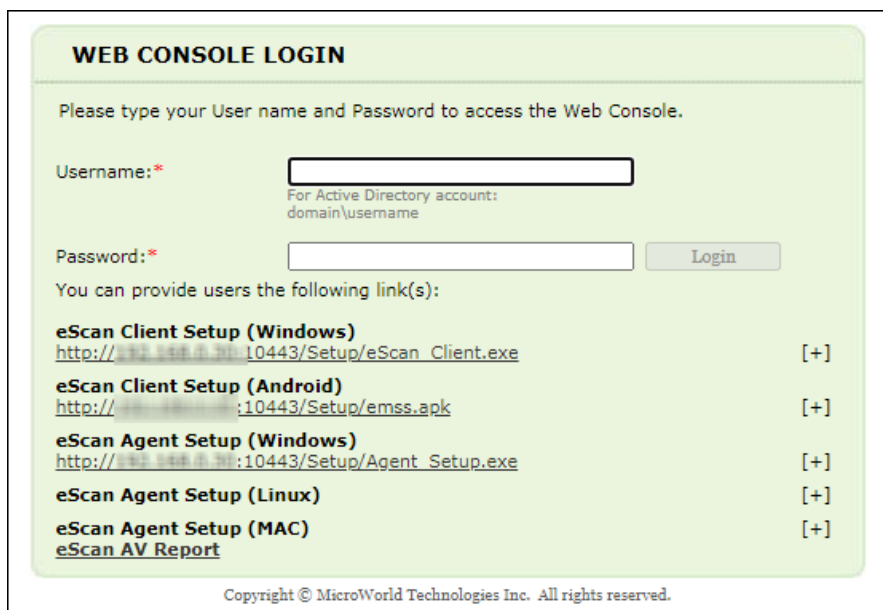




## Manual installation of eScan Client on network computers

If remote installation is not possible, you may manually install the eScan Management Console.

To install manually, the download links for manual installation of the **eScan Client** or **Agent** are displayed on the **Login Page** of eScan Management Console. Forward this link to the user of the Client computer on mail and guide the user through the installation process.



**WEB CONSOLE LOGIN**

Please type your User name and Password to access the Web Console.

Username:\*   
For Active Directory account:  
domain\username

Password:\*

You can provide users the following link(s):

<b>eScan Client Setup (Windows)</b>	
<a href="http://10.10.10.10:10443/Setup/eScan_Client.exe">http://10.10.10.10:10443/Setup/eScan_Client.exe</a>	[+]
<b>eScan Client Setup (Android)</b>	
<a href="http://10.10.10.10:10443/Setup/emss.apk">http://10.10.10.10:10443/Setup/emss.apk</a>	[+]
<b>eScan Agent Setup (Windows)</b>	
<a href="http://10.10.10.10:10443/Setup/Agent_Setup.exe">http://10.10.10.10:10443/Setup/Agent_Setup.exe</a>	[+]
<b>eScan Agent Setup (Linux)</b>	[+]
<b>eScan Agent Setup (MAC)</b>	[+]
<a href="#">eScan AV Report</a>	

Copyright © MicroWorld Technologies Inc. All rights reserved.

## Installing eScan Client Using Agent

You may install the eScan Client using an Agent in following ways:

- Remotely installing agent on Client computer(s)
- Manually installing agent on Client computer(s)

### Remotely installing agent on Client computer(s)


1. Click Managed Computers.
2. Select the computer(s) from a group.
3. Click **Client Action List > Deploy/Upgrade Client**.
4. Select **Install Agent** option and click **Install**. eScan Agent will be installed on selected computers.

<b>NOTE</b>	This option useful in case there are glitches in the network connectivity between
-------------	---

server and Client computer. It will overcome those glitches and speed up the client installation on the selected computers.

## Manually installing eScan Agent on Client computer(s)

To manually install eScan Agent on computers, please send the link displayed on the **Login Page** of eScan Management Console to the users of the Client computer on mail.



**WEB CONSOLE LOGIN**

Please type your User name and Password to access the Web Console.

Username: \*   
For Active Directory account: domain\username

Password: \*

You can provide users the following link(s):

**eScan Client Setup (Windows)** [+]  
[http://.../Setup/eScan\\_Client.exe](http://.../Setup/eScan_Client.exe)

**eScan Client Setup (Android)** [-]  
<http://.../>  
<http://.../>  
<http://.../>  
<http://.../>

**eScan Agent Setup (Windows)** [+]  
[http://.../Setup/Agent\\_Setup.exe](http://.../Setup/Agent_Setup.exe)

**eScan Agent Setup (Linux)** [-]  
<http://.../>  
<http://.../>  
<http://.../>  
<http://.../>  
<http://.../>  
<http://.../>  
<http://.../>

**eScan Agent Setup (MAC)** [-]  
<http://.../>  
<http://.../>  
<http://.../>  
<http://.../>

**eScan AV Report**

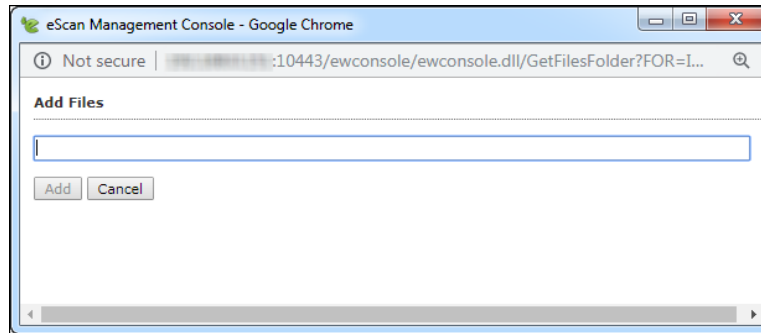
Copyright © MicroWorld Technologies Inc. All rights reserved.

## Installing other Software (Third Party Software)

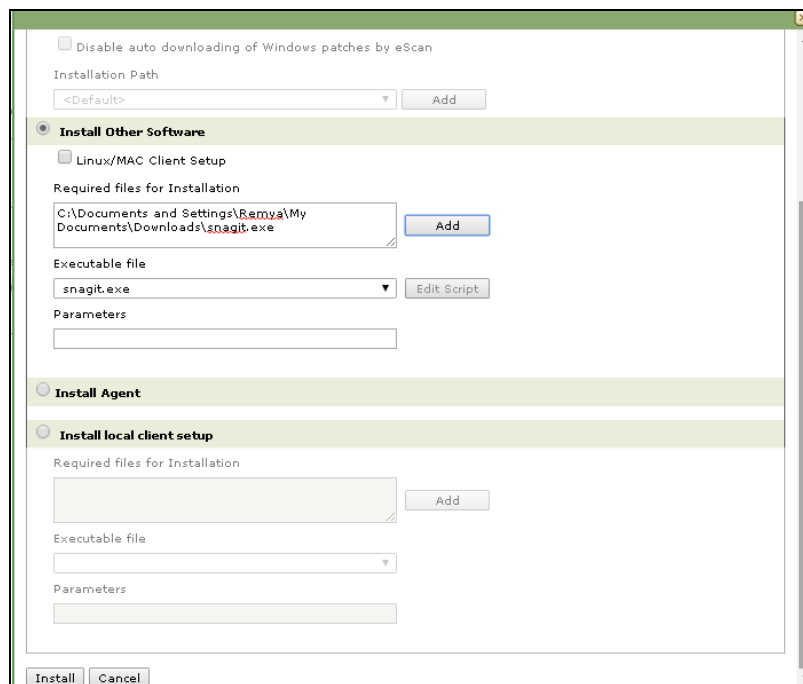
To install third party software on computers, follow the steps given below:

1. Click Managed Computers.
2. Select a computer from a group.
3. Click **Client Action List** > **Deploy/Upgrade Client**. Client Installation window appears.

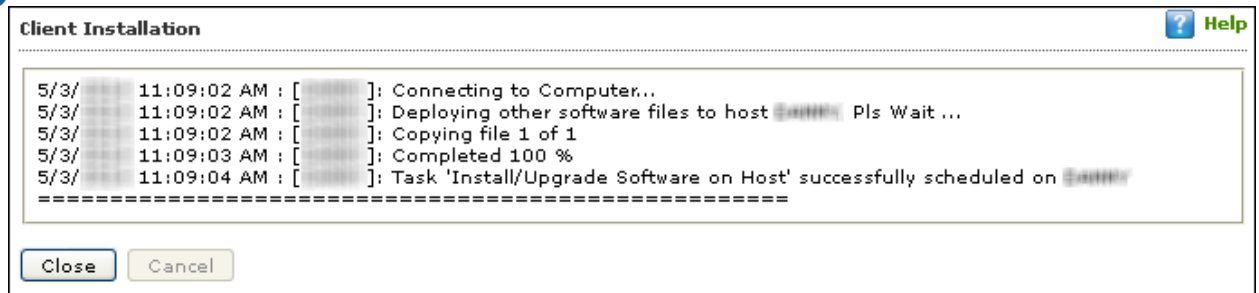
4. Select **Install Other Software** option.
5. Click **Add**.  
Add Files window appears.



6. Enter the exact path of the EXE (on eScan Server) and click **Add**. The selected **EXE** will be added to the "Required files for Installation" list.



7. The Executable Filename will be displayed in the respective drop-down menu.
8. Define the command line parameters if required.
9. Click **Install** to initiate the installation process. A confirmation message appears.

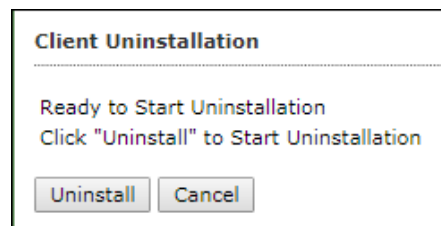


## Uninstall eScan Client (Windows, Mac, and Linux)

To uninstall eScan Client on all the computer from a group, follow the steps given below:

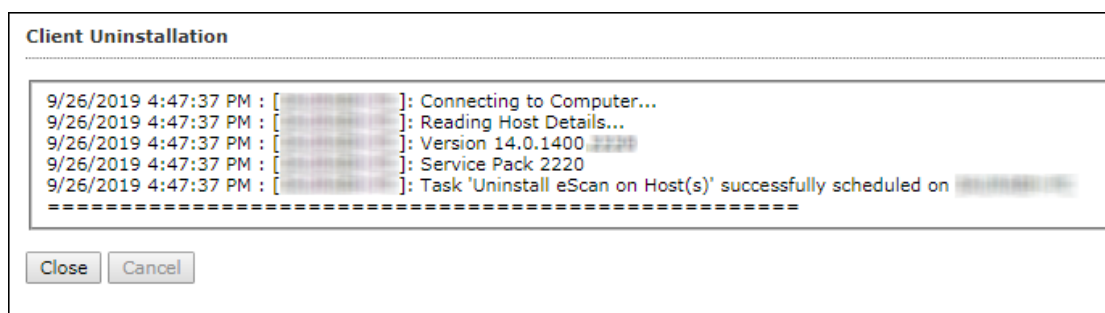
1. Select the group of computers for uninstallation.
2. Click **Action List > Uninstall eScan Client**.

Client Uninstallation window appears.



3. Click **Uninstall**.

The Client Uninstallation window displays the progress.



After the uninstallation process is over, click **Close**.

**NOTE** You can uninstall eScan Client from all the computers in the group by selecting the Group and then Click **Action List > Uninstall eScan Client**.

## Synchronize with Active Directory

To synchronize a group with Active Directory, follow the steps given below:

1. In the Managed Computers folder tree, select a group for synchronization.
2. Click **Action List** > **Synchronize with Active Directory**.

Synchronize with Active Directory window appears.

**Synchronize with Active Directory**

Target Groups :

Source Active Directory Organisation Unit :

Synchronization interval :  Minutes (Minimum 5 Minutes)

Exclude From ADS Sync

<input type="checkbox"/> Excluded ADS Sources

Search Filter :

☐ Install eScan client automatically

Select eScan Installation Options:

☐ Install Without Firewall

\*AD sync will not add the computers that are already present in any of the groups under Managed computers. Check "eScan\log\ADSync.log" for more details.

### Source Active Directory Organization Unit

Click **Browse** and select an Active Directory.

### Synchronization Interval

Enter the preferred duration (in minutes).

### Exclude from ADS Sync

This field displays a list of excluded Active Directory sources.

To delete a source, select the checkbox **Excluded ADS Sources**. Select a source(s) and then click **Delete**.

To exclude a source, select the source and then click **Add to Exclude**.

### **Search Filter**

It lets you search an Active Directory for an object class.

### **Install eScan manually**

Selecting this option lets you install eScan manually on the computers.

### **Install without Firewall**

Selecting this option lets you install eScan without firewall.

3. After performing the necessary actions, click **OK**.  
The group will be synchronized with the Active Directory.

## Outbreak Prevention

Upon virus detection, eScan quarantines the virus and restricts it from spreading across the network. The Outbreak Prevention feature lets you configure policies for the network.

### Deploying Outbreak Prevention

To deploy Outbreak Prevention feature, follow the steps given below:

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

### Limit access to shared folders

Select this checkbox to limit the infection's access to shared folders.

### Deny write access to local files and folder

Select this checkbox to deny the infection write access for any file. Clicking the link displays another window that lets you specifically select folders and subfolders that should be denied and allowed access for modification.

### Block specific ports

Select this checkbox to prevent infection from accessing specific ports. Clicking the link displays another window that lets you block incoming and outgoing data packets along with TCP and UDP ports.

### Block All Ports (Other than trusted client-server ports)

Select this checkbox to block all ports other than trusted client server ports.

### Automatically restore the outbreak prevention after hour(s)

This feature lets you restore outbreak prevention automatically after set duration (hours). Click the drop-down and select the preferred duration.

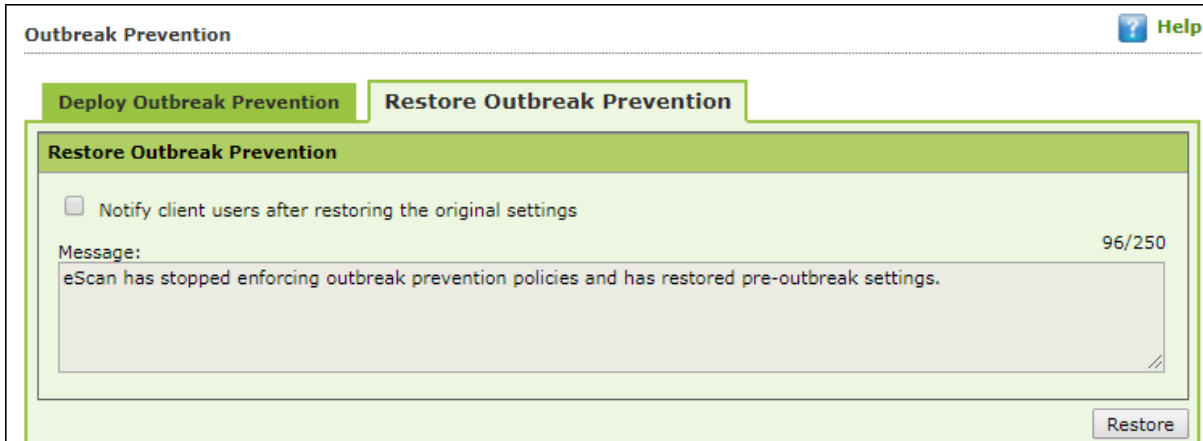
### Outbreak Prevention Notification

To send a notification to client users after Outbreak Prevention is deployed, select the checkbox **Notify client users when outbreak prevention starts**. You can even write your own custom message for this feature in the Message field.

After making the necessary selections, click **Deploy**. The Outbreak Prevention feature will be deployed for the selected group.

## Restore Outbreak Prevention

In the Outbreak Prevention window, click **Restore Outbreak Prevention** tab.



The screenshot shows the 'Outbreak Prevention' window with a 'Help' icon in the top right. There are two tabs: 'Deploy Outbreak Prevention' and 'Restore Outbreak Prevention'. The 'Restore Outbreak Prevention' tab is active. Inside this tab, there is a checkbox labeled 'Notify client users after restoring the original settings'. Below the checkbox is a text area for a message, with a character count '96/250'. The message text reads: 'eScan has stopped enforcing outbreak prevention policies and has restored pre-outbreak settings.' At the bottom right of the window is a 'Restore' button.

To restore Outbreak Prevention manually, click **Restore**.

To notify clients about Outbreak Prevention restoration, select the checkbox **Notify client users after the original settings**.



## 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.

The 'Create Client Setup' dialog box has a title bar with a 'Help' button. Below the title bar is a section titled 'Setup Settings' with a green header. Inside this section are two checkboxes: 'Add Policy' and 'Auto add to group'. At the bottom of the dialog are two buttons: 'Create Setup' and 'Cancel'.

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

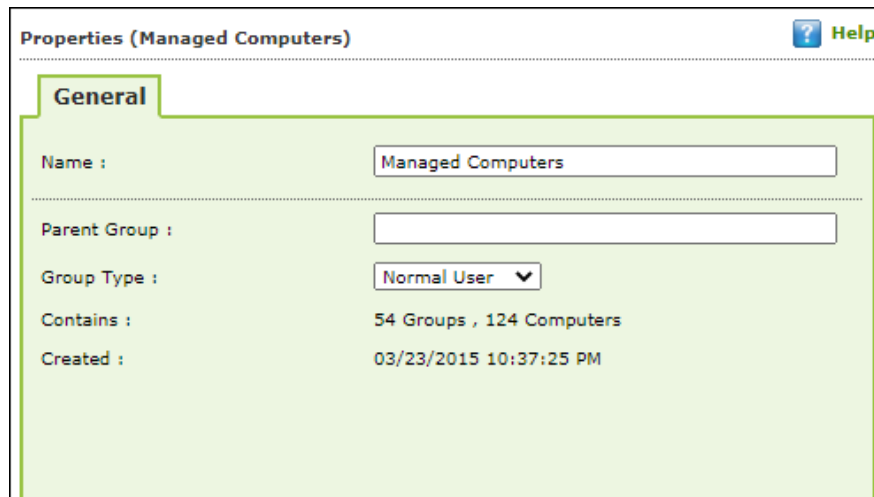
Name		Download Client Setup
	Policy	
	Group Tasks	
	Client Computers	
Group Information		
AD Sync		Not Configured
Total Subgroups		1
Total Computers		3

## 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.



The screenshot shows a window titled "Properties (Managed Computers)" with a "Help" button in the top right corner. The "General" tab is selected and highlighted. The tab contains the following fields and values:

Field	Value
Name :	Managed Computers
Parent Group :	
Group Type :	Normal User
Contains :	54 Groups , 124 Computers
Created :	03/23/2015 10:37:25 PM

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

- Group Name
- Parent Group
- Group Type – Normal or Roaming User
- Sub Groups or Number of Computers in that Group
- Creation date of the Group

# Group Tasks

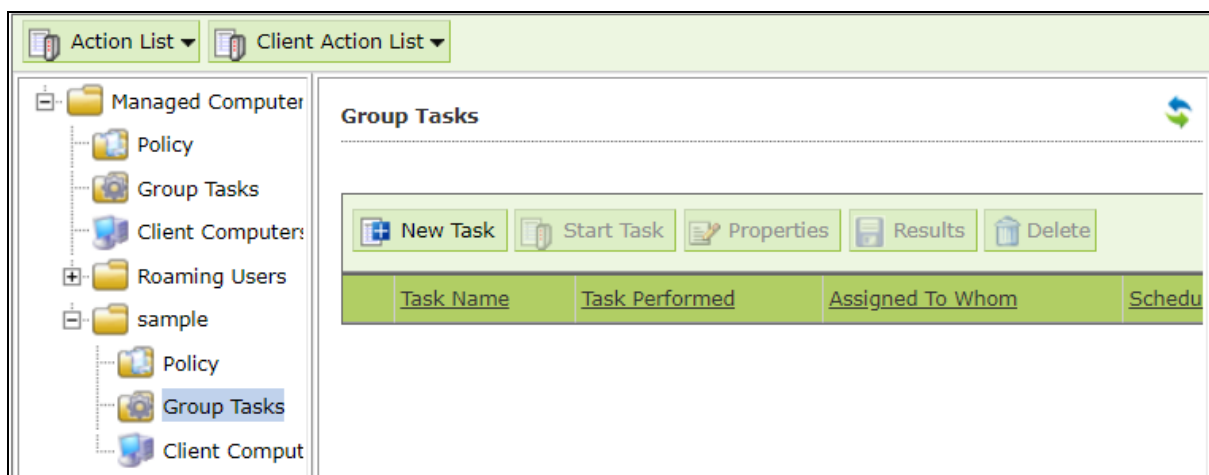
With the **Group Tasks** option, you can create a task, start a task, select a task and view its properties, view task results as well as delete an already created task. Tasks can include the following.

- Enable/Disable desired Module
- Set Update Server
- Scheduling Scan on Networked Computers

## Creating a Group Task

To create a Group Task, follow the steps given below:

1. Select a group.
2. In group's folder tree, click **Group Tasks**.
3. In the Group Tasks pane, click **New Task**.



New Task Template window appears. This window lets you define Task Name, assign a task as well as schedule a task on computers.

4. Enter the Task Name and configure the desired task settings.



5. Click **Save**. The selected group will be assigned a task template.

## Managing a Group Task

Selecting a Group Task enables **Start Task**, **Properties**, **Results** and **Delete** buttons.

Group Tasks				
<a href="#">New Task</a> <a href="#">Start Task</a> <a href="#">Properties</a> <a href="#">Results</a> <a href="#">Delete</a>				
Task Name	Task Performed	Assigned To Whom	Schedule Type	Task Status
<input checked="" type="checkbox"/> security	Not Performed Yet	'Managed Computers'	Automatic Scheduler	

### Start Task

To start a task manually, select a task and then click **Start Task**.

### Delete Task

To delete a task, select a task and then click **Delete**.

### Properties

To view the properties of a task, select a task and then click **Properties**. It also lets you modify or redefine the entire settings configured. After making the necessary changes, click **Save**. The properties for the group task will be saved and updated.

security

General

Schedule

Settings

Task Name

security

Task Creation Time:

05/28/20 06:10:59 PM

Status:

Task not performed yet

Last Run:

Save

Close

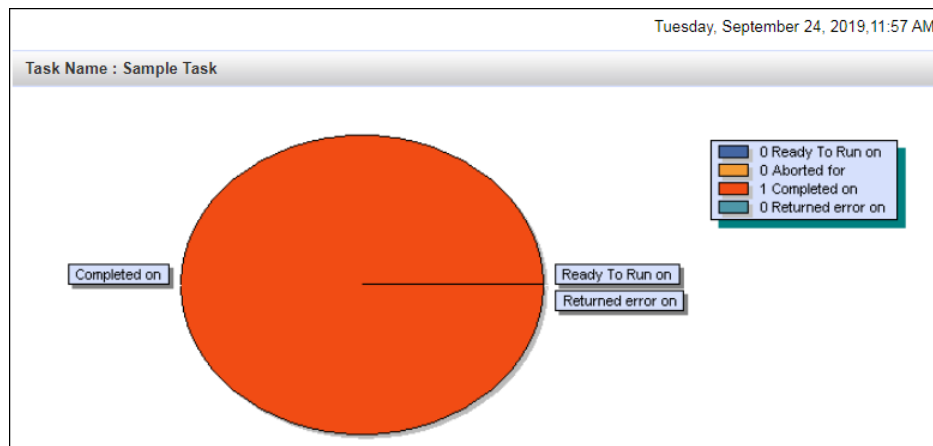
### Results

To view the results of a completed task, select a task and then click **Results**.

Task Results (Sample Task)			
Group Tasks > Task Results			
Client Computers	Group	Status	Time
	Managed Computers\Sample Group	Completed	09/24/19 11:52:29 AM

## Task Status

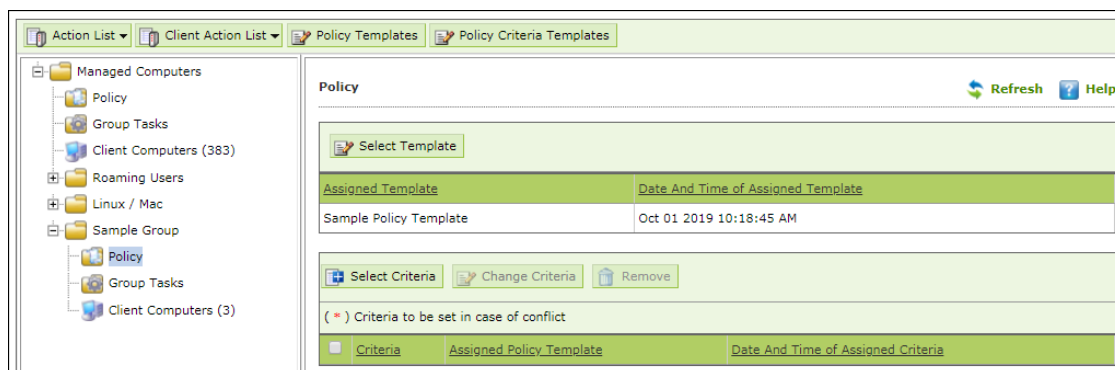
To view the status, select a task and then click **Task Status**. A brief task summary is displayed.



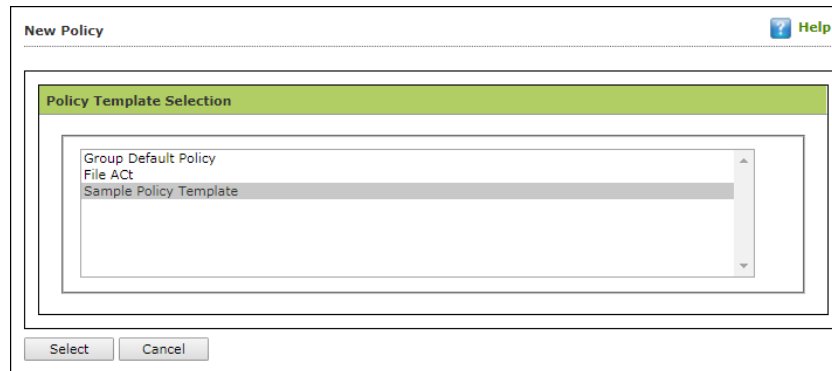
## Assigning a Policy to the group

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

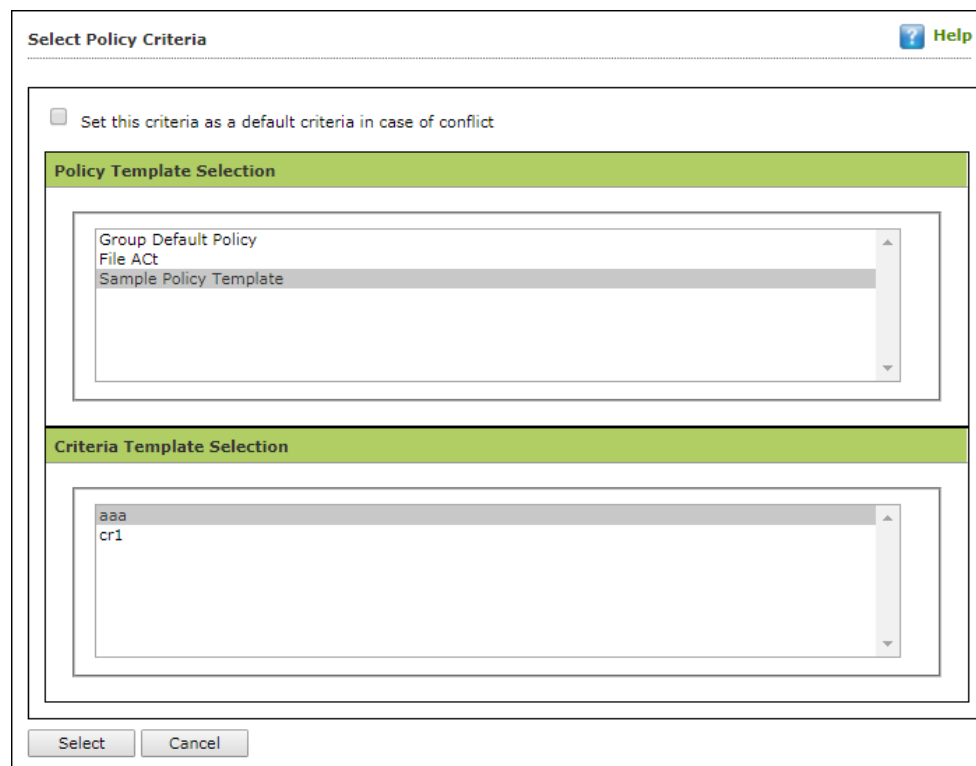
1. In the Managed Computers folder tree, select a group.
  2. Under the group name, click **Policy**.
- Policy pane appears on the right side.



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



7. Select a policy template and then click **Select**.
8. To assign criteria to group, click **Select Criteria**.  
Select Policy Criteria window appears.



9. If a computer falls under both conditions created by you, it will create a conflict. To avoid such conflict, select the checkbox **Set this criteria as a default criteria in case of conflict**. Then select the Policy Template and Criteria Template to be used in case of conflict.
10. Click **Select**. The default Policy Template and Criteria Template for group will be saved and updated.



## 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:

- **Set Host Configuration**
- **Deploy/Upgrade Client**
- **Uninstall eScan Client**
- **Move to Group**
- **Remove from Group**
- **Connect to Client RMM**
- **Add to RMM License**
- **Manage Add-on License**
- **Export**
- **Show Installed Softwares**
- **Force Download**
- **Send Message**
- **Outbreak Prevention**
- **Delete All Quarantine Files**
- **Create OTP**
- **Pause Protection**
- **Resume Protection**
- **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).

<b>NOTE</b>	Some options vary based on issue of License
-------------	---

## Set Host Configuration

If you are unable to view details of Windows OS installed computer with **Properties** option, set its **Host Configuration**. Doing so will build communication between the server and selected computer, displaying its details.

To set Host Configuration for a selected computer, follow the steps given below:

1. Select the computer.
2. Click **Client Action List > Set Host Configuration**.

Set Host Configuration window appears.



The image shows a 'Set Host Configuration' dialog box. It has a title bar with the text 'Set Host Configuration'. Below the title bar is a green header section with the text 'Login Information'. The main area contains four input fields: 'Computer Name:' with a dropdown menu showing 'localhost', 'Remarks:' with an empty text box, 'User name:' with a text box containing 'Administrator', and 'Password:' with an empty text box. At the bottom of the dialog box is a green footer section with the text 'Note: If Host Name is in another Domain, Please mention Domain Name Ex. Domain1\HostName'. Below the footer are two buttons: 'Save' and 'Cancel'.

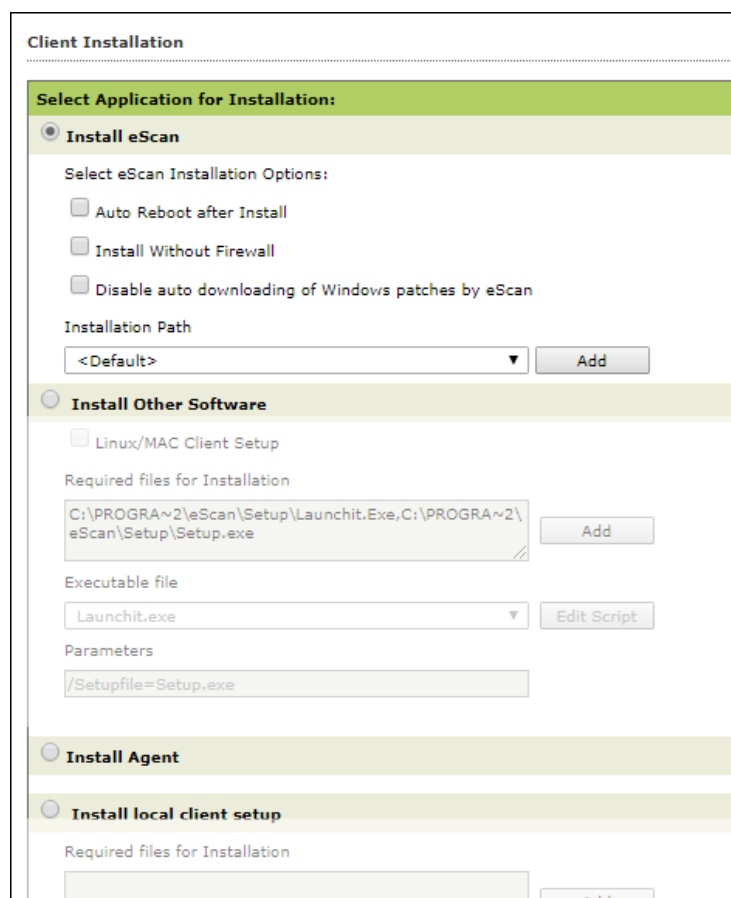
3. Enter Remarks and login credentials.
  4. Click **Save**.
- The Host will be configured as per new settings.

## Deploy/Upgrade Client

To Deploy/Upgrade eScan client on selective computers in a group or an individual computer, follow the steps given below:

### Installing eScan Client on a Client Computer

1. Select a client computer within a group to install eScan client.
2. Click **Client Action List > Deploy/Upgrade Client**. Client Installation window appears.



The screenshot shows the 'Client Installation' window. It has a title bar 'Client Installation'. Below it is a section 'Select Application for Installation:' with three radio buttons: 'Install eScan' (selected), 'Install Other Software', and 'Install Agent'. Under 'Install eScan', there are three checkboxes: 'Auto Reboot after Install', 'Install Without Firewall', and 'Disable auto downloading of Windows patches by eScan'. Below these is an 'Installation Path' section with a dropdown menu showing '<Default>' and an 'Add' button. Under 'Install Other Software', there is a checkbox for 'Linux/MAC Client Setup'. Below that is a 'Required files for Installation' section with a text box containing 'C:\PROGRA~2\eScan\Setup\Launchit.Exe,C:\PROGRA~2\eScan\Setup\Setup.exe' and an 'Add' button. Below that is an 'Executable file' section with a dropdown menu showing 'Launchit.exe' and an 'Edit Script' button. Below that is a 'Parameters' section with a text box containing '/Setupfile=Setup.exe'. Under 'Install Agent', there is a checkbox for 'Install local client setup'. Below that is a 'Required files for Installation' section with a text box and an 'Add' button.

3. Select **Install eScan** option.  
By Default eScan is installed at the following Path on a Client computer.  
C:\Program Files\eScan (default path for 32-bit computer)  
OR  
C:\Program Files (x86)\eScan (default path for 64-bit computers).
4. To define a different installation path, click **Add**. (Skip this step if default path chosen).
5. Click **Install**.

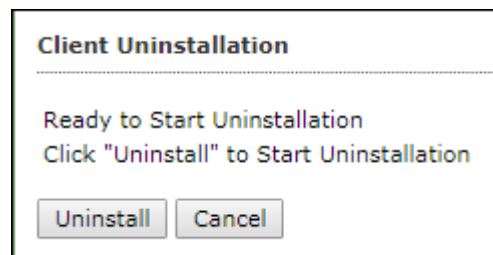
A window displays File transfer progress. After Installation, the eScan status will be updated in Managed Computers list.

## Uninstall eScan Client

To uninstall eScan Client on any computer, follow the steps given below:

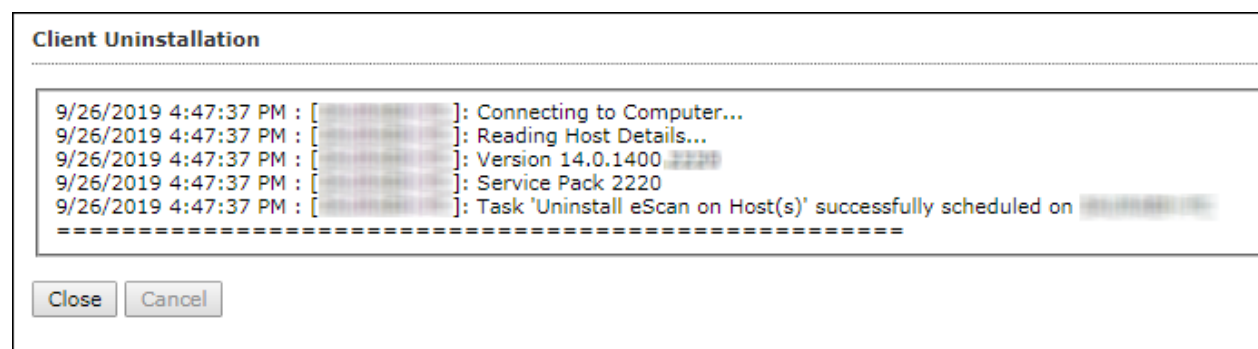
1. Select the computer for uninstallation.
2. Click **Client Action List > Uninstall eScan Client**.

Client Uninstallation window appears.



3. Click **Uninstall**.

The Client Uninstallation window displays the progress.



4. After the uninstallation process is over, click **Close**.

<b>NOTE</b>	You can uninstall eScan Client from all the computers in the group by selecting the Group and then Click <b>Action List &gt; Uninstall eScan Client</b> .
-------------	---

## 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.


## Connect to Client (RMM)

To connect to client via RMM service, follow the steps given below:

1. Go to **Managed Computers**.
2. Select the client computer for which you want to take remote connection.
3. Click **Client Action List > Connect to Client (RMM)**.  
RMM disclaimer appears.
4. Click **Accept**.  
You will get connected to the client computer via RMM service. Read more about RMM configuration.

## Add to RMM License

To add a computer to RMM licensed category, follow the steps given below:

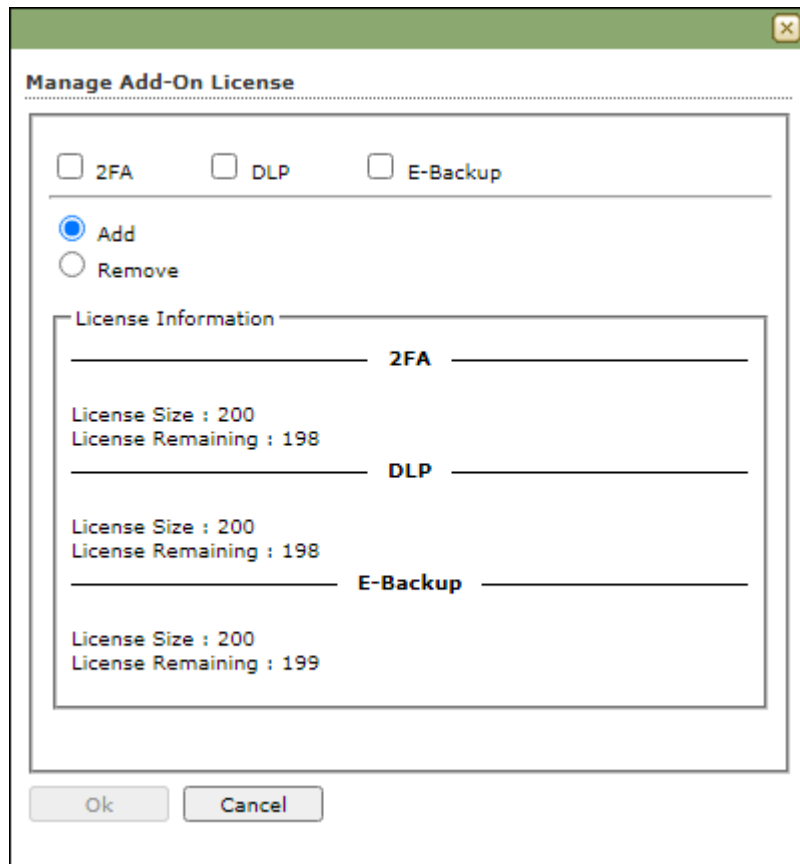
1. Go to **Managed Computers**.
2. Select the client computer which you want to add to RMM License.
3. Click **Client Action List > Add to RMM License**.  
RMM disclaimer appears.
4. Read the disclaimer thoroughly as this action is irreversible. To proceed, click **OK**.  
The endpoint gets added to RMM license. After adding the endpoint to RMM license  icon appears next to the RMM enabled endpoints.

<b>NOTE</b>	After adding a client endpoint to RMM license, it is mandatory that the client endpoint should be updated with latest eScan updates.
-------------	--

## Manage Add-On License

To manage add-on licenses, follow the steps given below:

1. Go to **Managed Computers**.
2. Select the client computer which you want to manage 2FA, DLP, and E-Backup Licenses.
3. Click **Client Action List > Manage Add-On License**.
4. Manage Add-On License window appears.



The screenshot shows a dialog box titled "Manage Add-On License". At the top, there are three checkboxes: "2FA", "DLP", and "E-Backup", all of which are currently unchecked. Below these is a section with two radio buttons: "Add" (which is selected) and "Remove". Underneath the radio buttons is a section titled "License Information" which contains three rows of data. Each row corresponds to one of the license types (2FA, DLP, and E-Backup) and shows the "License Size : 200" and the "License Remaining" value. For 2FA and DLP, the remaining value is 198, and for E-Backup, it is 199. At the bottom of the dialog box are "Ok" and "Cancel" buttons.

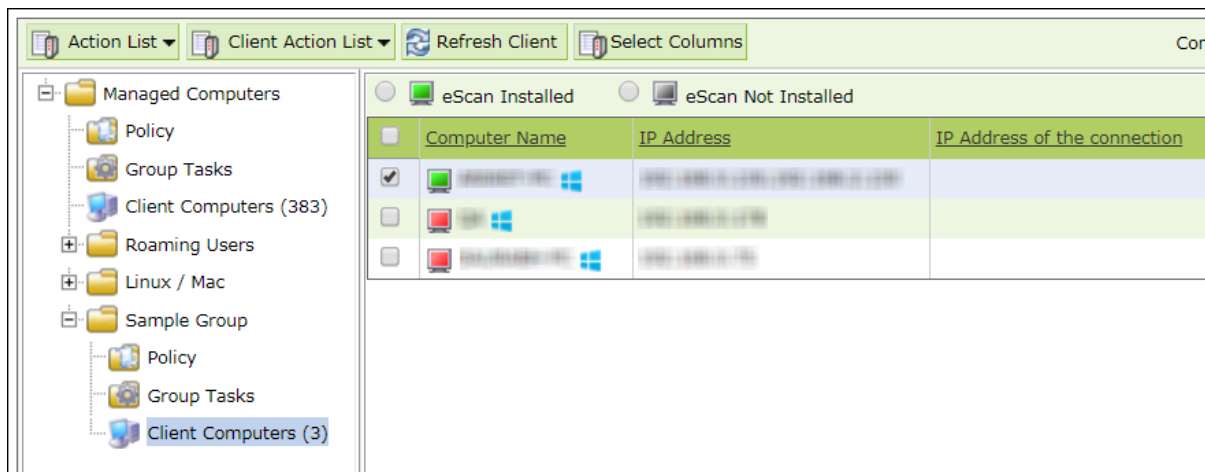
5. Select **Add** to add a client computer to 2FA, DLP, and E-Backup licenses or **Remove** to remove the added client computer and then click **OK**.  
The computer gets added or removed from 2FA, DLP, and E-Backup licenses as per your preferred option.

## Export

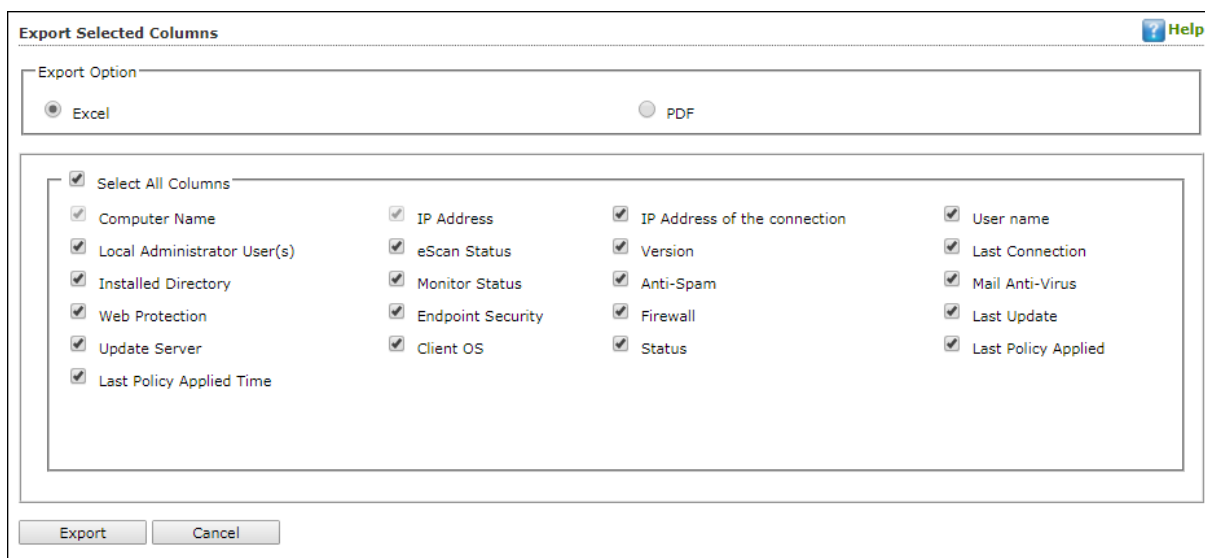
To export a client computer's data, follow the steps given below:

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.



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.



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



The report will be exported as per your preferences.



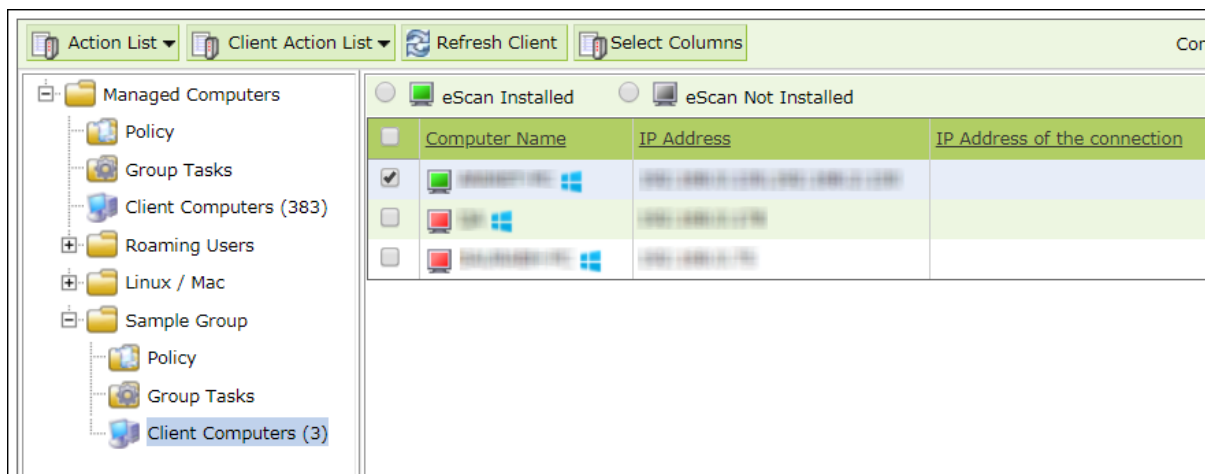
## Show Installed Softwares

This feature displays a list of installed softwares on a computer.

To view the list of installed softwares, follow the steps given below:

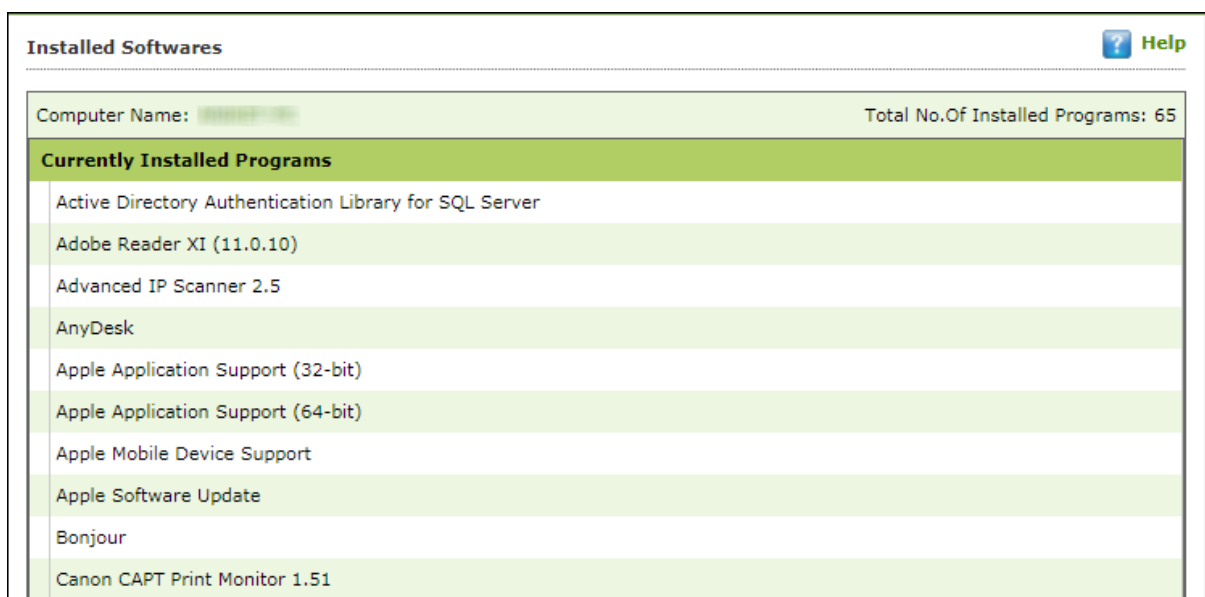
1. In the Managed Computers folder tree, select a group and then click **Client Computers**.

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.



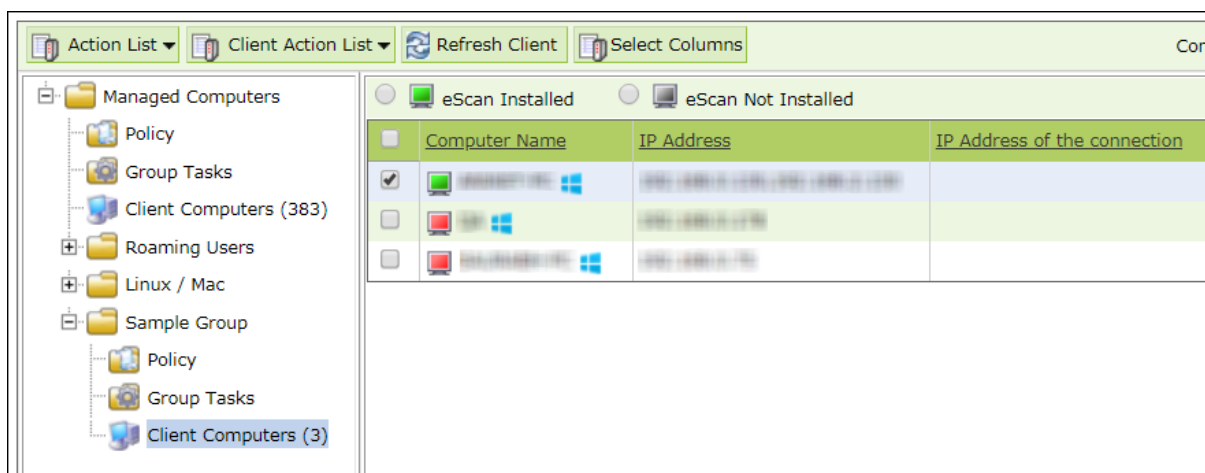
## Force Download

The Force Download feature forces a client computer to download Policy Template modifications (if any) and updated virus signature database.

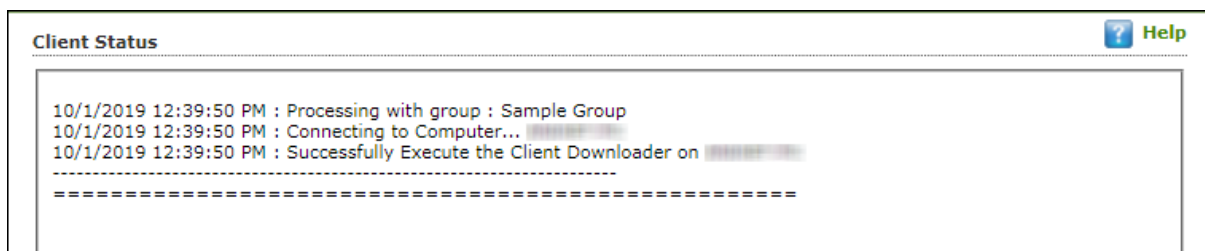
To activate this feature for computers, follow the steps given below:

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 client computers and then click **Client Action List > Force Download**. Client Status window appears displaying the process.

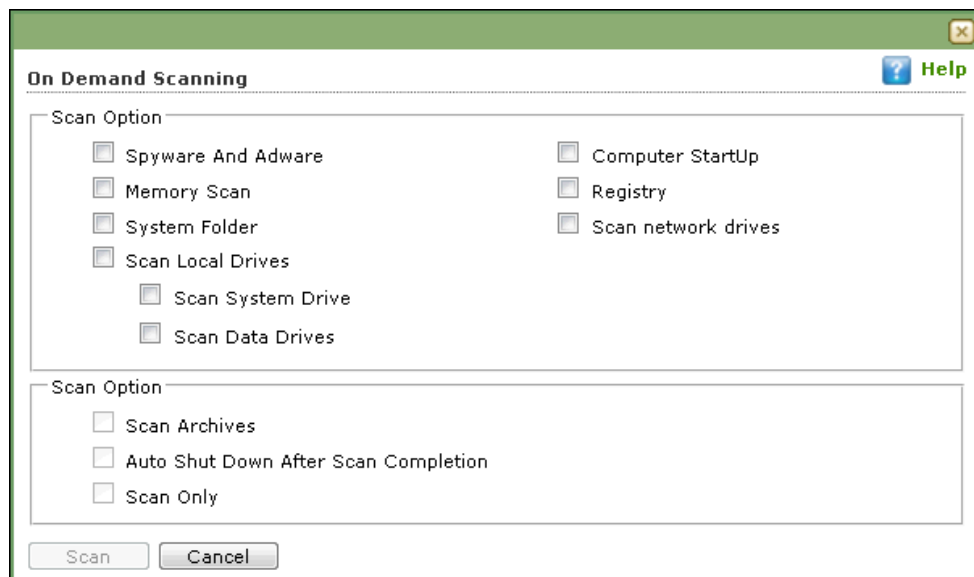


## On Demand Scanning

This option lets you scan a eScan installed client computer. To scan a client computer on demand, follow the steps given below:

1. Go to **Managed Computers**.
2. Select the client computer which you want to scan.
3. Click **Client Action List > On Demand Scanning**.

On Demand Scanning window appears.



4. Select the preferred scan options and then click **Scan**.  
The On Demand Scan for selected client computer begins.

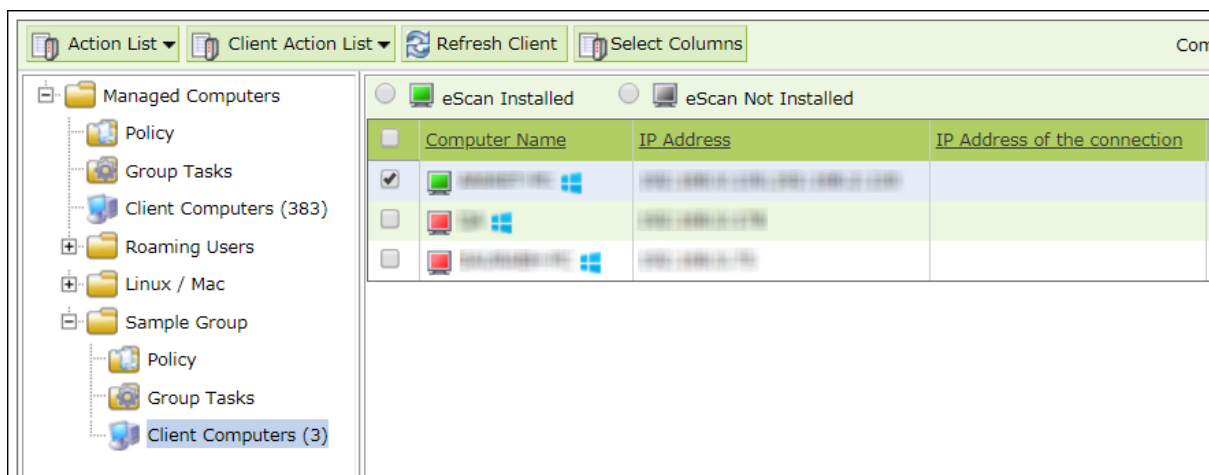
## Send Message

The Send Message feature lets you send a message to computers.

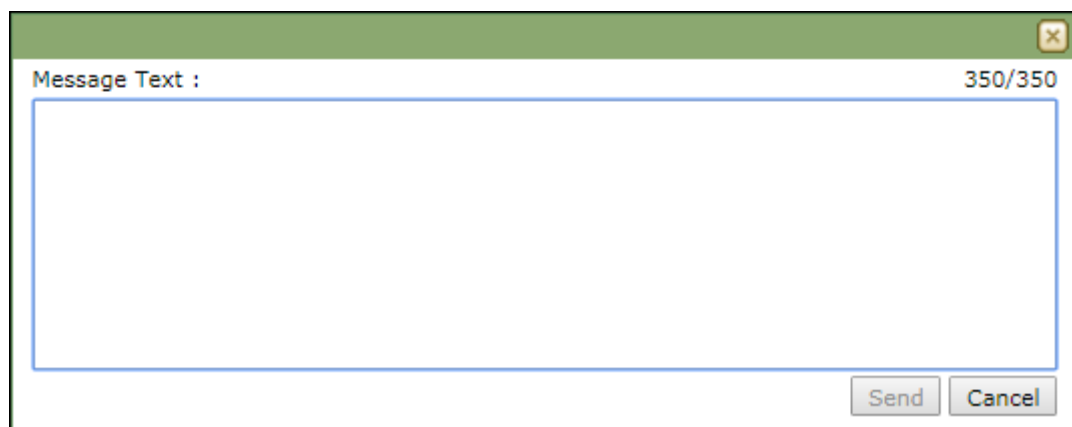
To send message to computers, follow the steps given below:

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 client computers and then click **Client Action List > Send Message**. Send Message window appears.



3. Enter the message and click **Send**. The message will be sent to the selected computers.

## Outbreak Prevention

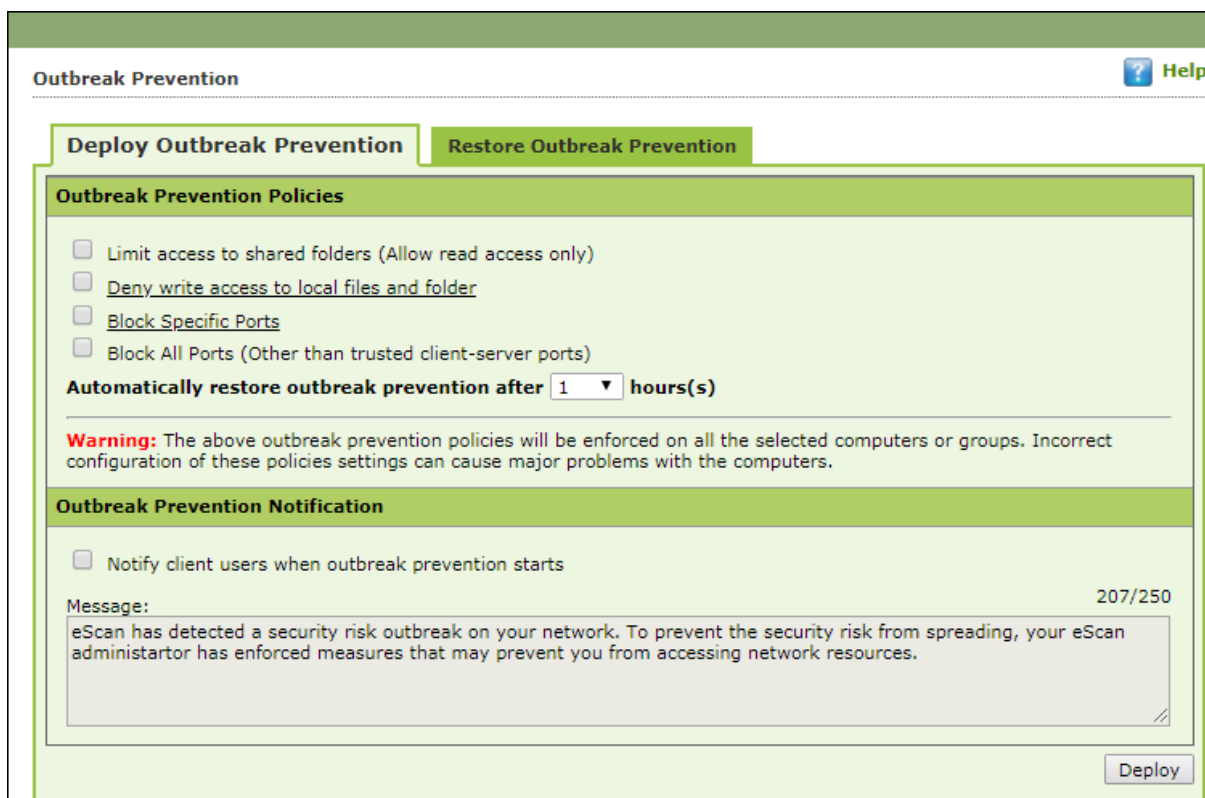
Upon virus detection, eScan quarantines the virus and restricts it from spreading across the network. The Outbreak Prevention feature lets you configure policies for the network.

### Deploying Outbreak Prevention

To deploy Outbreak Prevention feature for specific client computer(s), follow the steps given below:

1. Go to **Managed Computers**.
2. Select the computer(s) for which you want to deploy Outbreak Prevention.
3. Click **Client Action List > Outbreak Prevention**.

Outbreak Prevention window appears.



#### Limit access to shared folders

Select this checkbox to limit the infection's access to shared folders.

#### Deny write access to local files and folder

Select this checkbox to deny the infection write access for any file. Clicking the link displays another window that lets you specifically select folders and subfolders that should be denied and allowed access for modification.

### Block specific ports

Select this checkbox to prevent infection from accessing specific ports. Clicking the link displays another window that lets you block incoming and outgoing data packets along with TCP and UDP ports.

### Block All Ports (Other than trusted client-server ports)

Select this checkbox to block all ports other than trusted client server ports.

### Automatically restore the outbreak prevention after hour(s)

This feature lets you restore outbreak prevention automatically after set duration (hours). Click the drop-down and select the preferred duration.

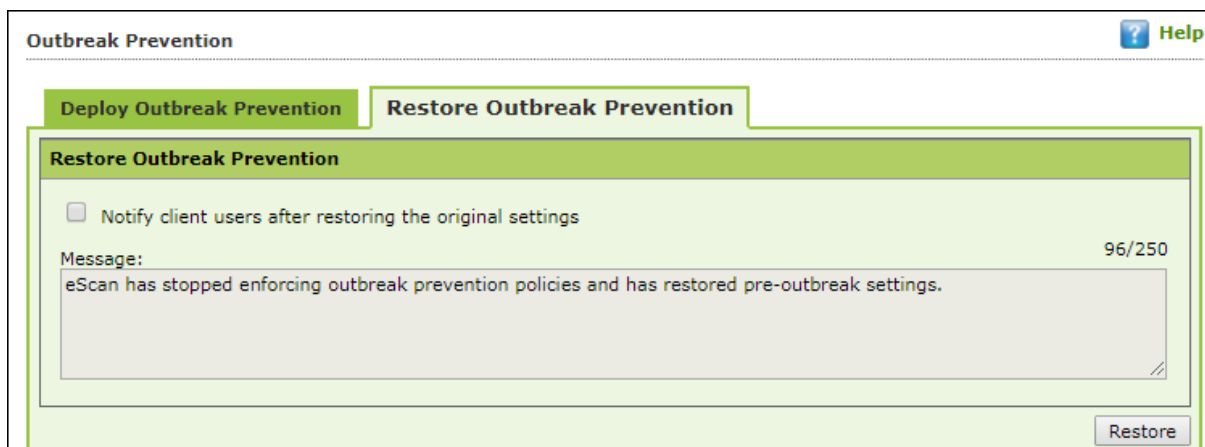
### Outbreak Prevention Notification

To send a notification to client users after Outbreak Prevention is deployed, select the checkbox **Notify client users when outbreak prevention starts**. You can even write your own custom message for this feature in the Message field.

After making the necessary selections, click **Deploy**. The Outbreak Prevention feature will be deployed for the selected group.

## Restore Outbreak Prevention

In the Outbreak Prevention window, click **Restore Outbreak Prevention** tab.



The screenshot shows the 'Outbreak Prevention' window with the 'Restore Outbreak Prevention' tab selected. The window has a title bar with 'Outbreak Prevention' and a 'Help' button. Below the title bar are two tabs: 'Deploy Outbreak Prevention' and 'Restore Outbreak Prevention'. The 'Restore Outbreak Prevention' tab is active and contains a green header bar with the same text. Below the header bar is a checkbox labeled 'Notify client users after restoring the original settings'. To the right of the checkbox is a character count '96/250'. Below the checkbox is a text area with the message: 'eScan has stopped enforcing outbreak prevention policies and has restored pre-outbreak settings.' At the bottom right of the window is a 'Restore' button.

To restore Outbreak Prevention manually, click **Restore**.

To notify clients about Outbreak Prevention restoration, select the checkbox **Notify client users after the original settings**.

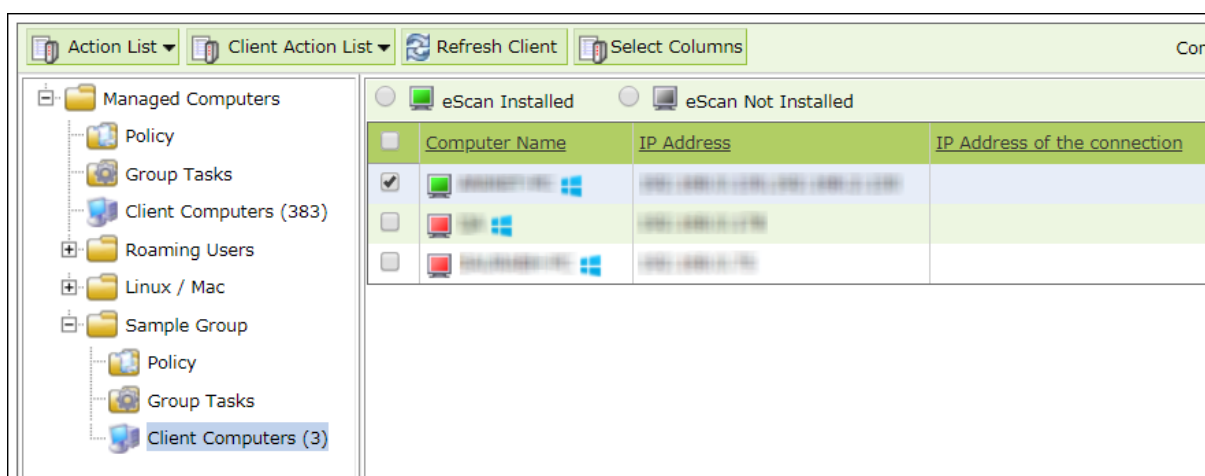
## Delete All Quarantine Files

The Delete All Quarantine Files feature lets you delete all quarantine files stored on a computer.

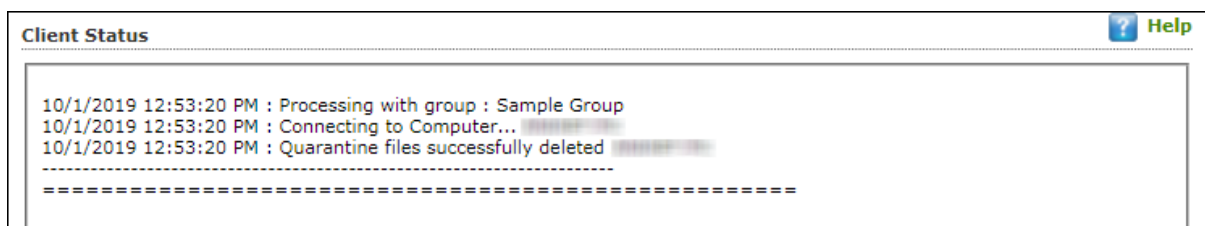
To delete all quarantine files on computers, follow the steps given below:

1. In the Managed Computers folder tree, select a group and under it click **Client Computers**.

The right pane displays the list of computers in the group and their detailed information.



2. Select client computers and then click **Client Action List > Delete All Quarantine Files**. Client Status window appears displaying the progress.



## 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.

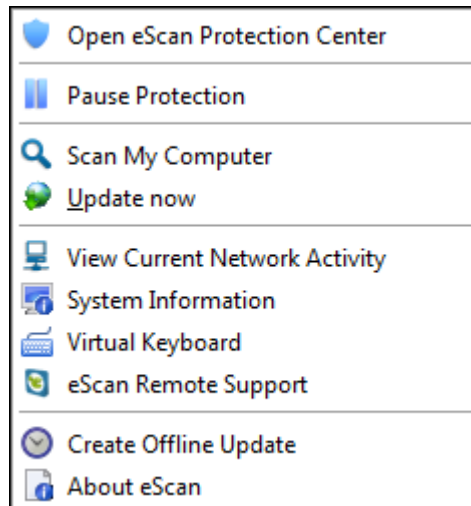
1. In the **Valid for** drop-down, select the preferred duration to bypass the protection module.
2. In Select Option section, select the module you want to disable.
3. Click **Generate Password**. An OTP will be generated and displayed in **Password** field.



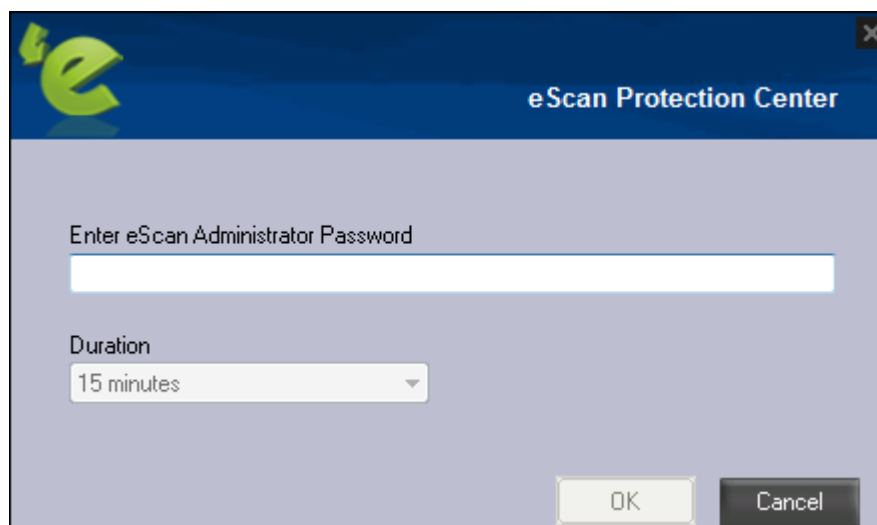
## Entering an OTP

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.

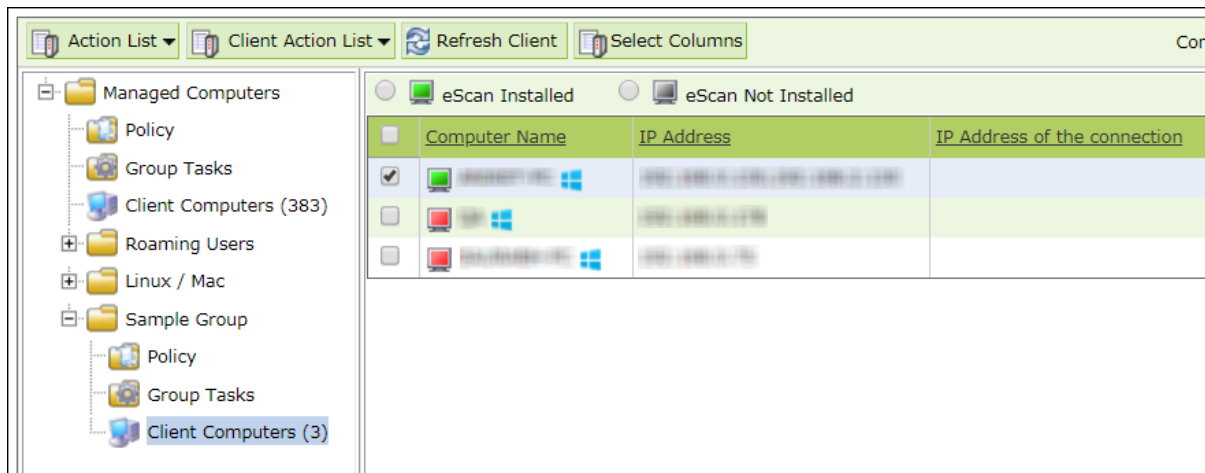
## Pause Protection

The Pause Protection feature lets you pause the protection for computers.

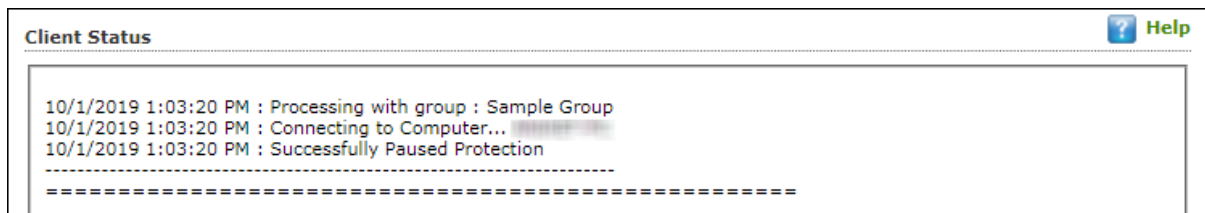
To pause the protection for computers, follow the steps given below:

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 client computers and then click **Client Action List > Pause Protection**. Client Status window appears displaying the progress.



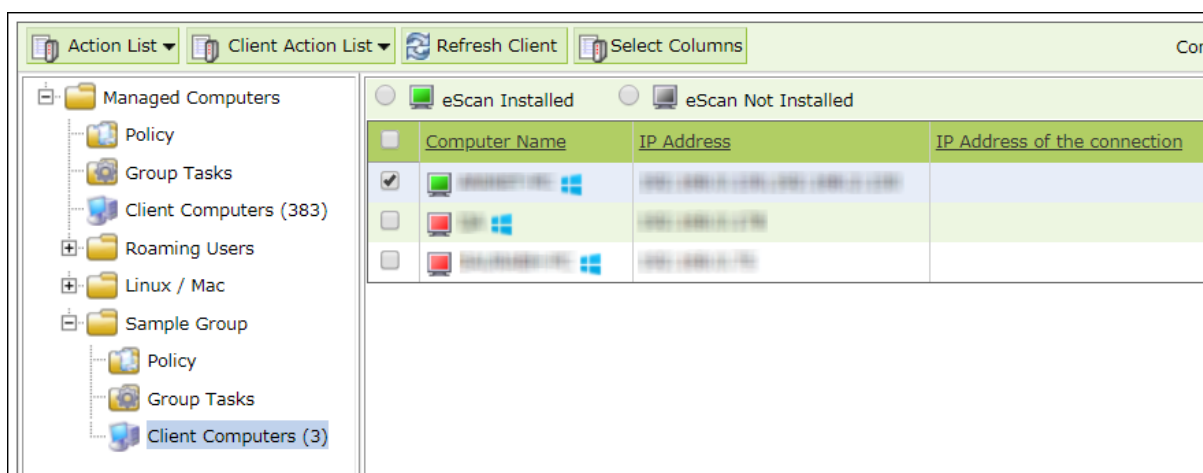
## Resume Protection

The Resume Protection feature lets you resume protection for computers whose protection is paused.

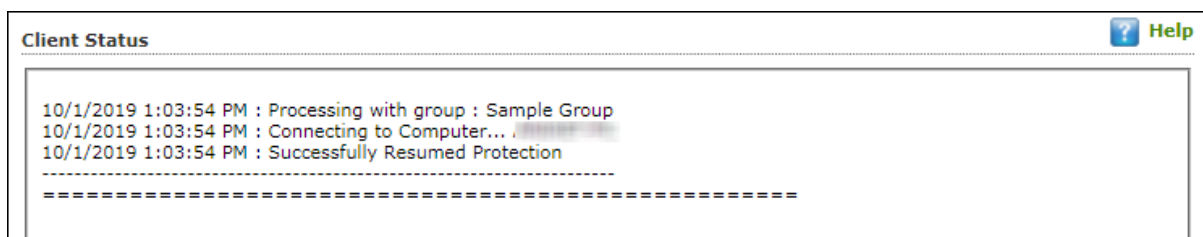
To resume protection for computers, follow the steps given below:

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 client computers and then click **Client Action List > Resume Protection**. Client Status window appears displaying the progress.



## 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.

The screenshot shows a 'Properties' window with a green header bar and a 'Help' button. The window is divided into three main sections: General, AV-Status, and Protection.

General	
Computer Name	XXXXXXXXXX
IP Address	192.168.1.100
User name	XXXXXXXXXX
Operating System	Windows 7 (64-bit)

AV-Status	
Anti-Virus Installed	eScan installation aborted
Version	14.0.1400.0000
Installed Directory	C:\Program Files (x86)\eScan\
Update Server	XXXXXXXXXX
Last Update	2019/09/18 09:31

Protection	
File Anti-Virus	Enabled
Mail Anti-Virus	Disabled
Anti-Spam	Disabled
Web Protection	Disabled
Firewall	Disabled (Allow All)
Endpoint Security	Enabled

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

# 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 Windows computers

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

#### File Anti-virus

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

#### Mail Anti-Virus

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

#### Anti-Spam

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

#### Firewall

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

#### Privacy Control

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

#### Web Protection

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

#### Endpoint Security



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

## Defining Policies Mac or Linux computers

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

### File Anti-Virus

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

### Endpoint Security

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

### On Demand Scanning

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

### Schedule Scan

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

### Schedule Update

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

### Administrator Password

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

### Web Protection

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

<b>NOTE</b>	Priority will be given to Policy assigned through <b>Policy Criteria</b> 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.

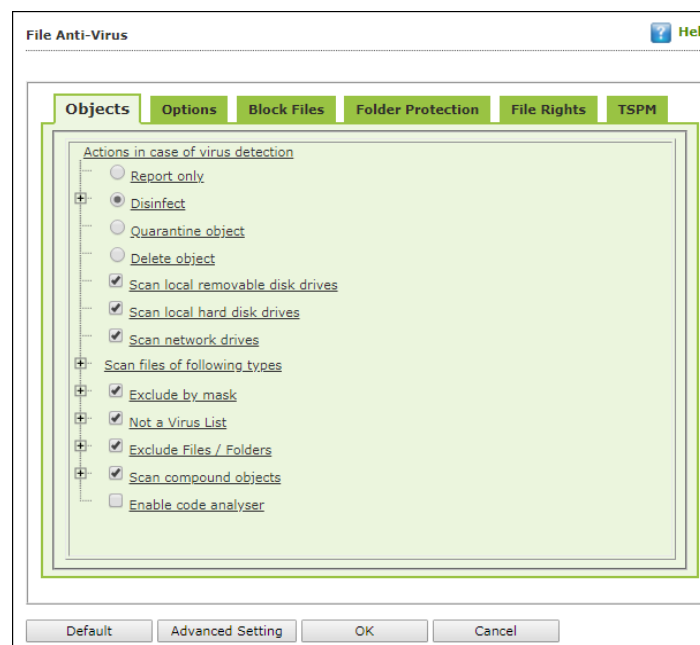
## File Anti-Virus

Editing File Anti-Virus module displays following tabs:

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

### Objects

The Objects tab lets you configure following options.



### Actions in case of virus detection

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

#### Report Only

Upon virus detection, eScan will only report the virus and won't take any action.

**Disinfect** and **If disinfection is impossible** it will **Quarantine Object** or **Delete Object**"

Out of these, the **Disinfect** option is selected by default. By default, the quarantined files are saved in **C:\Program Files\eScan\Infected folder**. You can select the **Make backup file before disinfection** option if you would like to make a backup of the files before they are disinfected.

#### **Scan local removable disk drives [Default]**

Select this option if you want eScan to scan all the local removable drives attached to the computer.

#### **Scan local hard disk drives [Default]**

Select this option if you want eScan to scan all the local hard drives installed on the computer.

#### **Scan network drives [Default]**

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

#### **Scan files of following types**

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

#### **Exclude by mask [Default]**

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

#### **Not a virus list [Default]**

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

#### **Exclude Files/Folders [Default]**

Select this check box if you want File Anti-Virus to exclude all the listed files, folders, and sub folders while it is monitoring or scanning folders. The files/folders added to this list

will be excluded from only real-time scan as well as on demand scan. You can add or delete files/folders from the list of by clicking **Add/Delete**.

### Scan compound objects [Default]

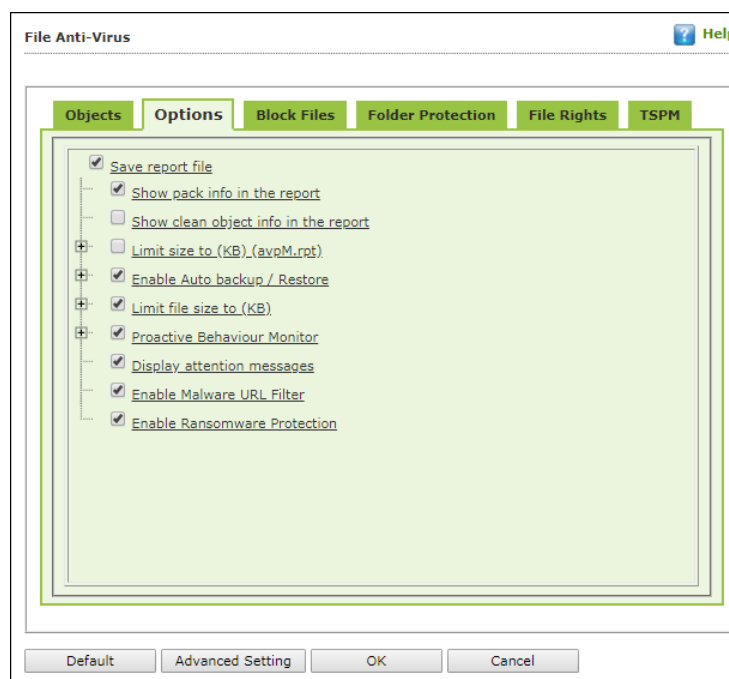
Select this check box if you want eScan to scan archives and packed files during scan operations. By default, **Packed** is selected.

### Enable code Analyzer

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

## Options

The Options tab lets you configure following options:



### Save report file [Default]

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

### Show pack info in the report [Default]

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

**Show clean object info in the report**

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

**Limit size to (Kb) (avpM.rpt)**

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

**Enable Auto backup/Restore [Default]**

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

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

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

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

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

**Limit file size to (KB) [Default]**

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

**Proactive Behavior Monitor**

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

**Whitelist Option**

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

**Use sound effects for the following events**

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

### **Display attention messages [Default]**

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

### **Enable Malware URL Filter**

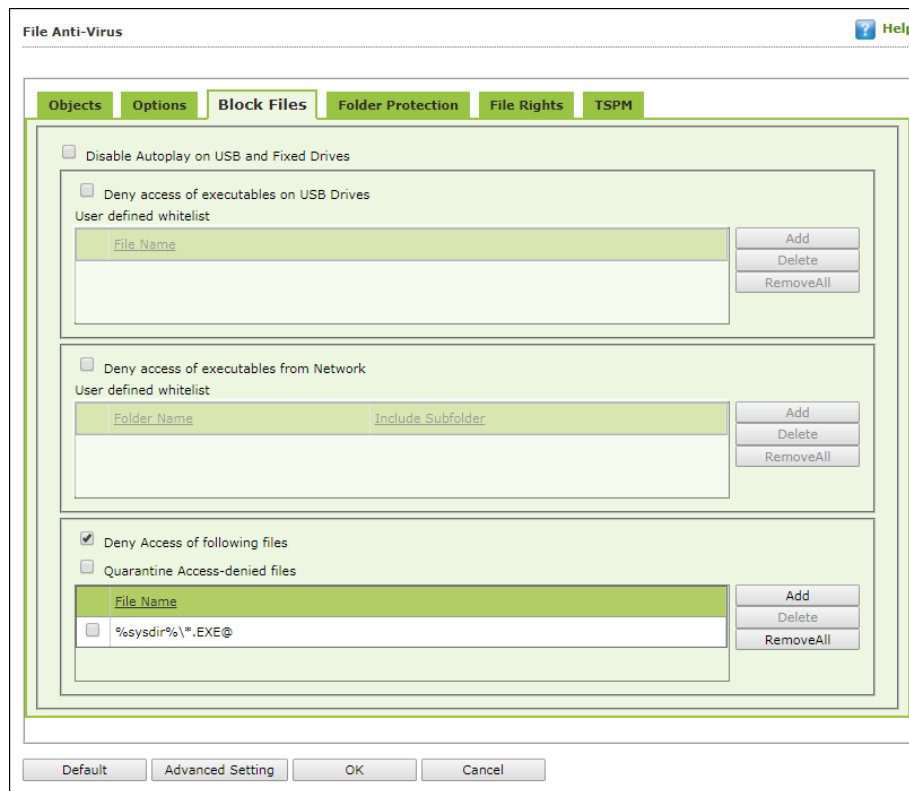
This option lets you enable a Malware URL filter where eScan blocks all URLs that are suspected to be malwares. You can exclude specific websites by whitelisting them from the eScan pop up displayed when you try to access the site.

### **Enable Ransomware Protection**

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

## **Block Files**

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



You can configure the following settings:

### **Disable AutoPlay on USB and Fixed Drives [Default]**

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

### **Deny access of executables on USB Drives**

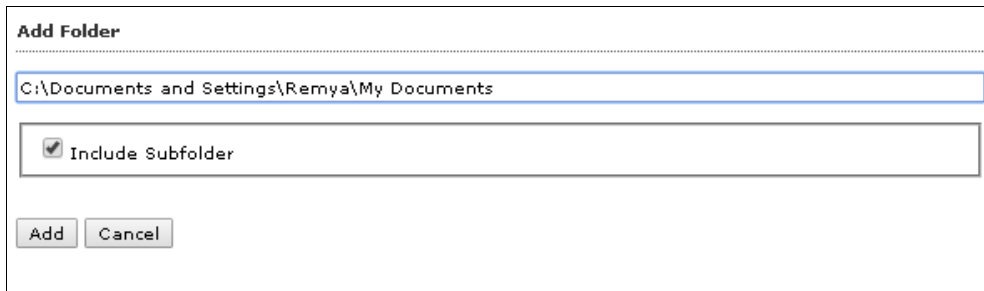
Select this check box if you want eScan to prevent executables stored on USB drives from being accessed.

### **Deny access of executable from Network**

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

### **User defined whitelist**

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



The 'Add Folder' dialog box contains a text input field with the path 'C:\Documents and Settings\Remya\My Documents'. Below the text field is a checkbox labeled 'Include Subfolder' which is checked. At the bottom of the dialog are two buttons: 'Add' and '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 check box if you want eScan to prevent the files in the list from running on the computers.

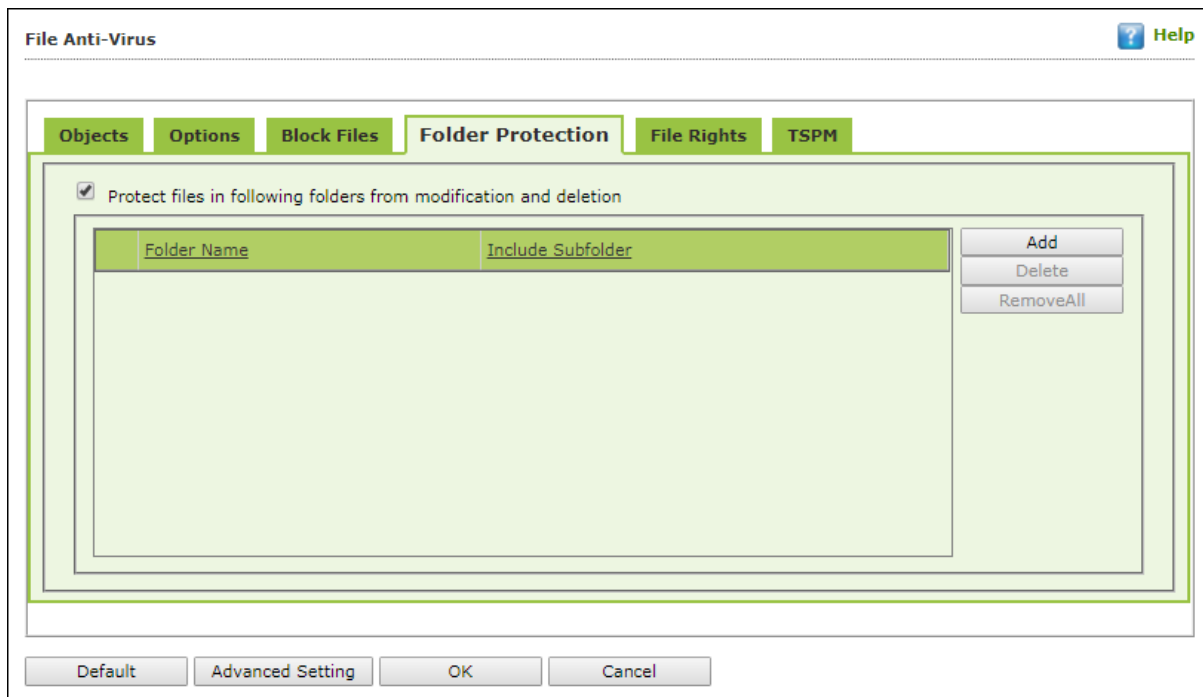
### Quarantine Access-denied files

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

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

## Folder Protection

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



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

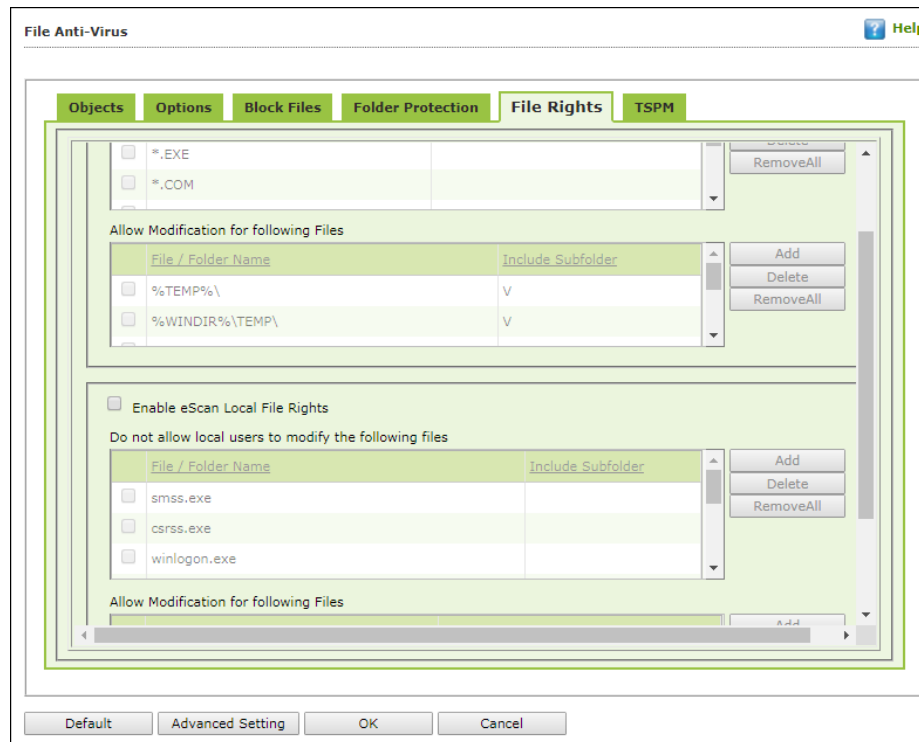
This option is selected by default.

Selecting this check box enables File Anti-Virus module to protect files in specific folders from being modified or deleted on the client systems. Click **Add**. Enter the complete path of the folder to be protected on the client systems. You can either protect the parent folder only or select the **Include subfolder** option to protect the subfolders as well.



## File Rights

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



### Enable eScan Remote File Rights

Select this check box to allow/restrict the remote users to make any modifications to the files and folders.

### Do not allow remote users to modify the following local files

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

### Allow modification for following files

The files added to this list can be modified by the remote user.

### Enable eScan local file rights

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

### Do not allow local users to modify the following files

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

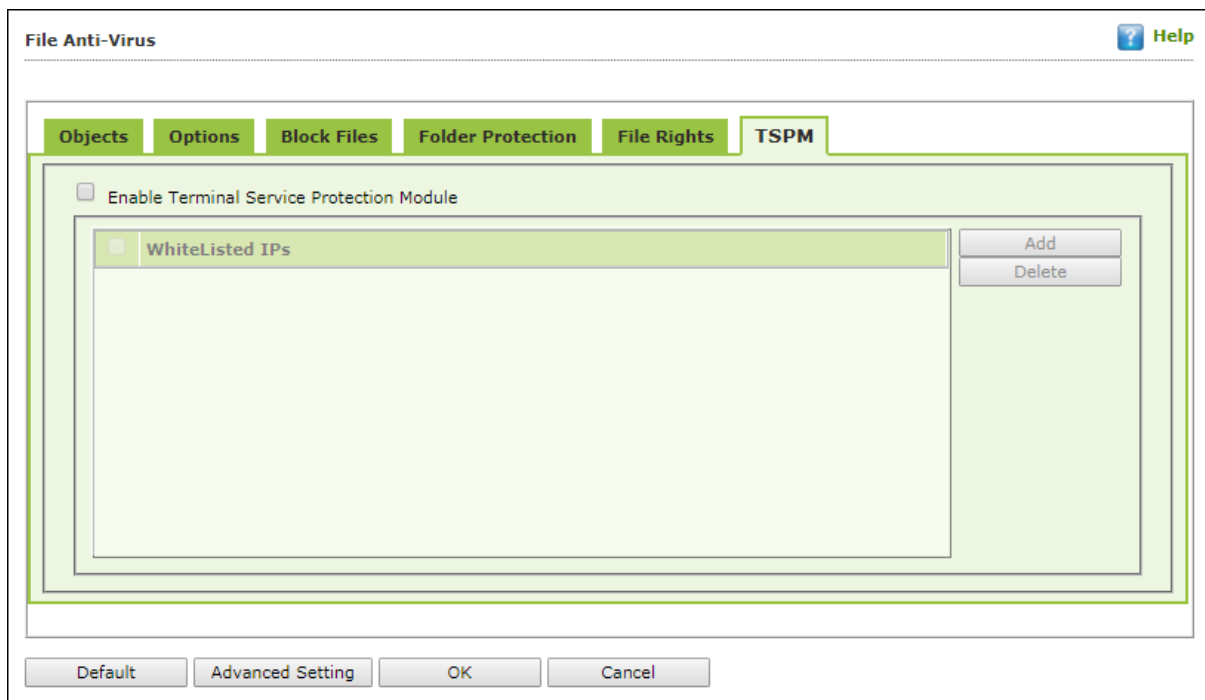
### Allow modification for files



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

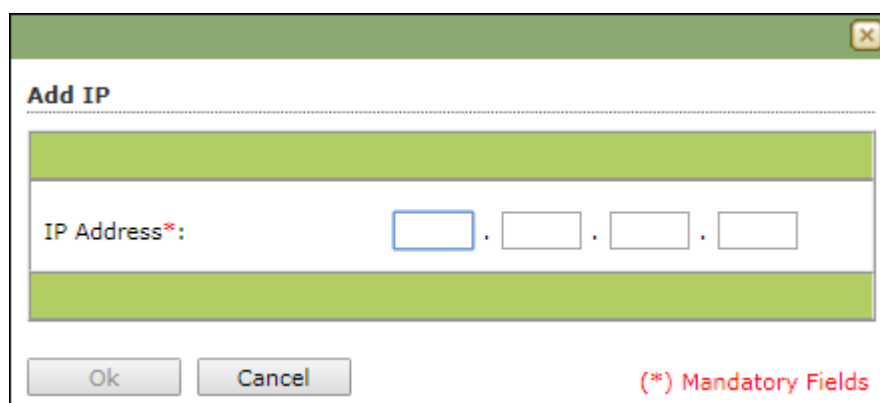
## TSPM

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



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

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



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

## Advanced Settings

Clicking Advanced Settings lets you configure advanced settings for console.

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

Ok

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

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

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

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

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

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

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

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

### Clear Quarantine folder after Days specified

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

**Clear Quarantine Folder after Size Limit specified in MB**

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

**Exclude System PID from Scanning (1 = Enable/0 = Disable)**

This option lets you exclude system process ID (Microsoft assigned System PIDs) from scanning on Managed Computers.

**Disable Virtual Key Board Shortcut key (1 = Enable/0 = Disable)**

This option lets you disable shortcut for using Virtual Keyboard on Managed Computers.

**Show eScan Tray Menu (1 = Show/0 = Hide)**

This option lets you Hide or Show eScan Tray menu on Managed Computers.

**Show eScan Tray Icon (1 = Show/0 = Hide)**

This option lets you hide or show eScan Tray Icon on Managed Computers.

**Show eScan Desktop Protection Icon (1 = Show/0 = Hide)**

This option lets you hide or show eScan Protection icon on Managed Computers.

**Enable eScan Remote Support in Non-Administrator mode (1 = Enable/0 = Disable)**

This option lets you enable/disable eScan Remote Support in Non-Administrator Mode. eScan will not prompt for entering Administrator Password to start eScan Remote Support from Managed Computers.

**Define Virus Alert Time (in seconds)**

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

**Show Malware URL Warning (1 = Show/0 = Hide)**

This option lets you show or hide Malware URL warning messages on Managed Computers.

**Protect Windows Hosts File (1 = Allow/0 = Block)**

Use this option to Allow/Block modifications to Windows Host Files.

**Search for HTML Scripts (1 = Allow/0 = Block)**

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

**Show Network Executable block alert (1 = Show/0 = Hide)**

This option lets you show/hide Network executable block alerts on Managed Computers.

**Show USB Executable Block Alert (1 = Show/0 = Hide)**

This option lets you show/hide USB executable block alerts on Managed Computers.

**Show eScan Tray Icon on Terminal Client (1 = Show/0 = Hide)**

This option lets you show/hide eScan Tray Icon on Terminal Clients on Managed Computers.

**Enable eScan Self Protection (1 = Enable/0 = Disable)**

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

**Enable eScan Registry Protection (1 = Enable/0 = Disable)**

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

**Enable backup of DLL files (1 = Enable/0 = Disable)**

This option lets you Enable/Disable backup of DLL files on Managed Computers.

**Integrate Server Service dependency with Real-time monitor (1 = Enable/0 = Disable)**

This option lets you Integrate Server Service dependency with real-time monitor.

**Send Installed Software Events (1 = Enable/0 = Disable)**

This option lets you receive Installed Software Events from Managed Computers.

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

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

**Enable Cloud (1 = Enable/0 = Disable)**

This option lets you Enable/Disable eScan Cloud Security Protection on Managed Computers.

**Enable Cloud Scanning (1 = Enable/0 = Disable)**

This option lets you Enable/Disable Cloud Scanning on Managed Computers.

**Remove LNK (Real-Time) (1 = Enable/0 = Disable)**

This option lets you Enable/Disable Removal of LNK on real-time basis.

**Whitelisted AutoConfigURL**

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

**Disable Add-ons/Extension blocking (1 = Enable/0 = Disable)**

Selecting this option disables Add-ons and Extension blocking.

**Include files to scan for archive (Eg: abc\*.exe)**

This option lets you add file types that needs to be when archive scanning enabled.

**Block Date-Time Modification (1 = Enable/0 = Disable)**

This option lets you block the modification of the system date and time.

**Allow CMD-Registry for Date-Time blocking (Depends upon Block Date-Time Modification) (1 = Enable/0 = Disable)**

Selecting this option lets you block date-time modification from the CMD-Registry.

**Domain list for exclusion of Host file scanning (e.g. abc.mwti)**

Selecting this option lets you add the list of domains to be excluded from host file scanning.

**Disable Pause Protection and Open Protection center on Right Click (Set 192 for disable)**

This option disables Pause Protection and Open Protection center on Right Click if you set it to 192.

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

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

**NOTE**

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

**List of comma-separated servers and/or shares and/or wildcards which needs to be given NO ACCESS e.g. \\192.168.1.1\temp or \\192.168.1.1\temp\\*.doc or \*.doc (Work only when "Enable Share Access Control" is set)**

Selecting this option lets you add the List of comma-separated servers and/or shares and/or wildcards that should not be accessible.

**List of comma-separated servers and/or shares and/or wildcards which needs to be given READ ONLY ACCESS e.g. \\192.168.1.1\temp or \\192.168.1.1\temp\\*.doc or \*.doc (Work only when "Enable Share Access Control" is set)**

Selecting this option lets you add the List of comma-separated servers and/or shares and/or wildcards that should be given only view access and not be editable.

**Include files to scan for archive (eg: abc\*.exe)**

Selecting this option lets you add file types that should be scanned.

**Whitelist IP Address (Depends on IP Address Change Allowed) (E.G 192.168.1.\* You can put comma-separated list)**

Selecting this option lets you add the list of IP addresses separated by commas to whitelist them.

**Block Access to Control Panel (1 = Enable/0 = Disable)**

Selecting this option lets you block the user from accessing the control panel.

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

Selecting this option lets you disable Copy/Paste actions.

**Enable logging of sharing activity from suspected malware system (WSmbFilt.log on client system) (1 = Enable/0 = Disable)**

Enabling this option directs eScan to log any sharing activity performed by suspected malware system. By default, this feature is enabled.

**Block all RDP Session except Whitelisted under TSPM**

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

**Allow RDP (1=Block Foreign IP and allow Local IP/0 =Block Local & Foreign IP but allow Whitelisted IP)**

This option lets you allow or block the foreign and local IP addresses excluding the whitelisted ones.

**PowerShell Exclusion list**

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



**Allow Uninstallers (1 = Enable/0 = Disable)**

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

**Block Renaming of Hostname (1 = Enable/0 = Disable)**

Selecting this option lets you enable/disable block Hostname renaming.

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

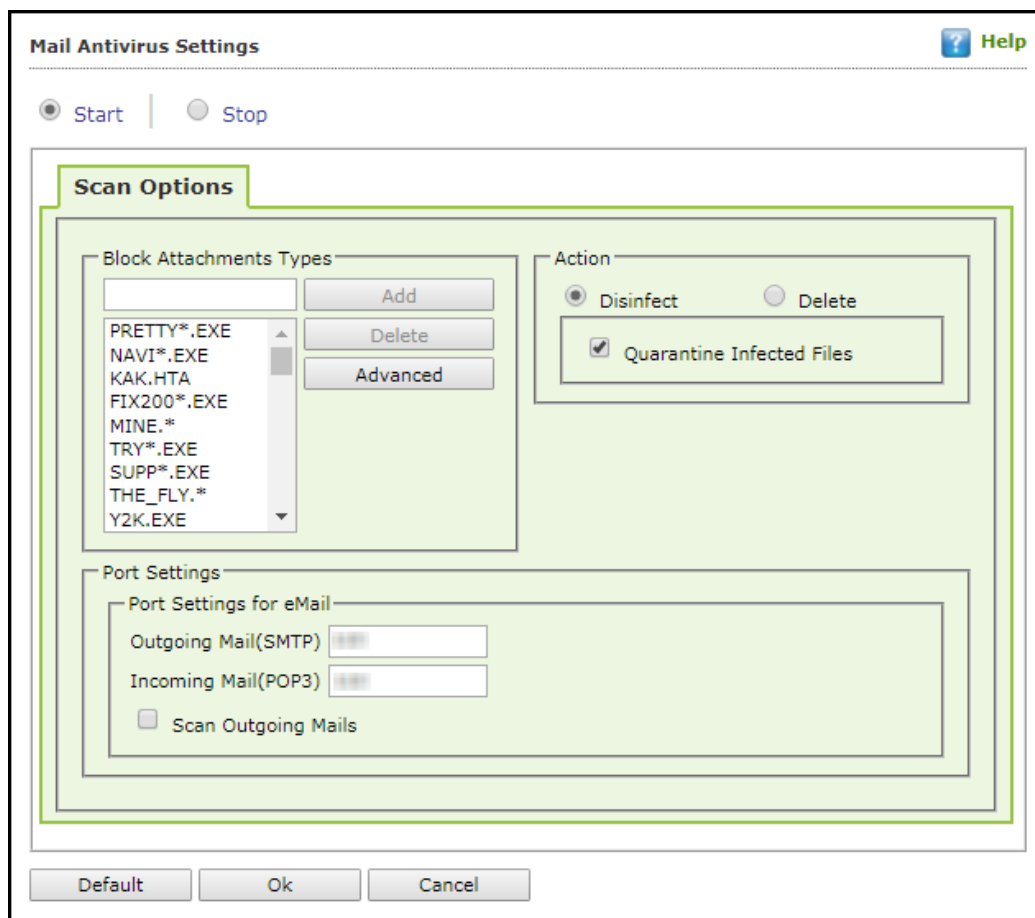
Selecting this option lets you enable/disable restrict environment settings.

**Block eternal blue (wannacry) exploits (1 = Enable/0 = Disable)**

Selecting this option lets you block eternal blue (wannacry) exploits. By default, this option is enabled.

## Mail Antivirus

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



### 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]**

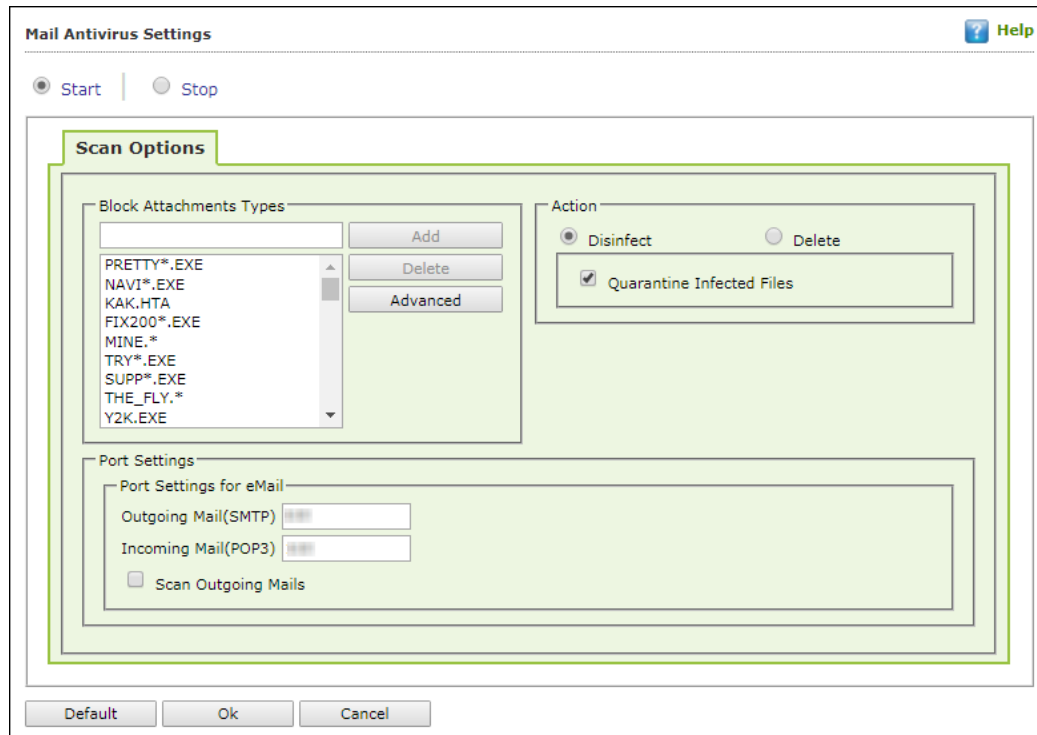
You need to specify a port number for POP3.

### **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 check box to quarantine an entire email if it contains an attachment not scanned by Mail Anti-Virus.

### **Quarantine Attachments if they are scanned**

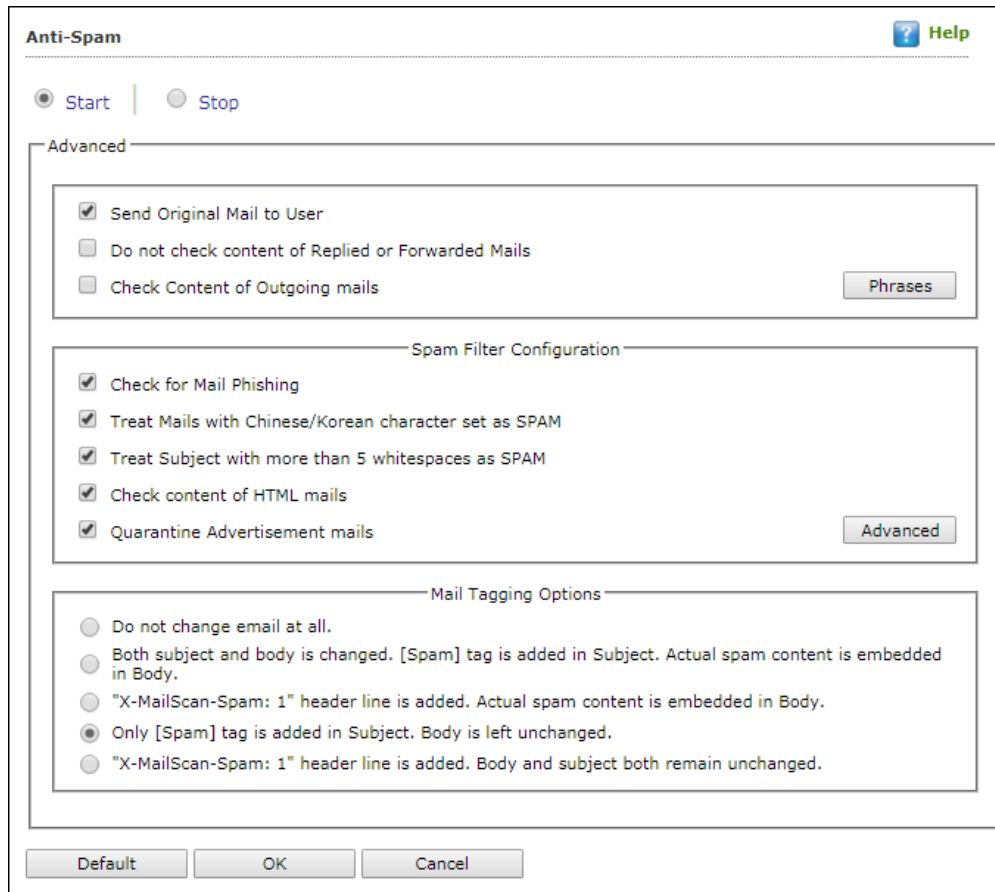
Select this check box if you want eScan to quarantine attachments that are scanned by Mail Anti-Virus.

### **Exclude Attachments (White List)**

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

## Anti-Spam

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



The screenshot shows the 'Anti-Spam' configuration window. At the top, there are radio buttons for 'Start' (selected) and 'Stop'. Below this is the 'Advanced' section, which is expanded. It contains three sub-sections: 'General', 'Spam Filter Configuration', and 'Mail Tagging Options'. In the 'General' section, 'Send Original Mail to User' is checked, while 'Do not check content of Replied or Forwarded Mails' and 'Check Content of Outgoing mails' are unchecked. A 'Phrases' button is to the right. The 'Spam Filter Configuration' section has five checked options: 'Check for Mail Phishing', 'Treat Mails with Chinese/Korean character set as SPAM', 'Treat Subject with more than 5 whitespaces as SPAM', 'Check content of HTML mails', and 'Quarantine Advertisement mails'. An 'Advanced' button is to the right. The 'Mail Tagging Options' section has four radio button options, with the second one selected: 'Both subject and body is changed. [Spam] tag is added in Subject. Actual spam content is embedded in Body.' At the bottom are 'Default', 'OK', and 'Cancel' buttons.

### Advanced

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

#### Send Original Mail to User [Default]

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

#### Do not check content of Replied or Forwarded Mails

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

#### Check Content of Outgoing mails

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

### Phrases

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

#### **User specified whitelist of words/phrases** (Color Code: **GREEN**)

This option indicates the list of words or phrases that are present in the whitelist. A phrase added to the whitelist cannot be edited, enabled, or disabled.

#### **User specified List of Blocked words/phrases:** (Color Code: **RED**)

This option indicates the list of words or phrases that are defined in block list.

#### **User specified words/phrases disabled:** (Color Code: **GRAY**)

This option indicates the list of words or phrases that are defined to be excluded during scans. The options in the **Phrases to Check** dialog box are disabled by default.

### Action List

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

### Spam Filter Configuration

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

#### **Check for Mail Phishing [Default]**

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

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

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

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

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

### Check content of HTML mails [Default]

Select this option if you want Anti-Spam to scan emails in HTML format along with text content.

### Quarantine Advertisement mails [Default]

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

## Advanced

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

The dialog box titled "Advanced Spam Filtering Options" contains the following sections:

- Checkboxes:**
  - ☒ Enable Non Intrusive Learning Pattern (NILP) check
  - ☒ Enable eMail Header check
  - ☒ Enable X-Spam Rules check
  - ☐ Enable Sender Policy Framework (SPF) check
  - ☐ Enable Spam URI Realtime Blacklist (SURBL) check
  - ☐ Enable Real-time Blackhole List (RBL) check
- RBL Servers:**
  - Input field: [ ]
  - Buttons: Add, Delete, Remove All
  - List: bl.spamcop.net, b.barracudacentral.org
- Auto-Spam Whitelist:**
  - Input field: [ ]
  - Buttons: Add, Delete, Remove All
  - List: \*@analytics.bounces.goog, \*@irctc.co.in, \*@sourcenext.co.jp, \*@sourcenext.com, \*@sourcenext.info
- Footer:**
  - Buttons: Save, Cancel



### **Enable Non- Intrusive Learning Pattern (NILP) check [Default]**

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

### **Enable email Header check [Default]**

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

### **Enable X Spam Rules check [Default]**

X Spam Rules are rules that describe certain characteristics of an email. It checks whether the words in the content of emails are present in eScan's database. This database contains a list of words and phrases, each of which is assigned a score or threshold. The Spam Rules Check technology matches X Spam Rules with the mail header, body, and attachments of each email to generate a score. If the score crosses a threshold value, the mail is considered as spam. Anti-Spam refers to this database to identify emails and takes action on them.

### **Enable Sender Policy Framework (SPF) check**

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

### **Enable Spam URI Real-time Blacklist (SURBL) check**

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

### **Enable Real-time Blackhole List (RBL) check**

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

### **RBL Servers**

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

### **Auto Spam Whitelist**

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

### **Mail Tagging Options**

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

#### **Do not change email at all**

Select this option if you want to prevent Anti-Spam from adding the [Spam] tag to emails that have been identified as spam.

#### **Both subject and body are changed: [Spam] tag is added in Subject: Actual spam content is embedded in Body**

This option lets you identify spam emails. When you select this option, Anti-Spam adds a [Spam] tag in the subject line and the body of the email that has been identified as spam.

#### **"X MailScan Spam: 1" header line is added: Actual spam content is embedded in Body**

This option lets you add a [Spam] tag in the body of the email that has been identified as spam. In addition, it adds a line in the header line of the email.

#### **Only [Spam] tag is added in Subject: Body is left unchanged [Default]**

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

#### **"X MailScan Spam: 1" header line is added: Body and subject both remain unchanged**

This option lets you add a header line to the email. However, it does not add any tag to the subject line or body of the email.

## Web Protection

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

**Web Protection** [Help]

☒ Start ☐ Stop ☐ Start Phishing Filter ☐ Start Malware URL Filter

**Filtering Options** | Scanning Options | Define Time-Restriction

Status: ☒ Active ☐ Block Web Access

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

Site Names:

☐ Add sites rejected by the filter to Block category

Default | Advanced Setting | OK | Cancel

You can configure the following settings.

### Filtering Options

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

#### Status

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

#### Filter Categories

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

## Green

It represents an allowed websites category.

## Red

It represents a blocked websites category.

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

## Category Name

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

## Filter Options

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

## Scanning Options

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

## Actions

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

## Log Violations [Default]

This check box is selected by default. Select this option if you want Web Protection to log all security violations for your future reference.

### Shutdown Program in 30 Secs

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

### Port Setting

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

### Internet Access (HTTP Port)

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

## Define Time Restriction

This section lets you define policies to restrict access to the Internet.

### Enable Time Restrictions for Web Access

Select this option if you want to set restrictions on when a user can access the Internet. By default, all the fields appear dimmed. The fields are available only when you select this option.

The time restriction feature is a grid-based module. The grid is divided into columns based on the days of the week vertically and the time interval horizontally.

### Active

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

### Inactive

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

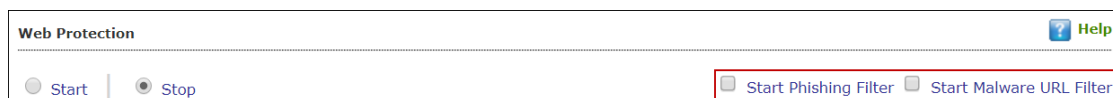
### Block Web Access

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

### Phishing and Malware URL Filter

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

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



## Advanced Settings

Clicking **Advanced** displays Advanced Settings.

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

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

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

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

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

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

### Block Microsoft EDGE Browser (1 = Enable/0 = Disable)

Select this option to enable/disable blocking Microsoft Edge browser.

### Enable Web Protection using Filter driver (1 = Enable/0 = Disable)

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

### Force Disable Web Protection using Filter driver (1 = Enable/0 = Disable)

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

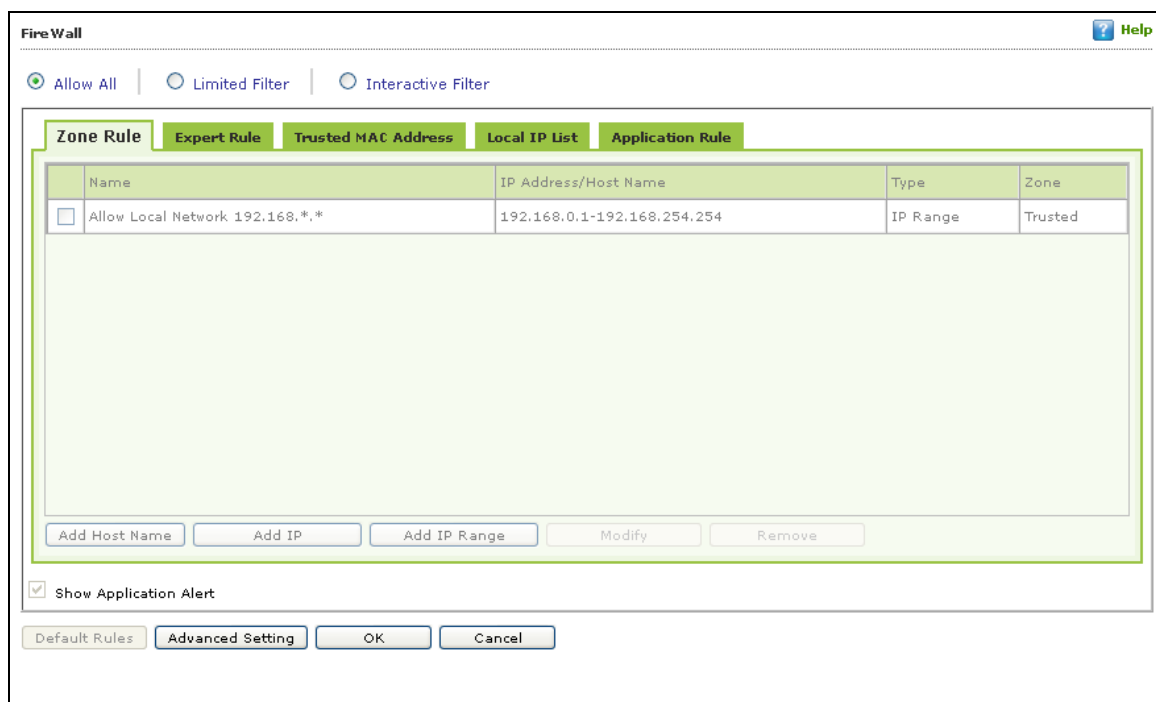


**WFP Exclude IP List (1 = Enable/0 = Disable)**

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

## Firewall

Firewall module is designed to monitor all incoming and outgoing network traffic and protect your computer from all types of network based attacks. eScan includes a set of predefined access control rules that you can remove or customize as per your requirements. These rules enforce a boundary between your computer and the network. Therefore, the Firewall feature first checks the rules, analyzes network packets, and filters them on the basis of the specified rules. When you connect to the Internet, you expose your computer to various security threats.



The Firewall feature of eScan protects your data when you:

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

By default, the firewall operates in the **Allow All** mode. However, you can customize the firewall by using options like **Limited Filter** for filtering only incoming traffic and



**Interactive Filter** to monitor incoming and outgoing traffic. The eScan Firewall also lets you specify different set of rules for allowing or blocking incoming or outgoing traffic. These rules include Zone Rules, Expert Rules, Trusted Media Access Control (MAC) Address, and Local IP list. This page provides you with options for configuring the module. You can configure the following settings to be deployed to the eScan client systems.

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

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

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

Following tabs are available:

**Zone Rule**

**Expert Rule**

**Trusted MAC Address**

**Local IP List**

**Application Rule**

## Zone Rule

This is a set of network access rules to make the decision of allowing/blocking of the access to the system. This will contain the source IP address or source Host name or IP range either to be allowed or blocked.

Buttons (to configure a zone rule)

**Add Host Name** – This option lets you add a "host" in the zone rule. After clicking **Add Host Name**, enter the HOST name of the system, select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the zone rule.

**Add IP** – This option lets you add an IP address of a system to be added in the zone rule. After clicking **Add IP**, enter the IP address of the system, select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the Zone Rule.

**Add IP Range** – This option lets you add an IP range to be added in the zone rule. After clicking **Add IP Range**, add the IP Range (i.e. a range of IP that the zone rules should be

applied), select the zone (Trusted/Blocked) and enter a name for the zone rule. Click **OK** to create the zone rule.

**Modify** – To modify/change any listed zone rule (s), select the zone rule to be modified and then click **Modify**.

**Remove** - To remove any listed zone rule (s), select the zone rule and then click **Remove**.

## Expert Rule

This tab lets you specify advanced rules and settings for the eScan firewall. You can configure expert rules on the basis of the various rules, protocols, source IP address and port, destination IP address and port, and ICMP types. You can create new expert rules. However, configure these rules only if you are familiar with firewalls and networking protocols.

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

### Buttons (to configure an Expert Rule)

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

**Add Firewall Rule**

**General** | Source | Destination | Advanced

Rule Name

Rule Action  
☒ Permit Packet ☐ Deny Packet

Protocol

Apply Rule on Interface

OK Cancel

### General tab

In this section, specify the Rule settings:

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

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

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

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

### Source tab

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

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

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

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

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

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

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

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

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

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

**NOTE**

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

**Destination tab**

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

**Destination IP Address –**

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

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

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

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

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

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

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

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

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

<b>NOTE</b>	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.

ICMP Type	In	Out
Destination Unreachable	<input type="checkbox"/>	<input type="checkbox"/>
Echo Reply (ping)	<input type="checkbox"/>	<input type="checkbox"/>
Echo Request (ping)	<input type="checkbox"/>	<input type="checkbox"/>
Information Reply	<input type="checkbox"/>	<input type="checkbox"/>
Information Request	<input type="checkbox"/>	<input type="checkbox"/>
Parameter Problem	<input type="checkbox"/>	<input type="checkbox"/>
Redirect	<input type="checkbox"/>	<input type="checkbox"/>
Source Quench	<input type="checkbox"/>	<input type="checkbox"/>
TTL Exceeded	<input type="checkbox"/>	<input type="checkbox"/>

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

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

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

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

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

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

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

## Trusted MAC Address

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

Buttons (to configure the Trusted MAC Address)

**Add** – To add a MAC address click on this button. Enter the MAC address to be added in the list for e.g. 00-13-8F-27-00-47

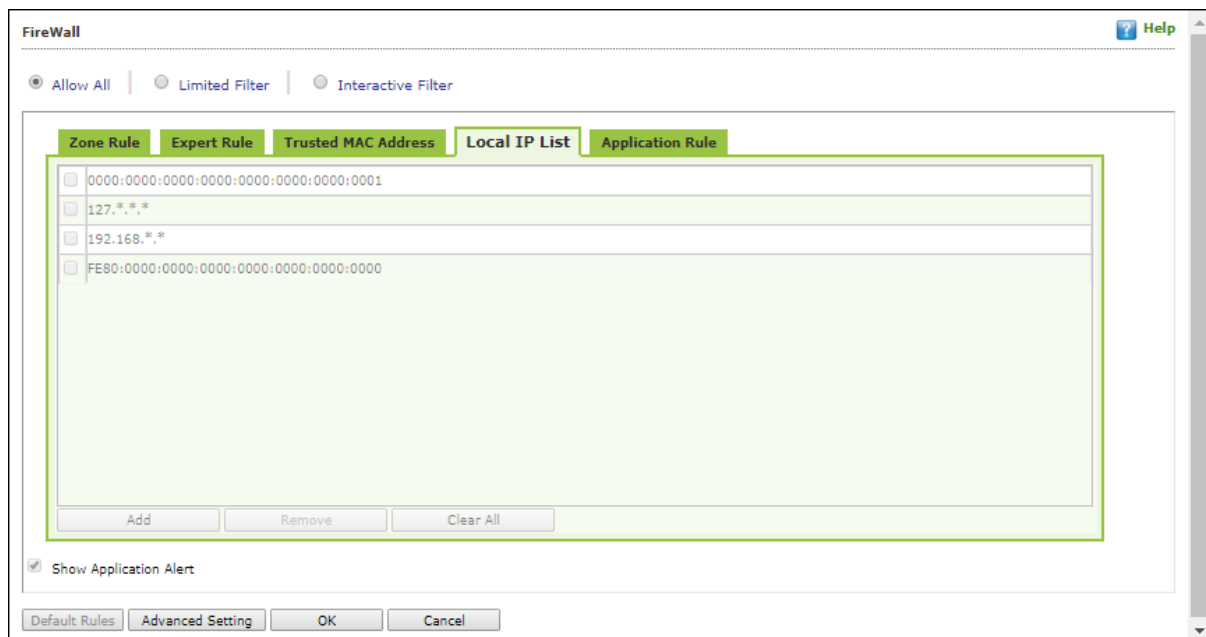
**Edit** – To modify/change the MAC Address, click **Edit**.

**Remove** – To delete the MAC Address, click **Remove**.

**Clear All** – To delete the entire listed MAC Address, click **Clear All**.

## Local IP List

This section contains a list of Local IP addresses.



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

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

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

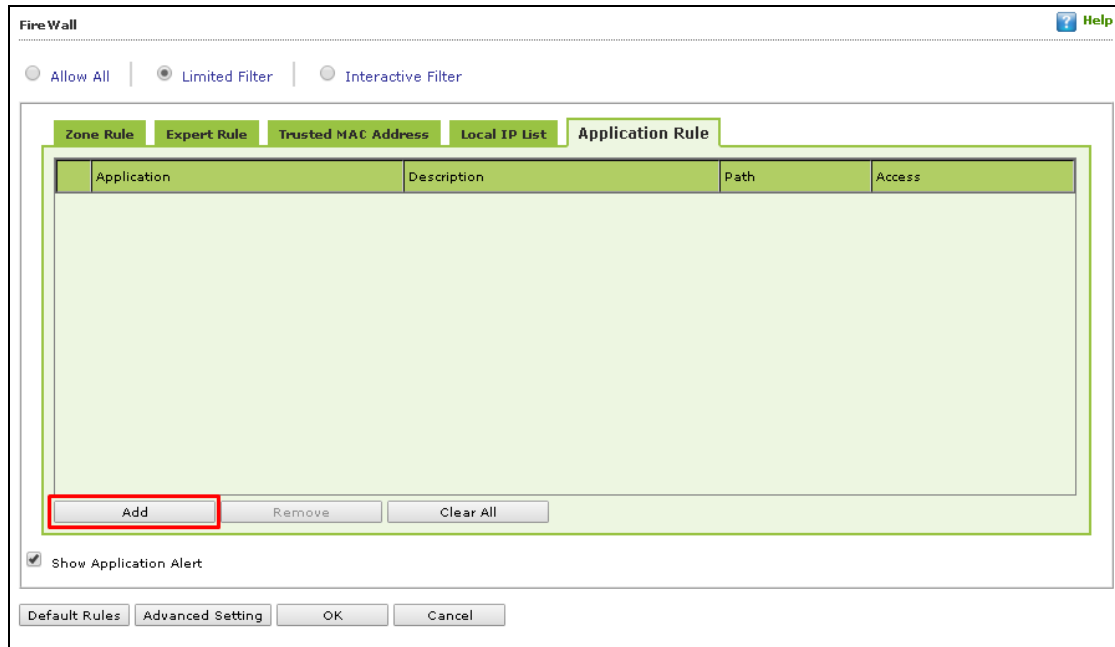




**Default List** – To load the default list of IP addresses, click **Default List**.

## Application Rule

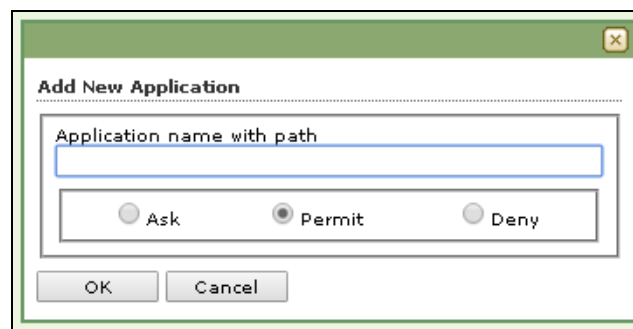
In this section you can define the permissions for different application. The application can be set to Ask, Permit or Deny mode.



### Defining permission for an application

To define permission for an application,

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



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

The permission for the application will be defined.

### Removing permission of an application

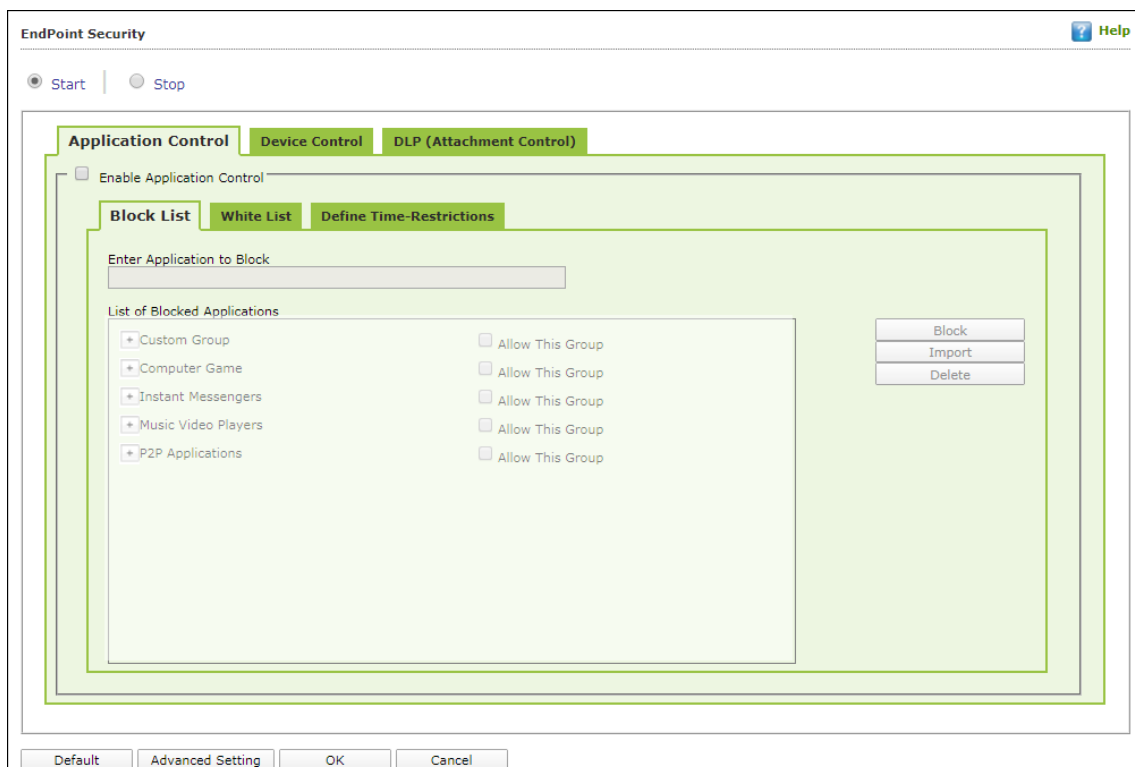
Select an application and then click **Remove**. The application will no longer have the permission.

#### Other Buttons

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

## Endpoint Security

Endpoint Security module protects your computer or Computers from data thefts and security threats through USB or FireWire® based portable devices. It comes with Application Control feature that lets you block unwanted applications from running on your computer. In addition, this feature provides you with a comprehensive reporting feature that lets you determine which applications and portable devices are allowed or blocked by eScan.



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

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

There are two tabs – Application Control and USB Control, which are as follows:

### Application Control

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

#### Enable Application Control

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

### **Block List**

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

### **List of Blocked Applications**

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

### **White List**

#### **Enable White Listing**

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

#### **Enter Application to whitelist**

Enter the name of the application to be whitelisted.

### **White Listed Applications**

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

### **Define Time Restrictions**

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

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

#### **Datewise Restrictions**

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

## Device Control

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

**EndPoint Security** Help

☒ Start | ☐ Stop

**Application Control** | **Device Control** | **DLP (Attachment Control)**

☒ Enable Device Control

**USB Settings**

☐ Block USB Ports ☐ Ask for Password

☒ Use eScan Administrator Password

☐ Use Other Password

☒ Do Virus Scan ☒ Allow user to cancel scan

☐ Read Only - USB ☒ Disable AutoPlay

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

☐ Record Files Copied To Network ☒ Ignore System Drive

**Whitelist**

☐ Scan Whitelisted USB Devices

Serial No.	Device Name	Description

☐ Disable Web Cam ☐ Disable Bluetooth

☐ Disable SD Cards

**CD / DVD Settings**

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

You can configure the following settings:

### Enable Device Control [Default]

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



## USB Settings

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

### Block USB Ports

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

### Ask for Password

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

### Use eScan Administrator

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

### Use Other Password

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

### Do Virus Scan [Default]

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

### Allow user to cancel scan

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

### Disable AutoPlay [Default]

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

### Read Only USB

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

### Record Files Copied To USB

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



### **Record Files Copied To Network**

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

### **Record Files Copied To Local**

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

### **Ignore System Drive**

Select this option in case of you do not want eScan to record files that are copied from system drive of managed computers to either network drive or any local drive.

### **Whitelist**

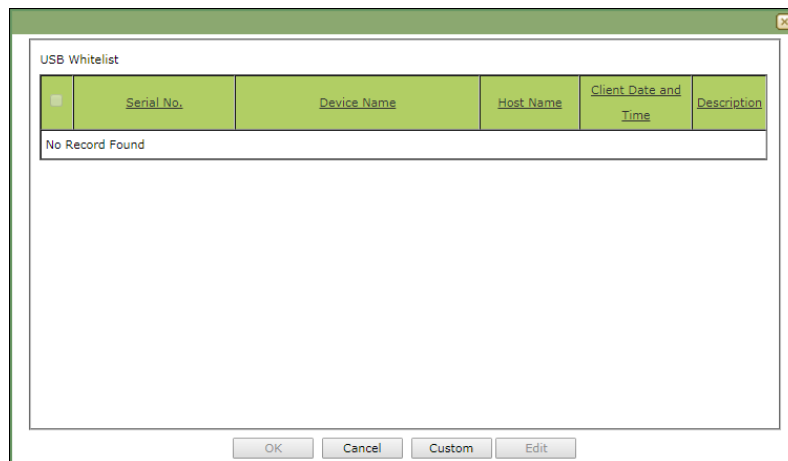
eScan provides a greater level of endpoint security by prompting you for a password whenever you connect a USB drive. To disable password protection for a specific device, you can add it along with its serial number to the whitelist. The next time you connect the device it will not ask for a password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

### **Scan Whitelisted USB Devices**

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

### **Add**

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



To whitelist a USB device, its details are required. If a USB device is connected to any eScan installed endpoint, the USB details are sent to the server. The administrator will have to manually whitelist the USB device.

To manually add a USB device in USB Whitelist without connecting to an endpoint, click **Custom**.

USB Whitelist

Serial No.

Device Name

Description

OK Cancel

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

### Import

To whitelist USB devices from a csv file, click **Import**.

Click **Choose File** to import the file with the list.

The list should be in following format:

Serial No 1, Device Name 1, Device Description 1(Optional)

Serial No 2, Device Name 2

**Eg:** SDFSD677GFQW8N6CN8CBN7CXVB, USB Drive 2.5, Whitelist by xyzDFRGHHR54456HGDF347OMCNAK, Flash Drive 2.2

**Disable Web Cam:** Select this option to disable Webcams.



**Disable SD Cards:** Select this option to disable SD cards.

**Disable Bluetooth:** Select this option to disable Bluetooth.

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

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

**NOTE**

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

## DLP (Attachment Control)

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

You can configure the following settings:

### Attachment Allowed

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

### Attachment Blocked

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

### Enter Process Name

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

### Blacklisted Process

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

### Whitelisted Process

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

### Enter Site Name

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

### Whitelisted Sites

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

## Advanced Settings

Advanced Setting

Name	Value
<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 USB on Terminal Client (1 = Enable/0 = Disable)**

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

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

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

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

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

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

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

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

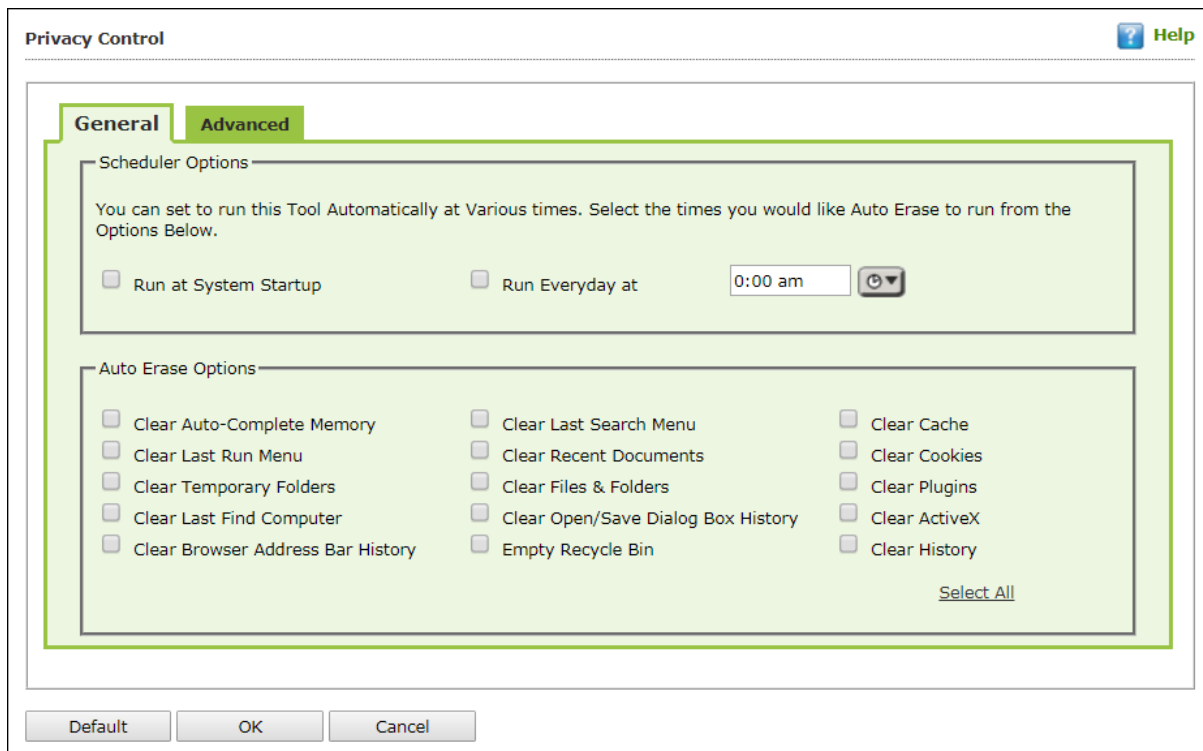
Select this option to allow/block use of network printers.

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

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

## Privacy Control

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



It consists following tabs:

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

### General tab

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

#### Scheduler Options

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

#### Run at System Startup



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

### **Run Every day at**

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

### **Auto Erase Options**

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

### **Clear Auto Complete Memory**

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

### **Clear Last Run Menu**

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

### **Clear Temporary Folders**

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

### **Clear Last Find Computer**

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

### **Clear Browser Address Bar History**

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

### **Clear Last Search Menu**





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

**Clear Recent Documents**

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

**Clear Files & Folders**

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

**Clear Open/Save Dialog box History**

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

**Empty Recycle Bin**

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

**Clear Cache**

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

**Clear Cookies**

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

**Clear Plugins**

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

**Clear ActiveX**

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

**Clear History**

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

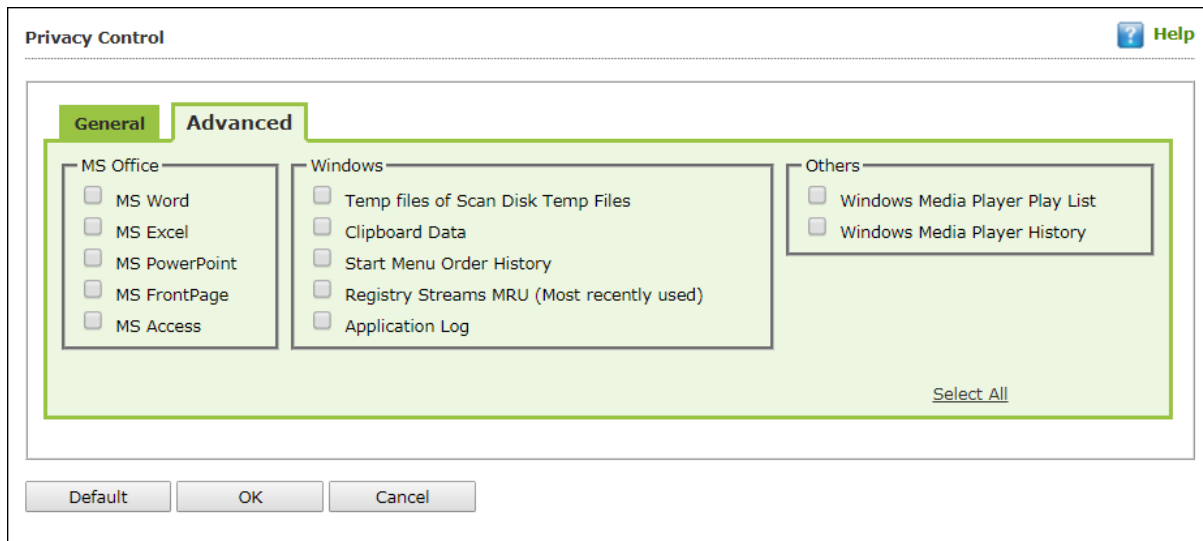
In addition to these options, the **Auto Erase Options** section has

**Select All/ Unselect All**

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

## Advanced tab

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



### MS Office

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

### Windows

The respective unwanted files like temp files will be cleared.

### Others

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

<b>NOTE</b>	Click <b>Default</b> to apply default settings, which are done during installation of eScan. It loads and resets the values to the default settings.
-------------	--

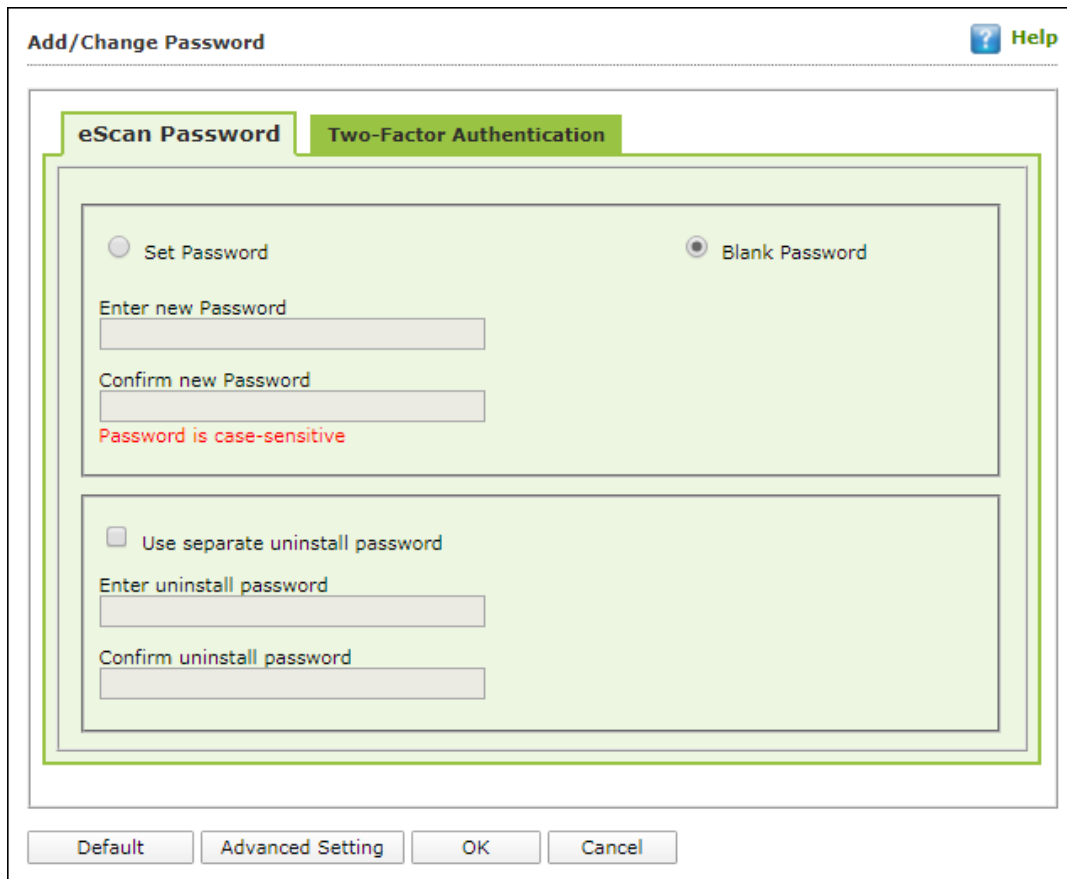
Policy Details also lets you do the following for Windows Operating System.

## Administrator Password

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

### eScan Password

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



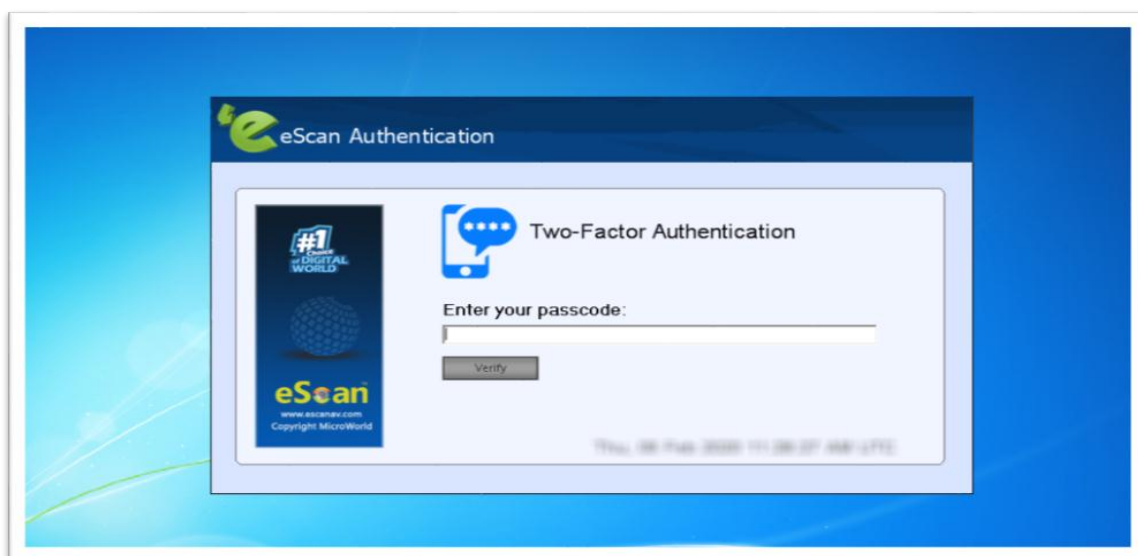
The image shows a screenshot of the 'Add/Change Password' dialog box. The dialog has a title bar with 'Add/Change Password' and a 'Help' button. Inside, there are two tabs: 'eScan Password' (selected) and 'Two-Factor Authentication'. Under the 'eScan Password' tab, there are two radio buttons: 'Set Password' and 'Blank Password'. The 'Blank Password' option is selected. Below these are two text input fields: 'Enter new Password' and 'Confirm new Password'. A red text label 'Password is case-sensitive' is displayed below the 'Enter new Password' field. Below the password fields, there is a checkbox labeled 'Use separate uninstall password'. Below this checkbox are two more text input fields: 'Enter uninstall password' and 'Confirm uninstall password'. At the bottom of the dialog, there are four buttons: 'Default', 'Advanced Setting', 'OK', and 'Cancel'.

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

## Two-Factor Authentication

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

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



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

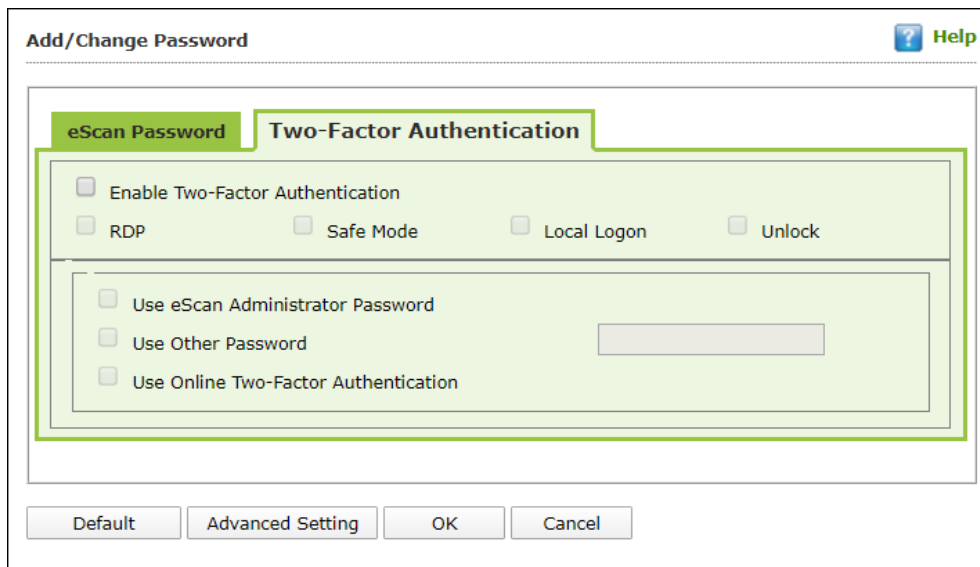
1. In the eScan web console, go to **Managed Computers**.
2. Click **Policy Templates > New Template**.

**NOTE**

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

3. Select **Administrator Password** check box and then click **Edit**.
4. Click **Two-Factor Authentication** tab.

Following window appears.



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

## Login Scenarios

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

### RDP

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

### Safe Mode

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

### Local Logon

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

### Unlock

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

## Password Types

If the policy is applied to a group, the 2FA passcode will be same for all group members. The 2FA passcode can also be set for specific computer(s).

You can use following all password types to log in:

### **Use eScan Administrator Password**

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

### **Use Other Password**

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

### **Use Online Two-Factor Authentication**

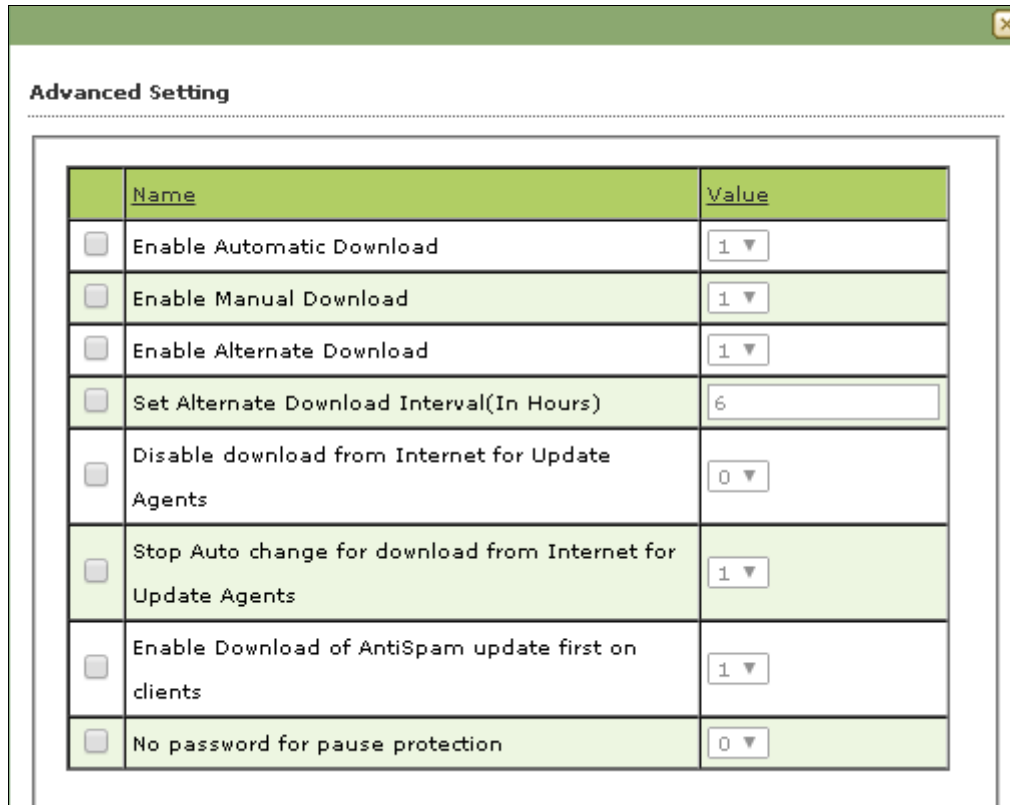
To use this feature, follow the steps given below:

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

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

## Advanced Setting

Clicking **Advanced Setting** displays Advance setting.



	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 ▼

### 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.

## ODS/Schedule Scan

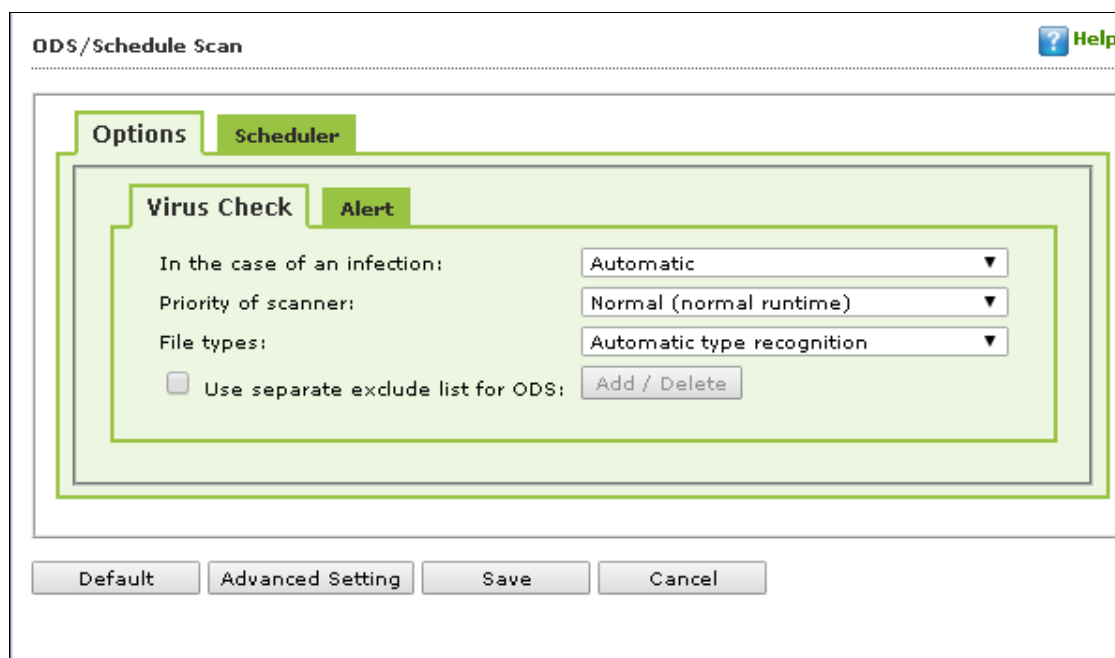
**ODS (On Demand Scanning)/Schedule Scan** provides you with various options like – checking for viruses, and making settings for creating logs and receiving alerts. You can also create task in the scheduler for automatic virus scanning.

### 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**



## Options

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

- Virus check
- Alerts

### Virus Check

It lets you configure the settings for checking viruses.

To set virus check,

1. Specify the following field details.
  - **In the case of an infection:** Select an appropriate option from the drop-down list. For example, Log only, Delete infected file, and [Default] Automatic.
  - **Priority of scanner:** Select an appropriate option from the drop-down list. For example,
    - 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.
2. Click **Save**.

### Alerts tab

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

To set alerts,

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

<b>NOTE</b>	Click <b>Default</b> 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.

The screenshot shows the 'ODS/Schedule Scan' window with the 'Scheduler' tab selected. The window has a 'Help' icon in the top right corner. Inside the window, there are two tabs: 'Options' and 'Scheduler'. The 'Scheduler' tab contains a table with three columns: 'Name', 'Schedule', and 'Next start'. Below the table are four buttons: 'Clear All', 'Add task', 'Delete task', and 'Edit'. At the bottom of the window, there are four buttons: 'Default', 'Advanced Setting', 'Save', and 'Cancel'.

Name	Schedule	Next start
------	----------	------------

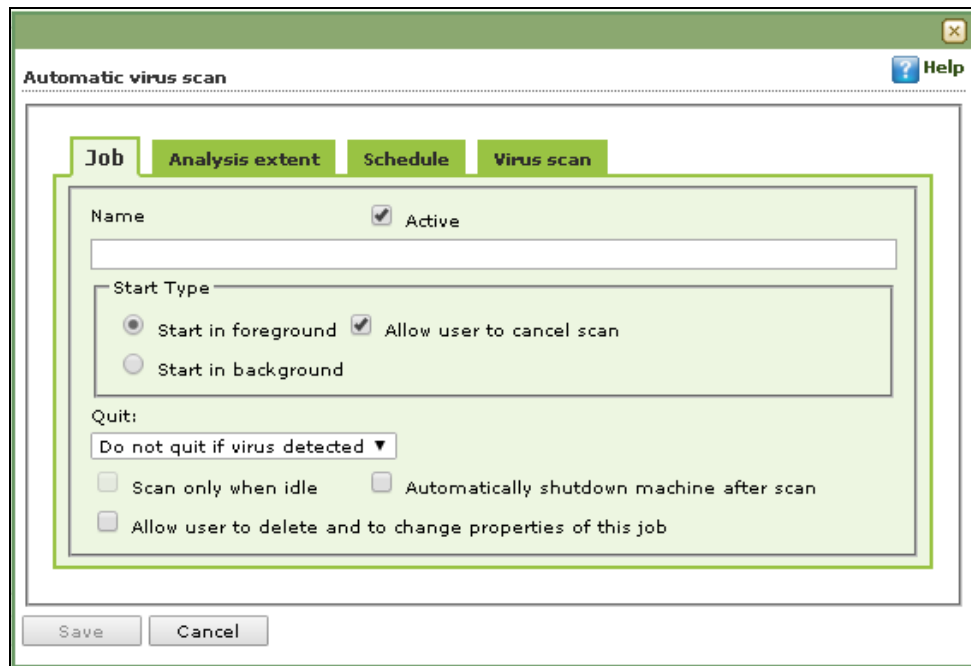
Buttons: Clear All, Add task, Delete task, Edit

Bottom Buttons: Default, Advanced Setting, Save, Cancel

**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 lets you do following activities:

- Creating job
- Setting analysis extent
- Scheduling virus execution
- Scheduling virus scan

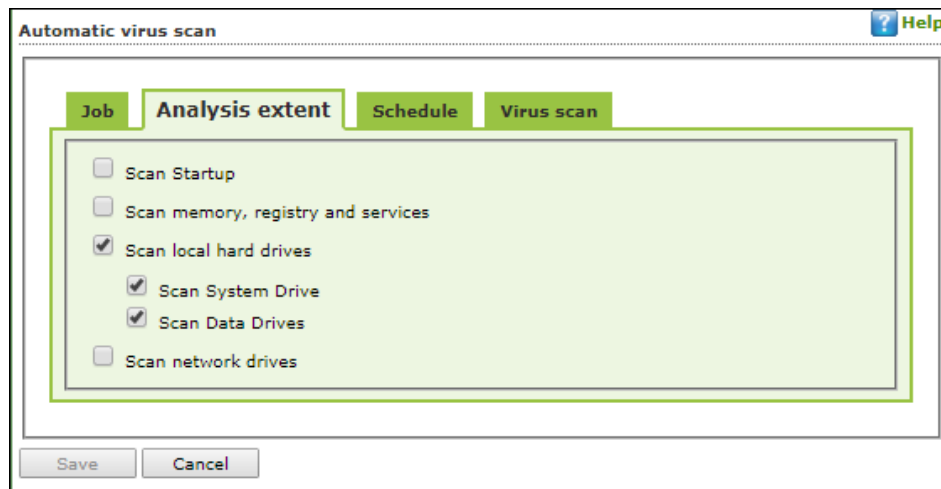
### a) Job

It lets you create the job details for virus scanning.

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

### b) Analysis Extent

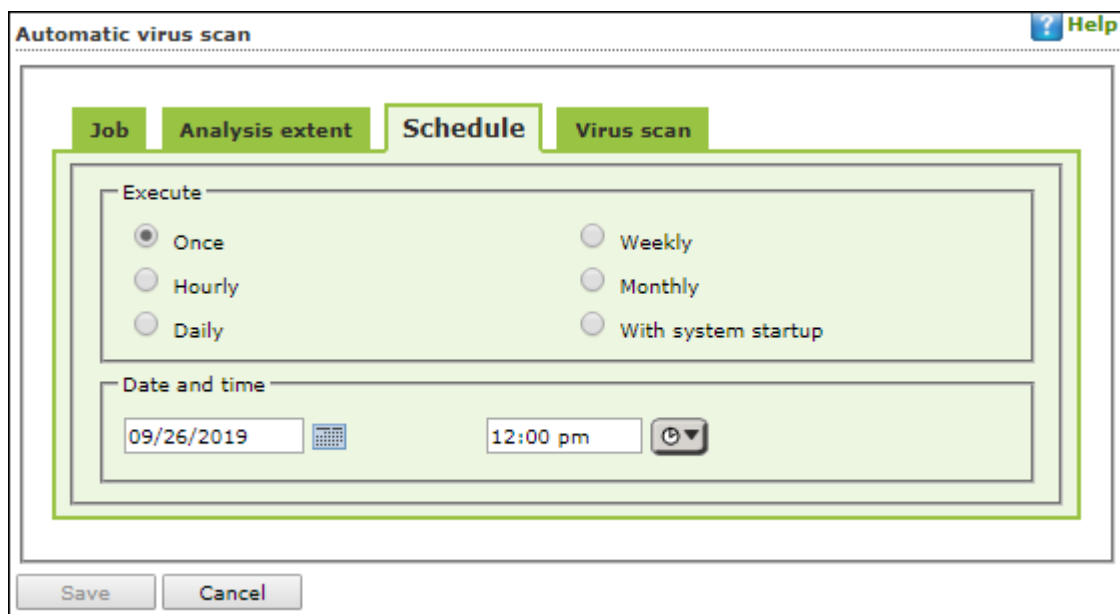
It lets you configure analysis extent settings for virus scanning.



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.

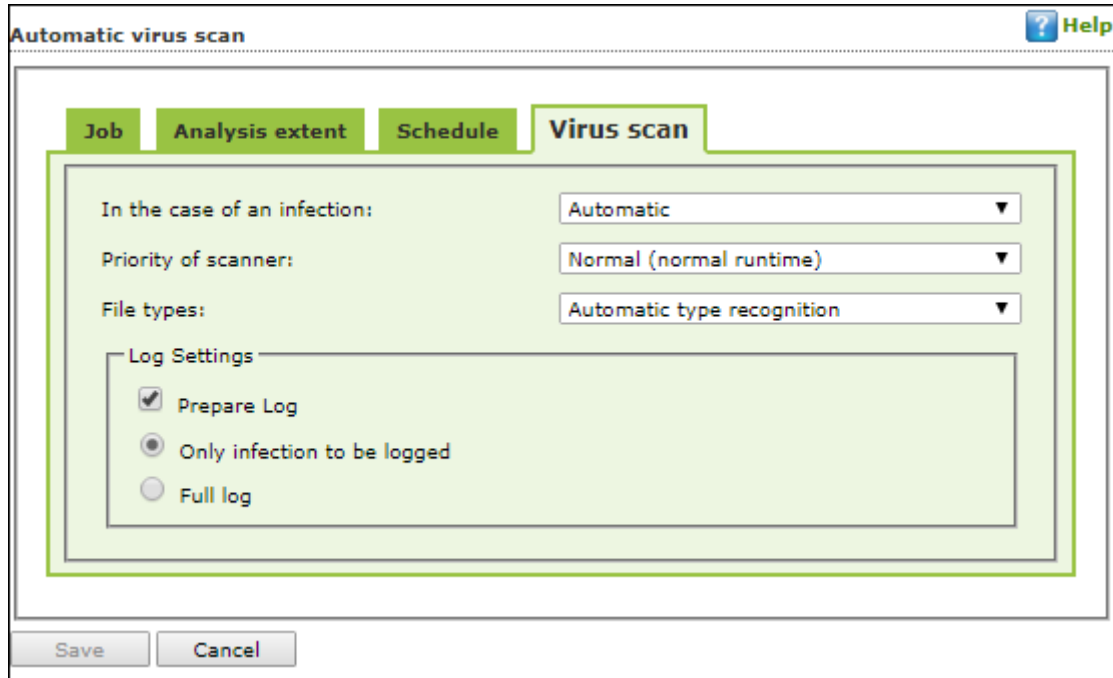
**NOTE**

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.



The screenshot shows the 'Automatic virus scan' dialog box with the 'Virus scan' tab selected. The dialog has four tabs: 'Job', 'Analysis extent', 'Schedule', and 'Virus scan'. The 'Virus scan' tab contains the following settings:

- In the case of an infection:** A dropdown menu set to 'Automatic'.
- Priority of scanner:** A dropdown menu set to 'Normal (normal runtime)'.
- File types:** A dropdown menu set to 'Automatic type recognition'.
- Log Settings:** A section with three radio button options:
  - ☒ Prepare Log
  - ☐ Only infection to be logged
  - ☐ Full log

At the bottom of the dialog are 'Save' and 'Cancel' buttons. A 'Help' button is located in the top right corner of the dialog.

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

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

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



## MWL (MicroWorld WinSock Layer)

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

## MWL Inclusion List

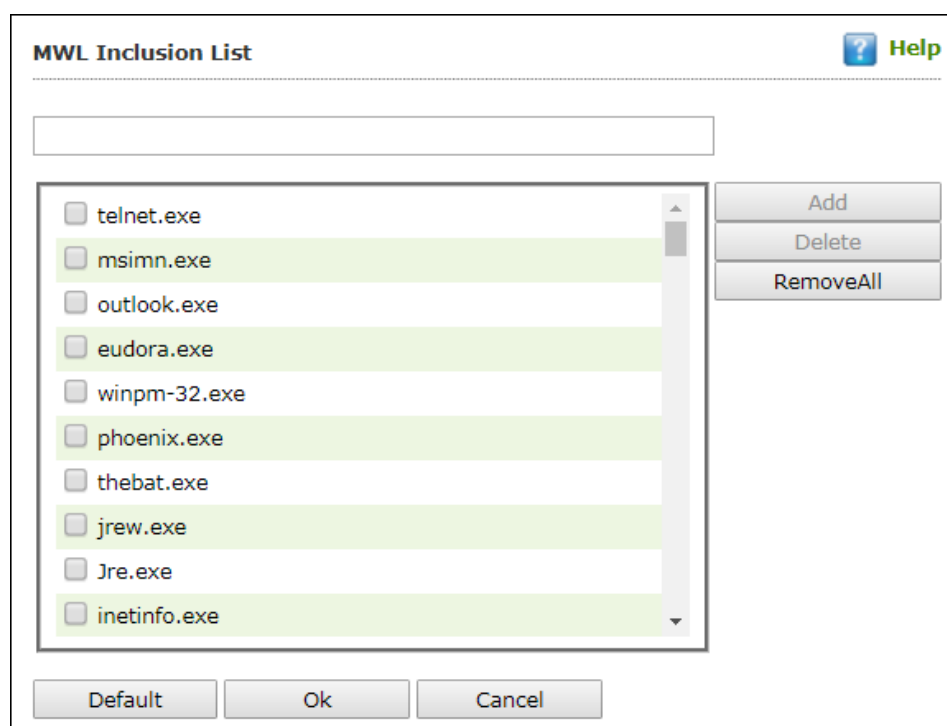
Inclusion List contains the name of all executable files which will bind itself to MWTSP.DLL. All other files are excluded.

### NOTE

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

You can do the following activities.

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



## Add files to Inclusion List

To add executable files to the Inclusion List,

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

## Delete files from Inclusion List

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

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

## Remove all files from Inclusion List

To remove all executable files from the Inclusion List,

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

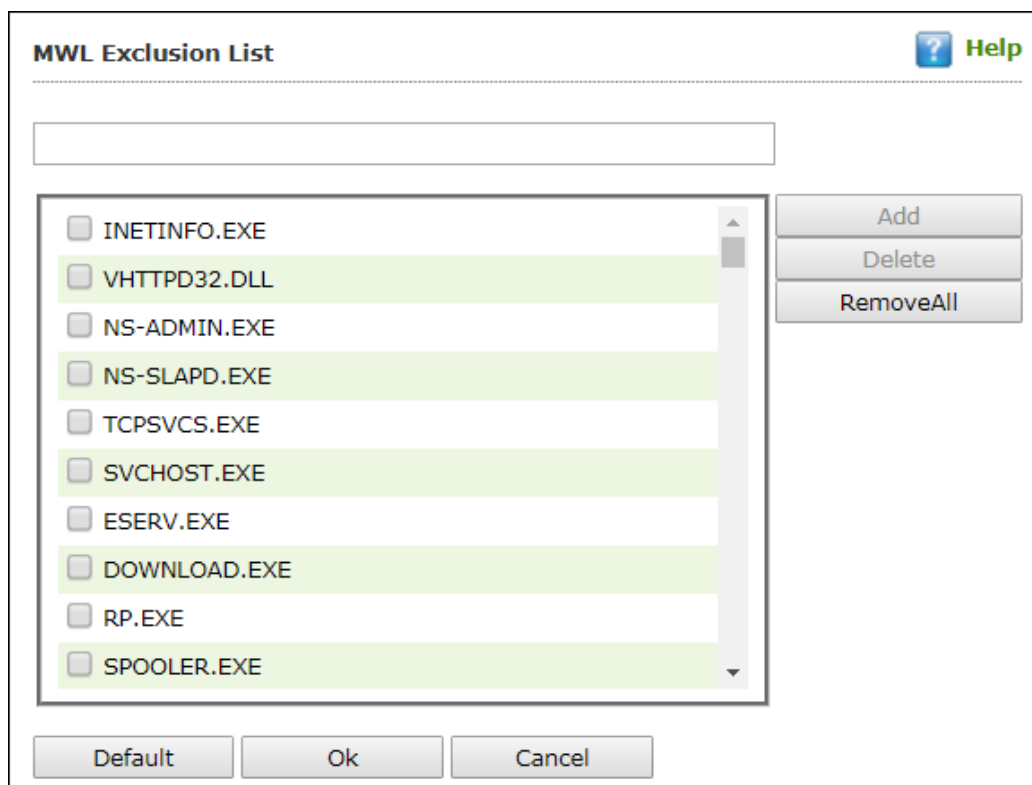
## MWL Exclusion List

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

<b>NOTE</b>	Click <b>Default</b> 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



The MWL Exclusion List dialog box features a title bar with a question mark icon and a 'Help' button. Below the title bar is a text input field. A list box contains several files, each with a checkbox: INETINFO.EXE, VHTTDP32.DLL, NS-ADMIN.EXE, NS-SLAPD.EXE, TCPSVCS.EXE, SVCHOST.EXE, ESERV.EXE, DOWNLOAD.EXE, RP.EXE, and SPOOLER.EXE. To the right of the list box are three buttons: 'Add', 'Delete', and 'RemoveAll'. At the bottom of the dialog are three buttons: 'Default', 'Ok', and 'Cancel'.

## Adding files to Exclusion List

To add executable files to the Exclusion List,

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

## Deleting files from Exclusion List

To delete executable files from the Exclusion List,

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

## Removing all files from Exclusion List

To remove all executable files from the Exclusion List,

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

## Notifications and Events

### Notifications

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

#### Virus Alerts [Default]

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

#### Warning Mails

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

#### Attachment Removed Warning to Sender [Default]

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

#### **Attachment Removed Warning to Recipient [Default]**

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

#### **Virus Warning to Sender [Default]**

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

#### **Virus Warning to Recipient [Default]**

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

#### **Content Warning to Sender**

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

#### **Content Warning to Recipient [Default]**

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

#### **Delete Mails from User**

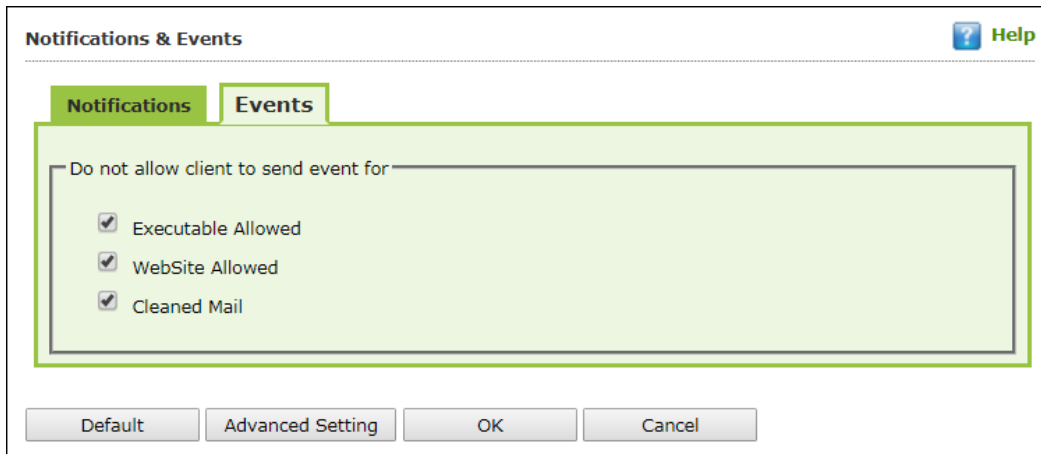
You can configure eScan to automatically delete emails that have been sent by specific users. For this, you need to add the email addresses of such users to the **Delete Mails From User** field. The **Add**, **Delete**, and **Remove All** buttons appear as dimmed. After you enter text in the **Delete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

## Events

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

- Executable Allowed
- Website Allowed
- Cleaned Mail

By default, all events are selected.



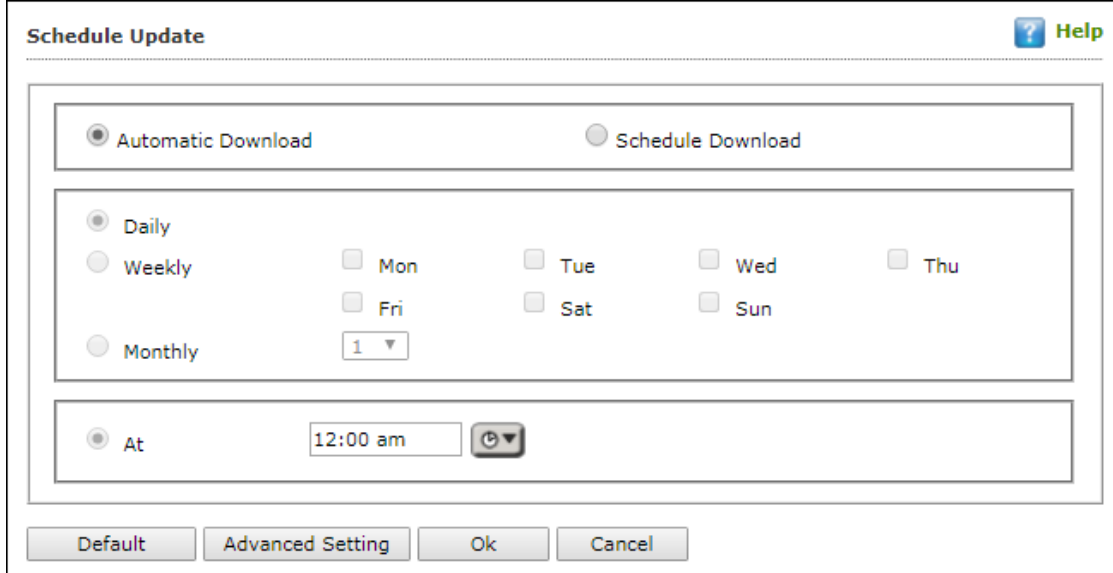
The screenshot shows a window titled "Notifications & Events" with a "Help" icon in the top right. It has two tabs: "Notifications" and "Events", with "Events" being the active tab. Inside the "Events" tab, there is a text label "Do not allow client to send event for" followed by a large empty rectangular box. Below this box, there are three checked checkboxes with the following labels: "Executable Allowed", "WebSite Allowed", and "Cleaned Mail". At the bottom of the window, there are four buttons: "Default", "Advanced Setting", "OK", and "Cancel".

### NOTE

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

## Schedule Update

The Schedule Update lets you schedule eScan database updates.



The screenshot shows the 'Schedule Update' dialog box. It has a title bar with a 'Help' button. The main area contains three sections:
 

- Download Method:** Two radio buttons: 'Automatic Download' (selected) and 'Schedule Download'.
- Schedule Options:**
  - Daily:** Selected radio button.
  - Weekly:** Radio button with checkboxes for Mon, Tue, Wed, Thu, Fri, Sat, and Sun.
  - Monthly:** Radio button with a dropdown menu showing '1'.
- Time:** A radio button labeled 'At' is selected, followed by a text box containing '12:00 am' and a clock icon.

 At the bottom, there are four buttons: 'Default', 'Advanced Setting', 'Ok', and 'Cancel'.

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

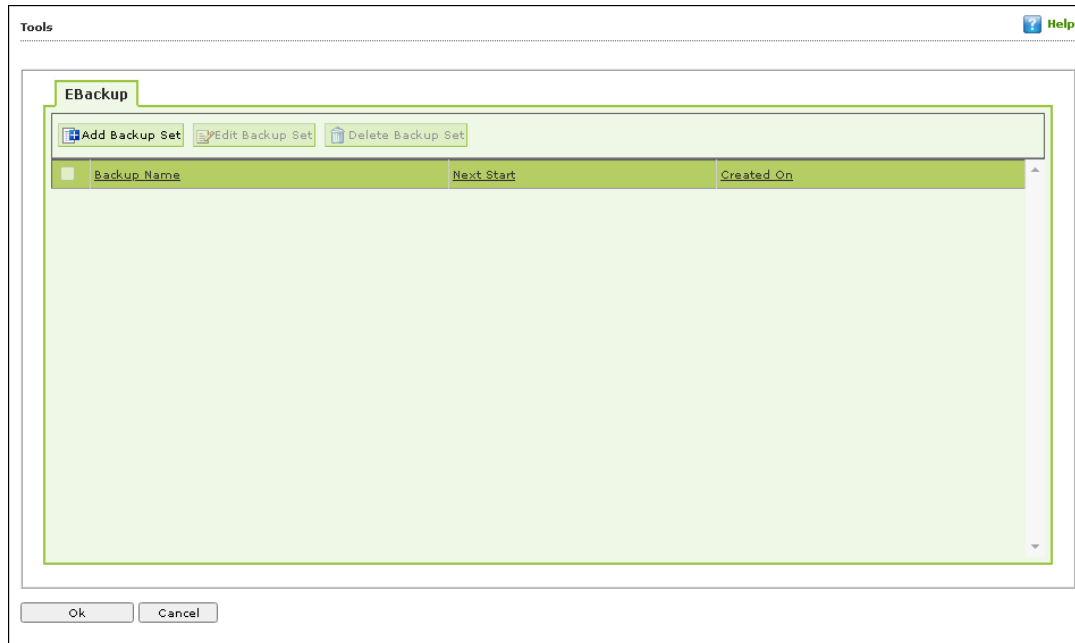
-OR-

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



## Tools

The Tools lets you configure eBackup Settings.



### eBackup

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

With eBackup feature you can:

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

## Add Backup Set

To create a Backup Set,

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

### NOTE

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

3. Select **Tools** check box and then click **Edit**.
4. Click **Add Backup Set**.

Add Backup Set window appears.

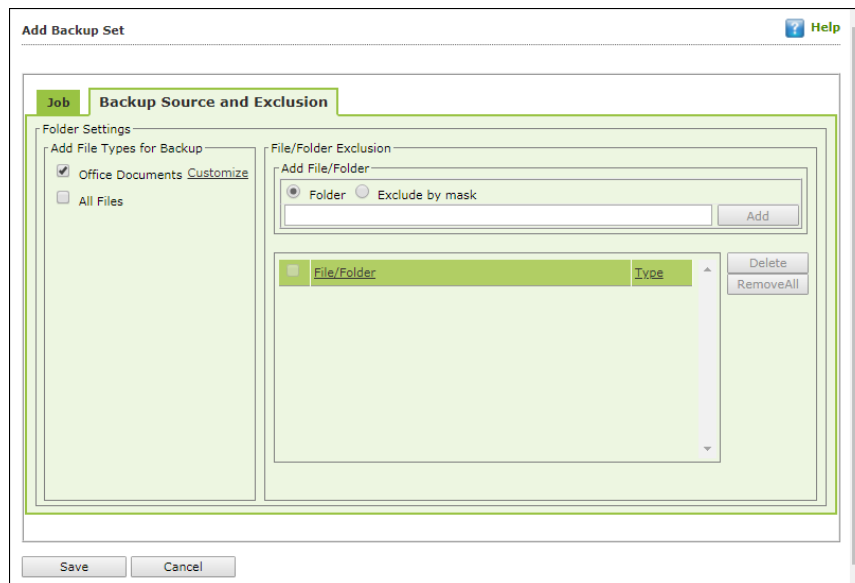
5. Enter a name.
6. In the Scheduler section, select a preferred interval for backup execution.
7. Administrator can save the backup set in the Network Drive by providing the path of the drive and Username and password for the network drive.

### NOTE

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.

In case of system crash or hardware failure, user can recover the created data backup, so storing the backup in the network drive, mapped drive, or NAS drive would be useful in such scenarios.

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



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

**NOTE**

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

### Edit Backup Set

To edit a Backup Set,

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

### Delete Backup Set

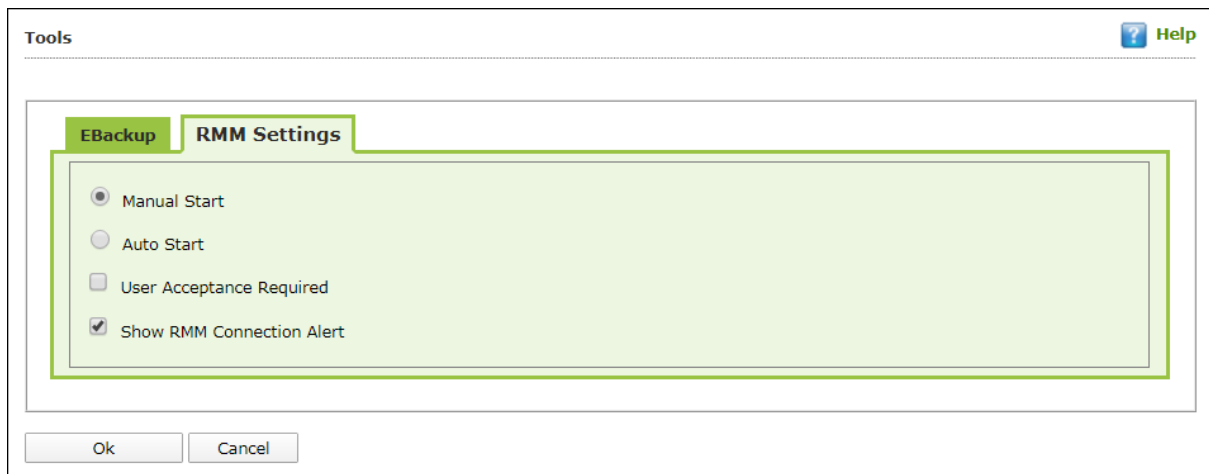
To delete a Backup Set,

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

The Backup Set will be deleted.

## RMM Settings

The RMM settings let you configure default connection settings for connecting to client computers. You will get the following configuration options:



- **Manual Start:** If this option is selected, client endpoint users have to manually start the RMM service to establish a RMM connection.
- **Auto Start:** If this option is selected, RMM service will be started automatically and all client endpoints will be connected to your main eScan server.
- **User Acceptance Required:** If this check box is selected, a pop-up appears on client endpoint for RMM connection acceptance. If left unselected, pop-up doesn't appear and you get direct access to the client endpoint.
- **Show RMM Connection Alert:** If this check box is selected, a notification appears on client endpoint informing about active RMM connection. If left unselected, notification doesn't appear on client endpoint.

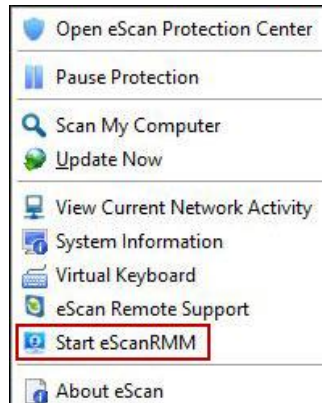
After making the necessary changes click **OK**.

Click **Save**. The Policy Template gets saved.

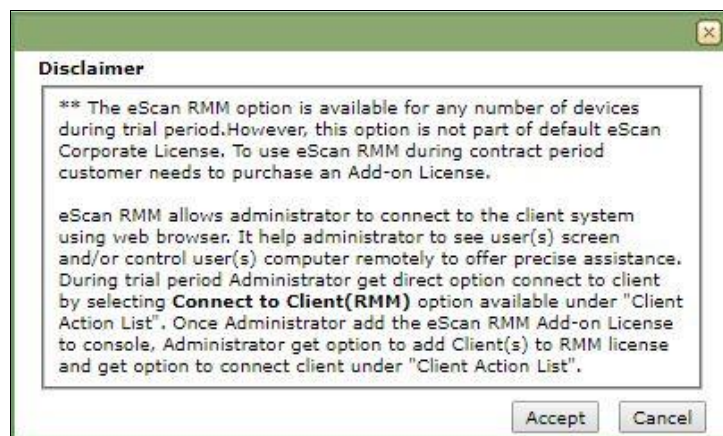
## RMM - Manual Start

To take a remote connection by using **Manual Start** option

1. Tell the client endpoint user to right-click the eScan Protection Center icon and click **Start eScanRMM**.



2. After the client endpoint user has clicked **Start eScanRMM**, select the target endpoint and then click **Client Action List > Connect to Client (RMM)**. Following disclaimer appears.

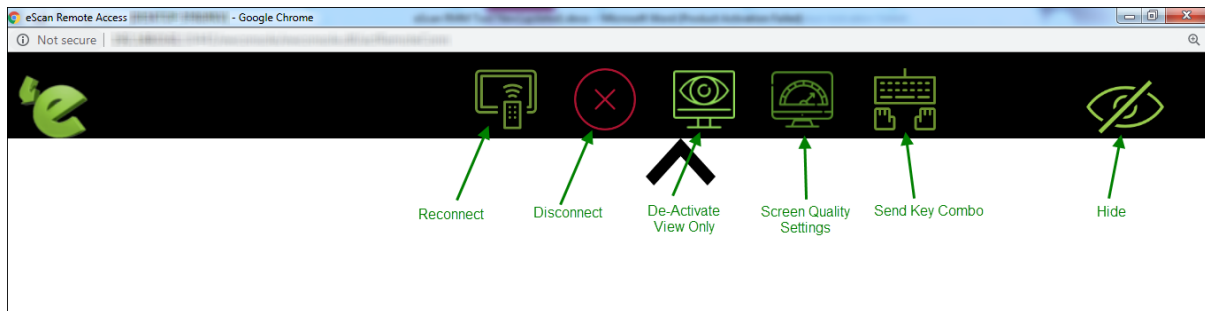


### NOTE

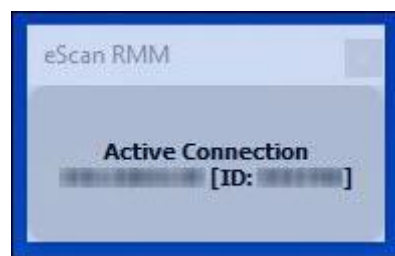
If you are using eScan product in Trial version, this disclaimer will appear each time you are connecting to an endpoint via RMM feature.

A local server won't be part of RMM and can't be connected via RMM.

3. Read the disclaimer thoroughly and then click **Accept**.  
Your default browser opens eScan Remote Access window (Google Chrome, Mozilla Firefox, MS Edge, etc.)



Following notification appears on client endpoint displaying IP address of RMM connecting endpoint and connection ID (If **Show RMM Connection Alert** option is selected).



## RMM - Auto Start

If **Auto Start** option is selected, then client endpoints get automatically connected to your eScan server.

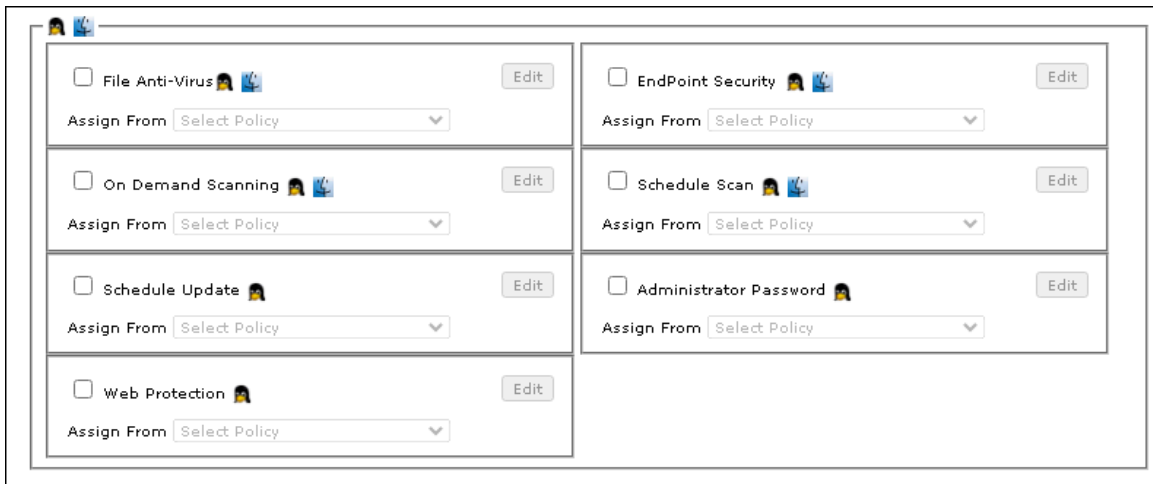
1. Go to **Managed Computers**, select the target endpoint and then click **Client Action List > Connect to Client (RMM)**.  
RMM disclaimer appears.
2. Read the disclaimer thoroughly and then click **Accept**.  
Your default browser opens eScan Remote Access window (Google Chrome, Mozilla Firefox, MS Edge, etc.)

After you are done performing an activity, click the **Disconnect** icon to end remote connection.

<b>NOTE</b>	To get detailed information about RMM feature, <a href="#">click here</a> .
-------------	---

## 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.



<b>NOTE</b>	<p>Icons next to every module displays that the settings are valid for the respective operating systems only.</p> <p>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.</p>
-------------	--

## File Anti-Virus 🐧 🐧

File Anti-Virus 🐧 🐧
Help

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

☐ Archives 🐧 🐧
☒ Packed 🐧 🐧
☐ Follow symbolic links 🐧

☐ Mails 🐧
☐ Cross file system 🐧

☒ Display attention messages  
Number of days log should be kept 365

☐ Exclude by mask 🐧

Add

Delete
RemoveAll

☐ Exclude Files / Folders 🐧 🐧

Add

Delete
RemoveAll

☒ Add Directory for realtime scan 🐧

Add

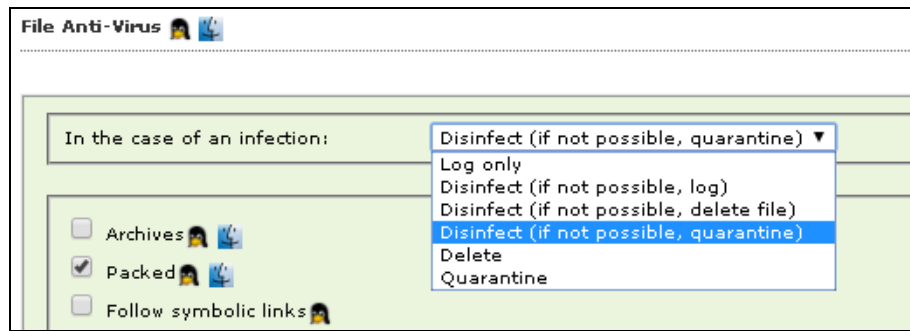
☐ /home
☐ /tmp
Delete
RemoveAll

Default
OK
Cancel

### Actions in case of infection [Drop-down]

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





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

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

### Scan Settings

- **Mails** - It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.
- **Archives** - It indicates the archived files, such as zip, rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.
- **Packed** - It indicates the compressed executable. Select this check box if you want eScan real-time protection to scan packed files.
- **Cross File System** that facilitates scanning of files over cross-file systems.
- **Follow Symbolic Links:** scans the files following the symbolic links.

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

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

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



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

# Endpoint Security

The Endpoint Security module lets you centrally manage all endpoints on your network and closely monitor all USB activities in real-time. With eScan USB control, you can prevent data theft by blocking all except your trusted USB storage devices and Stop your files from being taken away on thumb drives, iPod, mp3 players and portable USB hard drives.

**Endpoint Security**

Start | Stop

---

**USB Control**

☐ Enable Device Control

☒ Allow All     
 ☐ Block All     
 ☐ Ask Password  
☐ Use Escan Administrator Password  
☐ Use Other Password

**Blacklist**

☐ Block Blacklisted USB Devices

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

Add  
Edit  
Delete  
RemoveAll  
Print

☐ Monitor to USB      ☐ Autoscan to USB

**CD / DVD Settings**

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

Default OK Cancel

**Enable Device Control:** Select this check box to configure the Device Control settings.

- **USB Control:** This option lets you to allow, block, or ask password for the USB device connected to the endpoint. It has following options:
  - **Allow All:** Select this option to allow all the connected USB devices.
  - **Block All:** Select this option to block all the connected USB devices.
  - **Ask Password:** Select this option to set password for the connected USB devices. This will ask password before allowing USB devices to connect to the system. You can either set a password or use the administrator password using options **Use Other Password** and **Use Escan Administrator Password** respectively.
- **Blacklist:** This option let's you to add USB devices to the blacklist. You can add, delete, modify using the following options:

- **Add:** Click **Add** to add the USB serial number, name, and description of the USB devices. The USB will be added to the list.



- **Edit:** Click **Edit** to edit the details of the USB devices.
- **Delete:** Select the USB device and click **Delete** to remove the device from the list.
- **Remove All:** To remove all the USB devices from the list, click **Remove All**.
- **Print:** This will print all the USB devices in the list along with details for the same.
- **Monitor to USB:** Select this check box to monitor all the connected USB devices connected to the endpoints.
- **Autoscan to USB:** Select this option to auto-scan all the USB devices connected to the endpoints.

### CD/DVD Settings

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

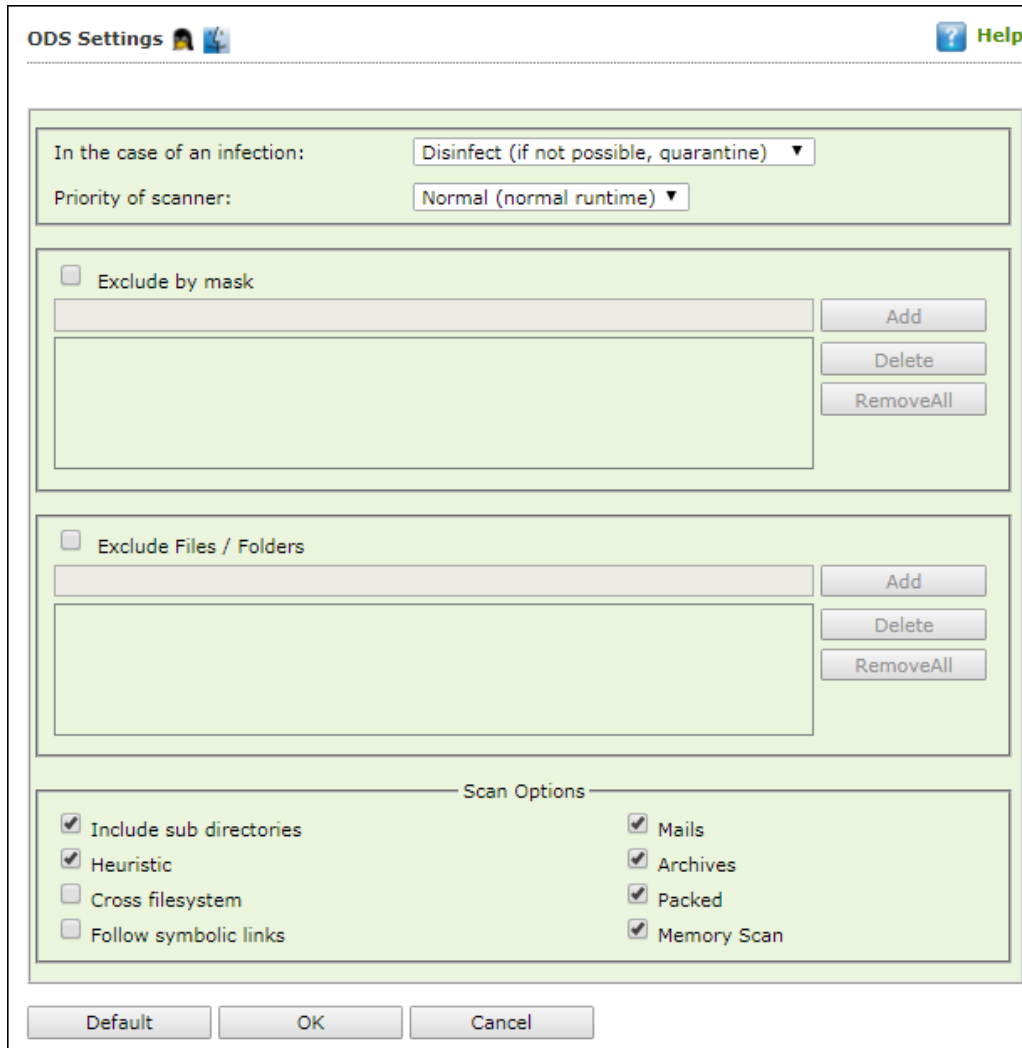
- **Block CD/DVD:** This option block all the CD and DVD.
- **Read Only CD/DVD:** This option allows user to only read the content CD and DVD.
- **Disable:** This option disables all the CD and DVD.

### Default

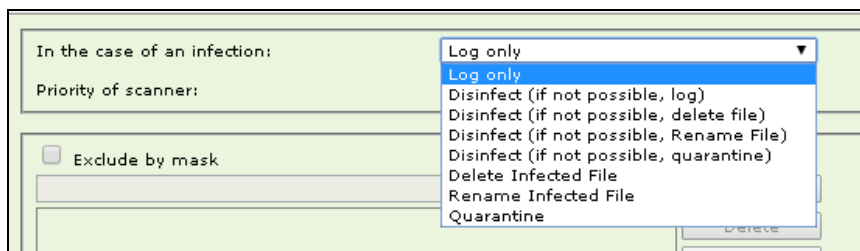
This button resets all the setting to default.

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

**Priority of Scanner** – You can select the priority of scanning as **High (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 check box if you want eScan real-time protection to exclude specific files, and Remove any or all Added Files whenever required.

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

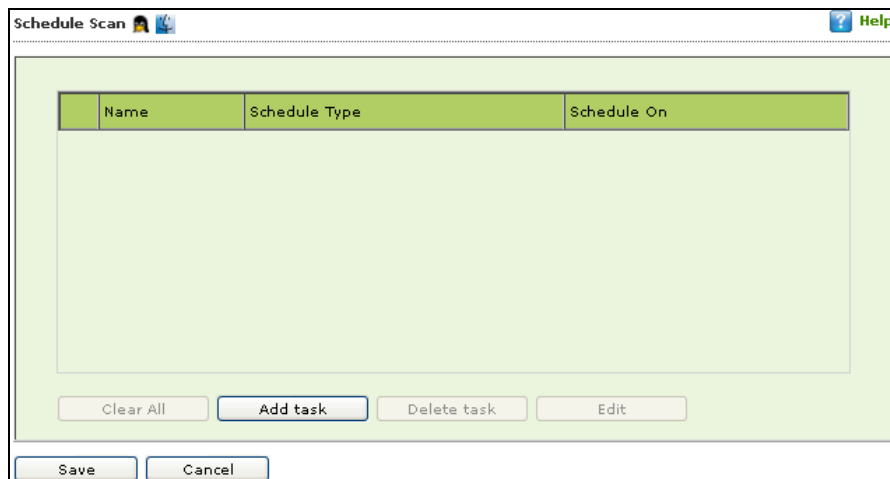
#### Scan options

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

- **Heuristic** – Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application.
- **Cross File System** that facilitates scanning of files over cross-file systems.
- **Follow Symbolic Links:** scans the files following the symbolic links.
- **Memory Scan:** This will scan the memory of the system.

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

## Schedule Scan

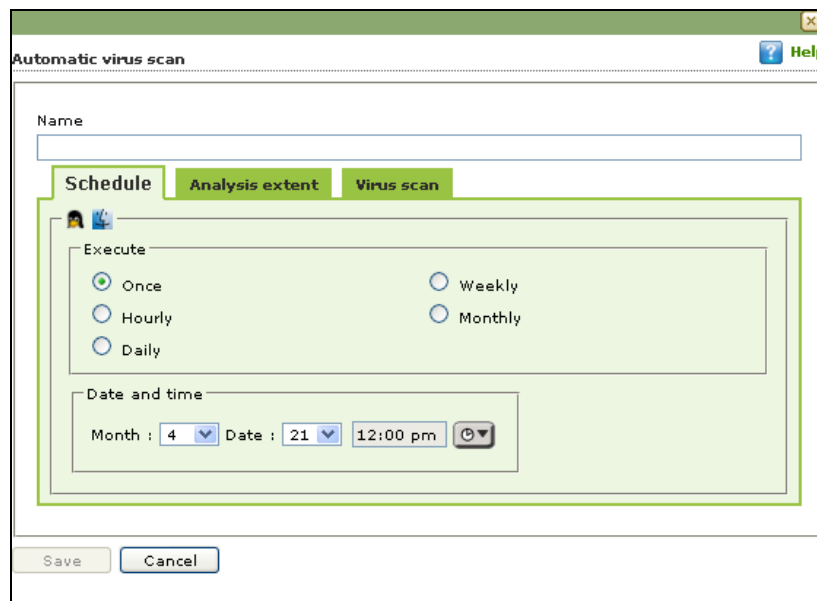


It lets you add a task for scheduling a scan.

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

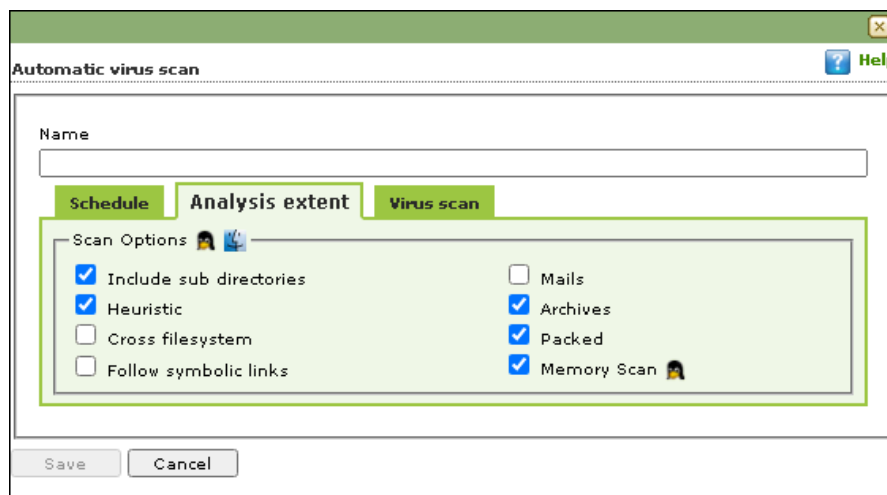
## Automatic Virus Scan

### Schedule



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

## Analysis Extent



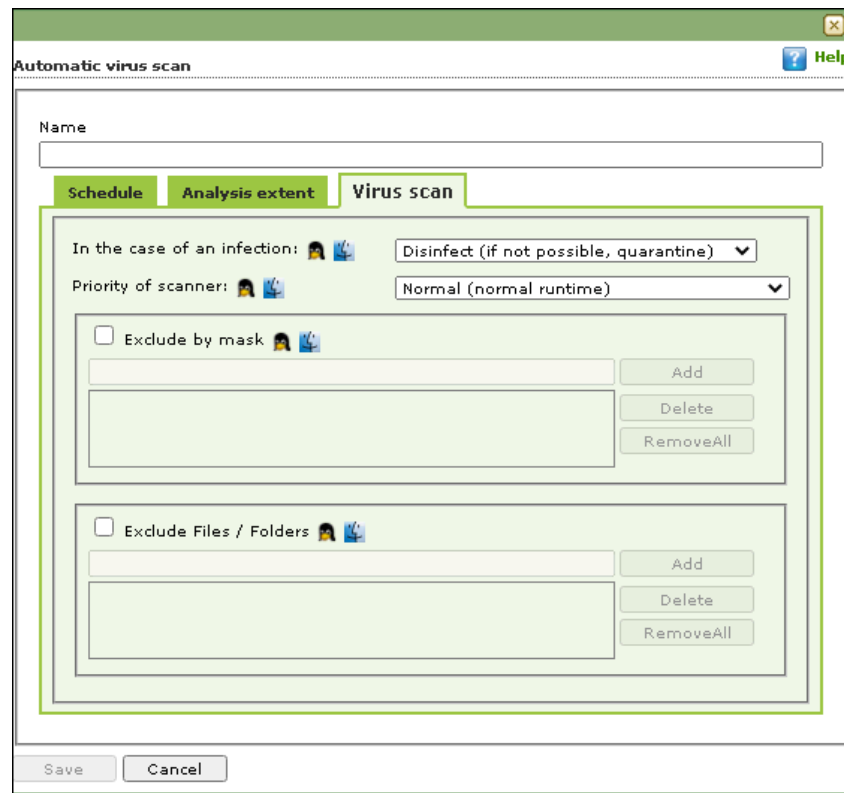
Using this tab you can define the scan options for Linux and Mac computers connected to the network.

- **Include sub Directories** – This option lets you include sub directories while conducting an automatic scan.
- **Heuristic Scan** – Heuristic scanning is almost identical to signature scanning, which instead of looking for specific signatures looks for certain instructions or commands within a program/application. This results in the detection of potentially malicious function in program/application.





- **Cross File System** that facilitates scanning of files over cross-file systems.
- **Symbolic Link Scanning** scans the files following the symbolic links.
- **Mails** - It indicates scanning the mail files. By default, it is selected. Select this check box if you want eScan real-time protection to scan mails.
- **Archives** - It indicates the archived files, such as zip, rar, and so on. Select this check box if you want eScan real-time protection to scan archived files.
- **Packed** - It indicates the compressed executable. Select this check box if you want eScan real-time protection to scan packed files.
- **Memory Scan** - This option will only scan the memory of the system.



### Actions in case of Infection [Drop-down]

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

- **Log Only:** It indicates or alerts the user about the infection detected.
- **Disinfect (if not possible, log):** It tries to disinfect and if disinfection is not possible it logs the information of only the infected object.
- **Disinfect (if not possible, delete file):** It tries to disinfect and if disinfection is not possible it deletes the infected object.
- **Disinfect (if not possible, quarantine file):** It tries to disinfect and if disinfection is not possible it quarantines the infected object.
- **Delete:** Infected objects are deleted with this option.
- **Quarantine:** Infected objects are quarantined with this option.

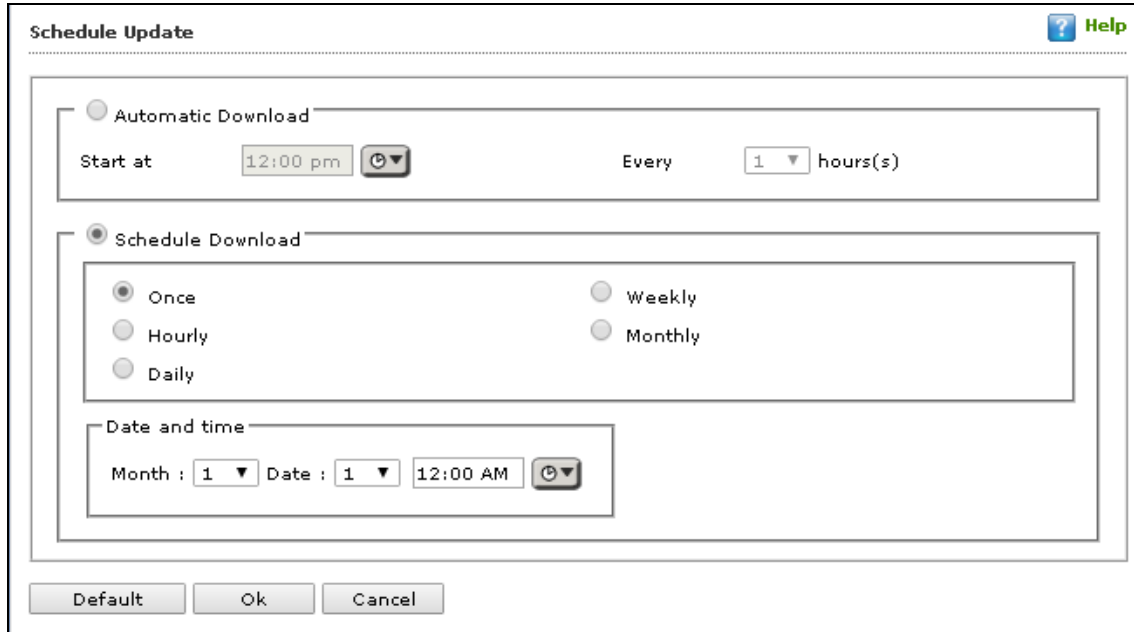
**Exclude file types (Mask)** - Select this check box if you want eScan real-time protection to exclude specific files, and then add the directories and files that you want to exclude by clicking **Add**. eScan lets you Remove any or all Added Files whenever required.



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

## Schedule Update 🐧

This module lets you schedule the updates for Linux computers.

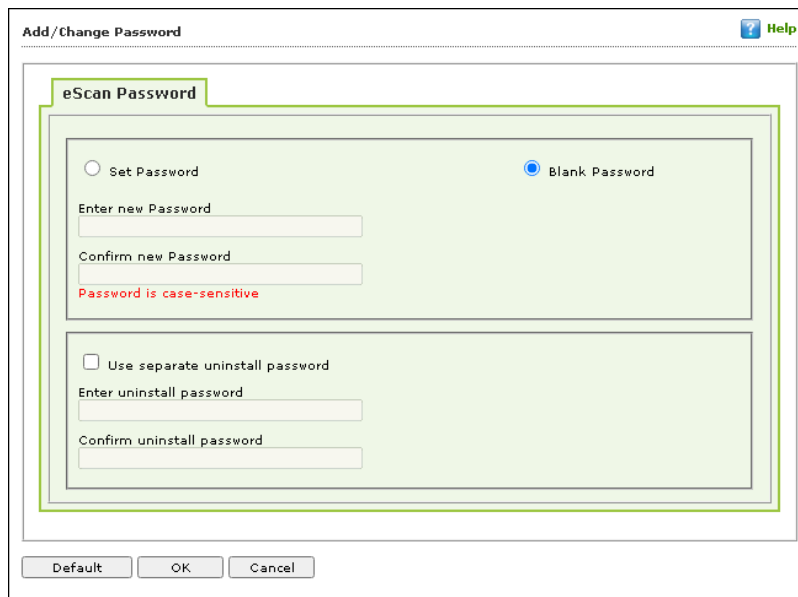


The screenshot shows the 'Schedule Update' dialog box. It has a title bar with a 'Help' button. The dialog is divided into two main sections: 'Automatic Download' and 'Schedule Download'. The 'Automatic Download' section is currently selected and shows a 'Start at' field set to '12:00 pm' with a clock icon, and an 'Every' field set to '1' with a dropdown arrow, followed by 'hours(s)'. The 'Schedule Download' section is also visible and contains five radio button options: 'Once', 'Hourly', 'Daily', 'Weekly', and 'Monthly'. Below these options is a 'Date and time' section with 'Month' and 'Date' dropdowns both set to '1', and a time field set to '12:00 AM' with a clock icon. At the bottom of the dialog 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.



The image shows a dialog box titled "Add/Change Password" with a "Help" icon in the top right corner. The dialog has a tab labeled "eScan Password". Inside the tab, there are two radio buttons: "Set Password" (unselected) and "Blank Password" (selected). Below the "Set Password" option, there are two text input fields: "Enter new Password" and "Confirm new Password". A red text label "Password is case-sensitive" is positioned below the "Confirm new Password" field. Below the "Blank Password" option, there is a checkbox labeled "Use separate uninstall password" which is currently unchecked. Below this checkbox, there are two text input fields: "Enter uninstall password" and "Confirm uninstall password". At the bottom of the dialog, there are three buttons: "Default", "OK", and "Cancel".

### 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.

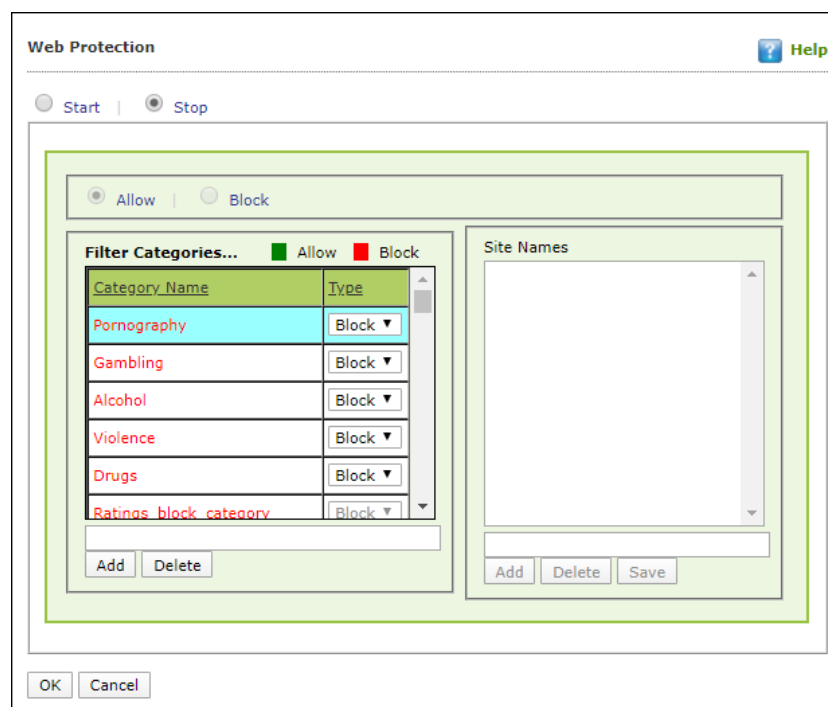
After filling all fields, click **OK**. The Password will be saved.

## 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

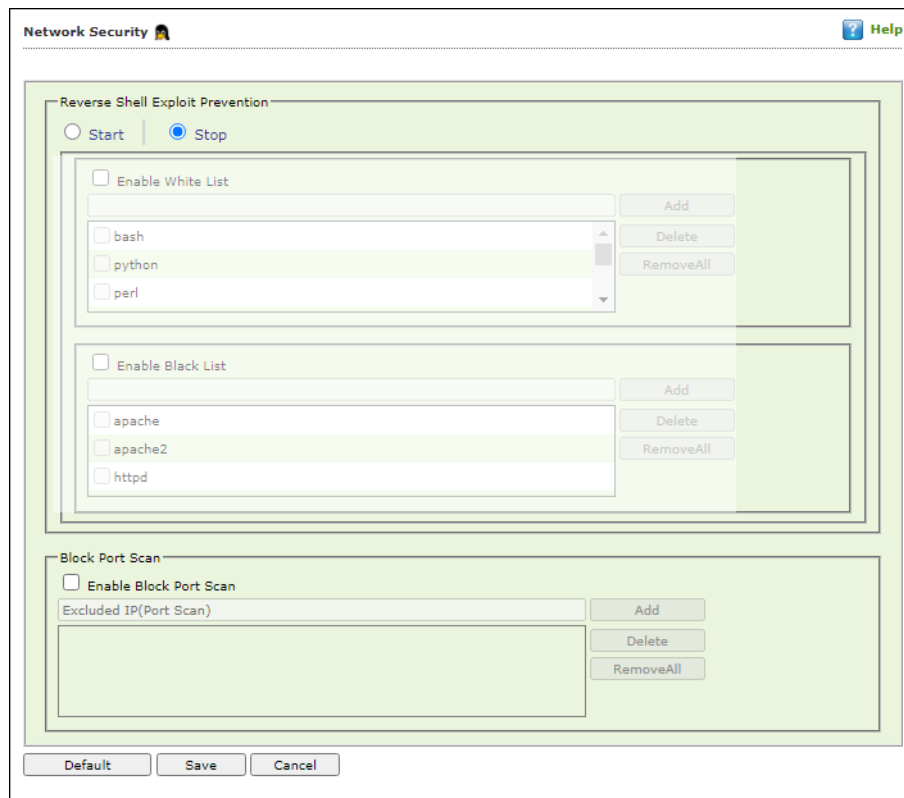
This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category. You can also add or delete filter categories depending on your requirement.

### Filter Options

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

## Network Security 🛡️

Network Security module helps to prevent the Reverse Shell Exploit and blocks the Port Scan. Enabling this features will prevents Zero-day attacks and all other cyber threats.



## Start/Stop

It lets you enable/disable **Network Security** module. Click the appropriate option.

After enabling this, you can configure the following settings:

## Enable White List

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

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

## Enable Black List

Select this checkbox to blacklist the scripting languages, such as bash, Python, Perl, and more. You can add and delete the scripting languages from blacklisting.

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

## Block Port Scan

### 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**.

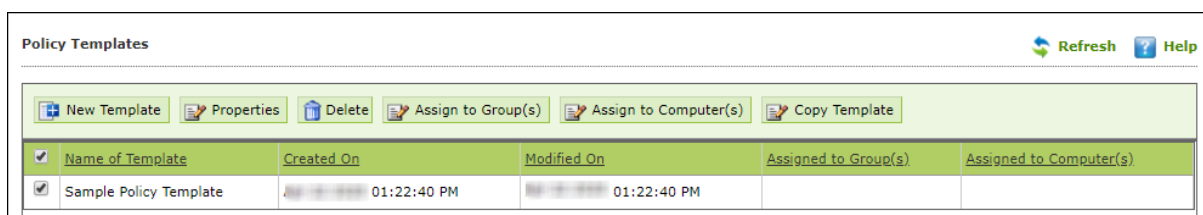
## Assigning Policy Template to a group

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

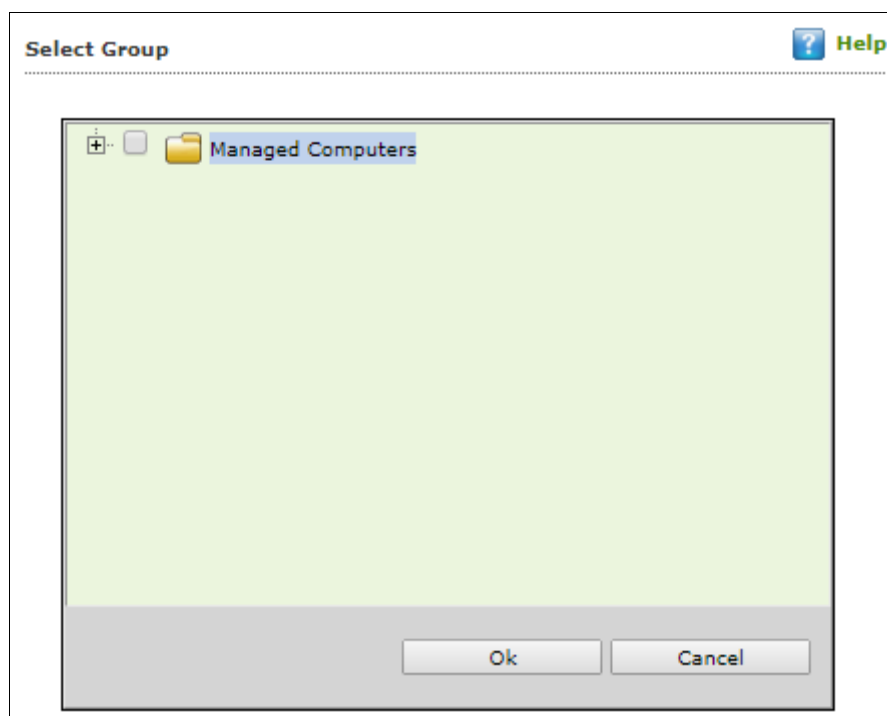
### Method 1

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.

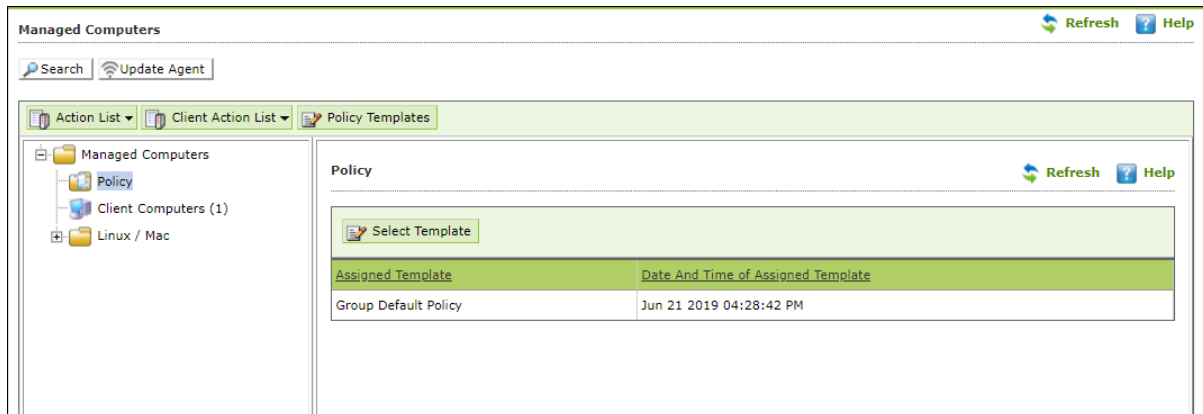


4. Select the group(s) and then click **OK**.  
The policy will be assigned to the selected group(s).

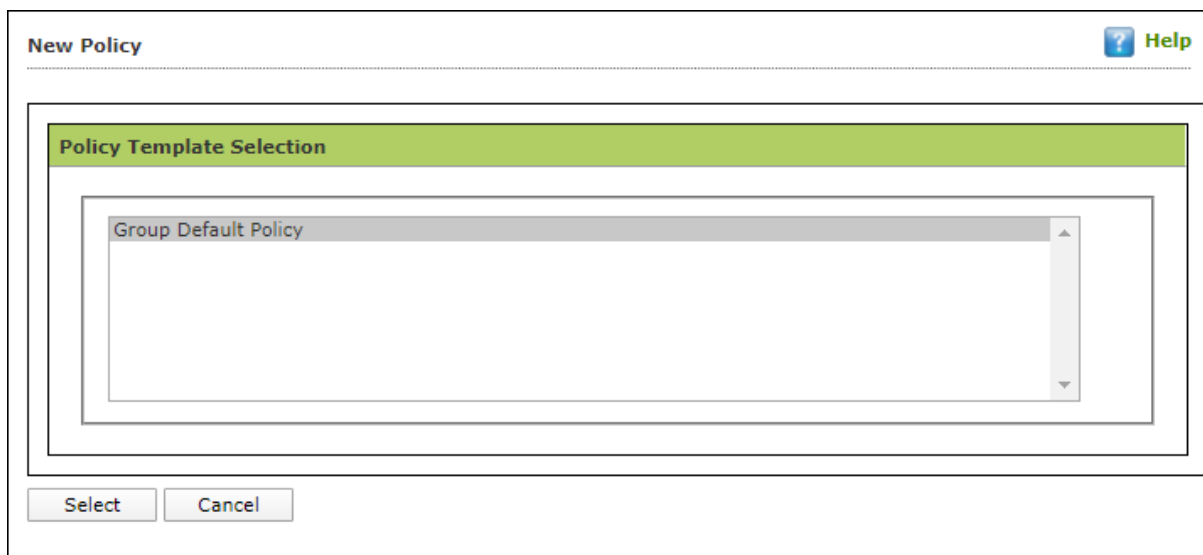
## Method 2

To assign a Policy to the group:

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



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

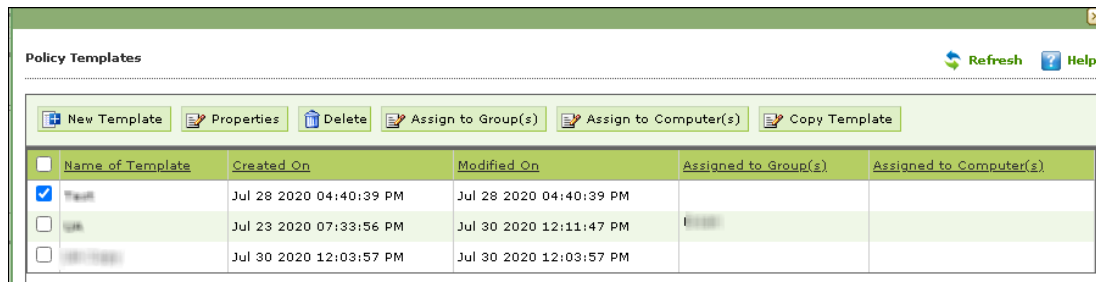


4. Select a policy template and then click **Select**.  
The default Policy Template for group will be saved and updated.

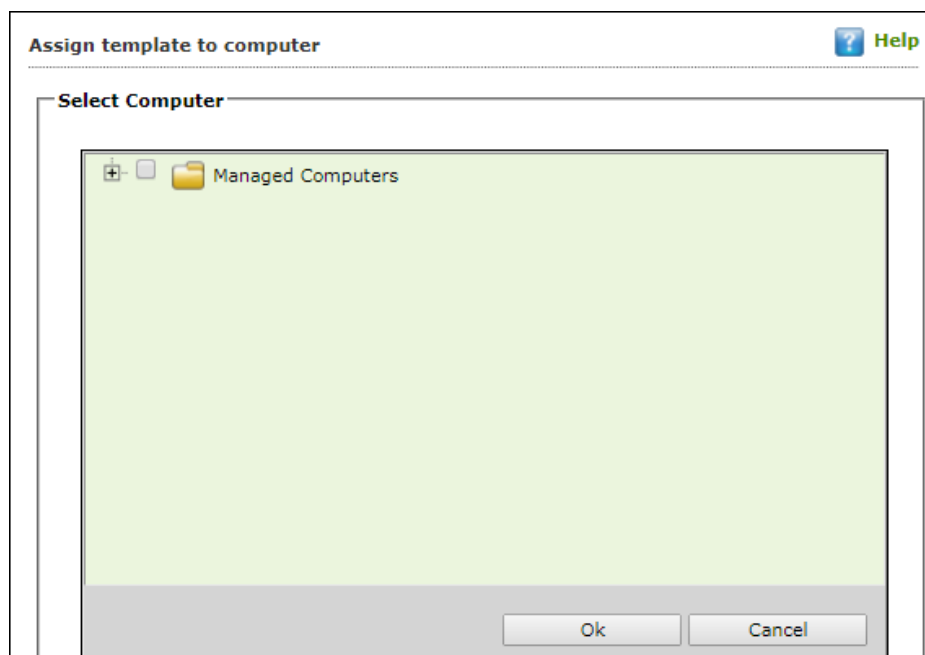
## Assigning Policy Template to Computer(s)

To assign a policy template to computers,

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



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

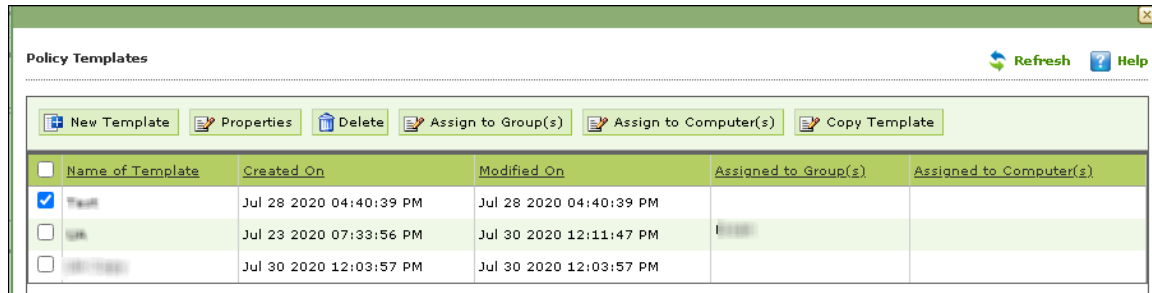


4. Click **Managed Computers**.
  5. Select the computer(s) and then click **OK**.
- The policy template will be assigned to the selected computers.

## Copy a Policy Template

To copy a Policy Template,

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



	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
<input checked="" type="checkbox"/>	Default	Jul 28 2020 04:40:39 PM	Jul 28 2020 04:40:39 PM		
<input type="checkbox"/>	Lock	Jul 23 2020 07:33:56 PM	Jul 30 2020 12:11:47 PM		
<input type="checkbox"/>	Off-Topic	Jul 30 2020 12:03:57 PM	Jul 30 2020 12:03:57 PM		

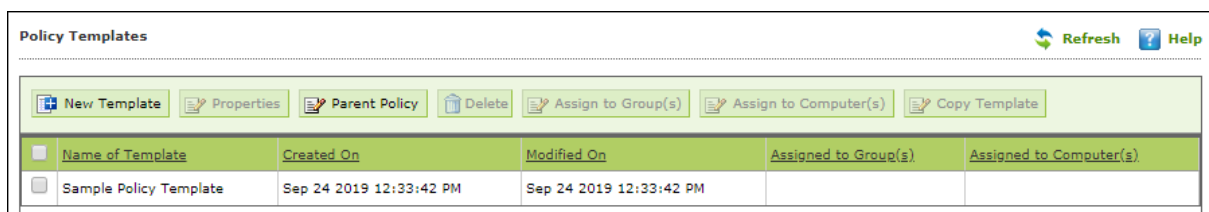
3. Click **Copy Template**.  
New Template window appears displaying settings from the original template.
4. Enter a name for the template.
5. Make the necessary changes and then click **Save**.  
The template will be copied.

## Parent Policy

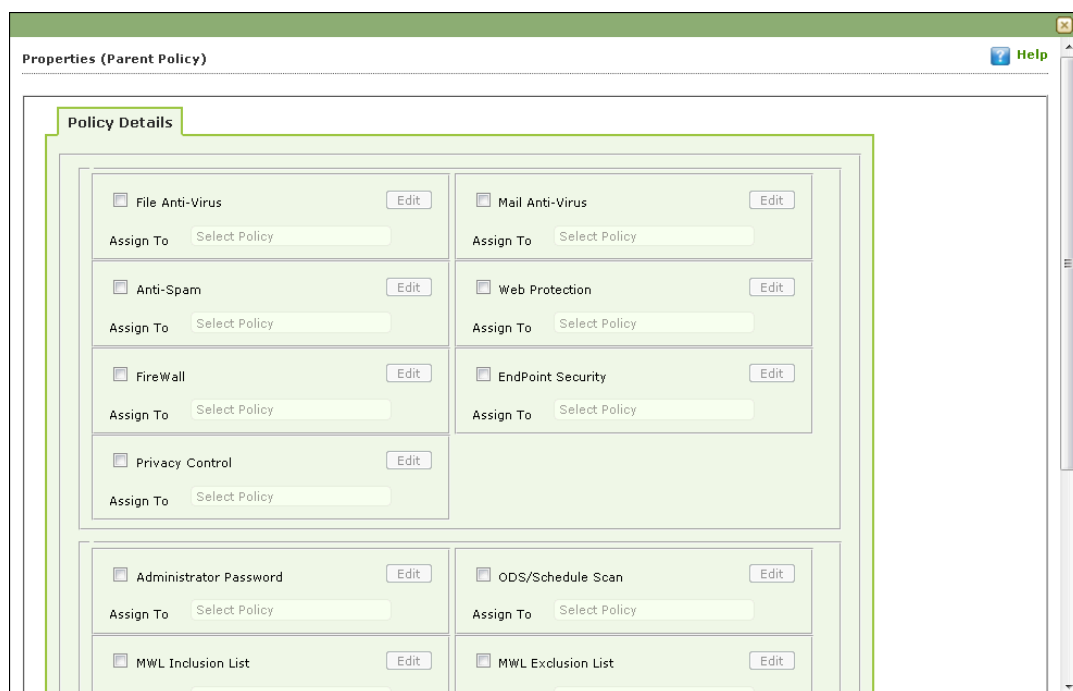
The **Parent Policy** lets you to implement a change in policy setting to multiple policies at the same time. For example, if you want to make a policy change in a single module like **File Anti-Virus** in multiple policies; you can do this all at a time using Parent Policy.

To configure Parent Policy, follow the steps given below:

4. In the Managed Computers screen, click **Policy Templates**.  
Policy Templates window appears.
5. In the Policy Template window, click **Parent Policy**.

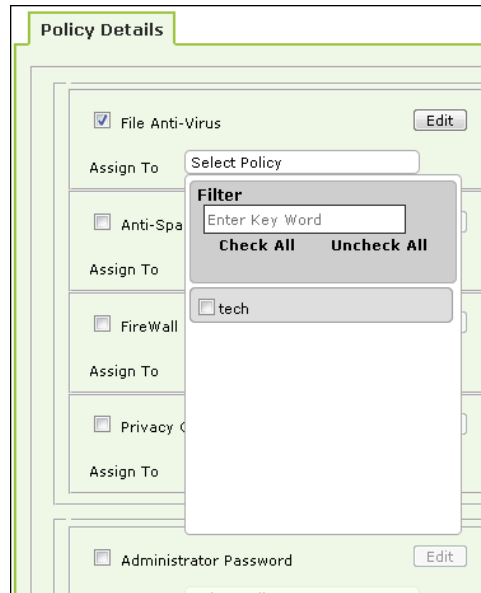


Properties (Parent Policy) window appears displaying all the policies.



6. Select and edit the required module according to your preferences.

7. Click **Assign To** drop-down and select the policies for which the parent policy changes should be applied.



8. Click **OK**. The Parent policy will be updated and changes will be applied to all the policies selected.

**NOTE**

Before disabling a module in Parent Policy, ensure that policies are unchecked from **Assign To** drop-down.

# Data Encryption

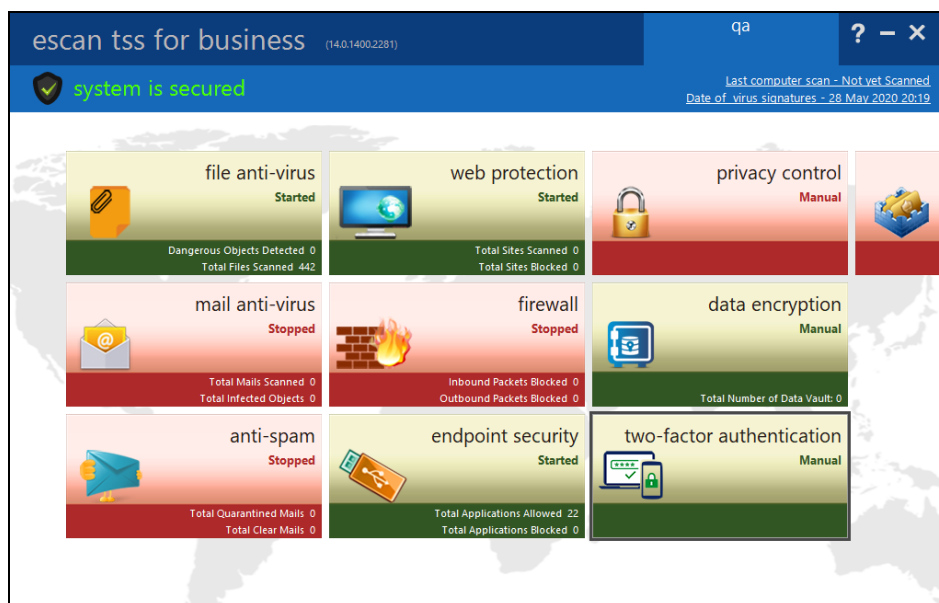
The Data Encryption module lets you protect sensitive and confidential data from unauthorized access and data leak. With this module, the user can create a Vault that stores data in encrypted format.

The Vault is encrypted using 256-bit Advanced Encryption Standard (AES) and HMAC-SHA 256-bit key. A password is required to access the vault. After you access the vault, the data stored will be automatically decrypted. Vice versa, after you close the vault, the data stored will be automatically encrypted.

## How to Create a Vault?

To create a vault, follow the steps given below:

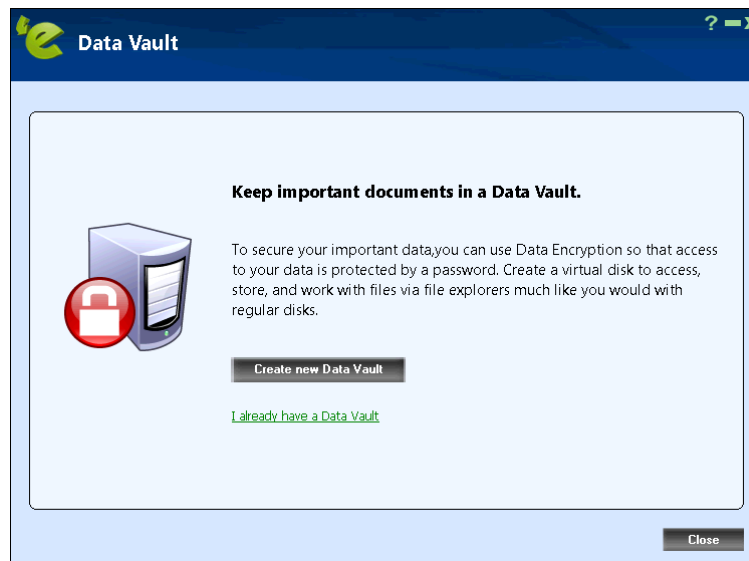
1. Launch eScan.
2. Click **data encryption**.



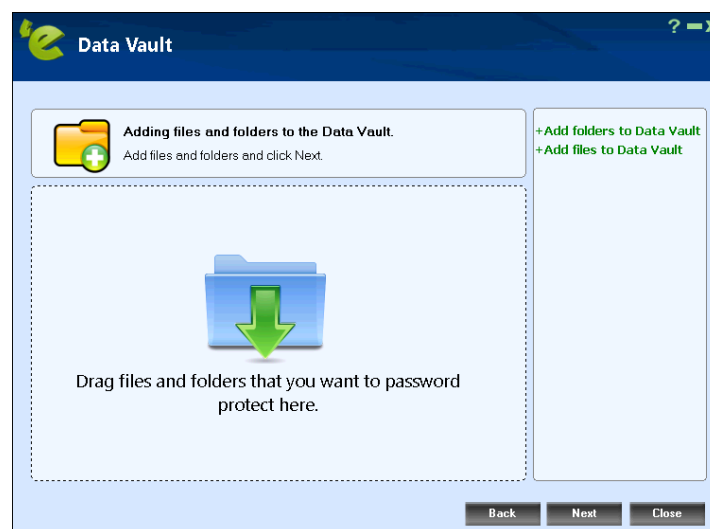
Data Vault window appears.



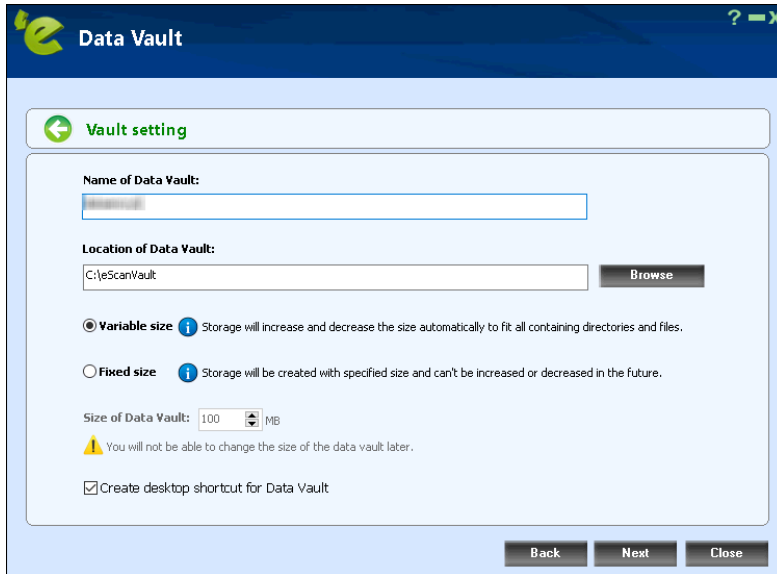
3. Click **Create new Data Vault**.



4. To add files or folders in Data Vault, click **Add folders to Data Vault** or **Add files to Data Vault**.



5. After adding required files and folder, click **Next**.
6. Configure the Data Vault:
  - **Name of Data Vault:** Enter a name for the vault.
  - **Location of Data Vault:** To select a custom location for Data Vault, click **Browse**. The default path for vault is **c:\eScanVault**.
  - Select a size for Data Vault, **Variable size** or **Fixed size**. If selected **Fixed size** enter the size in below field or use the arrow buttons to specify size.
  - Optionally, select the checkbox **Create desktop shortcut for Data Vault**.



**Data Vault**

← **Vault setting**

**Name of Data Vault:**

**Location of Data Vault:**  
 **Browse**

☒ **Variable size** ⓘ Storage will increase and decrease the size automatically to fit all containing directories and files.  
☐ **Fixed size** ⓘ Storage will be created with specified size and can't be increased or decreased in the future.

**Size of Data Vault:**  MB  
 ⚠ You will not be able to change the size of the data vault later.

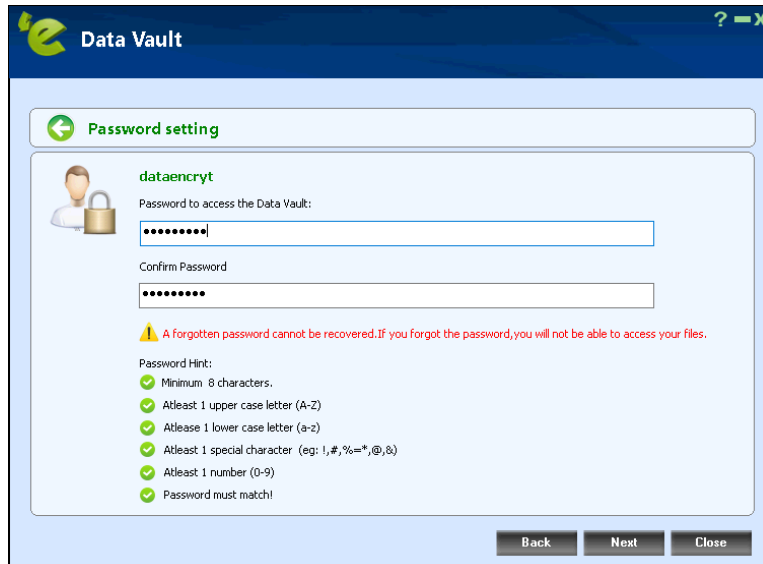
☒ Create desktop shortcut for Data Vault

**Back** **Next** **Close**

7. After filling all the details, click **Next**.
8. Read the **Password Hint** and then enter the password.

**NOTE**

A forgotten password cannot be recovered.  
 If you forgot the password, you cannot access your files.



**Data Vault**

← **Password setting**

**dataencrypt**

**Password to access the Data Vault:**

**Confirm Password:**

⚠ A forgotten password cannot be recovered. If you forgot the password, you will not be able to access your files.

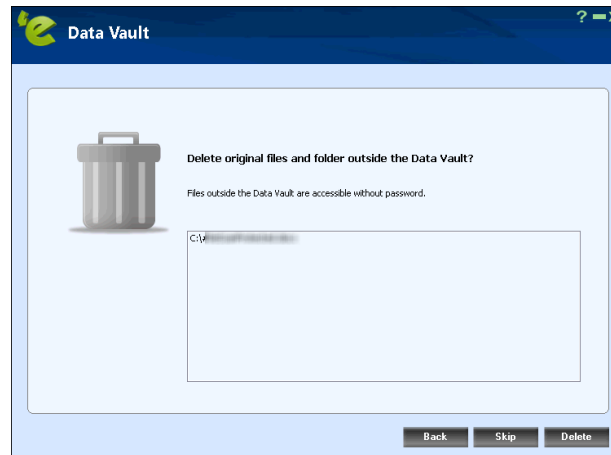
**Password Hint:**

- ✓ Minimum 8 characters.
- ✓ Atleast 1 upper case letter (A-Z)
- ✓ Atleast 1 lower case letter (a-z)
- ✓ Atleast 1 special character (eg: !, #, %, \*, @, &)
- ✓ Atleast 1 number (0-9)
- ✓ Password must match!

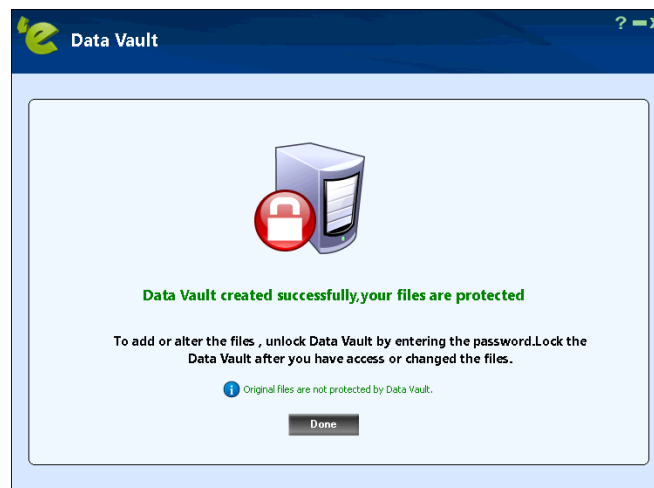
**Back** **Next** **Close**

9. Click **Next**.

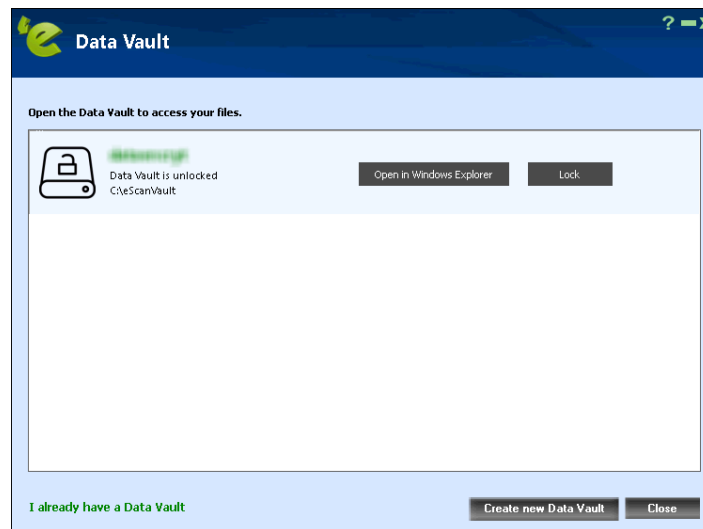
10. Data will be copied to the Data Vault. If you wish to delete the original files and folders outside the data vault by clicking **Delete** or else click **Skip**.



11. Click **Finish**. You will be forwarded to the following screen. Click **Done**.

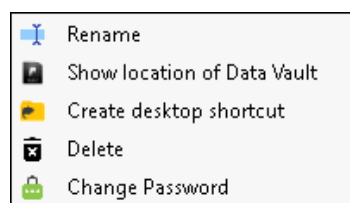


12. The Data Vault will be created and get displayed on the data encryption list. To encrypt your data, click **Lock**.



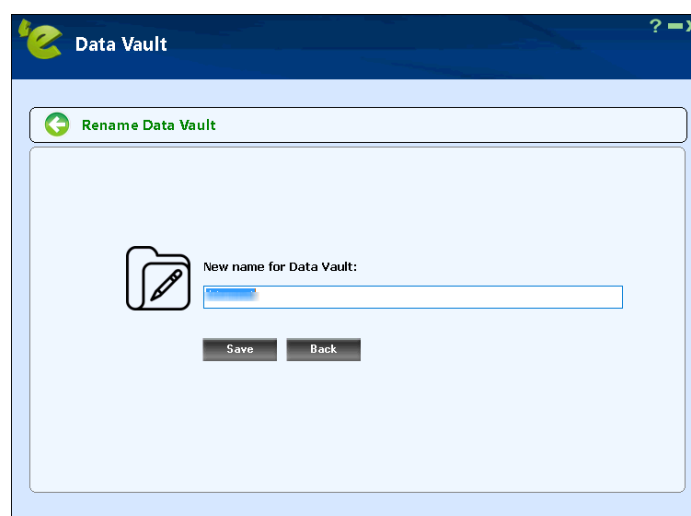
13. Click **Close**. The created Data Vault will be encrypted.

After the data vault is locked, you will get **More** button displayed the right-hand side of the screen. Through this option, you will get the following setting to configure the data vault:



## Rename

You can rename the existing data vault. After clicking on this option, you will get the following screen, where you can rename the vault.





After renaming, click **Save**.

### **Show location of Data Vault**

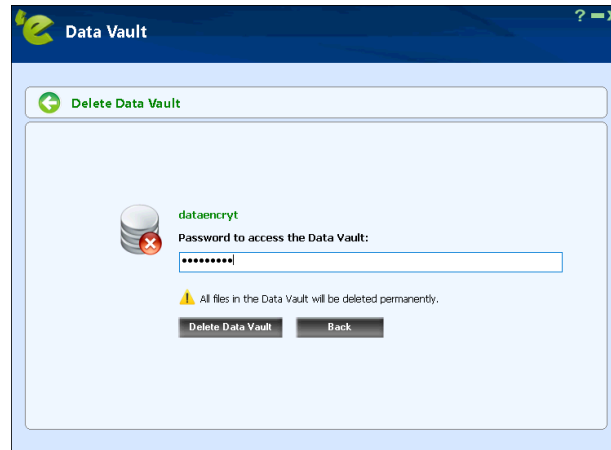
This option will open the location where data vault is created.

### **Create desktop shortcut**

This option will create shortcut for the created vault for accessing it easily.

## Delete

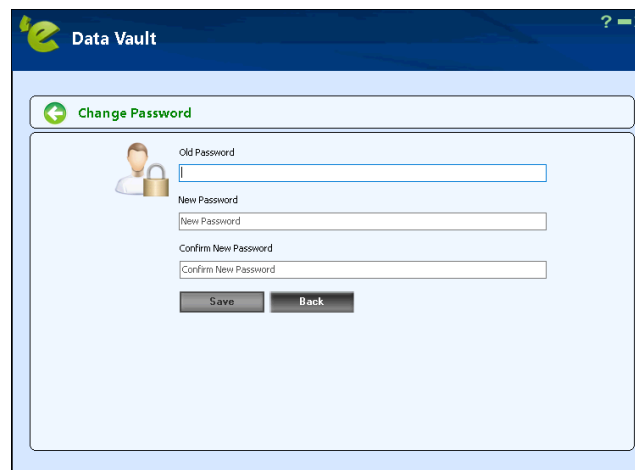
You can delete the existing data vault. Click on this option, you will get the following screen prompting for password.



After entering the password, click **Delete Data Vault**. This will delete the selected data vault.


## Change Password

This option allows you to change the password set for the data vault. Click this option; you will forward to the following screen.



Enter the **Old Password**, **New Password**, and **Confirm New Password**. Click **Save**. This will change the password of the data vault.

### Note

If you selected **Create desktop shortcut for Data Vault** checkbox, it will create a shortcut of data vault (  ).

# Policy Criteria Templates

This button allows to add criteria template based on the endpoints conditions.

## Adding a Policy Criteria Template

To define Policy Criteria Template, follow the steps given below:

1. In the Managed Computers screen, click **Policy Criteria Templates**.

Policy Criteria screen appears.

Name of Criteria	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
------------------	------------	-------------	----------------------	-------------------------

2. Click **New Criteria**.

Policy Criteria screen displays parameter for creation.

Criteria Name:

Description:

Conditions for criteria:

3. Enter **Name** and **Description**.
4. Click **Add** drop-down.
5. Click **Add AND Condition**.

Specify Criteria screen appears.

**Specify criteria** ? Help

Type : Computer IP Address ▼

☒ If the client computer has one of the IP addresses listed below  
☐ If all of the IP addresses of the client computer are listed below  
☐ If the client computer does not have any of the addresses listed below

Condition

Type	Content
------	---------

Add Edit Delete

Ok Cancel

6. Click the **Type** drop-down. It displays following options:

- Computer IP Address
- Management Server Connection
- Users
- Machine Name

Depending upon the option, the conditions and settings vary.

## Computer IP Address

1. Select the appropriate condition.
2. Click **Add**.

Address window appears.

**Address**

Type : IP Address ▼

IP Address :

Ok Cancel

3. Enter the IP address.



4. Click **OK**.

The Policy Criteria Template for an IP Address will be saved.

## Management Server Connection

The dialog box titled "Specify criteria" contains a dropdown menu labeled "Type :" with "Management Server Connection" selected. Below the dropdown are two radio button options: "If the client computer can connect to the management server" (which is selected) and "If the client computer can not connect to the management server". At the bottom are "Ok" and "Cancel" buttons.

1. Select the appropriate condition.
2. Click **OK**.

The Policy Criteria Template for Management Server Connection will be saved.

## Users

The dialog box titled "Specify criteria" has a "Help" icon in the top right corner. It features a dropdown menu labeled "Type :" with "Users" selected. Below this is a radio button option "If the client computer has one of the Username listed below" which is selected. Underneath is a section labeled "Condition" containing a list box with "Username" as the only entry. At the bottom of the list box are buttons "Add", "Add AD users", "Edit", and "Delete". Below the list box are "Ok" and "Cancel" buttons.

### Adding Local Users

1. To add local users, click **Add**.  
Username window appears.

A small dialog box titled "Username". It contains a text input field labeled "Username" and two buttons at the bottom: "Ok" and "Cancel".

2. Enter a Username.
  3. Click **OK**.
- The local user will be added.

## Adding Active Directory Users

To add Active Directory users, follow the steps given below:

1. Click **Add AD Users**.
- Add Active Directory Users window appears.

The "Add Active Directory Users" window is shown. It has a title bar with a "Help" icon. Below the title bar is a breadcrumb: "User Accounts > Add Active Directory Users". The main area is divided into two sections: "Search Criteria" and "Search Results".

**Search Criteria**

- User's name\*: [Text Input Field]
- For Example: user or user\*
- Domain\*: [Text Input Field]
- AD IP Address\*: [Text Input Field]
- AD Admin User name\*: [Text Input Field]
- For Active Directory account: domain\username
- AD Admin Password\*: [Text Input Field]
- Use SSL Auth.: ☐
- AdsPort\*: [Text Input Field with value 389]
- [Search Button]

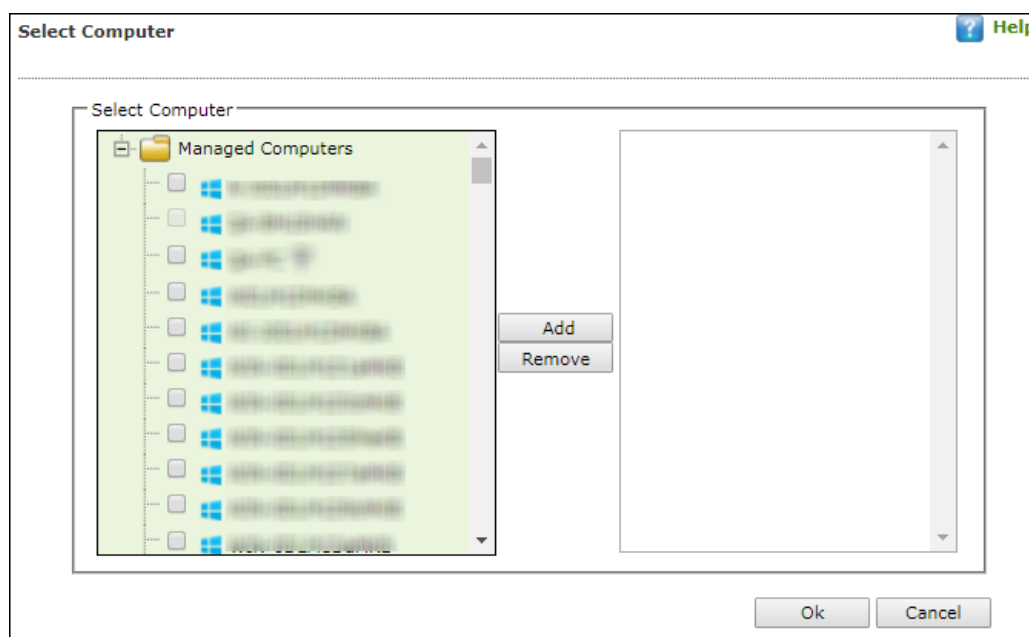
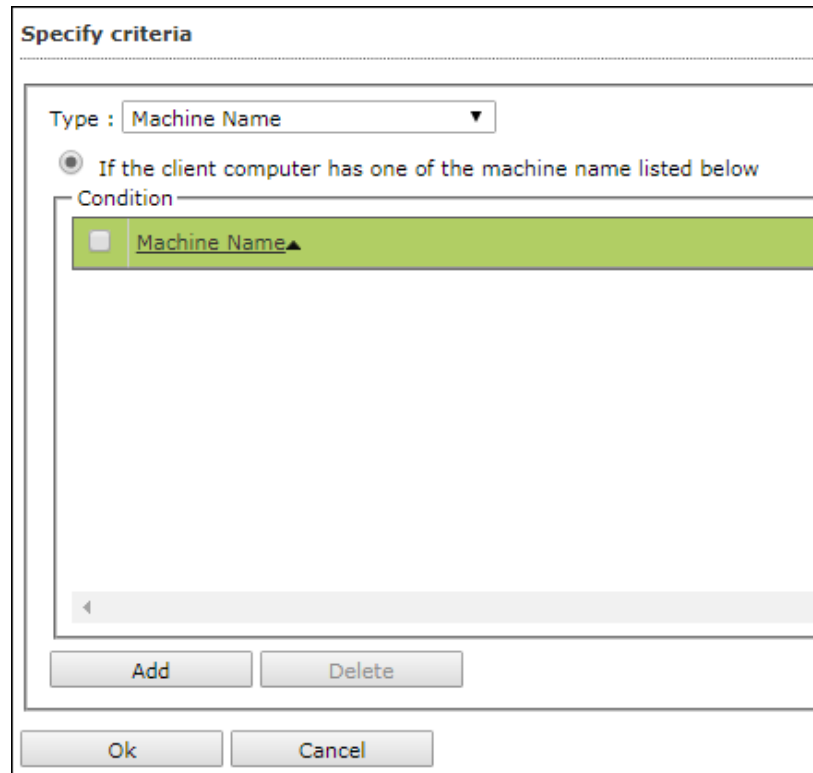
**Search Results**

Users	Selected Users
[List of users]	[List of selected users]

2. Enter data in mandatory fields.
3. Click **Search**.
4. Search Results section displays a list of discovered users in **Users** list. Select a user and then click button to add the user to **Selected Users** list. Vice versa the added user can be moved from Selected Users to Users by clicking .
5. Click **OK**.



The Policy Criteria Template for Users will be saved.



## Viewing Properties of a Policy Criteria template

To view the properties of a Policy Criteria Template, follow the steps given below:

1. Select a policy criteria template.
2. Click **Properties**.

Policy Criteria				
<div> </div>				
<input checked="" type="checkbox"/>	Name of Criteria	Created On	Modified On	Assigned to Group(s)
<input checked="" type="checkbox"/>	aaa	Sep 26 2019 03:44:12 PM	Sep 26 2019 03:44:12 PM	Group Default Policy Managed Computers

Policy Criteria window appears.

Policy Criteria

Criteria Name: aaa  
Description:

Conditions for criteria:

Add Edit Delete

Condition

- ☒ If all of the IP addresses of the client computer are listed below
  - ☐ - 192.168.0.01

Save Close

3. Make the necessary changes and click **Save**.  
The Policy Criteria template will be saved and updated.

## Copying a Policy Template

To copy a Policy Template, follow the steps given below:

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

Policy Templates				
<div> </div>				
<input checked="" type="checkbox"/>	Name of Template	Created On	Modified On	Assigned to Group(s)
<input checked="" type="checkbox"/>	Sample Policy Template	Sep 24 2019 12:33:42 PM	Sep 24 2019 12:33:42 PM	

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 click **Save**.  
The template will be copied.

## Deleting a Policy Criteria template

To delete assigned policy criteria template, follow the steps given below:

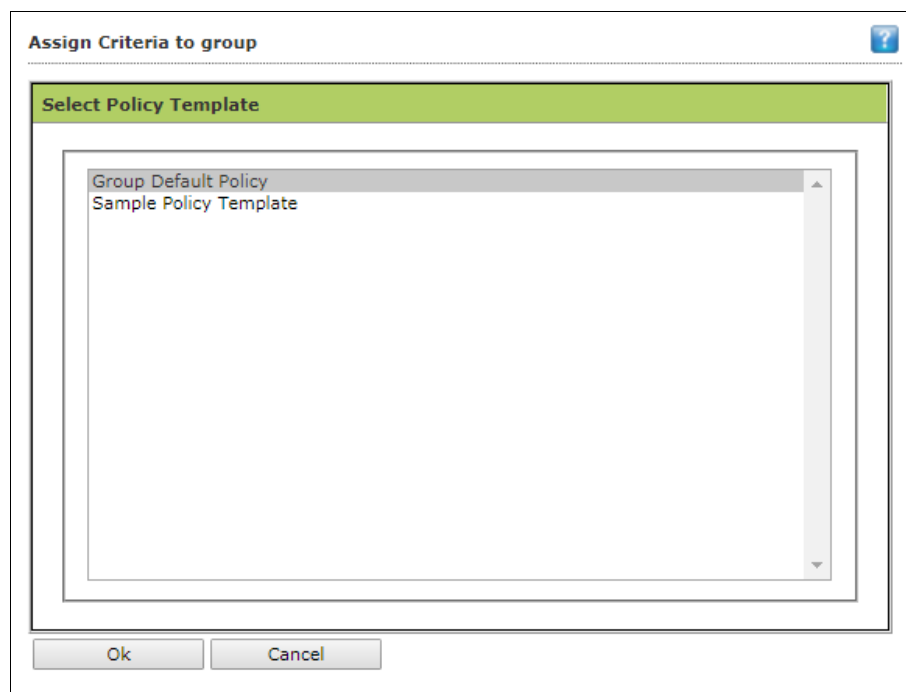
The Policy Criteria window displays to which group or computer the template is assigned in Assigned to Group(s) or Assigned to Computer(s) column.

For explanation, we are following the procedure as per the screenshot below

1. Select a policy criteria template.
2. Click **Assign To > Groups**.

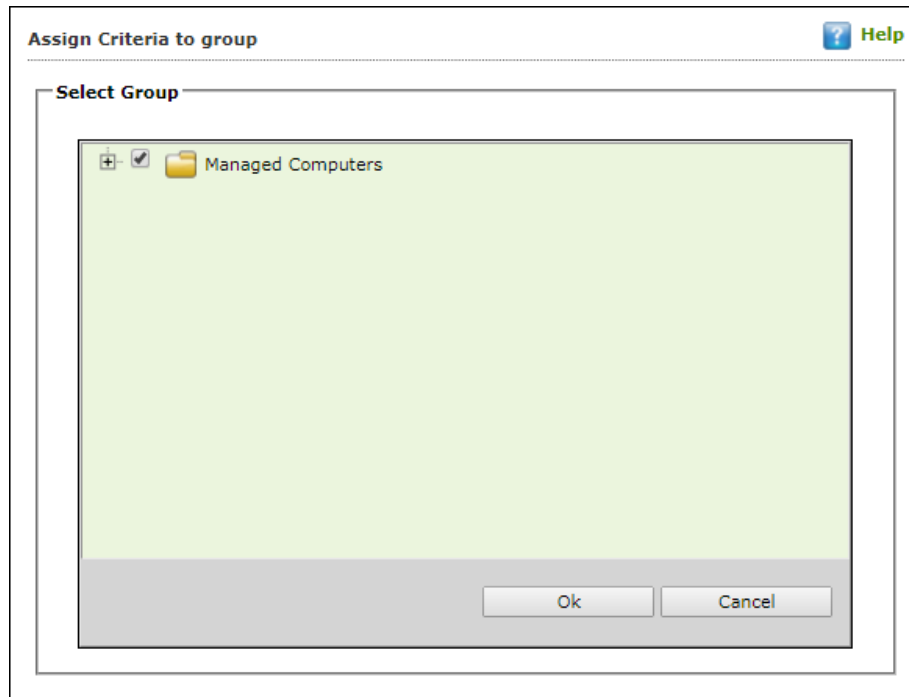
Policy Criteria				
<a href="#">New Criteria</a> <a href="#">Properties</a> <a href="#">Delete Criteria</a> <a href="#">Assign To</a>				
<input checked="" type="checkbox"/>	Name of Criteria	Created On	Modified On	
<input checked="" type="checkbox"/>	aaa	Sep 26 2019 03:44:12 PM	Sep 26 2019 03:44:12 PM	<b>Group Default Policy</b> Managed Computers

Assign Criteria to Group window appears.



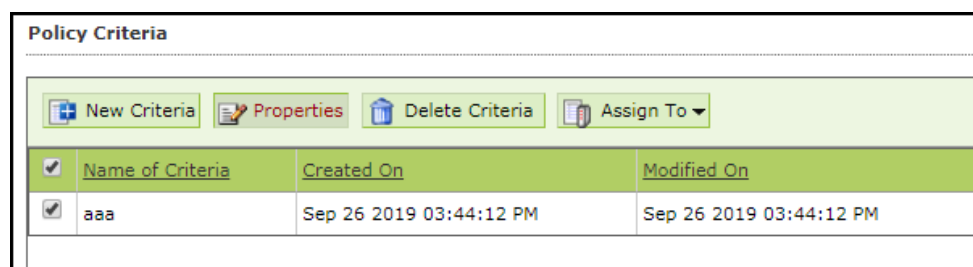
3. Click **Group Policy Template > OK**.

Assign Criteria to group window displays Managed Computers folder tree.



4. Uncheck the selected group.
5. Click **OK**.

The Policy Criteria Template will no longer be assigned to any group. This enables **Delete Criteria** button.



6. Select the template.
  7. Click **Delete Criteria**.
- The Policy Criteria Template will be deleted.

# Unmanaged Computers

To install eScan Client, define policies and tasks on the basis of group, it is necessary to move computers to the created groups. You can move the computers from **Unmanaged Computers** to desired groups created in the **Managed Computers** using the following submodules:

- **Network Computers**
- **IP Range**
- **Active Directory**
- **New Computers Found**

## Network Computers

This submodule displays a list of available networks. You can move the computers from the list of computers present in the Network Computers using the following steps –

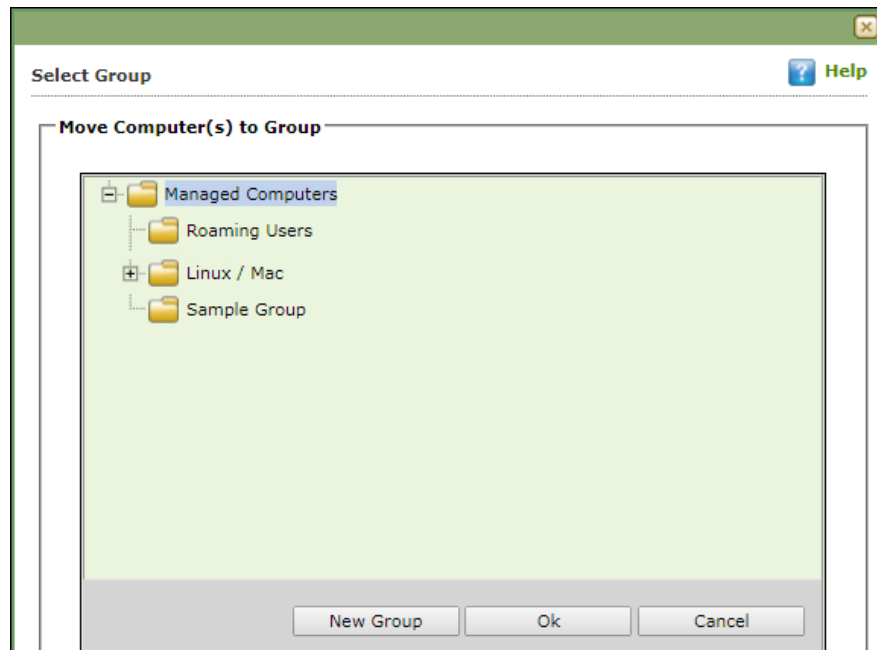
1. In the navigation panel, click **Unmanaged Computers > Network Computers**.
2. Click **Microsoft Windows Network**.
3. Select the workgroup from where you want to move computers to the group created in Managed Computers section. A list of computers appears.



4. Select the computer(s) you want to move to the desired groups.
5. Click **Action List > Move to Group**. Select Group window appears.



6. Click **Managed Computers** tree to view the groups.

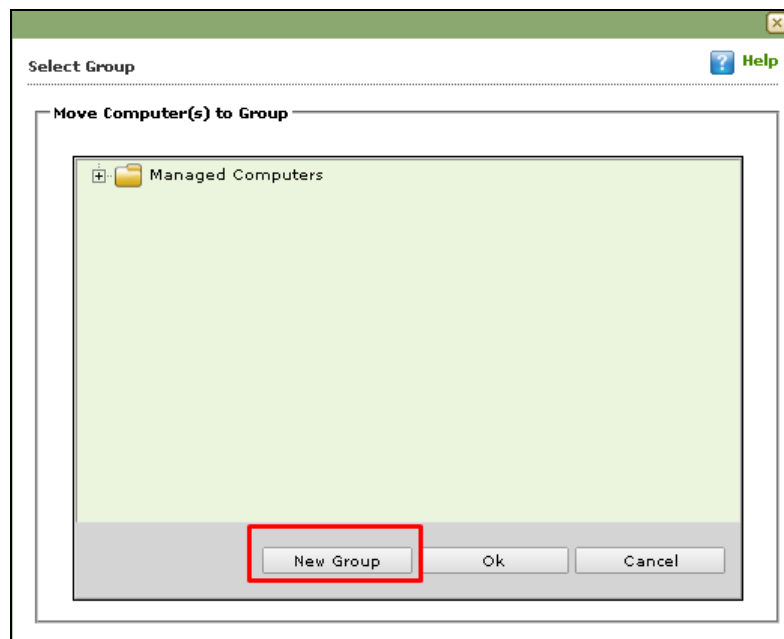


7. Select the group where you wish to move the selected computer(s) and click **OK**.  
The selected computer(s) will be moved to the group.

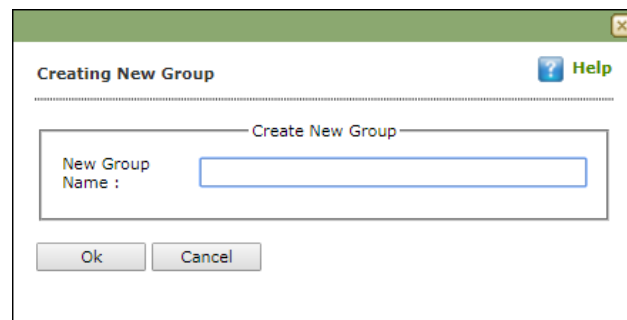
## Creating a New Group from the Select Group window

To create a new group from the Select Group window, follow the steps given below:

1. In the Select Group window, click **Managed Computers** > **New Group**.



Creating New Group window appears.



2. Enter a name for the group.
3. Click **OK**. A new group will be created.

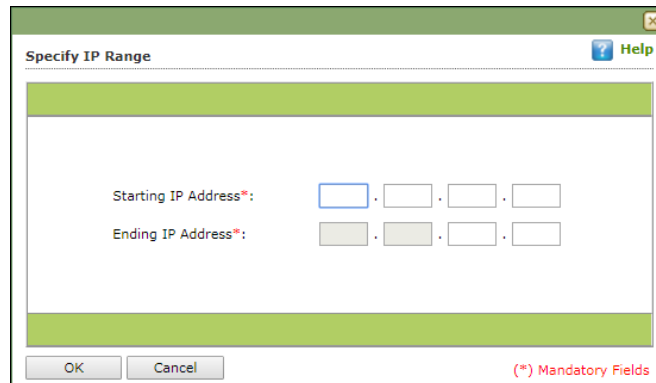
## IP Range

The **IP Range** submodule lets you scan the desired IP address or range of IP address and add the required computers to any of the managed groups. It also lets you add, search and delete an IP range.

## Adding New IP Range

To add an IP range, follow the steps given below:

1. In the IP range screen, click **New IP Range**.  
Specify IP Range window appears.



The dialog box titled "Specify IP Range" has a green header bar with a "Help" icon. It contains two rows of IP address input fields. The first row is labeled "Starting IP Address\*" and the second row is labeled "Ending IP Address\*". Each row has four input boxes separated by dots. At the bottom, there are "OK" and "Cancel" buttons. A red note at the bottom right states "(\*) Mandatory Fields".

2. Enter the Starting and Ending IP address.
3. Click **OK**. The IP Range will be added.

<b>NOTE</b>	<p>Please enter the start and end IP address even if you want to search for single IP address, both the entries will have the same IP address in such a case. The selected IP Range will be added to the IP Range tree.</p> <p>When you select the IP Range all computers present in that IP Range will be displayed on the interface in the right.</p>
-------------	---

Other details like IP Address of the computer, its group, Protection status (Unmanaged/Unknown/Protected/Not installed, Critical/Unknown); the table also displays Status of all modules of eScan.

## Moving an IP Range to a Group

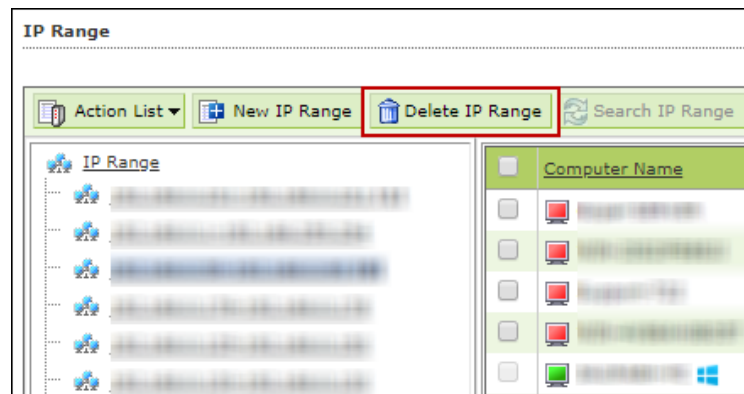
To move an entire IP range to a group, follow the steps given below:

1. Select an IP range.
2. Select the checkbox next to Computer Name column.
3. Click **Action List > Move to Group**. Select Group window appears.
4. Select the destination group.
5. Click **OK**. The IP range will be moved to the specified group.

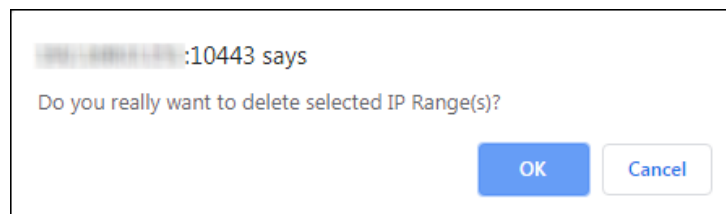
## Deleting an IP Range

To delete an IP range, follow the steps given below:

1. Select an IP Range.
2. Click **Delete IP Range**.



A confirmation prompt appears.



3. Click **OK**. The IP range will be deleted.

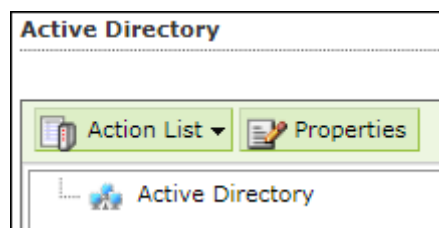
# Active Directory

The Active Directory submodule lets you add computers from an Active Directory.

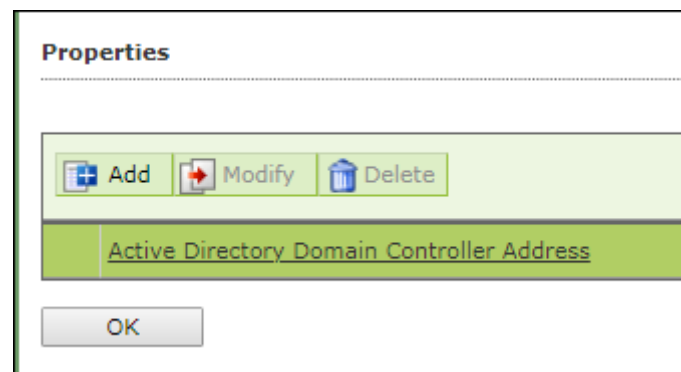
## Adding an Active Directory

To add an Active Directory, follow the steps given below:

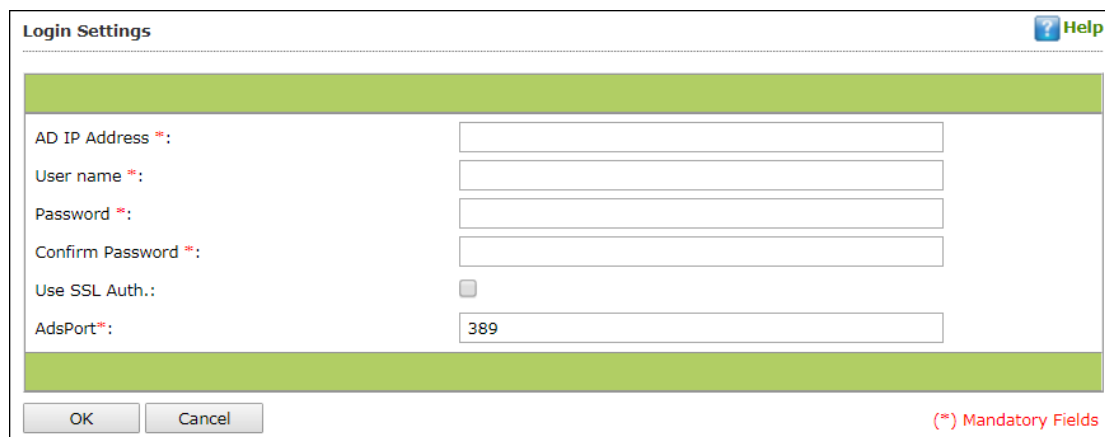
1. Click **Unmanaged Computers > Active Directory**.
2. Click **Properties**.



Properties window appears.



3. Click **Add**. Login Settings window appears.

The screenshot shows a window titled "Login Settings" with a "Help" icon in the top right corner. The window has a green header bar. Below the header, there are several input fields: "AD IP Address (\*)", "User name (\*)", "Password (\*)", "Confirm Password (\*)", "Use SSL Auth." with a checkbox, and "AdsPort(\*)" with the value "389". At the bottom, there are "OK" and "Cancel" buttons. A red note at the bottom right says "(\*) Mandatory Fields".

4. Fill in the required Login Credentials and click **OK**.

The details including IP Addresses from active directory will be added instantly.

Active Directory Domain Controller Address	
<input checked="" type="checkbox"/>	192.168.1.100

5. Select the Active Directory and click **OK**. The selected Active Directory will be added to the Active directory tree.
6. To view the details, click the **Active Directory**.

Computer Name	Status
GA54	Unknown status
GA55	Unknown status
GA56	Unknown status
GA57	Unknown status
GA58	Unknown status
GA59	Unknown status
GA60	Unknown status
GA61	Unknown status
GA62	Unknown status
GA63	Unknown status
GA64	Unknown status
GA65	Unknown status
GA66	Unknown status
GA67	Unknown status
GA68	Unknown status
GA69	Unknown status
GA70	Unknown status
GA71	Unknown status
GA72	Unknown status
GA73	Unknown status
GA74	Unknown status
GA75	Unknown status
GA76	Unknown status
GA77	Unknown status
GA78	Unknown status
GA79	Unknown status
GA80	Unknown status
GA81	Unknown status
GA82	Unknown status
GA83	Unknown status
GA84	Unknown status
GA85	Unknown status
GA86	Unknown status
GA87	Unknown status
GA88	Unknown status
GA89	Unknown status
GA90	Unknown status
GA91	Unknown status
GA92	Unknown status
GA93	Unknown status
GA94	Unknown status
GA95	Unknown status
GA96	Unknown status
GA97	Unknown status
GA98	Unknown status
GA99	Unknown status
GA100	Unknown status

## Moving Computers from an Active Directory

To move computers from an Active Directory, follow the steps given below:

1. Click an Active Directory.
2. Select the computers you want to move to other group.
3. Click **Action List > Move to Group**.  
Select Group window appears.
4. Select the Group and Click **OK**.

The selected computers will be moved to the selected group.

## New Computers Found

The New Computers Found submodule displays list of all new computers connected to the network. With the Action List drop-down you can set Host Configuration, Move Computers to a Group, view Properties and Refresh Client. You can also export the New Computers List to .xls file format.

After the computers are moved from Unmanaged Computers to groups under Managed Computers, you can assign it tasks, Set host configuration, Manage Policies, Deploy/Upgrade Client or deploy a Hotfix on all or any of the Managed Computer individually or in group.

New Computers Found						
<input type="text" value="Search"/>						
<div> <span>Action List ▼</span> <span>Filter Criteria ▲</span> </div>						
<input type="checkbox"/>	Computer Name	IP Address	User name	Last Seen	Belongs To	eScan Status
<input type="checkbox"/>	DESKTOP-1234567	192.168.1.101		23 Sep 2019 10:59:59	Server	Unknown status
<input type="checkbox"/>	DESKTOP-8765432	192.168.1.102		23 Sep 2019 10:59:54	Server	Unknown status
<input type="checkbox"/>	DESKTOP-9876543	192.168.1.103		23 Sep 2019 11:00:12	Server	Unknown status
<input type="checkbox"/>	DESKTOP-4567890	192.168.1.104		23 Sep 2019 11:00:12	Server	Unknown status
<input type="checkbox"/>	DESKTOP-0987654	192.168.1.105		23 Sep 2019 10:59:54	Server	Unknown status
<input type="checkbox"/>	DESKTOP-5678901	192.168.1.106		23 Sep 2019 10:59:54	Server	Unknown status
<input type="checkbox"/>	DESKTOP-2345678	192.168.1.107		23 Sep 2019 11:00:01	Server	Unknown status

## Filter Criteria

The Filter Criteria lets you filter new computers found according to date range.

New Computers Found	
<input type="text" value="Search"/>	
<div> <span>Action List ▼</span> <span>Filter Criteria ▼</span> </div>	
<div>Filter Criteria</div> <div> <div>Date Range</div> <div> From (MM/DD/YYYY) <input type="text" value="11/06/2019"/> </div> <div> To (MM/DD/YYYY) <input type="text" value="11/06/2019"/> </div> </div> <div> <input type="button" value="Search"/> <input type="button" value="Reset"/> </div>	

1. Select appropriate date in **From** and **To** fields.
2. Click **Search**.



A list of computers discovered by eScan in the date range will be displayed.



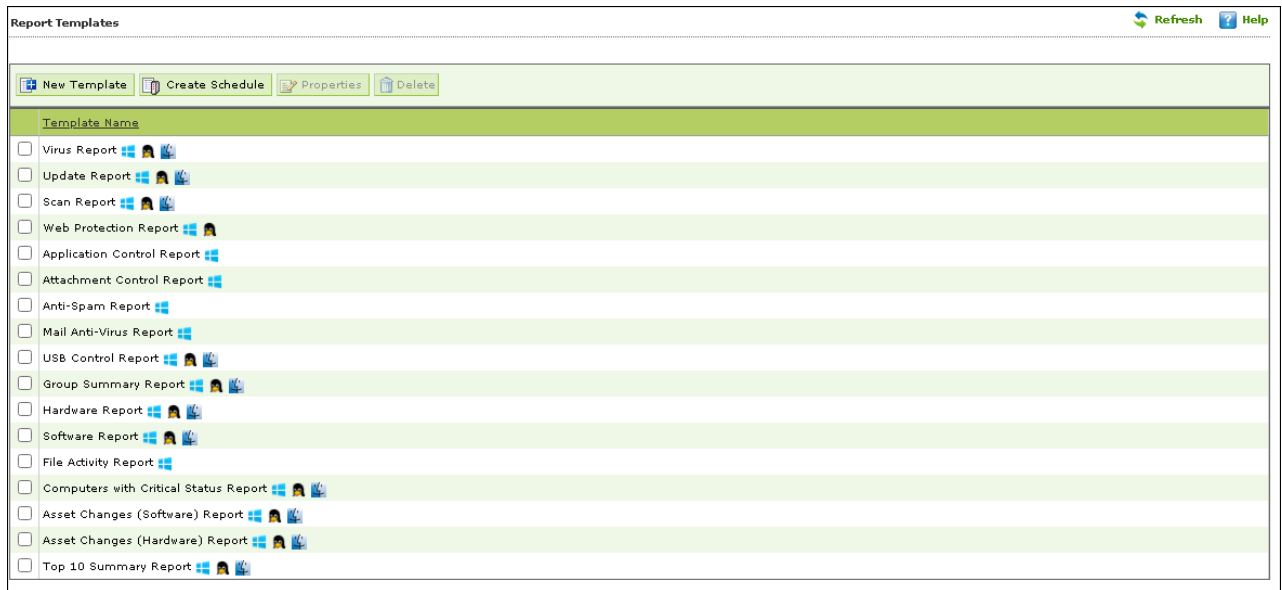
## Action List

This drop-down provides following options:

- **Set Host Configuration:** To learn more, [click here](#).
- **Deploy/Upgrade Client:** To learn more, [click here](#).
- **Move to Group:** To learn more, [click here](#).
- **Refresh Client:** To learn more, [click here](#).
- **Export to Excel:** This option lets you to export the status of particular system into Excel reports.
- **Properties:** To learn more, [click here](#).

# 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.



# 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.

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

# 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.

Details	
Selected Template Type:	VIRUS REPORT
Created:	5/29/2020 1:40:10 PM
Modified:	5/29/2020 1:40:10 PM

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

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

# 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.

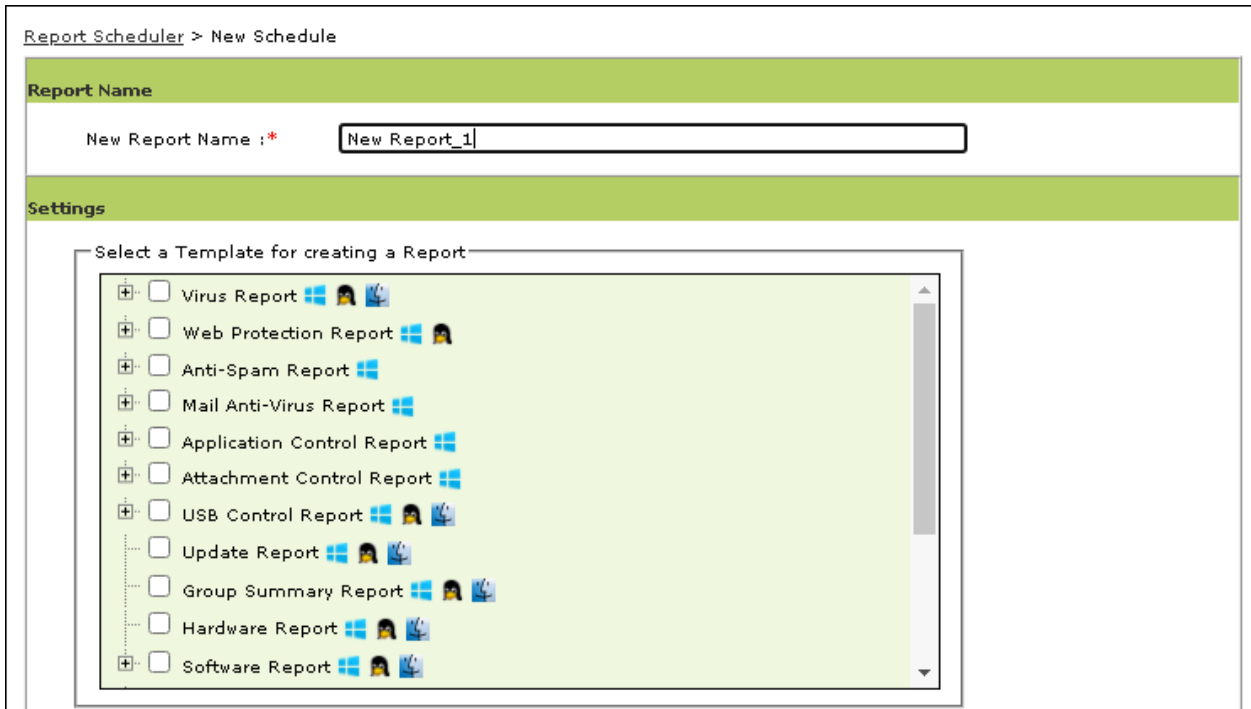
# Report Scheduler

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

Select Condition

☒ Generate a Report for Groups  
☐ Generate a Report for a List of Computers

**Select Target Groups**

☒ ☐  Managed Computers

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

**Send Report by Email**

Report Sender\*:

Report Recipient\*:

Mail Server IP Address:

Mail Server Port:

User Authentication:

Password Authentication:

\* For Example: user@yourcompany.com

**Select the Report Format**

HTML page

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

**Report Scheduling Settings**

☒ Enable Scheduler ☐ Manual Start

☒ Daily  
☐ Weekly  
☐ Monthly  
☐ Last Day of Month

☐ Mon ☐ Tue ☐ Wed ☐ Thu  
☐ Fri ☐ Sat ☐ Sun

1 ▼

☒ At

12:00 pm

Save

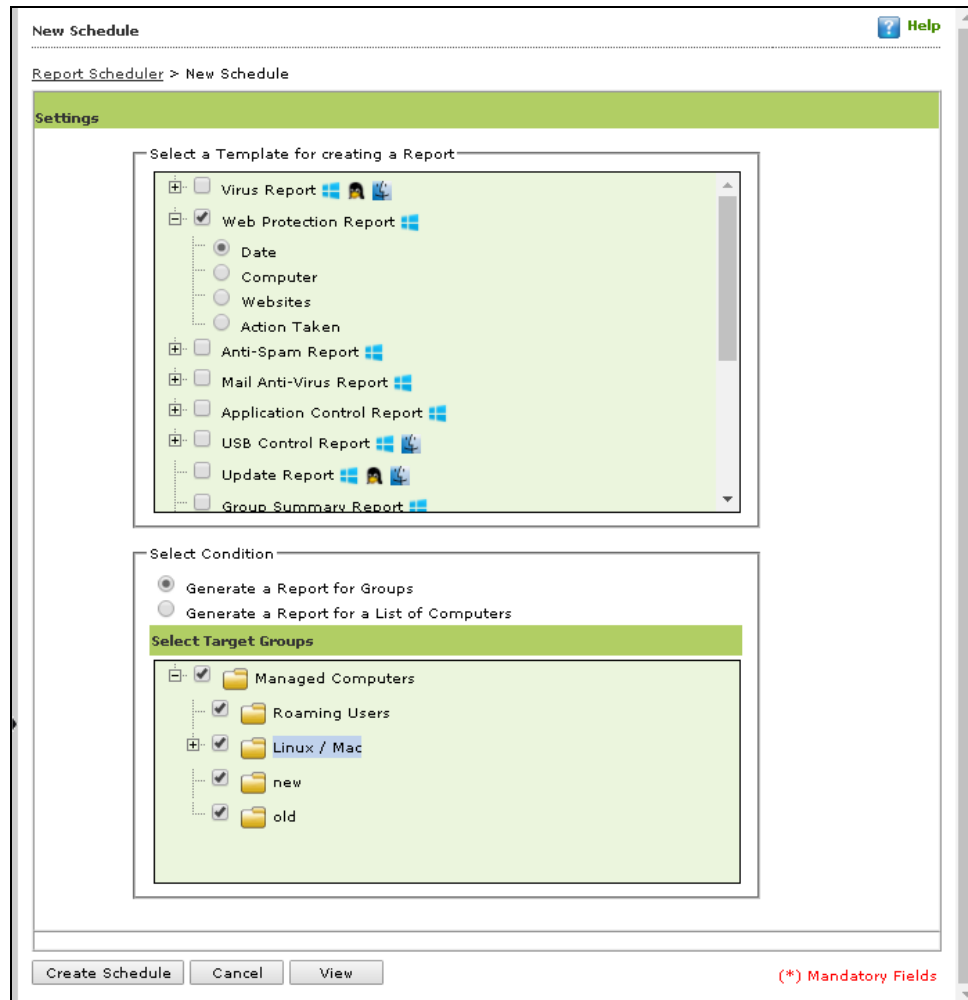
Cancel

- 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.



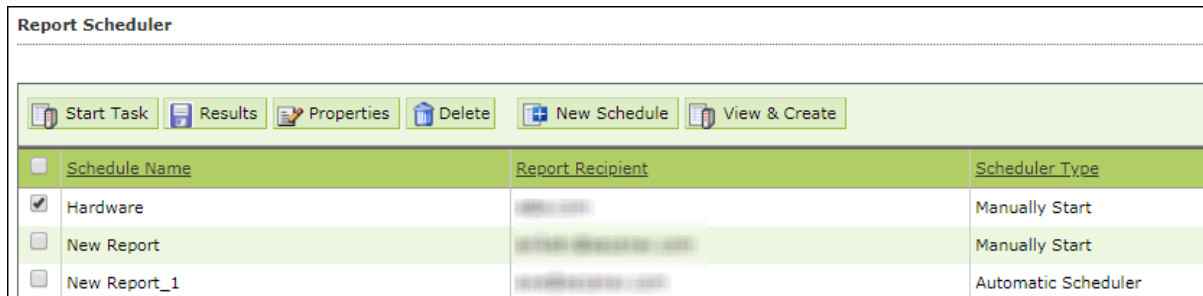
2. Select the **Template** options, the **Condition** and the **Target Groups**.
3. Click **View**.
4. A new window appears displaying the created report.

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' window. It has a toolbar with buttons: Start Task, Results, Properties, Delete, New Schedule, and View & Create. Below the toolbar is a table with three columns: Schedule Name, Report Recipient, and Scheduler Type.

Schedule Name	Report Recipient	Scheduler Type
<input checked="" type="checkbox"/> Hardware	Hardware	Manually Start
<input type="checkbox"/> New Report	New Report	Manually Start
<input type="checkbox"/> New Report_1	New Report_1	Automatic Scheduler

## Generating Task Report of a Schedule

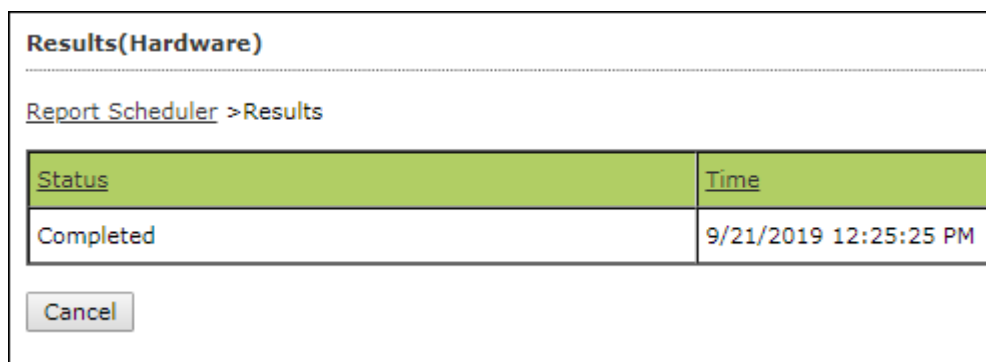
To generate a task report, select the preferred report schedule name and then click **Start Task**.

A task window appears displaying the name of the report being generated.

## Viewing Results of a Schedule

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

Results screen appears.



The screenshot shows the 'Results(Hardware)' window. It has a breadcrumb trail: Report Scheduler > Results. Below this is a table with two columns: Status and Time.

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

At the bottom of the window 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.

**Properties** Help

Report Scheduler > Properties

**General** | Schedule | Settings | Groups

Schedule Name :\*

Created:

Status:

(\*) 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.

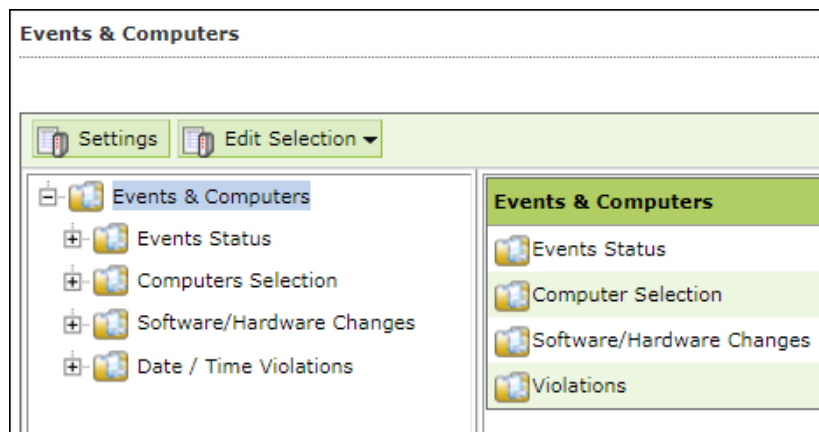
**Report Scheduler**

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

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

# Events and Computers

eScan Management Console maintains the record of all the events sent by the client computer. Through the events & computers module, the administrator can monitor the Events and Computers; 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.

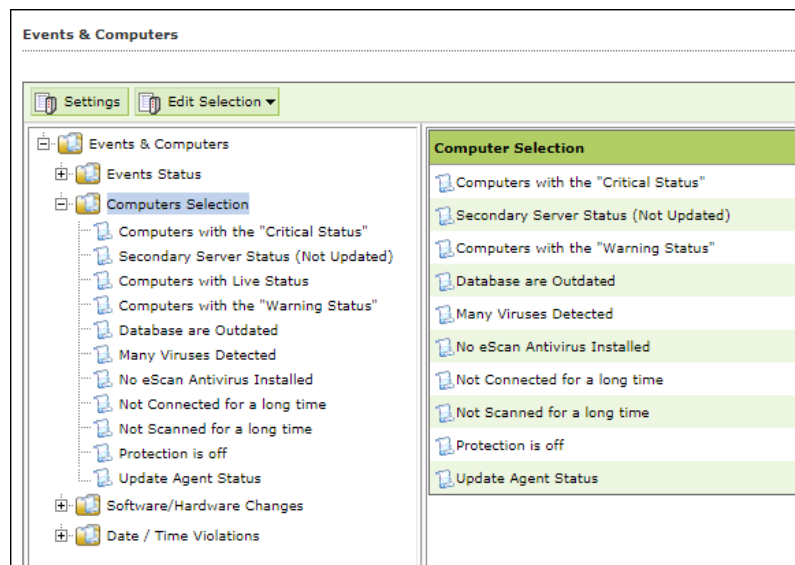
### Information

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**
- **Secondary Server Status (Not Updated)**
- **Computers with Live Status**
- **Computer with warning status**
- **Database is outdated**
- **Many Viruses Detected**
- **No eScan Installed**
- **Not connected for a long time**
- **Not scanned for a long time**
- **Protection is off**
- **Update Agent Status**
- **Computers with the "Critical Status"**

This section displays computers marked with Critical status.

## Computers with critical status

This section displays computers marked with Critical status.

## Secondary Server Status (Not Updated)



A secondary server receives downloads from the primary server and further distributes to the client computers. If the secondary server is not updated, it will be mentioned in the log.

### Computers with Live status

This section displays whether the computers present in the network are online or offline.

To get the details of the specific computers' status, select **Computers with Live Status** option. This will display the computers with default online status along with other details such as IP Address, Group, Description, and more. To display all the endpoints in the network, you can use filter options that filters out based on **Status Type**.

After selecting the computer from the list, you can choose **System Action List** drop-down option from the top panel. This option allows you to perform specific set of actions on the selected endpoints.

<b>NOTE</b>	<p>The required action can be performed only if the endpoint system is online. The  symbol indicates that the endpoint is online and  symbol indicates that the system is offline.</p>
-------------	--

The following actions can be performed on the online system according to the need of the user:

- **Log off:** This option will log off the system from the current user.
- **Force Log off:** This option will log off the current user forcefully.
- **Lock Machine:** This option will lock the system automatically.
- **Shutdown Machine:** This option will shut down the system.
- **Force Shutdown Machine:** This option will shut down the system forcefully.
- **Restart Machine:** This option will restart the system.
- **Force Restart Machine:** This option will restart the system forcefully.
- **Hibernate Machine:** This option will hibernate the system that will consume less power than sleep mode and resumes back to the previous states when you start-up the system.
- **Stand By Machine:** This option will put the machine in the standby mode. The standby mode is similar to as that of Hibernate mode.

### Computers with warning status

This section displays computer with a warning status.

### Database is outdated



This section displays computers whose virus database is outdated.

### **Many Viruses Detected**

This section displays the computers whose virus count has exceeded.

### **No eScan installed**

This section displays computers on which eScan is not installed.

### Not connected for a long time

This section displays the computers which didn't connect to the eScan server for the set duration.

### Not scanned for a long time

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

### Protection is off

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

### Update Agent Status

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

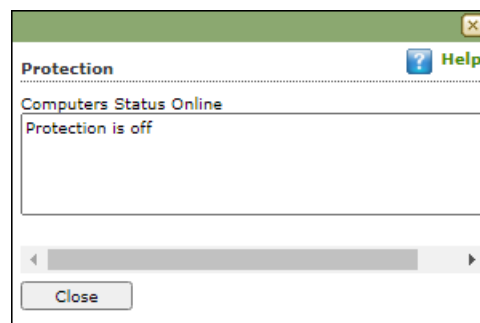
The additional settings vary depending upon the Computer Status.

## 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 the particular computer.

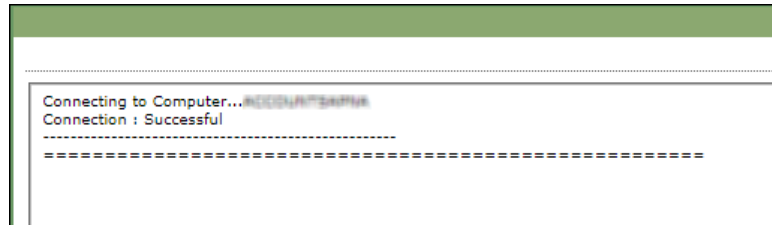
Events & Computers					
Recent Events (ACCOUNTS\Babu)					
Date	Time	User's name	Event Id	Module Name	Description
23-Jun-21	12:39:48	ACCOUNTS\Babu	File Anti-Virus (1754)	eScan Monitor	RegName:[HKEY_USERS\S-1-5-21-1330870860-2449891308-37588487
23-Jun-21	12:38:57	ACCOUNTS\Babu	Endpoint Security (102)	eScan EPS	Executable launched.
23-Jun-21	12:29:48	ACCOUNTS\Babu	File Anti-Virus (1754)	eScan Monitor	RegName:[HKEY_USERS\S-1-5-21-1330870860-2449891308-37588487
23-Jun-21	12:19:49	ACCOUNTS\Babu	File Anti-Virus (1754)	eScan Monitor	RegName:[HKEY_USERS\S-1-5-21-1330870860-2449891308-37588487
23-Jun-21	12:09:49	ACCOUNTS\Babu	File Anti-Virus (1754)	eScan Monitor	RegName:[HKEY_USERS\S-1-5-21-1330870860-2449891308-37588487
23-Jun-21	11:59:48	ACCOUNTS\Babu	File Anti-Virus (1754)	eScan Monitor	RegName:[HKEY_USERS\S-1-5-21-1330870860-2449891308-37588487
23-Jun-21	11:49:49	ACCOUNTS\Babu	File Anti-Virus (1754)	eScan Monitor	RegName:[HKEY_USERS\S-1-5-21-1330870860-2449891308-37588487
23-Jun-21	11:42:19	ACCOUNTS\Babu	File Anti-Virus (1752)	eScan Monitor	QBMgr Module



- **Deploy/Upgrade Client:** To learn about this option, [click here](#).



- **Check Connection:** This option will verify if the client machine is online or offline.

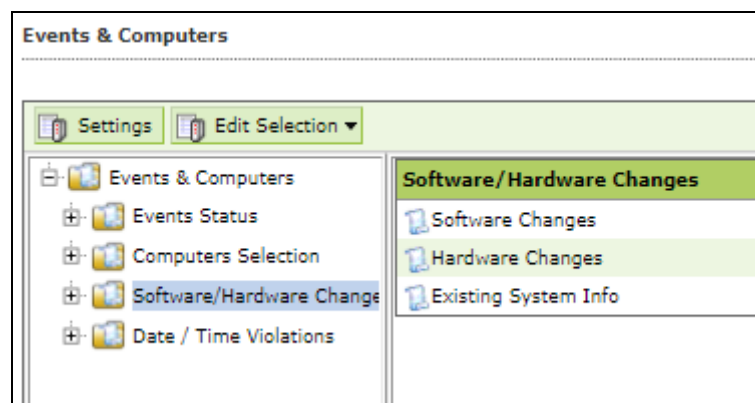


- **Remove from Group:** To learn about this option, [click here](#).
- **Connect to Client (RMM):** To learn about this option, [click here](#).
- **Force Download:** To learn about this option, [click here](#).
- **On Demand Scanning:** To learn about this option, [click here](#).
- **Send Message:** 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.

The screenshot shows the 'Events & Computers' window with the 'Violations' folder expanded. The 'Date / Time Violations' subfolder is selected, displaying a list of events. The table below represents the data shown in the screenshot.

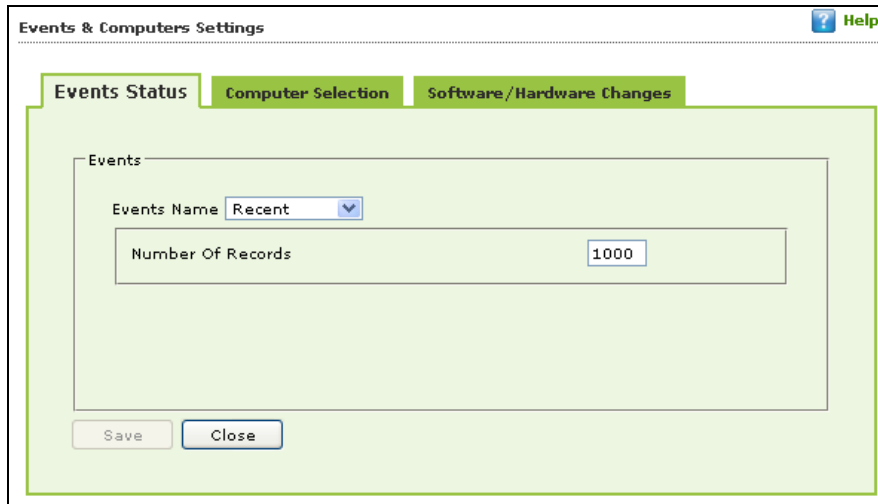
Time	Machine Name	IP Address	User name	Event Id	Module Name	Description
3/6/2018 15:58:18	COMPSS1	192.168.0.106	COMPSS1\	File Auto-Virus (1806)	eScan Monitor	Date/Time Modification Disabled
3/6/2018 15:58:04	COMPSS1	192.168.0.106	COMPSS1\	File Auto-Virus (1806)	eScan Monitor	Date/Time Modification Disabled
3/6/2018 15:58:02	COMPSS1	192.168.0.106	COMPSS1\	File Auto-Virus (1806)	eScan Monitor	Date/Time Modification Disabled
3/6/2018 14:50:16	WEAD17	192.168.7.84	WEAD17\	File Auto-Virus (1806)	eScan Monitor	Date/Time Modification Disabled
3/6/2018 12:30:35	WEAD18	192.168.0.257	WEAD18\	File Auto-Virus (1806)	eScan Monitor	Date/Time Modification Disabled
3/6/2018 12:30:15	WEAD18	192.168.7.79	WEAD18\	File Auto-Virus (1806)	eScan Monitor	Date/Time Modification Disabled
3/6/2018 12:30:15	WEAD18	192.168.7.79	WEAD18\	File Auto-Virus (1806)	eScan Monitor	Date/Time Modification Disabled
3/6/2018 12:30:14	WEAD18	192.168.7.79	WEAD18\	File Auto-Virus (1806)	eScan Monitor	Date/Time Modification Disabled
3/6/2018 12:30:14	WEAD18	192.168.7.79	WEAD18\	File Auto-Virus (1806)	eScan Monitor	Date/Time Modification Disabled

# Settings

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

## Event Status Setting

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



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

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

Steps to define event status settings:

Perform the following steps to save the event status settings:

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

## Computer Selection

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

## Steps to define computer settings

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

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

## Software/ Hardware Changes Setting

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

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.

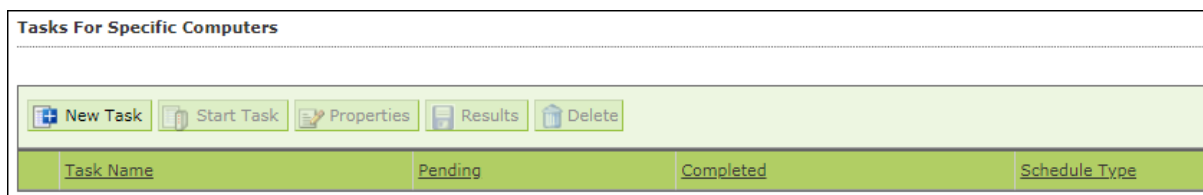
## Performing an action for computer

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.

## Tasks for Specific Computers

The Tasks for Specific Computers module lets you create a new task for computer(s) according to your preferences.



Tasks For Specific Computers			
<div>  New Task            Start Task            Properties            Results            Delete         </div>			
Task Name	Pending	Completed	Schedule Type

## Creating a task for specific computers

To create a task for specific computer(s), follow the steps given below:

1. In the navigation panel, click **Tasks for Specific Computers**.
2. Click **New Task**.  
New Task Template form appears.





New Task Template Help

Tasks For Specific Computers > New Task Template


Task Name

Task Name: \*


Assigned Tasks

☐ File Anti-Virus Status  



☐ Enabled
 ☒ Disabled

☐ Mail Anti-Virus Status 



☐ Enabled
 ☒ Disabled

☐ Anti-Spam Status 


☐ Enabled
 ☒ Disabled

☐ Web Protection Status  

☐ Enabled
 ☒ Disabled

☐ Endpoint Security Status  

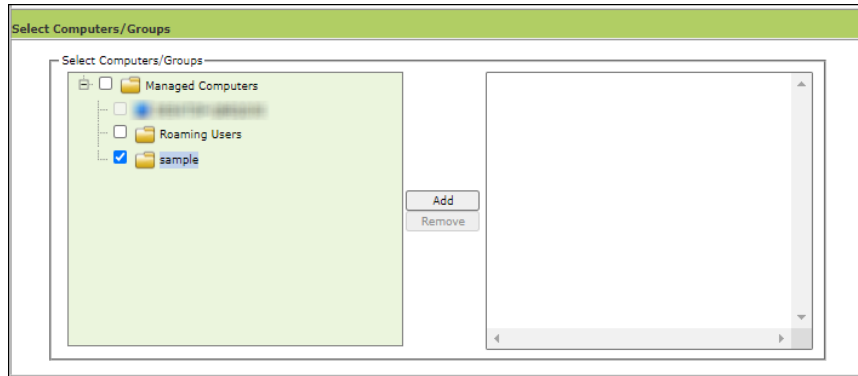
☐ Enabled
 ☒ Disabled

☐ Firewall Status 

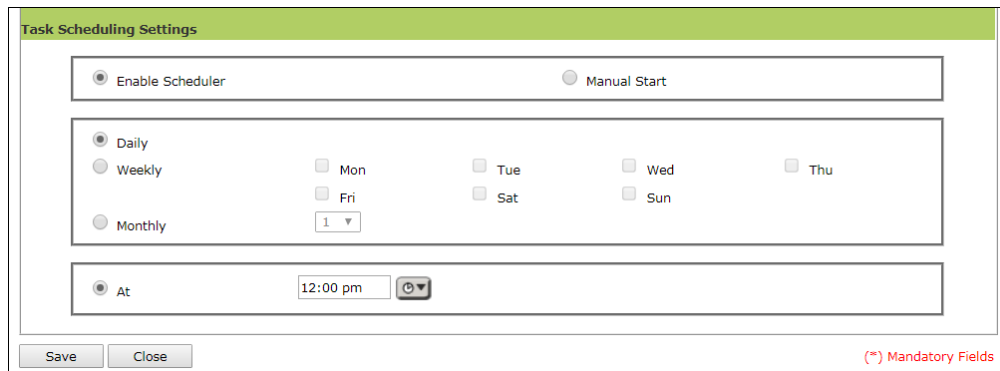
☐ Disable Firewall
 ☐ Enable Limited Filter Mode of Firewall

- Enter a name for task.
- In the **Assigned Tasks** section, select the modules and scans to be run.

- In the **Select Computers/Groups** section, select the computers/groups on which the tasks should be run and then click **Add**.



- In the **Tasks Scheduling Settings** section, configure the schedule settings.



- Click **Save**. The task will be saved and run for specific computers according to your preferences.

## Viewing Properties of a task

To view Properties of a task, select the task and click **Properties**.

sample Help

Tasks For Specific Computers > Properties

**General** | Schedule | Machines | Settings

Task Name: sample

Task Creation Time: 05/29/20 03:15:34 PM

Status: Task not performed yet

Last Run:

Save Close

This section will have following tabs to configure:

- **General:** This tab allows to change the task name and provides details about the task creation, status, and last run.
- **Schedule:** This tab allows to change the scheduler setting for the particular task.
- **Machines:** This tab allows to add or remove the endpoints added to the particular task.
- **Settings:** This tab allows to modify or select the modules and scans to be run.

**NOTE** To run a scheduled task manually, select the task and then click **Start Task**.

## Viewing Results of a task

To view Results of a task, select the task and click **Results**.

Task Results (sample) Help

Tasks For Specific Computers > Task Results

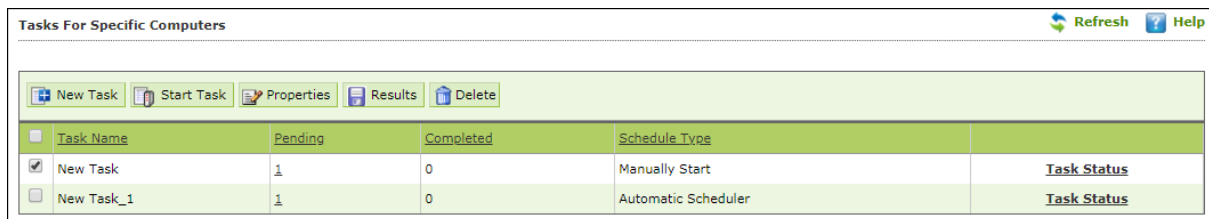
Client Computers	Group	Status	Date/Time
10.10.10.10	Managed Computers\TestGroup	Not Performed Yet	

This option will provide the summary details about the task like clients computers, group to which computers belong, status of the task, and more.

# Deleting a task for specific computers

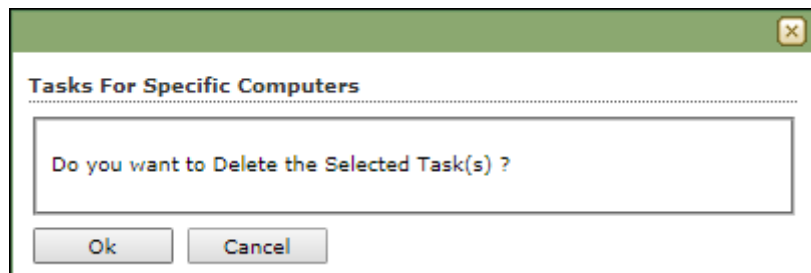
To delete a task, follow the steps given below:

1. In the Tasks for Specific Computers screen, select the task you want to delete.



Tasks For Specific Computers					Refresh	Help
<input type="button" value="New Task"/> <input type="button" value="Start Task"/> <input type="button" value="Properties"/> <input type="button" value="Results"/> <input type="button" value="Delete"/>						
<input type="checkbox"/>	Task Name	Pending	Completed	Schedule Type		
<input checked="" type="checkbox"/>	New Task	1	0	Manually Start	<u>Task Status</u>	
<input type="checkbox"/>	New Task_1	1	0	Automatic Scheduler	<u>Task Status</u>	

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



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

# 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.

Asset Management				
<a href="#">Refresh</a> <a href="#">Help</a>				
<a href="#">Hardware Report</a> <a href="#">Software Report</a> <a href="#">Software License</a> <a href="#">Software Report (Microsoft)</a>				
Filter Criteria		Export Option		
Computer Details				
Computer Name	Group	IP Address	User's name	Operating System
DESKTOP-XXXXXX	Managed Computers	192.168.1.100	DESKTOP-XXXXXX\ADMINISTRATOR	Windows 2008 R2 Standard Edition 64-bit
DESKTOP-XXXXXX	Managed Computers	192.168.1.101	DESKTOP-XXXXXX\USER	Windows 7 Professional 32-bit
DESKTOP-XXXXXX	Managed Computers	192.168.1.102	DESKTOP-XXXXXX\ADMINISTRATOR	Windows 7 Professional 64-bit
DESKTOP-XXXXXX	Managed Computers	192.168.1.103	DESKTOP-XXXXXX\ADMINISTRATOR	Windows 7 Professional 32-bit
DESKTOP-XXXXXX	Managed Computers	192.168.1.104	DESKTOP-XXXXXX\ADMINISTRATOR	Windows 10 Professional 64-bit
DESKTOP-XXXXXX	Managed Computers	192.168.1.105	DESKTOP-XXXXXX\ADMINISTRATOR	Windows 7 Professional 32-bit
DESKTOP-XXXXXX	Managed Computers	192.168.1.106	DESKTOP-XXXXXX\ADMINISTRATOR	Windows 10 Professional 64-bit

The tab displays following details of managed computers:

- Computer Name
- Group
- IP Address
- User name
- Operating System
- Service Pack
- OS Version
- OS Installed Date
- Internet Explorer
- Processor
- Motherboard
- RAM
- HDD
- Local MAC Adapter(s)
- Wi-Fi MAC [Adapter]

- USB MAC [Adapter]
- PC Identifying Number
- Motherboard Serial No
- Network Speed
- Disk Free Space
- PC Manufacturer
- PC Model
- MB Manufacturer
- Graphic Card Details
- Machine Type
- BitLocker Status
- Keyboard Vendor
- Software

To view the list of Software along with the installation dates, click **View** in **Software** column.

## Filtering Hardware Report

To filter the Hardware Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

**Filter Criteria** **Export Option**

Filter Criteria

☒ Select All Include All #Add Asset Information

<input checked="" type="checkbox"/> Computer Name	*	Include	<input checked="" type="checkbox"/> Internet Explorer	*	Include
<input checked="" type="checkbox"/> User's name	*	Include	<input checked="" type="checkbox"/> OS Version	*	Include
<input checked="" type="checkbox"/> Operating System	*	Include	<input checked="" type="checkbox"/> Processor	*	Include
<input checked="" type="checkbox"/> Motherboard	*	Include	<input checked="" type="checkbox"/> Local Adapter	*	Include
<input checked="" type="checkbox"/> RAM	*	Include	<input checked="" type="checkbox"/> Wifi Adapter	*	Include
<input checked="" type="checkbox"/> Group	*	Include	<input checked="" type="checkbox"/> USB Adapter	*	Include
<input checked="" type="checkbox"/> PC IdentifyingNumber	*	Include	<input checked="" type="checkbox"/> Motherboard Serial No	*	Include
<input checked="" type="checkbox"/> OS Type	*	Include	<input checked="" type="checkbox"/> HDD		
<input checked="" type="checkbox"/> IP Address	*	Include	<input checked="" type="checkbox"/> OS Installed Date		
<input checked="" type="checkbox"/> Service Pack	*	Include	<input checked="" type="checkbox"/> Disk Free Space		
<input checked="" type="checkbox"/> PC Manufacturer	*	Include	<input checked="" type="checkbox"/> PC Model	*	Include
<input checked="" type="checkbox"/> MB Manufacturer	*	Include	<input checked="" type="checkbox"/> Graphic Card Details	*	Include
<input checked="" type="checkbox"/> Machine Type	*	Include	<input checked="" type="checkbox"/> BitLocker Status		

Search Reset (\*) View All Items

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

### Include/Exclude

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

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

The Hardware Report will be filtered according to your preferences.

## Exporting Hardware Report

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

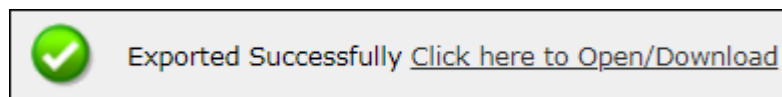
Export Option field expands.

▲ Filter Criteria ▼ Export Option

Export Option

☐ Excel ☐ PDF ☒ HTML Export

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



Click the link to open/download the file.

## Software Report

The Software Report tab displays list of Software along with the number of computers on which they are installed.

Asset Management Refresh Help

Hardware Report **Software Report** Software License Software Report (Microsoft)

▲ Filter Criteria ▲ Export Option

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

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

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

Computer list window appears displaying following details:

- Computer Name
- Group
- IP Address

- Operating System
- Software Version
- Installed Date

## Filtering Software Report

To filter Software Report, click **Filter Criteria** field.

Filter Criteria field expands.

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

### Software Name

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

### Computer Name

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

### OS Type

Enter the OS type.

### Group By

The results can be grouped by Software name, Computer name or Group. If Group option is selected, the report can be filtered for a specific group.

After entering data in all fields, click **Search**.

The Software Report will be filtered according to your preferences.

## Exporting Software Report

To export the Software Report, click **Export Option**.

Export Option field expands.

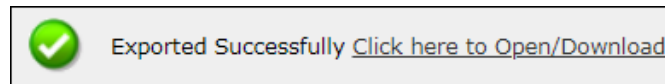


Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



Click the link to open/download the file.

## Software License

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

Asset Management

Refresh

Help

Hardware Report

Software Report

Software License

Software Report (Microsoft)

▲ Filter Criteria

▲ Export Option

1 - 3 of 3

◀◀ page 1 of 1 ▶▶

Rows per page: 100 ▼

License Key	Software Name	Computer Count
W2222-W2222-W2222-W2222-W2222	Windows 10 Professional 32-bit	1
W2222-W2222-W2222-W2222-W2222	Windows 10 Professional 64-bit	1
W2222-W2222-W2222-W2222-W2222	Windows XP Professional 32-bit	1

The log displays License Key, Software Name and Computer Count.

To see more details of the computer's license key installed, click the numerical value in License Key or Computer Count column.

## Filtering Software License Report

To filter Software Report, click **Filter Criteria** field.

Filter Criteria field expands.

Filter Criteria		Export Option	
Filter Criteria			
Software License Key	*	Include	
Software Name	*	Include	
Computer Name	*	Include	
IP Address	*	Include	
OS Type	*	Include	
Search		Reset	
		Group By	
		<input type="checkbox"/> Group	
		(*) 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).

### 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.

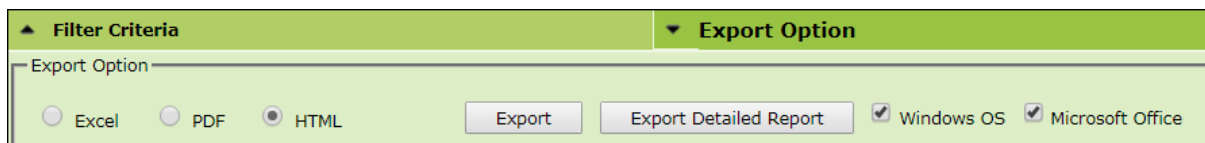
After entering data in all fields, click **Search**.

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.



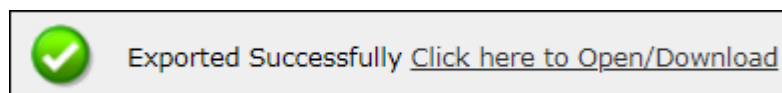
Select whether you want report for Windows OS and Microsoft Office.

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.

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

The tab consists following subtabs:

**MS Office Software Report** – It displays Microsoft software name and computer count.

**Microsoft OS** – It displays Operating System, Service Pack, OS version and computer count.

## Filtering Software Report (Microsoft)

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

Filter Criteria field expands.

### 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)

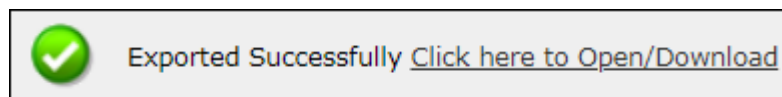
To export the Software Report (Microsoft), click **Export Option**.  
Export Option field expands.

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.

### Operating System

Entering the operating system name displays list of suggestions. Select the appropriate OS.

### Computer Name

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

### Service Pack

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

### OS Version

Entering the OS version displays list of suggestions. Select the appropriate OS version.

### Include/Exclude

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

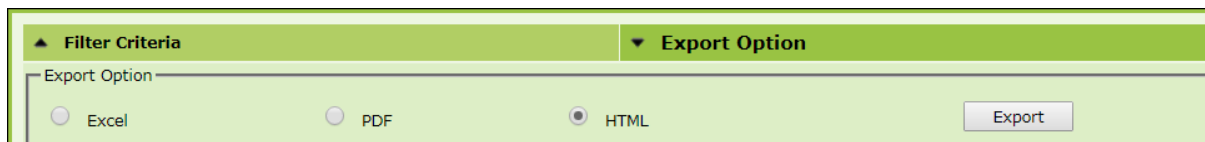
After filling all the fields, click **Search**.

The Microsoft OS report will be filtered according to your preferences.

## Exporting Microsoft OS Report

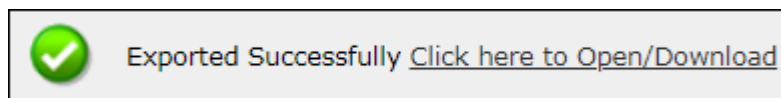
To export the Microsoft OS Report, click **Export Option**.

Export Option field expands.



The screenshot shows a web interface with two tabs: 'Filter Criteria' and 'Export Option'. The 'Export Option' tab is active, showing three radio buttons labeled '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.

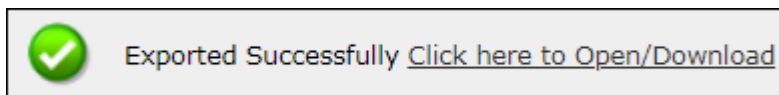


## Exporting Print Activity Log

To export this generated log,

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

A success message appears.



4. Click the link to open/download the file.

## Filtering Print Activity Log

To filter the print activity log, click **Filter Criteria**.

Filter criteria field expands.

### Computer Name

Click the drop-down and select the preferred computer.

### Printer

Enter the printer's name.

### User Name

Enter the User's name.

### Include/Exclude

Selecting Include/Exclude for a Machine or Printer lets you include or exclude it from the log.

### Date Range



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

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

The Print activity log will be filtered and generated according to your preferences.

### Group By

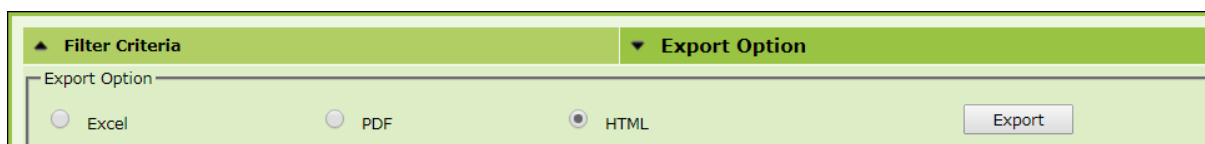
To view results by specific printer, select **Printer**, Date Range and then click **Search**.

To view results by specific user name, select **User name**, Date Range and then click **Search**.

## Exporting Print Activity Report

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

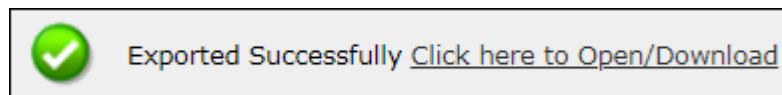
Export Option field expands.



The screenshot shows a web interface with two tabs: 'Filter Criteria' and 'Export Option'. The 'Export Option' tab is active, showing three radio button options: 'Excel', 'PDF', and 'HTML'. The 'HTML' option is selected. An 'Export' button is located to the right of the options.

Select the preferred option and then click **Export**.

A success message appears.



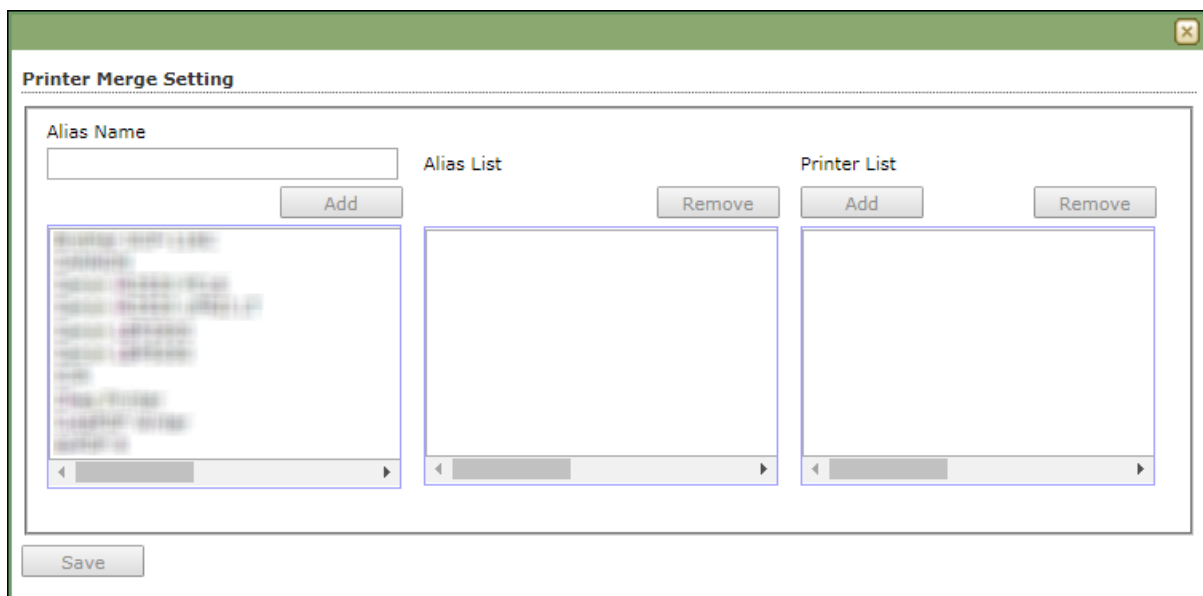
Click the link to open/download the file.

## Print Activity Settings

Print Activity Settings lets you keep track of printers by adding them in a group and assigning it an alias name. The printers can be added or removed from this alias group.

To configure Print Activity Settings:

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



The screenshot shows the 'Printer Merge Setting' window. It has a title bar with a close button. Inside, there's a section titled 'Printer Merge Setting'. Below this, there are three main areas: 'Alias Name' with a text input field and an 'Add' button; 'Alias List' with a list box and a 'Remove' button; and 'Printer List' with a list box and 'Add' and 'Remove' buttons. At the bottom left, there is a 'Save' button. The 'Alias Name' field is currently empty. The 'Alias List' and 'Printer List' boxes are also empty.

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

# Session Activity Report

This submodule monitors and logs the session activity of the managed computers. It displays a report of the Operation type, Date, Computer name, Group, IP address and event description. With this report the administrator can trace the user Logon and Logoff activity along with remote sessions that took place on all managed computers.

## Viewing Session Activity Log

In the navigation panel, click **User Activity > Session Activity Report**.

The log displays list of session activities and type of operation performed. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

Session Activity Report

Refresh

Help

Filter Criteria

Export Option

1 - 100 of 251

1 of 3

Rows per page: 100

Operation Type	Client Date	Computer Name/Ip	Group	IP Address	Description
Start up	18/09/19 7:21:44 PM	192.168.1.100	Marketing Team	192.168.1.100	
Session LogOn	18/09/19 7:21:44 PM	192.168.1.100	Marketing Team	192.168.1.100	User LogOn User name: 192.168.1.100
Shut Down	18/09/19 7:20:36 PM	192.168.1.100	Support Department	192.168.1.100	
Session LogOff	18/09/19 7:20:32 PM	192.168.1.100	Support Department	192.168.1.100	User LogOff User name: 192.168.1.100
Session LogOff	18/09/19 7:13:01 PM	192.168.1.100	Programming\Android	192.168.1.100	User LogOff User name: 192.168.1.100
Shut Down	18/09/19 7:01:51 PM	192.168.1.100	Production Dept	192.168.1.100	
Session LogOff	18/09/19 7:01:49 PM	192.168.1.100	Production Dept	192.168.1.100	User LogOff User name: 192.168.1.100

## Filtering Session Activity Log

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

Filter Criteria field expands.

Filter Criteria

Export Option

Filter Criteria

☒ Computer Name
  Include

☒ Operation Type
  Include

☒ Description

☒ Date Range
 From (MM/DD/YYYY)  To (MM/DD/YYYY)

☒ IP Address
  Include

☒ Group
  Include

(\*) View All Items

Filter Criteria lets you filter and generate the log according to your preferences. The check box selected will be added as a column in the report.

### Computer Name

Click the drop-down and select the preferred computers.

### Operation Type

Click the drop-down and select the preferred activities.


### Include/Exclude

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

### IP Address

Enter the IP address in this field.

### Group

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

### Date Range

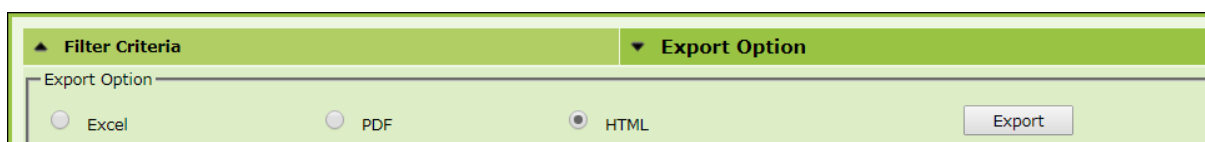
To search the log between specific dates, select **Date Range** check box. Afterwards, click the calendar icon and select **From** and **To** dates.

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

## Exporting Session Activity Report

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

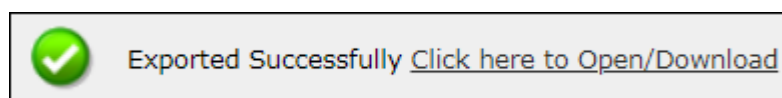
Export Option field expands.



The screenshot shows a green header bar with two tabs: 'Filter Criteria' and 'Export Option'. The 'Export Option' tab is active. Below the header, there is a section labeled 'Export Option' containing three radio buttons: 'Excel', 'PDF', and 'HTML'. The 'HTML' radio button is selected. To the right of the radio buttons is a button labeled 'Export'.

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.

1 - 10 of 112848 page 1 of 11285 Rows per page: 10								
Client Date	Computer Name/Ip	Group	IP Address	User's name	File Action Type	Drive Type	Source File	Destination File
4/20/2019 12:00:25 AM	...	...	...	...	CREATE	DRIVE_NETWORK	NewFile	\\...\\Images\\GR000
4/20/2019 12:00:25 AM	...	...	...	...	CREATE	DRIVE_NETWORK	NewFile	\\...\\Images\\GR000
4/20/2019 12:01:52 AM	...	...	...	...	CREATE	DRIVE_NETWORK	NewFile	\\...\\Images\\GR000
4/20/2019 12:01:52 AM	...	...	...	...	CREATE	DRIVE_NETWORK	NewFile	\\...\\Images\\GR000
4/20/2019 12:04:15 AM	...	...	...	...	CREATE	DRIVE_NETWORK	NewFile	\\...\\Images\\GR000
4/20/2019 12:04:15 AM	...	...	...	...	CREATE	DRIVE_NETWORK	NewFile	\\...\\Images\\GR000

## Filtering File Activity Log

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

**Filter Criteria**

**Export Option**

☒ Computer Name
  Include

☒ User's name
  Include

☒ File Action Type
  Include

☒ Source File
  Include

☒ Application
  Include

☒ Date Range
 From (MM/DD/YYYY)  To (MM/DD/YYYY)

☒ IP Address
  Include

☒ Group
  Include

☒ Drive Type
  Include

☒ Destination File
  Include

[\(\\*\) View All Items](#)

Filter Criteria lets you filter and generate the log according to your preferences. The check box selected will be added as a column in the report.

### Computer Name

Click the drop-down and select the preferred computers.

### Username

Enter the username of the computer.

### File Action type

Click the drop-down and select a preferred file action.

### Source File

Enter the source file's name.

### Application

Enter an application's name.


### Include/Exclude

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

### IP Address

Enter an IP address.

### Group

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

### Drive Type

Click the drop-down and select the drive type.

### Destination File

Enter the file path.

### Date Range

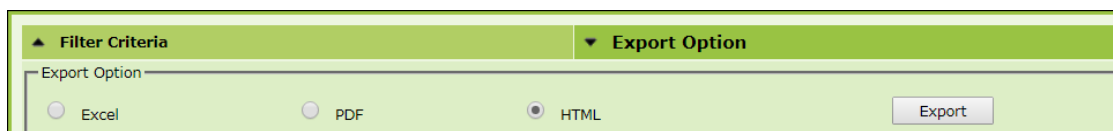
To search the log between specific dates, select **Date Range** check box. Afterwards, click the calendar icon and select **From** and **To** dates.

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

## Exporting File activity Report

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

Export Option field expands.



The screenshot shows a green header bar with two tabs: 'Filter Criteria' and 'Export Option'. Below the 'Export Option' tab, there is a section labeled 'Export Option' containing three radio buttons: 'Excel', 'PDF', and 'HTML'. The 'HTML' radio button is selected. To the right of these options is a button labeled 'Export'.

Select the preferred option and then click **Export**.

A success message appears.



Exported Successfully [Click here to Open/Download](#)

Click the link to open/download the file.

# 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)
adb.exe	00:00:00:05
Adobe Acrobat	00:00:00:15
Adobe Acrobat 8.0	00:00:00:14
Adobe Acrobat Reader DC	00:00:10:17
Adobe Collaboration Synchronizer 20.12	00:00:00:23
Adobe RdrCEF	00:00:24:08
Adobe Reader	00:01:21:46
Adobe Reader 9.3	00:00:06:35
Bullzip PDF Printer	00:00:00:37
CutePDF Application	00:00:01:06
EAgent	00:04:34:53

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)
ES-7203	00:00:00:05

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
Adobe Acrobat	03/12/20 10:37:38 AM	03/12/20 10:37:43 AM	00:00:00:05	C:\Program Files (x86)\Adobe\Acrobat 10.0\Acrobat\Acrobat.exe

You can export this report in various format such as PDF, CSV, and HTML.



## Filtering Application Access Report

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

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

### Group By

The results can be grouped by Application name or Computer name.

### Date Range

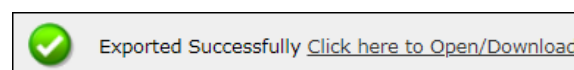
To search the log between specific dates, select **Date Range** check box. Afterwards, click the calendar icon and select **From** and **To** dates.

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.

# Patch Report

The Patch Report module displays the number of windows security patches installed and not installed on managed computers. This will help an administrator identify the number of vulnerable systems in the network and install the critical patches quickly.

Patch Name	Applied Count	Not Applied Count	Not Applicable Count
KB2207566	0	0	2
KB2286198	0	0	2
KB2305420	0	0	2
KB2347290	0	0	2
KB2393802	0	0	2
KB2412687	0	0	2
KB2419632	0	0	2
KB2419635	0	0	2
KB2419640	0	0	2
KB2425227	0	0	2

## Patch report

The Patch report tab displays the Patch Name, Applied Count, Not Applied Count and Not Applicable Count. Clicking the numerical displays the patch name, details about the computer, the group it belongs to, IP address and User's name.

Computer Name	Group	IP Address	User's name	Operating System
Managed Computers	Managed Computers	192.168.1.1	Administrator	Windows 10 Professional 32-bit
Managed Computers\TestGroup	Managed Computers\TestGroup	192.168.1.2	Administrator	Windows XP Professional x64 Edition 64-bit

## Filtering Patch Report

To filter the Patch Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

The screenshot shows the 'Patch Report' interface. At the top, there are two tabs: 'Patch Report' and 'All Patch Report'. Below the tabs, there are two main sections: 'Filter Criteria' and 'Export Option'. The 'Filter Criteria' section contains two input fields: 'Patch Name' and 'Computer Name', each with a search icon and a dropdown menu set to 'Include'. Below these fields are 'Search' and 'Reset' buttons. The 'Export Option' section contains a 'Group By' dropdown menu with two options: 'Patch Name' (selected) and 'Computer Name'. At the bottom right of the 'Filter Criteria' section, there is a link: '(\*) View All Items'.

Enter the Patch Name and Computer Name to be included in the filtered report.

### Include/Exclude

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

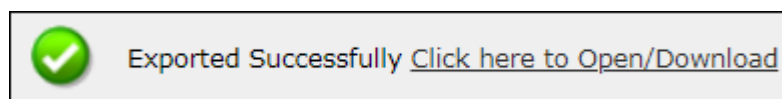
After making the necessary selections, click **Search**.

The Patch Report will be filtered according to your preferences.

## Exporting Patch Report

To export the Patch 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.

Other than security patch – for all patch Microsoft patch based on events

**File AV > Advanced Settings**

## All Patch Report

The All Patch Report tab displays all Microsoft patches based on following specific events.

- **1-KB patches**
- **2-Security Update**
- **4-Hotfix**
- **8-Update**
- **16-Service Pack**
- **31-All**

Patch Management

Refresh

Help

Patch Report

All Patch Report

▲ Filter Criteria

▲ Export Option

0 - 0 of 0

◀ page 0 of 0 ▶

Rows per page: 10 ▼

Patch Name

Computer Count

There are no items to show in this view.

## Filtering All Patch Report

To filter the All Patch Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

Enter the **Patch Name** and **Computer Name** to be included in the filtered report.

### NOTE

To enable All Patch Report Configure policy by going to **File Antivirus-->Advanced Setting-->Send Windows Security Patch Events.**

### Include/Exclude

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

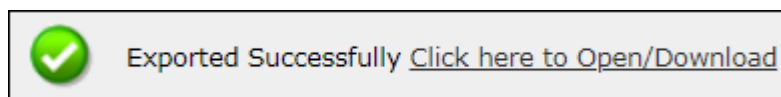
After making the necessary selections, click **Search**.

The Patch Report will be filtered according to your preferences.

## Exporting All Patch Report

To export the All Patch 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:

- **Outbreak Alert**
- **Event Alert**
- **Unlicensed Move Alert**
- **New Computer Alert**
- **Configure SIEM**
- **SMTP Settings**

## Outbreak Alert

If the virus count exceeds the limits set by you, an outbreak email notification will be sent to the recipient.

To set an outbreak alert, follow the steps given below:

1. In the navigation panel, click **Notifications > Outbreak Alert**.  
Outbreak Notification screen appears.

2. Select the checkbox **Send notification**.
3. Enter the preferred values in Number and Time Limit field.
4. Click **Save**. Outbreak Alert Settings will be saved.

<b>NOTE</b>	In order to receive notification emails, it is necessary to configure SMTP settings. Learn more about SMTP Settings by clicking <a href="#">here</a> .
-------------	--

# Event Alert

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

Event Notification

Events Alert Settings

☐ Enable email alert Notification
 [Configure SMTP Settings](#)

Save

Cancel

To enable the event alert,

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

Events Alert Settings

☒ Enable email alert Notification
 [Configure SMTP Settings](#)

☒ Send Information only in subject line

Select Event Ids

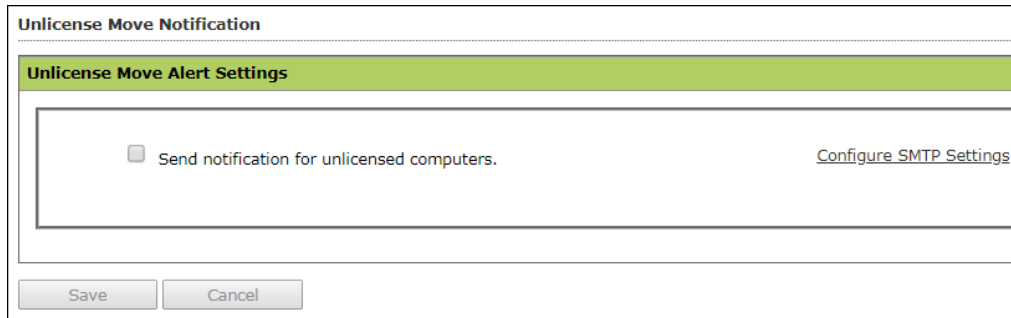
Select activities for which email alert is required

<input type="checkbox"/>	Event Id	Description
<input checked="" type="checkbox"/>	154	AVPMAPP_UPDATES_DONE
<input type="checkbox"/>	100	ESCAN_DUMMY_EVENT
<input type="checkbox"/>	1	MWAV_FOUND_MALWARE
<input type="checkbox"/>	2	MWAV_FOUND_VIRUS_AND_DELETED
<input type="checkbox"/>	3	MWAV_FOUND_VIRUS_AND_CLEANED
<input type="checkbox"/>	4	MWAV_FOUND_ADWARE
<input type="checkbox"/>	5	MWAV_FOUND_ERROR
<input type="checkbox"/>	6	MWAV_FOUND_VIRUS_AND_RENAMED
<input type="checkbox"/>	7	MWAV_FOUND_ADWARE_AND_DELETED
<input type="checkbox"/>	8	MWAV_LAST_COMPUTER_SCAN
<input type="checkbox"/>	9	MWAV_START
<input type="checkbox"/>	10	MWAV_SUMMARY
<input type="checkbox"/>	501	SCHED_MWAV_FOUND_MALWARE
<input type="checkbox"/>	502	SCHED_MWAV_FOUND_VIRUS_AND_DELETED
<input type="checkbox"/>	503	SCHED_MWAV_FOUND_VIRUS_AND_CLEANED
<input type="checkbox"/>	504	SCHED_MWAV_FOUND_ADWARE

4. Select the required hosts or group.
  5. Click **Save**.
- The Event Alert Settings will be saved.

## Unlicensed Move Alert

This submodule lets you enable notification alert when a computer automatically moves to Unlicensed Computers category based on the setting done (under events and computers) for the computer which is not connected to the server for a long time.



The dialog box titled "Unlicense Move Notification" contains a section "Unlicense Move Alert Settings". Inside this section, there is a checkbox labeled "Send notification for unlicensed computers." and a link "Configure SMTP Settings". At the bottom of the dialog, there are "Save" and "Cancel" buttons.

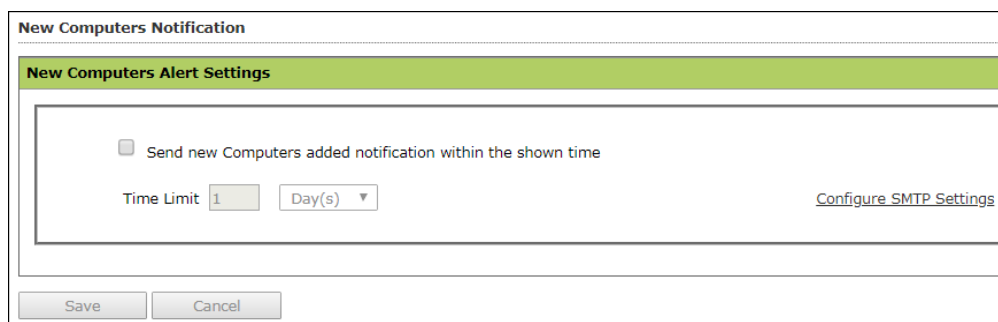
To enable the unlicensed move alert,

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

The Unlicensed Move Alert Settings will be saved.

## New Computer Alert

This submodule lets eScan send you a notification alert when a new computer is connected to the server within the IP range mentioned under the Managed Computers.



The dialog box titled "New Computers Notification" contains a section "New Computers Alert Settings". Inside this section, there is a checkbox labeled "Send new Computers added notification within the shown time". Below the checkbox, there is a "Time Limit" field with the value "1" and a "Day(s)" dropdown menu. A link "Configure SMTP Settings" is also present. At the bottom of the dialog, there are "Save" and "Cancel" buttons.

To enable the new computer alert, follow the steps given below:

1. In the navigation panel, click **Notifications > New Computer Alert**.
2. Select the checkbox **Send new Computers added notification within the shown time**.
3. Enter the preferred values in Time limit field.
4. Click **Save**.






The New Computer Alert Settings will be saved.

## Configure SIEM

SIEM technology provides real-time management of security events generated for hardware changes and applications installed/uninstalled/upgraded where eScan is installed. eScan is equipped with variety of features that facilitate real-time monitoring, correlating captured events, notifications and console views and provides long-term storage, analysis and reporting of data.



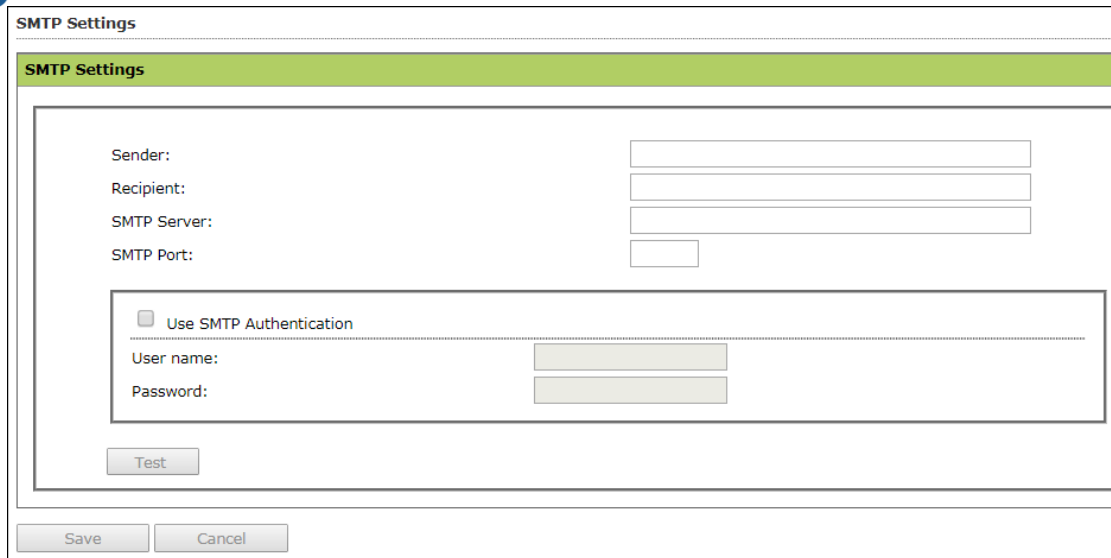
To configure SIEM, follow the steps given below:

1. In the navigation panel, click **Notification** > **Configure SIEM**.
2. Select the **Enable event forward to SIEM/SYSLOG Server** checkbox.
3. After selecting the checkbox, it will enable the rest of the options that can be configured. You can enter the details of the SIEM/SYSLOG Server.
4. Click **Save**.

The SIEM settings will be saved.

## SMTP Settings

This submodule lets you configure the SMTP settings for all the email notifications.



SMTP Settings

SMTP Settings

Sender:

Recipient:

SMTP Server:

SMTP Port:

☐ Use SMTP Authentication

User name:

Password:

Test

Save Cancel

To configure the SMTP settings, follow the steps given below:

1. In the navigation panel, click **Notifications > SMTP Settings**.
2. Enter all the details.
3. Click **Save**.

The SMTP Settings will be saved.

To test the newly saved settings, click **Test**.

# Settings

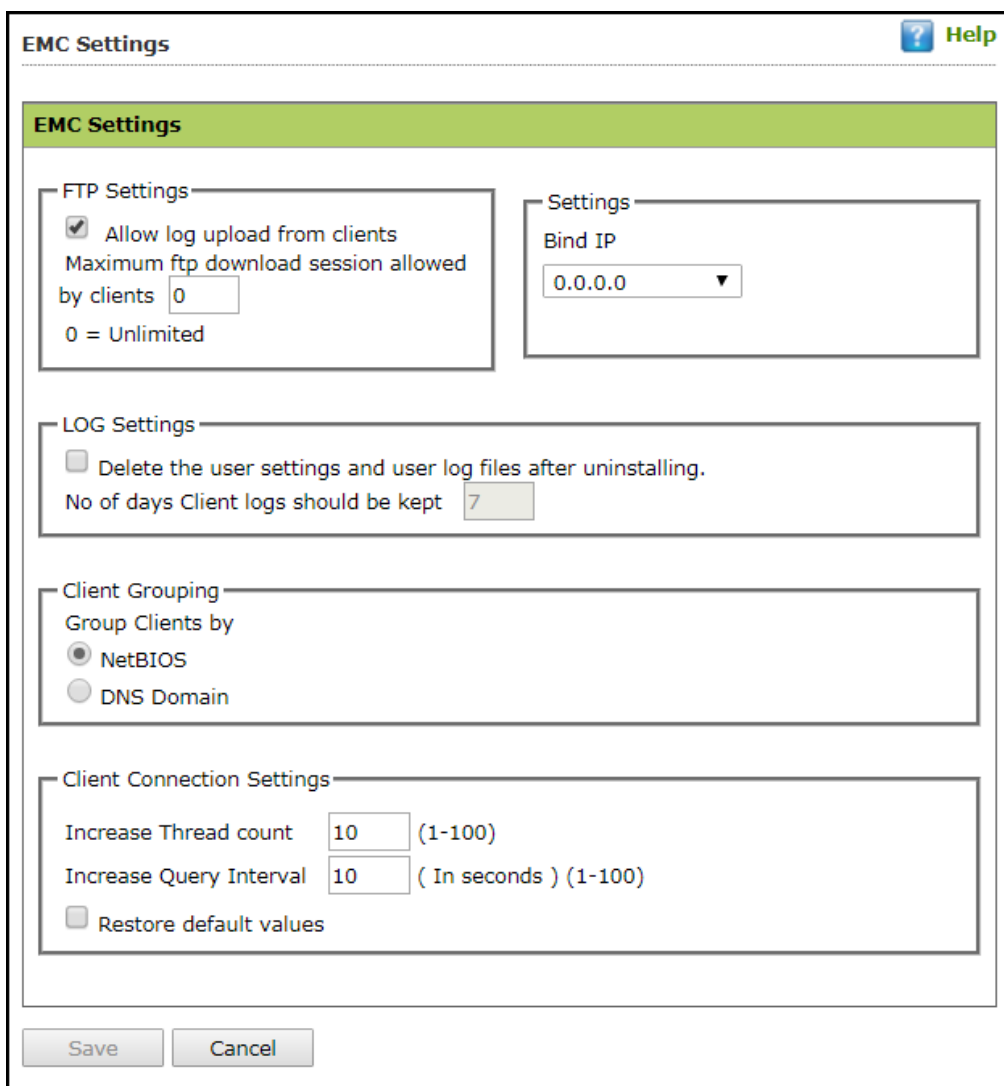
The Settings module lets you configure general settings. It contains following submodules.

- **EMC Settings:** This submodule lets you define settings for FTP sessions, Log Settings, Client Grouping and Client connection settings.
- **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.
- **Update Settings:** This submodule lets you define settings for General Configuration, Update Notifications, and Scheduling.
- **Auto-Grouping:** This submodule lets you define settings for Grouping of computers after installation of eScan client is carried out.
- **Two-Factor Authentication:** This submodule lets you to add extra layer of protection to your endpoints.

## EMC Settings

The **EMC** (eScan Management Console) **Settings** lets you configure the eScan Management Console. You can configure the FTP settings, Bind to IP Settings, Log Settings, Client Grouping and Client Connection Settings.

You can bind announcement of FTP server to particular IP by selecting the IP address in the list. However, you can choose to leave it as 0.0.0.0, which mean it will announce on all available interface/IP.



The screenshot shows the 'EMC Settings' window with a green header bar and a 'Help' button. The settings are organized into several sections:

- FTP Settings:**
  - ☒ Allow log upload from clients
  - Maximum ftp download session allowed by clients:  (0 = Unlimited)
- Settings:**
  - Bind IP:
- LOG Settings:**
  - ☐ Delete the user settings and user log files after uninstalling.
  - No of days Client logs should be kept:
- Client Grouping:**
  - Group Clients by:
    - ☒ NetBIOS
    - ☐ DNS Domain
- Client Connection Settings:**
  - Increase Thread count:  (1-100)
  - Increase Query Interval:  ( In seconds ) (1-100)
  - ☐ Restore default values

At the bottom, there are 'Save' and 'Cancel' buttons.

### FTP Settings

This setting lets you approve the log upload from client computers. It also lets you set the maximum FTP download sessions allowed for client computers. (Note: 0 means unlimited)

### Bind IP Settings

This setting lets you bind an IP address. Click the drop-down and select the preferred IP address for binding. The default IP address is 0.0.0.0.

### Log Settings

This setting provides you with the option to delete the User settings and Log files after uninstallation of eScan from the computer. To enable the above setting, select the checkbox. After selecting the checkbox, you can store client logs for the preferred number of days.

### Client Grouping

This setting lets you manually manage domains and computers grouped under them after performing fresh installations.

Select **NetBIOS**, if you want to group clients only by hostname.

Select **DNS Domain**, if you want to group clients by hostname containing the domain name.

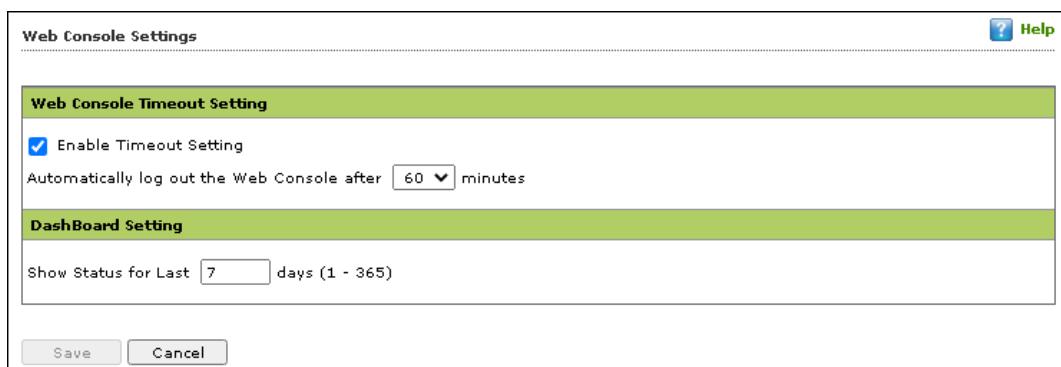
### Client Connection Settings

This setting lets you modify **Thread Count** and **Query Interval** (In Seconds). To reset the values, select **Restore default values** checkbox.

After performing the necessary changes, click **Save**. The EMC Settings will be updated.

## Web Console Settings

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



The screenshot shows the 'Web Console Settings' window. It has a title bar with a 'Help' icon. The window is divided into two main sections: 'Web Console Timeout Setting' and 'DashBoard Setting'. In the 'Web Console Timeout Setting' section, there is a checkbox labeled 'Enable Timeout Setting' which is checked. Below it, the text 'Automatically log out the Web Console after' is followed by a dropdown menu showing '60' and the word 'minutes'. The 'DashBoard Setting' section has a text input field labeled 'Show Status for Last' with the value '7' and the text 'days (1 - 365)'. At the bottom of the window, there are two buttons: 'Save' and 'Cancel'.

### Web Console Timeout Settings

To enable web console Timeout, select **Enable Timeout Setting** option.

After selecting the check box, click the drop-down and select the preferred duration.

### Dashboard Setting

This setting lets you set number of days for which you wish to View the Status, Statistics and Protection Status Charts in the Dashboard. Enter the preferred number of days.

### Login Page Setting

This setting lets you show or hide the download links shared for eScan Client setup, Agent setup and AV Report. To show the download links on login page, select the checkboxes of respective links.

### SQL Server Connection settings

This setting lets you select an authentication mode between Microsoft Windows Authentication Mode to SQL Server Authentication Mode. Select the **SQL Server Authentication Mode** and define **Server instance** and **Host Name** along with the credentials for connecting to the database.

#### Server Instance

It displays the current server instance in use. To select another server instance, click **Browse**. Select an instance from the list and click **OK**.

#### Hostname/IP Address

It displays the Hostname or IP Address of the server instance computer.

Enter the credentials in **Username** and **Password** fields.

To check whether correct credentials are entered, click **Test Connection**.

### SQL Database Purge Settings

This setting lets you define the maximum SQL database size in MB and purge data older than the specified days. To enable SQL Database Purge Settings, select **Enable Database Purge** checkbox.

Enter the preferred value in **Database Size threshold in (MB)** field.

Enter the preferred number of days in **Purge data older than specified days, if above threshold** is met field.

### RMM Settings

This setting lets you configure default RMM setting for connecting to client via RMM service:

#### Activate View Only

By default, after taking a remote connection, you can only view the endpoint screen and are unable to perform any activity.

#### De-Activate View Only

To perform activity on an endpoint after taking remote connection, click **De-Activate View Only**.

### Screen Quality Settings

This option lets you configure the screen as per your requirements. It consists following suboptions:

- **Screen Quality** can be set to **Medium** or **High**.

Screen Quality	Screen Ratio
Medium	80%

- **Screen Ratio** can be set to anywhere from **20%** to **100%**.

Screen Quality	Screen Ratio
Medium	80%

<b>NOTE</b>	To build a safe RMM connection between a Client to Server, Client to Update Agent, and Update Agent to Server, ensure that ports 2219, 2220 and 8098 are open.
-------------	--

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



# Update Settings

The Update Settings submodule keeps your virus definitions up-to-date and protects your computer from emerging species of viruses and other malicious programs. This submodule lets you configure update settings, update notifications and schedule updates according to your need.

You can configure eScan to download updates automatically either from eScan update servers or from the local network by using FTP or HTTP. You can configure following settings.

## General Config

The **General Config** tab lets you configure update settings. The settings let you select the mode of update and configure proxy settings.

The screenshot shows the 'Update Settings' dialog box with the 'General Config' tab selected. The dialog has four tabs: 'General Config', 'Update Notification', 'Scheduling', and 'Update Distribution'. The 'General Config' tab contains the following settings:

- Select Mode:** Two radio buttons, 'FTP' and 'HTTP'. 'HTTP' is selected.
- Proxy Settings:** A section with a checkbox 'Download via Proxy' which is unchecked.
- HTTP Section:** Fields for 'HTTP Proxy Server IP', 'Port', 'Login Name', and 'Password'.
- FTP Section:** Fields for 'FTP Proxy Server IP', 'Port', 'Login Name', and 'Password'.
- Logon Type:** A group box containing four radio buttons: 'User@siteaddress', 'OPEN siteaddress' (selected), 'PASV Mode', and 'Socks'. There is also a dropdown menu showing '4'.

At the bottom of the dialog are three buttons: 'Save', 'Cancel', and 'Update'.

### Select Mode

Select the mode for downloading updates. Following options are available:

- FTP
- HTTP

### Proxy Settings

Proxy Settings lets you configure proxy for downloading updates.

To enable Proxy Settings, select **Download via Proxy** checkbox. You will be able to configure proxy settings depending on the mode of selection.

If you are using HTTP proxy servers, enter the HTTP proxy server IP address, port number and HTTP proxy server's authentication credentials.

If you are using FTP proxy servers, along with HTTP settings mentioned above you will have to enter FTP proxy server IP address, Port number, FTP proxy server's authentication credentials and Logon enter.

After filling the necessary data, click **Save > Update**. The General Config tab will be saved and updated.

## Update Notification

The **Update Notification** tab lets you configure email address and SMTP settings for email notifications about database update.

### Update Notification

To receive email notifications from eScan about virus signature database update, select this option.

#### Sender

Enter an email ID for sender.

#### Recipient

Enter the notification recipient's email ID.

## SMTP Server and Port

Enter the SMTP server's IP address and Port number in the respective fields.

## Use SMTP Authentication

If the SMTP server requires authentication, select this checkbox and enter the login credentials in the **Username** and **Password** fields.

After filling the necessary data, click **Save > Update**. The Update Notification will be saved and updated.

## Scheduling

The Scheduling tab lets you schedule updates with Automatic or Schedule Download mode.

### Automatic Download

The eScan Scheduler sends a query to the update server at set intervals and downloads the latest updates if available. To set an interval, click the **Query Interval** drop-down and select a preferred duration.

### Schedule Download

The eScan Scheduler lets you set a schedule the download for daily, weekly, or monthly basis at a specified time. The scheduled query will be sent to the update server as per your preferences.

After filling the necessary data, click **Save > Update**. The Scheduling tab will be saved and updated.

## Update Distribution

The Update Distribution tab allows the admin to enable and disable the sharing of eScan Virus signature to be distributed to air-gapped/isolated network.

The screenshot shows the 'Update Settings' dialog box with the 'Update Distribution' tab selected. The 'Setting' section has two radio buttons: 'Enable Share' (unselected) and 'Disable Share' (selected). Below this, there are two sections for updates: 'Anti-spam/product Updates' and 'AntiVirus Updates'. Each section has a text input field for the update path. In the 'AntiVirus Updates' section, the 'Enable 64 bit update ( Required only if 64 bit Linux and MAC system are in network)' checkbox is checked. At the bottom, there is a red note: 'Note: Sharing to be enabled only incase of eScan Virus Signature to be distributed to air-gapped network. It is necessary to set the update mode to Network in air-gapped eScan server through eScan Protection Center. (Source UNC Path for Network mode to be set as \\ServerName\esupd or \\ServerIP\esupd )'. There are 'Save' and 'Cancel' buttons at the bottom.

Select **Enable Share** in **Setting** section, this will allow the distribution of eScan Virus Signatures to the isolated/air-gapped network. After enabling this, it is mandatory to set the update mode to the network in network that is isolated/air-gapped through eScan Protection Center.

To update it, follow the below steps:

1. Open the eScan Protection Center in air-gapped network; click **Update** option present in the Quick Link section.



2. Click **Settings**. Update Settings window appears.

Update Settings

General Config | After Update | Scheduling

Select Mode: ☐ FTP ☐ HTTP ☒ **Network**

Proxy Settings

☒ Download via Proxy

HTTP

HTTP Proxy Server IP:  Port:

Login Name:  Password:

FTP

FTP Proxy Server IP:  Port:

Login Name:  Password:

Logon Type

☐ User@siteaddress ☒ **OPEN siteaddress** ☐ PASV Mode ☐ Socks

Network

Source UNC Path:

Default OK Cancel Apply

3. Select **Network** option and set the **Source UNC Path** as **\\ServerName\esupd** or **\\ServerIP\esupd**.  
E.g.: **\\192.0.2.0\esupd**  
After setting UNC path for the air-gapped network, the update will be available automatically to the Isolated/Air-gapped network.

# Auto-Grouping

The Auto grouping submodule consists following subsections:

- **Auto Add Client setting**
- **Client(s) list excluded from Auto adding under Managed Group(s)**
- **Group and Client selection criteria for Auto adding under Managed Group(s)**

Auto Grouping
Refresh
Help

Auto Add Client setting

☒ Auto adding client(s) under Managed Group(s)

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

Add

Remove

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

Group and Client selection criteria for Auto adding under Managed Group(s)

Group Name

Add

Remove

Browse

Up

Down

e.g.: group1  
group1\subgroup...

Client Criteria

Add

Remove

Run Now

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

Save

Cancel

## Auto Add Client setting

Selecting the checkbox **Auto adding client(s) under Managed Group(s)** enables automatic adding computers under Managed group(s) after manual installation of eScan client.

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

Adding a client in this list ensures that it does not auto add itself again after you remove it from the Managed computer(s).

### Group and Client selection criteria for Auto adding under Managed Group(s)

This section lets you define/create groups with client criteria for auto adding under managed group(s). You can add a list of clients under a particular group name here and then add it under the exclusion list if required.

## Excluding clients from auto adding under Managed Group(s)

To exclude clients from auto adding under managed group(s), follow the steps given below:

1. Enter either the host name, host name with wildcard, IP address or IP address range.
2. Click **Add**. The computer will be displayed in the list below.

## Removing clients from the excluded list

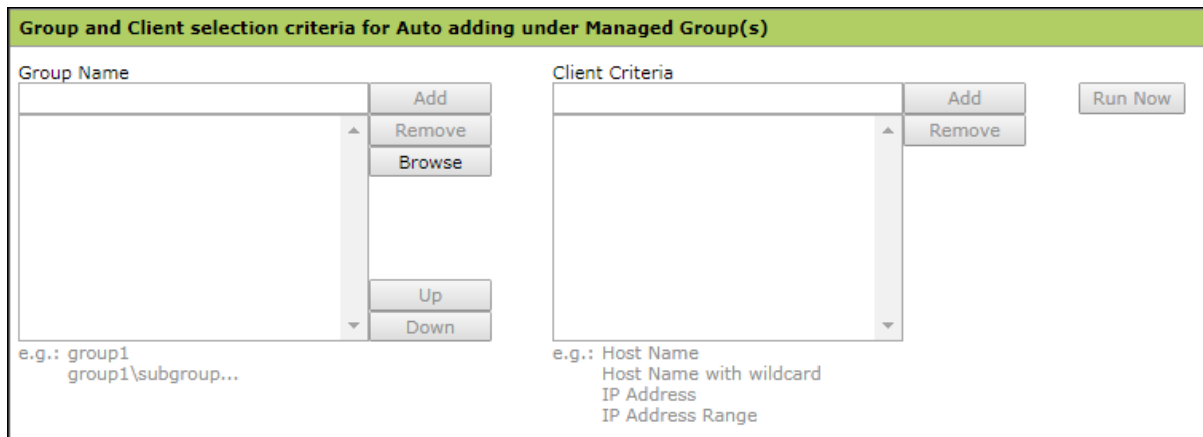
1. Select the computer you want to remove.
2. Click **Remove**. The computer will be removed from the list.

### Group and Client selection criteria for Auto adding under Managed Group(s)

This feature can be used to automate the process of adding computers/clients under a particular group. This process is manually done under unmanaged computers.

## Defining a group and client selection criteria for auto adding under managed computer(s)

To define group and client selection criteria for auto adding under managed groups(s), follow the steps given below:



1. Under the Group Name, enter the group's name and click **Add**.

OR

Click **Browse** and select the group from the existing list.

**NOTE** To browse through the list of groups, click **Up** or **Down**.

2. Select the group for which you want to define the criteria.
3. Under the Client Criteria, enter either Hostname, Hostname with wildcard, IP address or IP address range and click **Add**. The clients displayed in the list will be added under the selected group.
4. Click **Save**. The client will be saved under that group.
5. To apply the settings for the newly added client, click **Run Now**.



## Two-Factor Authentication (2FA)

The system login password is Single-Factor Authentication which is considered unsecure as it may put your organization's data at high risk of compromise. The Two-Factor Authentication, also more commonly known as 2FA, adds an extra layer of protection to your eScan web console login.

The 2FA feature mandates you to enter a Time-based One-Time Password (TOTP) after entering eScan credentials. So, even if somebody knows your eScan credentials, the 2FA feature secures data against unauthorized logins. Only administrator can enable/disable the 2FA feature. It can also be enabled for added users as well.

To use 2FA login feature, you need to install the Authenticator app 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, so ensure you get an appropriate approval to use device camera in your organization. If a COD or BYOD policy restricts you from using device camera in your organization, enter the Account Key in the Authenticator app.



### NOTE

Ensure that the smart device's date and time matches with the system's date and time or else TOTP's generated by app won't get validated.

### IMPORTANT

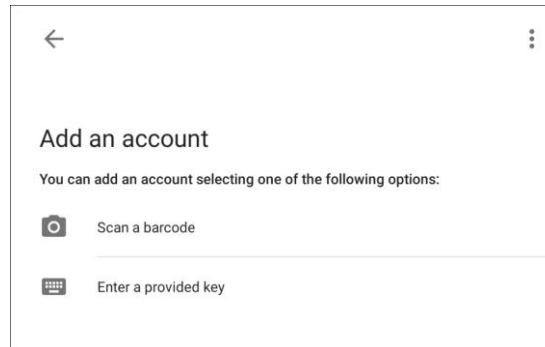
We recommend that you save/store the **Account Key** in offline storage or a paperback copy, in case you lose the account access.

## Enabling 2FA login

To enable 2FA login,

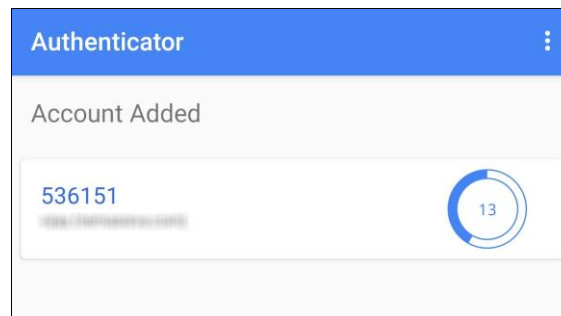
1. Go to **Settings > Two-Factor Authentication**.
2. Open the Authenticator app.

After basic configuration following screen appears on smart device.

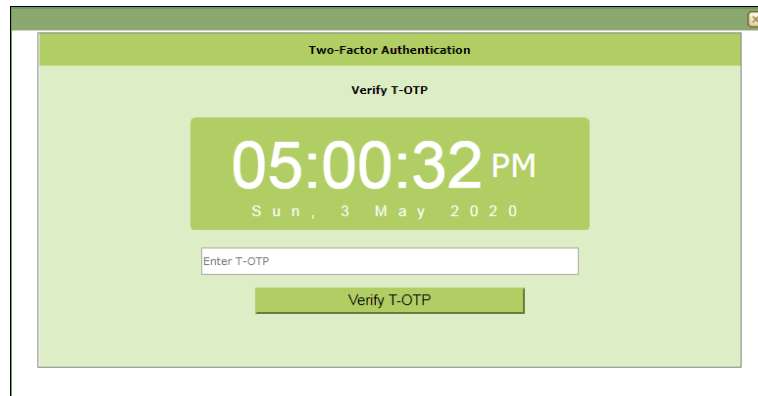




3. Select a preferred option. If you tapped **Scan a barcode**, scan the onscreen QR code via your smart device. If you tapped **Enter a provided key**, enter the Account Key and then tap **ADD**.

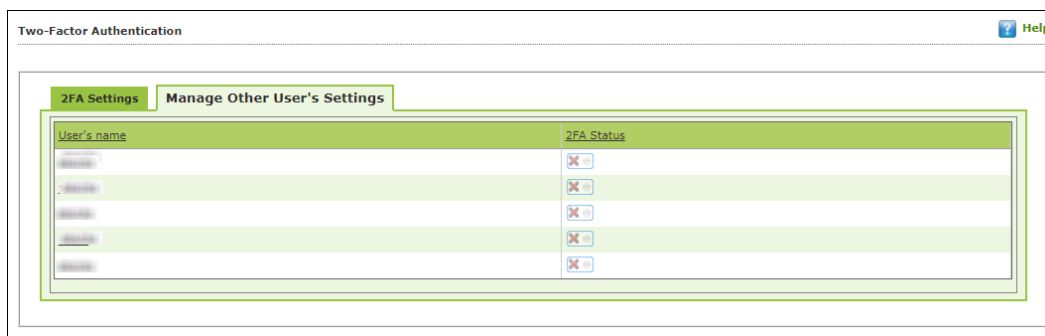
After scanning the Account QR code or entering Account Key the eScan server account gets added to the Authenticator app. The app then starts displaying a Time-based One-Time Password (TOTP) that is valid for 30 seconds.



4. Click **Enable Two-Factor Authentication**.  
Verify TOTP window appears.



5. Enter the TOTP displayed on smart device and then click **Verify TOTP**.  
The 2FA login feature gets enabled.
6. To apply the login feature for users, click **Manage Other User Settings** tab.  
The tab displays list of added users and whether 2FA status is enabled or disabled.
  -  - 2FA Disabled
  -  - 2FA Enabled

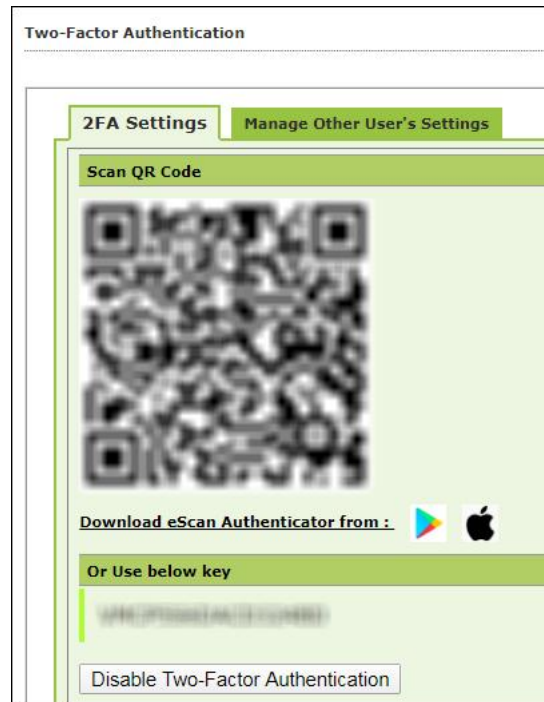


7. To enable 2FA login for an added user, click the button to check icon.  
The 2FA login for added users gets enabled. After enabling the 2FA login for users, whenever they log in to eScan web console Verify TOTP window appears.

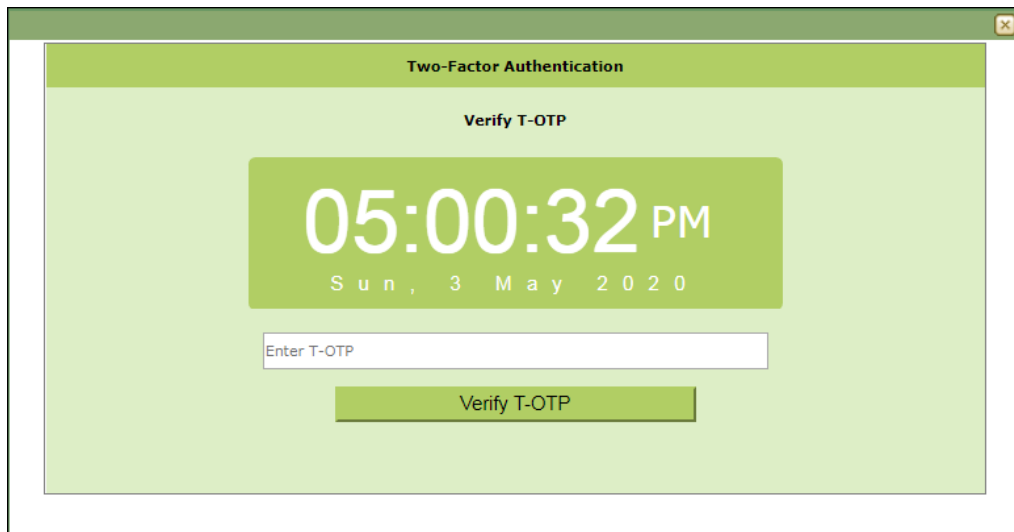
## Disabling 2FA login

To disable 2FA login,

1. Go to **Settings > Two Factor Authentication**.
2. Click **Disable Two-Factor Authentication**.



Verify TOTP window appears.



3. Enter the TOTP and then click **Verify TOTP**.  
The 2FA feature gets disabled.

**NOTE**

After disabling the 2FA feature and enabling it again, the 2FA login status will be reinstated for added users.

# 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**
- **Export & Import**
- **Customize Setup**

## 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 Accounts

Create New Account

Delete

1 - 1 of 1

page

1

of

1

Rows per page: 100

<div></div>	User name	Full Name	Domain	Role	Session Log	Status
	root	Administrator account created during installation		Administrator	<a href="#">View</a>	<div><div></div><div></div></div>

Create New Account

Delete

1 - 1 of 1

page

1

of

1

Rows per page: 100

## Create New Account

To create a User Account,

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

Create User Help

User Accounts > Create User

**Account Type and Information**

User name\*:

Full Name\*:

Password\*:

Confirm Password\*:

Email Address\*:

For Example: user@yourcompany.com

**Account Role**

Role\*:

(\*) Mandatory Fields

- After filling all the details, click **Save**.  
The user will be added to the User Accounts list.

## Delete a User Account

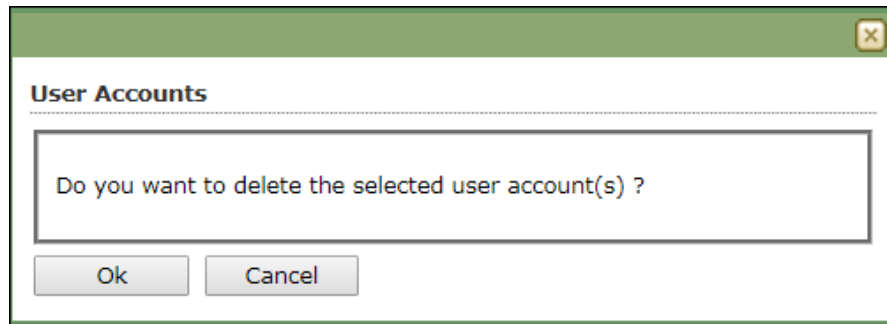
To delete a user account

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

**User Accounts**

<input checked="" type="checkbox"/>	User name	Full Name
<input type="checkbox"/>	<u>root</u>	Administrator account created during installation
<input checked="" type="checkbox"/>	<u>sample user</u>	Sample User

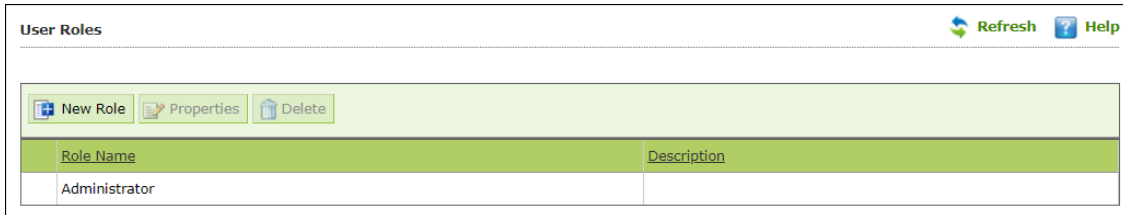
- Click **Delete**.  
A confirmation prompt appears.



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.



Role Name	Description
Administrator	

You can re-define the Properties of the created role for configuring access to various section of eScan Management Console and the networked Computers. It also lets you delete any existing role after the task is completed by them. It allows the administrator to give permission to sub administrators to access defined modules of eScan and perform installation/uninstallation of eScan Client on network computers or define Policies and tasks for the computers allocated to them.

## New Role

To add a user role,

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



**New Role**

User Roles > New Role

**Role Details**

New Role Name :\*

Description :

Select Group :

Managed Computers

Ok

2. Enter name and description for the role.
3. Click **Managed Computers** and select the specific group to assign the role.  
The added role will be able to manage and monitor only the selected group's activities.
4. Click **OK**.

Permissions section appears displaying Main Tree Menu and Client Tree Menu tabs. The Main Tree Menu consists of Navigation Panel Access permissions while the Client Tree Menu consists of selected groups on which permissions the user is allowed to take further.

Permissions		
Main Tree Menu Client Tree Menu		
Menu	View	Configure
DashBoard	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Managed Computers	<input checked="" type="checkbox"/>	<input checked="" 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"/>
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"/>
Notifications	<input type="checkbox"/>	<input type="checkbox"/>
Event Alert	<input type="checkbox"/>	<input type="checkbox"/>
Unlicense Move Alert	<input type="checkbox"/>	<input type="checkbox"/>
Settings	<input type="checkbox"/>	<input type="checkbox"/>
Web Console Settings	<input type="checkbox"/>	<input type="checkbox"/>




5. Select the check boxes that will allow the role to view/configure the module.

6. After selecting the necessary check boxes, click **Save**.  
The role will be added to the User Roles list.

## View Role Properties

To view the properties of a role

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

User Roles	
<div>  New Role            Properties            Delete         </div>	
Role Name	Description
Administrator	
<input checked="" type="checkbox"/> Monitor	For viewing activities

3. Click **Properties**.  
Properties screen appears. It lets you modify role description, permissions for accessing and configuring modules and assign the role to other groups by clicking **Select Group Tree**.

Properties Help

User Roles > Properties

---

**Role Details**

New Role Name :\*

Description :

Select Group :

---

**Permissions**

**Main Tree Menu** **Client Tree Menu**

Menu	View	Configure
DashBoard	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Managed Computers	<input checked="" type="checkbox"/>	<input checked="" 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"/>
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"/>
Notifications	<input type="checkbox"/>	<input type="checkbox"/>
Event Alert	<input type="checkbox"/>	<input type="checkbox"/>
Unlicense Move Alert	<input type="checkbox"/>	<input type="checkbox"/>
Settings	<input type="checkbox"/>	<input type="checkbox"/>
Web Console Settings	<input type="checkbox"/>	<input type="checkbox"/>
Excluded Clients	<input type="checkbox"/>	<input type="checkbox"/>
Administration	<input type="checkbox"/>	<input type="checkbox"/>
User Accounts	<input type="checkbox"/>	<input type="checkbox"/>
User Roles	<input type="checkbox"/>	<input type="checkbox"/>
License	<input type="checkbox"/>	<input type="checkbox"/>
Policy Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

4. To modify client configuration permissions, click **Client Tree Menu**.
- Client Tree Menu**

Define the Actions that the created role can configure for the allocated group. The menu has Action List, Client Action List, Select Policy Template, Policy Criteria, and Group Tasks.

Action	Configure
Menu	<input checked="" type="checkbox"/>
Action List	<input checked="" type="checkbox"/>
New Sub Group	<input checked="" type="checkbox"/>
Remove Group	<input checked="" type="checkbox"/>
Create Client Setup	<input checked="" type="checkbox"/>
Properties	<input checked="" type="checkbox"/>
Client Action List	<input checked="" type="checkbox"/>
Move to Group	<input checked="" type="checkbox"/>
Remove from Group	<input checked="" type="checkbox"/>
Manage Add-On License	<input checked="" type="checkbox"/>
Export	<input checked="" type="checkbox"/>
Show Installed Softwares	<input checked="" type="checkbox"/>
Create OTP	<input checked="" type="checkbox"/>
Properties	<input checked="" type="checkbox"/>
Anti-Theft Options	<input checked="" type="checkbox"/>
Disable Anti-Theft	<input checked="" type="checkbox"/>
Select Policy Template	<input checked="" type="checkbox"/>

- To let the role configure these actions, under the Configure column select the check boxes of corresponding actions.
- Click **Save**.  
The Role Properties will be updated accordingly.

## Delete a User Role

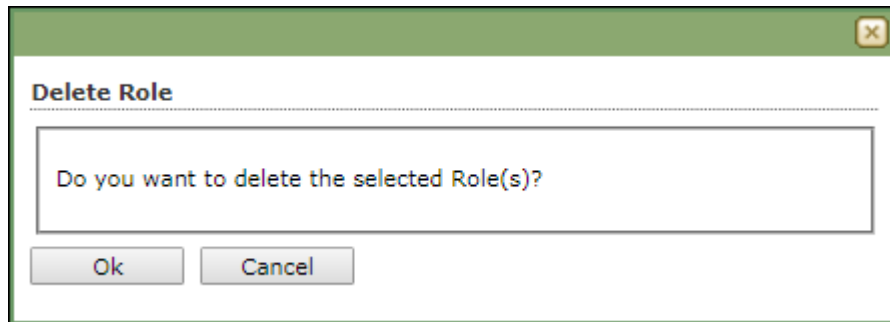
To delete a user role

- In the User Roles screen, select the user role you want to delete.

Role Name	Description
Administrator	
<input checked="" type="checkbox"/> Monitor	For viewing activities

- Click **Delete**.

A delete confirmation prompt appears.



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

# Export & Import

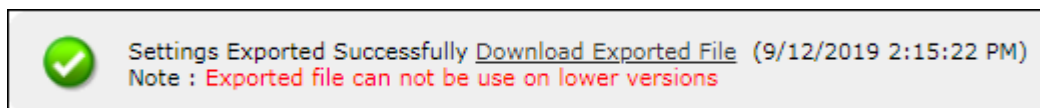
The Export & Import submodule lets you to take a backup of your eScan server settings, in case you want to replace the existing eScan server. You can export the Settings, Policies and the Database from existing server to a local drive and import it to the new server.

## Export Settings

This tab lets you export the eScan Server Settings, Policies, and Database. To export the eScan Server settings, follow the steps given below:

1. In the Export Import Settings screen, click **Export Settings** tab.

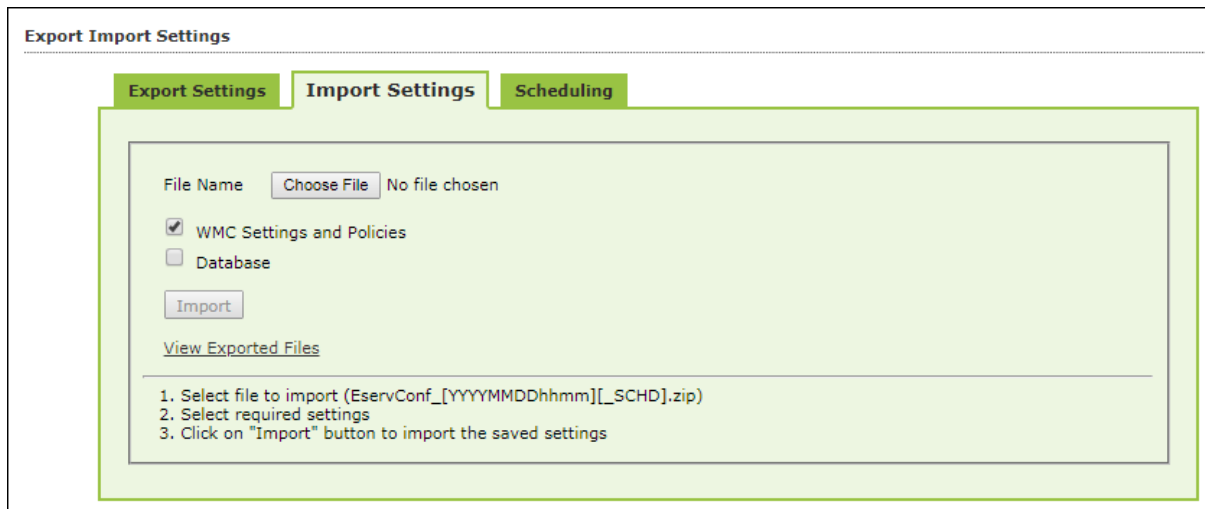
2. To backup Settings and Policies and Database, select both the checkboxes. The backup file will be exported to the path shown in Export File Path field. To change the file path, click **Change Path**. Enter the file path and click **Add**.
3. Click **Export**. The backup file will be exported to the destination path. A success message appears at the top displaying date, time and a download link for the exported file.



## Import Settings

This tab lets you import the eScan Server Settings, Policies, and Database. To import the eScan Server settings, follow the steps given below:

1. In the Export Import Settings screen, click **Import Settings** tab.



**Export Import Settings**

**Export Settings** **Import Settings** **Scheduling**

File Name  No file chosen

☒ WMC Settings and Policies

☐ Database

[View Exported Files](#)

1. Select file to import (EservConf\_[YYYYMMDDhhmm]\_[SCHD].zip)  
 2. Select required settings  
 3. Click on "Import" button to import the saved settings

2. Click **Choose File**.  
The Import Settings tab lets you import only Settings and Policies or Database.
3. To import Settings and Policies and Database, select both the checkboxes.
4. Click **Import**.  
The backup file will be imported. A success message is displayed after complete import.

<b>Note</b>	After successfully taking a backup, eScan asks you to restart the server.
-------------	---

## Scheduling

This tab lets you schedule auto-backing up of Settings, Policies, and Database.

**Export Import Settings** ? Help

**Export Settings** **Import Settings** **Scheduling**

☒ Enable Export Scheduler

☒ WMC Settings and Policies ☐ Database

☒ Daily  
☐ Weekly ☐ Mon ☐ Tue ☐ Wed ☐ Thu  
☐ Fri ☐ Sat ☐ Sun  
☐ Monthly

☒ At

☐ Enable Notification settings

Sender:   
 Recipient:   
 SMTP Server:   
 SMTP Port:

☐ Use SMTP Authentication

User name:   
 Password:

☒ Enable Optional Settings

Select how many backup files to store   
 Create the backup only if drive space is greater than or equal to :

[View Exported Files](#)

**Last schedule status :** Settings Exported Successfully On ( MM/DD/YYYY ) 11/02/2019 12:01 PM

To create a Schedule for export, follow the steps given below:

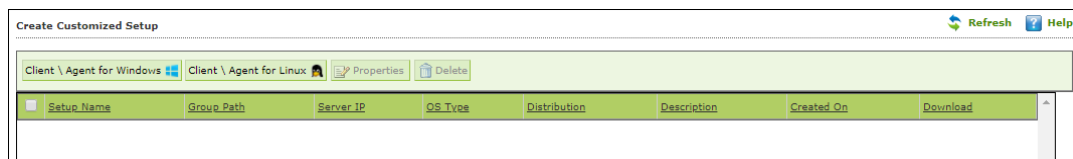
1. Select **Enable Export Scheduler** checkbox.
2. Select the checkboxes whether to back up both Settings and Policies and Database.
3. Schedule the backup for a **Daily**, **Weekly** (Select a day) or **Monthly** (Select a date) basis.



4. For the **At** field, click the drop-down and select a time for backing up data. If you want to receive email notifications about the procedure, select Enable Notifications Settings checkbox and fill in the necessary details. If the SMTP server requires authentication, select the Use SMTP Authentication checkbox and enter the credentials. To check if the SMTP settings are correct, click **Test**. A test email will be sent to recipient email ID.  
To configure additional settings for backup file, select the Enable Optional Settings, and make the necessary changes. To restore the changes made, click **Default**.
5. After performing all the necessary steps, click **Save**.  
The export schedule will be saved.

## Customize Setup

This submodule lets you create a customized setup for a Client or an Agent with fewer modules and deploy it to various locations. This can be very useful, if there are locations to which a server is unable to push the setup or locations that are unable to connect to the server directly. The custom setup can be downloaded as a file and sent to different locations.



## Creating a customized setup for Windows

To create a customized setup for Windows, follow the steps given below:

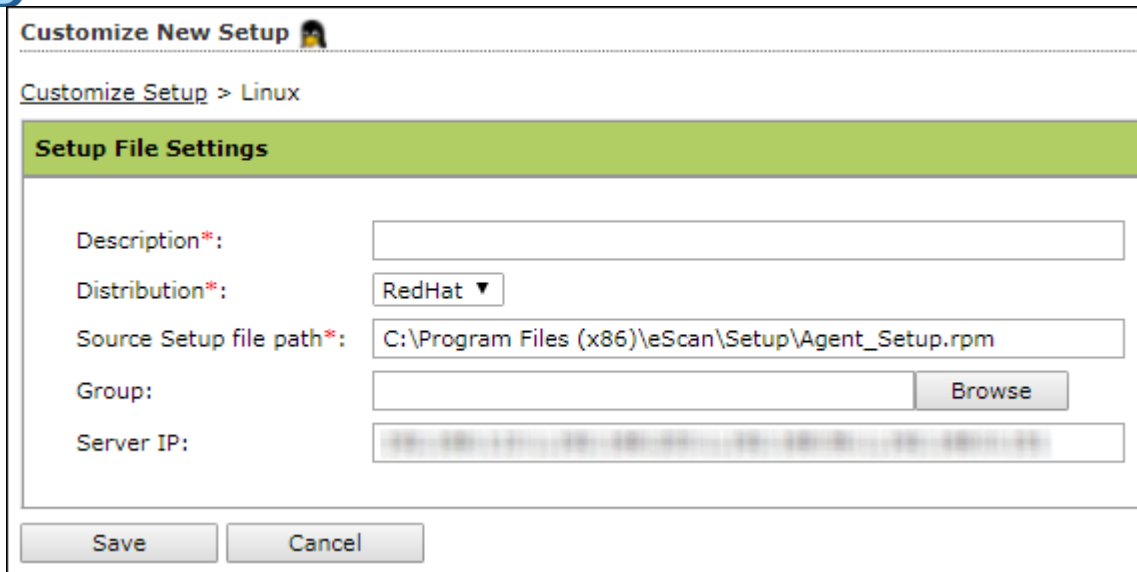
1. In Create Customized Setup screen, click **Client/Agent for Windows**.  
Customize New Setup screen appears.

2. Select whether the setup file is being created for **Client** or **Agent**.
  3. Enter description for the setup file.
  4. Click **Browse** and select a group for which this setup is being created.
  5. Enter eScan Server IP address.
  6. If you want to provide advanced settings with the setup, select the **Enable Advance Settings** checkbox. Doing so enables the bottom field. Select the setting checkboxes you want to provide.
  7. Click **Save**.
- The customized setup for Windows will be created.

## Creating a customized setup for Linux

To create a customized setup for Linux, follow the steps given below:

1. In Create Customized Setup screen, click **Client\Agent for Linux**.  
Customize New Setup screen appears.



Customize New Setup

Customize Setup > Linux

**Setup File Settings**

Description\*:

Distribution\*: RedHat ▼

Source Setup file path\*: C:\Program Files (x86)\eScan\Setup\Agent\_Setup.rpm

Group:  Browse

Server IP:

Save Cancel

2. Enter a description for the setup.
3. Click the drop-down select whether the setup is being created for Red Hat or Debian.
4. Source Setup file path field displays the setup file's location. If you want to change path, enter the new path in this field.
5. Click **Browse** and select a group for which this setup is being created.
6. Enter eScan Server IP address.
7. Click **Save**.

The customized setup for Linux will be created.

## Editing Setup Properties (only Windows)

The properties can be edited for only customized Windows setup. To edit the customized Windows setup's properties, follow the steps given below:

<div> Client \ Agent for Windows Client \ Agent for Linux Properties Delete </div>			
<input type="checkbox"/>	Setup Name	Group Path	Server IP
<input type="checkbox"/>	Managed Computers_20190913_144040721.rpm	Managed Computers	
<input checked="" type="checkbox"/>	Setup_20190913_144233504.exe	Managed Computers	

1. In the Create Customized Setup screen, select the Windows setup you want to edit.
2. Click **Properties**.  
Edit Customized Setup screen appears.

Edit Customized Setup

Customize Setup > Client \ Agent for Windows

Setup File Settings

Setup for\*:

Client
Agent

Description\*:

Sample

Group:

Managed Computers
Browse

Server IP\*:

☐ Enable Advance Settings

Advance Settings for Customized Setup

File AntiVirus

☐ Remove Mail Antivirus

☐ Remove AntiSpam

☐ Remove Firewall

☐ Remove End Point Security

☐ Remove Privacy Control

☐ Set Password

☐ Enable Schedule Scan

☐ Enable Cloud Scan

Client Installation Settings

Additional Settings

☐ Schedule Download

Save
Cancel

3. Make the necessary changes and then click **Save**. The setup will be updated.

## Deleting a Setup

To delete a setup, follow the steps given below:

<div> <div>Client \ Agent for Windows</div> <div>Client \ Agent for Linux</div> <div>Properties</div> <div>Delete</div> </div>			
<input type="checkbox"/>	Setup Name	Group Path	Server IP
<input type="checkbox"/>	Managed Computers_20190913_144040721.rpm	Managed Computers	
<input checked="" type="checkbox"/>	Setup_20190913_144233504.exe	Managed Computers	

1. In the Create Customized Setup screen, select the setup you want to delete.
2. Click **Delete**.

The setup will be deleted.

# License

The License module lets you manage user licenses. You can add, activate, and view the total number of licenses available for deployment, previously deployed, and licenses remaining with their corresponding values. The module also lets you move the licensed computers to non-licensed computers and vice versa. Here you can also view the number of add-on license along with the name of it. For example, as you can see here there are 15 add-on licenses for eBackup feature. The add-on license is available for eBackup, 2FA, and DLP features.

License

Refresh Help

Register Information

License Key(30 char)	Activation Code(50 char)	Registration Status	Contract Period Ends on	No. of Users	Add On License
	<a href="#">Activate Now</a>	Activate before 01-Jun-2020	-	10	---
		Activated	20-Apr-2021	200	EBackup+ RMM+ DLP+ 2FA
		Activated	13-May-2021	200	---

To Add License [Click Here](#)

License

License in Use

132

License Remaining

268

Total License Size

400

Manage License

## Adding and Activating a License

To add and activate a license

1. In the License screen, click the **Click Here** link.

To Add License [Click Here](#)

Add License Key dialog box appears.

Add 30 Character License Key.

OK Cancel

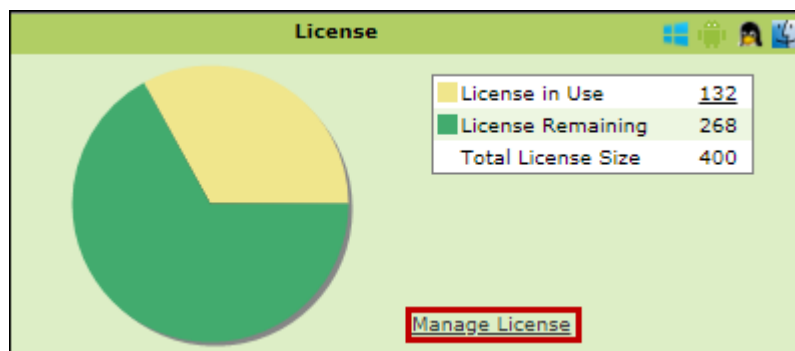
2. Enter the license key and then click **OK**.

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.

**Manage License** ? Help

---

**Licensed Computers / Devices (132)** Filter License: All v Move to Non-License

<input type="checkbox"/>	Machine Name	Group
<input type="checkbox"/>	WIN-7488	Managed - Computers (All Types)
<input type="checkbox"/>	WIN-7488	Managed - Computers (All Types)
<input type="checkbox"/>	WIN-7488	Managed - Computers (All Types)
<input type="checkbox"/>	WIN-7488	Managed - Computers (All Types)
<input type="checkbox"/>	WIN-7488	Managed - Computers (All Types)
<input type="checkbox"/>	WIN-7488	Managed - Computers (All Types)
<input type="checkbox"/>	WIN-7488	Managed - Computers (All Types)

---

**Non-Licensed Computers / Devices (327)** Filter License: All v Move to License

<input type="checkbox"/>	Machine Name	Group	Unlicense Date Time	Description
<input type="checkbox"/>	WIN-7488	Managed - Computers (All Types)	31/03/2018 02:08:25	
<input type="checkbox"/>	WIN-7488	Managed - Computers (All Types)	17/02/2018 11:10:01	
<input type="checkbox"/>	WIN-7488	Managed - Computers (All Types)	15/02/2018 11:50:10	

Close

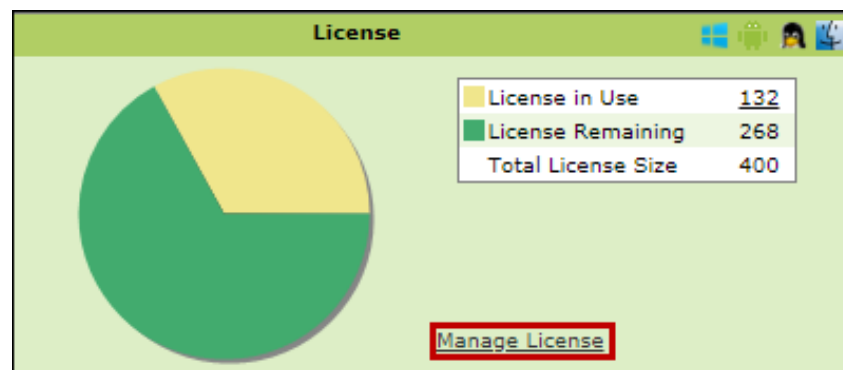


2. Under the Licensed Computers section, select the computer(s) that you want to move to Non-Licensed Computers section.
3. Click **Move to Non-License**.
4. The selected computer(s) will be moved to Non-Licensed computers section.

# Moving Non-Licensed Computers to Licensed Computers

To move licensed computers to non-licensed computers, follow the steps given below:

1. In the License statistics box, click **Manage License**.



Manage License window appears.

Manage License

Help

Licensed Computers (385)

Move to Non-License

<input type="checkbox"/>	Machine Name	Group
<input type="checkbox"/>	[blurred]	Managed Computers
<input type="checkbox"/>	[blurred]	Managed Computers
<input type="checkbox"/>	[blurred]	Managed Computers
<input type="checkbox"/>	[blurred]	Managed Computers
<input type="checkbox"/>	[blurred]	Managed Computers
<input type="checkbox"/>	[blurred]	Managed Computers

Non-Licensed Computers (2)

Move to License

<input type="checkbox"/>	Machine Name	Group	Unlicense Date Time	Description
<input type="checkbox"/>	[blurred]	Managed Computers	13/09/2019 17:13:16	
<input type="checkbox"/>	[blurred]	Managed Computers	13/09/2019 17:13:16	



2. Under the Non-Licensed Computers section, select the computer(s) that you want to move to Licensed Computers section.
3. Click **Move to License**.
4. The selected computer(s) will be moved to Licensed Computers section.

# 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**