



# eScan Enterprise DLP User Guide

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

Copyright © 2024 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>	<b>5BUG/27.12.2024/22.x</b>
<b>Current Software Version:</b>	<b>22.0.0000.xxxx</b>
<b>Technical Support:</b>	<b><u><a href="mailto:support@escanav.com">support@escanav.com</a></u></b>
<b>Sales:</b>	<b><u><a href="mailto:sales@escanav.com">sales@escanav.com</a></u></b>
<b>Forums:</b>	<b><u><a href="https://forums.escanav.com">https://forums.escanav.com</a></u></b>
<b>eScan Wiki:</b>	<b><u><a href="https://wiki.escanav.com/wiki/index.php/">https://wiki.escanav.com/wiki/index.php/</a></u></b>
<b>Published by:</b>	<b>MicroWorld Software Services Private Limited</b>
<b>Date:</b>	<b>December, 2024</b>

# Table of Contents

---

Introduction.....	9
Pre-requisites for eScan Enterprise DLP .....	9
System Requirements.....	10
Hardware and Software Requirements.....	10
Installing eScan Enterprise DLP.....	11
Installation.....	12
Components of eScan Server .....	20
Web Console Login .....	21
Setup Links .....	23
Main Interface.....	24
Setup Wizard.....	25
Navigation Panel.....	31
Dashboard .....	34
Deployment Status .....	34
eScan Status .....	35
License .....	35
eScan version .....	36
Protection Status .....	37
Web Protection.....	37
Endpoint Security.....	38
Privacy .....	39
Protection Statistics.....	40
Web Protection.....	40
Endpoint Security-USB.....	41
Endpoint Security-Application .....	42
Summary Top 10.....	43
Asset Changes.....	44
Live Status .....	45
DLP Protection Status.....	46
Sensitive Folder Protection .....	47
Attachment Upload Control.....	48
Device Encryption .....	48
RMM.....	49
DLP Statistics.....	50
Content Control.....	51
EBackup.....	53
Attachment Control.....	53
File Activity .....	54
File Integrity.....	54
DLP Discovery.....	55
Configure the Dashboard Display.....	56
Managed Computers .....	57
Search.....	58

Update Agent .....	59
Adding an Update Agent.....	59
Configuring UA Settings .....	60
Delete an Update Agent .....	61
Action List .....	62
Creating a Group.....	62
Removing a Group.....	63
Set Group Configuration.....	63
Managing Installations.....	64
Deploy/Upgrade Client .....	66
Manual installation of eScan Client on network computer(s).....	68
Installing eScan Client Using Agent.....	68
Installing other Software (Third Party Software).....	69
Uninstall eScan Client (Windows).....	70
Synchronize with Active Directory.....	71
Create Client Setup  .....	72
Properties of a group .....	73
Group Tasks .....	74
Creating a Group Task.....	74
Managing a Group Task.....	75
Assigning a Policy to the group .....	77
Client Action List.....	79
Set Host Configuration.....	80
Deploy/Upgrade Client .....	80
Uninstall eScan Client.....	81
Move to Group.....	82
Remove from Group .....	82
Refresh Client .....	82
Connect to Client (RMM).....	83
Assign Policy Template .....	83
Export.....	83
Show Installed Softwares.....	84
Force Download.....	85
Collect Debug/Logs .....	86
Check eScan Port(s).....	86
Send Message.....	87
Create OTP.....	88
Pause Protection.....	90
Resume Protection .....	91
Properties of Selected Computer.....	92
Refresh Client .....	92
Anti-Theft (requires additional license).....	93
Anti-Theft Options.....	93
Disable Anti-Theft .....	96
Understanding the eScan Client Protection Status.....	97
Select Columns .....	98

Policy Template .....	99
Managing Policies.....	99
Creating Policy Template for a group/specific computer .....	101
Configuring eScan Policies for Windows Computers .....	102
Configuring eScan Policies for Linux and Mac Computers .....	160
Assigning Policy Template to a group.....	177
Assigning Policy Template to Computer(s).....	180
Copy a Policy Template.....	181
Exporting a Policy Template report.....	181
Parent Policy .....	182
Policy Criteria Templates .....	184
Adding a Policy Criteria Template (AND condition).....	184
Adding a Policy Criteria Template (OR condition) .....	190
Viewing Properties of a Policy Criteria template .....	191
Assigning a Policy Criteria template to Group .....	192
Assigning a Policy Criteria template to Computer .....	194
Deleting a Policy Criteria template.....	195
Unmanaged Computers.....	198
Network Computers .....	198
Creating a New Group from the Select Group window .....	199
IP Range.....	200
Adding New IP Range .....	200
Moving an IP Range to a Group .....	201
Deleting an IP Range .....	201
Searching an IP Range .....	202
Refreshing Client in IP Range .....	202
Active Directory.....	204
Adding from Active Directory .....	204
Moving Computers from an Active Directory .....	205
New Computers Found .....	205
Filter Criteria.....	206
Action List .....	206
Report Templates .....	207
Creating a Report Template .....	208
Creating Schedule for a Report Template.....	208
Viewing Properties of a Report Template.....	208
Deleting a Report Template .....	209
Report Scheduler.....	210
Creating a Schedule .....	210
Viewing Reports on Demand.....	213
Managing Existing Schedule .....	214
Generating Task Report of a Schedule .....	214
Viewing Results of a Schedule .....	214
Viewing Properties of a Schedule .....	215
Deleting a Schedule .....	215
Events and Computers .....	216

Events Status.....	216
Computer Selection.....	217
Edit Selection .....	219
Software/Hardware Changes .....	220
Settings.....	221
Event Status .....	221
Computer Selection.....	222
Software/ Hardware Changes Setting .....	223
Performing an action for computer .....	224
Tasks for Specific Computers .....	225
Creating a task for specific computers .....	225
Viewing Properties of a task .....	227
Viewing Results of a task .....	227
Deleting a task for specific computers .....	228
Asset Management.....	229
Hardware Report.....	229
Filtering Hardware Report .....	230
Exporting Hardware Report.....	230
Software Report .....	231
Filtering Software Report.....	231
Exporting Software Report .....	232
Software License.....	232
Filtering Software License Report .....	233
Exporting Software License Report.....	233
Software Report (Microsoft).....	235
Filtering MS Office Software Report.....	235
Exporting MS Office Software Report .....	236
Filtering Microsoft OS Report .....	236
Exporting Microsoft OS Report.....	237
User Activity.....	238
Print Activity.....	238
Viewing Print Activity Log.....	238
Exporting Print Activity Log .....	238
Filtering Print Activity Log.....	239
Exporting Print Activity Report.....	239
Print Activity Settings.....	240
Session Activity Report .....	241
Viewing Session Activity Log .....	241
Filtering Session Activity Log .....	241
Exporting Session Activity Report .....	242
File Activity Report .....	243
Viewing File Activity Log .....	243
Filtering File Activity Log .....	243
Exporting File activity Report.....	244
Application Access Report .....	245
Viewing Application Access Report.....	245

Filtering Application Access Report.....	246
Exporting Application Access Report.....	246
Notifications.....	248
Event Alert.....	248
Unlicensed Move Alert.....	250
New Computer Alert.....	250
SMTP Settings.....	251
Settings.....	252
EMC Settings.....	253
Web Console Settings.....	255
Update Settings.....	258
General Config.....	258
Update Notification.....	259
Scheduling.....	259
Auto-Grouping.....	261
Two-Factor Authentication (2FA).....	262
Enabling 2FA login.....	264
Disabling 2FA login.....	265
Users For 2FA.....	266
Administration.....	270
User Accounts.....	270
Create New Account.....	270
Adding a User from Active Directory.....	271
Delete a User Account.....	272
User Roles.....	273
New Role.....	273
View Role Properties.....	274
Delete a User Role.....	276
Export & Import.....	277
Export Settings.....	277
Import Settings.....	278
Scheduling.....	279
Customize Setup.....	281
Creating a customized setup for Windows.....	281
Editing Setup Properties.....	282
Deleting a Setup.....	283
Creating a customized setup for Linux.....	283
Audit Trail.....	284
Filter all Audit Trail report.....	284
Exporting Audit Trail.....	284
License.....	285
Adding and Activating a License.....	285
Moving Licensed Computers to Non-Licensed Computers.....	286
Moving Non-Licensed Computers to Licensed Computers.....	288
Getting Started.....	290
Graphical User Interface (GUI).....	290



Data Encryption .....	291
How to Create a Vault? .....	291
Two-Factor Authentication .....	298
Enabling 2FA login .....	298
Disabling 2FA login .....	302
Quick Access Links .....	303
Update .....	303
eScan Remote Support .....	306
Password .....	307
License Information .....	308
Tools .....	310
Reports .....	314
Contact Us .....	316
Forums .....	316
Chat Support .....	316
Email Support .....	316



# Introduction

eScan Enterprise Data Leak Prevention (DLP) security solution based on set of strategies, technologies, and techniques that ensure end users do not transmit critical or sensitive data outside an organization. Whether transmission of data is through message, email, file transfers, or some other way, information can end up in unauthorized locations, leading to compliance issues.

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

## Pre-requisites for eScan Enterprise DLP

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

- Access to system 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).



**NOTE**

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

# System Requirements

## Hardware and Software Requirements

The software and hardware requirements for installing eScan are as follows:

### **Windows Requirements**

#### **Platforms Supported (Windows server & workstations)**

Microsoft® Windows® 2022 / 2019 / 2016 / 2012 / SBS 2011 / Essential / 2008 R2 / 2008 / 2003 R2 / 2003 / 11 / 10 / 8.1 / 8 / 7 / Vista / XP SP 2 / 2000 Service Pack 4 and Rollup Pack 1 (For 32-Bit and 64-Bit Editions)

#### **Hardware Requirement for Server**

- CPU - 2GHz Intel™ Core™ Duo processor or equivalent.
- Memory - 4 GB and above
- Disk Space (Free) – 8 GB and above

#### **Hardware Requirement for Endpoints (Windows)**

- CPU - 1.4 Ghz minimum (2.0 Ghz recommended) Intel Pentium or equivalent
- Memory - 1.0 GB and above
- Disk Space (Free) – 1 GB and above

#### **eScan Management Console can be accessed by using below browsers:**

- Internet Explorer 11 and above
- Firefox latest version
- Google Chrome latest version and all chromium-based browser

### **Linux Requirements**

#### **Platforms Supported (Linux Endpoints)**

- 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)
- Mint 12 and above (32 and 64-bit)

#### **Hardware Requirements (Endpoints)**

- CPU - Intel® Pentium or compatible or equivalent.
- Memory – 2 GB and above
- Disk Space – 2 GB free hard drive space for installation of the application and storage of temporary files

## Mac Requirements

### Platforms Supported (Mac Endpoints)

- 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 or later)
- macOS Monterey (12.0 or later)

### Hardware Requirements (Endpoints)

- CPU - Intel based Macintosh
- Memory – 2 GB and More recommended
- Disk Space – 2 GB and above

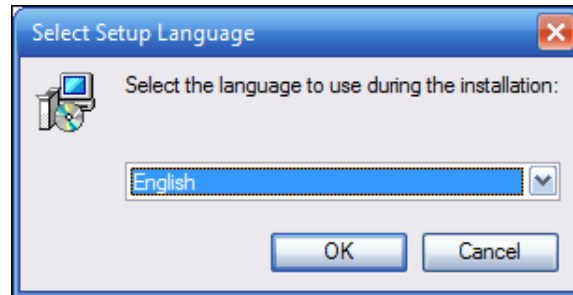
## Installing eScan Enterprise DLP

- **Installing eScan Enterprise DLP from CD/DVD**  
Installing eScan Enterprise DLP 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 on **WMXXXXXX.exe** file on CD-ROM. This will run the installation wizard based setup of eScan Enterprise DLP. To complete the installation, follow the instructions on screen.
- **Downloading and installing eScan Enterprise DLP from internet**  
To download the setup file click [here](#). To install eScan Server from the downloaded file, double click on **WMCTOTxxxx.exe** file and follow the instructions on screen to complete the installation process.

# Installation

To install the eScan Enterprise DLP, follow the steps given below:

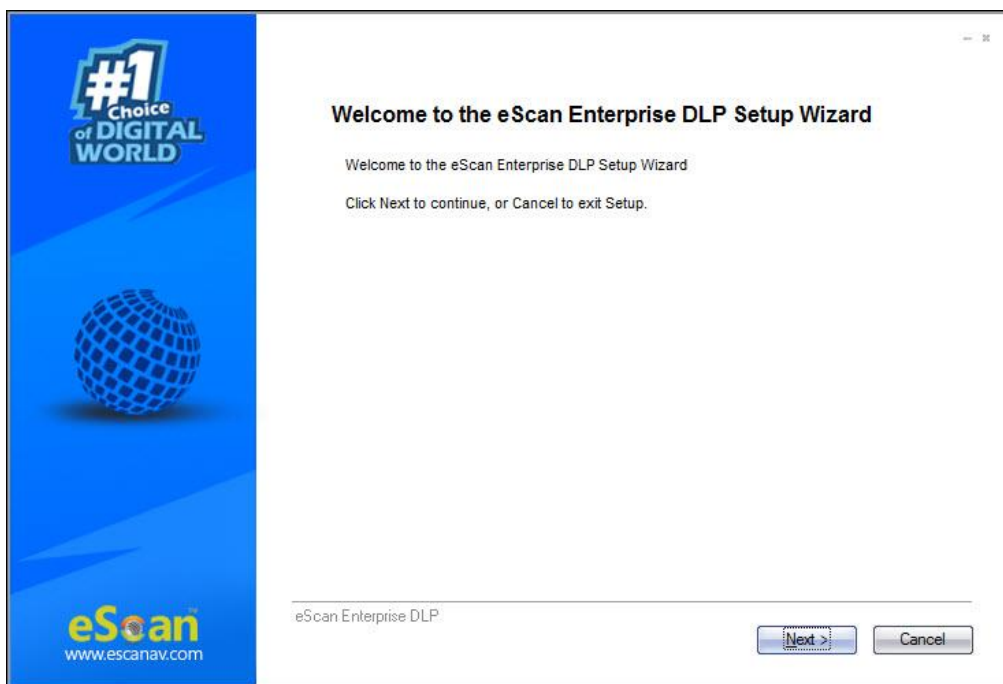
1. The installation wizard displays following window.



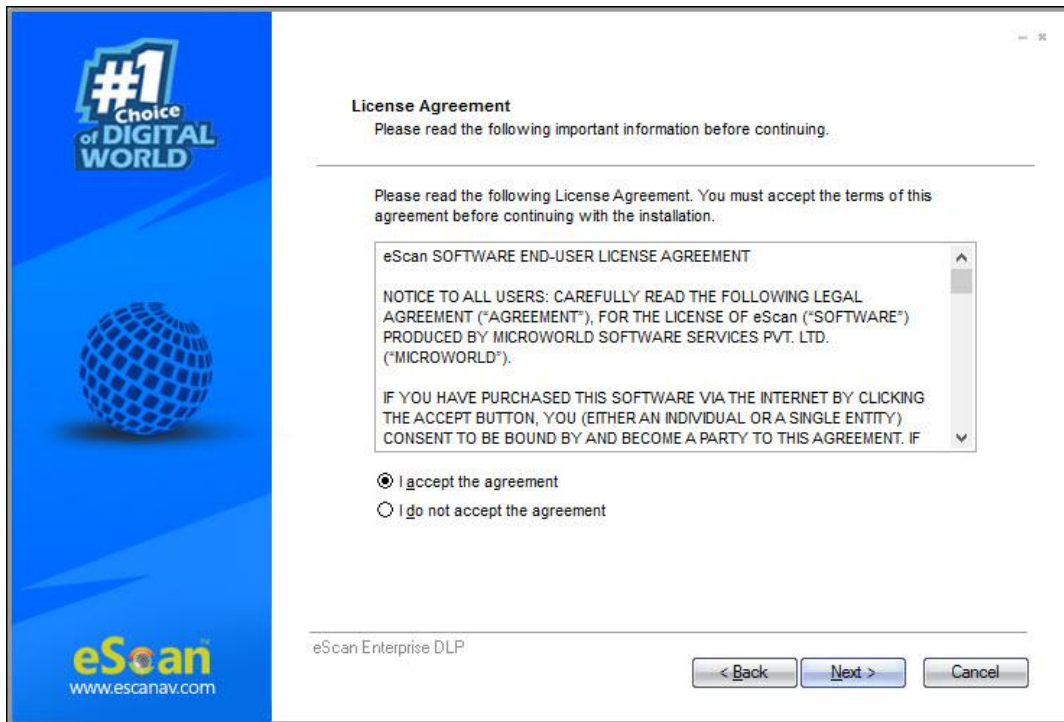
2. Click the drop-down and select a desired language for installation.
3. Click **OK**.

**NOTE** ! The Default Language displayed in the drop-down menu is dependent on the Operating System's language installed on the computer.

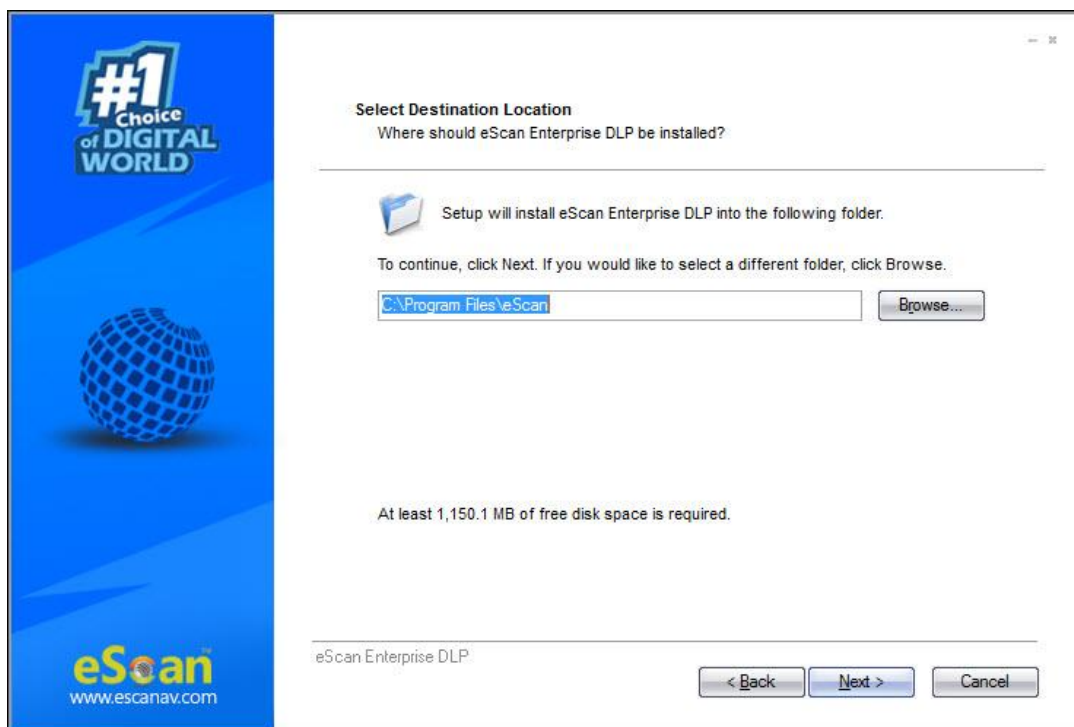
The installation wizard welcomes you.



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

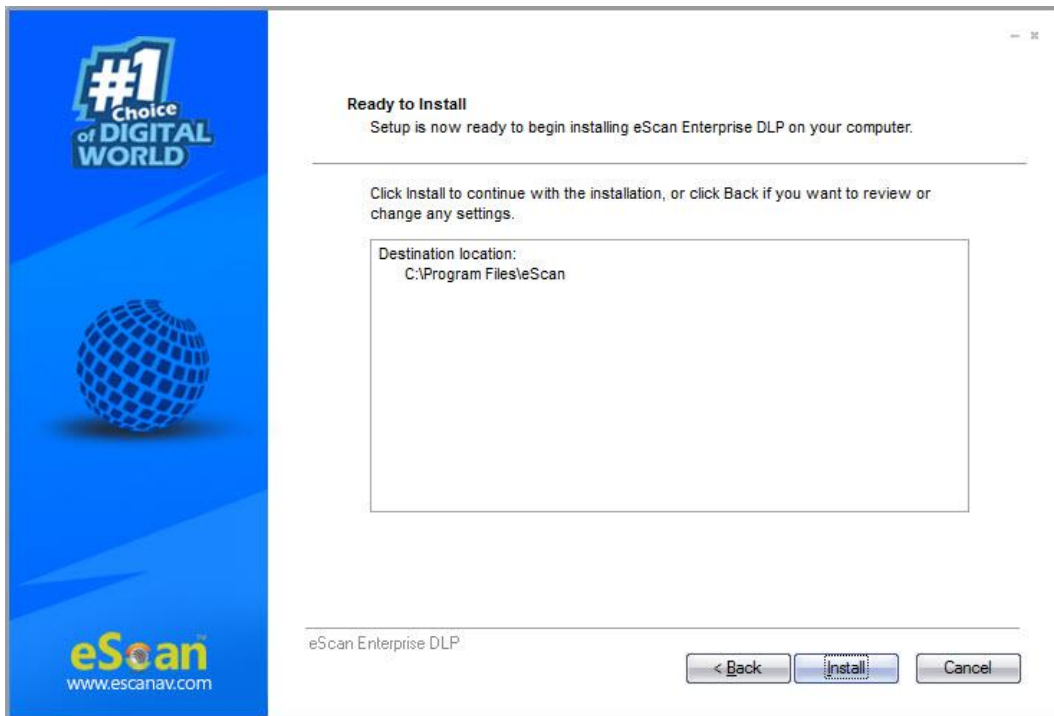


6. Select Destination Location for the installation of eScan Enterprise DLP. If you want to select a different installation location, click **Browse** and select the destination folder for installation.



	<p><b>NOTE</b> Default Path for eScan installation on a 32-bit PC – <b>C:\Program Files\eScan</b>          Default path for eScan installation on a 64-bit PC – <b>C:\Program Files (x86)\eScan</b></p>
--	---

7. Click **Next >**.  
The Ready to Install window appears.



8. Click **Install**.  
The installation wizard initiates installation and displays the process.



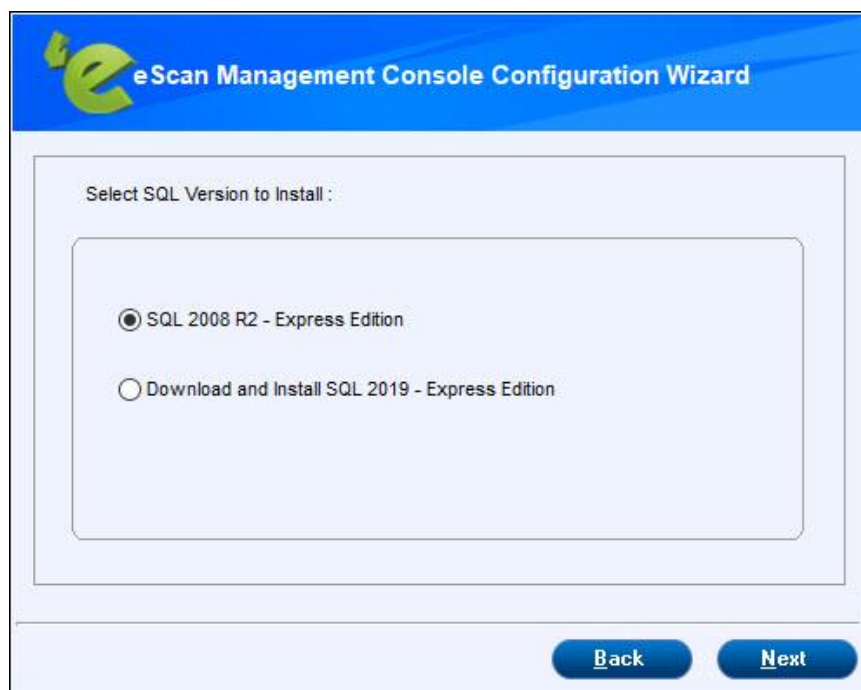
After the installation, the wizard asks you to configure the settings for SQL Server hosting and Login settings for the eScan Management console.



9. To proceed, click **Next**. The configuration wizard requests you to select following SQL version to install:

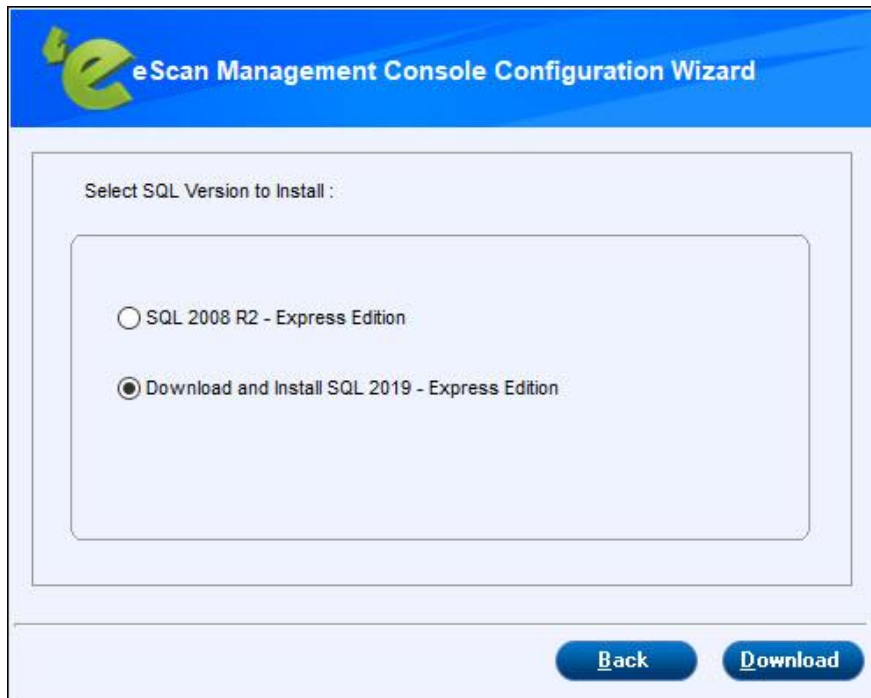
- **SQL 2008 R2 - Express Edition**

Select this option to install SQL version 2008 R2 - Express Edition.

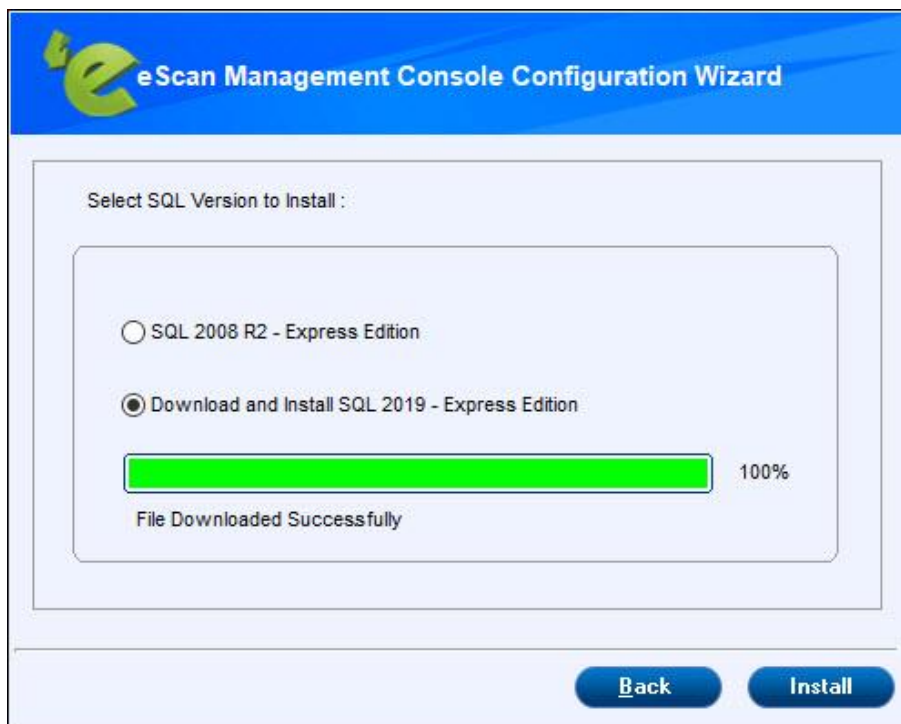


- **Download and Install SQL 2019 - Express Edition**

To download and install SQL version 2019 – Express Edition, select this option and click on **Download**.



The download process will begin as shown in the below window:



10. After file gets downloaded, click on **Install**.  
The configuration wizard will begin installation process of the Microsoft SQL Server Express.



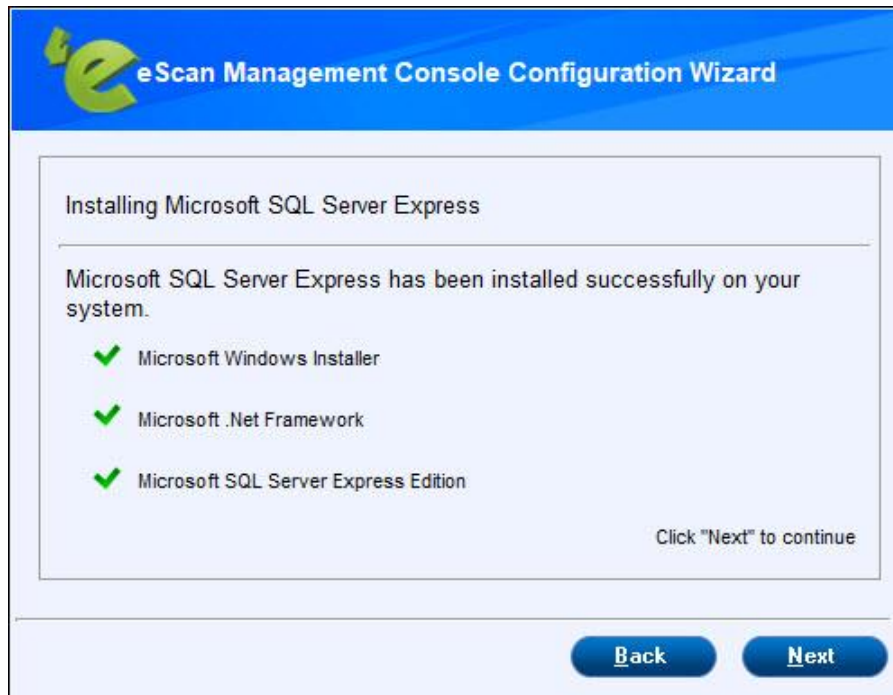


11. To proceed, click **Install**.  
Choose Directory For Extracted Files window appears.



12. Select the destination folder and click **Ok**.  
The SQL will be installed as confirmed by below window:

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

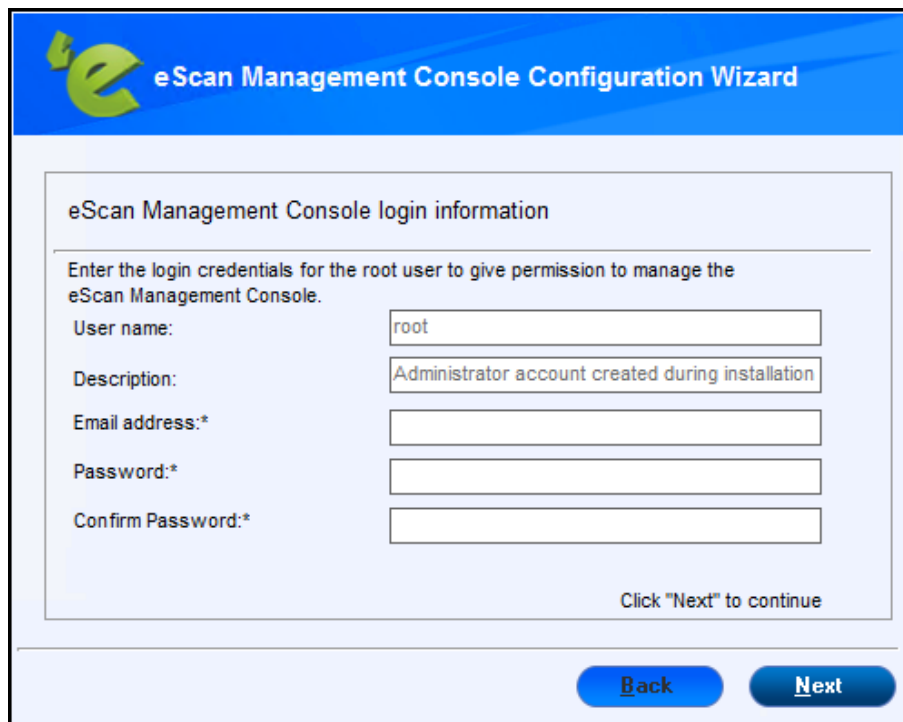


13. To proceed, click **Next**.

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



The default username for web console is **root**.

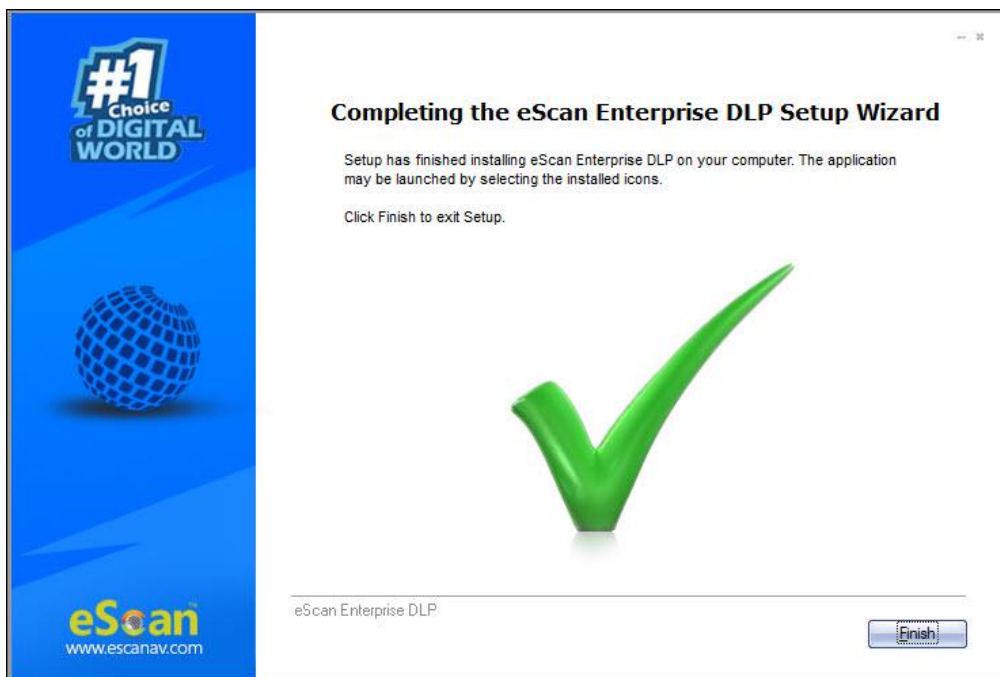


14. After filling all the details, click **Next**.

The wizard displays installation successful message.



15. To exit the installation wizard, click **Finish**.



16. Click **Finish** to complete the installation process.

	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.



For Windows 11 / 10 / 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.

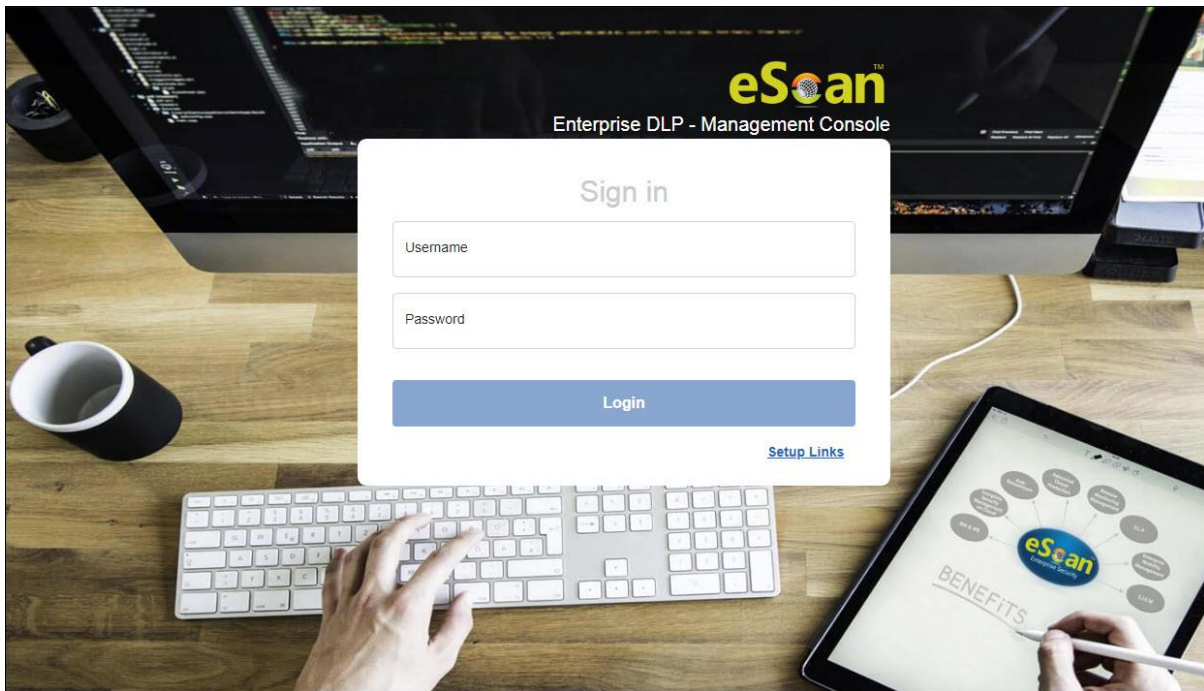
Uninstallation of eScan server won't remove SQL and APACHE from the endpoint. The user will have to uninstall these components manually.

## 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:

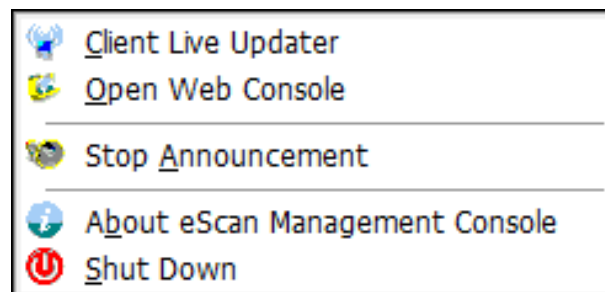
1. Launch a web browser.
2. Enter the following URL: <IP address of the eScan Server installed system>:10443  
Web console login page appears.



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
30 Jul 2021	12:22:26	WIN-GSPP...	192.168.0.67	WIN-GSPP...	File Anti...	[C] eScan M...	Windo
30 Jul 2021	12:22:26	WIN-GSPP...	192.168.0.67	WIN-GSPP...	File Anti...	[C] eScan M...	C:\Pro
30 Jul 2021	12:22:27	WIN-GSPP...	192.168.0.67	WIN-GSPP...	File Anti...	[C] eScan M...	Admini
30 Jul 2021	12:22:28	WIN-GSPP...	192.168.0.67	WIN-GSPP...	File Anti...	[C] eScan M...	REMO
30 Jul 2021	12:22:29	WIN-GSPP...	192.168.0.67	WIN-GSPP...	File Anti...	[C] WinEvent	A logo
30 Jul 2021	12:22:30	WIN-GSPP...	192.168.0.67	WIN-GSPP...	File Anti...	[C] WinEvent	Remot
30 Jul 2021	12:22:32	WIN-GSPP...	192.168.0.67	WIN-GSPP...	File Anti...	[C] eScan M...	REMO
30 Jul 2021	12:22:36	WIN-GSPP...	192.168.0.67	WIN-GSPP...	File Anti...	[C] eScan M...	REMO
30 Jul 2021	12:32:03	751-3034295	-	Device_Nes...	Device_Nes...	Android	Policy
30 Jul 2021	12:32:03	751-3034295	-	Device_Nes...	File Anti...	ConfigAndr...	Auto s
30 Jul 2021	12:32:03	751-3034295	-	Device_Nes...	File Anti...	Anti-Theft (A...	Anti-TI
30 Jul 2021	12:32:03	751-3034295	-	Device_Nes...	File Anti...	Web and A...	Web C
30 Jul 2021	12:32:03	751-3034295	-	Device_Nes...	File Anti...	Web and A...	Applic
30 Jul 2021	12:32:04	751-3034295	-	Device_Nes...	File Anti...	ConfigAndr...	Protec
30 Jul 2021	12:32:04	751-3034295	-	Device_Nes...	File Anti...	Call & SMS ...	Call/SI
30 Jul 2021	12:32:04	751-3034295	-	Device_Nes...	File Anti...	Android	Compli
30 Jul 2021	13:32:09	751-3034295	-	Device_Nes...	File Anti...	Android	Policy

### 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.

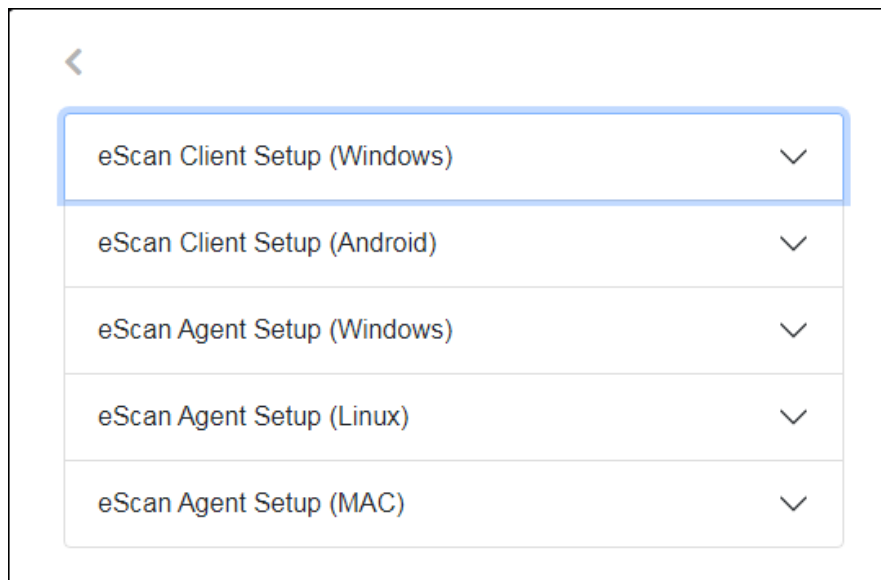


It is recommended that you do not shut down the server, as doing so will stop the communications between client and server.

The "root" is the Superuser account created by eScan during Installation.

## Setup Links

The web console login page displays **Setup Links** options that let you to download client and agent setup files.



- **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 Client Setup (Android)**  
This link can be shared via email to the android users where remote installation is impossible. By clicking this link users can download the EMM application from eScan Client Setup and install it manually on their android device. Users can also directly access the eScan Management console from their Android device.
- **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)**  
This link can be shared with the Linux computer user for manual installation.
- **eScan Agent Setup (Mac)**  
This link can be shared with the Mac computer user for manual installation.

# Main Interface

Upon first login, console displays Setup Wizard that familiarizes you with the basic procedures.



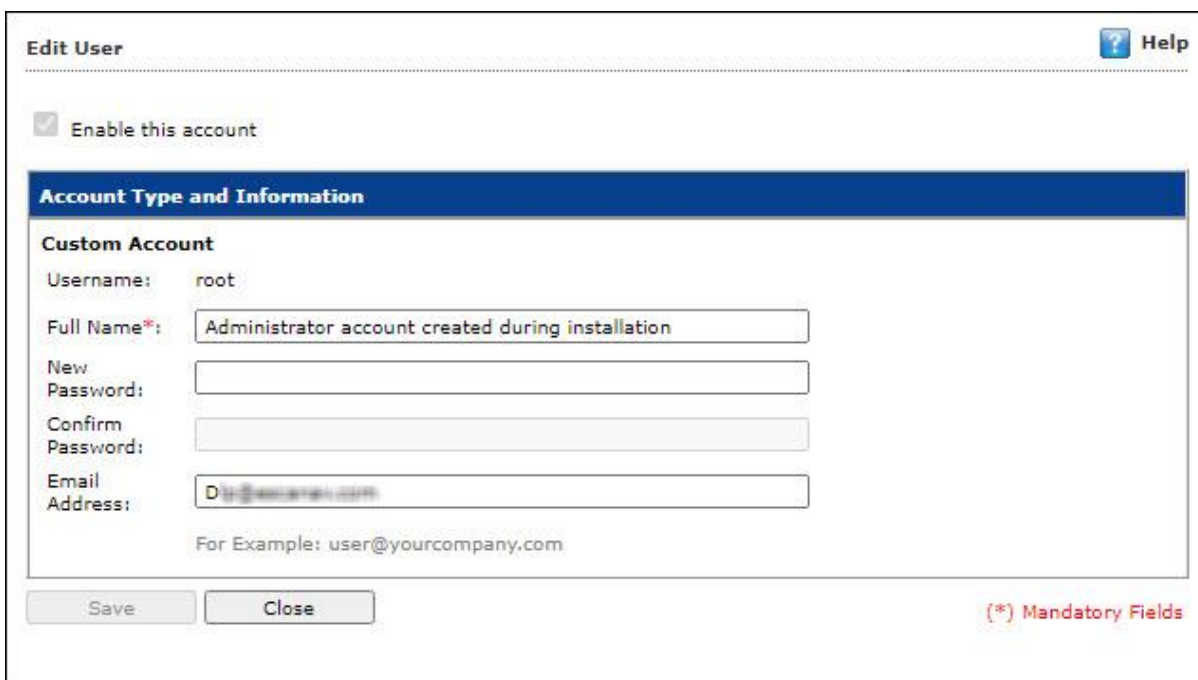
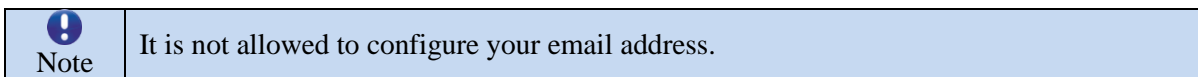
The links in the top right corner are explained below:

## 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.

## Refresh

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

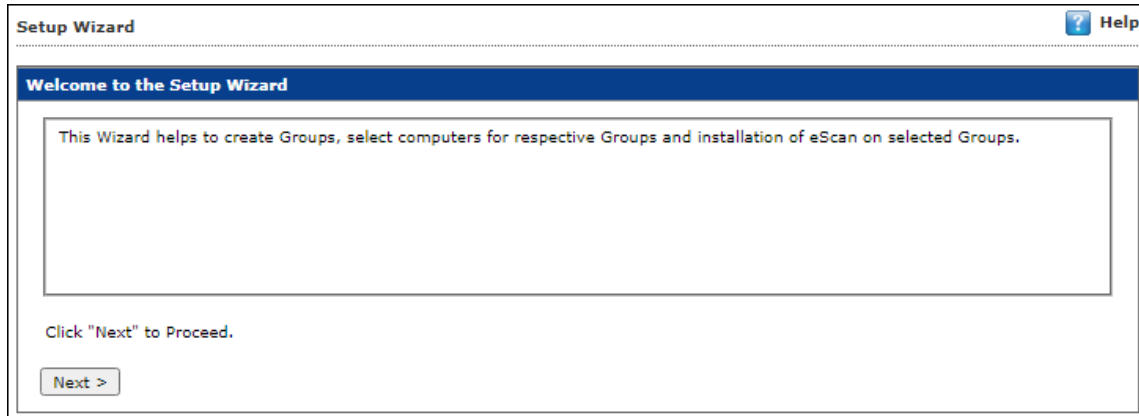
## Help

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

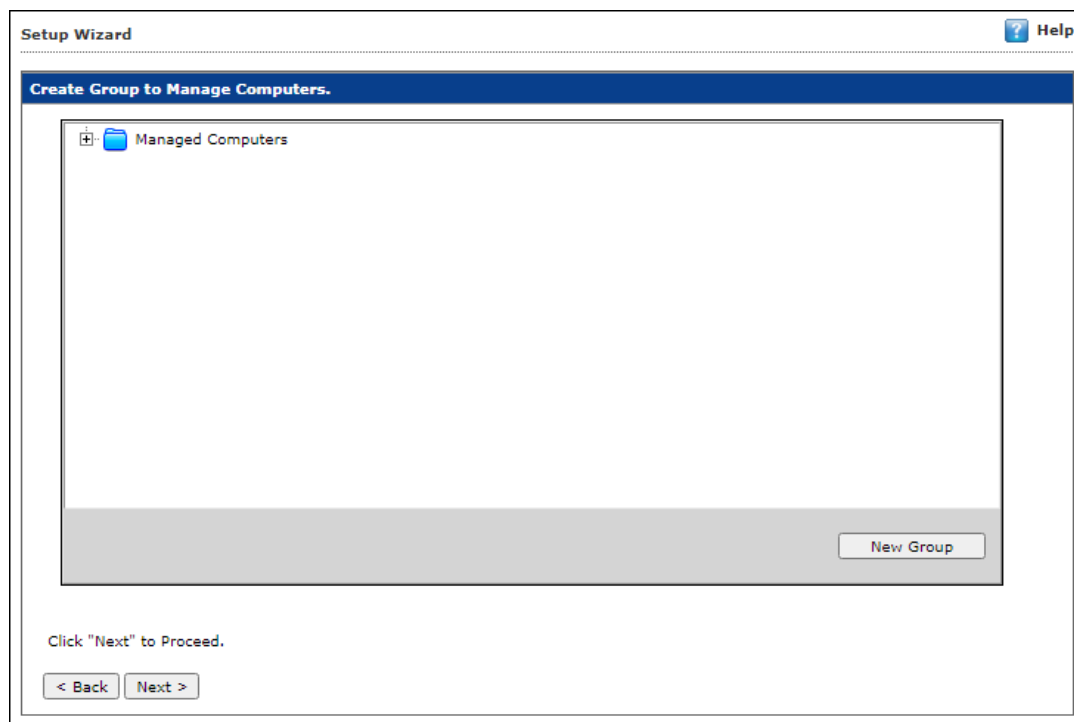


# Setup Wizard

The Setup Wizard helps you to quick start with the eScan Management Console, by allowing admin to perform basic functions such as creating groups, adding computers to it, and installing eScan on it. It is recommended that you follow the steps displayed, before proceeding to the other modules:

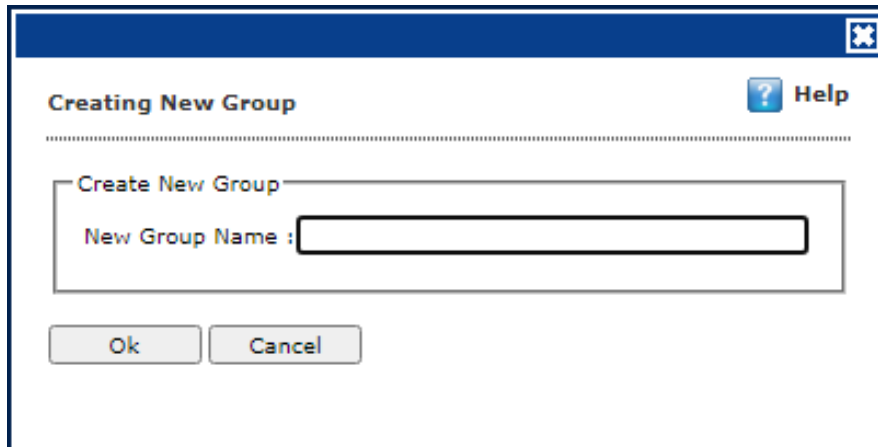


1. In the Setup Wizard screen, click **Next**.  
Create Group to Manage Computers window appears.

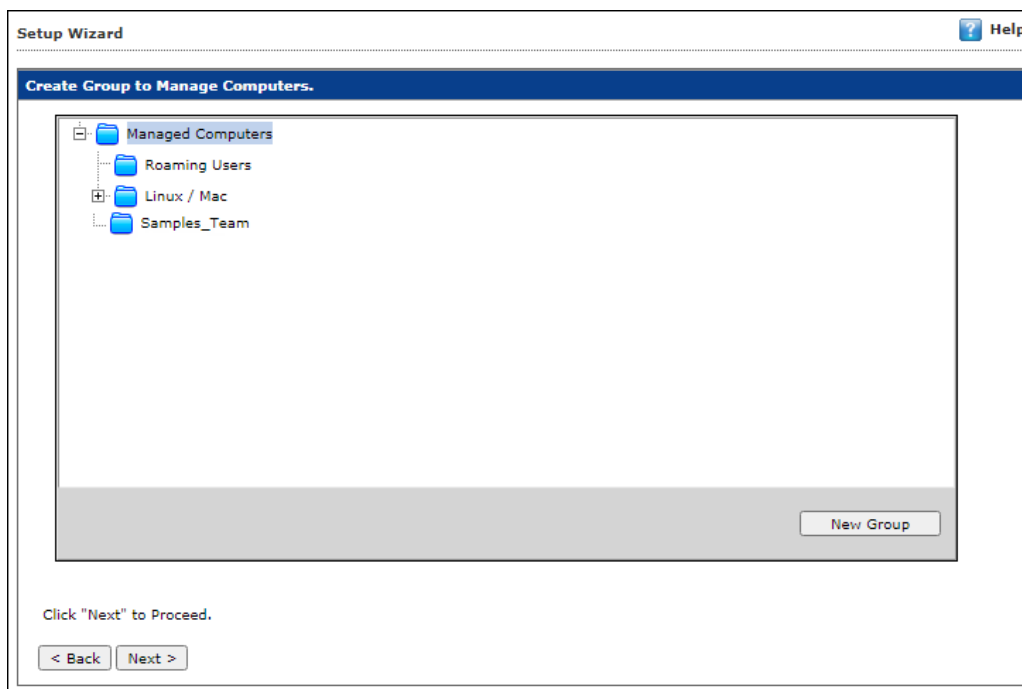


2. To create a new group, select a group (Managed Computers) and click **New Group**.

Creating New Group popup appears.

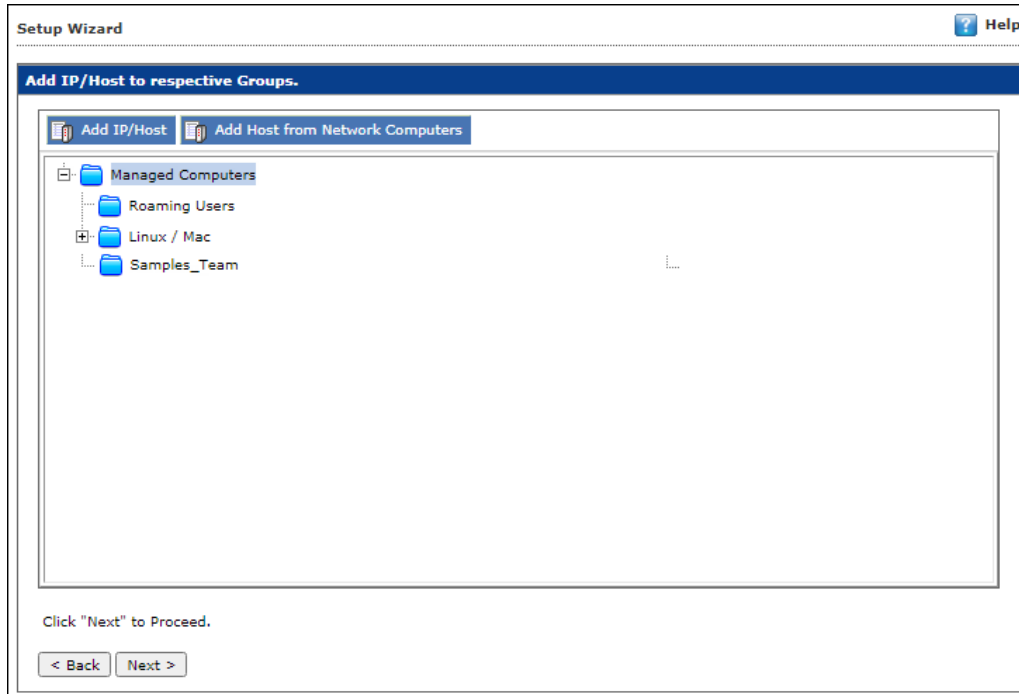


3. Enter the name of the group and click **OK**.
4. After creating group, click **Next>** to add computers to the respective group.  
Add IP/Host to respective Groups window appears.



After creating a group, you can add computers to the group via following methods:

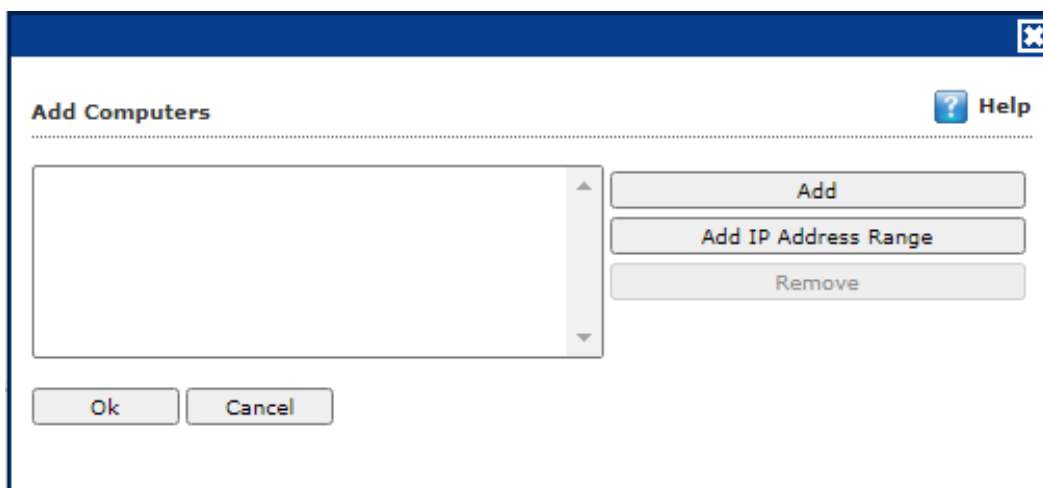
- IP Address/Host name
- Host from Network Computers



## Adding computers via IP Address/Host Name

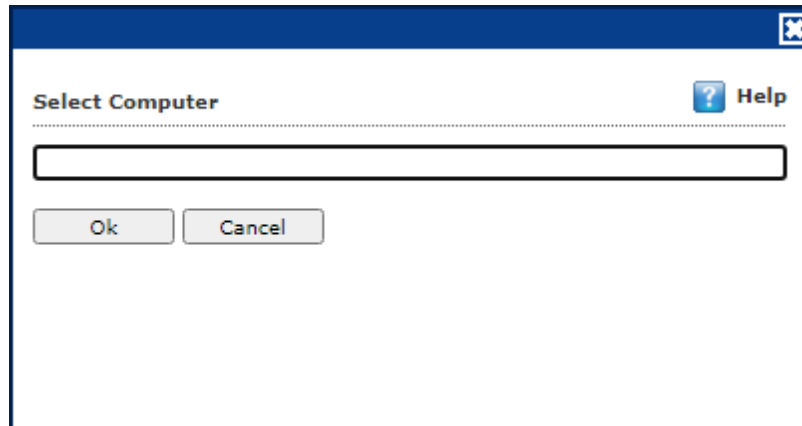
To add the computers through IP Address, follow the below steps:

1. Select the group and click **Add IP Address/Host Name**.  
Add Computers window appears.



2. Click **Add**.

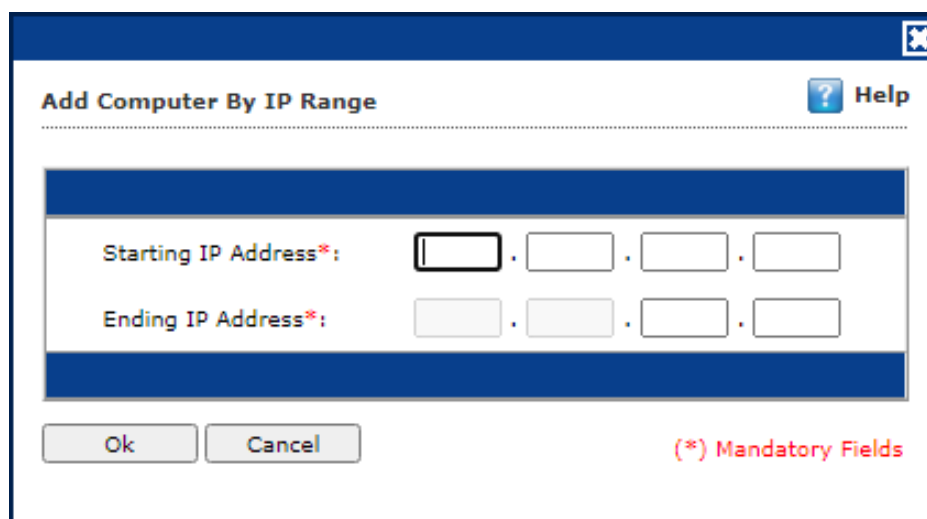
Select Computers popup appears.



3. Enter the **IP Address/Host name** and click **OK**.  
The computer will be added.

OR

4. To add an IP range, click **Add IP Address Range**.  
Add Computers By IP Range popup appears.

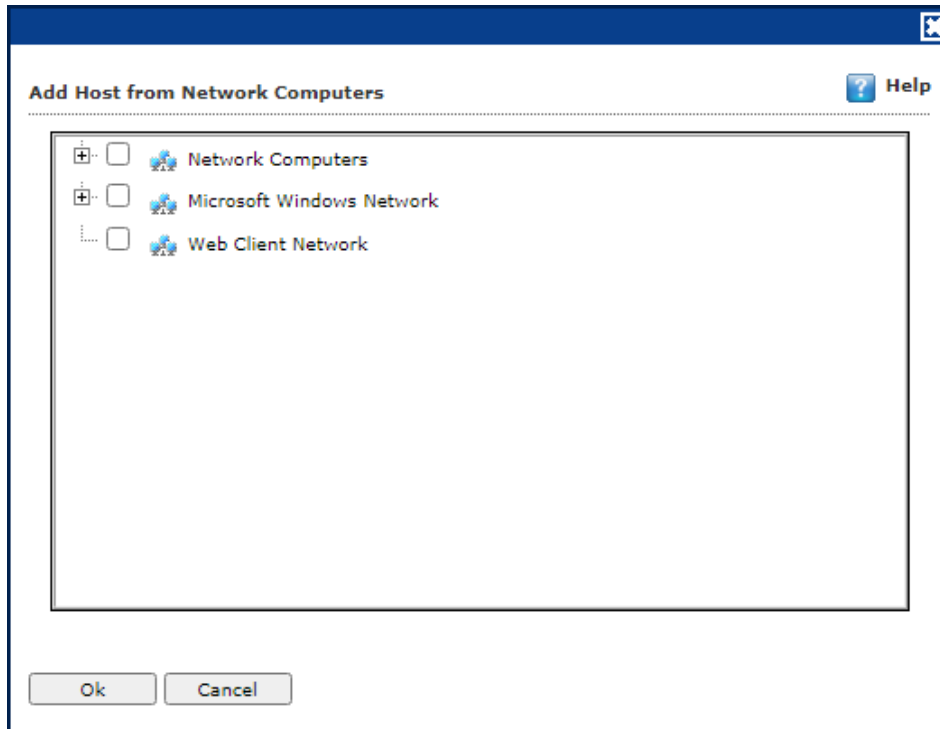


5. Enter the **Start** and **End IP Address**.
6. Click **Ok**.  
The computers will be added in the group.

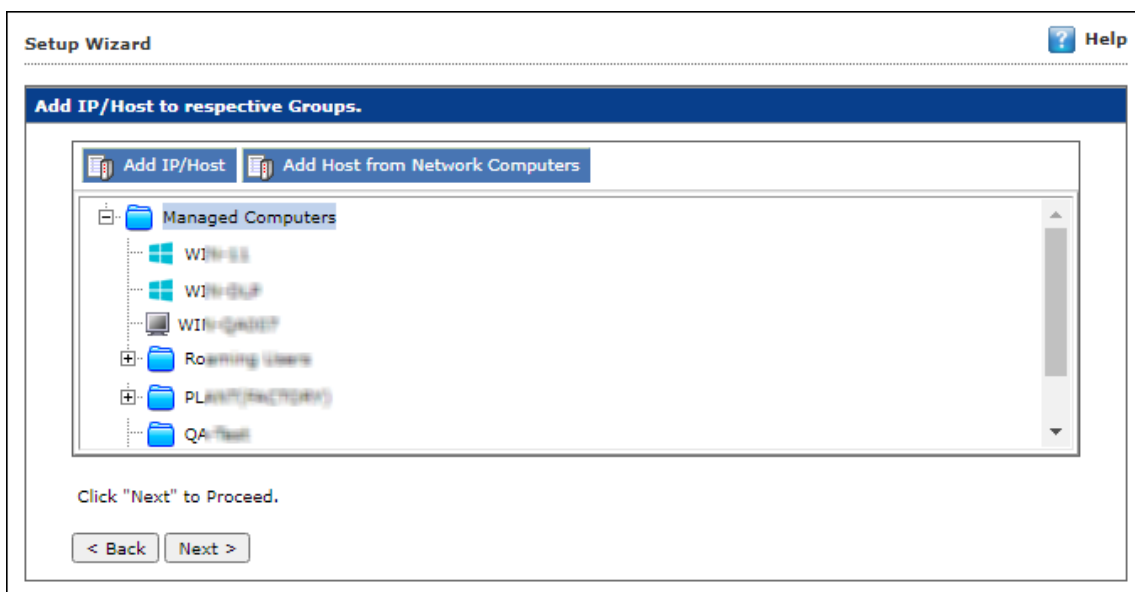
## Adding Host Name from Network Computers

To add the computers from network, follow the below steps:

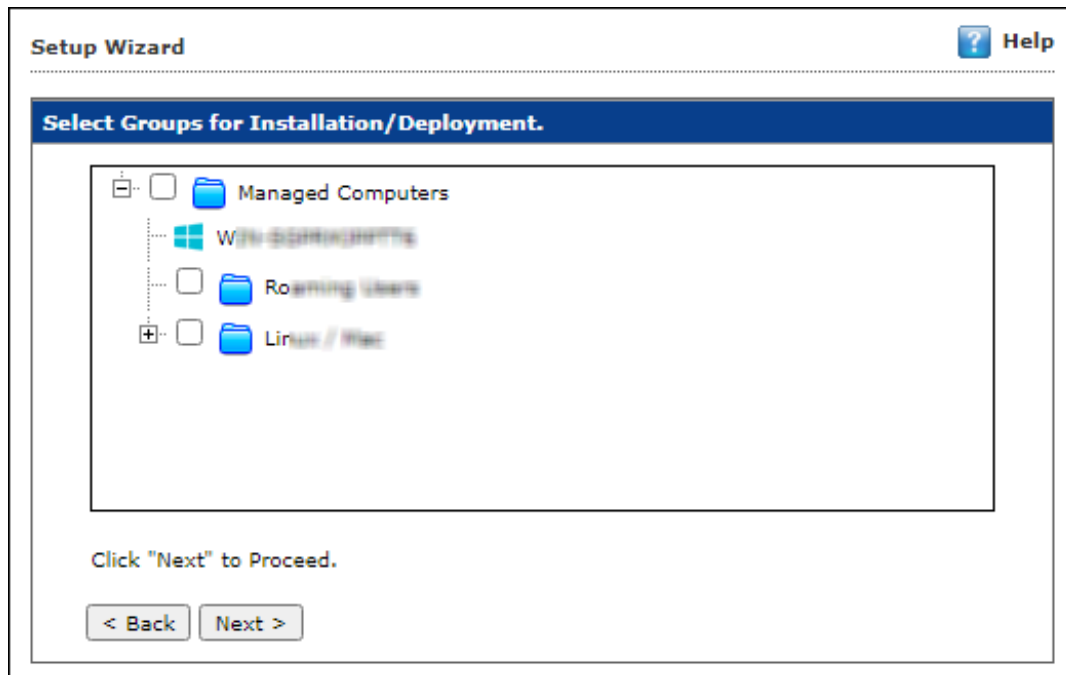
1. Select the group and click **Add Host from Network Computers**.  
Add Host from Network Computers window appears.



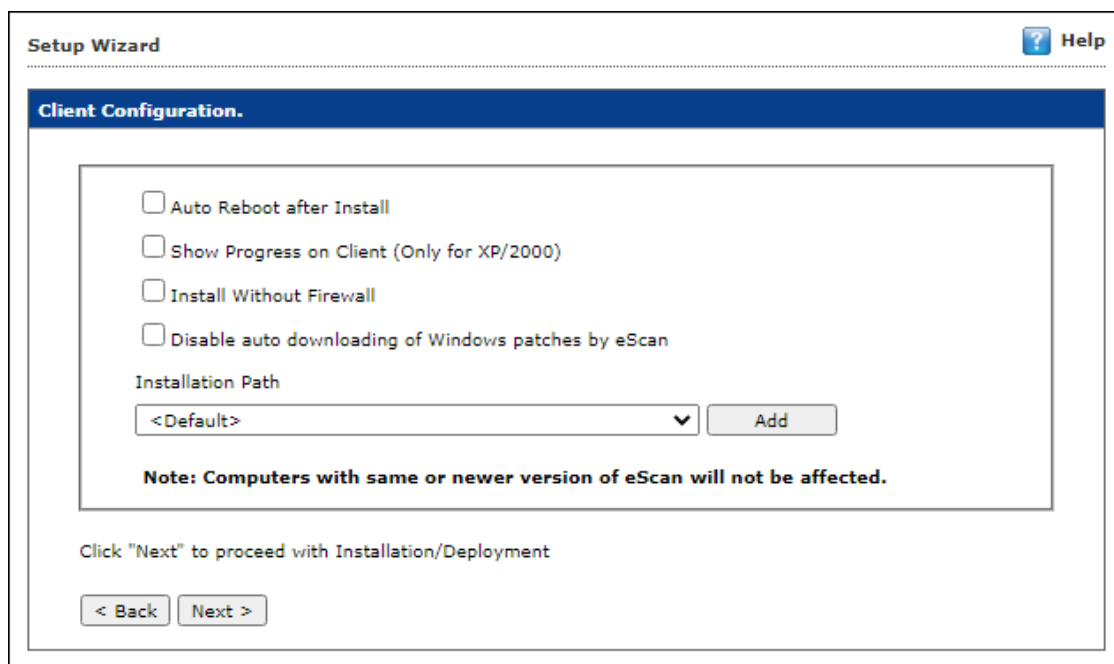
2. Select the network computers and click **Ok**.  
The computers will be added to the group.



3. After adding IP address and Client/Network computer in group, click **Next**.



4. Select the group having client computers then click **Next**.  
Client Configuration window appears.

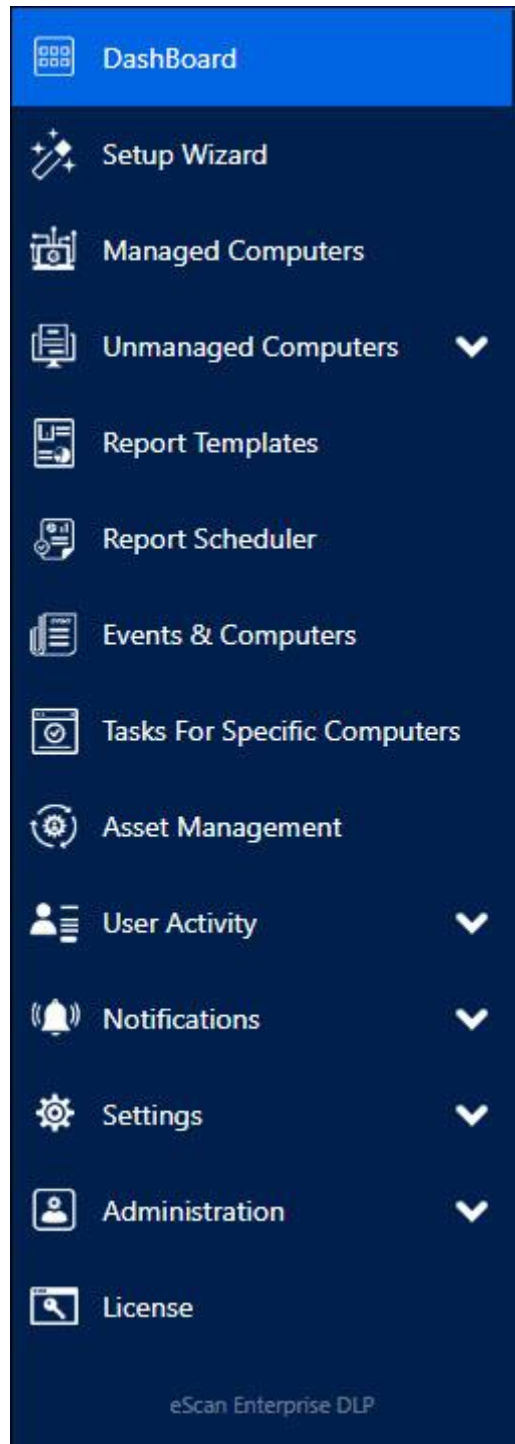


5. To define a different installation path, click **Add**. (Skip this step if default path chosen).
6. Click **Next**.

A window displays File transfer progress.

After Installation, the eScan status will be updated in Managed Computers list.

## Navigation Panel



## Dashboard

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

## Setup Wizard

The Setup Wizard familiarizes you with the basic procedures and setup that is recommended by the eScan. To learn more, [click here](#).

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

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

## Report Templates

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

## Report Scheduler

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

## Events and Computers

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

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

## Asset Management

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



### **User Activity**

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

### **Notifications**

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

### **Settings**

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

### **Administration**

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

### **License**

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

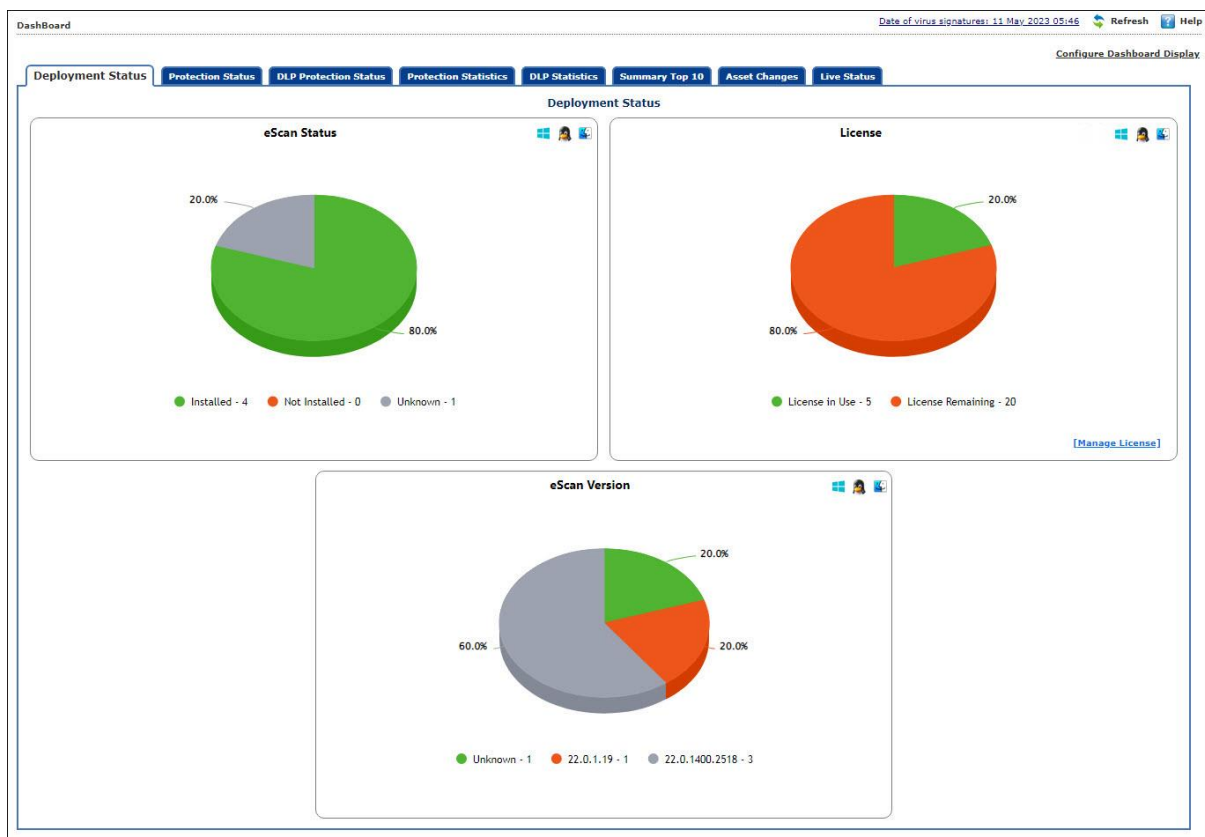
# Dashboard

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

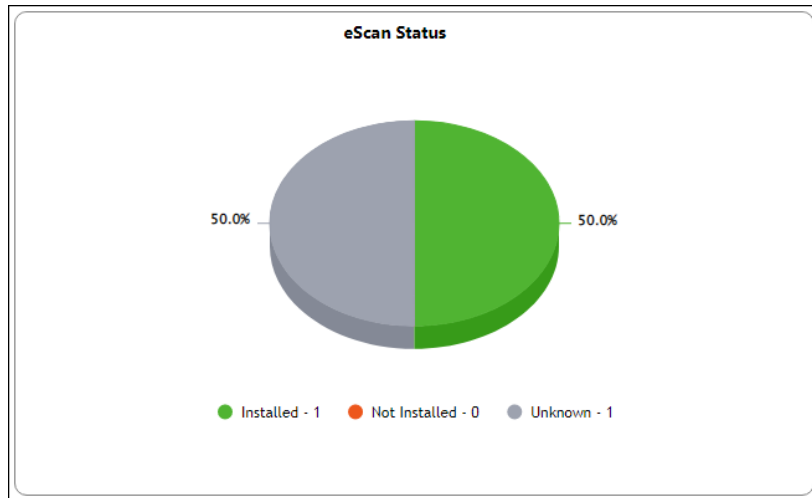
- **Deployment Status**
- **Protection Status**
- **Protection Statistics**
- **Summary Top 10**
- **Asset Changes**
- **Live Status**
- **DLP Protection Status**
- **DLP Statistics**
- **DLP Discovery**

## Deployment Status

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



## eScan Status

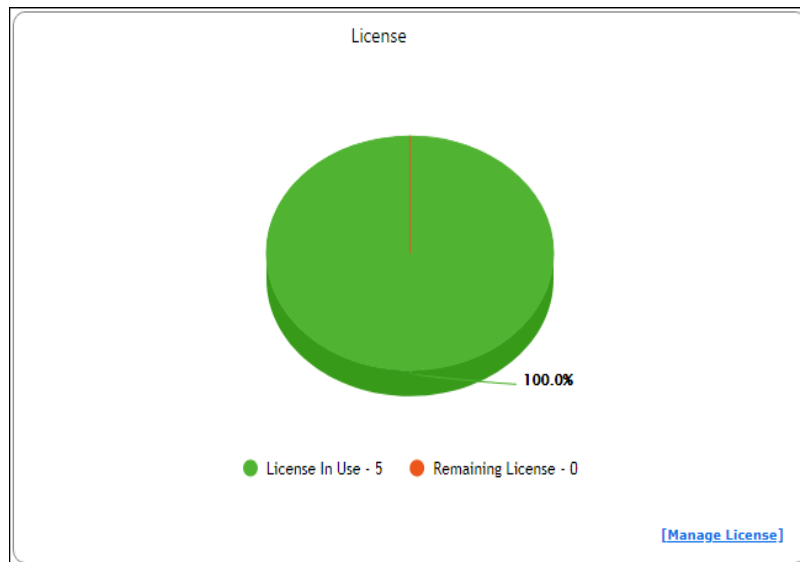


**Installed** – It displays the number of computers on which eScan Client is installed.

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

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

## License

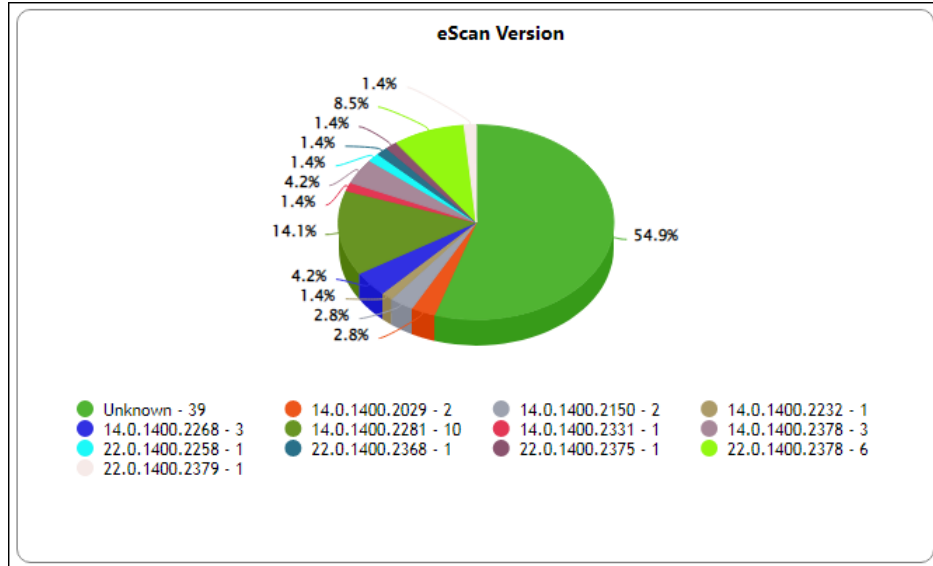


**License in Use** - It displays the number of licenses that are active.

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

## eScan version

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



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

Deployment Status >> eScan Version >> Unknown

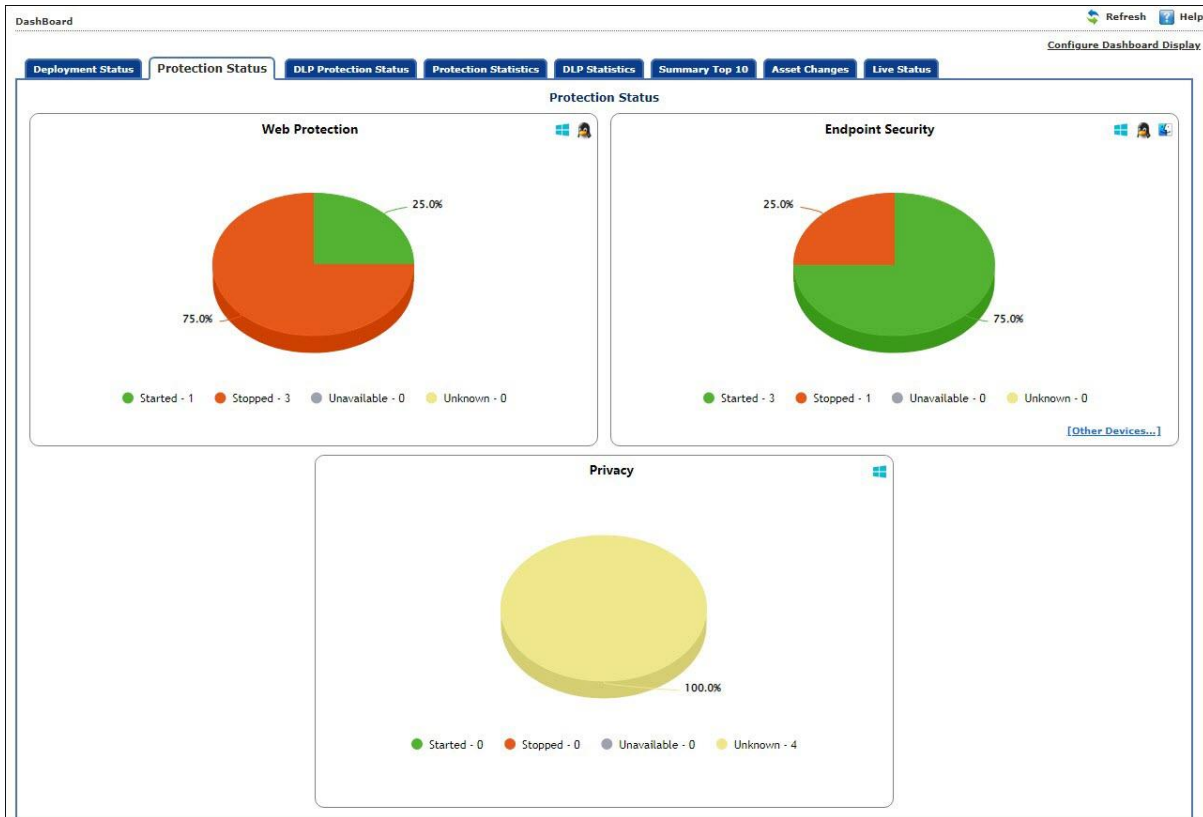
Machine Name	Version	Group
QI-883P2RUCES	<a href="#">Unknown</a>	Managed Computers



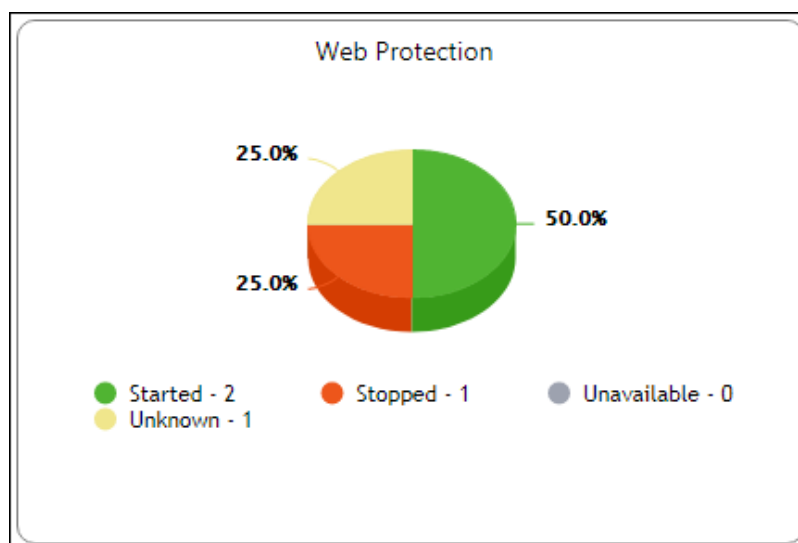
Clicking underlined numerical displays detailed information for computers.

# Protection Status

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



## Web Protection

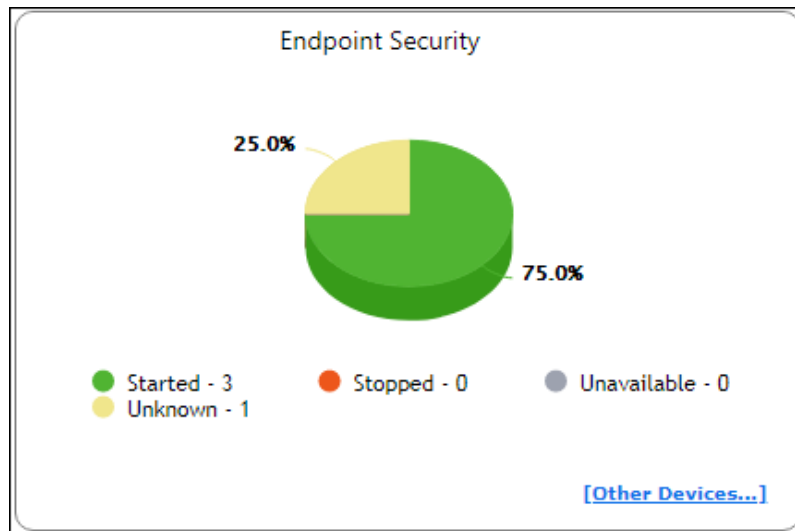


**Started** – It displays the number of computers on which the Web Protection module is in started state.  
**Stopped** – It displays the number of computers on which the Web Protection module is in stopped state.

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

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

## Endpoint Security



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

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

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

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

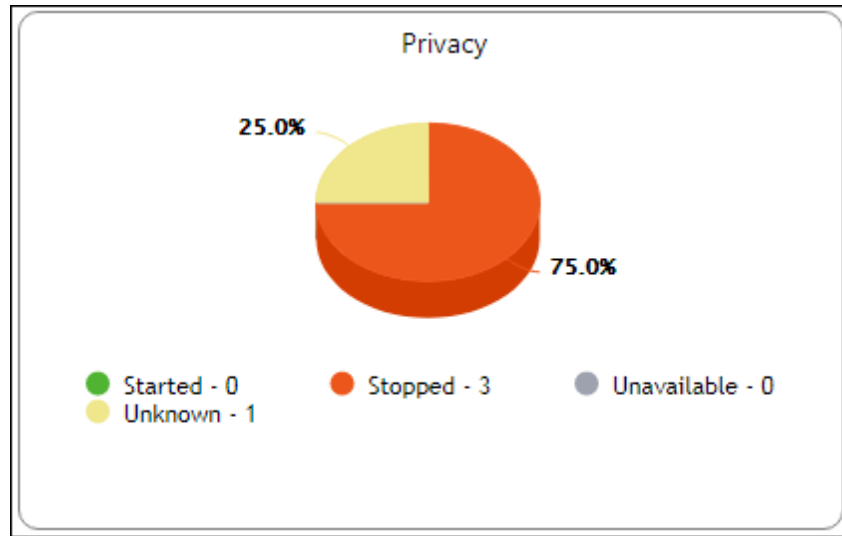
Clicking **Other Devices** displays details about other devices.

The "Other Devices Status" dialog box contains a table with the following data:

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

A "Close" button is located at the bottom center of the dialog box.

## Privacy



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

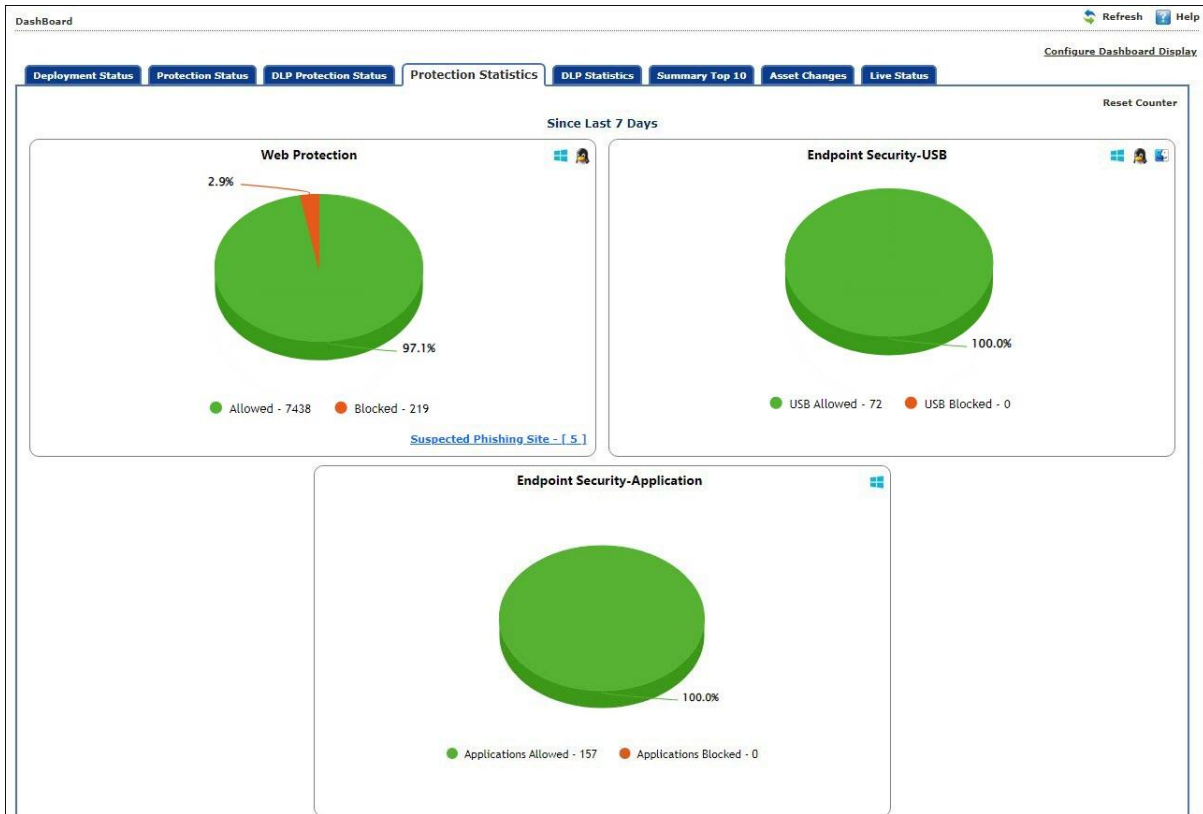
**Stopped** - It displays the number of computers on which the Privacy Control module is in stopped state.

**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.

## Protection Statistics

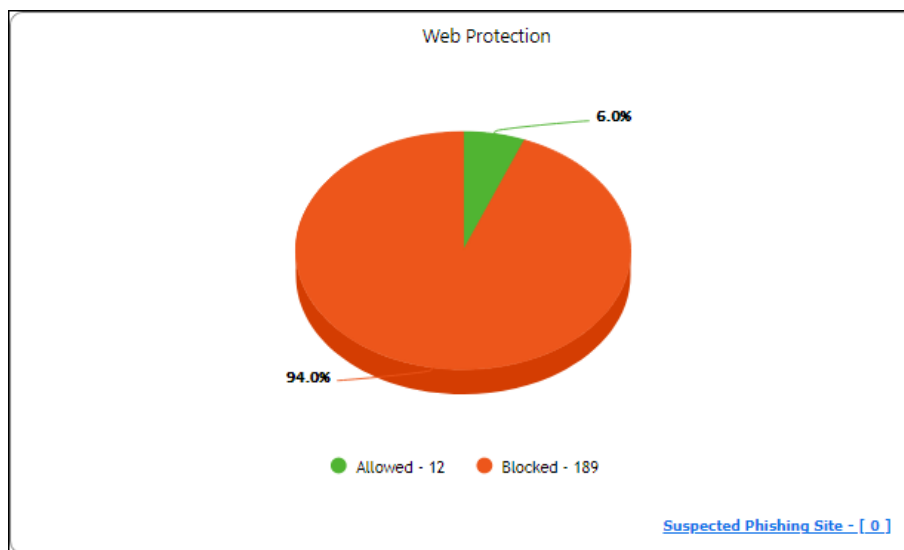
This tab displays activity statistics and action taken by all modules of eScan Client since last seven days in pie chart format.



### Reset Counter

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

## Web Protection





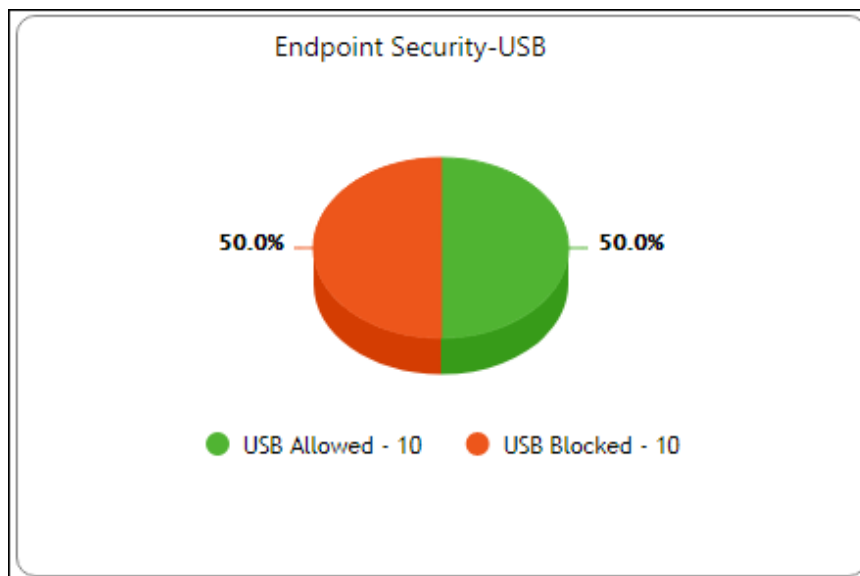
**Allowed** – It displays the number of websites to which access was allowed by Web Protection module.

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

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

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

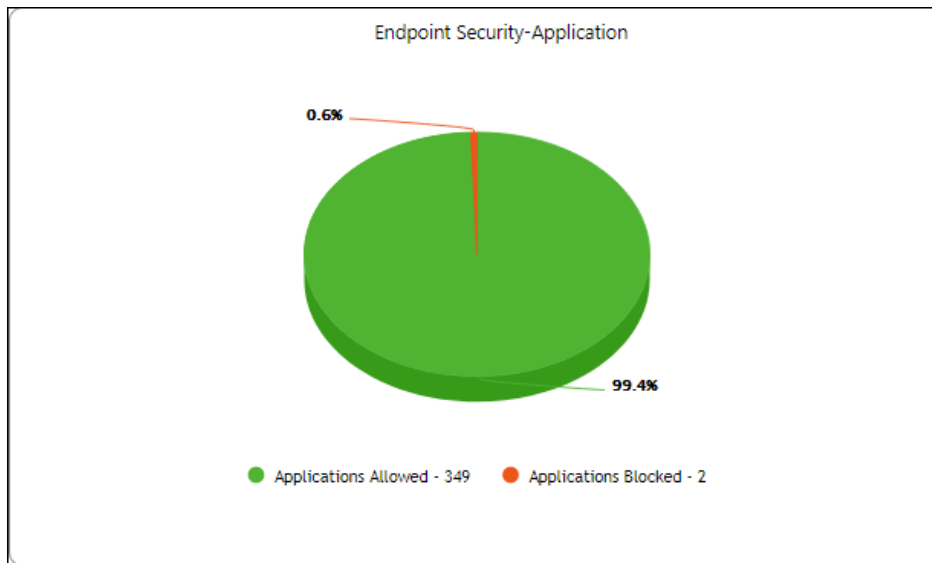
## Endpoint Security-USB



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

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

## Endpoint Security-Application

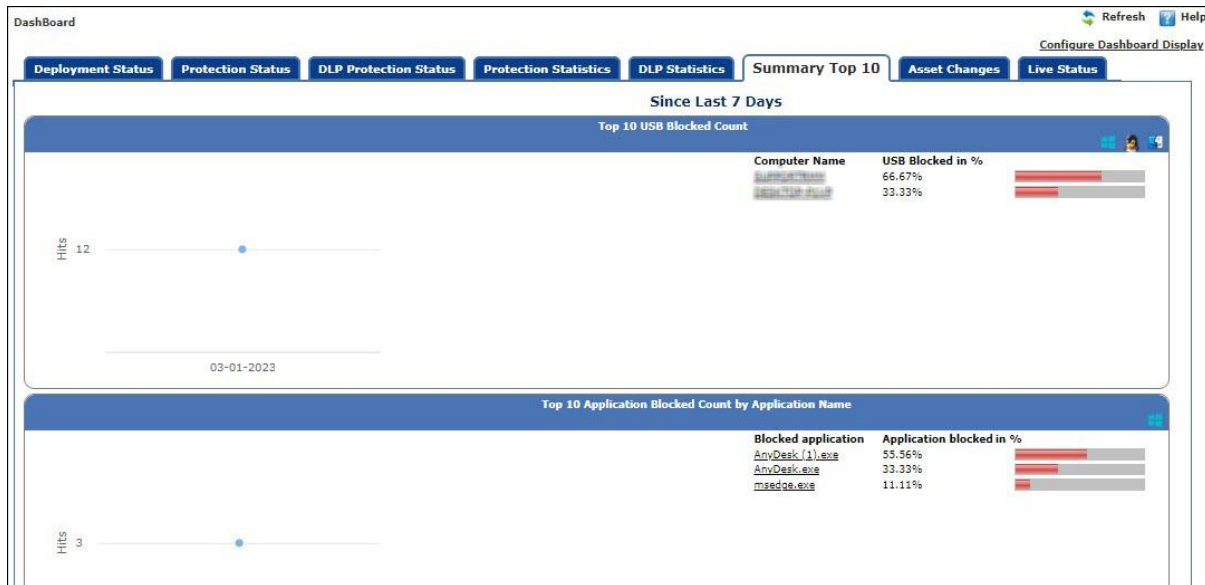


**Applications Allowed** – It displays the number of applications allowed by Endpoint Security-Application module.

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

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

# Asset Changes

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

The screenshot shows the 'Asset Changes' tab in the eScan dashboard. The dashboard has a top navigation bar with tabs: Deployment Status, Protection Status, DLP Protection Status, Protection Statistics, DLP Statistics, Summary Top 10, Asset Changes, and Live Status. The 'Asset Changes' tab is active and displays data for the last 7 days.

**Hardware Changes**

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

**Software Changes**

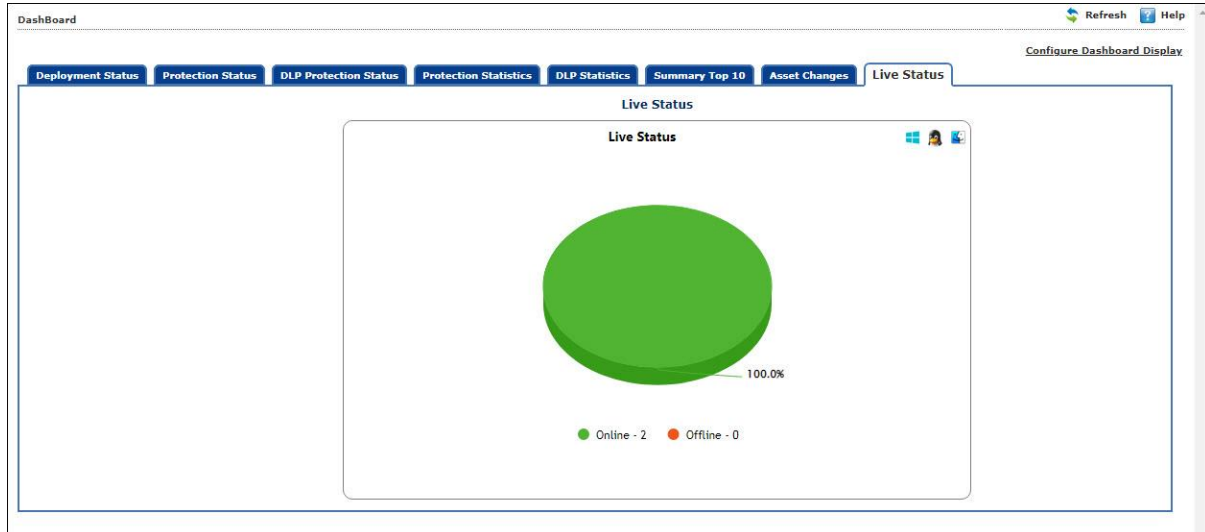
Machine Name	New Installed Softwares	Uninstalled Softwares
<u>WIN-SCANDIUM</u>	1	0
<u>WIN-SCANDIUM</u>	2	1

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

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

## Live Status

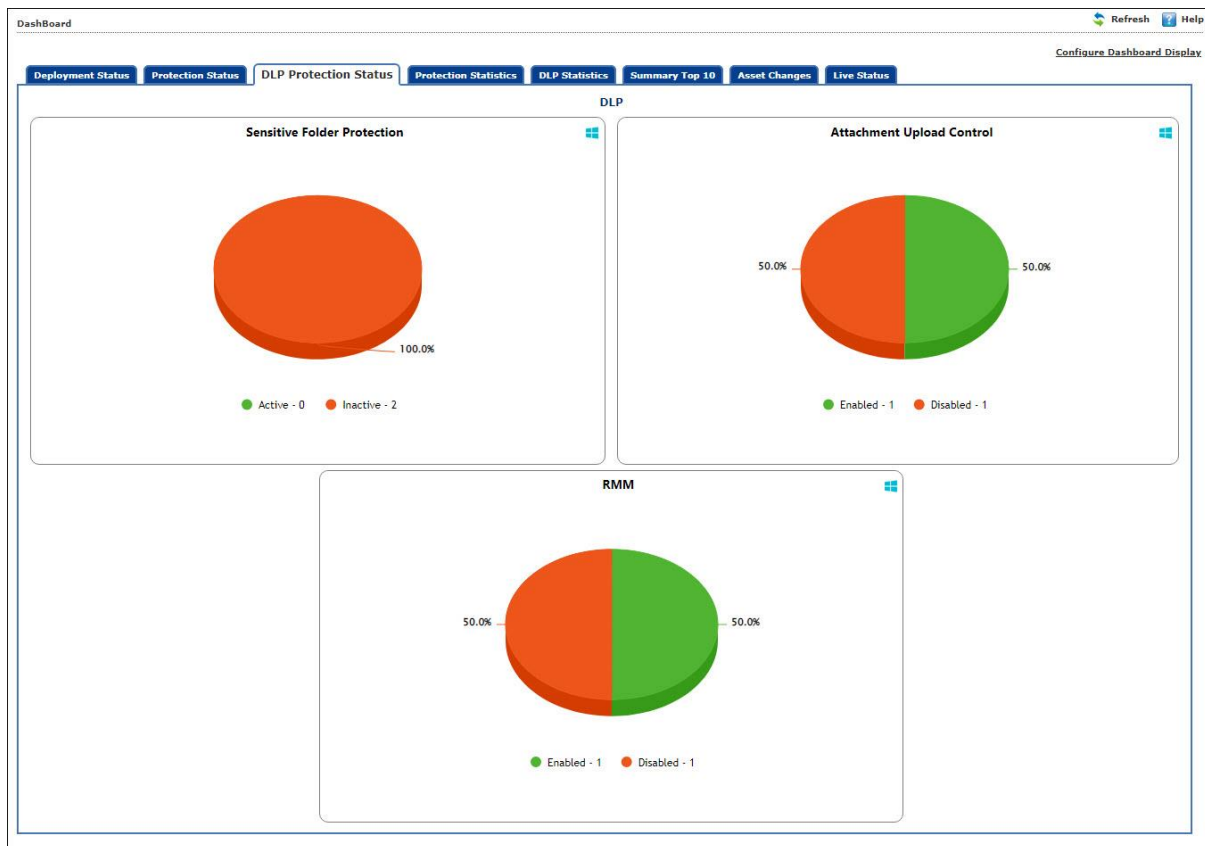
This tab displays the number of computers that are online and offline in a network.



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

# DLP Protection Status

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

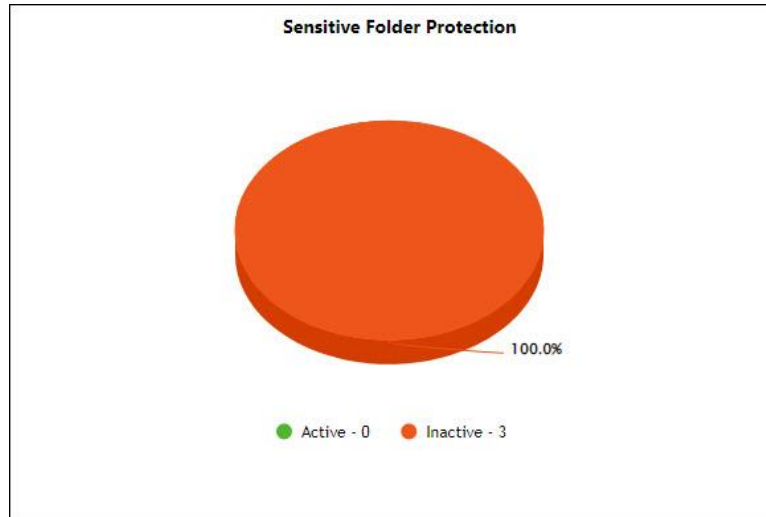


The DLP Protection Status tab contains the status information of the following modules:

- Sensitive Folder Protection
- Attachment Upload Control
- Device Encryption
- RMM

## Sensitive Folder Protection

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



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



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

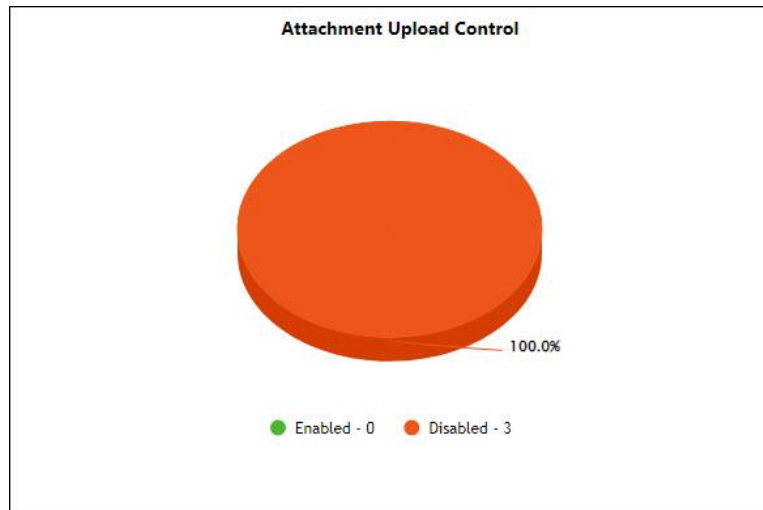
After clicking on the displayed number, a window opens as shown below, displaying the computer details of the module:

Machine Name	IP Address	Group
VIRALINK	192.168.0.222	Managed Computers
WIN-GEQV8E82830M	192.168.0.117	Managed Computers/DLP
VICTORU	192.168.0.104	Managed Computers/Linux / Mac
ESCAN-WP-LAPTOP-12-482011	192.168.0.112, 192.168.0.24	Managed Computers/Linux / Mac

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

## Attachment Upload Control

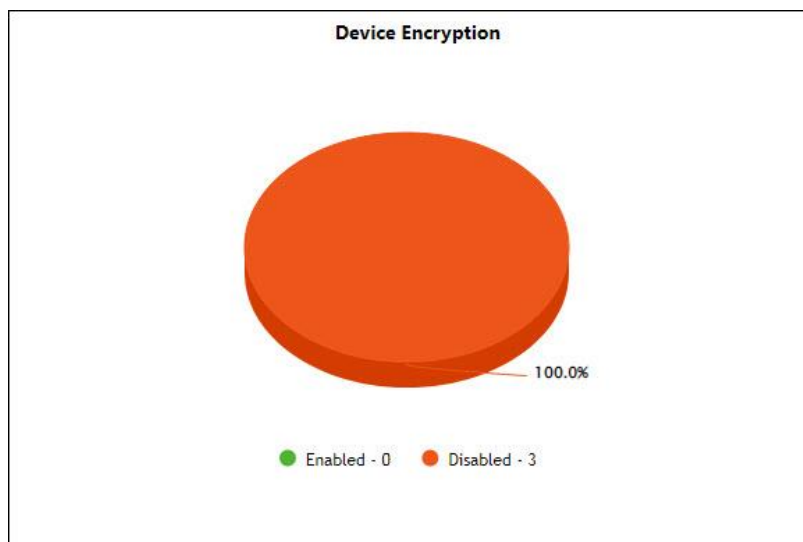
This chart displays the protection status of Attachment Upload Control module:



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

## Device Encryption

This chart displays the protection status of Device Encryption module:



- **Enabled:** It shows the number of computers on which the Device Encryption is turned on.
- **Disabled:** It shows the number of computers on which the Device Encryption is turned off.

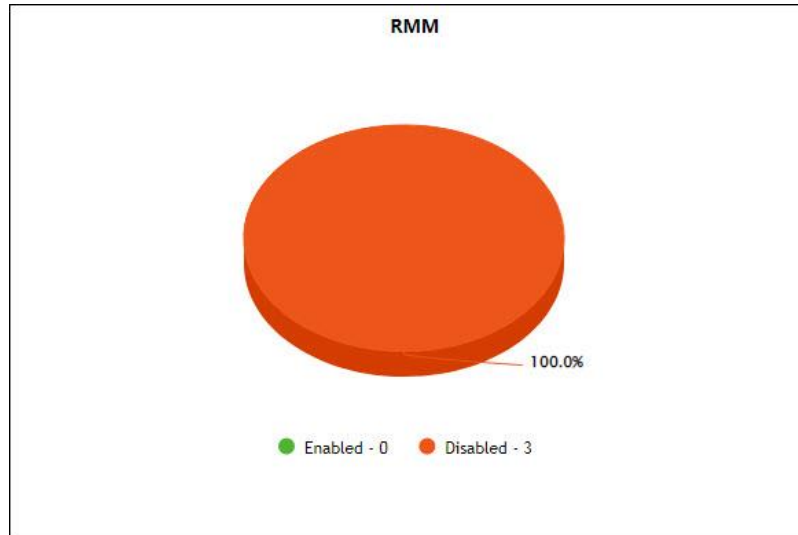
**NOTE**

Device Encryption is an Add-On feature and will be available after purchasing its Add-On license.



## RMM

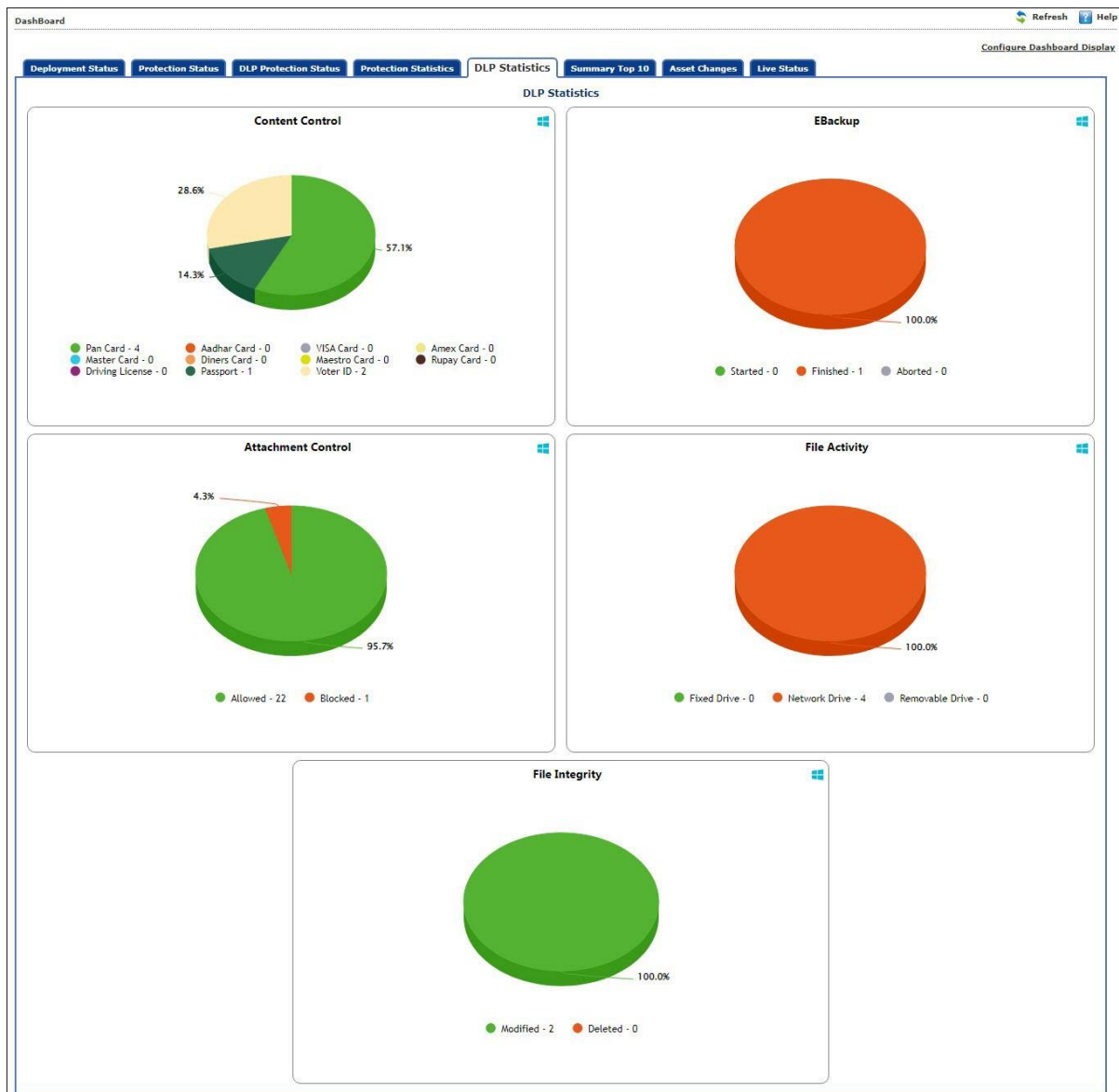
This chart displays the protection status of RMM (Remote Monitoring & Management) module:



- **Enabled:** It shows the number of computers on which the RMM feature is turned on.
- **Disabled:** It shows the number of computers on which the RMM feature is turned off.

## DLP Statistics

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

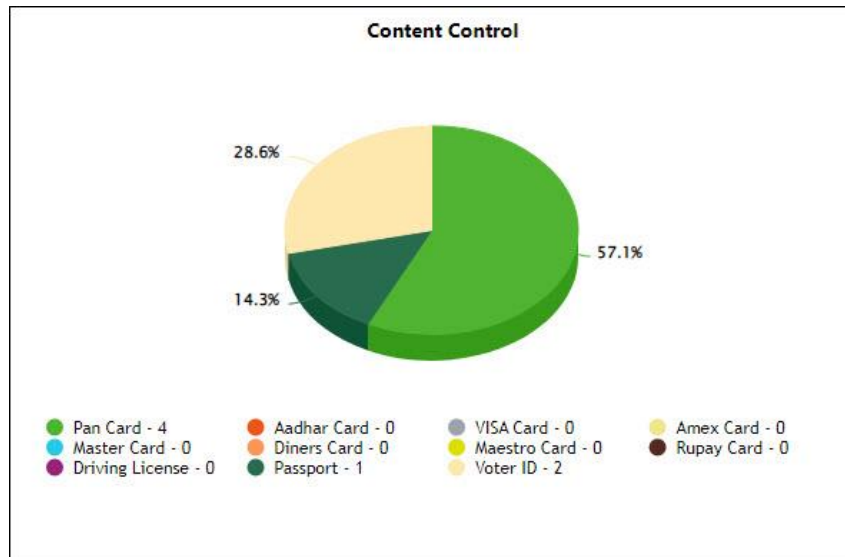


The DLP Statistics tab contains the statistical information of the following modules:

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

## Content Control

This chart displays the protection statistics of Content Control module:



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

**NOTE**

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

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

Machine Name	Drive Count	IP Address	Group
WIN-QRQV5UEZ-OCW	4	192.168.0.117	Managed Computers/DLP

Click on the **Drive Count** to view the uploaded document details.

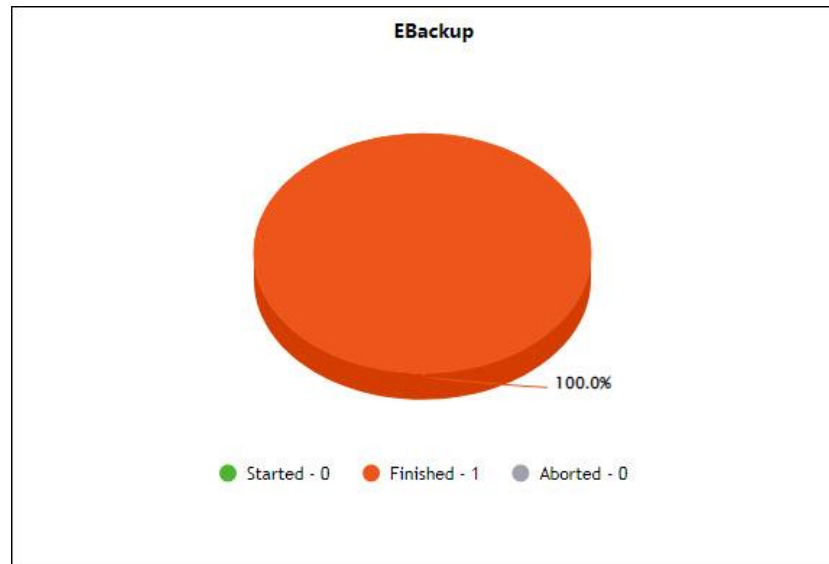
Another window opens as shown below displaying the computer name and the path from where the user attempted to upload/leak the confidential file.

Machine Name	File Upload
WIN-QRQV5UEZ-OCW	C:\Users\user\...
WIN-QRQV5UEZ-OCW	C:\Users\user\...
WIN-QRQV5UEZ-OCW	C:\Users\user\...
WIN-QRQV5UEZ-OCW	C:\Users\user\...

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

## EBackup

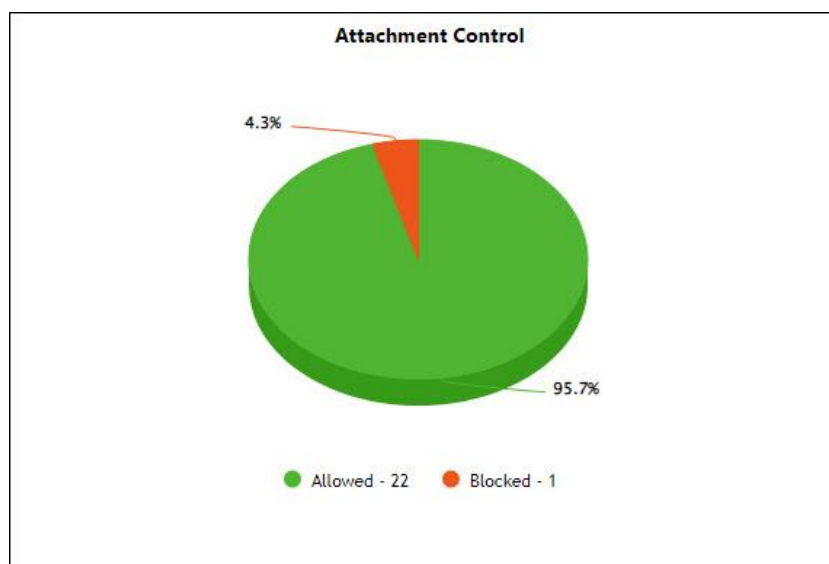
This chart displays the protection statistics of EBackup module:



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

## Attachment Control

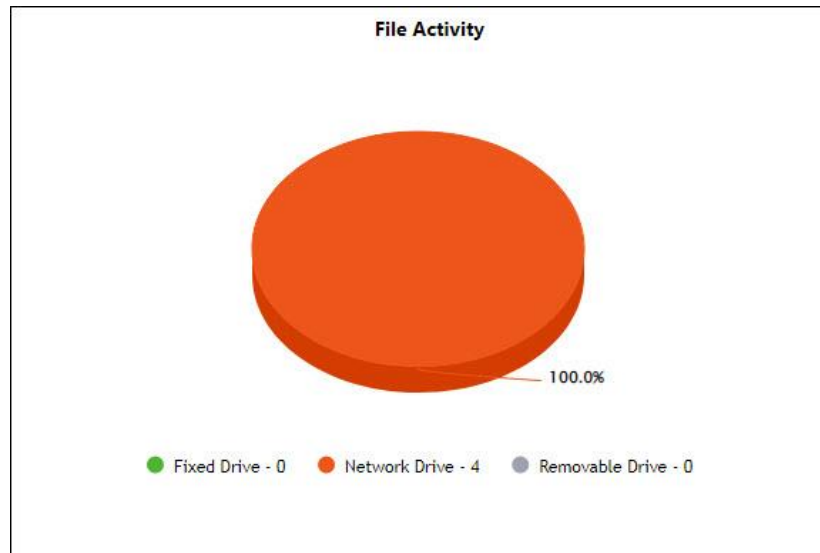
This chart displays the protection statistics of Attachment Control module:



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

## File Activity

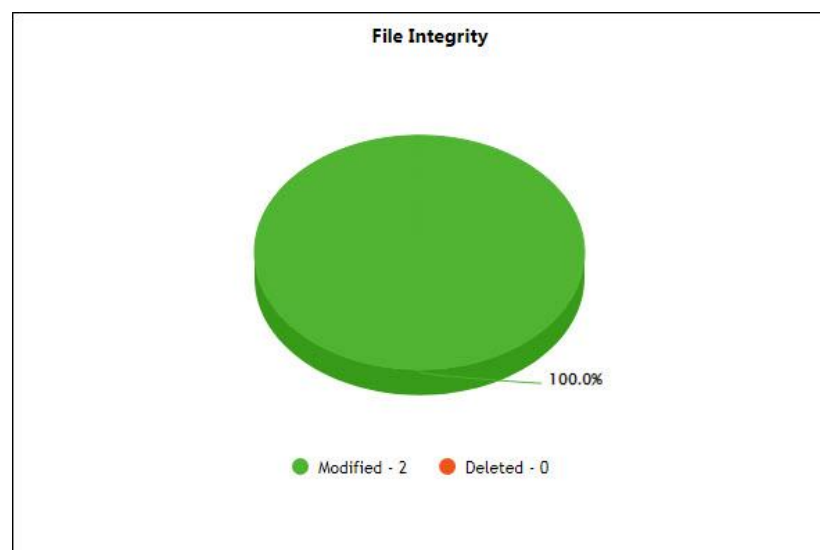
This chart displays the protection statistics of File Activity module:



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

## File Integrity

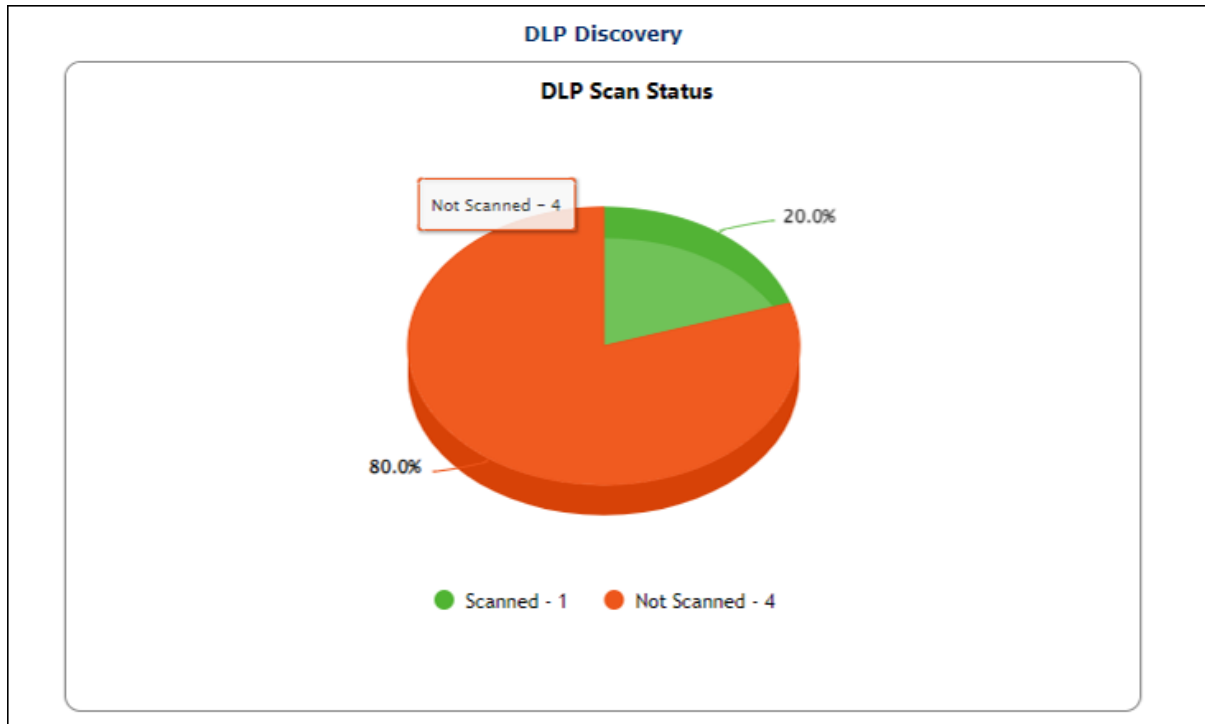
This chart displays the protection statistics of File Integrity module:



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

## DLP Discovery

This tab displays DLP scan status for sensitive data on all the managed computers with eScan client installed.

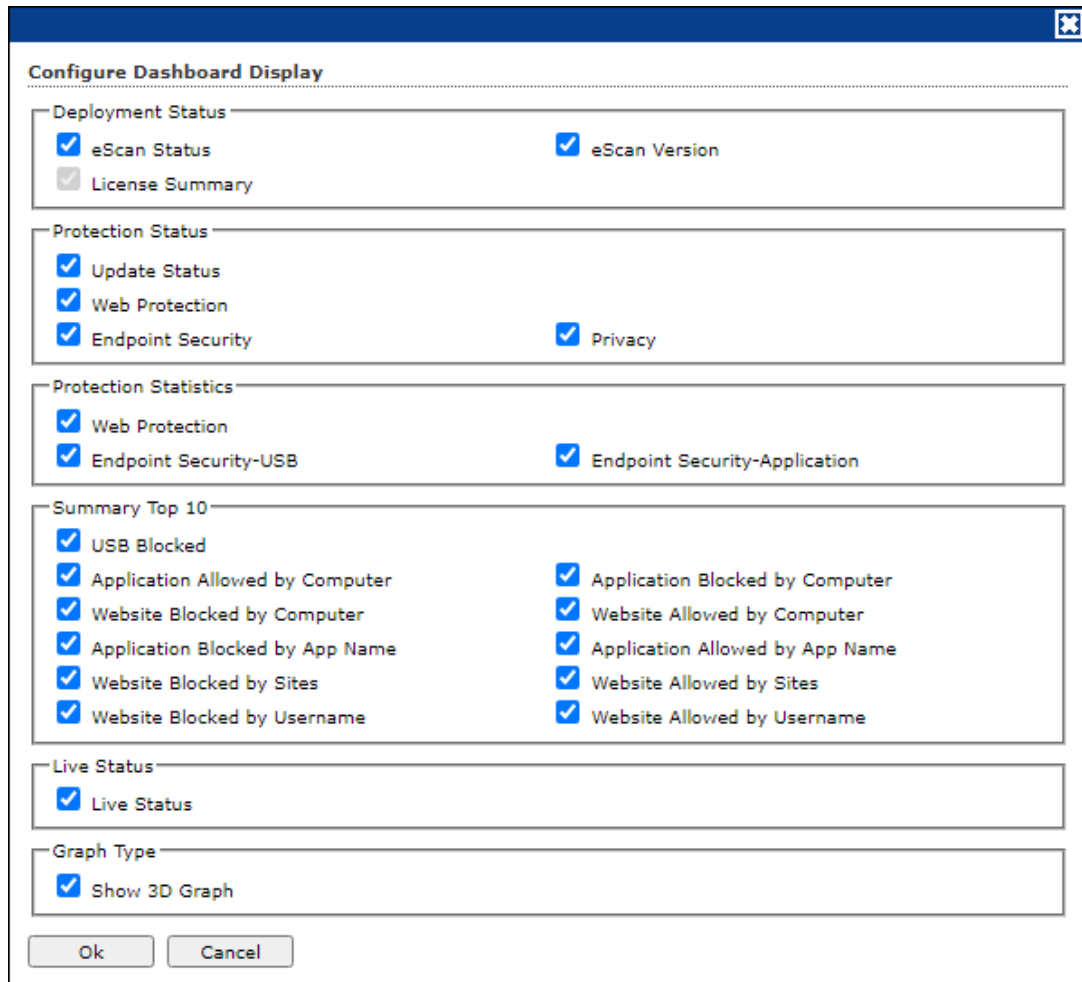


- **Scanned:** It shows the number of managed endpoints scanned for the files with sensitive data.
- **Not Scanned:** It shows the number of endpoints not yet scanned.

# Configure the Dashboard Display

To configure the Dashboard display:

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



**Configure Dashboard Display**

Deployment Status

- eScan Status
- License Summary
- eScan Version

Protection Status

- Update Status
- Web Protection
- Endpoint Security
- Privacy

Protection Statistics

- Web Protection
- Endpoint Security-USB
- Endpoint Security-Application

Summary Top 10

- USB Blocked
- Application Allowed by Computer
- Website Blocked by Computer
- Application Blocked by Computer
- Application Blocked by App Name
- Website Allowed by Computer
- Website Blocked by Sites
- Application Allowed by App Name
- Website Allowed by Sites
- Website Blocked by Username
- Website Allowed by Username

Live Status

- Live Status

Graph Type

- Show 3D Graph

Ok Cancel

2. Select the parameters checkboxes to be displayed in the respective tabs.
3. Select the **Live Status** checkbox to display the live status managed computers on dashboard.
4. Graph Type: select **Shows 3D Graph** checkbox to display 3D graph on dashboard.
5. Click **OK**.

The tabs will be updated according to the changes.

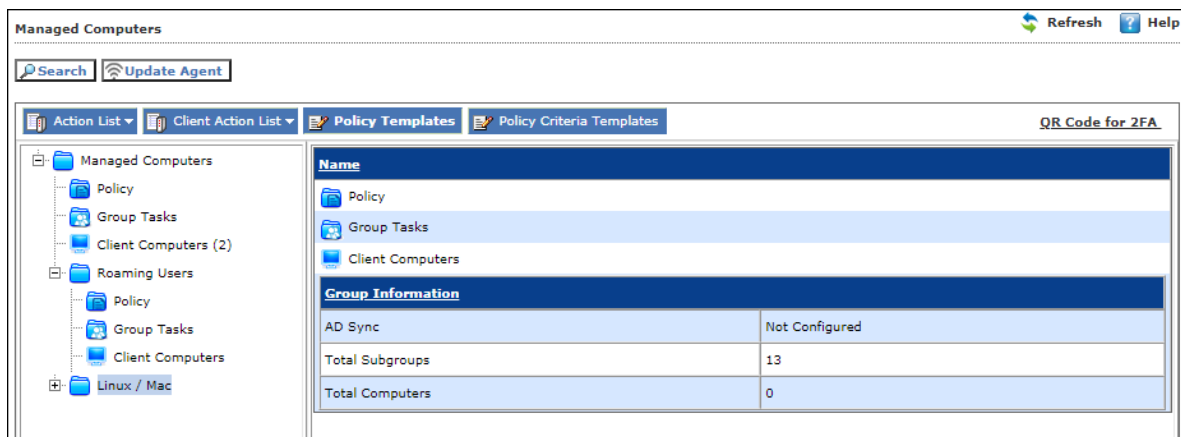


# Managed Computers

To secure, manage, and monitor computers, it is necessary to add them in a group. The Managed Computers module lets you create computer groups, add computers to group, define policy templates for created groups and computers, 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 screenshot shows the 'Managed Computers' interface. At the top, there are 'Search' and 'Update Agent' buttons. Below that, there are tabs for 'Action List', 'Client Action List', 'Policy Templates', and 'Policy Criteria Templates'. A 'QR Code for 2FA' link is also visible. The left sidebar shows a navigation tree with 'Managed Computers' selected. The main content area displays a table with the following data:

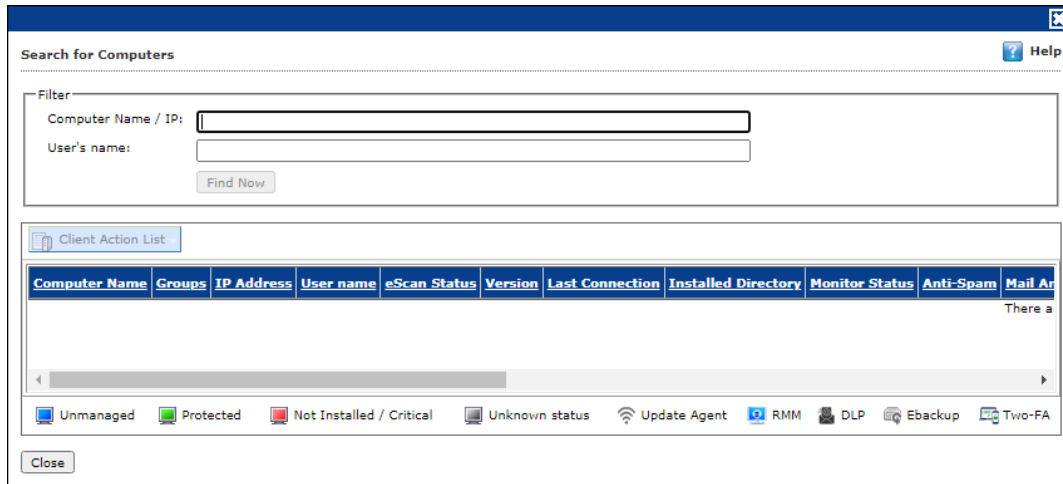
Group Information	
AD Sync	Not Configured
Total Subgroups	13
Total Computers	0

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.



### Computer Name/IP

Enter a computer name or IP address.

### Username

Enter a username.

Click **Find Now**.

The console will display the result.

### Client Action List

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

## Update Agent

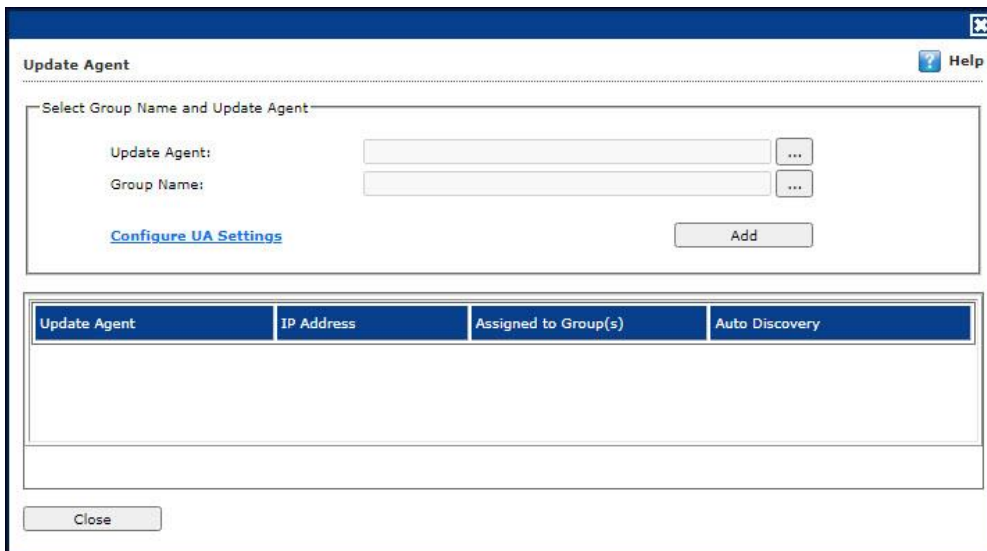
eScan lets you use a client computer as an update agent to deploy updates on group of computers. By default, eScan server distributes the virus definitions and policies to all the clients added in the web console. But, to reduce server's workload, you can create an Update Agent for the respective group(s).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


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

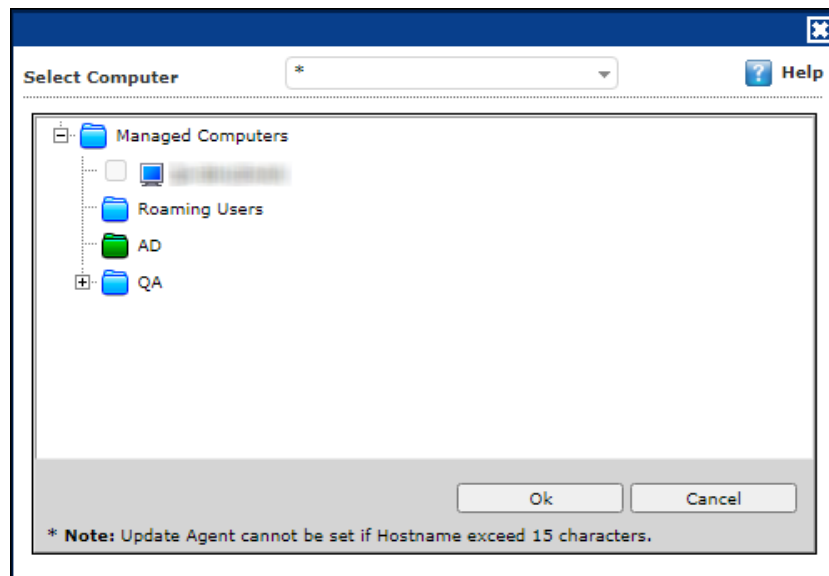
## Adding an Update Agent

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

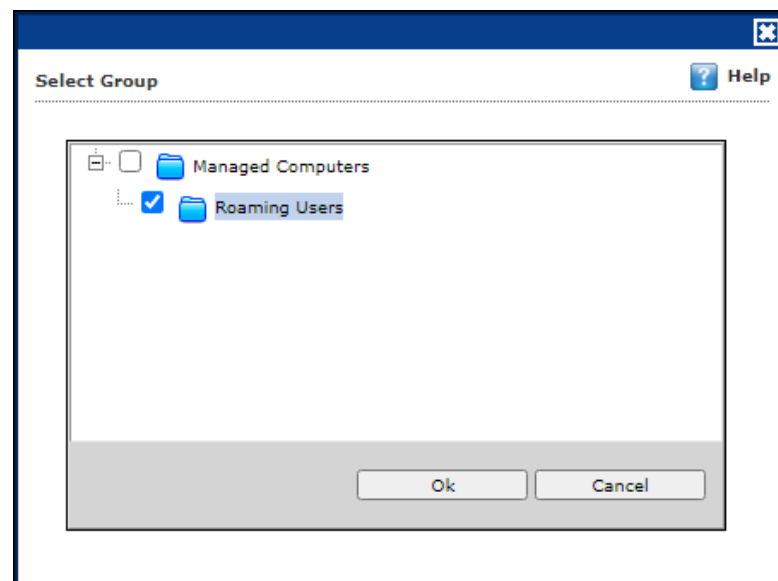
1. In Managed computers screen, click **Update Agent**.  
Update Agent window appears.



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



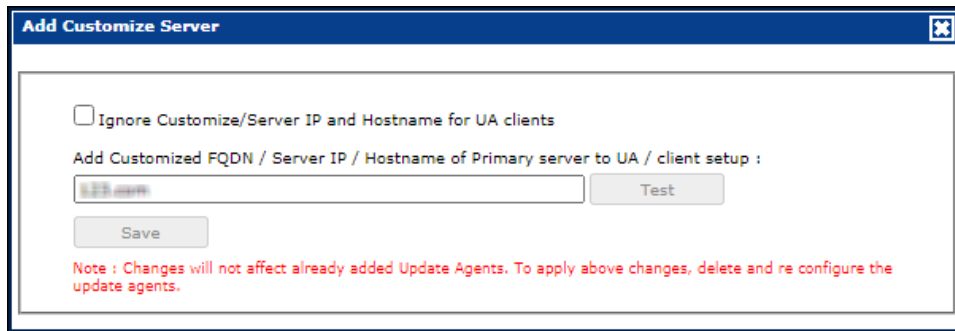
3. Select a computer and click **OK**.
4. Click  next to Group Name field, to select the Group Name.  
The computer will act as an Update Agent for selected group and provide updates to computers present in the group.



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

## Configuring UA Settings

This option allows admin to configure the eScan Server by defining public IP address for directly downloading the updates in case of Update Agent is not available.



### Ignore Customize/Server IP and Hostname for UA clients

Select this option to pause the update download for the clients until Update Agent is available to distribute the updates.

### Add Customized FQDN / Server IP / Hostname of Primary server to UA / client setup

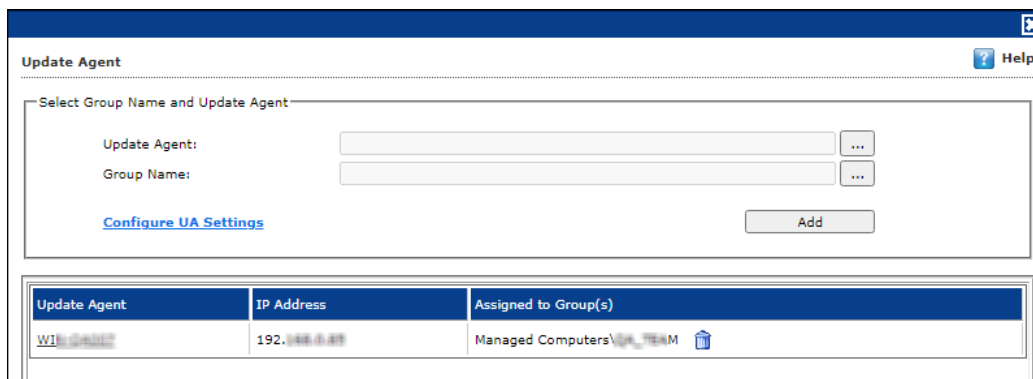
Enter the public address that has been assigned to the eScan Server through which clients can download the updates directly.

After assigning the IP address, click **Test** to test the connection.

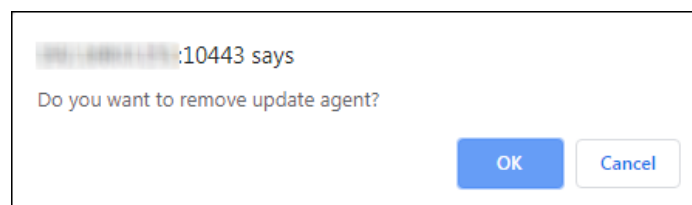
## Delete an Update Agent

To delete an Update Agent:

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




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



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

## Action List

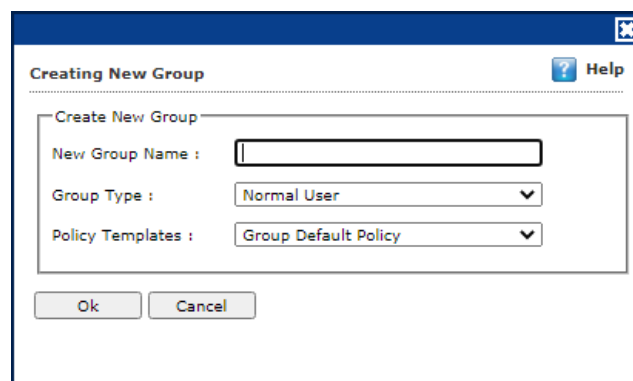
The Action List takes you action for a group. The drop-down contains following options:

- **New Subgroup**
- **Set Group Configuration**
- **Deploy/Upgrade Client**
- **Uninstall eScan Client**
- **Remove Group**
- **Synchronize with Active Directory**
- **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.

### NOTE

If the Group type is set to **Normal User**, then server will try to connect to the client computer using the hostname.

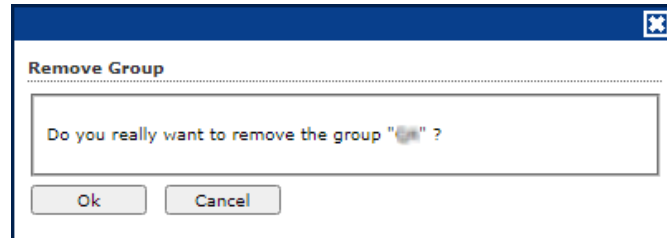
If the Group type is set to **Roaming User**, then server will try to connect to the client computer using the IP address.

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 Group**.  
A confirmation prompt appears.



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



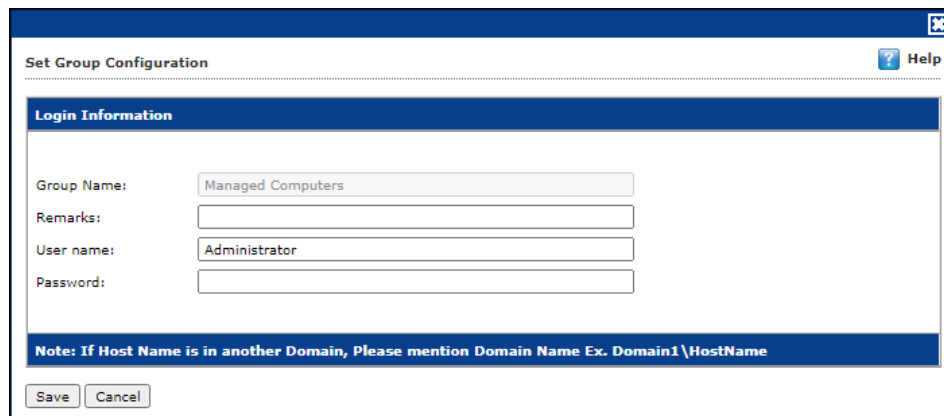
A group will be removed only if it contains no computers.

## 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.



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



Please specify the Domain name, if hostname is in another Domain.

## 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 force download process on selected Client computers.

 <b>NOTE</b>	<p>Conditions for third party software installation:</p> <ul style="list-style-type: none"><li>• After starting the installation from eScan Management Console, no manual intervention should be required to complete the installation on Client computer.</li><li>• Only automated installations can be done through eScan Management Console.</li><li>• Care should be taken that the installation file is not huge as it may impact internal network speed of your organization.</li></ul>
--	---

## Remote Installation of eScan Client

### Pre-Installation

To prepare a client computer for the remote deployment of eScan Enterprise DLP; 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 / Windows 11



## 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 **Local Security Policy** 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 / Windows 11

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:

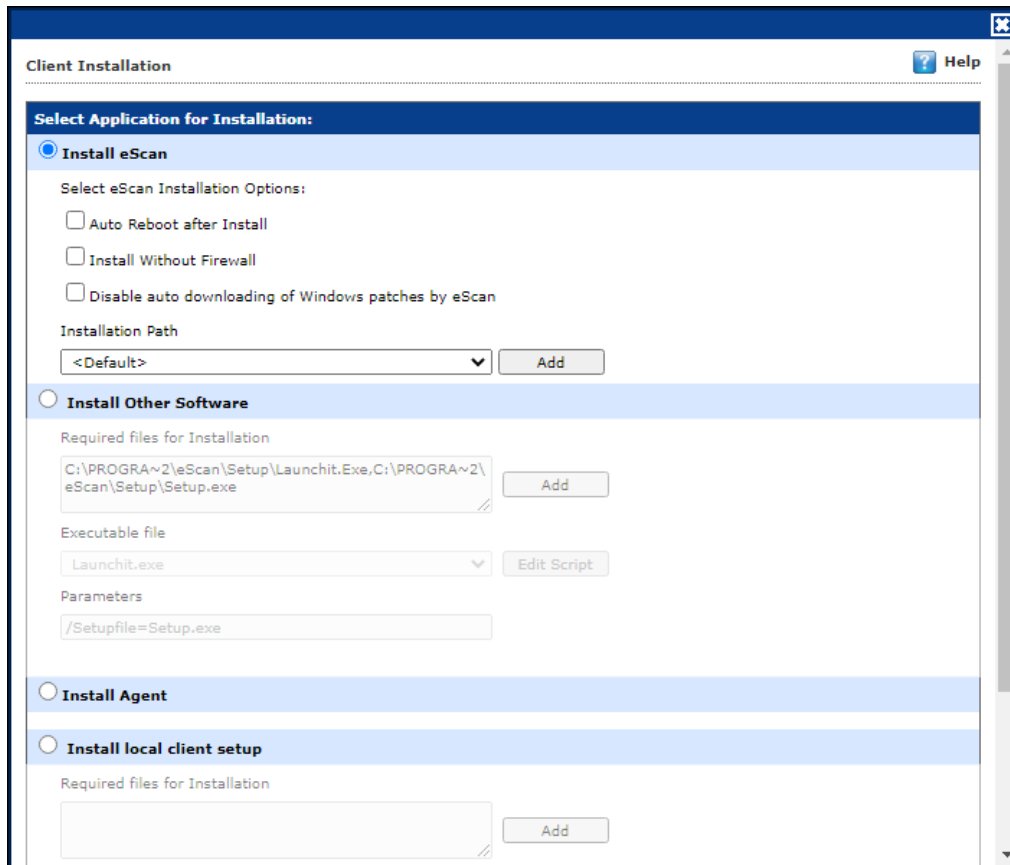
### Installing eScan Client on a Group

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

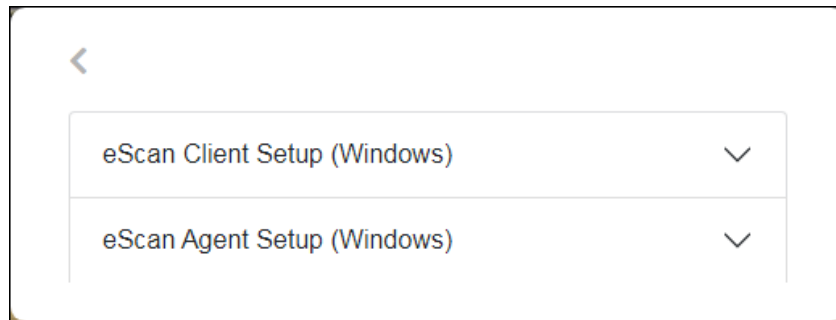
1. Select a group.
2. Under the group, click **Client Computers**.
3. Select a computer.
4. Click **Client Action List > Deploy/Upgrade Client**.  
Client Installation window appears.



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.

## Manual installation of eScan Client on network computer(s)

If remote installation is not possible, you may manually install the eScan Management Console. To install manually, the download links for manually installation of the eScan Client or Agent are displayed on the **Login Page > Setup Links** of eScan Management Console. Forward this link to the user of the client computer on mail and guide the user through the installation process.



## 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)

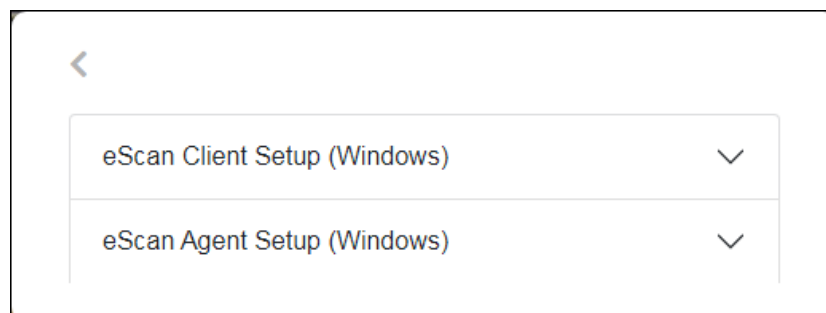
1. Click **Managed Computers**.
2. Select the computer(s) from a group.
3. Click **Client Action List > Deploy/Upgrade Client**.
4. Select **Install Agent** option and click **Install**.  
eScan Agent will be installed on selected computers.



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)

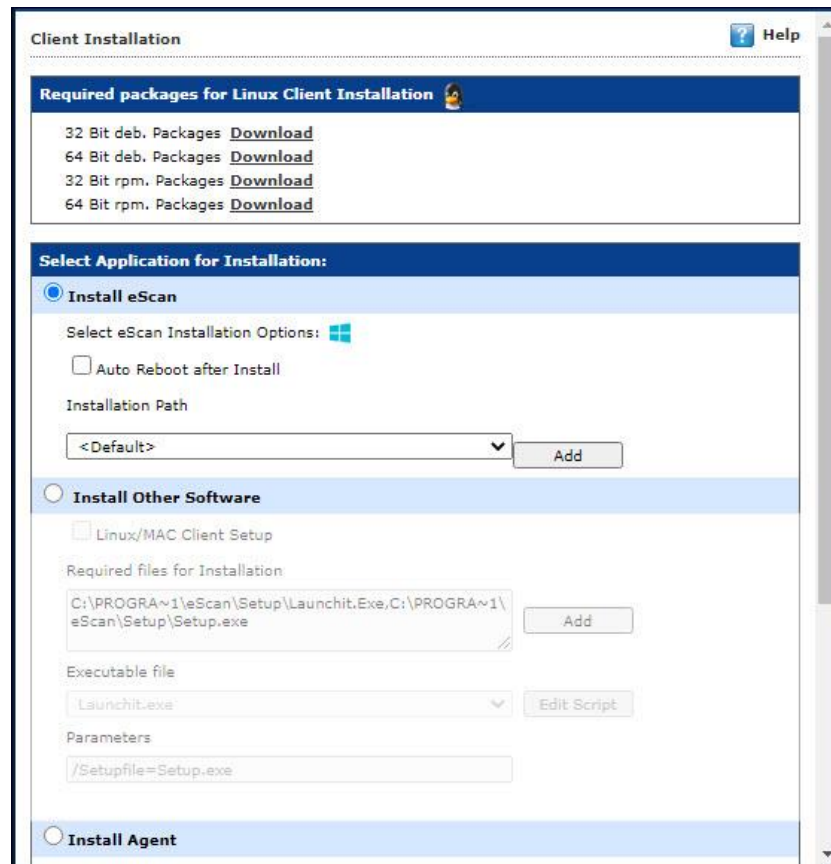
To manually install eScan Agent on computers, please send the link displayed on the **Login Page > Setup Links** of eScan Management Console to the users of the Client computer on mail.



## Installing other Software (Third Party Software)

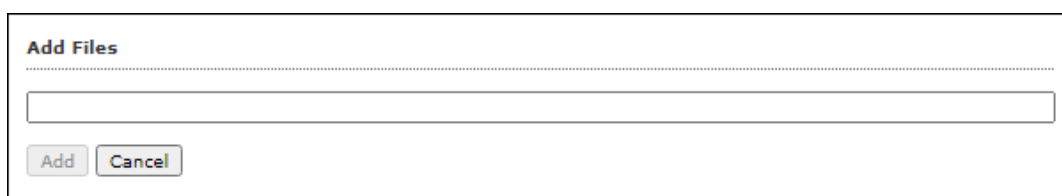
To install third party software on computers, follow the steps given below:

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.



The screenshot shows the 'Client Installation' window. At the top, there is a 'Help' icon. Below it, a section titled 'Required packages for Linux Client Installation' lists four items: '32 Bit deb, Packages', '64 Bit deb, Packages', '32 Bit rpm, Packages', and '64 Bit rpm, Packages', each with a 'Download' link. The main section is 'Select Application for Installation:' and has three radio button options: 'Install eScan' (selected), 'Install Other Software', and 'Install Agent'. Under 'Install eScan', there are checkboxes for 'Auto Reboot after Install' and a field for 'Installation Path' with a dropdown menu set to '<Default>' and an 'Add' button. Under 'Install Other Software', there is a checkbox for 'Linux/MAC Client Setup', a section for 'Required files for Installation' with a text input field containing a file path and an 'Add' button, an 'Executable file' dropdown menu set to 'Launchit.exe' with an 'Edit Script' button, and a 'Parameters' text input field containing '/Setupfile=Setup.exe'.

5. Click **Add**.  
Add Files window appears.



The screenshot shows the 'Add Files' dialog box. It has a title bar 'Add Files' and a large empty text input field. Below the input field are two buttons: 'Add' and 'Cancel'.

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.

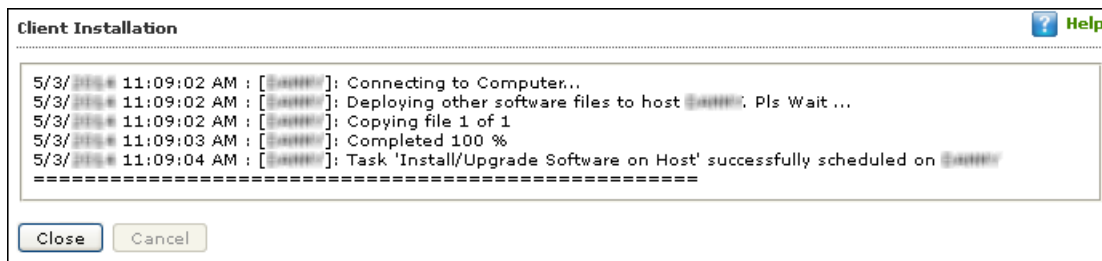
**Install Other Software**

Required files for Installation

Executable file

Parameters

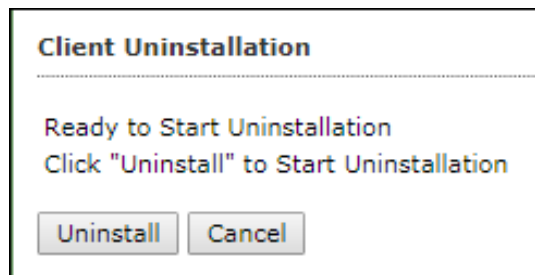
7. The Executable Filename will be displayed in the respective drop-down menu.
8. Define the command line parameters if required.
9. Click **Install** to initiate the installation process.  
A confirmation message appears.



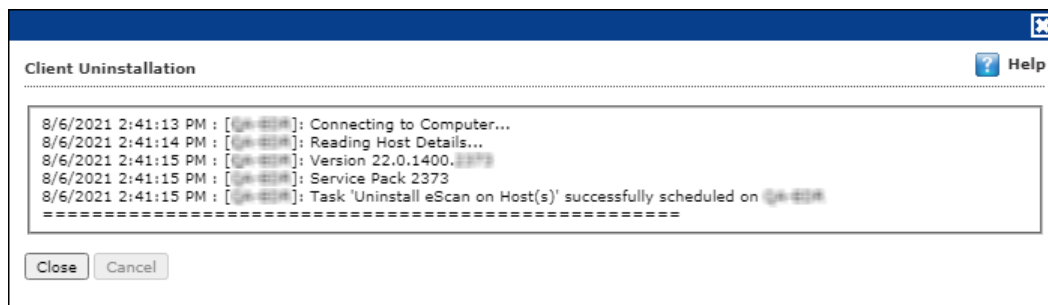
## Uninstall eScan Client (Windows)

To uninstall eScan Client on all the computers in 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**.



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 :  
Managed Computers

Source Active Directory Organisation Unit :

Synchronization interval :  
60 Minutes (Minimum 5 Minutes)

Exclude From ADS Sync

<input type="checkbox"/>	Excluded ADS Sources	<input type="button" value="Add to Exclude"/>
		<input type="button" value="Delete"/>

Search Filter :  
e.g.: (objectClass=\*)

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.

### Target Groups

Click **Browse** and select a Managed Group.

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

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

### Search Filter

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

### Install eScan client automatically

Selecting this option lets you install eScan client automatically on the computers.

### Install without Firewall

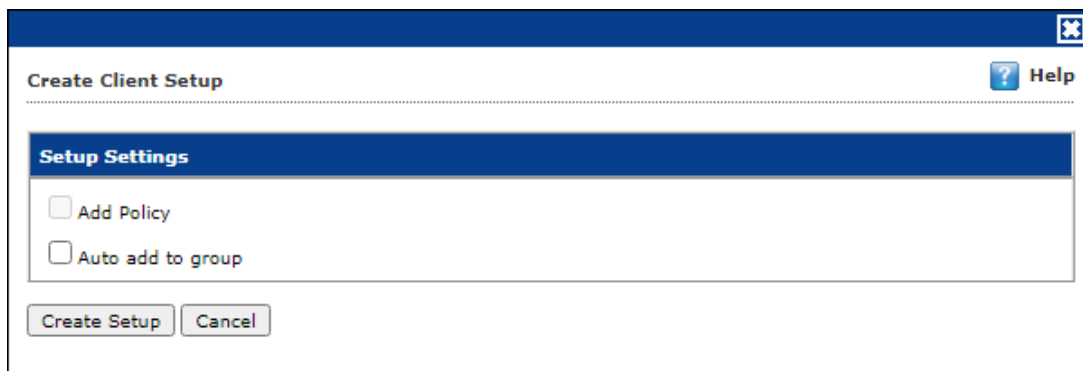
Selecting this option lets you install eScan without firewall.

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

## 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.



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



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

## Properties of a group

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

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

**Properties (Managed Computers)** Help

**General**

Name :

Parent Group :

Group Type :  ▼

Contains : 16 Groups , 2 Computers

Created : 2022 01:19:28 PM

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

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

# Group Tasks

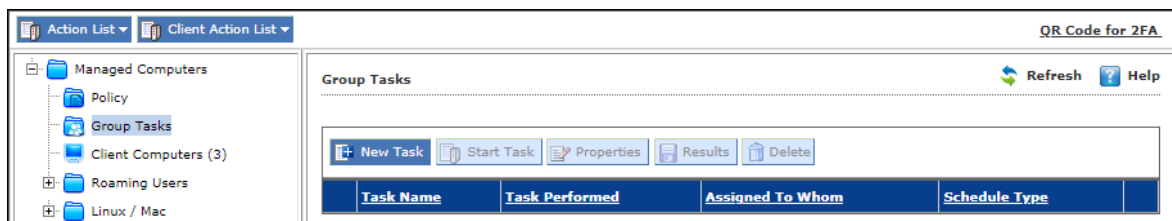
With the Group Tasks option, you can create a task, start a task, select a task and view its properties and results as well as delete an already created task for a particular group. Tasks can include the following.

- Enable/Disable desired Module
- Set Update Server
- Task Scheduling

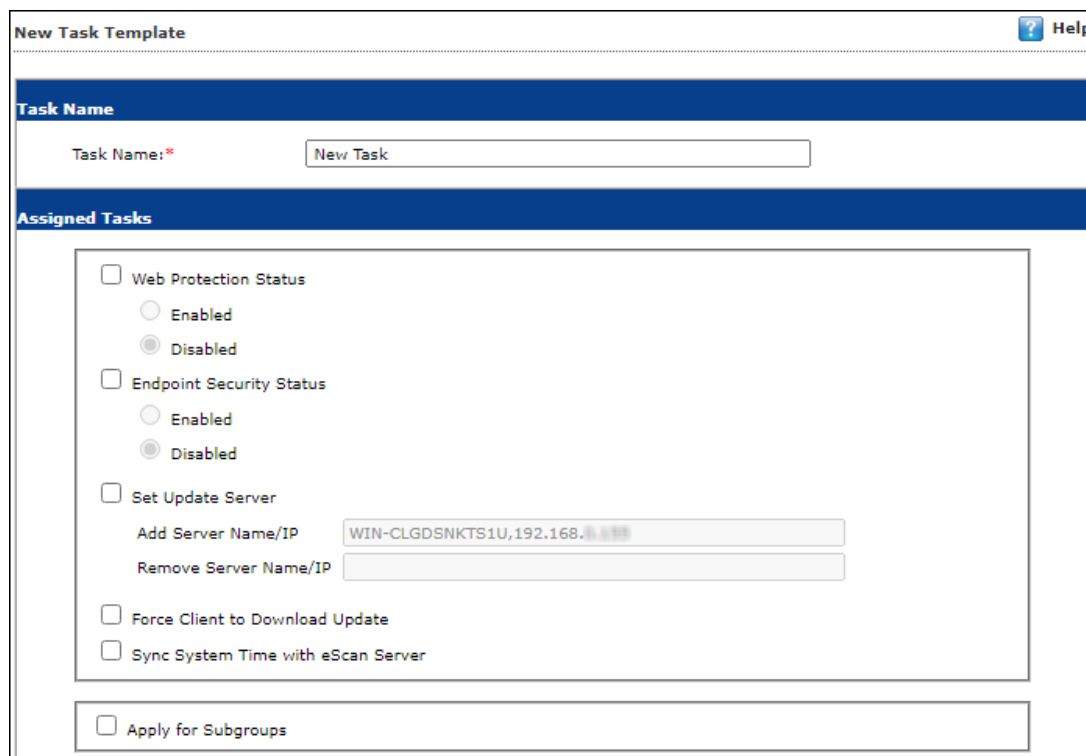
## Creating a Group Task

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.



4. Enter the Task Name and configure the desired task settings.
5. Select the checkbox **Apply for Subgroups**, to assign the created task for subgroup also.

- Schedule the date and time for the execution of task.

**Task Scheduling Settings**

Enable Scheduler
  Manual Start

---

Daily
  Weekly
 Mon
 Tue
 Wed
 Thu

Fri
 Sat
 Sun

Monthly
 1

---

At
 12:00 pm
⌵

- 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**  Refresh Help

---

	Task Name	Task Performed	Assigned To Whom	Schedule Type	
<input checked="" type="checkbox"/>	tech	Not Performed Yet	'Managed Computers'	Automatic Scheduler	<a href="#">Task Status</a>

### Start Task

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

### Properties

To view the properties of a task, select a task and then click **Properties**. The General tab displays the information such as task name, creation date and time, status of the task, and last run date of task. It also lets you modify or redefine the entire settings configured using **Schedule** and **Settings** tab. After making the necessary changes, click **Save**.

The properties for the group task will be saved and updated.

### Results

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

	Task Name	Task Performed	Assigned To Whom	Schedule Type	Task Status
<input type="checkbox"/>	tech	Completed	'Managed Computers'	Automatic Scheduler	

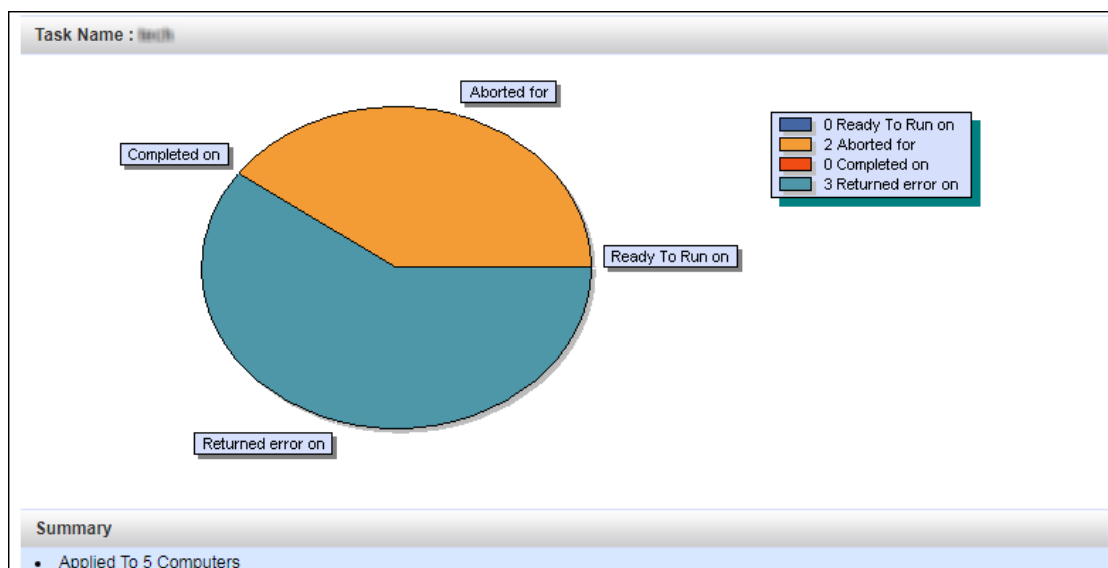
### Delete Task

To delete a task, select a particular task. The confirmation prompt appears. Click **Delete**.

### Task Status

To view the status, select a task and then click **Task Status**.

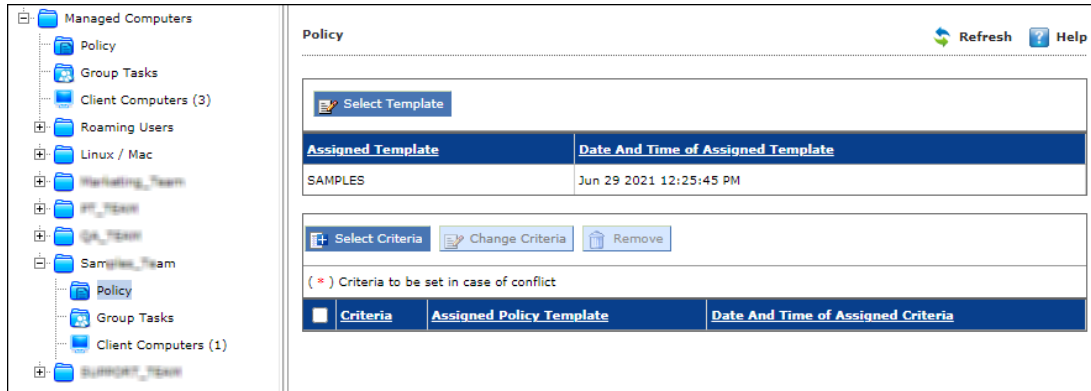
A brief task summary is displayed.



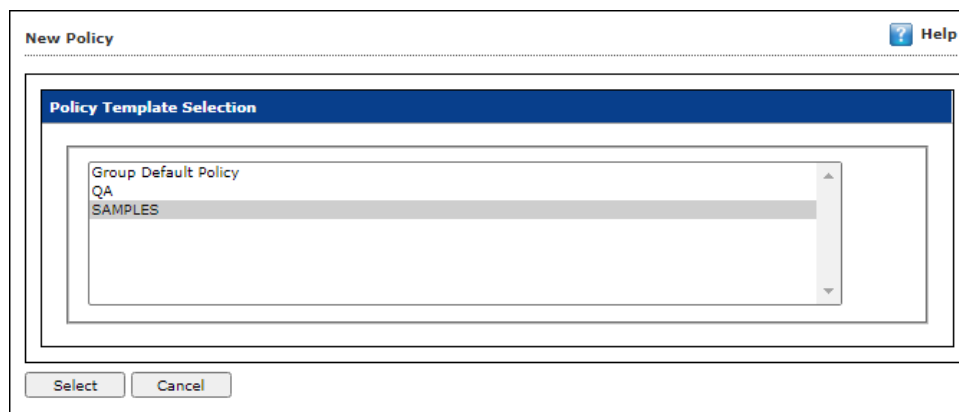
## Assigning a Policy to the group

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.



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



4. Select a policy template and then click **Select**.
5. To assign criteria to the group, click **Select Criteria**.  
Select Policy Criteria window appears.

Select Policy Criteria Help

Set this criteria as a default criteria in case of conflict

**Policy Template Selection**

Group Default Policy

**Criteria Template Selection**

dennis

Select Cancel

6. 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.
7. Click **Select**.  
The default Policy Template and Criteria Template for group will be saved and updated.
8. Click **Change Criteria**, to change the selected policy criteria.
9. Click **Remove**, it will delete the criteria for that group.

## Client Action List

The Client Action List lets you take action for specific computer(s) in a group. To enable this button, select computer and then click **Client Action List**.

The drop-down consists of following options:

- **Set Host Configuration**
- **Deploy/Upgrade Client**
- **Uninstall eScan Client**
- **Move to Group**
- **Remove from Group**
- **Refresh Client**
- **Connect to Client (RMM)**
- **Assign Policy Template**
- **Export**
- **Show Installed Softwares**
- **Force Download**
- **Collect Debug/Logs**
- **Check eScan Port(s)**
- **Send Message**
- **Create OTP**
- **Pause Protection**
- **Resume Protection**
- **Properties**

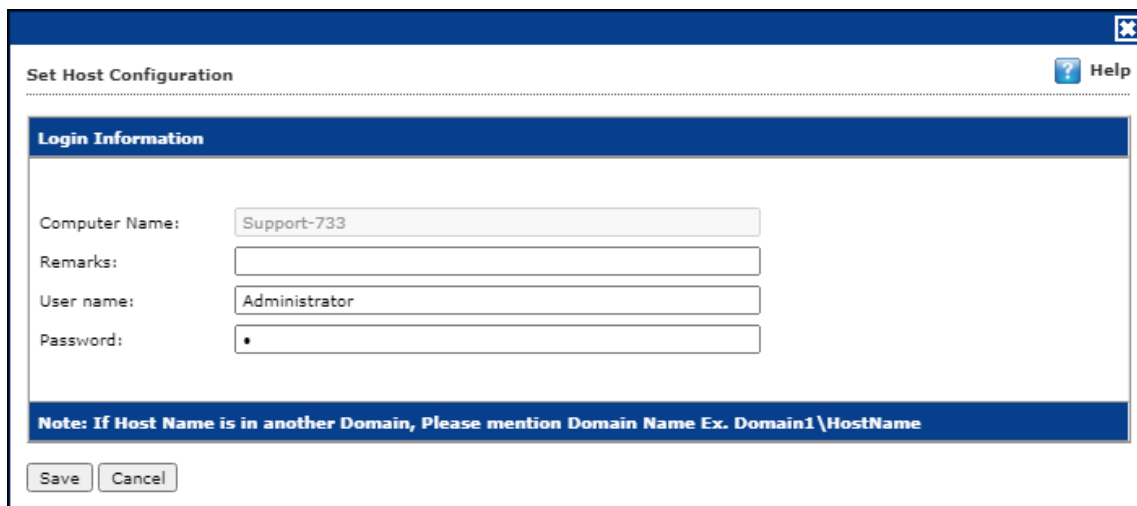
The Client Action List contains few options similar to Action List. These options perform same, except they perform the action only for selected computer(s).

## 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 screenshot shows a dialog box titled "Set Host Configuration" with a "Help" icon in the top right corner. The dialog has a "Login Information" section with the following fields:

- Computer Name: Support-733
- Remarks: (empty)
- User name: Administrator
- Password: (masked with a dot)

Below the fields is a blue bar with the text: **Note: If Host Name is in another Domain, Please mention Domain Name Ex. Domain1\HostName**

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

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

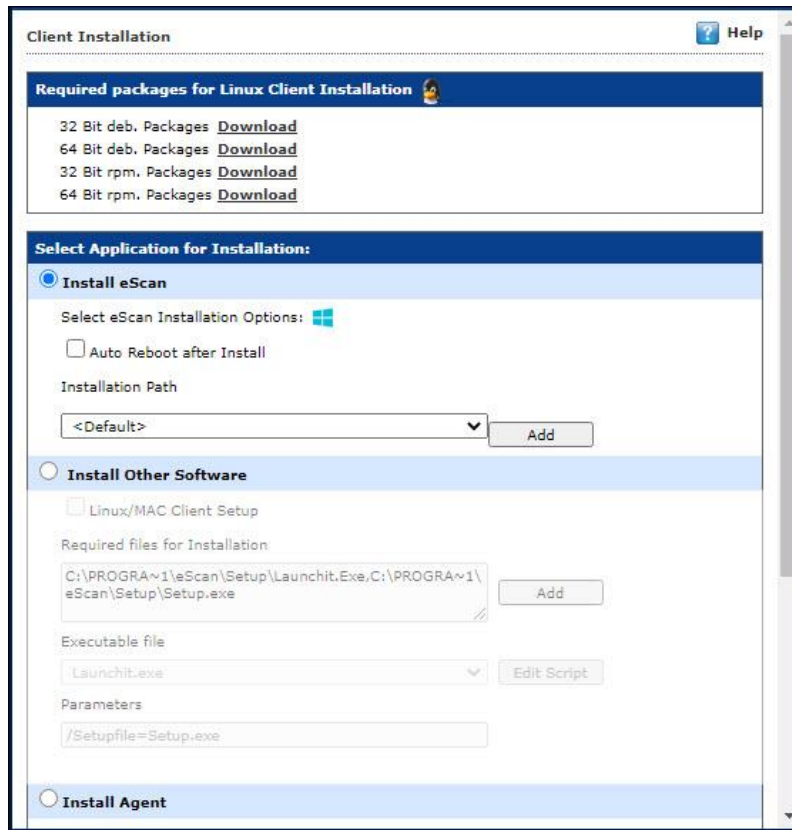
## Deploy/Upgrade Client

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.





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.

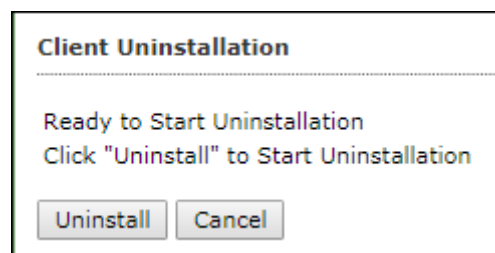
After Installation, the eScan status will be updated in Managed Computers list.

## Uninstall eScan Client

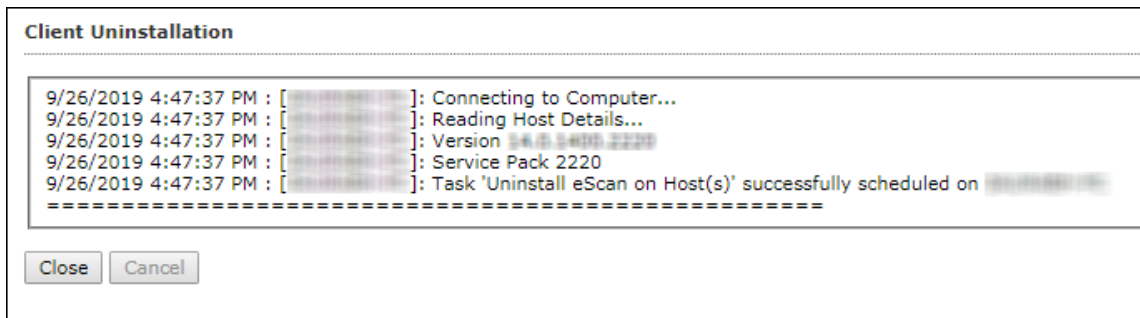
To uninstall eScan Client on any computer, follow the steps given below:

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**.

**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**.

## Move to Group

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

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

## Remove from Group

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

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

## Refresh Client

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

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

## Connect to Client (RMM)

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 connect to RMM.
3. Click **Client Action List > Connect to Client (RMM)**.
4. Read the disclaimer thoroughly and then click **Accept**.  
Your default browser opens eScan Remote Access window (Google Chrome, Mozilla Firefox, MS Edge, etc.).

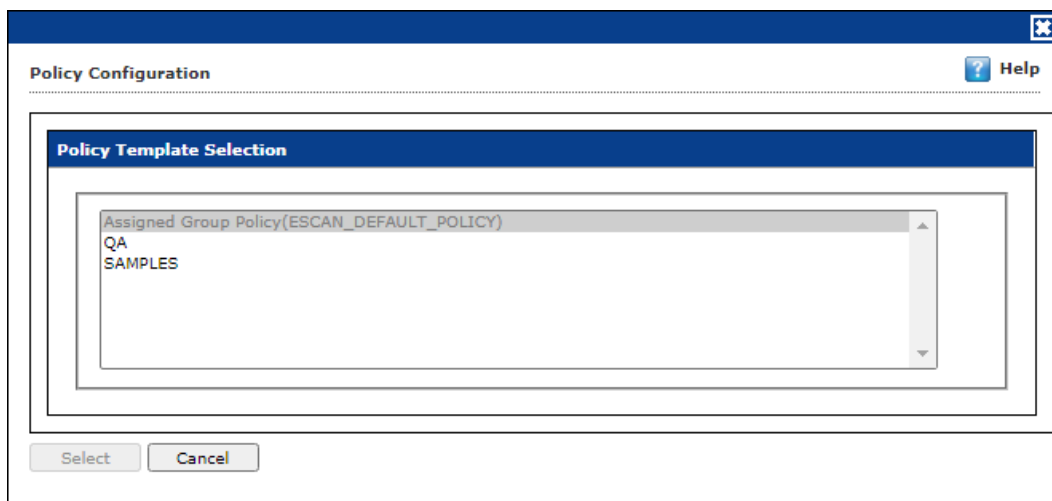


After you done with performing an activity, click **Disconnect** icon to end remote connection.

## Assign Policy Template

To assign policy template to specific computer, follow the steps given below:

1. Go to **Managed Computers**.
2. Select the client computer for which you want to assign policy template.
3. Click **Client Action List > Assign Policy Template**.  
Policy Configuration window appears.

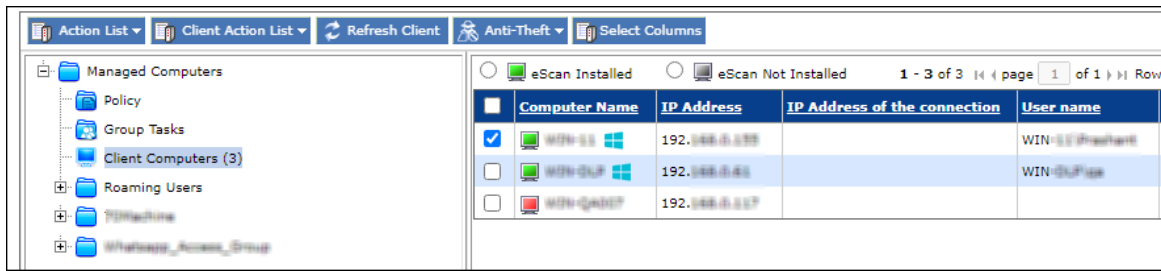


4. Select the policy template and click **Select** to add.  
The computer get assign with the selected policy template.

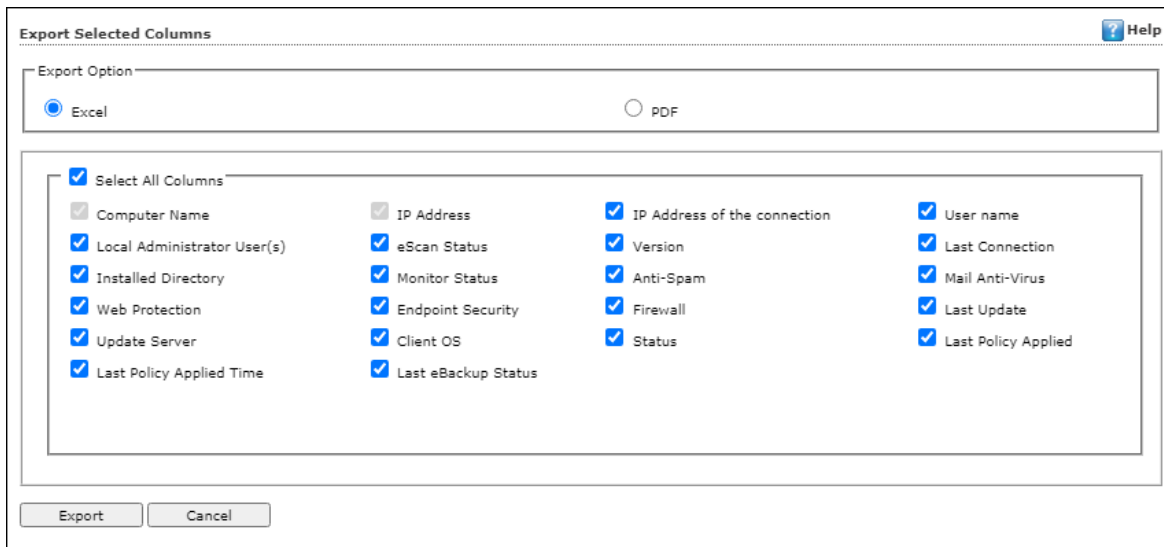
## Export

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

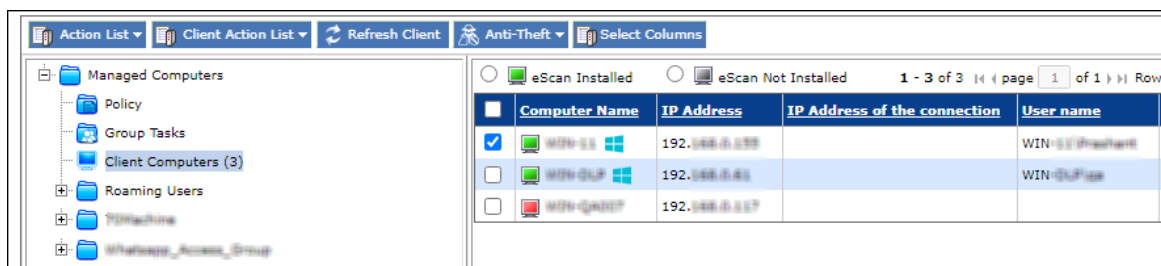


3. Select the preferred export option.
4. Select the preferred report columns.
5. Click **Export**.  
The report will be exported as per your preferences.

## Show Installed Softwares

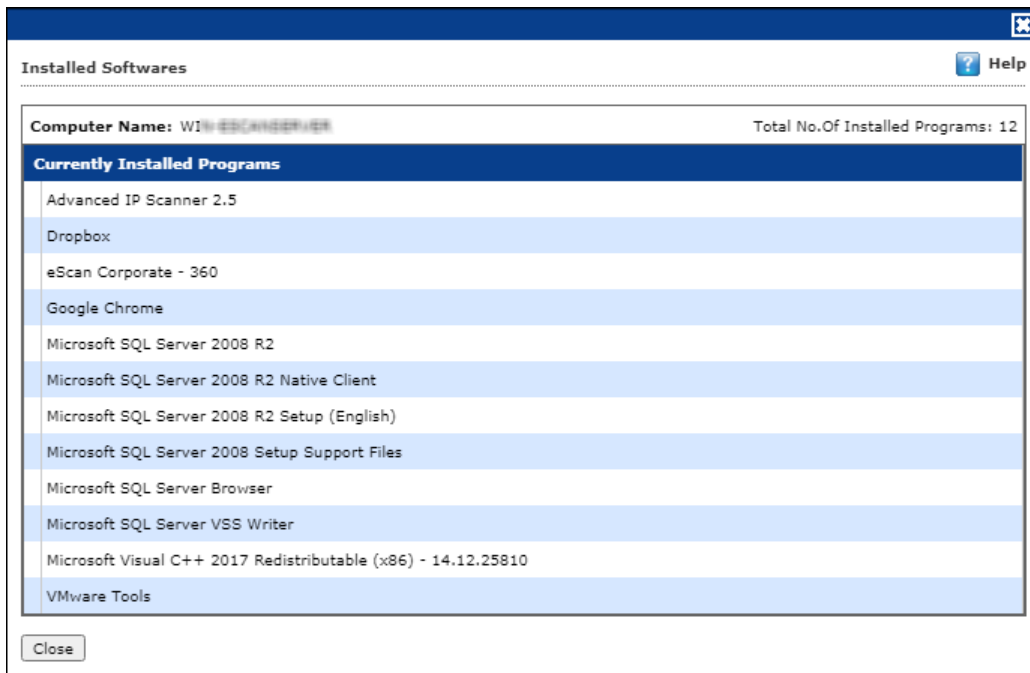
This feature displays a list of installed softwares on a computer. To view the list of installed softwares, follow the steps given below:

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**.

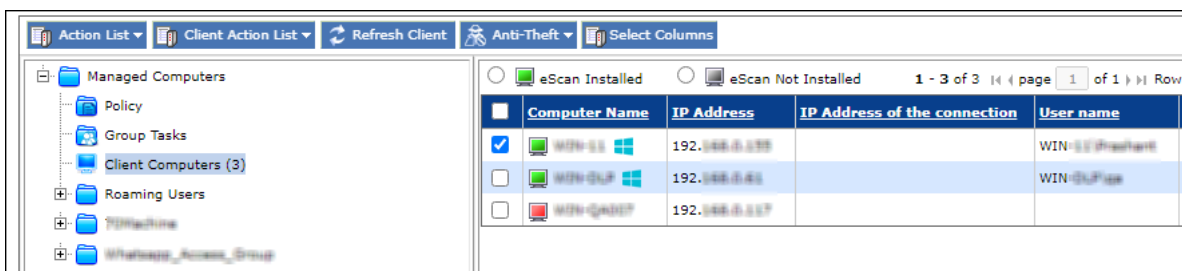
Installed Softwares window appears displaying list of installed softwares and in the top right corner displays total number of installed softwares.



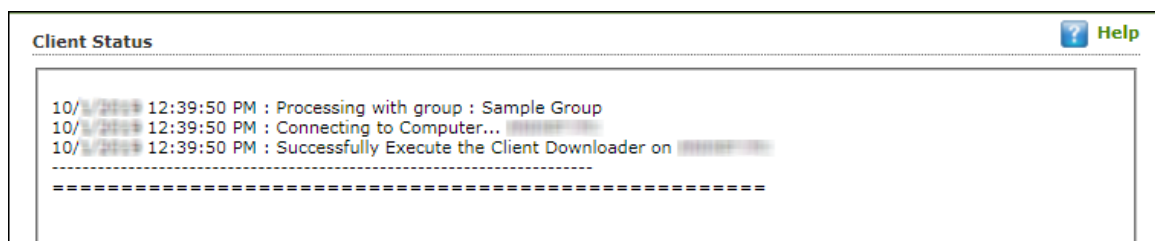
## Force Download

The Force Download feature forces a client computer to download Policy Template modifications (if any) and update virus signature database. To activate this feature, 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.



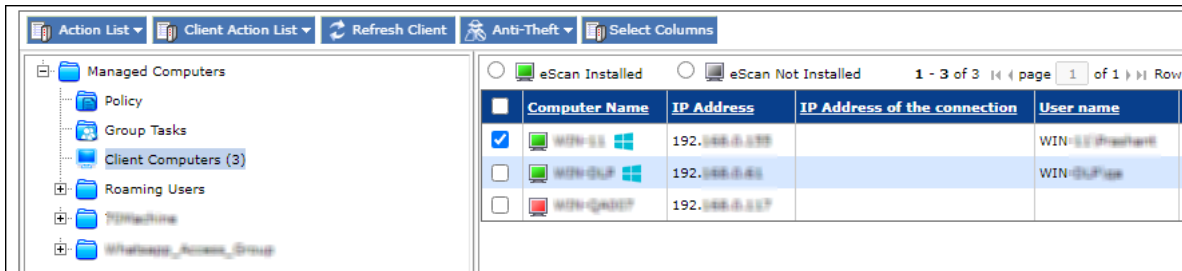
2. Select client computers and then click **Client Action List > Force Download**. Client Status window appears displaying the process.



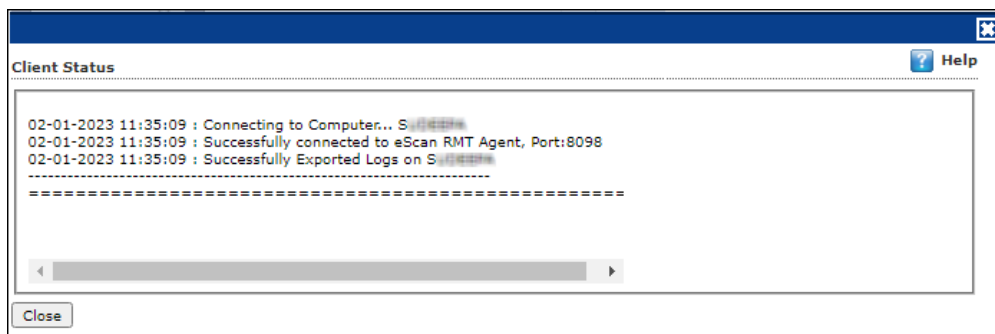
## Collect Debug/Logs

This option helps user to record the system operation and errors that occurs while performing any action on managed computers.

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.



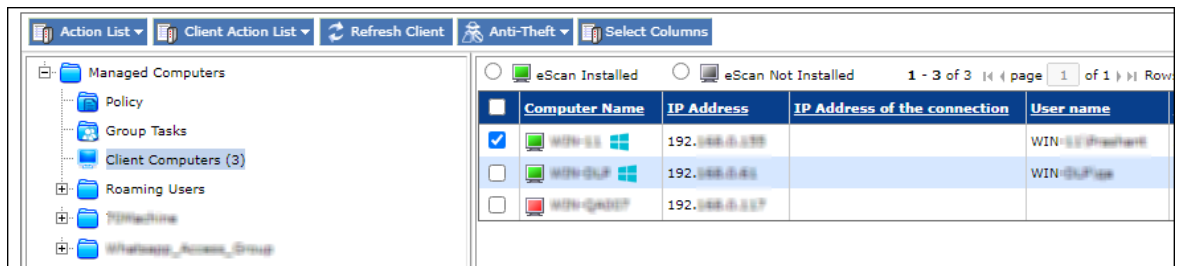
2. Select client computers and then click **Client Action List > Collect Debug/Logs**. Client Status window appears displaying the process.



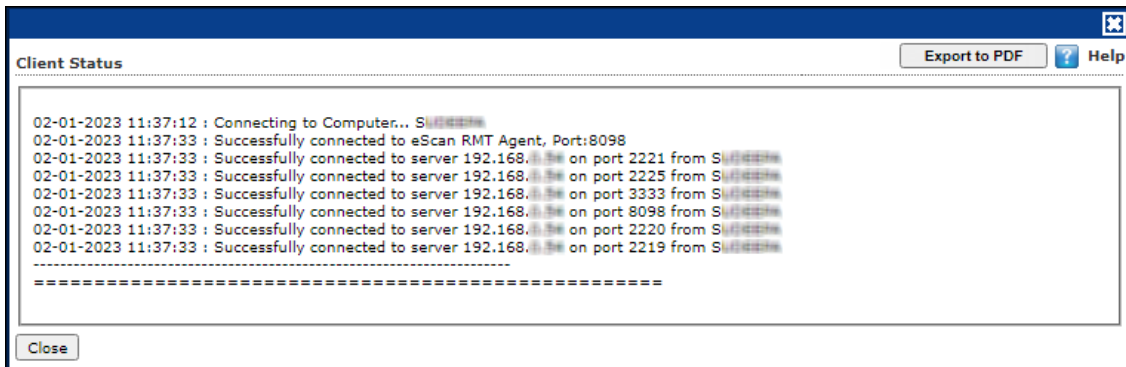
## Check eScan Port(s)

This option used to figure out the opened ports on particular client machine. Checking ports regularly will help you to close the unnecessary ports.

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.



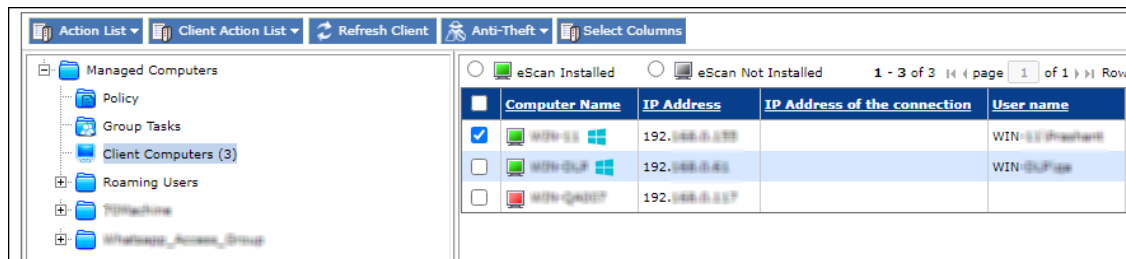
2. Select client computers and then click **Client Action List > Check eScan Ports**. Client Status window appears displaying the process.



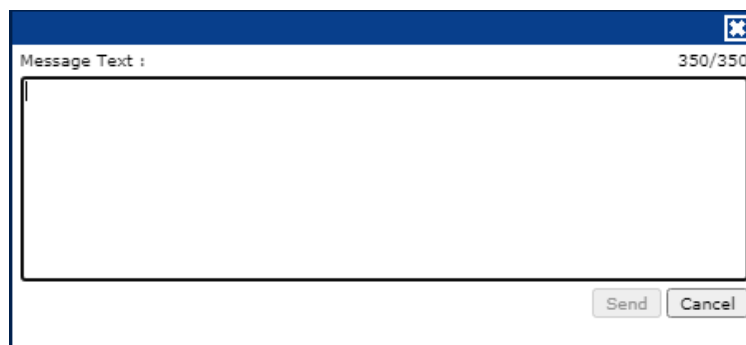
## Send Message

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 computer.

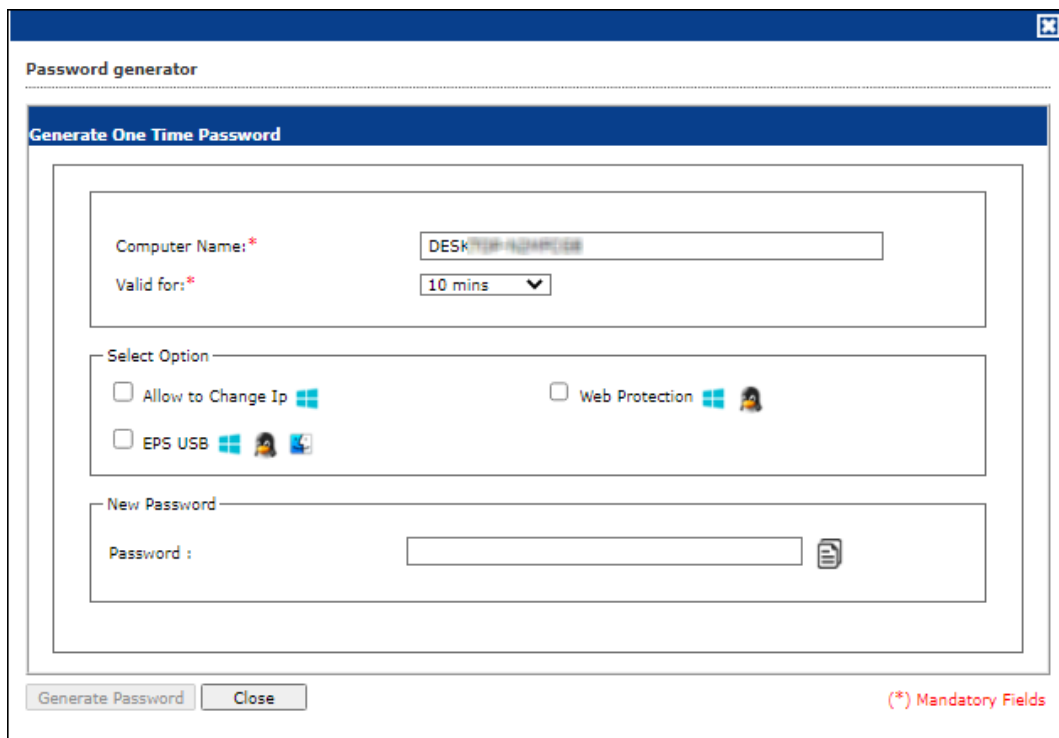
## Create OTP

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

## Generating an OTP

To generate an OTP, follow the steps given below:

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



The screenshot shows a web-based "Password generator" window. The title bar reads "Password generator". Below the title bar is a blue header with the text "Generate One Time Password". The main content area is enclosed in a white border and contains the following fields and options:

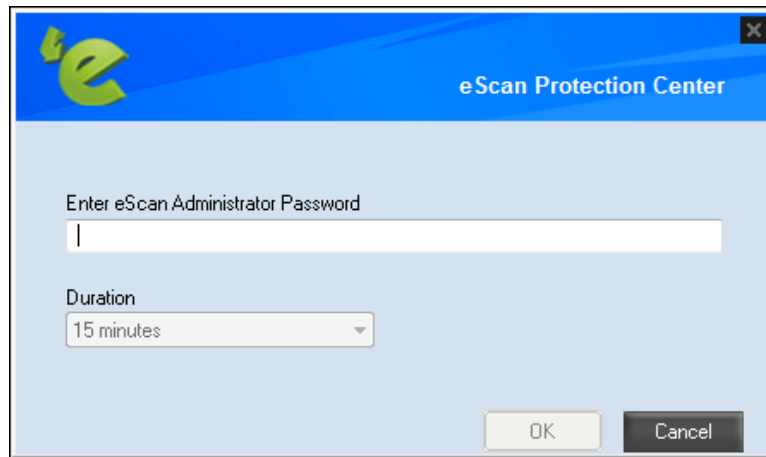
- Computer Name:** A text input field containing "DESKTOP-1234567".
- Valid for:** A dropdown menu currently set to "10 mins".
- Select Option:** A section with four checkboxes:
  - Allow to Change Ip
  - EPS USB
  - Web Protection
  - (unlabeled)
- New Password:** A section with a "Password:" label and a text input field.

At the bottom of the window, there are two buttons: "Generate Password" and "Close". A red note "(\*) Mandatory Fields" is located in the bottom right corner.

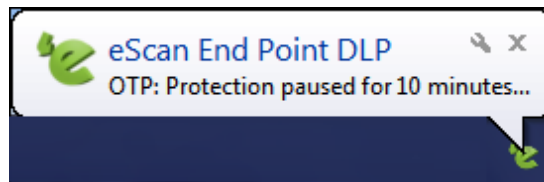
3. In the **Valid for** drop-down, select the preferred duration to bypass the protection module.
4. In **Select Option** section, select the module you want to disable.
5. Click **Generate Password**.  
An OTP will be generated and displayed in **Password** field.







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

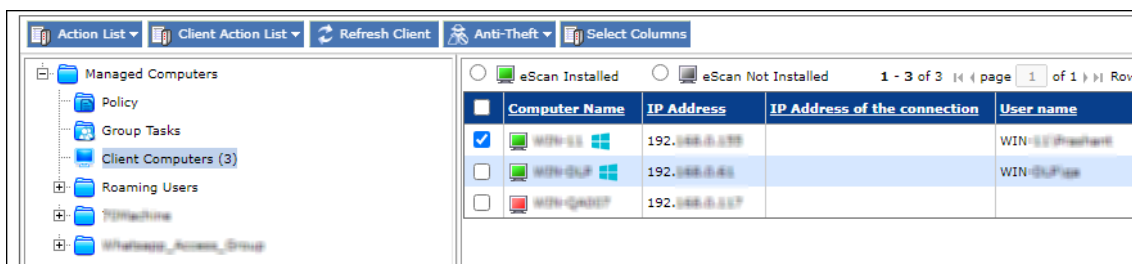


The selected module will be disabled for set duration.

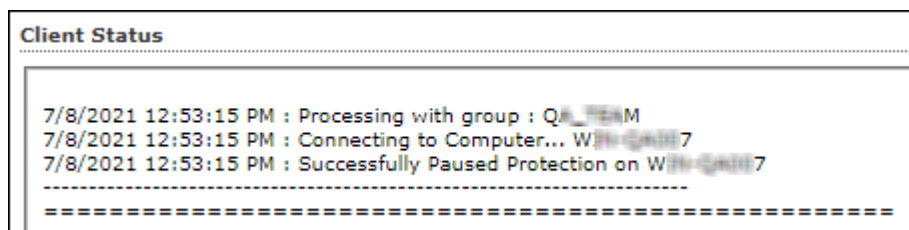
## Pause Protection

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.



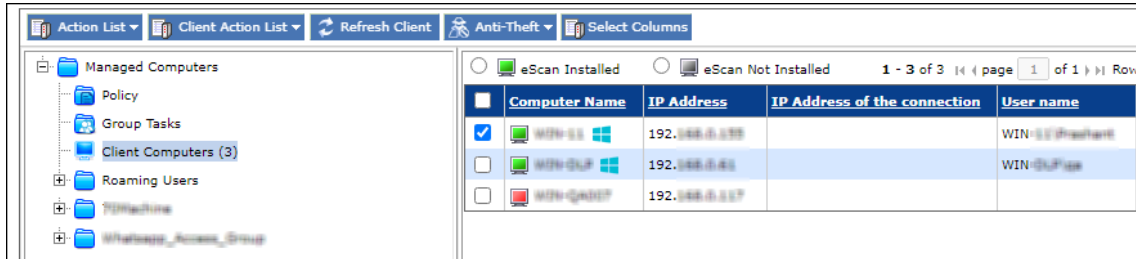
2. Select client computers and then click **Client Action List > Pause Protection**. Client Status window appears displaying the progress.



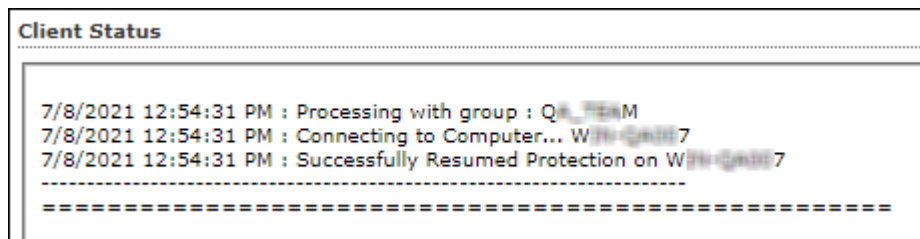
## Resume Protection

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.



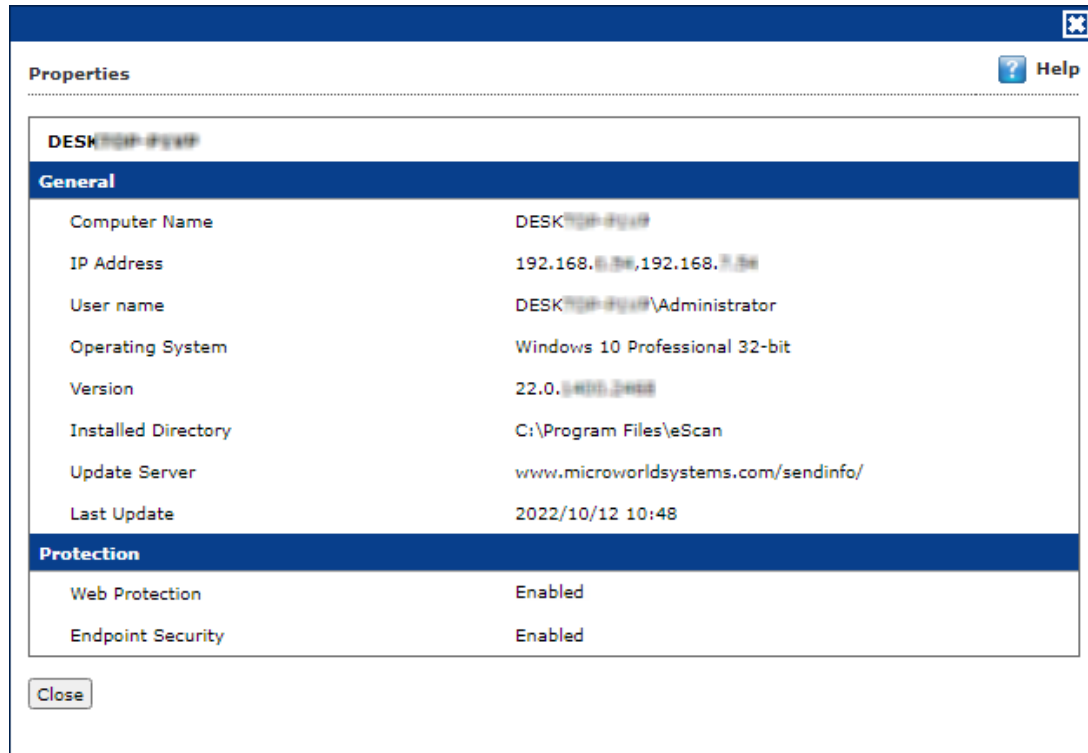
2. Select client computers and then click **Client Action List > Resume Protection**. Client Status window appears displaying the progress.



## 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.



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

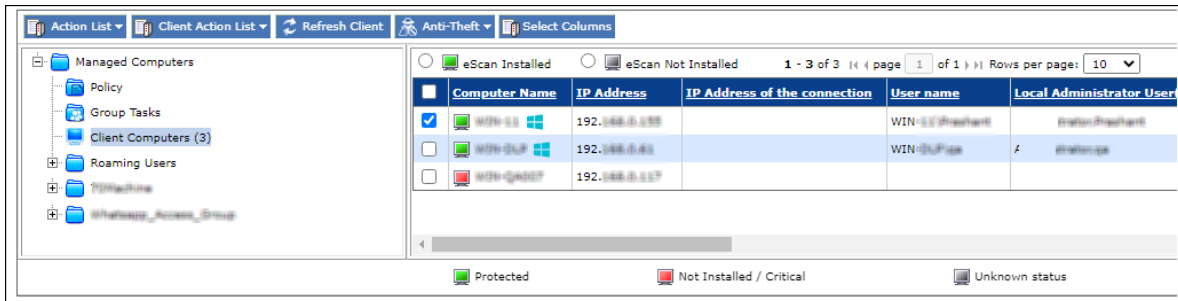
## Refresh Client

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

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

## Anti-Theft (requires additional license)

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

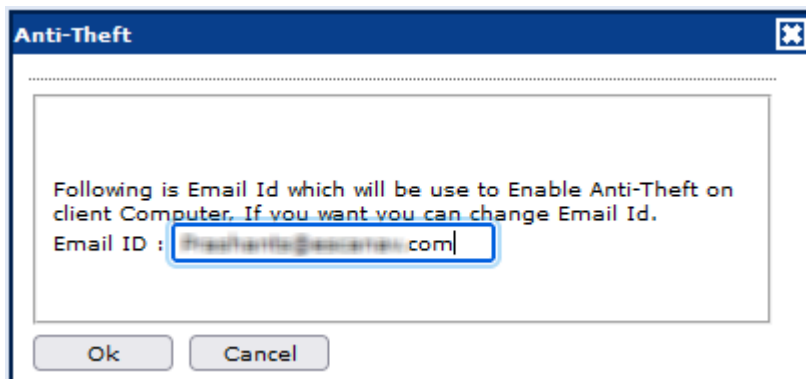


## Anti-Theft Options

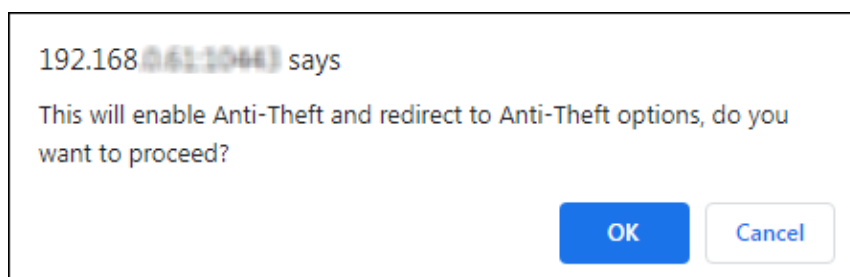
To add computers in an Anti-theft, follow the steps given below:

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

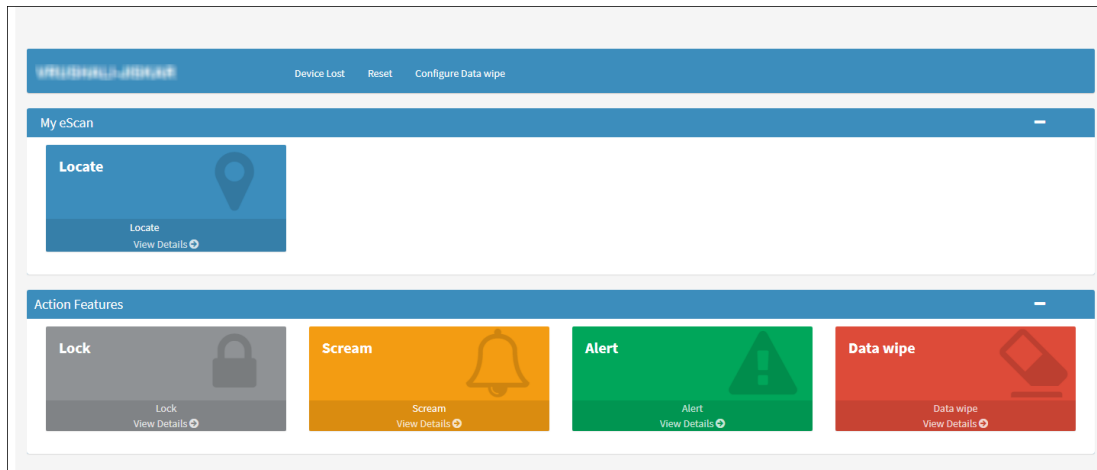
The computer will add in Anti-Theft Portal.



A confirmation prompt appears.

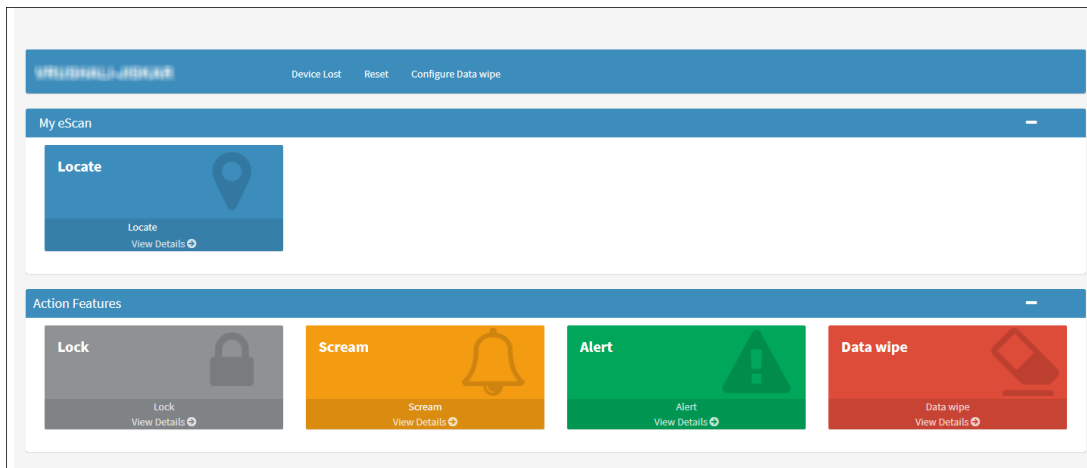


5. Click **OK**.  
This will redirect to Anti-Theft options.



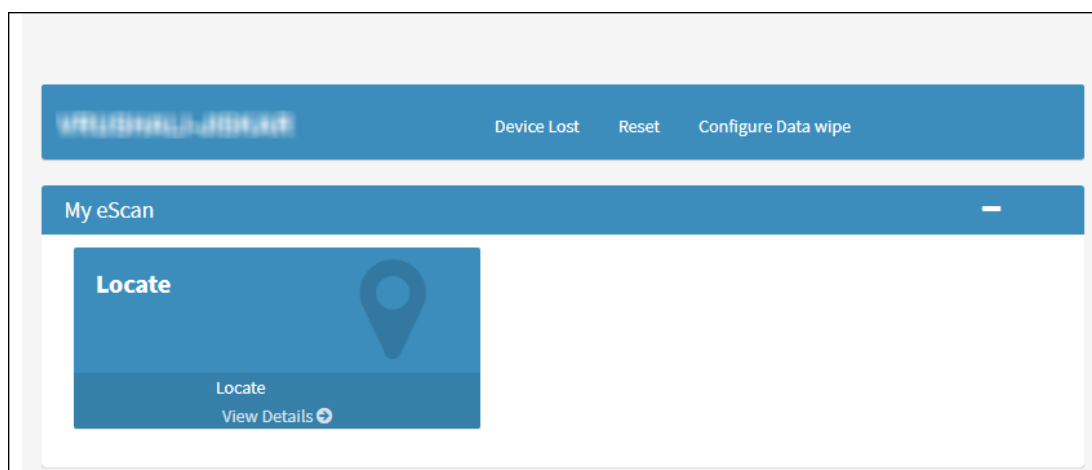
## Anti-Theft Portal

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

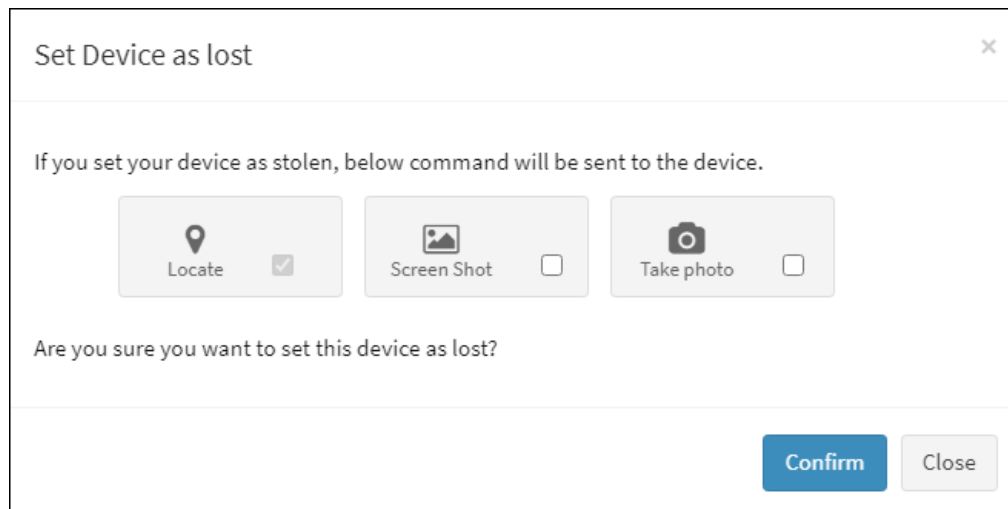


In case of loss or theft, click on the system name that has been lost or stolen, the status bar under it will display the system name again and when it was last seen.

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

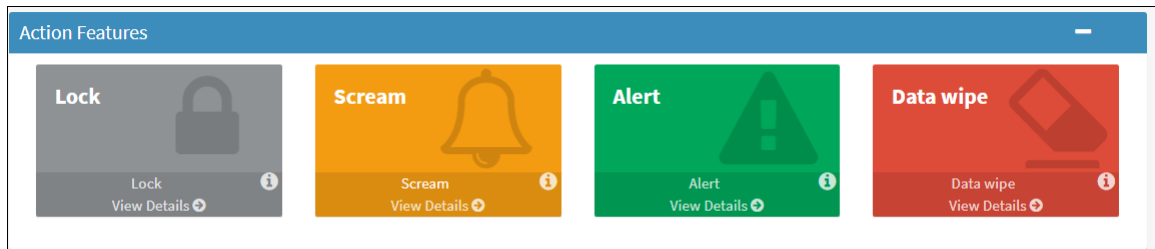


2. Click **Confirm** to confirm that your system has been lost and to execute the commands Locate, Screenshot, and Camera.



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

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



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

## Disable Anti-Theft

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

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



## Understanding the eScan Client Protection Status

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

## Select Columns

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

Select All Columns	
<input type="checkbox"/> Computer Name	<input checked="" type="checkbox"/> IP Address
<input checked="" type="checkbox"/> IP Address of the connection	<input checked="" type="checkbox"/> User name
<input checked="" type="checkbox"/> Local Administrator User(s)	<input checked="" type="checkbox"/> eScan Status
<input checked="" type="checkbox"/> Version	<input checked="" type="checkbox"/> Last Connection
<input checked="" type="checkbox"/> Installed Directory	<input checked="" type="checkbox"/> Last Update
<input checked="" type="checkbox"/> Web Protection	<input checked="" type="checkbox"/> Endpoint Security
<input checked="" type="checkbox"/> Update Server	<input checked="" type="checkbox"/> Client OS
<input checked="" type="checkbox"/> Status	<input checked="" type="checkbox"/> Installation Status
<input checked="" type="checkbox"/> Last Policy Applied	<input checked="" type="checkbox"/> Last Policy Applied Time
<input checked="" type="checkbox"/> Last eBackup Status	<input checked="" type="checkbox"/> PC Model
<input checked="" type="checkbox"/> PC IdentifyingNumber	<input checked="" type="checkbox"/> Domain/Workgroup
<input checked="" type="checkbox"/> Screen Capture	<input checked="" type="checkbox"/> Debug

Apply Cancel

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

## Policy Template

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

## Managing Policies

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

## Defining Policies Windows computers

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

### **Web Protection**

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

### **Endpoint Security**

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

### **Privacy Control**

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

### **Administrator Password**

The Administrator Password lets you create and change password for administrative login and uninstallation password for eScan protection. To learn more, [click here](#).

### **MWL Inclusion List**

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

### **MWL Exclusion List**

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

### **Notifications & Events**

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

### **Schedule Update**

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

### **Tools**

The Tools policy let you configure EBackup and RMM Settings. To learn more, [click here](#).

### **DLP Discovery Scan**

This policy allows you to scan (discover) the sensitive data present in the managed endpoints. To learn more, [click here](#).

## Defining Policies Mac or Linux computers

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

### Endpoint Security

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

### Schedule Update

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

### Administrator Password

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

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

### Network Security

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

### Tools

Tools policy let you configure RMM Settings on Linux based systems. To learn more, [click here](#).

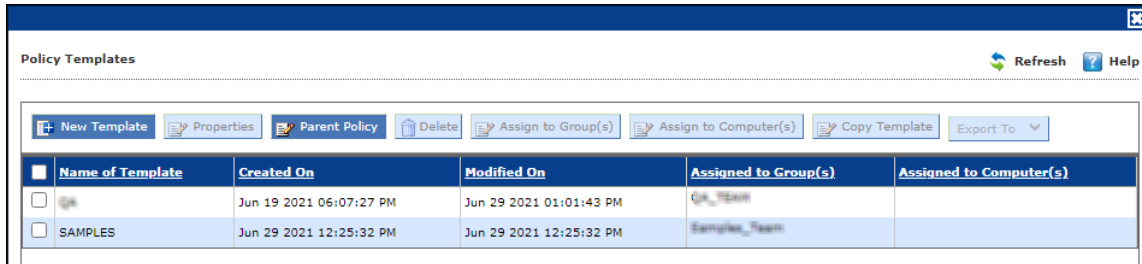
#### NOTE

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

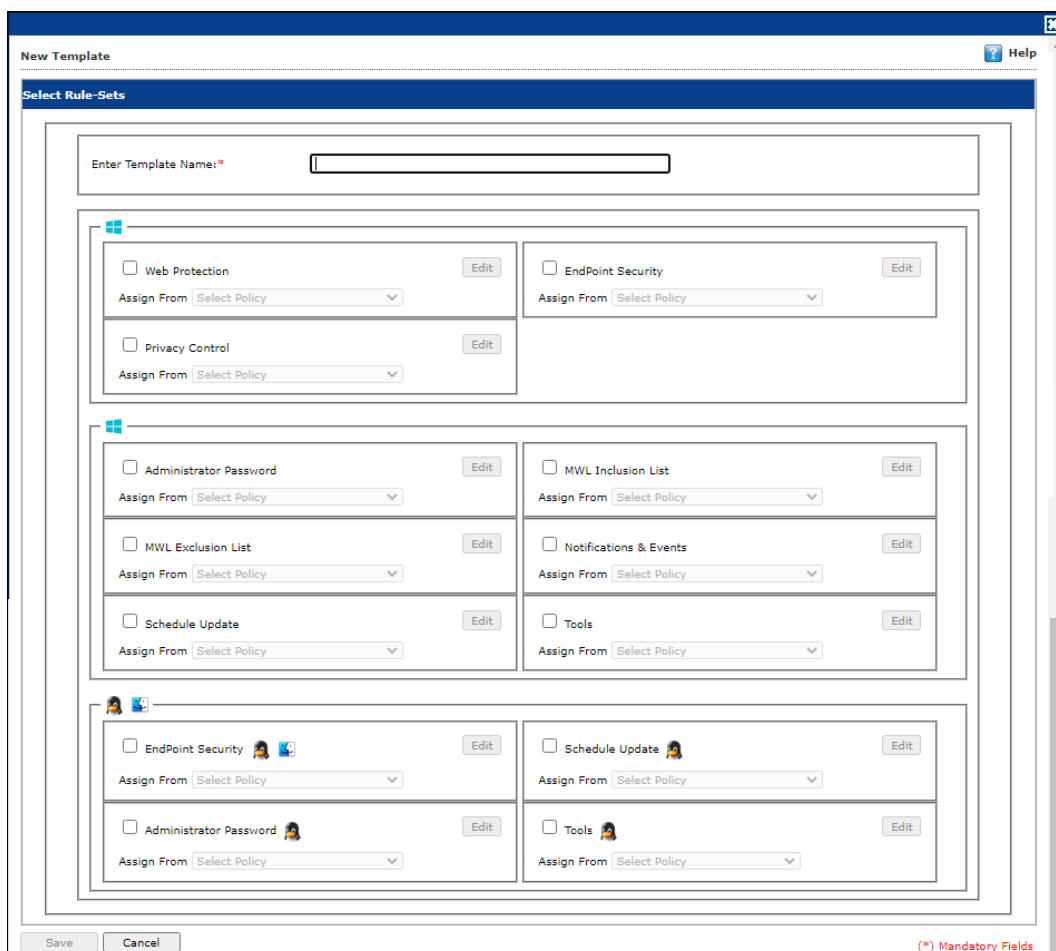
# Creating Policy Template for a group/specific computer

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

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



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



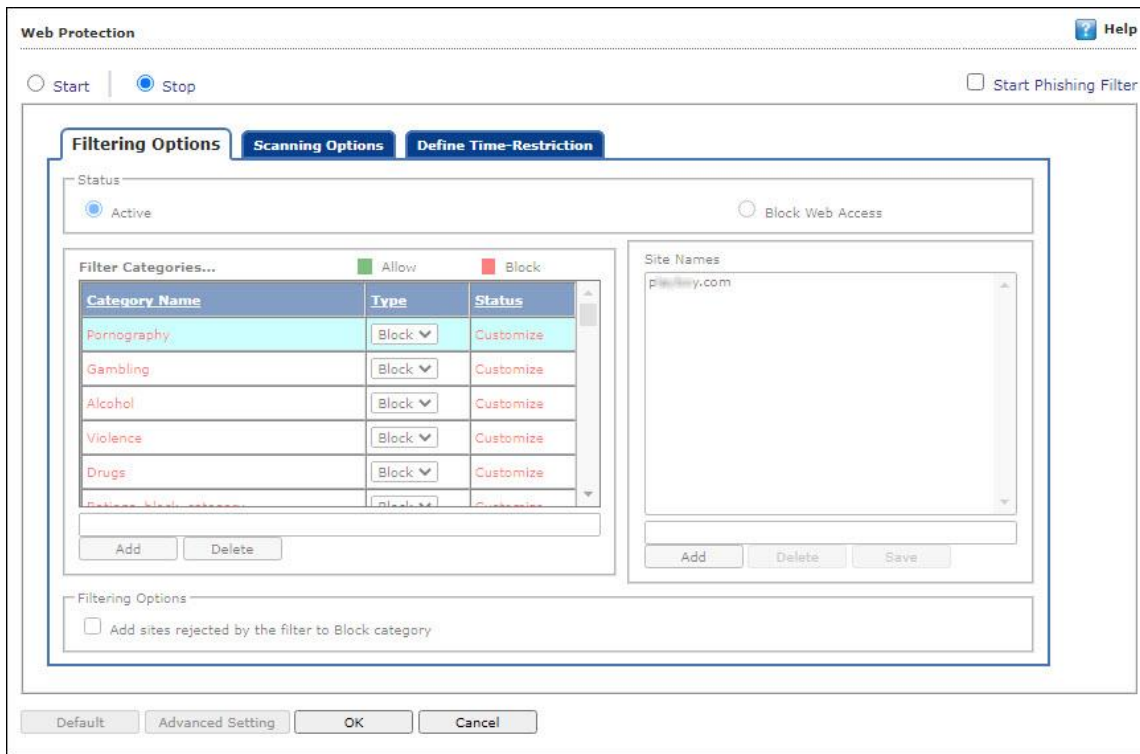
4. Enter name for Template.
5. To edit a module, select it and then click **Edit**.
6. Make a changes and click **Save**.  
The Policy Template will be saved.

# Configuring eScan Policies for Windows Computers

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

## Web Protection

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



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

### Filtering Options

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

#### Status

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

#### Filter Categories

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

#### Green [Allow]

It represents an allowed websites category.

#### Red [Block]

It represents a blocked websites category.

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

### Category Name

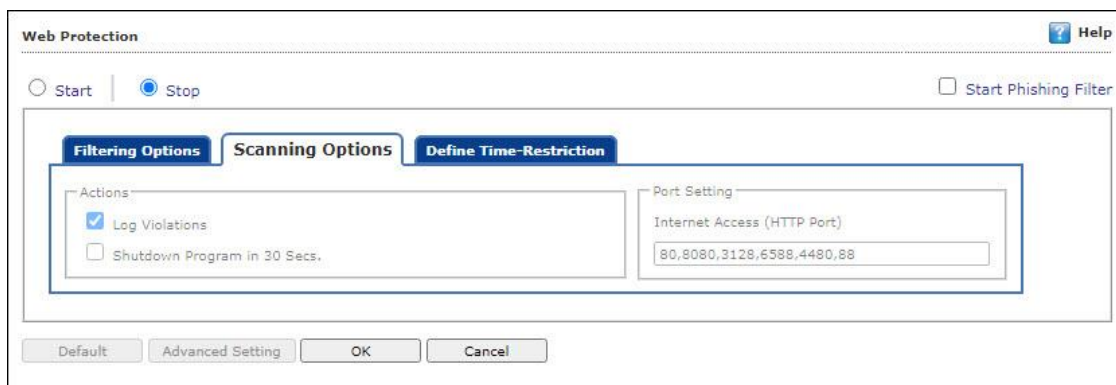
This section shows the **Words/Phrases** list. It lists the words or phrases present in the selected category. In addition, the section displays the **Site Names** list, which lists the websites belonging to the selected category.

### Filtering Options

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

## Scanning Options

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



### Actions

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

#### Log Violations [Default]

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

#### Shutdown Program in 30 Secs

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

### Port Setting

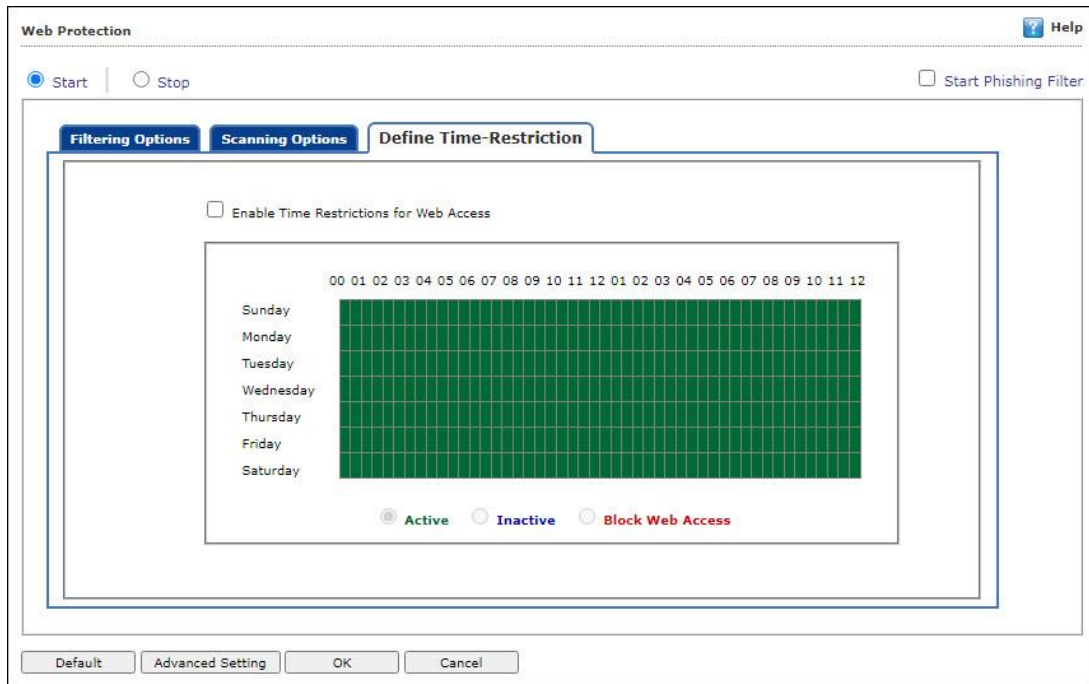
This section lets you specify the port numbers that eScan should monitor for suspicious traffic.

#### Internet Access (HTTP Port)

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

## Define Time Restriction

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



### Enable Time Restrictions for Web Access

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

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

#### Active

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

#### Inactive

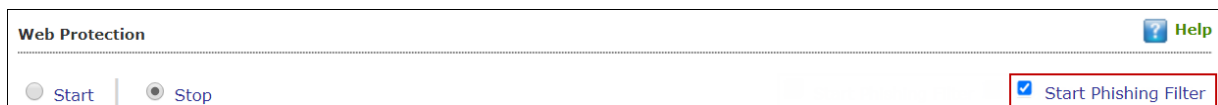
Select this option if you want to keep web access inactive on certain days for a specific interval.

#### Block Web Access

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

### Phishing Filter

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



## Advanced Settings

Clicking **Advanced** displays Advanced Settings.



**Advanced Setting**

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

**Ignore IP address from Web-scanning**

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

**Enable Unknown Browser detection (1 = Enable/0 = Disable)**

Select this option to enable/disable unknown browser detection.

**Enable allowing of WhiteListed Site during BlockTime (1 = Enable/0 = Disable)**

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

**Enable Online Web-Scanning Module (2 =eScan Cloud Server/1 =Online database/0 = Offline database)**

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

**Disable Web Warning Page (1 = Enable/0 = Disable)**

Select this option to enable/disable web warning page.

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

Select this option to enable/disable HTTPS Popup.

**Show External Page for Web blocking (Page to be define under External Page) (1 = Enable/0 = Disable)**

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

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

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

**Force inclusion of Application into Layer scanning (MW Layer)**

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

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

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

**Ignore Reference of sub-link (1 = Enable/0 = Disable)**

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

**Allow access to SubDomain for Whitelisted sites (Only HTTP Sites) (1 = Enable/0 = Disable)**

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

**Allow access to SubDomain for Whitelisted sites (Only HTTPS Sites) (1 = Enable/0 = Disable)**

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

**Enable logging of visited websites (1 = Enable/0 = Disable)**

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

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

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

**Block HTTP Traffic only on Web Browser (1 = Enable/0 = Disable)**

Select this option to enable/disable blocks HTTP Traffic on Web Browser.

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

Select this option to enter the website name need to be allowed.

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

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

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

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

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

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

**WFP Exclude IP List**

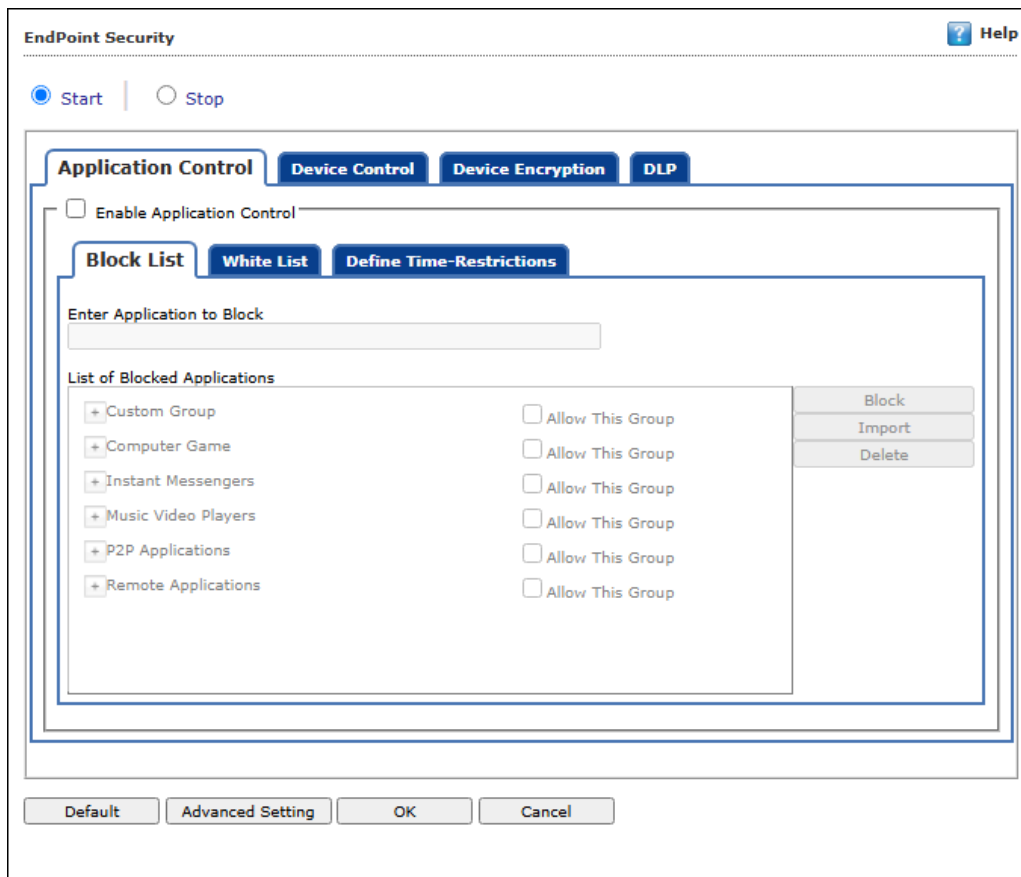
This option excludes entered IP address from web protect filter.



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

## Endpoint Security

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



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

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

## Application Control

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

### Enable Application Control

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

### Block List

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

### List of Blocked Applications

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

### Allow This Group

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

### Import

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

### Delete

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

### White List

#### Enable Whitelisting

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

The screenshot shows the 'White List' configuration window. At the top, there are three tabs: 'Block List', 'White List' (selected), and 'Define Time-Restrictions'. Below the tabs, there is a checkbox labeled 'Enable Whitelisting'. Underneath, there is a text input field labeled 'Enter Application to White List'. The main area contains a table titled 'White Listed Applications'. The table has columns for 'Allow/Block Application Name', 'Original Name', 'Internal Name', and 'Description'. To the right of the table, there are two buttons: 'Whitelist' and 'Delete'. The table contains the following data:

Allow/Block Application Name	Original Name	Internal Name	Description
netsetup.exe			network setup wizard
ntsd.exe			symbolic debugger for
nslookup.exe	nslookup.exe.mui	nslookup.exe	nslookup
narrator.exe			microsoft narrator
notepad.exe	notepad.exe	notepad	notepad
mmc.exe	mmc.exe.mui	mmc.exe	microsoft management console
mshearts.exe			hearts
mstsc.exe	mstsc.exe.mui	mstsc.exe	remote desktop connection
mspaint.exe	mspaint.exe.mui	mspaint	paint

### Enter Application to White List

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

### White Listed Applications

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

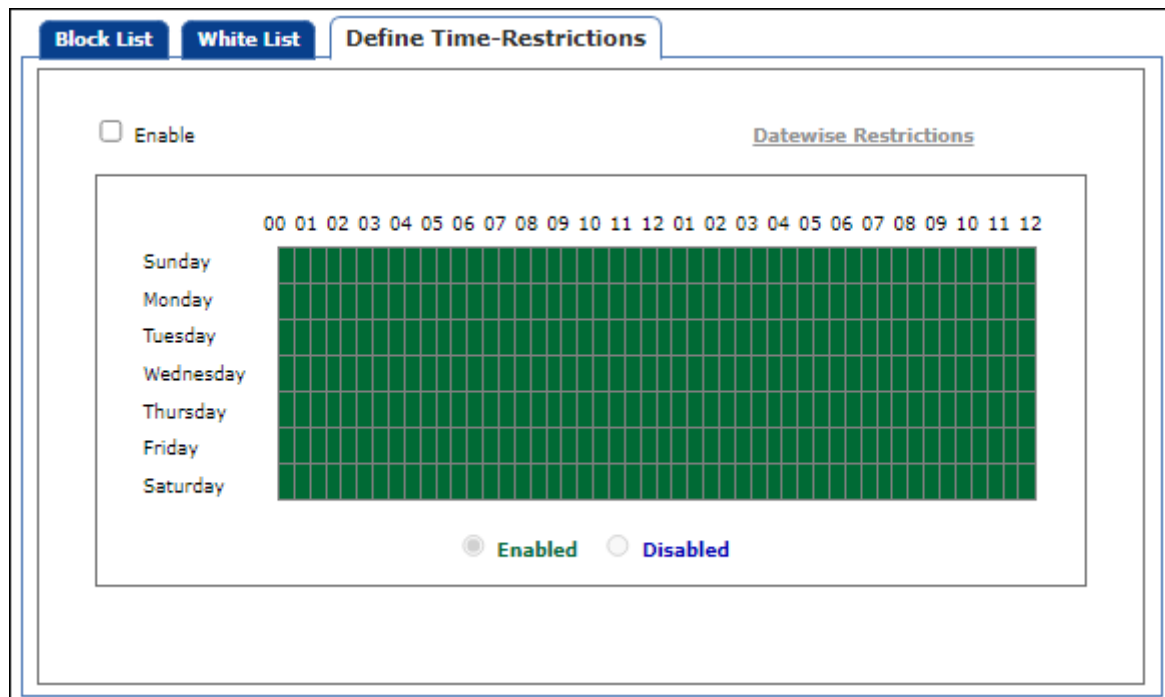
### Delete

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

### Define Time-Restrictions

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

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



### Enable

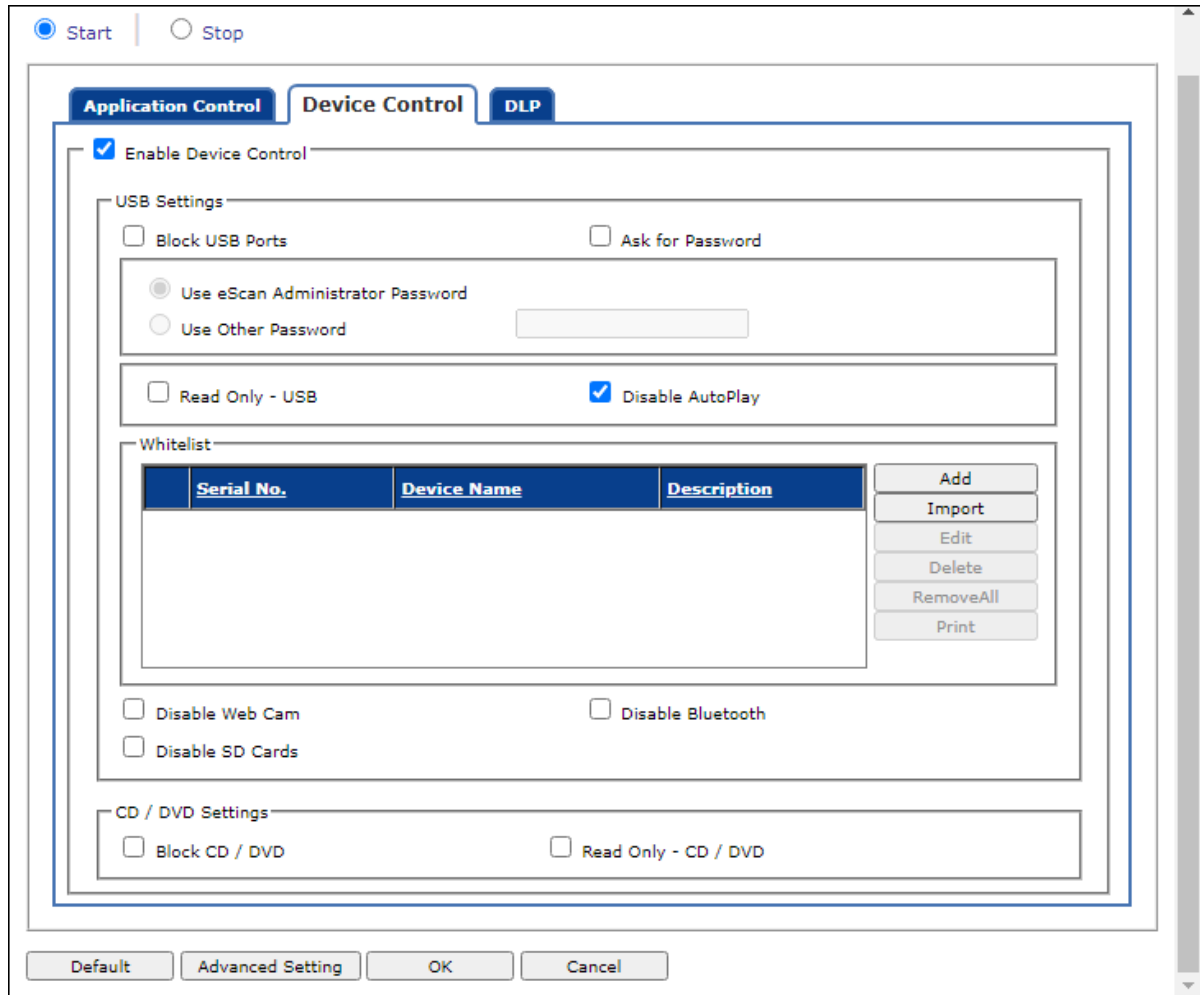
This option lets you enable/disable Datewise Restriction feature.

### Datewise Restrictions

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

## Device Control

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



### 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 checkbox selected. Following options are available only when you select the **Ask for Password** checkbox.

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

### Read Only –USB

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

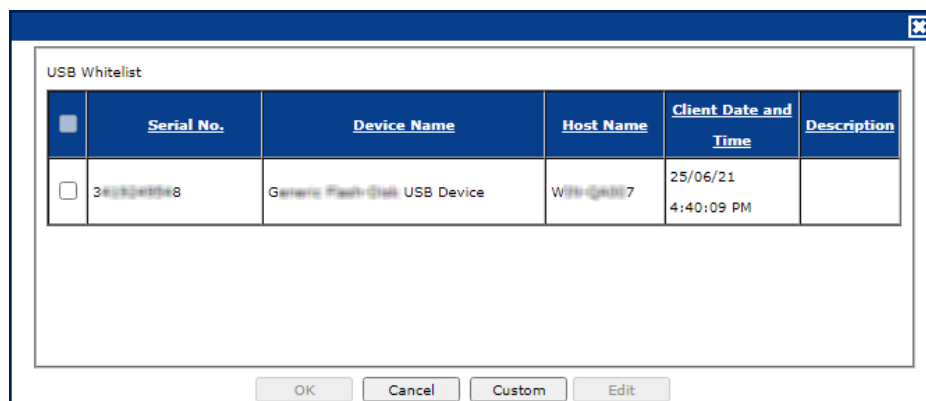
### Disable AutoPlay [Default]

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

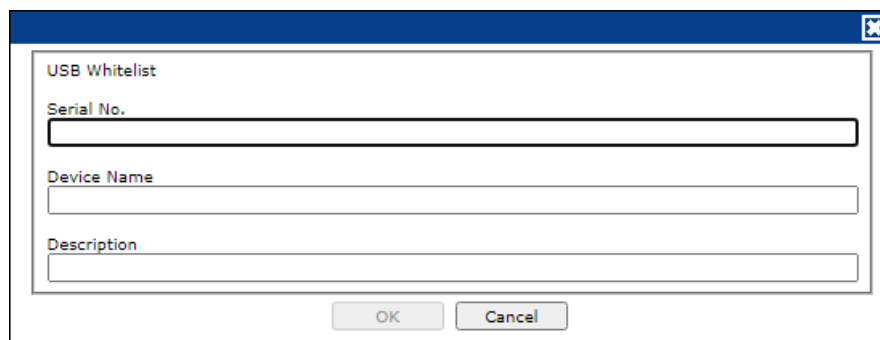
### Whitelist

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

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




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



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

- **Import**

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

 <b>NOTE</b>	The list should be in following format: Serial No 1, Device Name 1, Device Description 1(Optional) Serial No 2, Device Name 2 <b>For Example:</b> SDFSD677GFQW8N6CN8CBN7CXVB, USB Drive 2.5, Whitelist by xyzDFRGHRS54456HGDF347OMCNAK, Flash Drive 2.2
--	--

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

**Disable Web Cam:** Select this option to disable Webcams.

**Disable SD Cards:** Select this option to disable SD cards.

**Disable Bluetooth:** Select this option to disable Bluetooth.

#### CD/DVD Settings

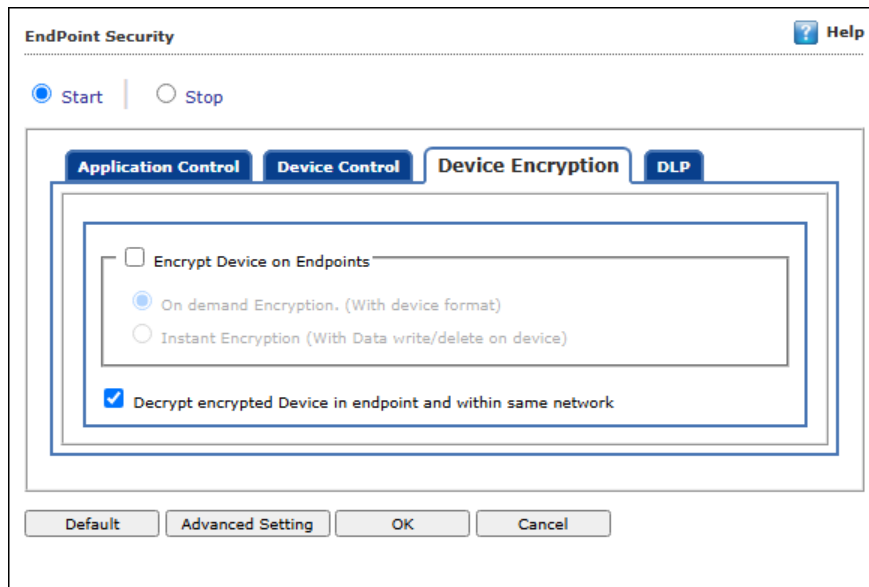
**Block CD / DVD:** Select this option to block all CD/DVD access.

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



## Device Encryption

eScan Device Encryption protects devices and data with full device encryption method for Windows systems managed under eScan management console. It gives admin a visibility of devices across their organization. The device encryption can be deployed on endpoints where administrator/users are authorized to encrypt storage devices which are connected to the system. Once the encryption process is completed, it gives an alert to the user. A notification will be sent to the server and administrator can trigger an alert for the same.



### Encrypt Device on Endpoints

This option enables encryption settings to be configured for storage devices like external hard disks and USB drives that are connected to the endpoint.

- **On demand Encryption (With device format):** This option formats the connected USB device and encrypts it for further use of storing data in encrypted format.
- **Instant Encryption (With Data write/delete on device):** This option instantly encrypts the device without formatting existing data.

### Decrypt encrypted device in endpoint and within same network

This option allows the user to access the content of the encrypted device only when it is connected within the same network.

## DLP

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

EndPoint Security
 Help

Start |  Stop

Application Control
Device Control
Device Encryption
DLP

Attachment Control
Content Control
IM / Print Screen
Sensitive File/Folder Protection

Clipboard Control
File Activity Monitoring
Workspace Apps
Disk Encryption
Remote Access Software

Control sync settings

Attachment Allowed  
 Attachment Blocked

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

Add
Delete

Blacklisted Process  Ignore Whitelisted Sites only for Blacklisted process

Process Name	Allow Only Whitelisted Site

---

Attachments will be allowed from below sites irrespective of the above settings  
 Enter Site Name : **Eg. Gmail.com, Yahoo**  
  

Add
Delete

Whitelisted sites

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

Enable Shadow Copy for Attachment Allowed  
 Shadow Copy folder path :  
  
Note : Only Drive name or full UNC path is Allowed. Eg:  
 1. "c:\"  
 2. "\\192.168.0.96\external\backup"

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

Default
Advanced Setting
OK
Cancel

## Attachment Control

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

### **Attachment Allowed [Default]**

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

### **Attachment Blocked**

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

### **Configure Extension/Group based Whitelisting**

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

### **Enter Process Name**

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

### **Blacklisted Process**

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

### **Whitelisted Process**

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

### **Ignore Whitelisted Sites only for Blacklisted process [Default]**

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

### **Enter Site Name**

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

### **Whitelisted Sites**

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

## **Attachment / Email report**

### **Report for Attachment Allowed**

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

### **Report for all email (Including Attachment)**

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

### **Enable Shadow Copy for Attachment Allowed**

Select this checkbox to create shadow copies of outgoing attachments. Enter the drive name or complete UNC path in the provided field where these shadow copies need to be saved.

### **Advance Document settings**

It disables the exporting of MS Office documents in PDF format.

## Content Control

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

The screenshot displays the 'Content Control' configuration window in EndPoint Security. The window is titled 'EndPoint Security' and has a 'Help' icon in the top right corner. At the top, there are radio buttons for 'Start' (selected) and 'Stop'. Below this, there are tabs for 'Application Control', 'Device Control', and 'DLP'. The 'DLP' tab is active, and within it, there are sub-tabs for 'Attachment Control', 'Content Control' (selected), 'IM / Print Screen', 'Sensitive File/Folder Protection', 'Clipboard Control', 'File Activity Monitoring', 'Workspace Apps', 'Disk Encryption', 'Remote Access Software', and 'Control sync settings'.

The main configuration area includes the following sections:

- Enable Blocking:** A checked checkbox. Below it are radio buttons for 'Block' (selected) and 'Monitor'.
- Content list:** A list of content types with checkboxes:
  - Indian PAN Card
  - Indian Passport
  - Indian Voter ID
  - International Bank Account Number (IBAN)
  - American Express - Credit Card
  - Mastercard - Credit Card
- Channels:**
  - Clipboard Protection:**
    - Checked: Chat Applications, Allow Drag and Drop
    - Unchecked: All Applications
  - Application File Access Protection:**
    - Checked: Password Protected Archives, Password Protected Documents, Scan Archives
  - Removable Storage Protection:**
    - Unchecked: Removable Storage, CD/DVD
  - Printer Protection:**
    - Unchecked: Printers
- Recipient Email Domain control:**
  - Checked: Enable Sending Content to whitelisted Recipient Domain
  - Whitelisted Recipient Domain(s): A list box containing 'Whitelisted Recipient Domain(s)' with 'Add' and 'Delete' buttons.
- Customised Content List:**
  - Enable White List Content:**
    - Checked: Enable White List Content
    - White List: A list box containing 'White List' with 'Add', 'Delete', and 'Edit' buttons.
  - Enable Black List Content:**
    - Checked: Enable Black List Content
    - Black List: A list box containing 'Black List' with 'Add', 'Delete', and 'Edit' buttons.

At the bottom of the window, there are buttons for 'Default', 'Advanced Setting', 'OK', and 'Cancel'.

### Enable Blocking

Select this checkbox to allow all listed settings to be configured. Further, you can either select **Block** to completely prevent any outflow of information, ensuring no data is transmitted, or select **Monitor** to only report the outgoing information for specific analysis purposes without terminating the activity.

### Content List

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

### Sensitivity Labels

The Sensitivity Labels (Data Classification) is a critical data security component that helps organizations manage and protect their sensitive information. By categorizing data based on its sensitivity and importance, organizations can apply appropriate security measures tailored to the data's classification labels and respond quickly to potential data leaks, thus enhancing their overall security system. Below are the three categories under which the data gets labelled:

- **Normal:** Regular, productivity data circulating in a network and can be shared externally for business purpose.
- **Internal:** Internal, business data circulating in a network which cannot be shared externally.
- **Confidential:** Sensitive data which is not intended for sharing and needs to be protected from being leaked outside the network (or an endpoint).

To configure this option for MS Office applications, follow the steps given below:

1. Under Sensitivity Labels, select the checkbox **Classify using Sensitivity Labels and Restrict**.
2. Select the checkbox **Sensitivity Labels Integration in MS Office Ribbon**.

### Channels

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

#### Clipboard Protection

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

#### Application File Access Protection

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

#### Removable Storage Protection

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

## Printer Protection

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

## Image DLP [OCR]

Similar to regular DLP that monitors text based content in order to prevent its leakage outside the network, the Image DLP prevents leakage of visual (images) data like photocopy of Credit/Debit card, PAN card, Aadhar card, Passport, and many more image files of sensitive documents. Follow the steps given below to configure this feature:

1. After expanding the section, select the checkbox **OCR**.
2. In **Time out in seconds** field, define the maximum time (in seconds) eScan should consume to scan the document.
3. Select the checkbox **Save visual image** to save the scanned image on a server.

## Recipient Email Domain control

Enable this option to whitelist the domains through which content can be sent. It cannot be sent via email domains other than the listed ones.

## Customized Content List

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

## Printer

This section allows you to add tight restrictions on print activity within the network. This helps protecting the sensitive data present in each endpoint. To configure, follow the steps given below:

1. Enable the Printer DLP by selecting the provided checkbox.
2. Select the checkbox **Printer Block Print with Sensitive Content** to directly block the print command for the documents that involve sensitive content in visual form.  
(In case you do not want to block the print activity, add customized watermark on the same prints by following the steps below)
3. Select the checkbox **Enable adding watermark**.
4. From the **Watermark String** drop-down, select the preferred string that needs to be appeared on the prints. Alternatively, you can enter the string of your choice in the provided textbox.
5. In the Opacity field, define the opacity of the watermark from the value 16 to 192 where 16 being the lightest and 192 being the darkest watermark.
6. To block the applications from printing the files, select the checkbox **Block Applications from Printing**.
7. To blacklist the applications from printing, click on provided **Add** button.

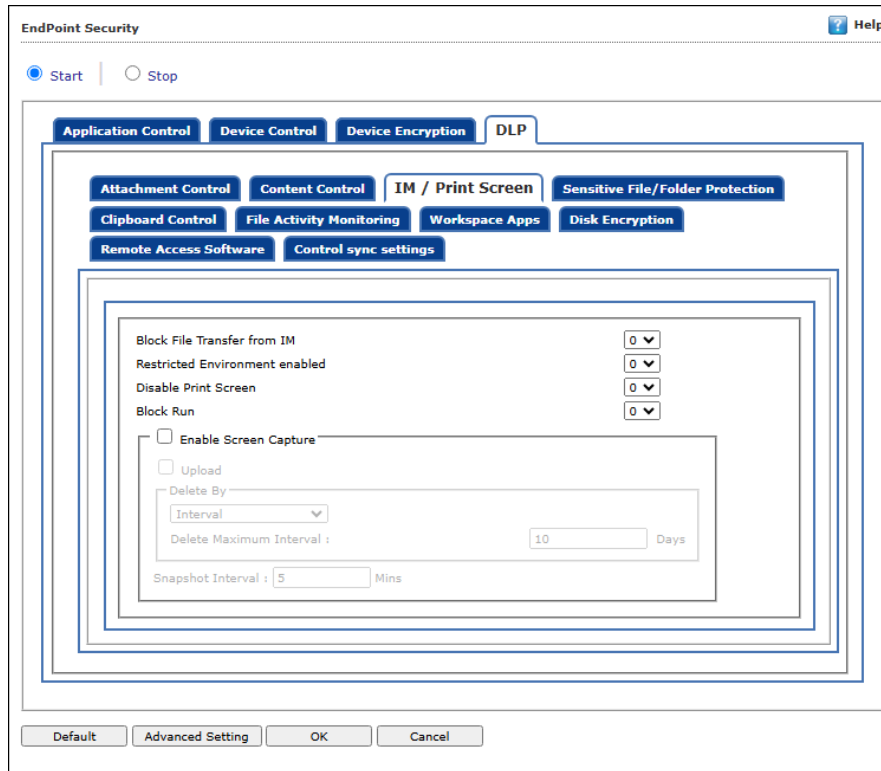
The 'Add Application name which will be blocked from printing' prompt appears

8. Enter the application name with the extension .exe and click on **Save**.  
The application will be blacklisted.
9. To whitelist the applications for printing, click on provided **Add** button.  
The 'Add Application name which will only be allowed to print' prompt appears
10. Enter the application name with the extension .exe and click on **Save**.  
The application will be whitelisted.
11. Select the checkbox **Enable Shadow Copy for printer allowed** to save the shadow copies for the prints that are allowed.



## IM / Print Screen

The IM (Instant Messenger) / Print Screen tab allows user to configure settings such as blocking file transfer via Instant messenger, disabling print screen, and screen capture options.



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

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

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

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

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

Select this option to enable/disable use of print screen feature.

### Block Run (1 = Enable/0 = Disable)

Select this option to enable/disable Windows Run (Win+R) command.

### Enable Screen Capture

Selecting this checkbox allow endpoint users to take screenshot.

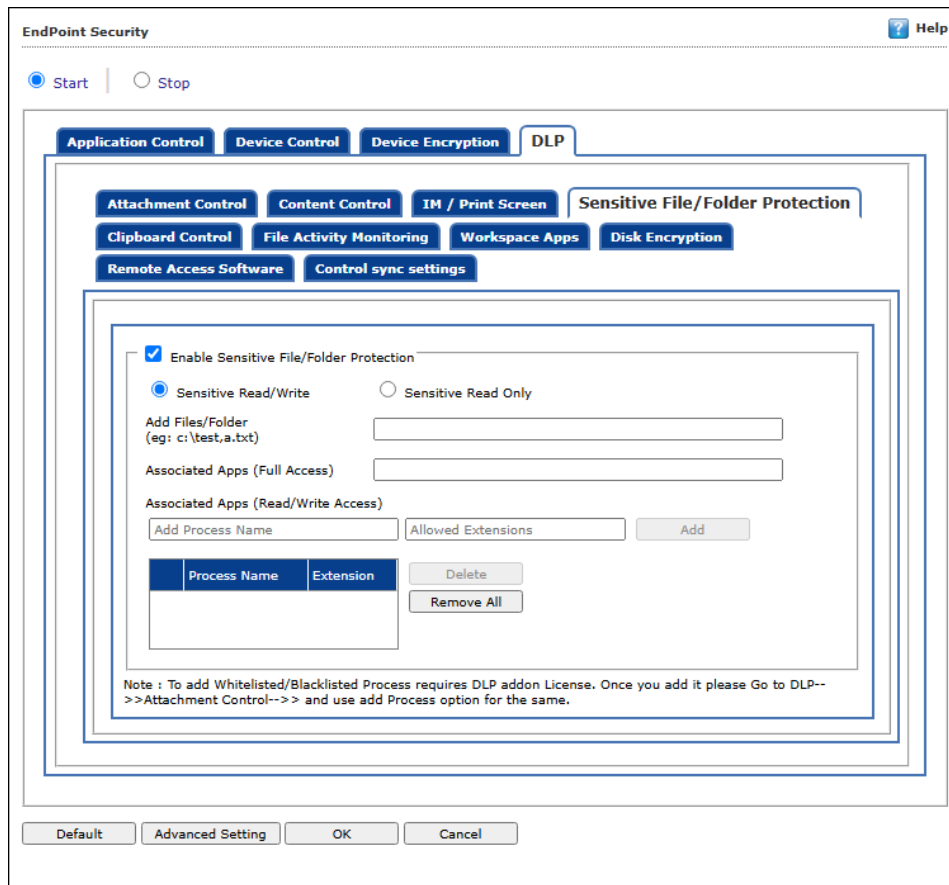
- **Upload:** Select this checkbox to upload the captured screen shots on server.
- **Delete By:** Select the appropriate option from drop down list to delete the screenshot.
  - Interval: If **Interval** option is selected, mention the maximum interval in days.
  - Size: If **Size** option is selected, mention the maximum size in Mb.
  - Both (Interval & Size): if **Both** option is selected, mention the maximum interval in days and maximum size in Mb.

### Snapshot Interval

It lets you define interval time in minutes to take snapshot of endpoint.

## Sensitive File/Folder Protection

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



### Enable Sensitive File/Folder Protection

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

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

### Add Folder or Add Files

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

### Add Exclude Process List

This option excludes entered process from accessing sensitive files/folders.

### Associated Apps (Full Access)

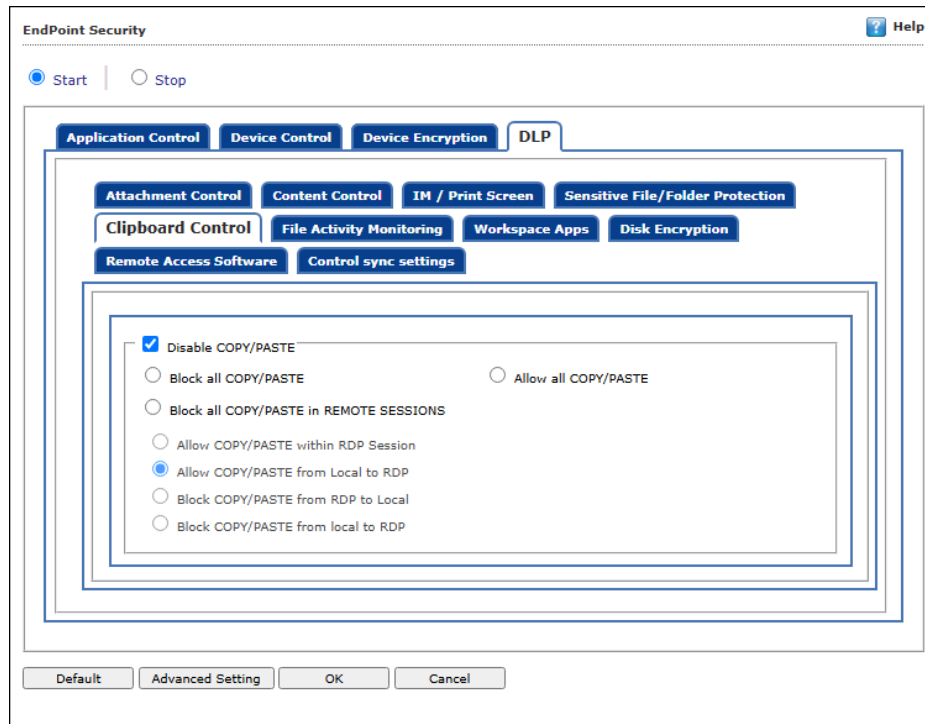
Enter the associated application name that has full access on sensitive files/folders.

### Associated Apps (Read/Write Access)

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

## Clipboard Control

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



### Disable COPY/PASTE

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

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

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

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

**Block all shares (clipboard, printer, localdrives etc.):** Select this option to block all shares which performs through the remote sessions (clipboard, printer, localdrives etc.).

**Allow clipboard control for local to RDP [Default]:** Select this option to allow clipboard control for local to RDP.

**Allow clipboard control for RDP to local:** Select this option to allow clipboard control for RDP to local.

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

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

## File Activity Monitoring

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

The screenshot shows the 'File Activity Monitoring' configuration window in EndPoint Security. The window has a title bar 'EndPoint Security' and a 'Help' icon. Below the title bar are 'Start' and 'Stop' radio buttons. The main content area is divided into several sections:

- Navigation Tabs:** Application Control, Device Control, Device Encryption, DLP, Attachment Control, Content Control, IM / Print Screen, Sensitive File/Folder Protection, Clipboard Control, File Activity Monitoring (selected), Workspace Apps, Disk Encryption, Remote Access Software, and Control sync settings.
- Monitoring Options:**
  - Enable File Activity Monitoring
  - Record Files Copied To USB / CD
  - Record Files Copied To Local
  - Record Files Copied To Network
  - Ignore System Drive
- Log Files Copy to User Network Path:**
  - Log Files Copy to User Network Path
  - Add User Path from connected Network:(Eg.\\192.168.0.96\external)
  - Input field with 'Add' and 'Delete' buttons.
- Force Include/Exclude Extensions:**
  - Add Force Include Extensions: (Input field, Add, Delete buttons)
  - Add Force Exclude Extensions: (Input field, Add, Delete buttons)
- System Drive and Folder Monitoring:**
  - Add System Drive Folder to monitor: (Input field, Add, Delete buttons)
  - Add Folders to Exclude: (Input field, Add, Delete buttons)
  - Predefined folders list: Contacts\, Desktop\, Documents\, Downloads\, Music\, Pictures\, Videos\, Dropbox\, Google Drive\, OneDrive\
- Shadow Copy:**
  - Enable Shadow Copy for files copied to USB
  - Shadow Copy folder path: (Input field)
- Notes:**
  - Note : Only Drive name or full UNC path is Allowed.Eg:
  - 1. "c:\\"
  - 2. "\\192.168.0.96\external\backup"

At the bottom of the window are buttons for 'Default', 'Advanced Setting', 'OK', and 'Cancel'.

**Enable File Activity Monitoring**

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

**Record Files copied To USB/CD**

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

**Record Files Copied To Local**

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

**Record Files Copied To Network**

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

**Ignore System Drive**

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

**Log Files Copy to User Network Path****Add User Path from connected Network: (E.g. \\192.168.X.XX\abc)**

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

**Add Force Include Extensions**

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

**Add Force Exclude Extensions**

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

**Add System Drive Folder to monitor**

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

**Add Folder to Exclude**

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

**Enable Shadow Copy for files copied to USB**

Select this checkbox to create shadow copies of files copied to USB devices. Enter the drive name or complete UNC path in the provided field where these shadow copies need to be saved.

## Workspace Apps

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

The screenshot shows the 'Workspace Apps' configuration window within the 'DLP' tab of the 'EndPoint Security' application. The window is titled 'EndPoint Security' and has a 'Help' icon in the top right corner. Below the title bar, there are radio buttons for 'Start' (selected) and 'Stop'. The main content area is divided into several sub-sections, each with a checkbox and a text input field. The sub-sections are: 'Block Gmail' (with 'Enter Google Domain' input), 'Block Microsoft Outlook' (with 'Enter Outlook Domain' and 'Outlook Tenant ID' inputs), 'Block Personal Microsoft Account' (with a sub-section for 'Block Microsoft Teams & Office 365 Account'), 'Advance Level Settings' (with 'Disabled Repair Profile Option for MS Outlook' checkbox), 'Block Dropbox Login' (with 'Allowed DropBox team name' input), 'Block Slack Login' (with 'Allowed Slack Workspace' and 'Allowed Slack Workspace Requester' inputs), 'Block Webex Login' (with 'Allowed Webex Domain' input), 'Block Zoom Login' (with 'Allowed Zoom Email Account/Domain' and 'Allowed Zoom Account ID' inputs), 'Block WeTransfer Login' (with 'Allowed WeTransfer Email Account/Domain' input), 'Block AutoDesk' (with 'Allowed AutoDesk Email Account/Domain' input), and 'Block BitBucket' (with 'Allowed BitBucket Email Account/Domain' input). Each input field has a red note below it: '(If left blank all Corporate [Service] Account will be allowed)'. At the bottom of the window, there are buttons for 'Default', 'Advanced Setting', 'OK', and 'Cancel'.

### Block Gmail

Select this checkbox to block the personal Gmail account.

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

### Block Outlook

Select this checkbox to block the personal Microsoft Outlook account.

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

### Block Dropbox Login

Select this checkbox to block the Dropbox login.

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

### Block Slack Login

Select this checkbox to block the Slack login.

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

### Block Webex Login

Select this checkbox to block the Webex login.

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

### Block Zoom Login

Select this checkbox to block the zoom login.

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

### Block WeTransfer Login

Select this checkbox to block the WeTransfer Login.

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

### Block AutoDesk

Select this checkbox to block AutoDesk login.

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

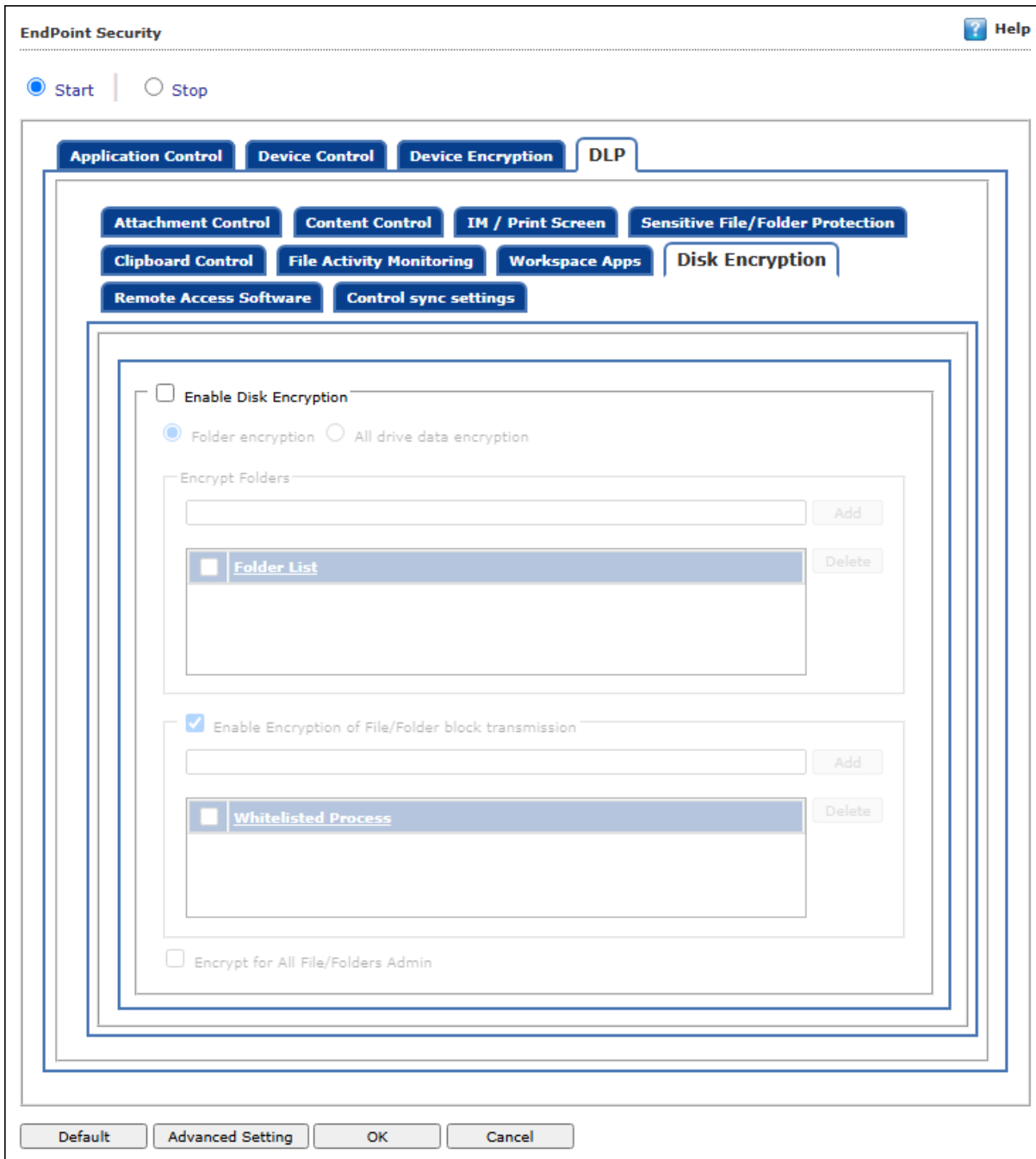
### Block BitBucket

Select this checkbox to block BitBucket login.

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

## Disk Encryption

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



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



## Folder Encryption

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

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

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

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

## All drive data encryption

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

## Enable Encryption of File/Folder block transmission

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


Follow the steps mentioned below to whitelist the processes:

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

The process will be whitelisted for transmitting the encrypted data.

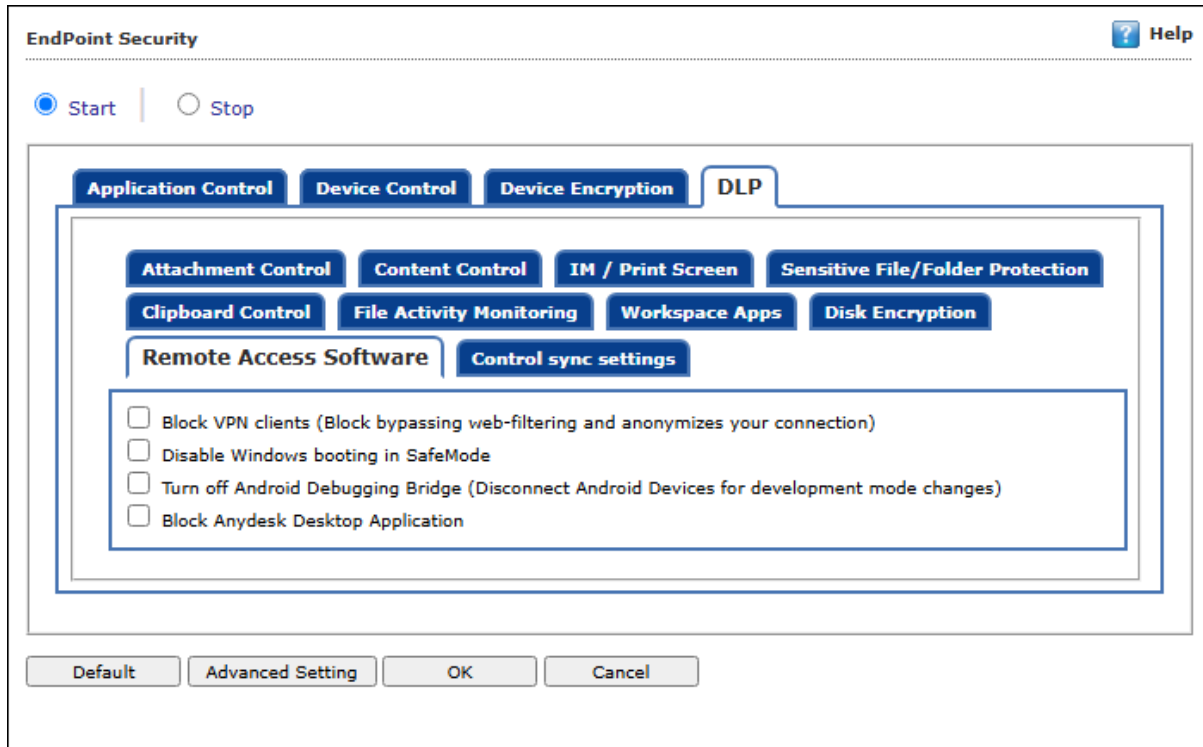
## Encrypt for All File/Folders Admin

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

 <b>NOTE</b>	<ul style="list-style-type: none"><li>• This option will encrypt only folders if <b>Folder encryption</b> option is selected.</li><li>• If the <b>All drive data encryption</b> is selected, it will encrypt folders as well as files.</li></ul>
--	--

## Remote Access Software

Organizations frequently use remote access software to perform specific tasks such as technical support sessions, system configuration, and installing workspace applications. This tab allows you to access the settings needed to define critical restrictions on the remote access software used on client endpoints.



These restrictions are essential to prevent endpoints from performing unauthorized activities initiated by an intruder or any other user. You can set these restrictions as explained below:

### **Block VPN clients (Block bypassing web-filtering and anonymizes your connection)**

It blocks VPN clients on endpoints so users cannot bypass web-filtering to access unauthorized content.

### **Disable Windows booting in SafeMode**

It restricts booting of Windows in SafeMode on an endpoint via remote session.

### **Turn off Android Debugging Bridge (Disconnect Android Devices for Development mode changes)**

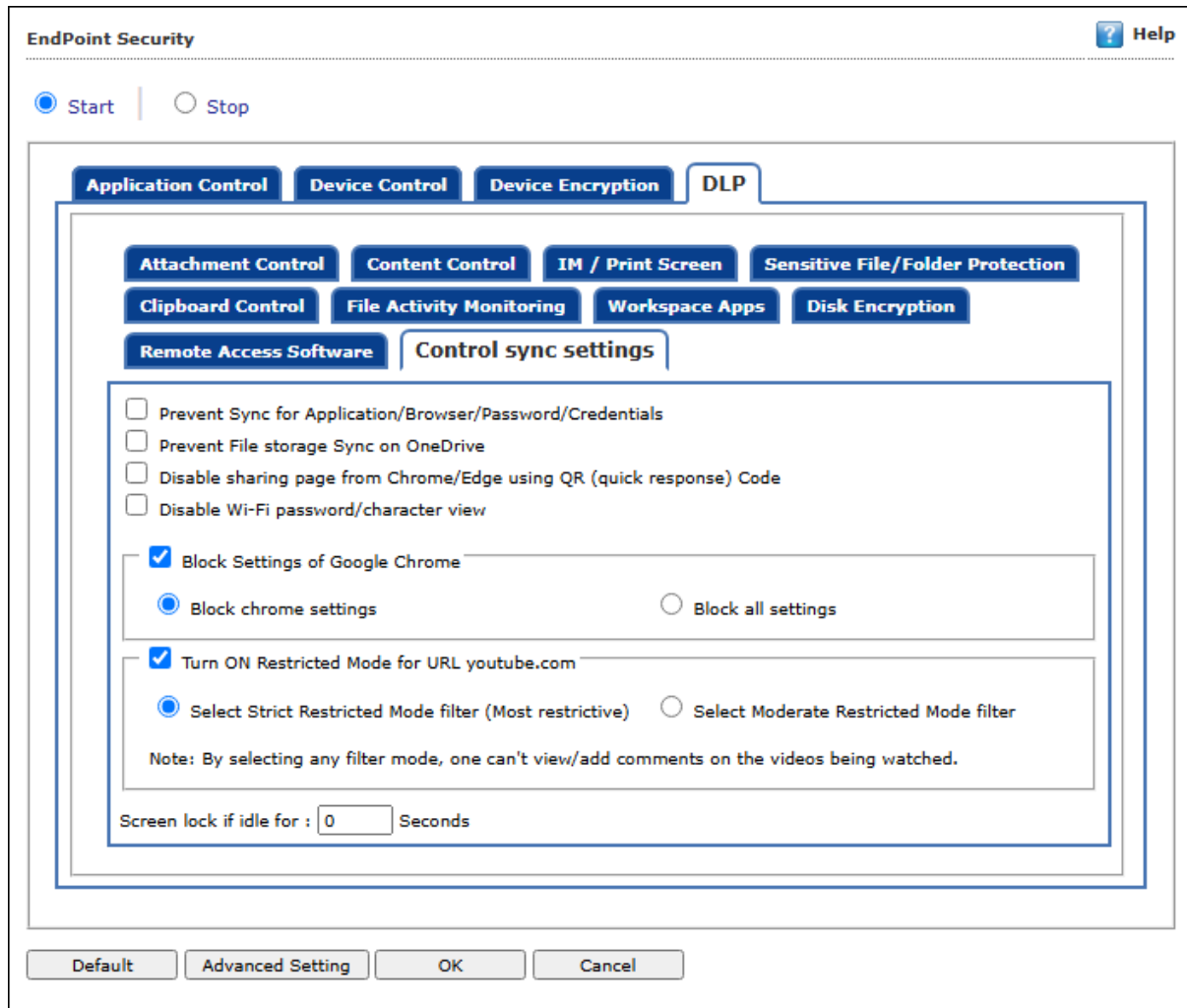
It denies the user to access Android device in its Development mode to avoid the misuse of Development mode features.

### **Block Anydesk Desktop Application**

It prevents launching of Anydesk Desktop Application on an endpoint. Only corporate Anydesk account will be allowed use.

## Control sync settings

Controlling sync settings in corporate network is essential for safeguarding data, maintaining network performance, and ensuring compliance with security and privacy regulations. It enables organizations to prevent unauthorized data sharing, protect user privacy, and optimize network resources.



As an administrator or security team, you can provide greater network security by retaining control over where and how data is accessed and synced. Below are the options you can configure:

### Prevent Sync for Application/Browser/Password/Credentials

Select this checkbox to disable synchronization activity for application/browser/password/credentials on a client endpoint.

### Prevent File storage Sync on OneDrive

Select this checkbox to disable synchronization activity for storing files on OneDrive.

### Disable sharing page from Chrome/Edge using QR (quick response) Code

Select this checkbox to disable the page sharing using QR Code from the browsers (Chrome and Edge) installed on client machines.

### Disable Wi-Fi password/character view

Select this checkbox to prevent viewing of Wi-Fi password/characters.

### Block Settings of Google Chrome

- **Block chrome settings:** Select this option to restrict users from accessing the Chrome settings.
- **Block all settings:** Select this option to restrict users from configuring Chrome settings like appearance and notifications settings.

### Turn ON Restricted Mode for URL youtube.com

- **Select Strict Restricted Mode filter (Most restrictive):** It restricts adult videos that may contain pornography, violence, nudity, and other videos that are sensitive in nature. It is applicable for G Suite (corporate account) users.
- **Select Moderate Restricted Mode filter:** Select this option if you don't want the restriction to be extremely strict. This mode filters out less videos than the Strict restricted mode.

**NOTE** If any of the Youtube restriction modes is selected, users cannot view/add comments on the videos being watched.

The option **Screen lock if idle for** allows you to define auto screen lock time (in seconds) for client computers. Define the value of seconds in provided field to enable this functionality.

## Advanced Setting

Clicking **Advanced Setting** displays additional 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="text"/>
<input type="checkbox"/>	Allow Network Printer	1 ▾
<input type="checkbox"/>	Whitelisted Network Printer list(Comma Separated)	<input type="text"/>
<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)	<input type="text"/>

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Select this option allow/block system files execution events.

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

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

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

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

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

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

**Whitelisted WIFI SSID (Comma Separated)**

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

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

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

**Whitelisted Network Printer list (Comma Separated)**

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

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

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

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

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

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

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

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

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

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

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

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

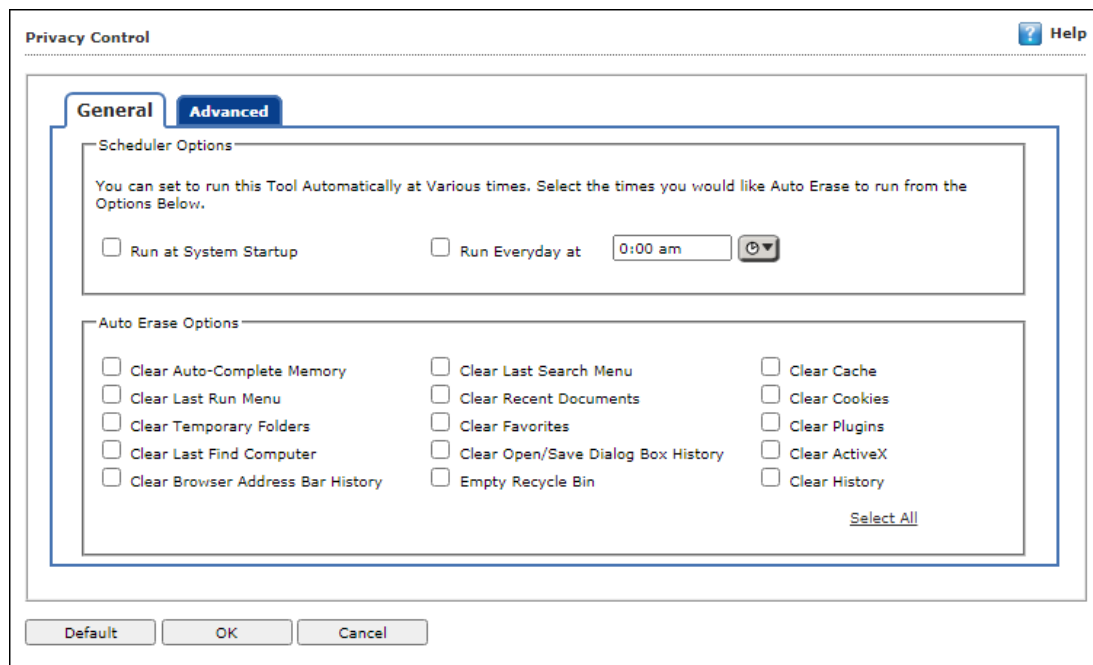
Select this option to allow/block ask password for whitelisted devices.



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

## Privacy Control

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



### General

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

#### Scheduler Options

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

#### Run at System Startup

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

**Run 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 checkbox, Privacy Control clears all this information from the computer.

**Clear Last Run Menu**

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

**Clear Temporary Folders**

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

**Clear Last Find Computer**

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

**Clear Browser Address Bar History**

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

**Clear Last Search Menu**

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

**Clear Recent Documents**

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

**Clear Favorites**

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

**Clear Open/Save Dialog Box History**

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

**Empty Recycle Bin**

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

**Clear Cache**

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

### Clear Cookies

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

### Clear Plugins

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

### Clear ActiveX

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

### Clear History

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

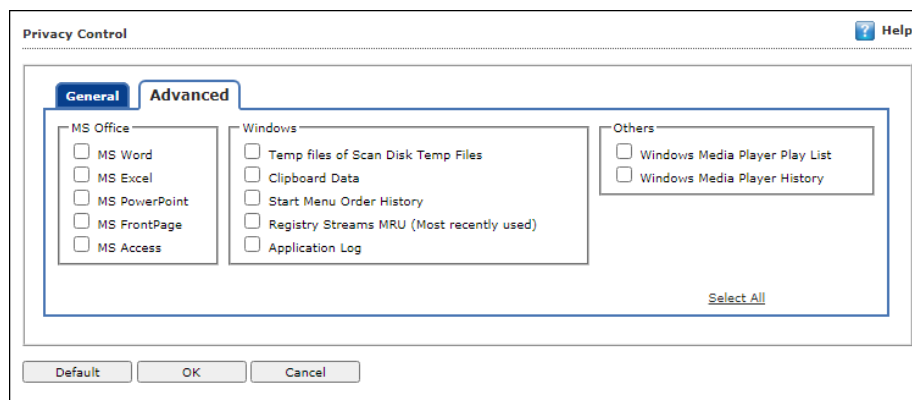
In addition to these options, the **Auto Erase Options** section has below option as well.

### Select All/ Unselect All

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

## Advanced

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



### MS Office

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

### Windows

The respective unwanted files like temp files will be cleared.

### Others

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

### Select All/ Unselect All

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



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

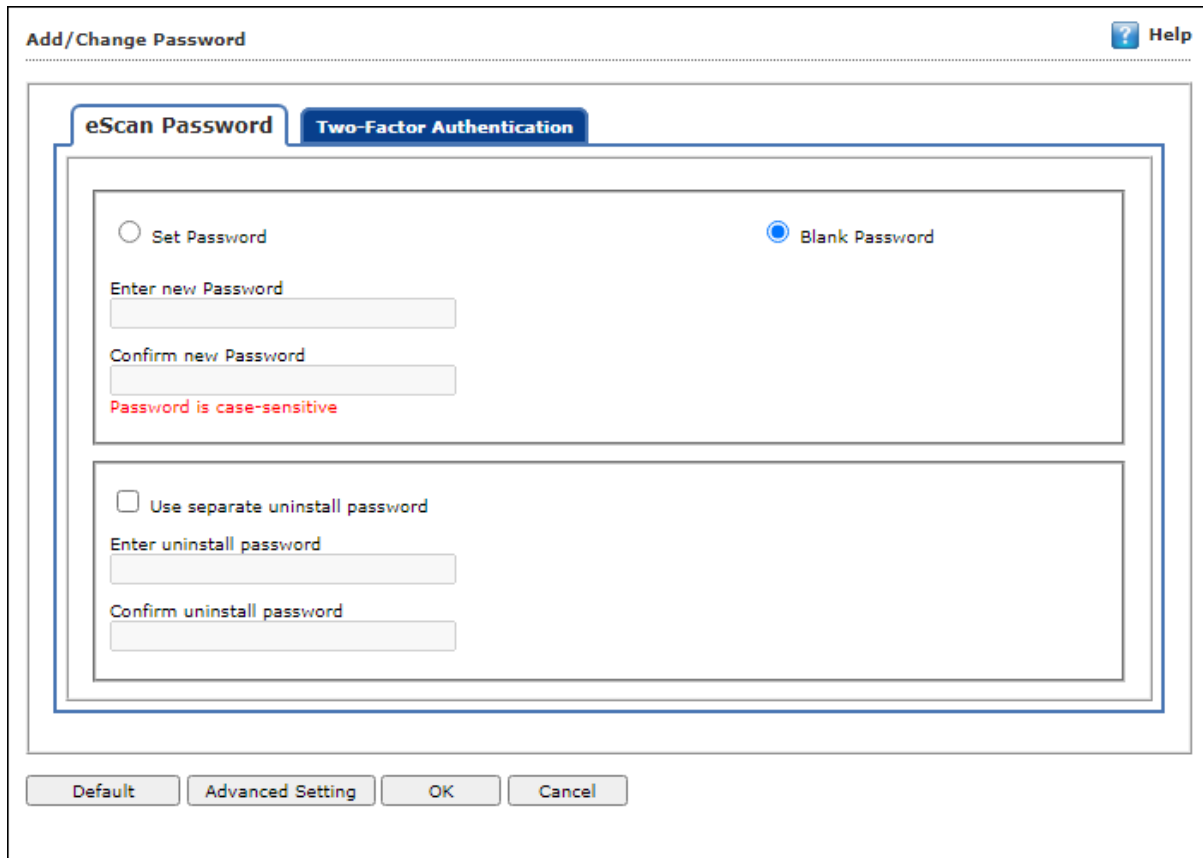


## Administrator Password

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

## eScan Password

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



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**.



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

## Two-Factor Authentication (requires additional license)

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

system login password. So, even if an unauthorized person knows your system credentials, the 2FA feature secures a system against unauthorized access.

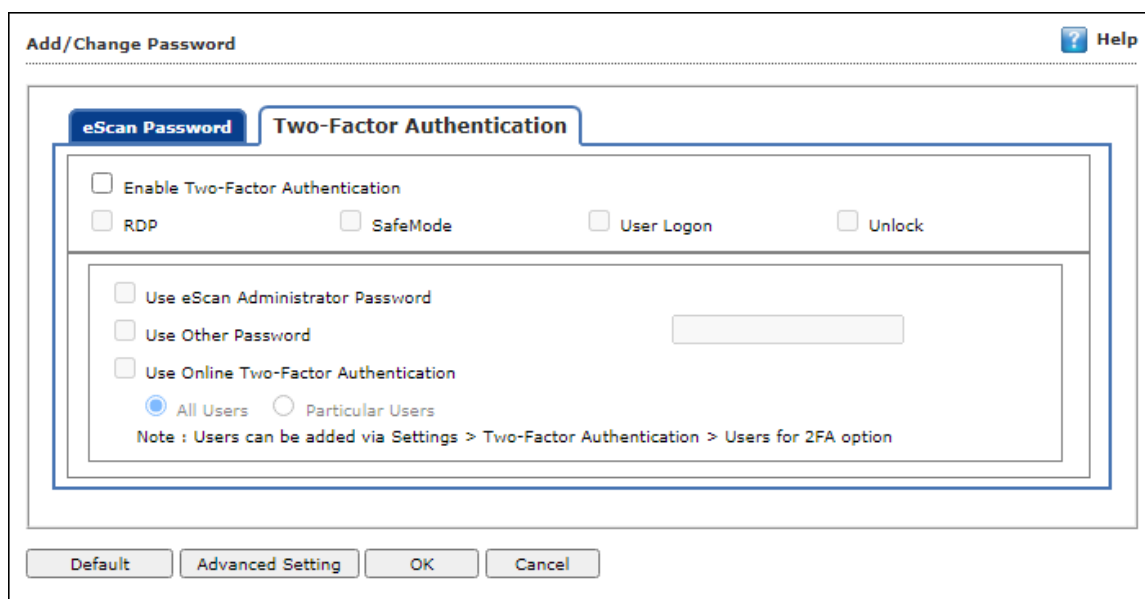
With the 2FA feature enabled, the system will be protected with basic system login and eScan 2FA. After entering the system credentials, eScan Authentication screen will appear as shown in the below image. The personnel will have to enter the 2FA passcode to access the system. A maximum of three attempts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

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

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

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

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



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

## Login Scenarios

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

### RDP

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

### Safe Mode

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

### Local Logon

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

### Unlock

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

### Password Types

If the policy is applied to a group, the 2FA passcode will be same for all group members.

The 2FA passcode can also be set for specific computer(s).

You can use following all password types to log in:

#### Use eScan Administrator Password

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

#### Use Other Password

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

#### Use Online Two-Factor Authentication

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

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



#### NOTE

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

To use this feature, follow the steps given below:

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

Forward this TOTP to personnel for login.

## Advanced Setting

Clicking **Advanced Setting** displays Advance setting.

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

Ok

### **Enable Automatic Download (1 = Enable/0 = Disable)**

It lets you Enable/Disable Automatic download of Antivirus signature updates.

### **Enable Manual Download (1 = Enable/0 = Disable)**

It lets you Enable/Disable Manual download of Antivirus signature updates.

### **Enable Alternate Download (1 = Enable/0 = Disable)**

It lets you Enable/Disable download of signatures from eScan (Internet) if eScan Server is not reachable.

### **Set Alternate Download Interval (In Hours)**

It lets you define time interval to check for updates from eScan (Internet) and download it on managed computers.

### **Disable download from Internet for Update Agents (1 = Enable/0 = Disable)**

Selecting this option lets you disable Update Agents from downloading the virus signature from internet.

### **Stop Auto change for download from Internet for Update Agents (1 = Enable/0 = Disable)**

This option is used when an Update Agent didn't find the primary server to download virus signature, then it tries to get virus signature from internet, so to stop Update Agent from downloading from internet this option is to be set to 1(one).

### **Enable Download of Anti-Spam update first on clients (1 = Enable/0 = Disable)**

Normally while updating a system for virus signatures, we first download the anti-virus signature and then anti-spam signature. This option lets you first download Anti-spam updates on clients.

### **No password for pause protection**

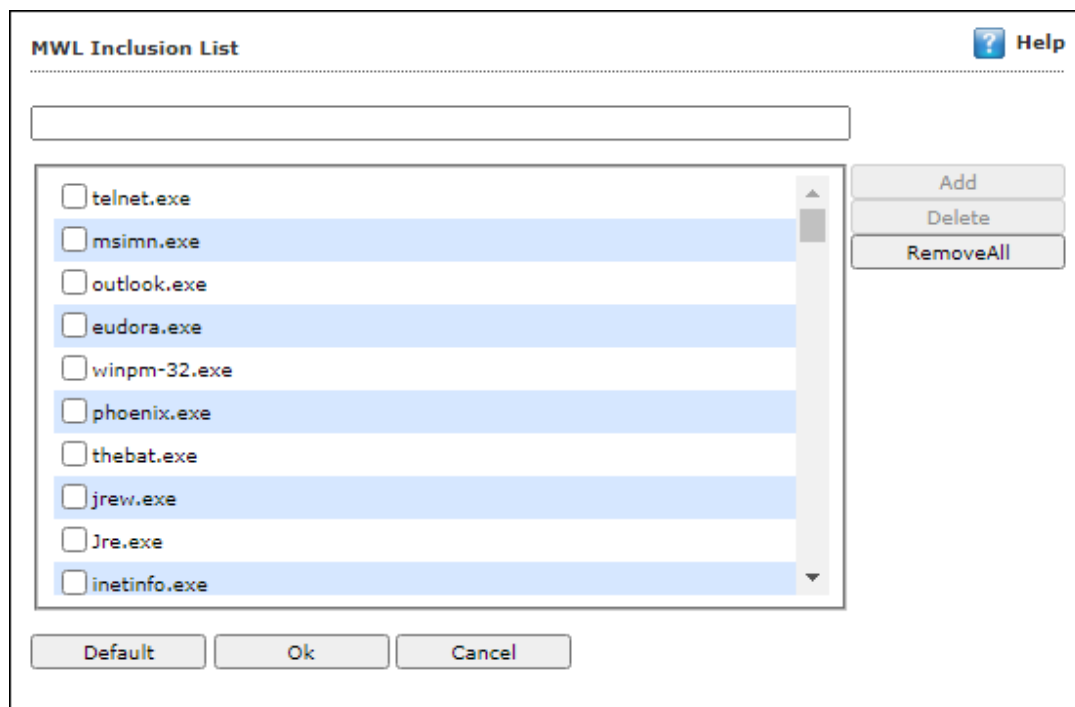
Selecting this option lets you pause the eScan protection without entering password.

## MWL (MicroWorld WinSock Layer)

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

## MWL Inclusion List

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



### 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.

### 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,

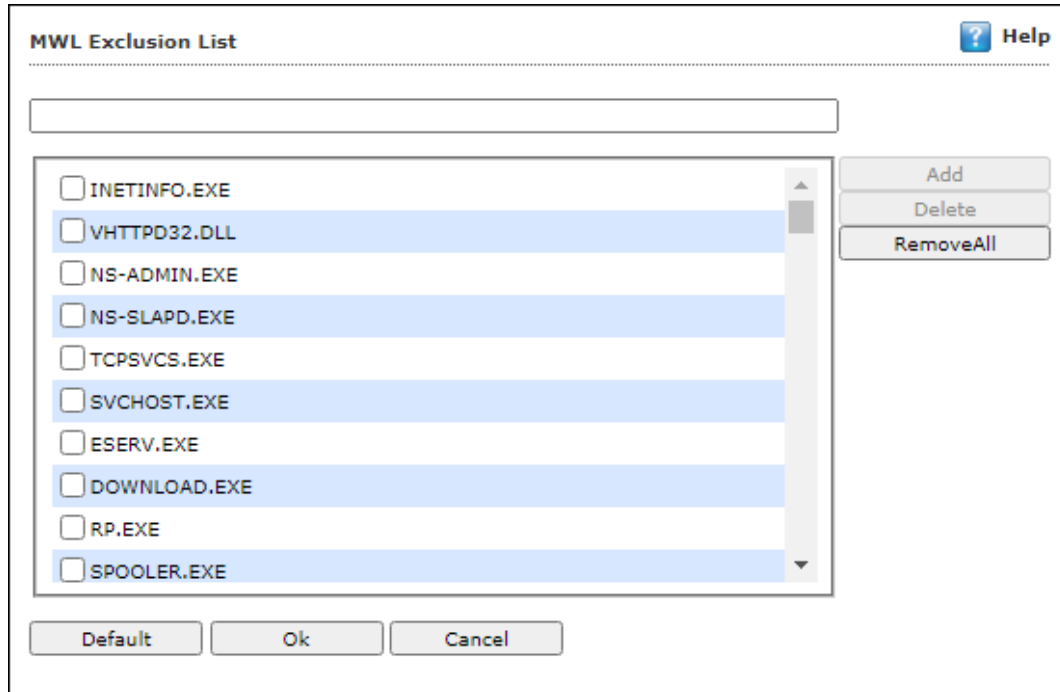
1. Click **Remove All**.  
A confirmation prompt appears.
2. Click **OK**.  
All executable files will be removed from the Inclusion List.



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

## MWL Exclusion List

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



### 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 will be added to the Exclusion List.

### Deleting files from Exclusion List

To delete executable files from the Exclusion List,

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

### Removing all files from Exclusion List

To remove all executable files from the Exclusion List,

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



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

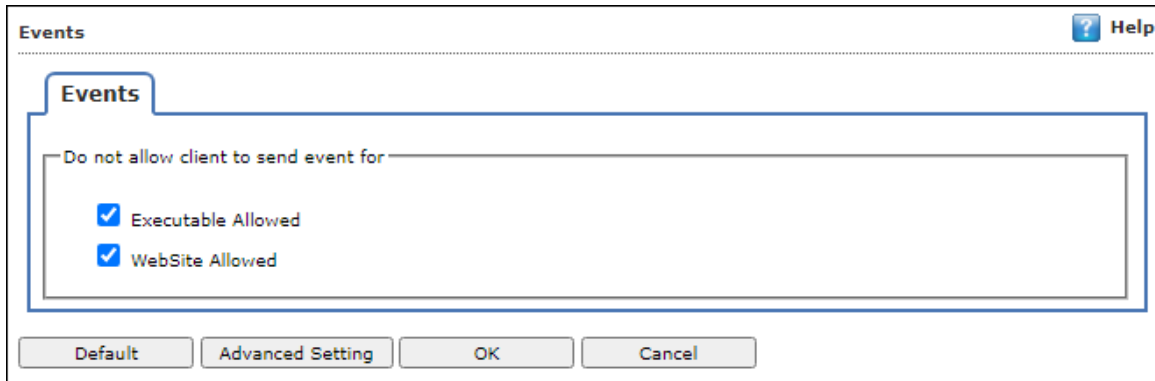
# Notifications and Events

## Events

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

- Executable Allowed
- Website Allowed

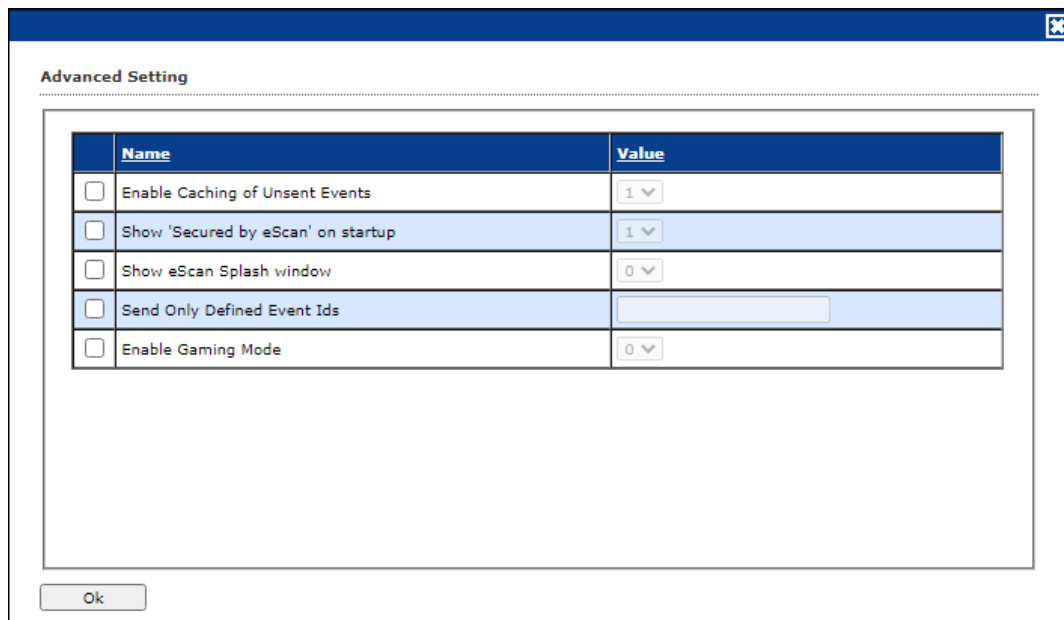
By default, all events are selected.



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

## Advanced Settings

Clicking **Advanced Setting** displays Advance setting.



### Enable Caching of Unsent Events (1 = Enable/0= Disable)

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

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

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



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

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

**Send Only Defined Event Ids**

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

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

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

## Schedule Update

The Schedule Update lets you schedule eScan database updates.

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

-OR-

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

## Advanced Settings

Clicking **Advanced Setting** displays Advance setting.

	Name	Value
<input type="checkbox"/>	Set bandwidth limit for download (in kb/sec)	
<input type="checkbox"/>	Retry schedule download (Default retry interval is 15 minutes)	15

### Set bandwidth limit for download (in kb/sec)

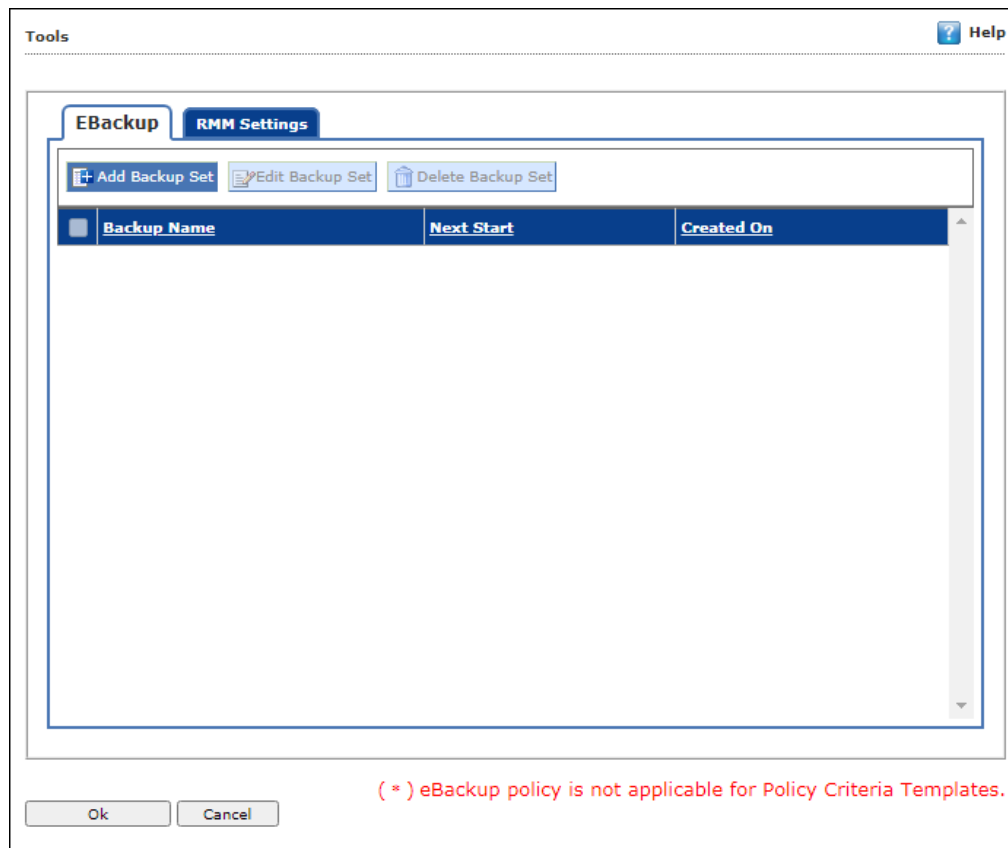
It lets you define bandwidth limit for download on managed computers.

### Retry schedule download (Default retry interval is 15 minutes)

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

## Tools

The Tools lets you configure EBackup and Remote Monitoring Management (RMM) Settings.



### EBackup (requires additional license for Network storage)

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

With eBackup tab you can:

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

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

### Job

This tab you can schedule the eBackup option.

### Active

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

### Name

Enter a name for an eBackup task.

### Scheduler

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

### Date and time

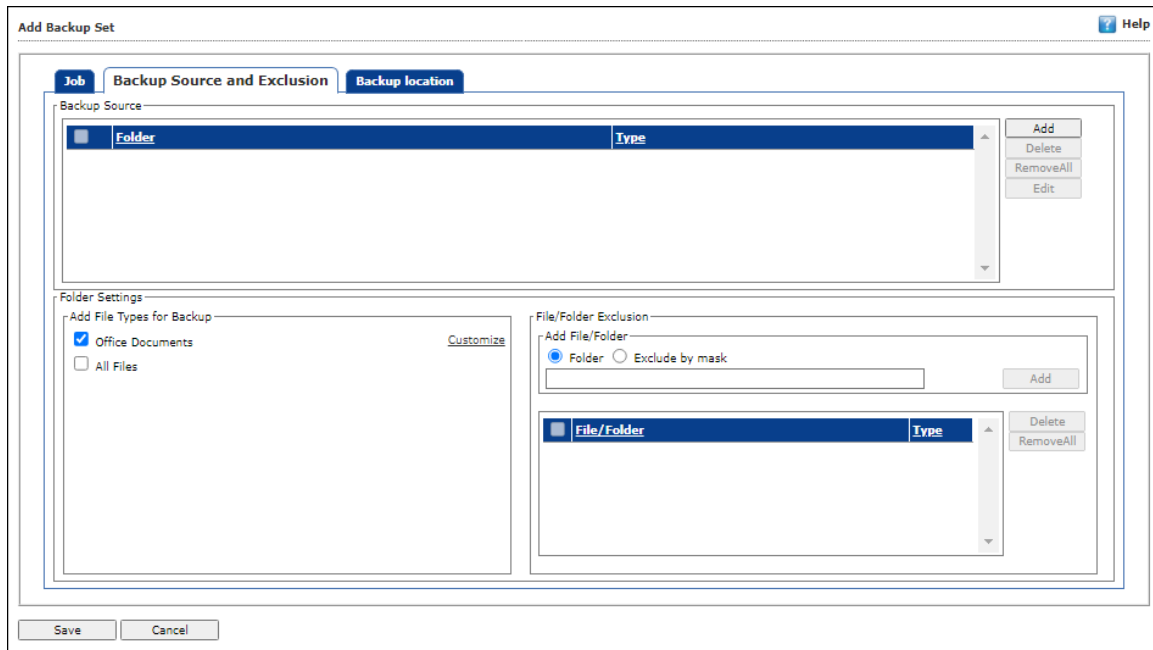
This option allows you select the day, time, and date for running the scheduled eBackup task.

### Set Restore Password

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

## Backup Source and Exclusion

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



### Backup Source

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



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

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

### Folder Settings

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

### File/Folder Exclusion

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

## Backup Location

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

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

### Local/Network

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

	Network storage for 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.

## Google Drive

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

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

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

## DropBox

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



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



## OneDrive

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

### NOTE

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

## Add Backup Set

To create a Backup Set,

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

### NOTE

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

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

The Backup Set will be created.

### NOTE

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

## Edit Backup Set

To edit a Backup Set,

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

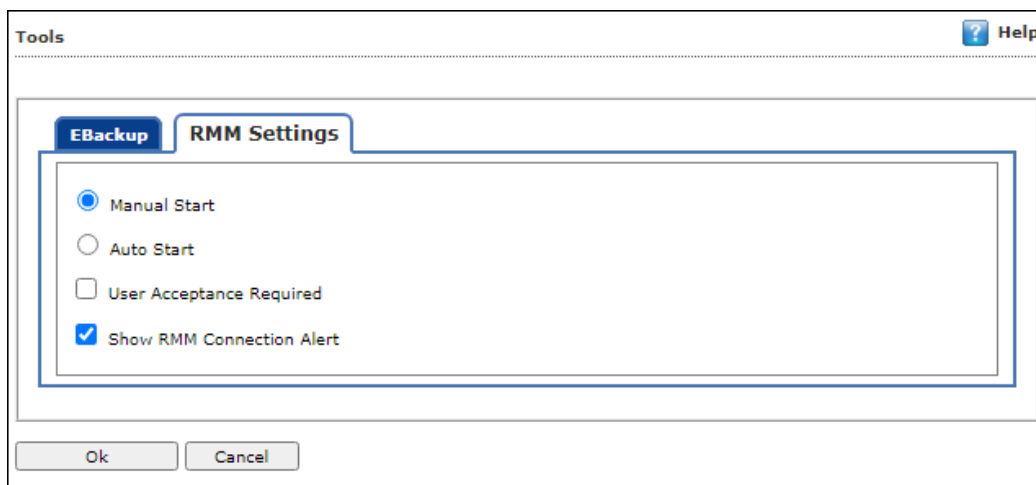
## Delete Backup Set

To delete a Backup Set,

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

## RMM Settings (requires additional license)

The RMM settings let you configure default connection settings for connecting to client computers.



**Manual Start [Default]:** If this option is selected by default, 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 checkbox 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 [Default]:** If this checkbox 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.

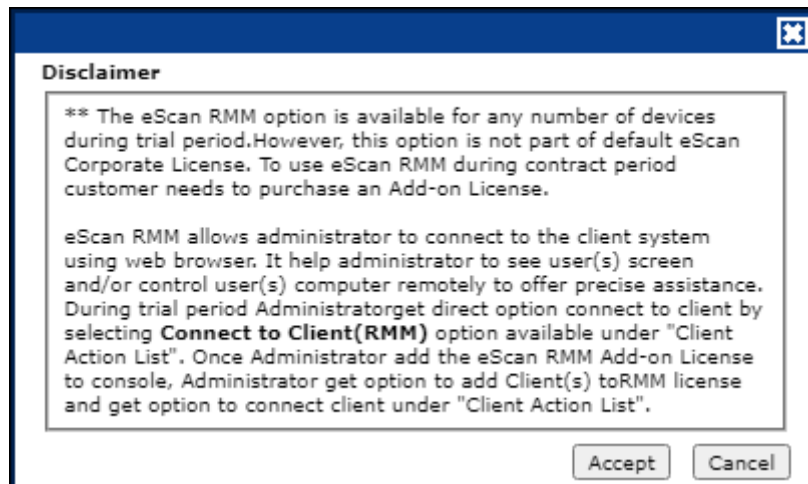
## RMM - Manual Start

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**.



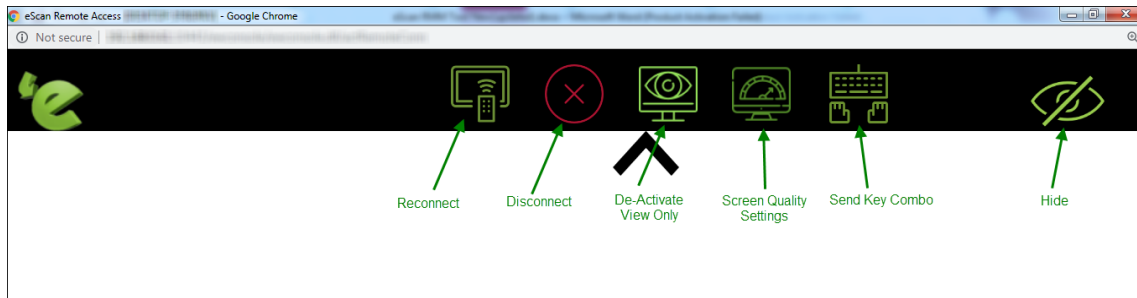
2. After the client endpoint user has clicked **Start eScanRMM**, select the target endpoint and then click **Client Action List > Connect to Client (RMM)**.  
Following disclaimer appears.



  
**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.

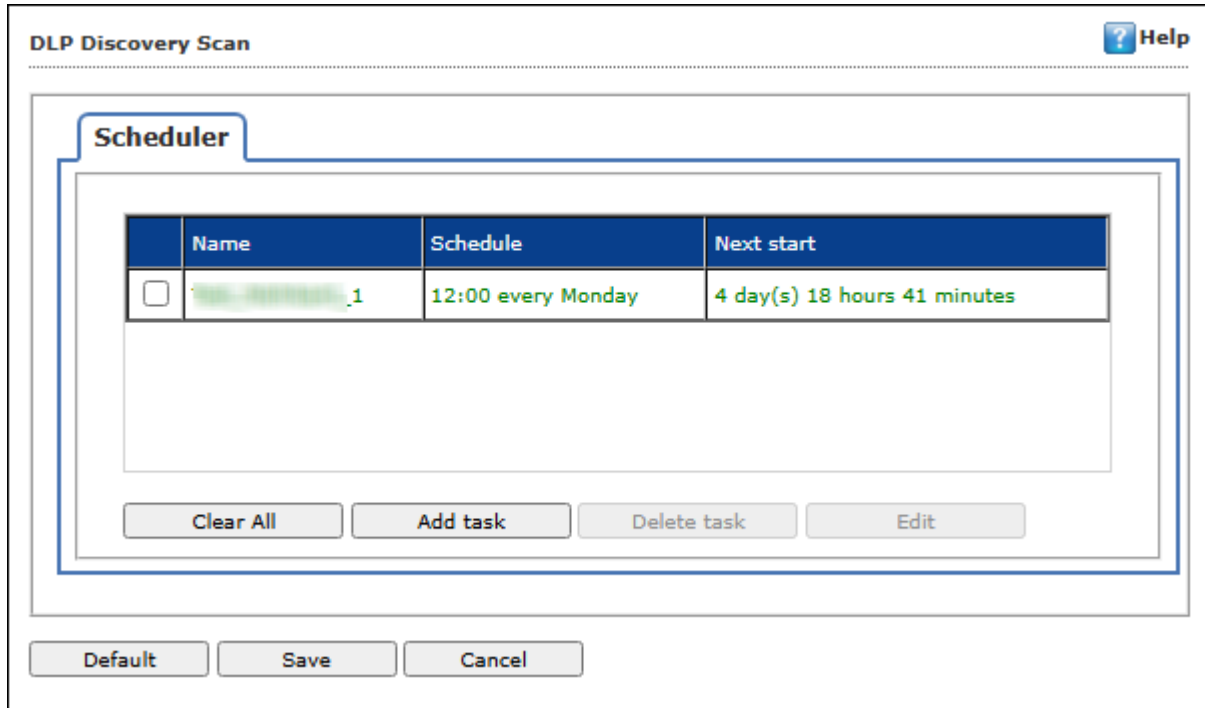
1. Go to **Managed Computers**, select the target endpoint and then click **Client Action List > Connect to Client (RMM)**.  
RMM disclaimer appears.
2. Read the disclaimer thoroughly and then click **Accept**.  
Your default browser opens eScan Remote Access window (Google Chrome, Mozilla Firefox, MS Edge, etc.)

After you are done performing an activity, click the **Disconnect** icon to end remote connection.

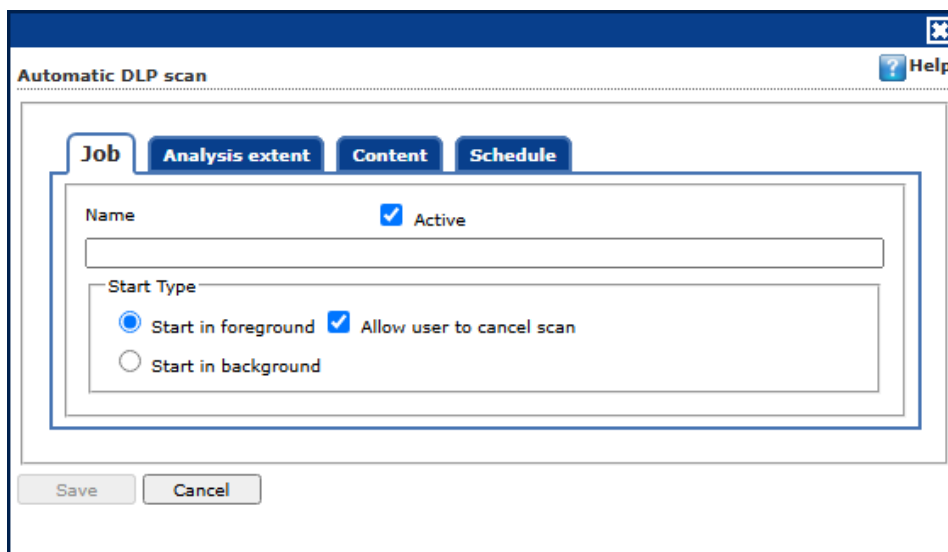
 <b>NOTE</b>	To get detailed information about RMM feature, <a href="#">click here</a> .
--	---

## DLP Discovery

The policy Data Discovery allows you to locate and manage sensitive data across an organization’s network and endpoints. It scans and generates a detailed report of your sensitive data present in the endpoints. This helps you take informed decisions regarding the same and ultimately mitigate risks associated with data breaches. Configure the policy using below steps:

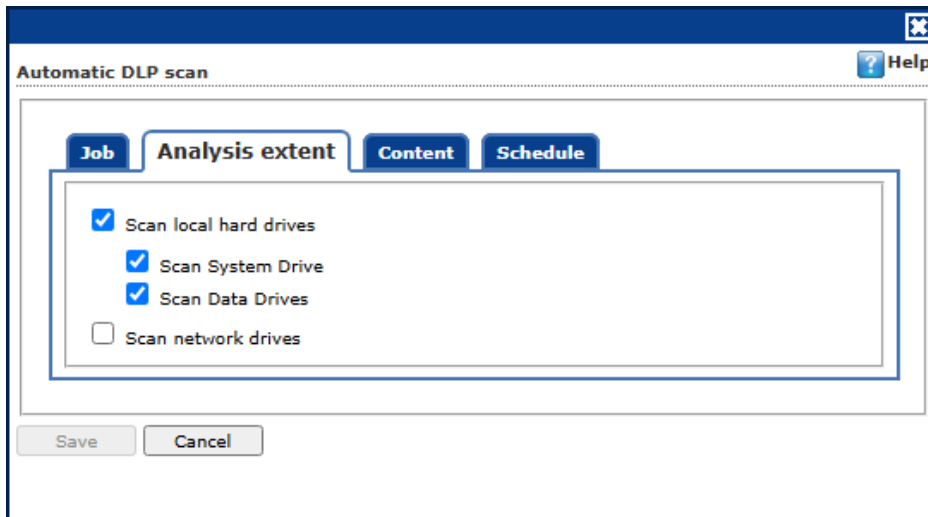


1. In the DLP Discovery Scan window, click on **Add task** button to create new scanning job.  
The Automatic DLP scan window opens

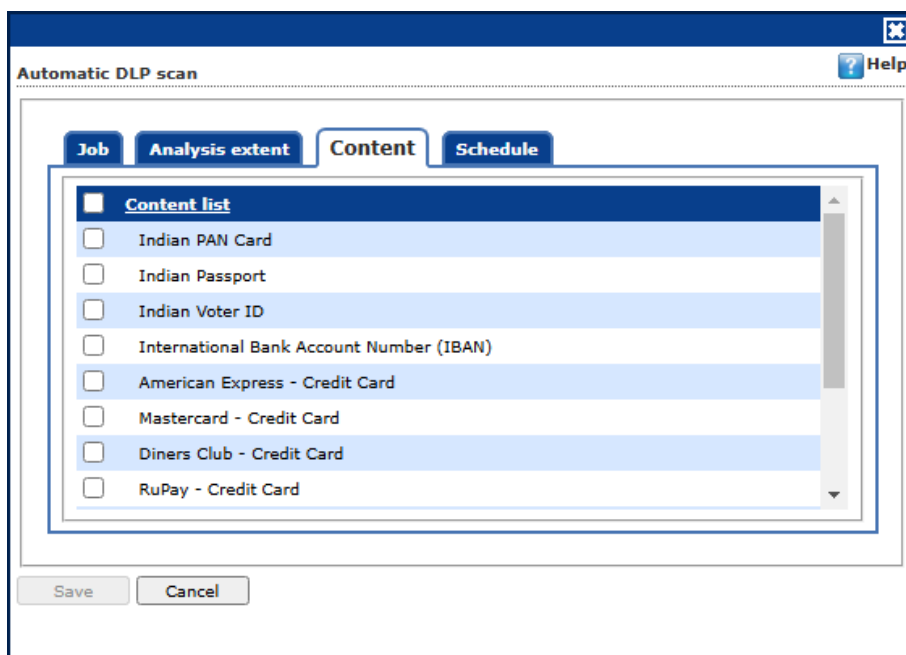


2. Under the Job tab, select the **Active** checkbox to enable the job status and ensure execution according to the defined schedule(s). If left unchecked, the job will not be executed.
3. Enter the job name in the provided field.

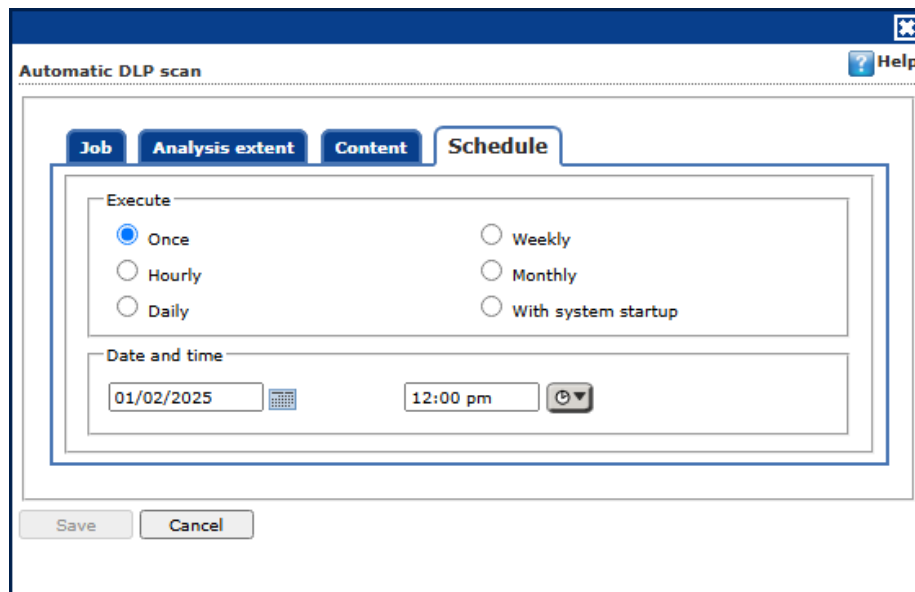
4. Under the Start Type section, select the option **Start in foreground** to initiate scanning in the foreground or select **Start in background** to start scanning in background on a target endpoint(s).
5. Select the checkbox **Allow user to cancel scan** if you want users to cancel the scan if required.



6. Under the Analysis extent tab, select target locations for scanning from system drive, data drives, or network drives.



7. Under the Content tab, select the content types you want to scan.



8. Under the Schedule tab, select the scan execution option from once, hourly, daily, weekly, monthly, or with system startup.
9. Define the date and time for scanning to initiate.
10. Click on **Save** to save the policy.

DLP Discovery Scan window has below buttons apart from Add task button:

- **Clear All:** This removes all the jobs from the list.
- **Delete task:** This deletes the selected jobs from the list.
- **Edit:** This allows you to view and make changes in the existing jobs.

# Configuring eScan Policies for Linux and Mac Computers

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

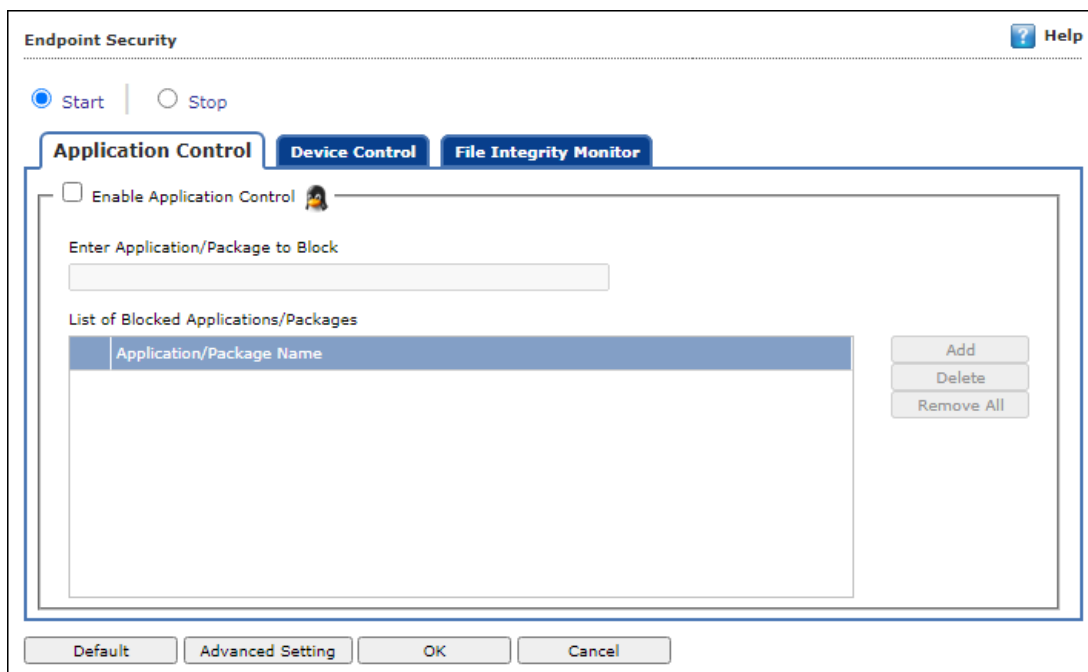
	Icons next to every module displays that the settings are valid for the respective operating systems only.
	It lets you define settings for Scanning; you can also define action to be taken in case of an infection. It also lets you define the number of days for which the logs should be kept as well as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

## 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. Allows to monitor and detect the modifications in the files using File Integrity Monitor feature.

## Application Control

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



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

### Enable Application Control

Select this checkbox to enable the Application Control feature.



### Enter Application/Package to block

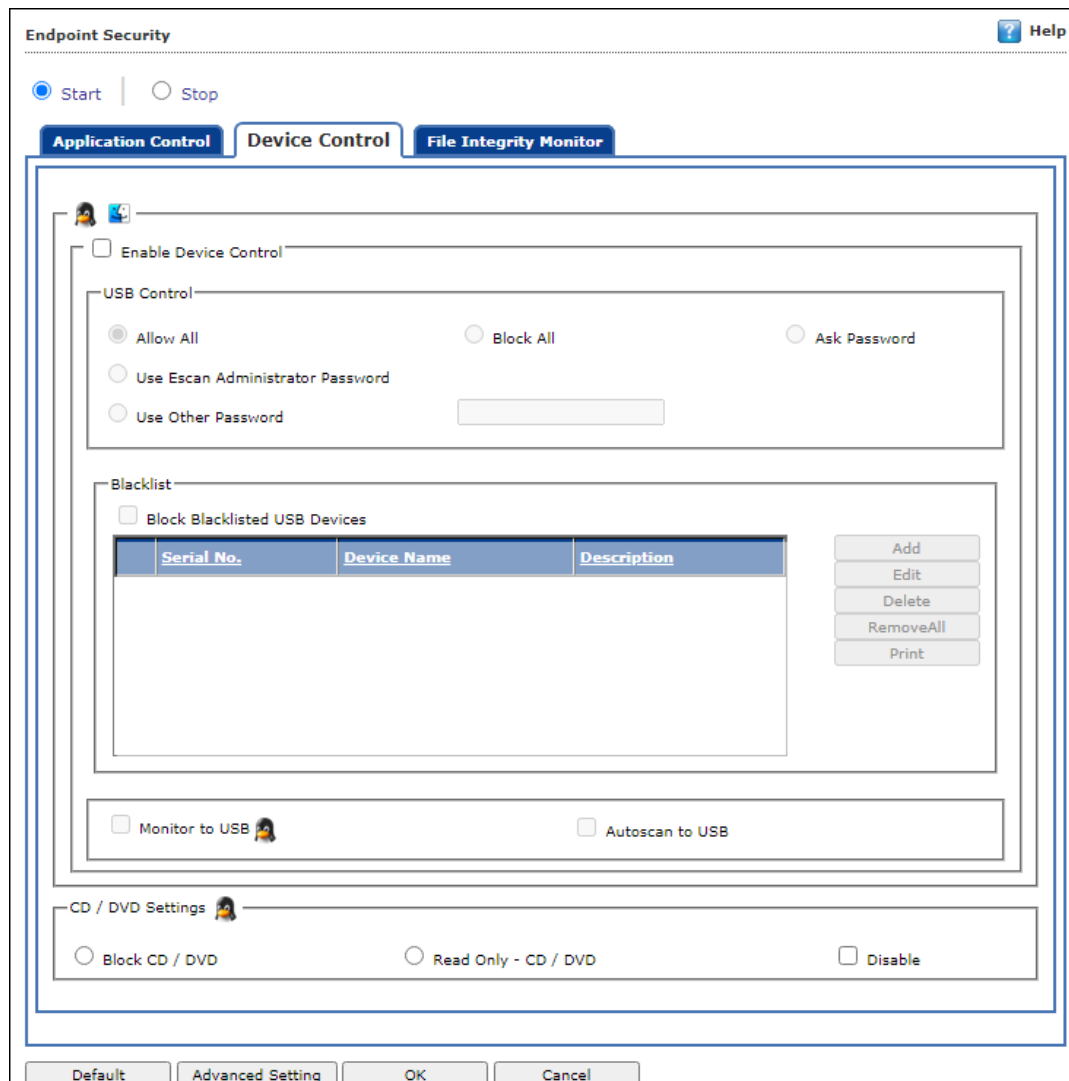
Enter the application or package name to add them in the list of application/packages blocked. Click **Add**. The application will be blocked.

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

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

## Device Control

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



### Enable Device Control

Select this checkbox to configure the Device Control settings.

### USB Control

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

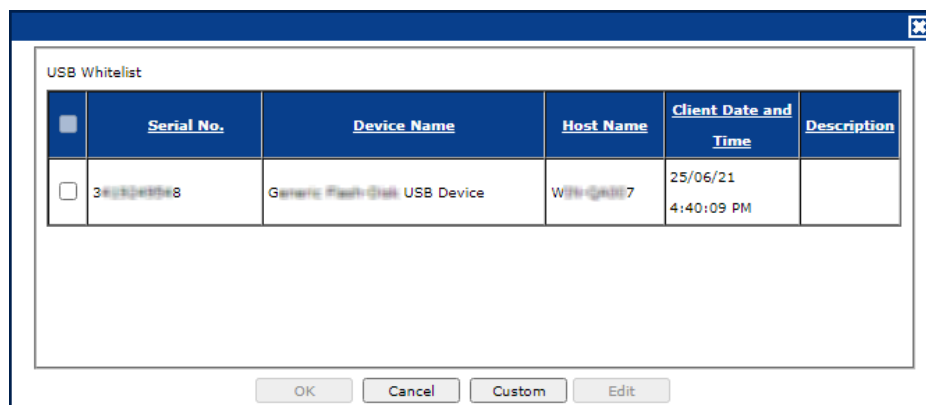
- **Allow All:** Select this option to allow all the connected USB devices.
- **Block All:** Select this option to block all the connected USB devices.

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

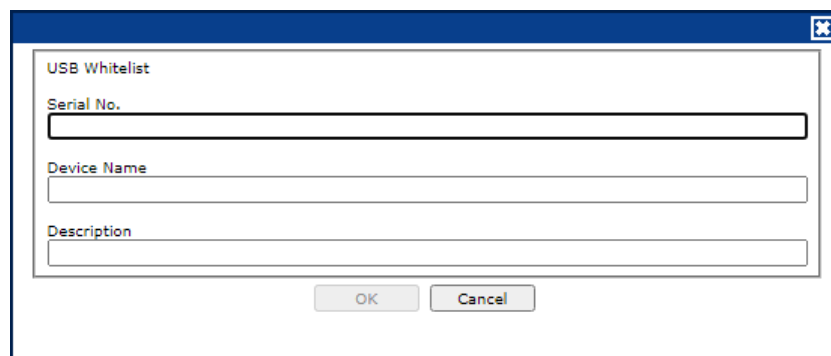
### Blacklist

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

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



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

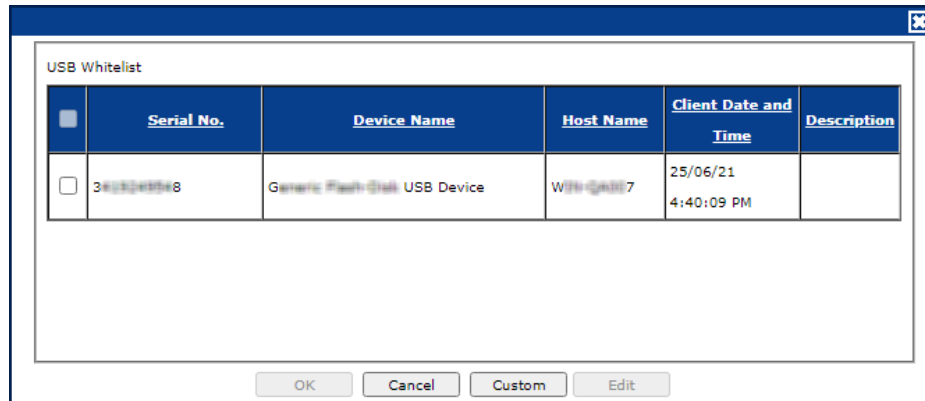


- **Edit:** Click **Edit** to edit the details of the USB devices.
- **Delete:** Select the USB device and click **Delete** to remove the device from the list.
- **Remove All:** To remove all the USB devices from the list, click **Remove All**.
- **Print:** This will print all the USB devices in the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

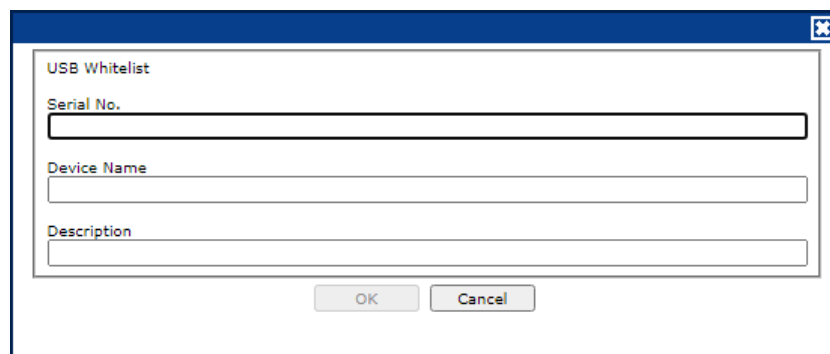
### Whitelist

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

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



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



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

### Monitor to USB

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

### Autoscan to USB

Select this option to auto-scan all the USB devices connected to the endpoints.

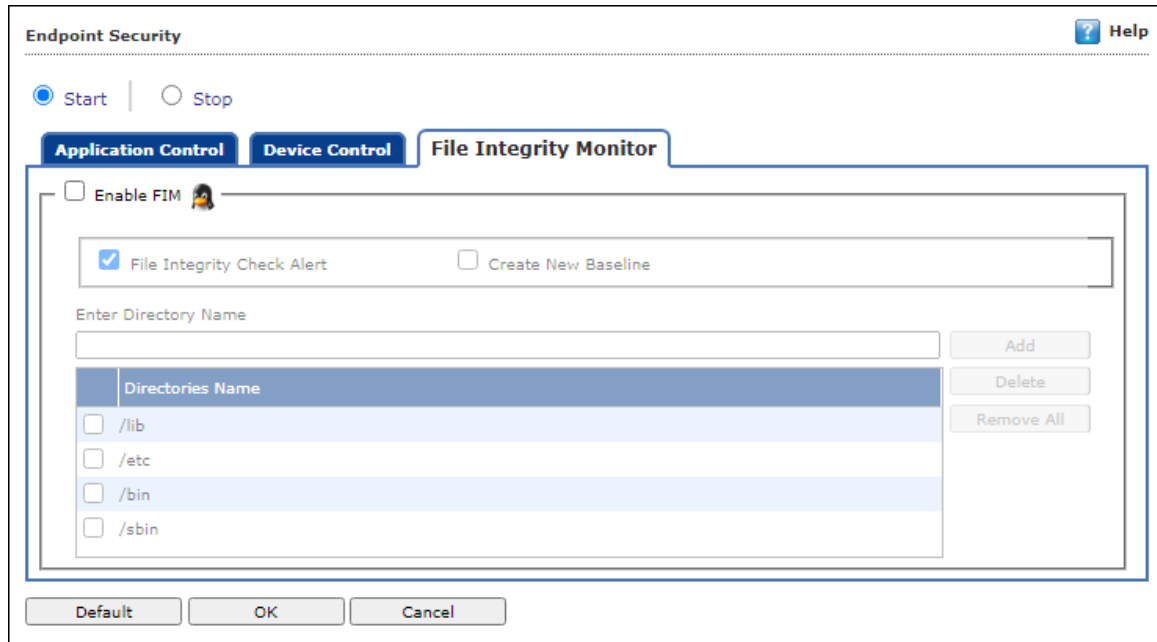
### CD/DVD Settings

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.

## File Integrity Monitor

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



### Enable FIM

Select this checkbox to enable the File Integrity Monitoring.

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

### Enter Directory Name

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

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

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



#### NOTE

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

## Schedule Update

This module lets you schedule the updates for Linux computers.

**Schedule Update** ? Help

Automatic Download

Start at: 12:00 pm [dropdown] Every: 1 hours(s)

Schedule Download

Once  Weekly  
 Hourly  Monthly  
 Daily

Date and time

Month : 1 Date : 1 12:00 AM [dropdown]

Default Ok Cancel

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

OR

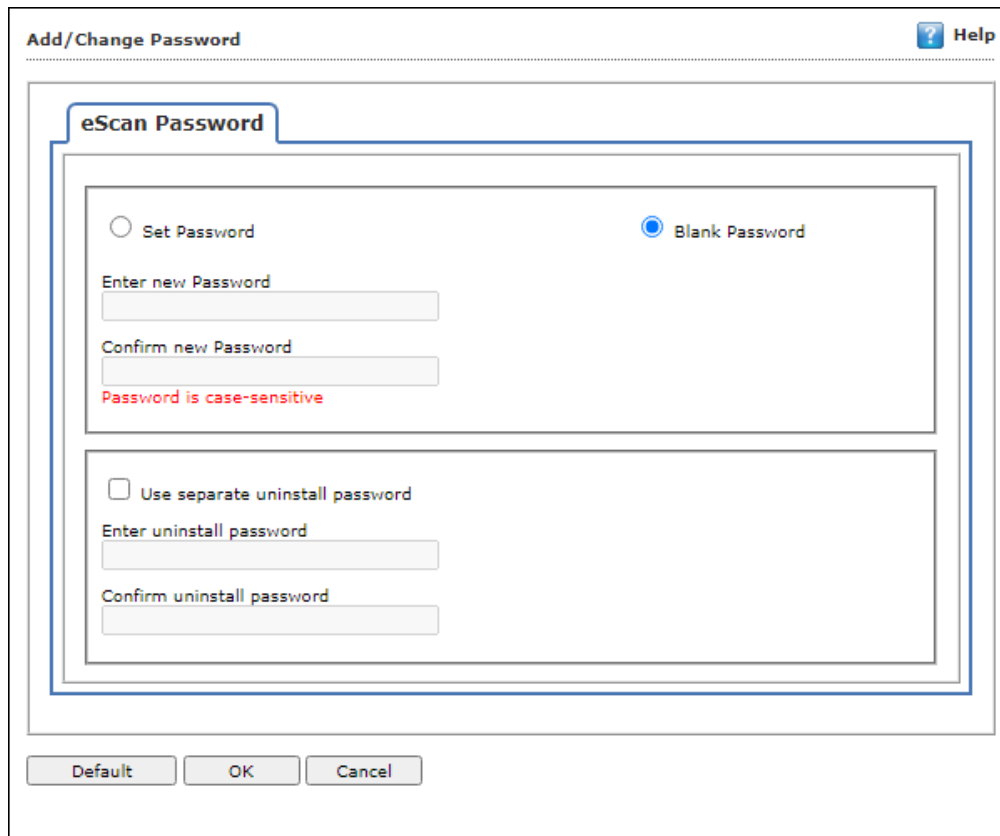
The updates can be downloaded on a schedule basis with **Schedule Download** option. Select intervals and time basis as per your preferences.

  
**NOTE**

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

## Administrator Password

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



### Set Password

Click this option, if you want to set password.

### Blank Password

Click this option, if you do not want to set any password for login.

When you click this option, the **Enter new Password** and **Confirm new Password** fields become unavailable.

### Enter new Password

Enter the new password.

### Confirm new Password

Re-enter the new password for confirmation.

### Use separate uninstall password

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

### Enter uninstall Password

Enter the uninstallation password.

### Confirm uninstall Password

Re-enter the uninstallation password for confirmation.

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

The Password will be saved.

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

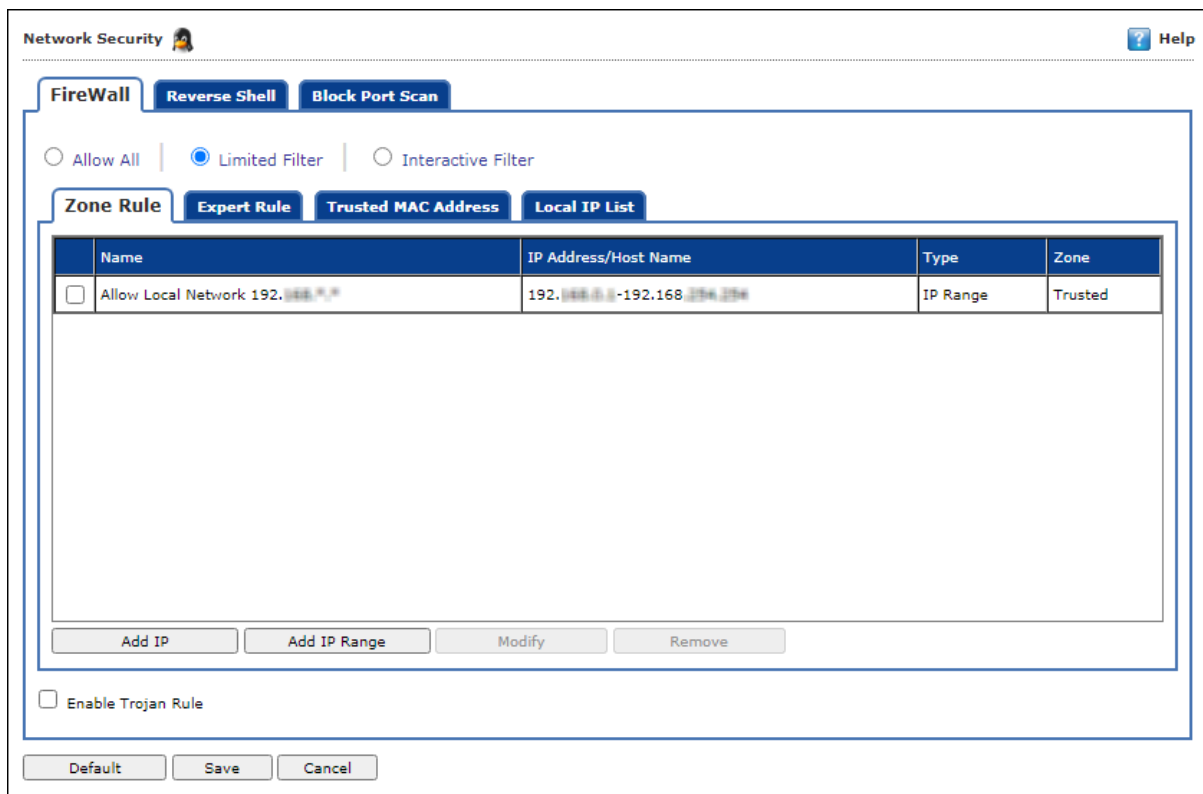
## Network Security

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

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

## Firewall

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



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

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

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

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

Following tabs are available:

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



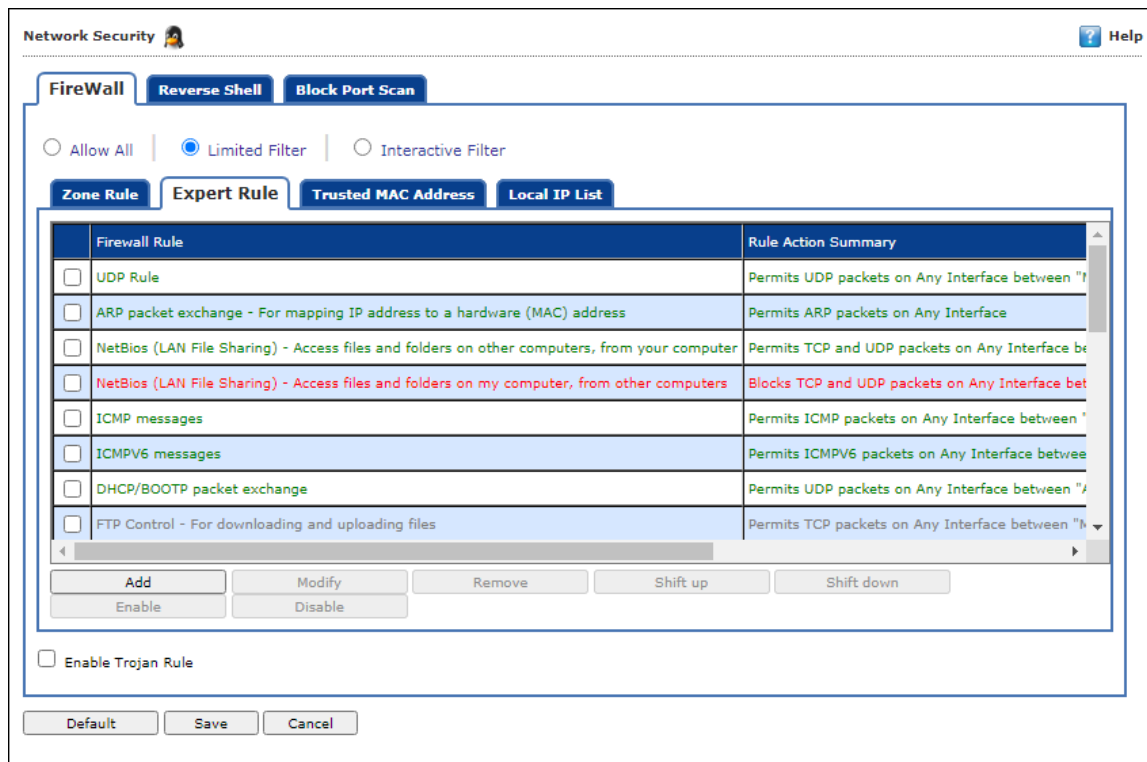
## Zone Rule

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

- **Add 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.



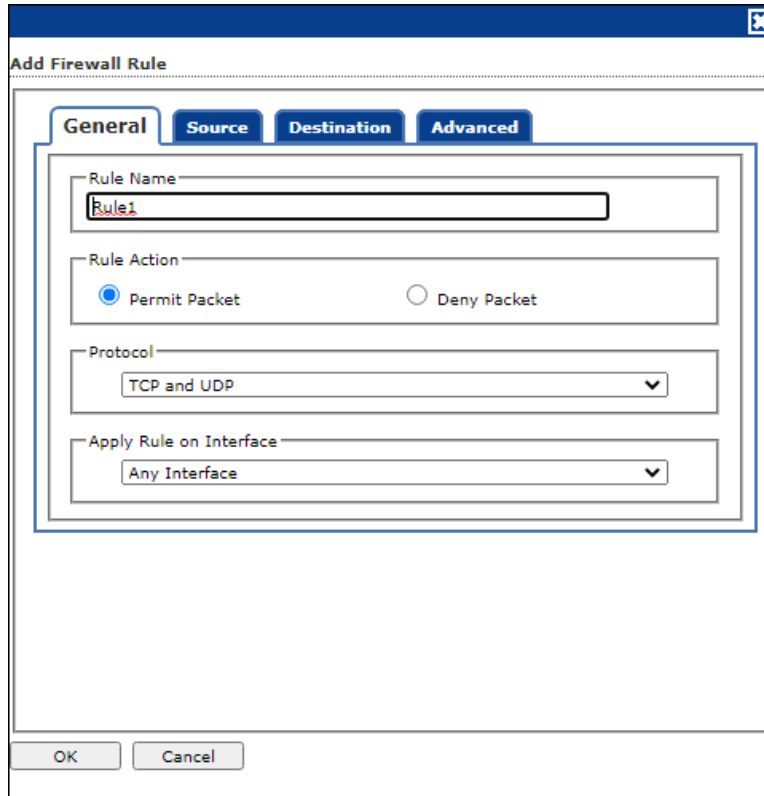
However, configure these rules only if you are familiar with firewalls and networking protocols.

- Source IP Address/Host Name
- Source Port Number

- Destination IP Address/Host Name
- Destination Port Number

The following buttons are available to configure an Expert Rule:

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



### General tab

In this section, specify the Rule settings:

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

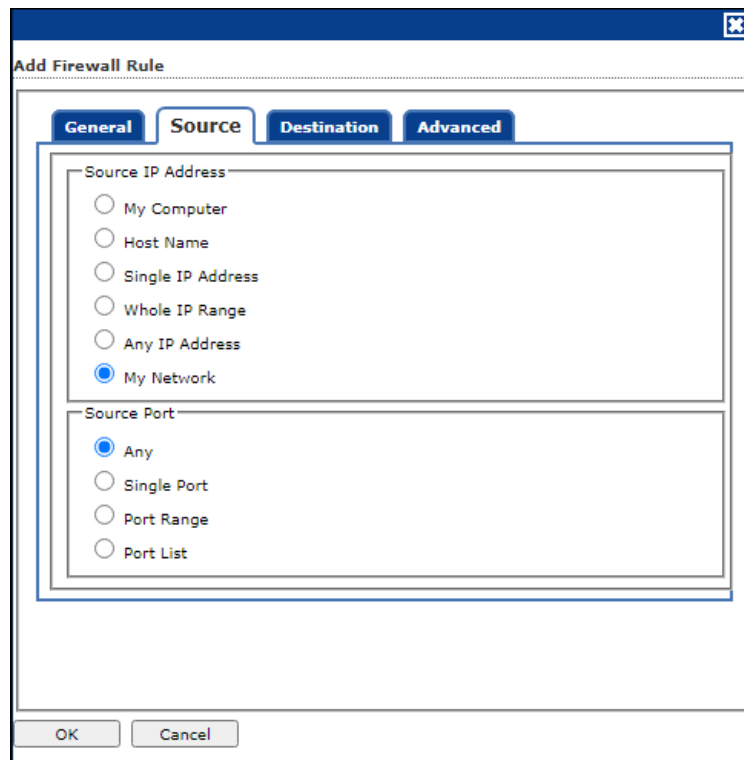
**Rule Action** – Action to be taken, whether to Permit Packet or Deny Packet.

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

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

## Source tab

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



### Source IP Address:

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

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

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

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

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

### Source Port:

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

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

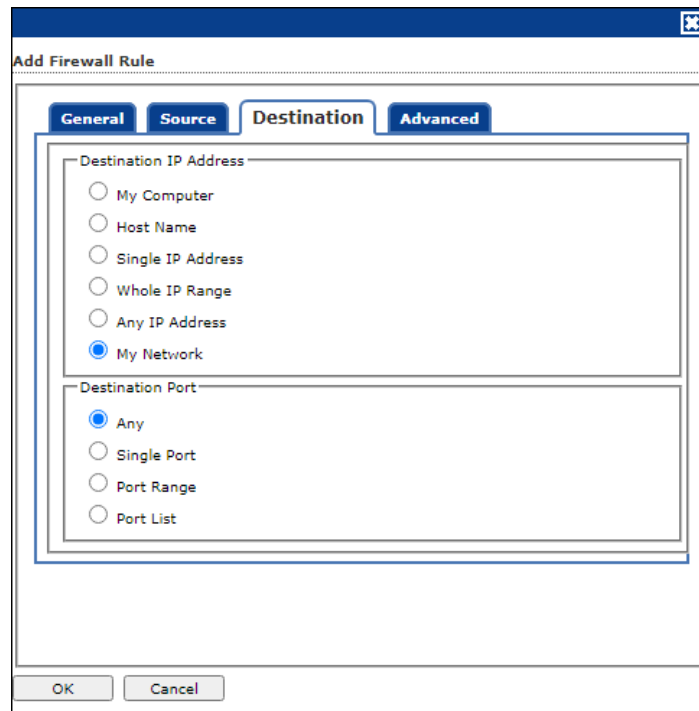
**Port Range** – To enable the rule on a group of ports in series, you can specify a range of ports. The rule will be applied for the outgoing traffic originating from the port which is within the defined range of ports.

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

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

### Destination tab

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



### Destination IP Address:

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

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

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

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

### Destination IP Port:

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

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

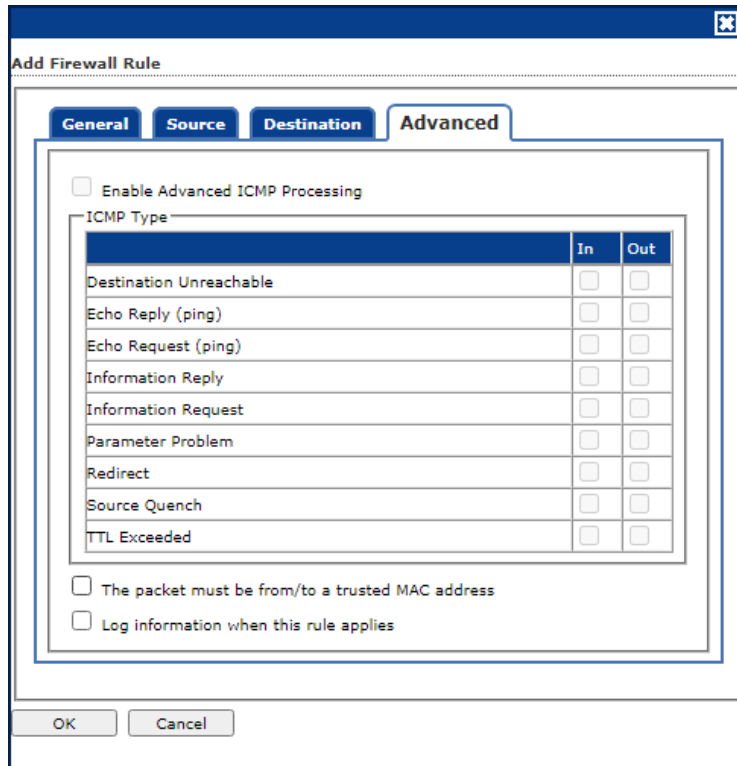
**Port Range** – To enable the rule on a group of ports in series, you can specify a range of ports.

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

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

**Advanced tab**

This tab contains advance setting for Expert Rule.



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

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

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

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

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

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

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

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

**Trusted MAC Address**

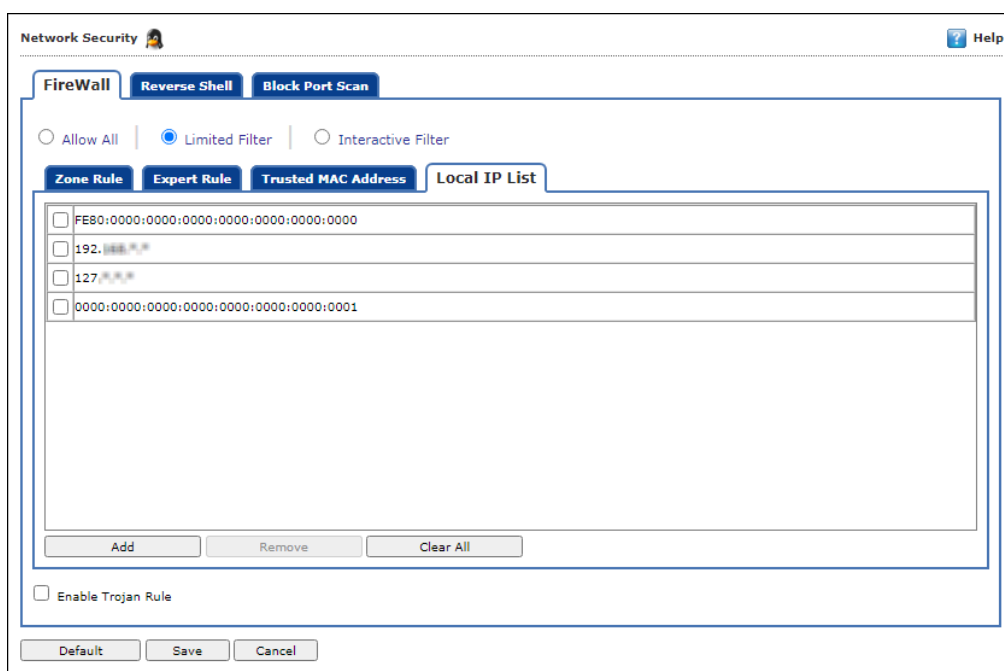
This section contains the information of the MAC address of the system. A MAC address is a hardware address that uniquely identifies each node of a network. The Trusted MAC address list will

be checked along with the Expert Rule only when "The packet must be from/to a trusted MAC address" option is checked and the action will be as per specified in the rule. (Refer to the *Advance Tab* of the [Expert Rule](#)). The following buttons are available to configure the Trusted Mac Address:

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



The screenshot shows the 'Network Security' configuration window with the 'Local IP List' tab selected. The window has a title bar with 'Network Security' and a 'Help' icon. Below the title bar are three tabs: 'FireWall', 'Reverse Shell', and 'Block Port Scan'. Underneath these are three radio buttons: 'Allow All', 'Limited Filter' (which is selected), and 'Interactive Filter'. Below the radio buttons are four sub-tabs: 'Zone Rule', 'Expert Rule', 'Trusted MAC Address', and 'Local IP List'. The 'Local IP List' sub-tab is active, showing a list of four entries, each with a checkbox and a text field containing an IP address:   
1.  FE80:0000:0000:0000:0000:0000:0000:0000  
2.  192.168.1.1  
3.  127.0.0.1  
4.  0000:0000:0000:0000:0000:0000:0000:0001  
Below the list are three buttons: 'Add', 'Remove', and 'Clear All'. At the bottom of the window is a checkbox labeled 'Enable Trojan Rule' which is currently unchecked. At the very bottom are three buttons: 'Default', 'Save', and 'Cancel'.

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

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

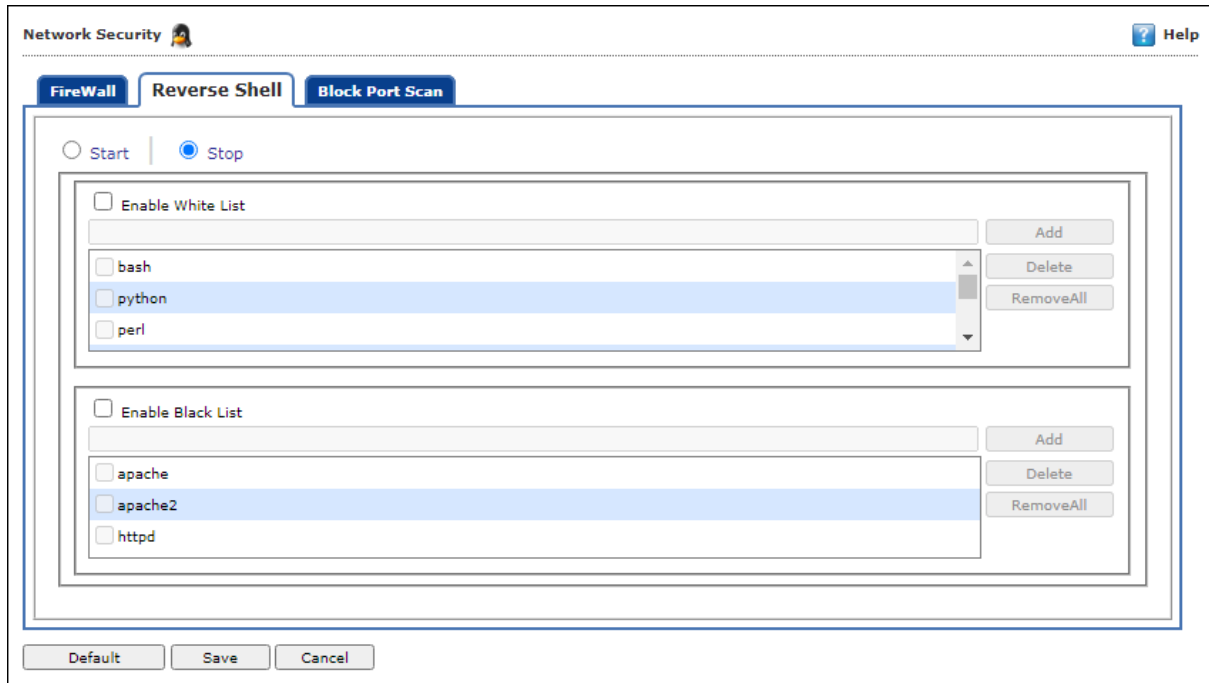
**Clear All** – To clear all local IP addresses, click **Clear All**.

### Enable Trojan Rule

Select this checkbox, to enable the Trojan Rule.

## Reverse Shell

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



### Start/Stop

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

After enabling this, you can configure the following settings:

### Enable White List

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

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

### Enable Black List

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

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

## Block Port Scan

This tab allows admin to configure the port scan option.

### 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**.

## Tools

The Tools lets you configure Remote Monitoring Management (RMM) Settings on Linux based systems.

## RMM Settings

The RMM settings let you configure default connection settings for connecting to client computers.

### Manual Start [Default]

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 checkbox 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 [Default]

If this checkbox 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.

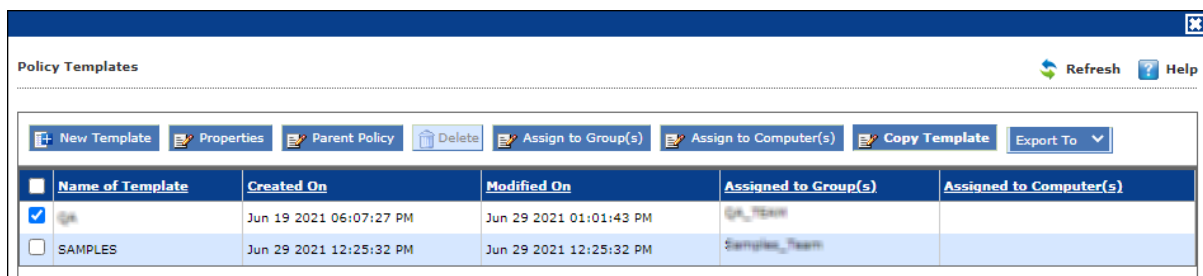
## Assigning Policy Template to a group

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

### Method 1

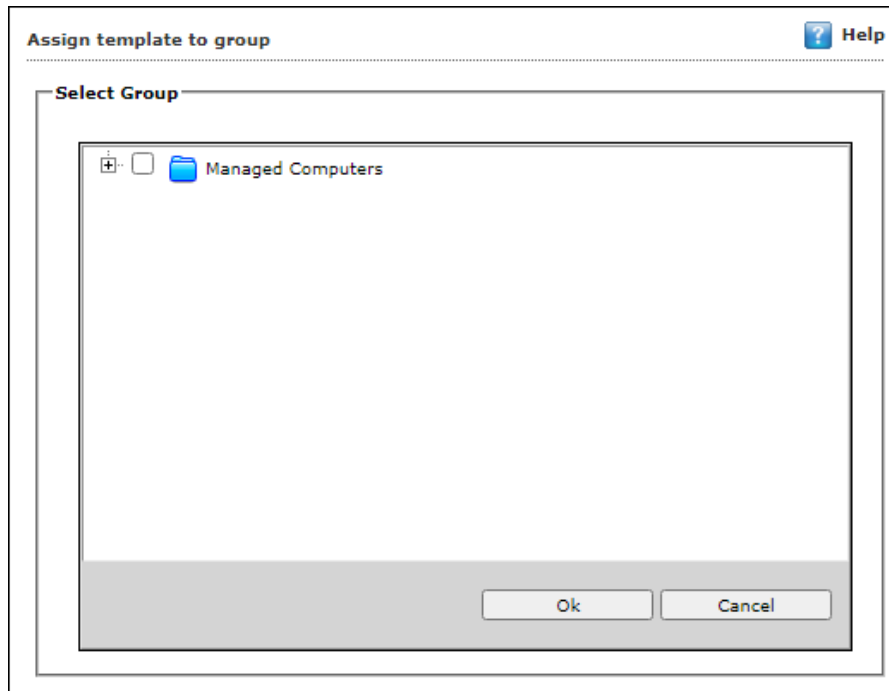
To assign a Policy to a group,

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



<input type="checkbox"/>	Name of Template	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
<input checked="" type="checkbox"/>	QA	Jun 19 2021 06:07:27 PM	Jun 29 2021 01:01:43 PM	QA_Team	
<input type="checkbox"/>	SAMPLES	Jun 29 2021 12:25:32 PM	Jun 29 2021 12:25:32 PM	Sample_Team	

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

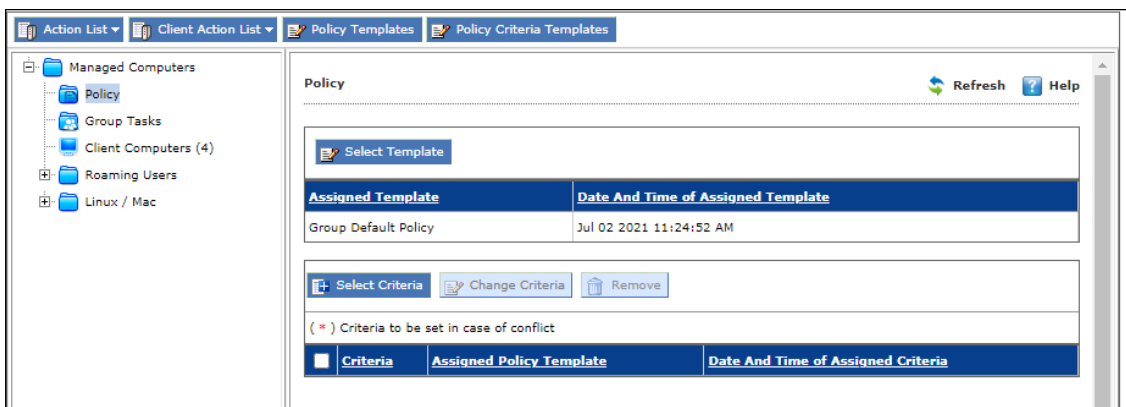


4. Select the group(s) and then click **OK**.  
The policy will be assigned to the selected group(s).

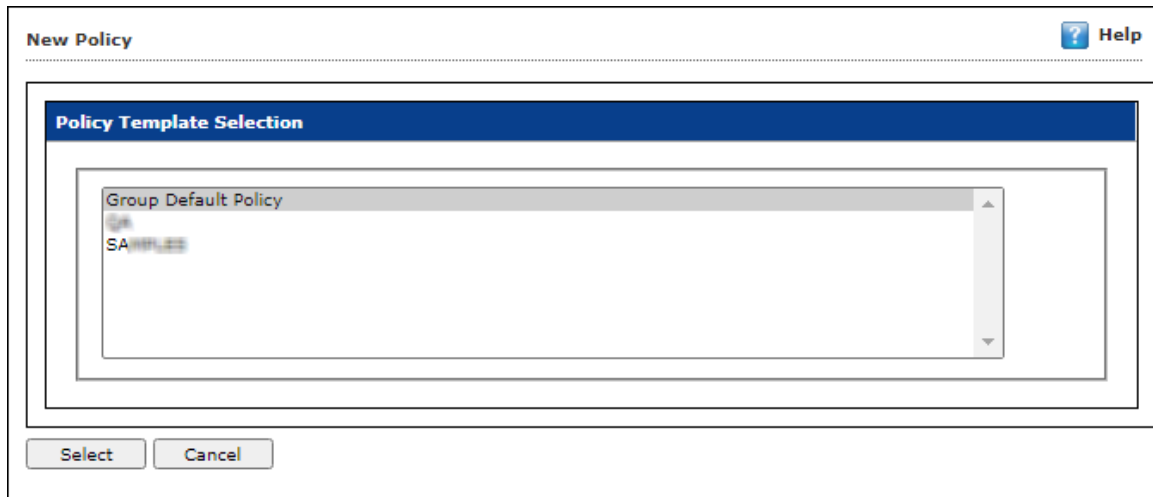
## Method 2

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.

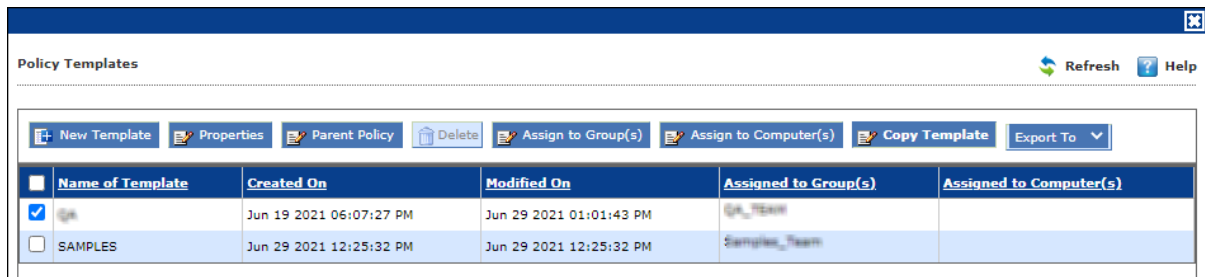


4. Select a policy template and then click **Select**.  
The default Policy Template for group will be saved and updated.

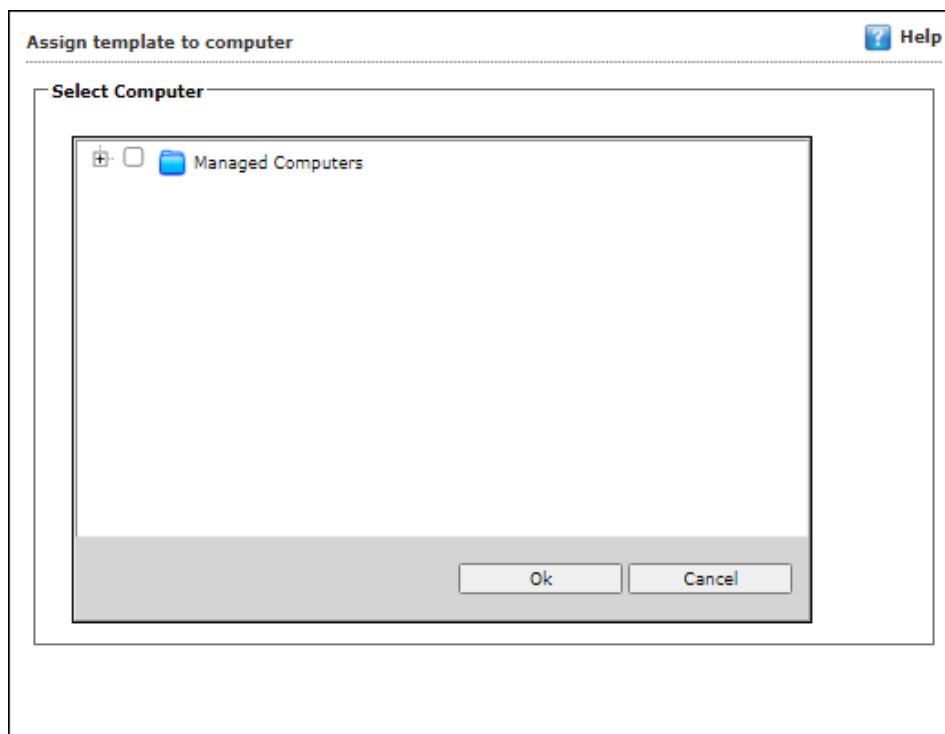
## Assigning Policy Template to Computer(s)

To assign a policy template to computers,

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



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

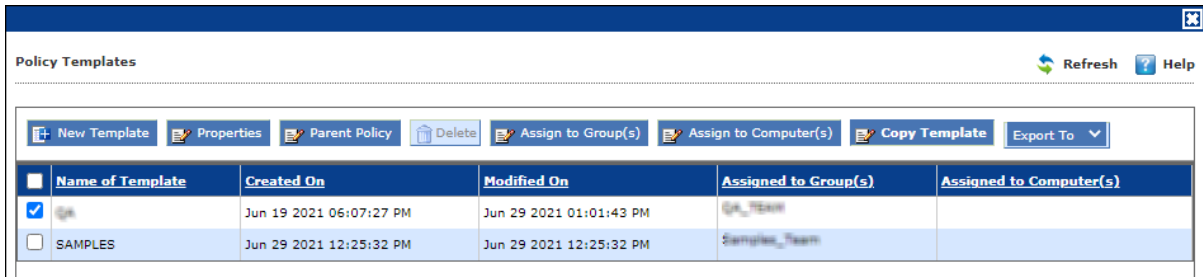


3. Click **Managed Computers**.
4. Select the computer(s) and then click **OK**.  
The policy template will be assigned to the selected computers.

## Copy a Policy Template

To copy a Policy Template,

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

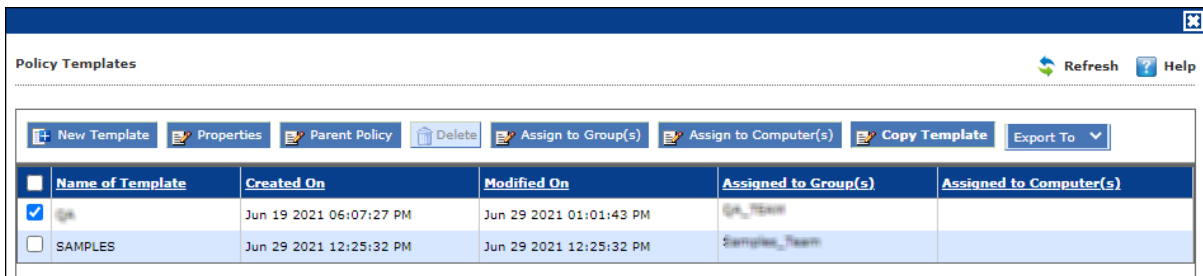


2. Click **Copy Template**.  
New Template window appears displaying settings from the original template.
3. Enter a name for the template.
4. Make the necessary changes and then click **Save**.  
The template will be copied.

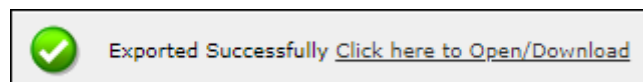
## Exporting a Policy Template report

To copy a Policy Template,

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



2. Click **Export To**.
3. Select the file format from the drop-down menu (HTML, PDF, and Excel).  
The Policy template report will be generated.

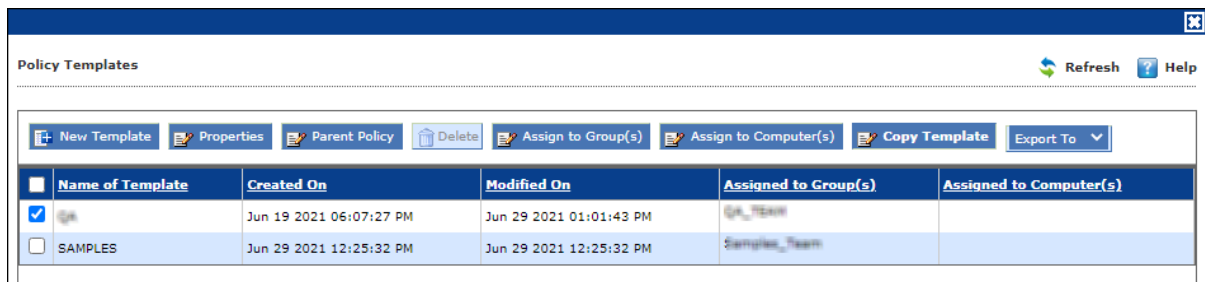


## Parent Policy

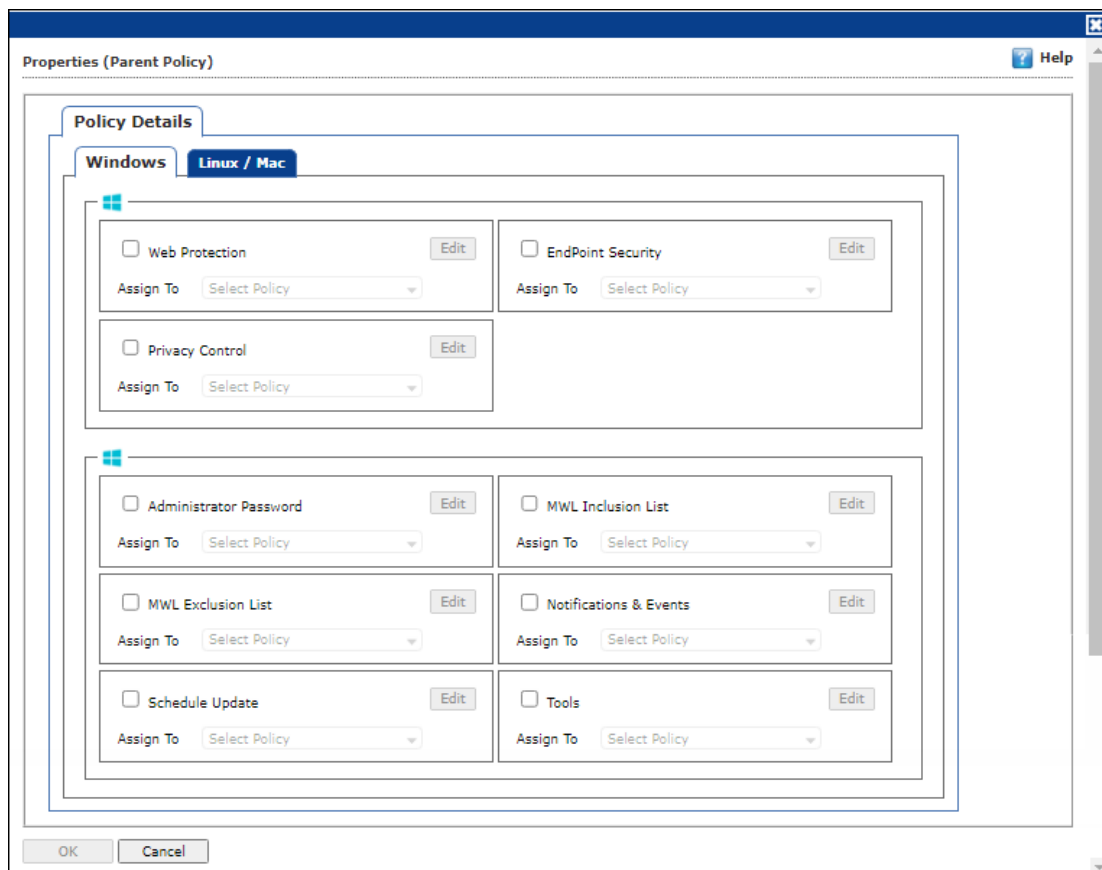
The Parent Policy lets you to implement a change in policy setting to multiple policies at the same time. For example, if you want to make a policy change in a single module like File Anti-Virus in multiple policies; you can do this all at a time using Parent Policy.

To configure Parent Policy, follow the steps given below:

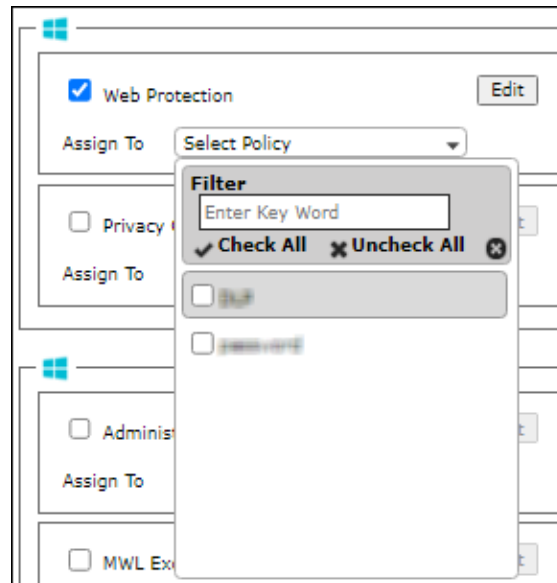
1. In the Managed Computers screen, click **Policy Templates**.  
Policy Templates window appears.
2. In the Policy Template window, click **Parent Policy**.




Properties (Parent Policy) window appears displaying all the policies.



3. Select and edit the required module according to your preferences.
4. Click **Assign To** drop-down and select the policies for which the parent policy changes should be applied.



5. Click **OK**.  
The Parent policy will be updated and changes will be applied to all the policies selected.

 <b>NOTE</b>	Before disabling a module in Parent Policy, ensure that policies are unchecked from <b>Assign To</b> drop-down.
---	---

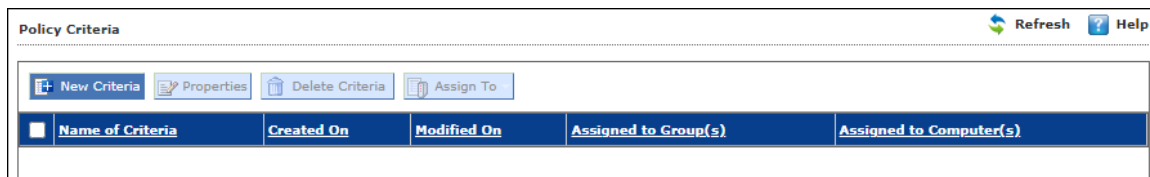
# Policy Criteria Templates

This button allows to add policy criteria template based on the endpoints conditions.

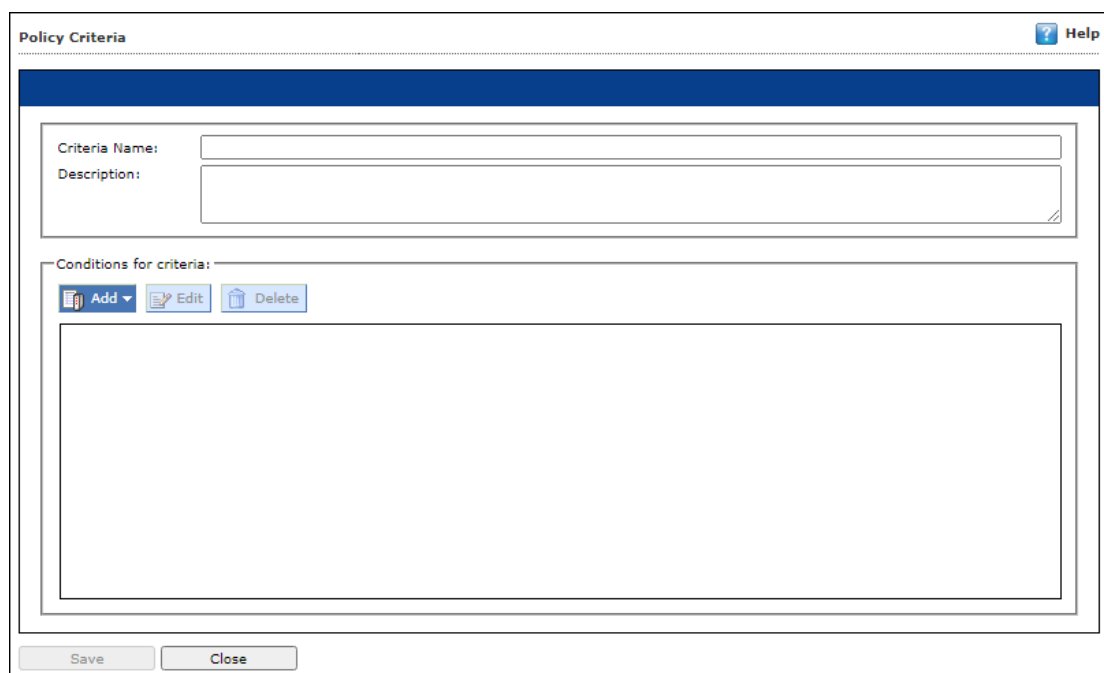
## Adding a Policy Criteria Template (AND condition)

To define Policy Criteria Template, follow the steps given below:

1. In the Managed Computers screen, click **Policy Criteria Templates**.  
Policy Criteria screen appears.



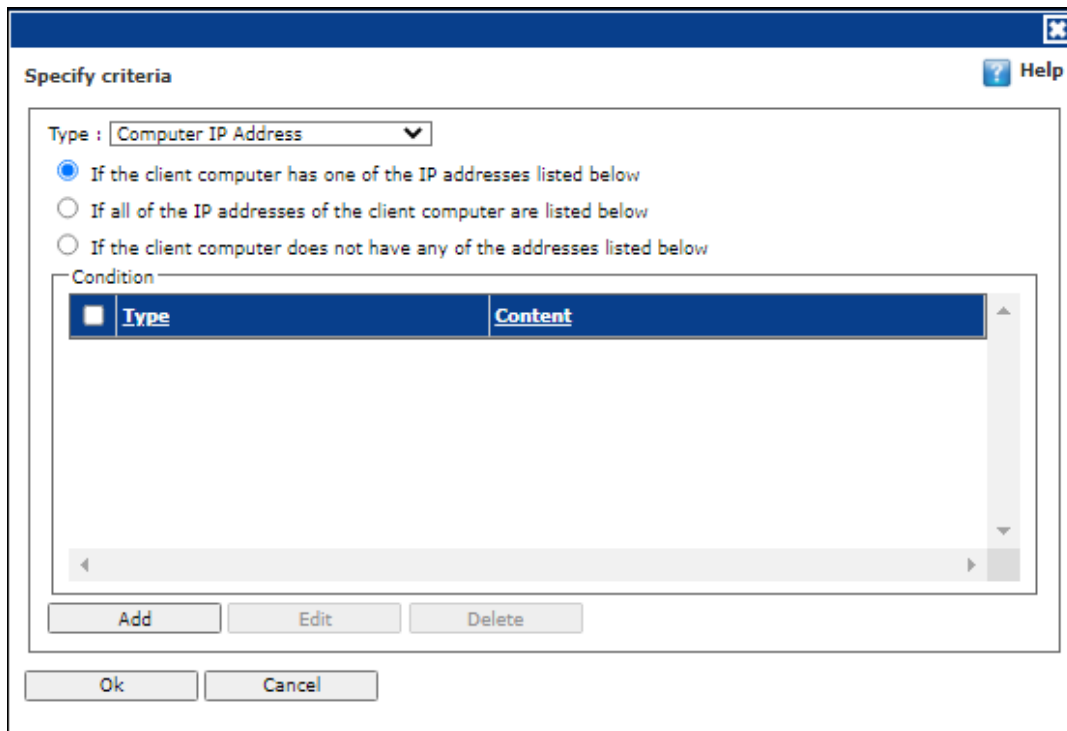
2. Click **New Criteria**.  
Policy Criteria screen displays parameter for creation.



3. Enter **Name** and **Description** for criteria.
4. Click **Add** drop-down.
5. Click **Add AND Condition**.



Specify Criteria screen appears.



6. Click the **Type** drop-down. It displays following options:
  - Computer IP Address
  - Management Server Connection
  - Users
  - Machine Name

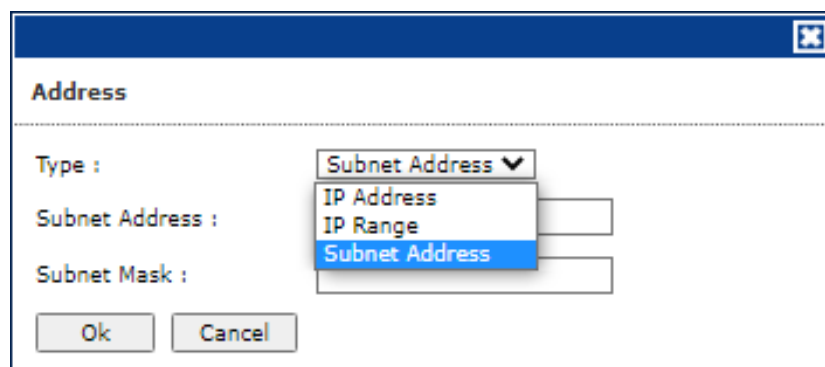
Depending upon the option, the conditions and settings vary.

## Computer IP Address

This option let you display list of computer IP address connected to client computer.

1. Select the appropriate condition.
2. Click **Add**.

Address window appears.



3. Select the type of address from the drop-down list (HTML, PDF, and Excel). Enter the IP address, if **IP Address** option is selected. Enter Start and End IP address, if **IP Range** option is selected. Enter subnet address and mask, if **Subnet Address** option is selected.
4. Click **OK**.  
The Policy Criteria Template for an IP Address will be saved.

**Edit** – Clicking **Edit** lets you edit the IP address of the policy template from the list.

**Delete** – Clicking **Delete** lets you delete the IP address of the policy template from the list.

## Management Server Connection

It display the client computer connect to the management server.

1. Select the appropriate condition.
2. Click **OK**.  
The Policy Criteria Template for Management Server Connection will be saved.

## Users

This option shows the list of username connected with client computer.

### Adding Local Users

1. To add local users, click **Add**.  
Username window appears.

A dialog box titled "Username" with a close button in the top right corner. It contains a label "Username:" followed by an empty text input field. Below the input field are two buttons: "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 features a breadcrumb trail "User Accounts > Add Active Directory Users" and a "Help" icon. It is divided into two main sections: "Search Criteria" and "Search Results".

**Search Criteria:**

- User's name\*: [Text Input] (Example: user or user\*)
- Domain\*: [Text Input]
- AD IP Address\*: [Text Input]
- AD Admin User name\*: [Text Input] (Example: domain\username)
- AD Admin Password\*: [Text Input]
- Use SSL Auth.:
- AdsPort\*: [Text Input] (Value: 389)


A "Search" button is located below the search criteria fields.

**Search Results:**

This section contains two lists: "Users" and "Selected Users", each with a scrollable list box. Between the two lists are two buttons: ">" and "<".

At the bottom of the window are "Ok" and "Cancel" buttons, and a red note: "(\*) Mandatory Fields".

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  button.

5. Click **OK**.

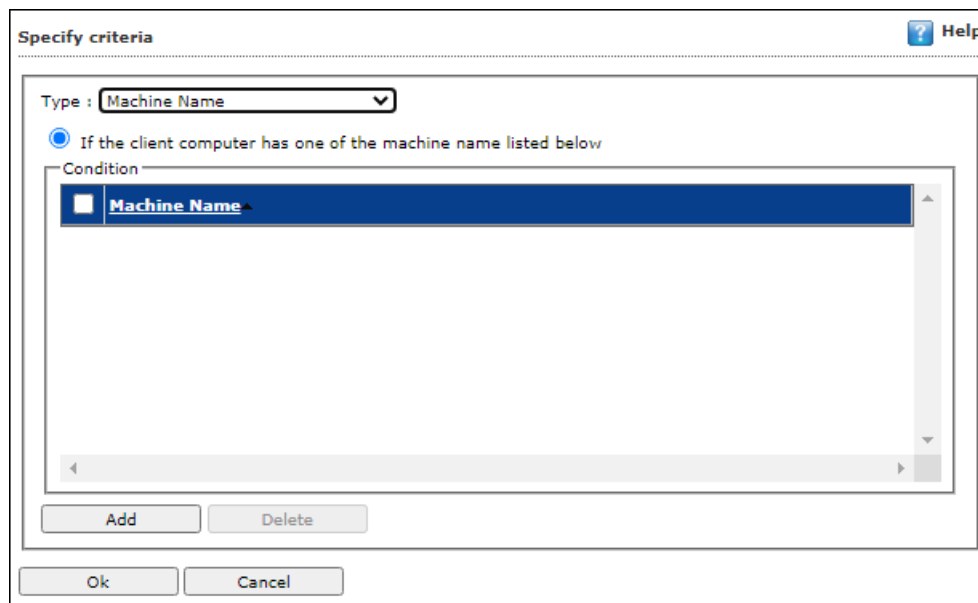
The Policy Criteria Template for Users will be saved.

**Edit** – Clicking **Edit** lets you edit user details of the policy template from the list.

**Delete** – Clicking **Delete** lets you delete user of the policy template from the list.

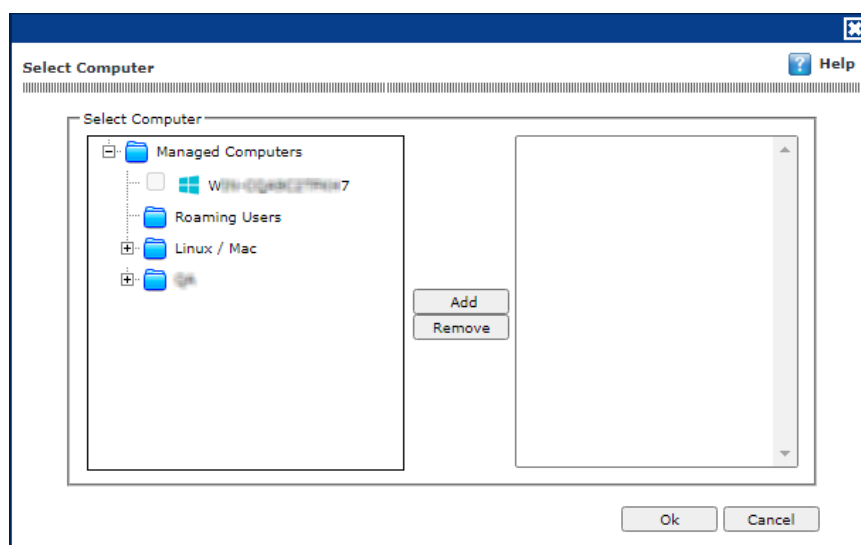
## Machine Name

This option show list of machine name connected to the client computer.



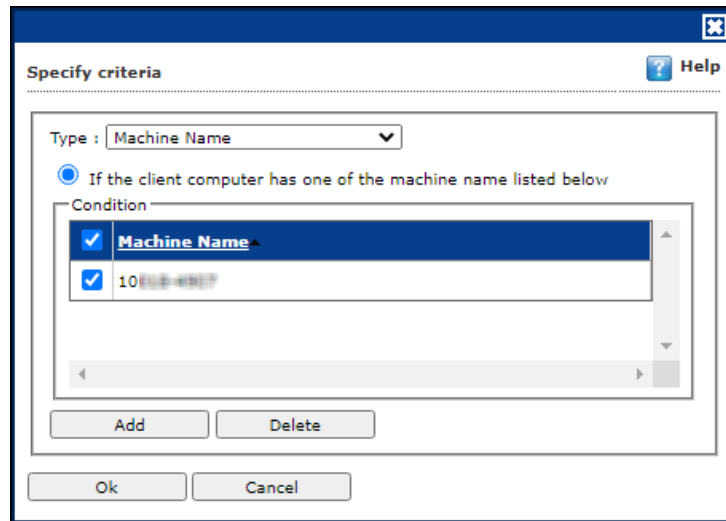
1. Click **Add**.

Select Computer screen appears displaying all managed computers.



2. Select the computer(s) to be added under this criterion and click **Add > OK**.

The Policy Criteria Template for selected machines will be saved.



3. Select the Machine Name. This enable Delete button, click **Delete** to delete the selected machine.  
The machine will be deleted.

To modify the existing condition,

1. Select the Condition.
2. Click **Edit**.
3. Make required changes and click **OK**.  
The condition will be updated.

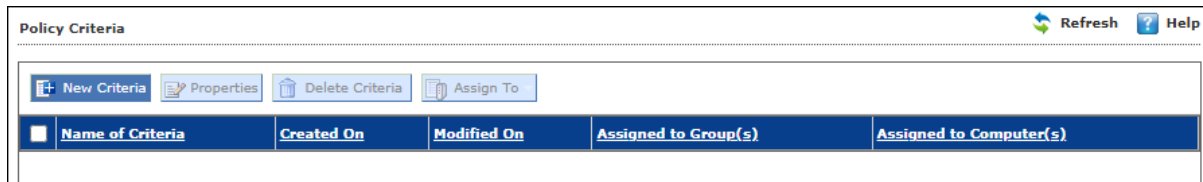
To delete the condition,

4. Select the Condition.
5. Click **Delete**.  
The condition will be deleted.

## Adding a Policy Criteria Template (OR condition)

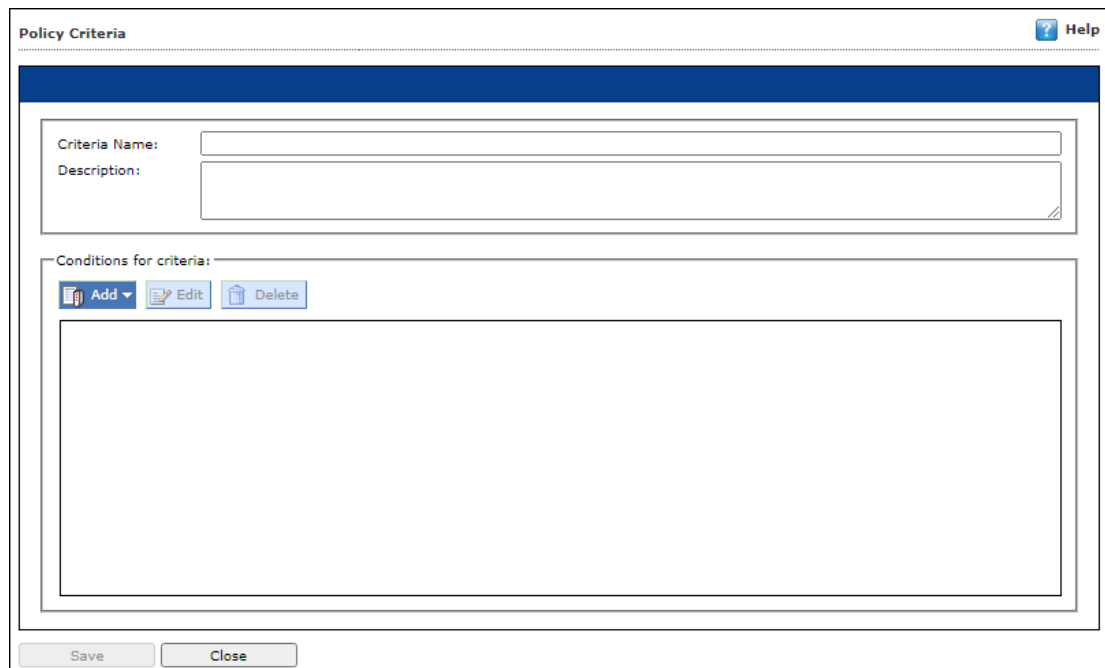
To define Policy Criteria Template, follow the steps given below:

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 OR Conditions**.



Before creating **OR Condition** in policy criteria, ensure that **AND Condition** is created.

Specify Criteria screen appears.

The 'Specify criteria' dialog box features a 'Type' dropdown menu set to 'Computer IP Address'. Below it are three radio button options: 'If the client computer has one of the IP addresses listed below' (selected), 'If all of the IP addresses of the client computer are listed below', and 'If the client computer does not have any of the addresses listed below'. A 'Condition' table is present with columns for 'Type' and 'Content'. At the bottom are 'Add', 'Edit', and 'Delete' buttons, and 'Ok' and 'Cancel' buttons.

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

## 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**.

The 'Policy Criteria' window displays a table with the following data:

Name of Criteria	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
demo	Jul 17 2015 04:21:58 PM	Jul 17 2015 04:21:58 PM	Group Default Policy Managed Computers	

Policy Criteria window appears.

3. Make the necessary changes and click **Save**.  
The Policy Criteria template will be saved and updated.

## Assigning a Policy Criteria template to Group

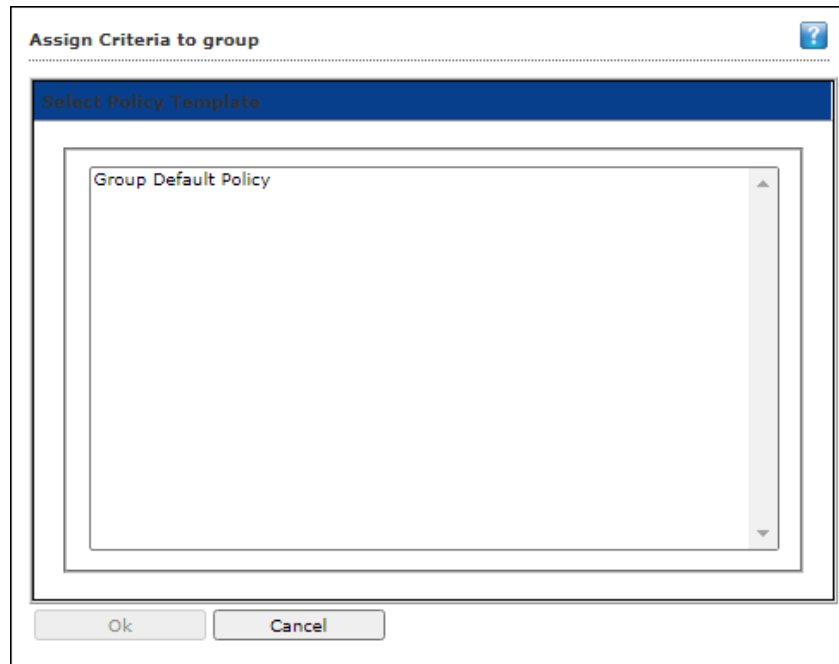
To assign policy criteria template, follow the steps given below:

1. Select a policy criteria template.
2. Click **Assign To > Groups**.

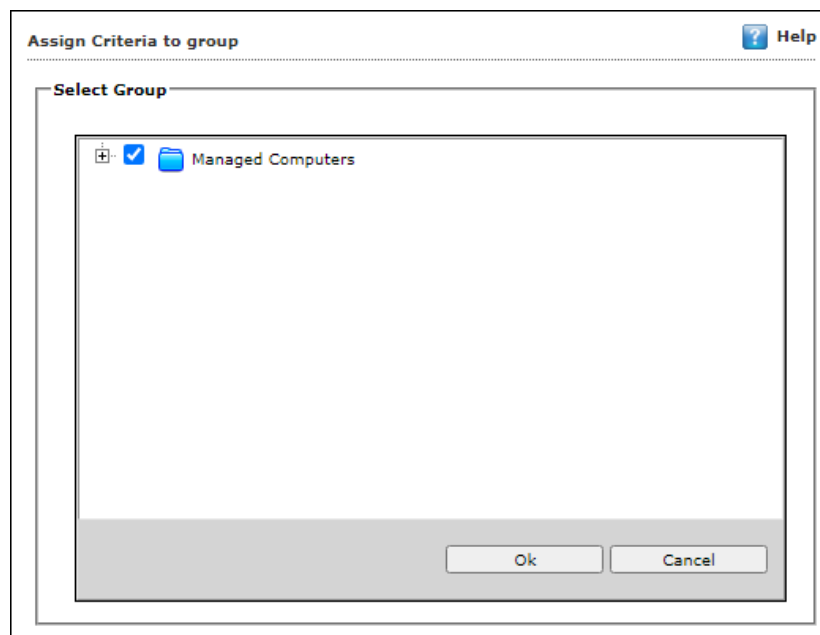
<input checked="" type="checkbox"/>	Name of Criteria	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
<input checked="" type="checkbox"/>	demo	Jul 17 2015 04:21:58 PM	Jul 17 2015 04:21:58 PM	Group Default Policy Managed Computers	

Assign Criteria to group window appears.





3. Select the policy template.  
Assign Criteria to group window displays Managed Computers folder tree.



4. Select group and click **Ok**.  
The Policy Criteria Template assigned to selected group.

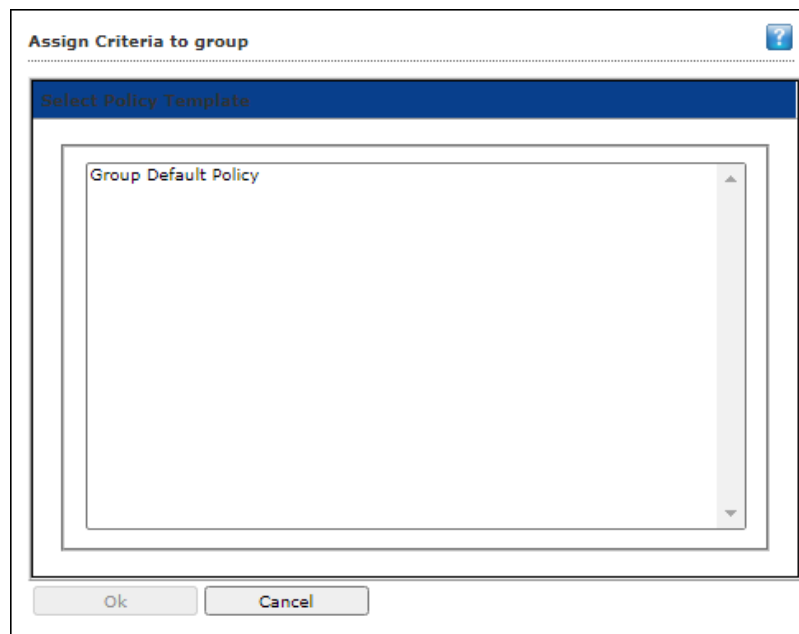
## Assigning a Policy Criteria template to Computer

To assign policy criteria template, follow the steps given below:

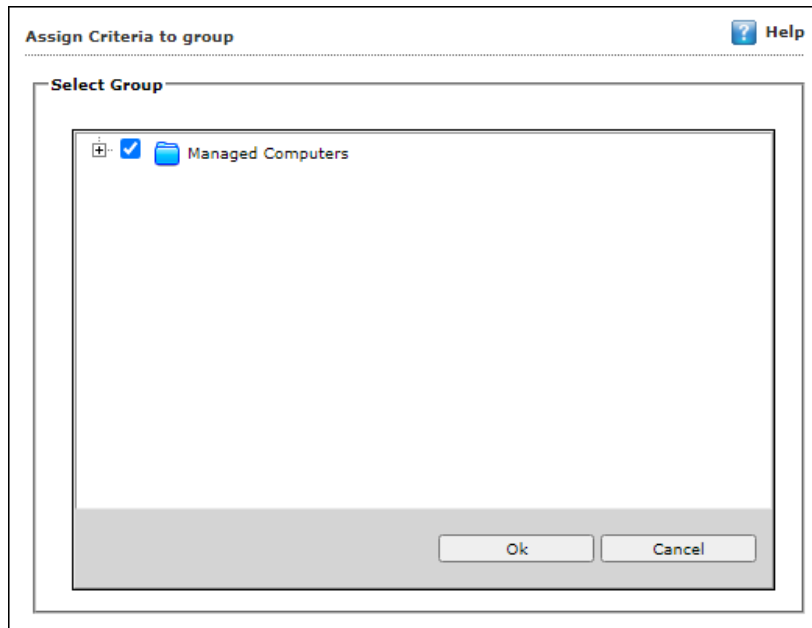
1. Select a policy criteria template.
2. Click **Assign To > Computers**.

<input checked="" type="checkbox"/>	Name of Criteria	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
<input checked="" type="checkbox"/>	dms	Jul 17 2013 04:21:58 PM	Jul 17 2013 04:21:58 PM	Group Default Policy Managed Computers	

Assign Criteria to computer window appears.



3. Select the policy template.  
Assign Criteria to group window displays Managed Computers folder tree.



4. Select computer and click **Ok**.  
The Policy Criteria Template assigned to selected computer.

## Deleting a Policy Criteria template

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.



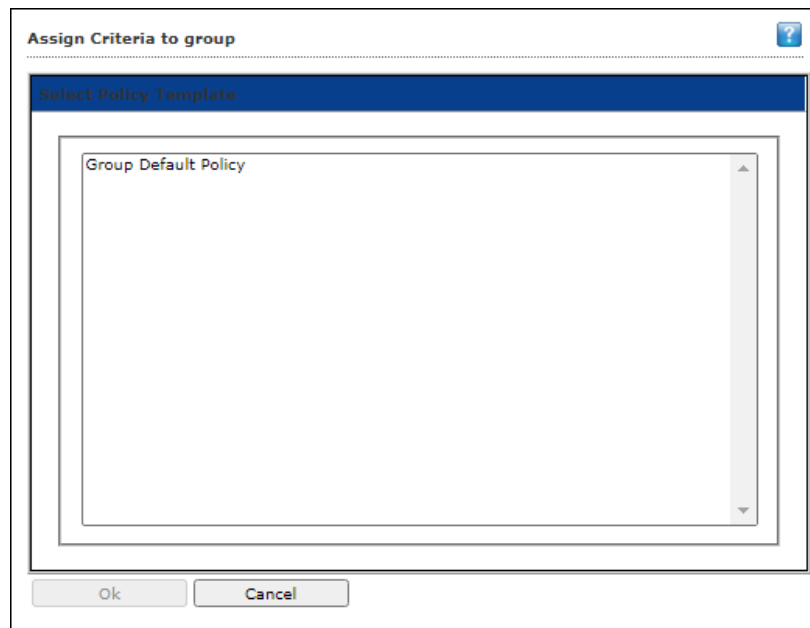
It will not allow you to delete the criteria, If it is assigned to any group or computer.

To delete assigned policy criteria template, follow the steps given below:

1. Select a policy criteria template.
2. Click **Assign To > Groups**.

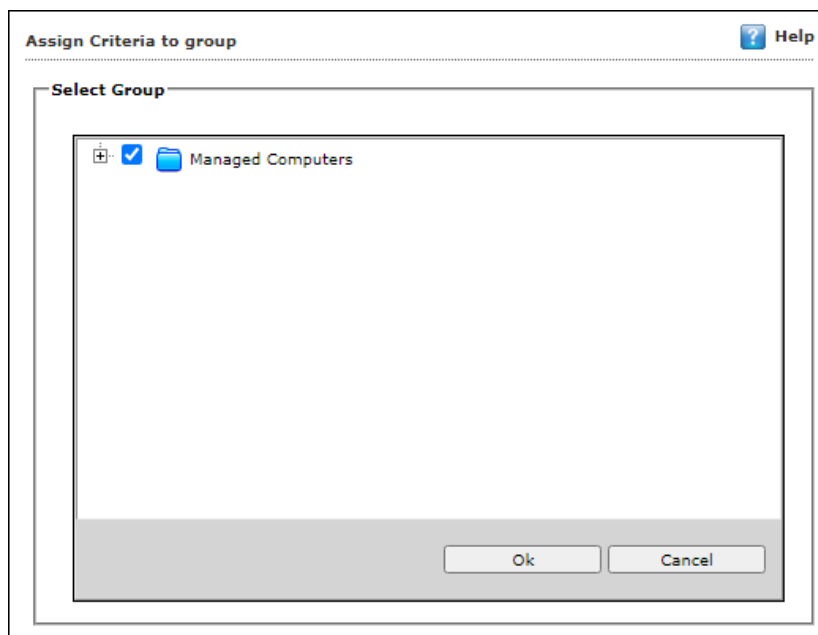
Policy Criteria					
<input checked="" type="checkbox"/> New Criteria <input type="checkbox"/> Properties <input type="checkbox"/> Delete Criteria <input type="checkbox"/> Assign To					
<input checked="" type="checkbox"/>	Name of Criteria	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
<input checked="" type="checkbox"/>	demo	Jul 17 2025 04:21:58 PM	Jul 17 2025 04:21:58 PM	Group Default Policy Managed Computers	

Assign Criteria to Group window appears.



3. Click **Group Policy Template** > **OK**.

Assign Criteria to group window displays Managed Computers folder tree.



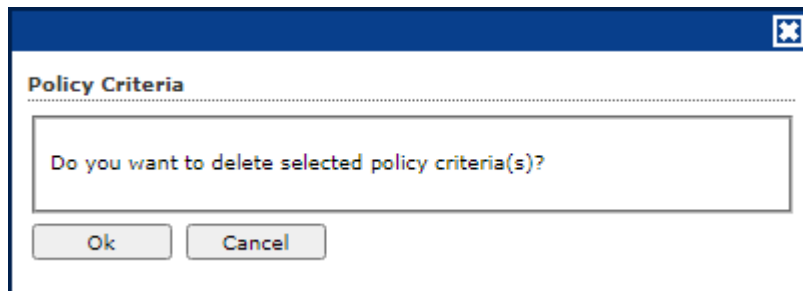
4. Uncheck the selected group.
5. Click **OK**.

The Policy Criteria Template will no longer be assigned to any group. This enables **Delete Criteria** button.

Policy Criteria Refresh Help

<input checked="" type="checkbox"/>	Name of Criteria	Created On	Modified On	Assigned to Group(s)	Assigned to Computer(s)
<input checked="" type="checkbox"/>	demo	Jul 17 2012 04:21:58 PM	Jul 17 2012 04:21:58 PM	Group Default Policy Managed Computers	

6. Select the template.
7. Click **Delete Criteria**.  
A confirmation window appears.



8. Click **Ok**.  
The Policy Criteria Template will be deleted.

# Unmanaged Computers

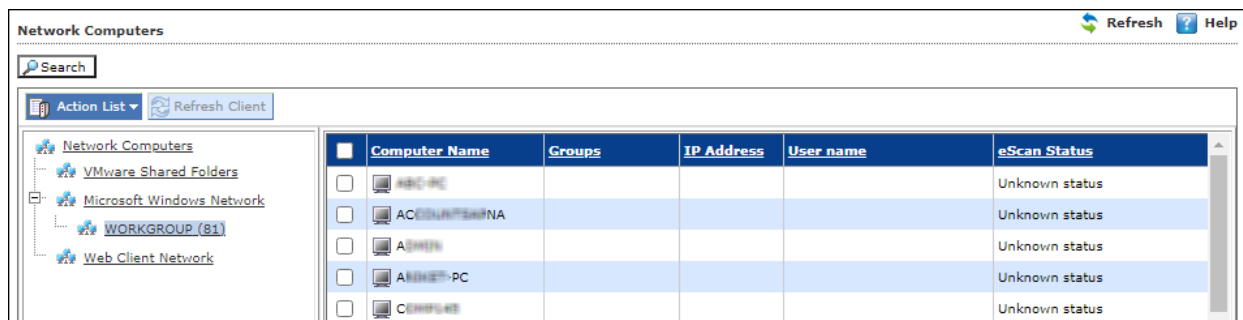
To install eScan Client, define policies and tasks on the basis of group, it is necessary to move computers to the created groups. You can move the computers from Unmanaged Computers to desired groups created in the Managed Computers using the following sub modules:

- **Network Computers**
- **IP Range**
- **Active Directory**
- **New Computers Found**

## Network Computers

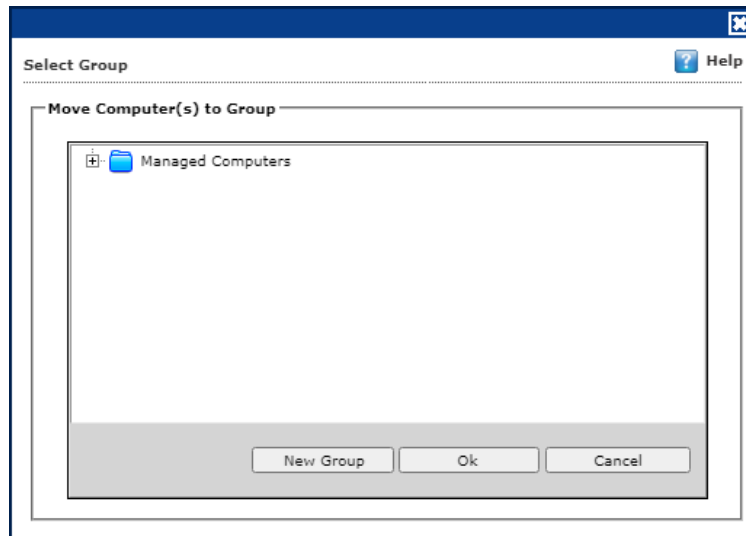
This sub module displays a list of available networks. You can move the computers from the list of computers present in the Network Computers using the following steps –

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.



Computer Name	Groups	IP Address	User name	eScan Status
ABC-PC				Unknown status
ACER-PC				Unknown status
ASUS-PC				Unknown status
ASUS-PC				Unknown status
ASUS-PC				Unknown status
ASUS-PC				Unknown status

4. Select the computer(s) you want to move to the desired group.
5. Click **Action List > Move to Group**.  
Select Group window appears.
6. Click **Managed Computers** tree to view the groups.

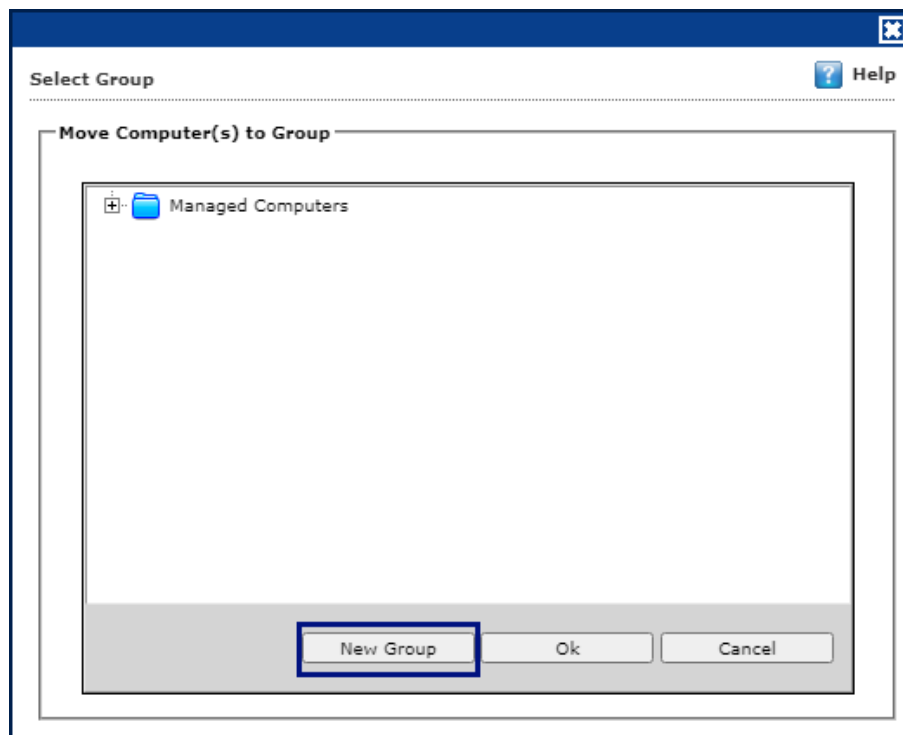


7. Select the group where you wish to move the selected computer(s) and click **OK**. The selected computer(s) will be moved to the group.

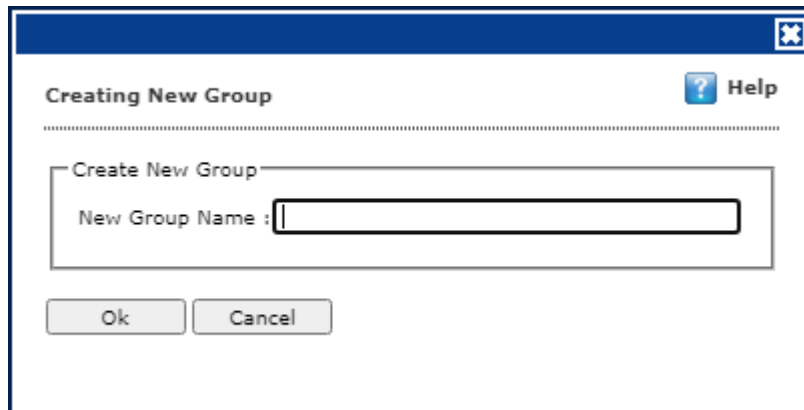
## Creating a New Group from the Select Group window

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**.



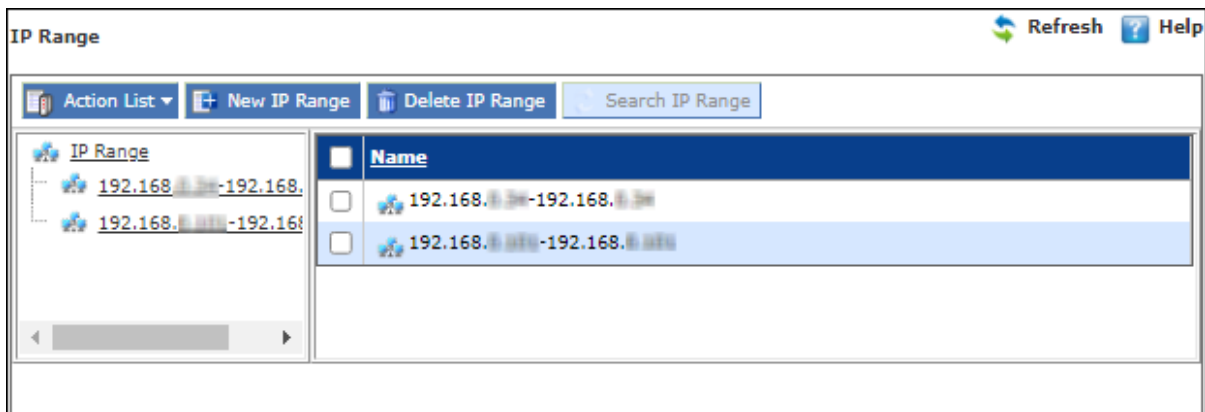
Creating New Group window appears.



2. Enter a name for the group.
  3. Click **OK**.
- A new group will be created.

## IP Range

The IP Range sub module 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.

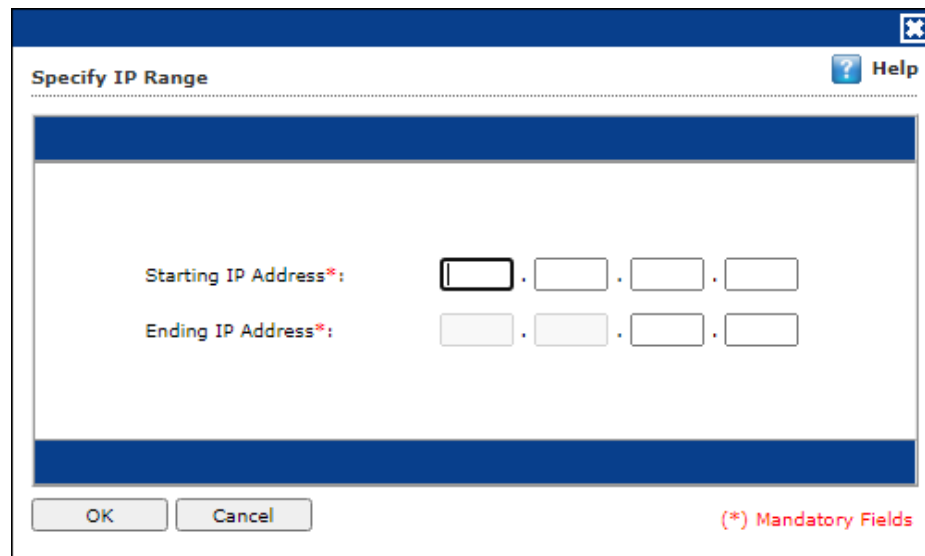


## Adding New IP Range

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 image shows a dialog box titled "Specify IP Range" with a "Help" button in the top right corner. It contains two rows of input fields. The first row is labeled "Starting IP Address\*" and the second row is labeled "Ending IP Address\*". Each label is followed by four small input boxes separated by dots, representing the four octets of an IP address. The first octet box in the "Starting IP Address\*" row is highlighted with a black border. At the bottom left are "OK" and "Cancel" buttons. At the bottom right is the text "(\*) Mandatory Fields".

2. Enter the Starting and Ending IP address of the range.
3. Click **OK**.

The entered IP Range will be added.

 **NOTE**

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.  
When you select the IP Range all computers present in that IP Range will be displayed on the interface in the right.

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

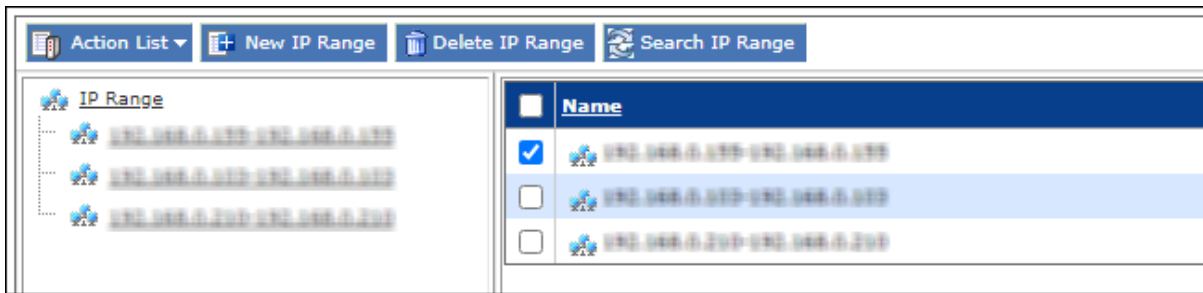
To move an entire IP range to a group, follow the steps given below:

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.

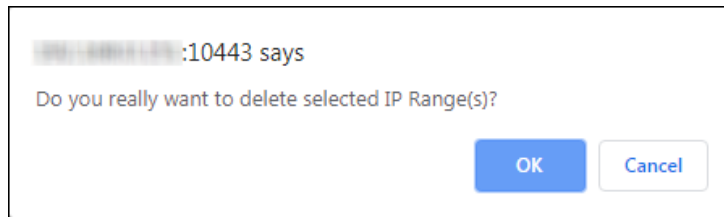
## Deleting an IP Range

To delete an IP range, follow the steps given below:

1. Select an IP Range.
2. Click **Delete IP Range**.



A confirmation prompt appears.

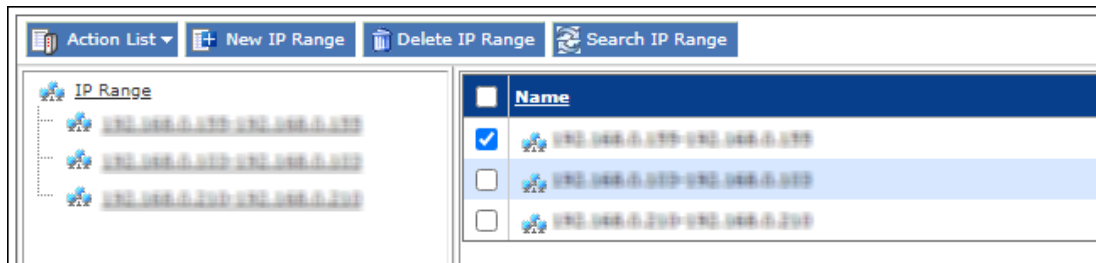


3. Click **OK**.  
The IP range will be deleted.

## Searching an IP Range

To search an IP range, follow the steps given below:

1. In the IP Range window, select an IP range.



2. Click on **Search IP Range**.  
The window displays the list of computers from the selected IP Range.



## Refreshing Client in IP Range

To refresh a client computer, follow the steps given below:

1. In the IP Range window, select an IP range.  
The window displays the list of computers from the selected IP Range.
2. Select the computer name.

<span>Action List</span> <span>New IP Range</span> <span>Delete IP Range</span> <span>Search IP Range</span> <span>Refresh Client</span>						
IP Range	<input type="checkbox"/>	Computer Name	Groups	IP Address	User name	eScan
192.168.1.1-192.168.1.255	<input type="checkbox"/>	COMPUTER		192.168.1.100		
192.168.1.1-192.168.1.255	<input type="checkbox"/>	NETWORKS		192.168.1.100		
192.168.1.1-192.168.1.255	<input type="checkbox"/>	VARIABLES		192.168.1.100		

- Click **Refresh Client**.  
The client computer status will be refreshed.

Client Status ? Help

```

02-01-2023 11:35:09 : Connecting to Computer... SUCCESSFUL
02-01-2023 11:35:09 : Successfully connected to eScan RMT Agent, Port:8098
=====

```

Close

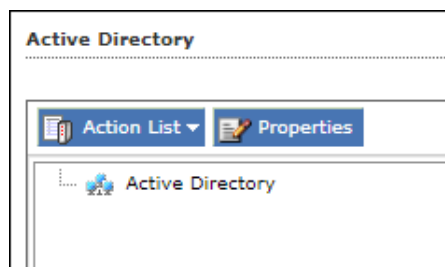
# Active Directory

The Active Directory sub module lets you add computers from an Active Directory.

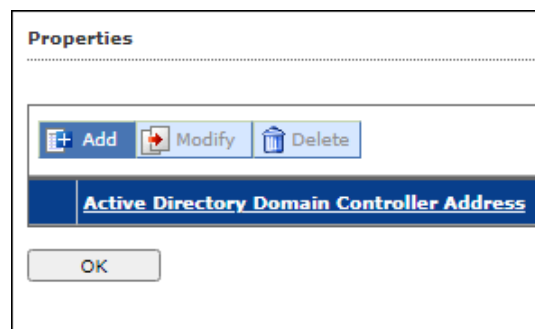
## Adding from Active Directory

To add computers from Active Directory, follow the steps given below:

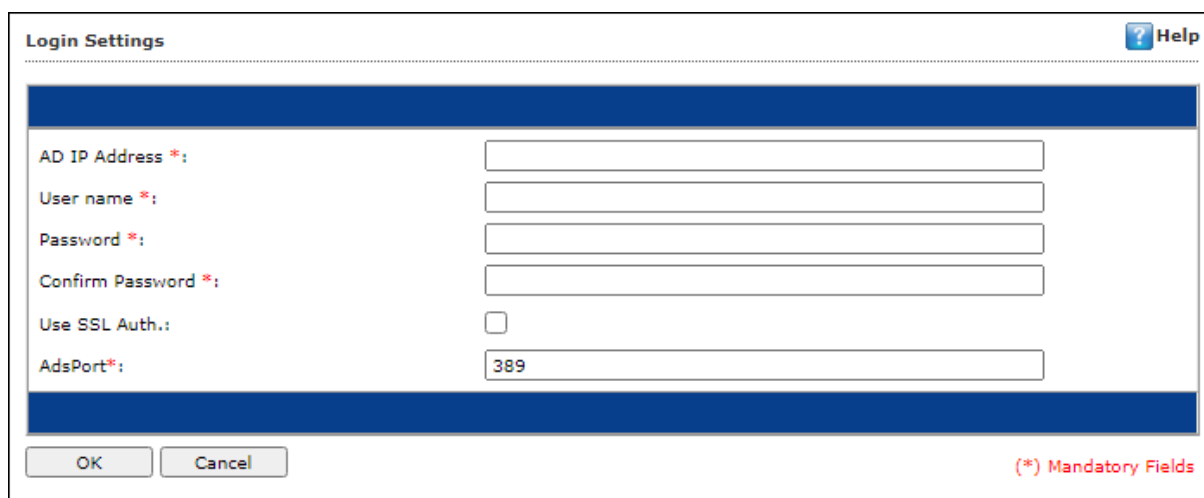
1. Click **Unmanaged Computers > Active Directory**.
2. Click **Properties**.



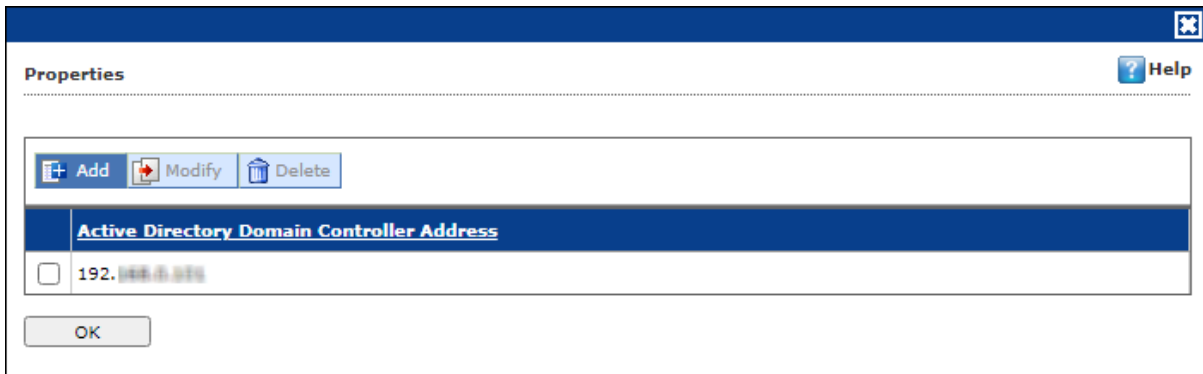
Properties window appears.



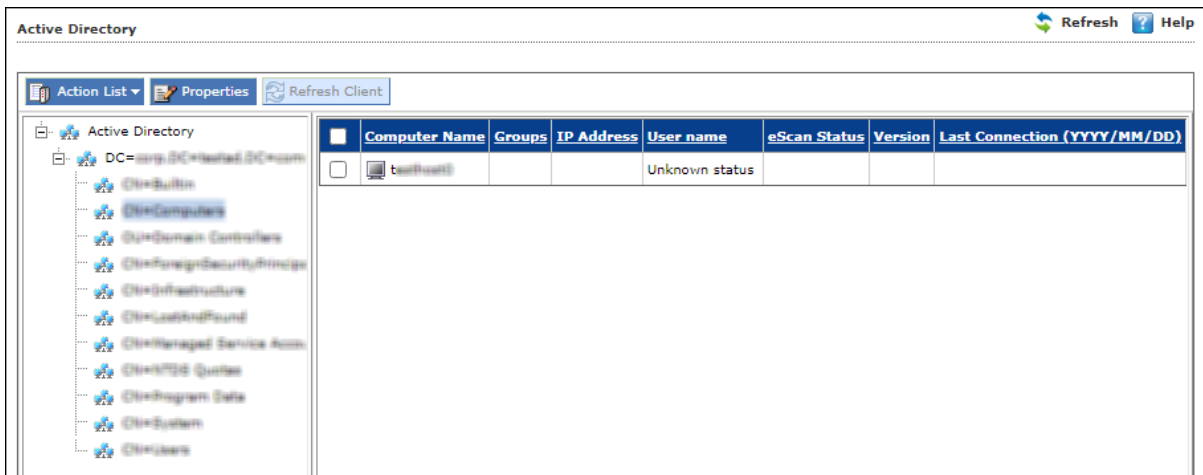
3. Click **Add**.  
Login Settings window appears.



4. Fill in the required Login Credentials and click **OK**.  
The details including IP Addresses from active directory will be added instantly.



4. Select the Active Directory and click **OK**.  
The selected Active Directory will be added to the Active directory tree.
5. To view the details, click the **Active Directory**.



## 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 sub module 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 Refresh Help

Search

Action List Filter Criteria

	Computer Name	IP Address	User name	Last Seen	Belongs To	eScan Status	Version	Last Connection	Installed Directory	Monitor Status	Anti-Spam
<input type="checkbox"/>	192.168.0.130	192.168.0.130		02 Jul 2021 13:54:27	Server	Unknown status					
<input type="checkbox"/>	192.168.0.137	192.168.0.137		02 Jul 2021 13:54:45	Server	Unknown status					
<input type="checkbox"/>	192.168.0.133	192.168.0.133		02 Jul 2021 13:54:26	Server	Unknown status					
<input type="checkbox"/>	192.168.0.170	192.168.0.170		02 Jul 2021 13:54:28	Server	Unknown status					
<input type="checkbox"/>	192.168.0.136	192.168.0.136		02 Jul 2021 13:54:27	Server	Unknown status					
<input type="checkbox"/>	192.168.0.176	192.168.0.176		02 Jul 2021 13:54:28	Server	Unknown status					
<input type="checkbox"/>	192.168.0.231	192.168.0.231		02 Jul 2021 13:54:28	Server	Unknown status					
<input type="checkbox"/>	192.168.0.238	192.168.0.238		02 Jul 2021 13:25:43	Server	Unknown status					
<input type="checkbox"/>	192.168.0.129	192.168.0.129		02 Jul 2021 13:54:27	Server	Unknown status					
<input type="checkbox"/>	192.168.0.46	192.168.0.46		02 Jul 2021 13:54:27	Server	Unknown status					
<input type="checkbox"/>	192.168.0.120	192.168.0.120		02 Jul 2021 13:54:27	Server	Unknown status					
<input type="checkbox"/>	192.168.0.76	192.168.0.76		02 Jul 2021 13:54:27	Server	Unknown status					
<input type="checkbox"/>	192.168.0.102	192.168.0.102		02 Jul 2021 13:54:46	Server	Unknown status					
<input type="checkbox"/>	192.168.0.44	192.168.0.44		02 Jul 2021 13:54:27	Server	Unknown status					

Unmanaged
  Protected
  Not Installed / Critical
  Unknown status

## Filter Criteria

The Filter Criteria lets you filter new computers found according to date range.

Action List Filter Criteria

Filter Criteria

**Date Range**

From (MM/DD/YYYY)

To (MM/DD/YYYY)

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.

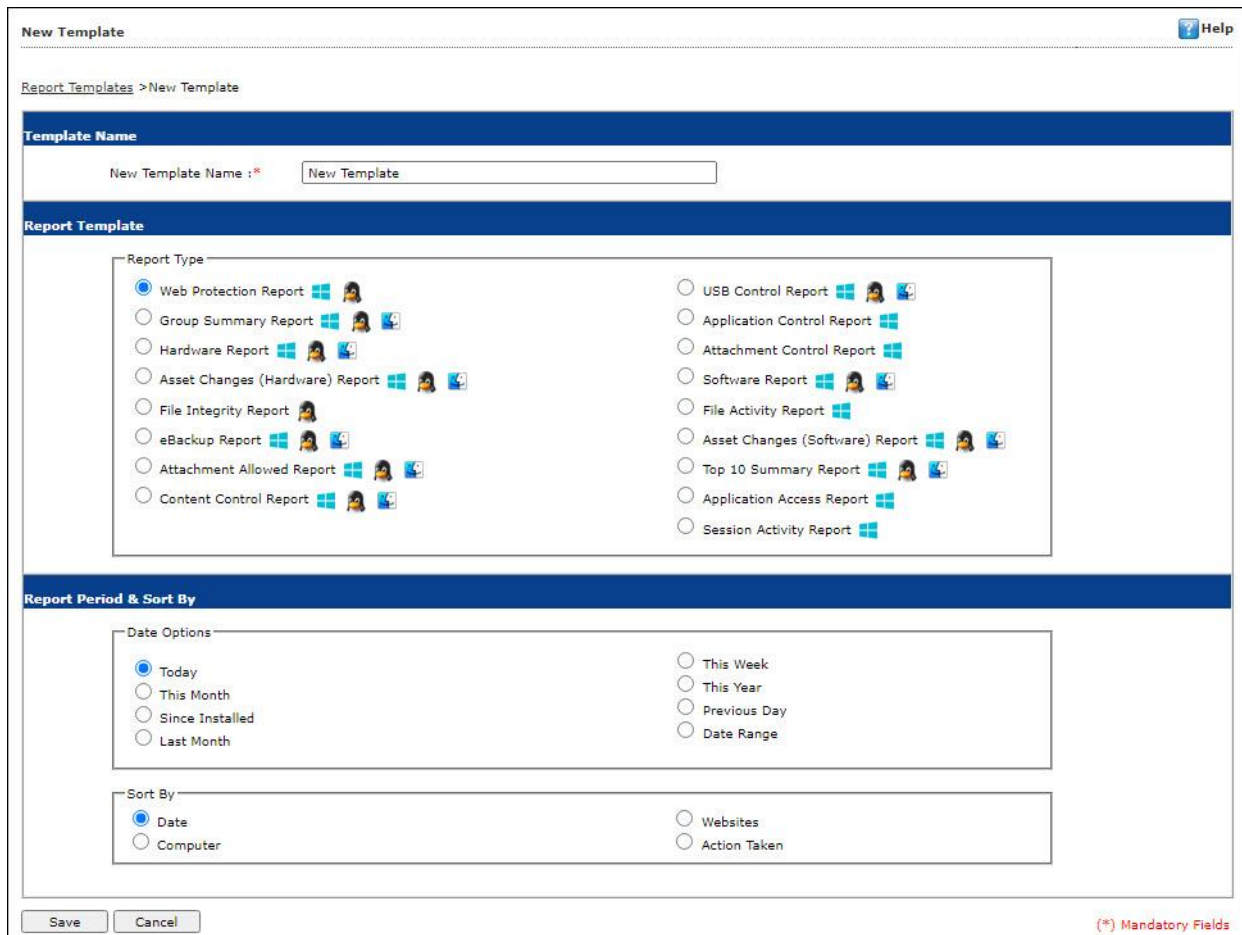
Template Name
<input type="checkbox"/> Web Protection Report
<input type="checkbox"/> Application Control Report
<input type="checkbox"/> Attachment Control Report
<input type="checkbox"/> Content Control Report
<input type="checkbox"/> USB Control Report
<input type="checkbox"/> Group Summary Report
<input type="checkbox"/> Hardware Report
<input type="checkbox"/> Software Report
<input type="checkbox"/> File Activity Report
<input type="checkbox"/> Asset Changes (Software) Report
<input type="checkbox"/> Asset Changes (Hardware) Report
<input type="checkbox"/> Top 10 Summary Report
<input type="checkbox"/> File Integrity Report
<input type="checkbox"/> Application Access Report
<input type="checkbox"/> Session Activity Report
<input type="checkbox"/> eBackup Report
<input type="checkbox"/> Attachment Allowed Report

## Creating a Report Template

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

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

New Template screen appears.



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

## Creating Schedule for a Report Template

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

## Viewing Properties of a Report Template

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

1. Select the Report Template whose properties you want to view.



2. Click **Properties**.  
Properties screen appears.

Properties ? Help

Report Templates > Application Control Report Properties

**General** | Report Period & Sort By

Report Name  
Report Name : Application Control Report

Details

Selected Template Type:	APPLICATION CONTROL REPORT
Created:	12/24/2012 03:26:58 PM
Modified:	03/26/2013 16:17:33

Save Cancel



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:

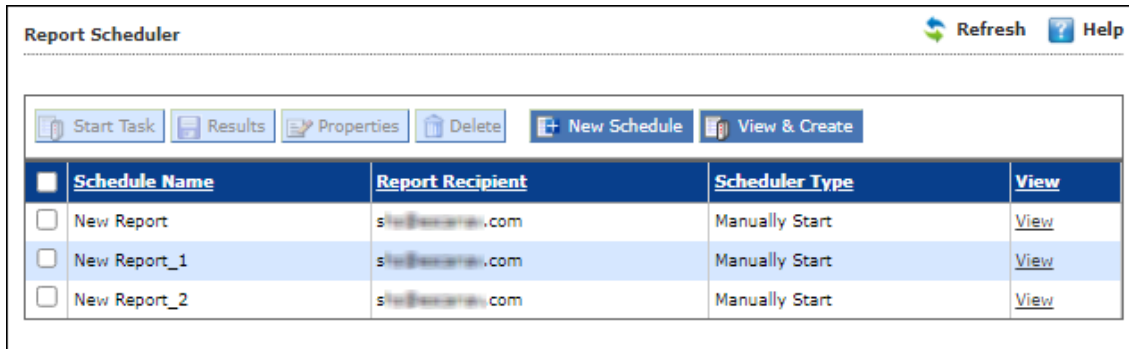
1. Select the template you want to delete.
2. Click **Delete**.  
A confirmation prompt appears.
3. Click **OK**.  
The Report Template will be deleted.



Default Report Templates cannot be deleted.

# Report Scheduler

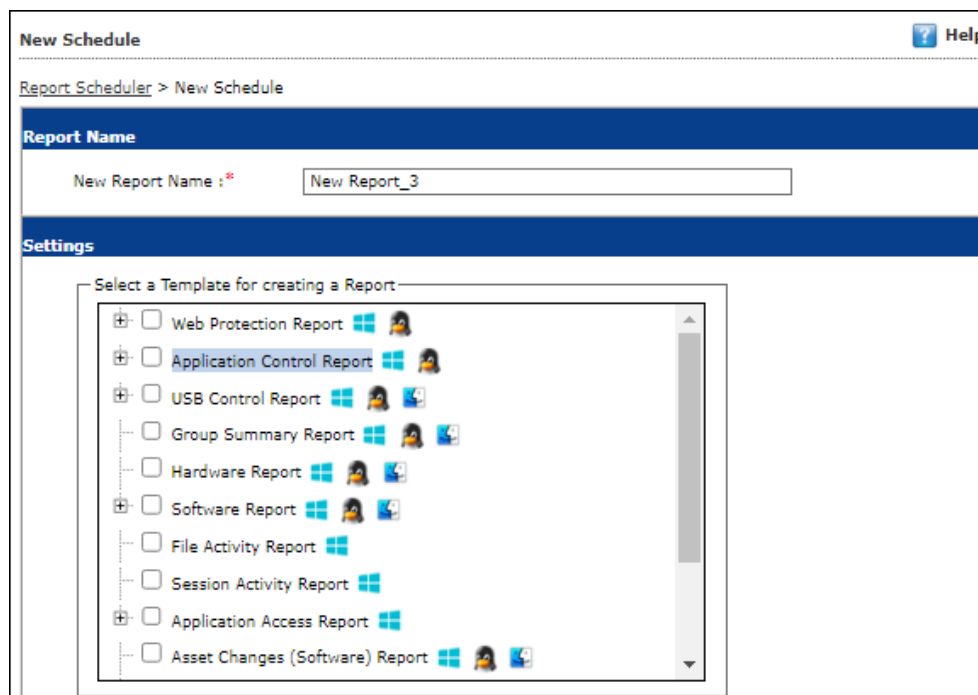
The Report Scheduler module lets you create schedule, update and run the task according to your preferences.



## Creating a Schedule

To create a Schedule,

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



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

Select Condition

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

Select Target Groups

Managed Computers

- 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  Mon  Tue  Wed  Thu  
 Fri  Sat  Sun

Monthly  Last Day of Month  ▾

At

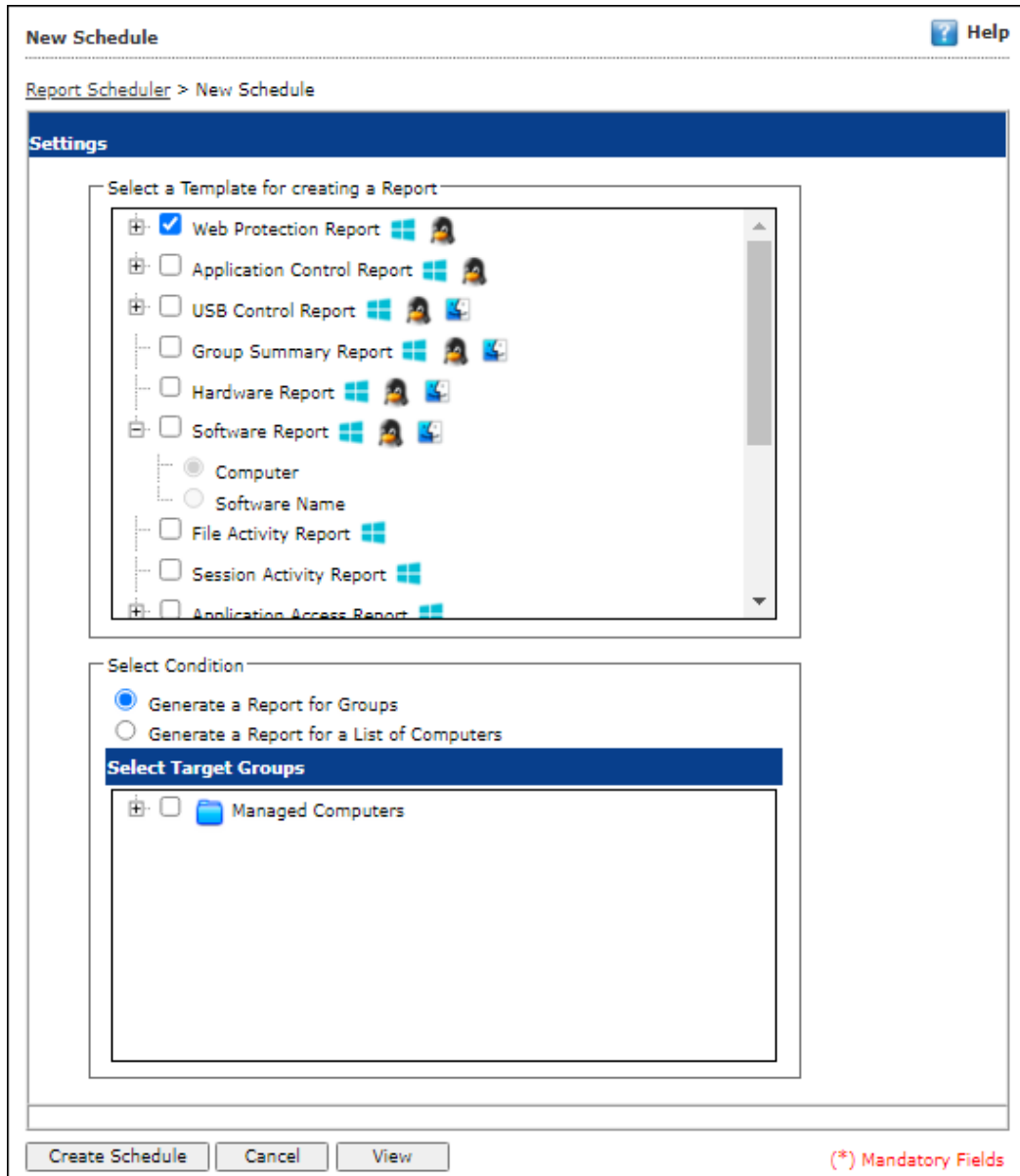
(\*) Mandatory Fields

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

# Viewing Reports on Demand

To view a report or a set of reports immediately,

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



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

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

# Managing Existing Schedule

The Report Scheduler module lets you manage the existing schedules.

**Report Scheduler**  Refresh Help

---

Start Task
 Results
 Properties
 Delete
 New Schedule
 View & Create

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

## Generating Task Report of a Schedule

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

## Viewing Results of a Schedule

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

**Results(New Report)**  Help

---

[Report Scheduler](#) > Results

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

## Viewing Properties of a Schedule

To view the properties of a schedule,

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

The screenshot shows a dialog box titled "Properties" with a "Help" icon in the top right corner. Below the title bar, the breadcrumb "Report Scheduler > Properties" is visible. The dialog has four tabs: "General" (selected), "Schedule", "Settings", and "Groups". The "General" tab contains three fields: "Schedule Name :\*" with the value "New Report", "Created:" with the value "07/03/21 11:17:33 AM", and "Status:" with the value "Task not performed yet". At the bottom left are "Ok" and "Cancel" buttons. At the bottom right is a red asterisk followed by the text "(\*) Mandatory Fields".

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

## Deleting a Schedule

To delete a report schedule,

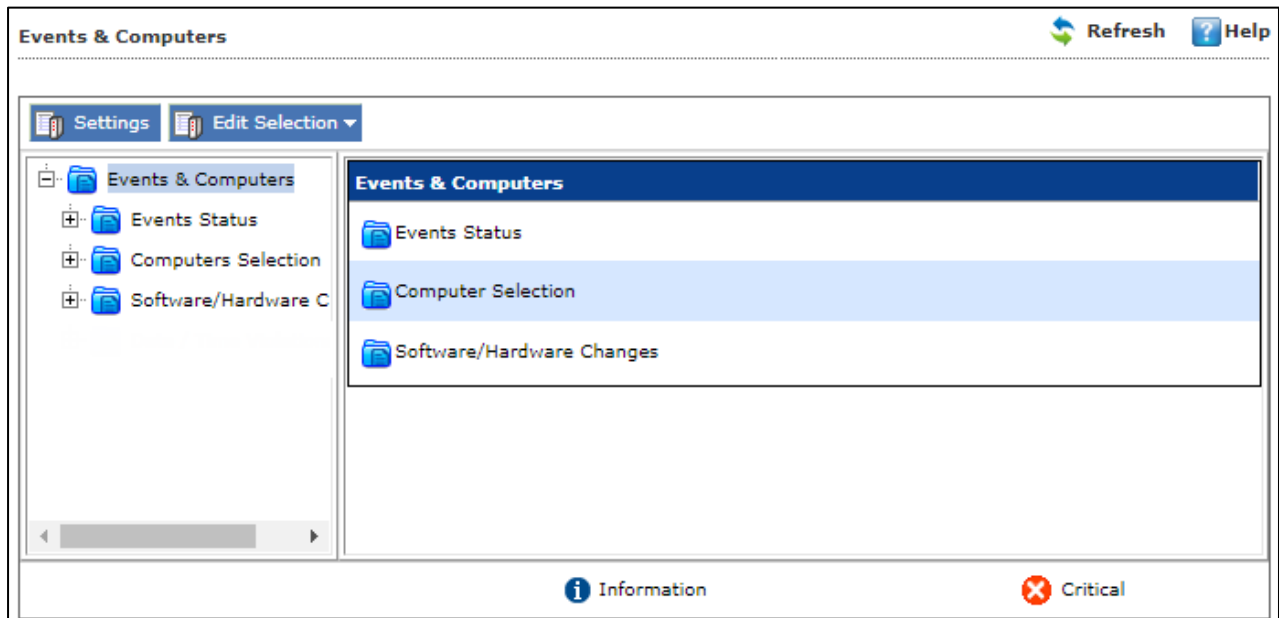
1. Select a schedule.
2. Click **Delete**.  
A confirmation prompt appears.

The screenshot shows a confirmation dialog box titled "Report Scheduler" with a close icon in the top right corner. The dialog contains a text box with the message "Do you want to Delete the Selected Task(s) ?". At the bottom are "Ok" and "Cancel" buttons.

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

# Events and Computers

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



## Events Status

The Event Status subfolder is divided into following sections:

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

### Recent

The Recent section displays both Information and Critical events.

### Critical

The Critical section displays Critical events and immediate attention.

For example, Virus detection, Monitor disabled.

The Critical events can be filtered on the basis of date range and the report can be exported in .xls or .html format.

### Information

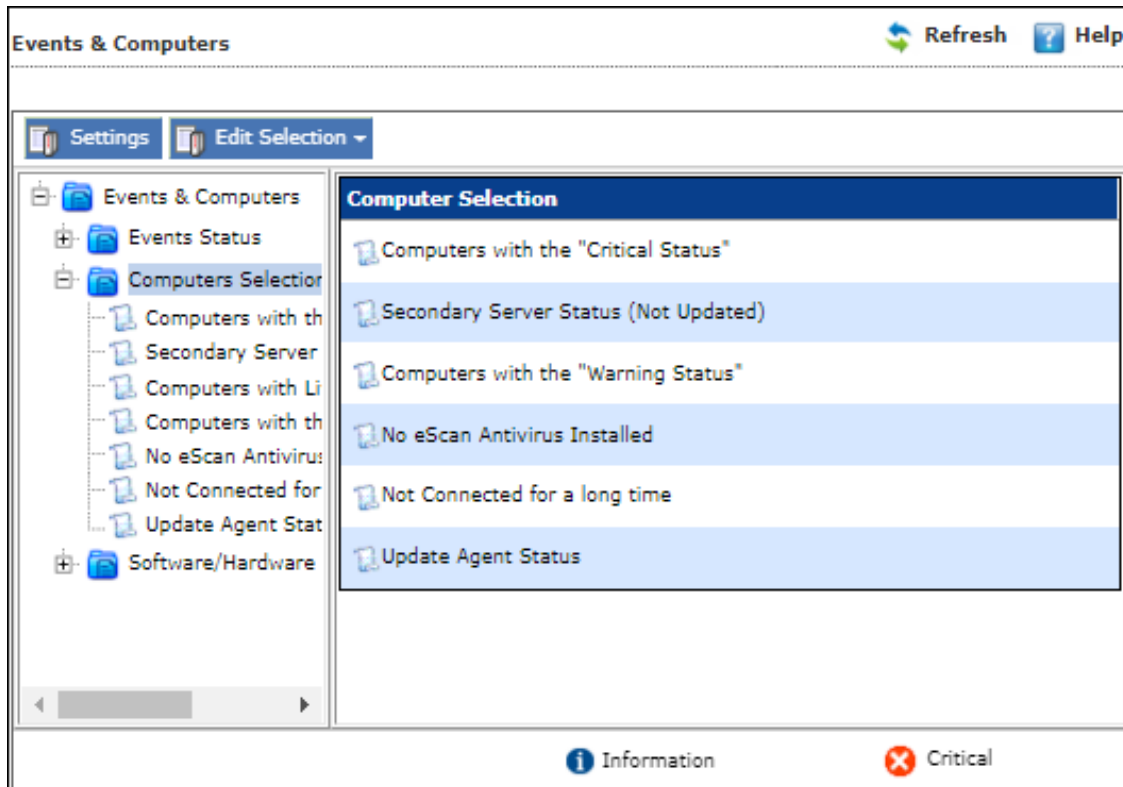
The Information section displays basic information events.

For example, Virus database update, Status.



# Computer Selection

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



The Computer Selection subfolder consists following sections:

- **Computers with the critical status**
- **Secondary Server Status (Not Updated)**
- **Computers with Live Status**
- **Computer with warning status**
- **No eScan Antivirus Installed**
- **Not connected for a long time**
- **Update Agent Status**

### Computers with the critical status

This section displays computers marked with Critical status.

### 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 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>	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.
--	---

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.

### No eScan Antivirus installed

This section displays computers on which eScan is not installed.

### Not connected for a long time

This section displays the computers which didn't connect to the eScan server for the set duration.

### Update Agent Status

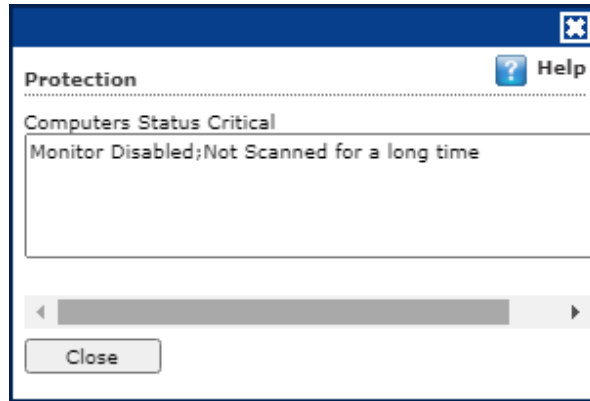
This section displays the status of computers assigned as Update Agent.

The additional settings vary depending upon the Computer Status.

## Edit Selection

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

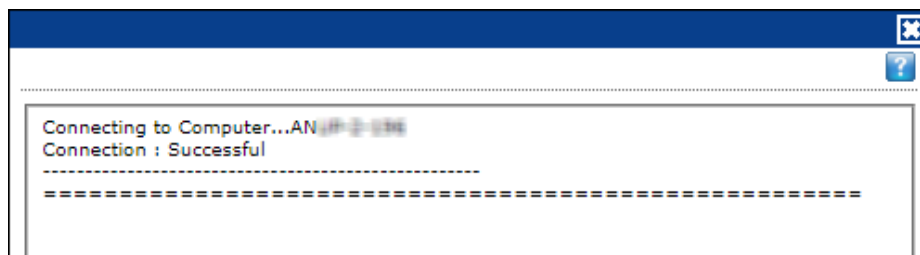
- **Protection:** This option displays the protection status of the selected computer.



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

Events & Computers							Refresh	Help
Date	Time	User's name	Event Id	Module Name	Description	Clie		
7/3/2021	12:52:35	root	File Anti-Virus (10154)	update	New virus database taken and applied [2021/07/03 07:02] [7.89103]	Upd	1 - 10 of 622   4 page	
7/3/2021	12:52:35	root	File Anti-Virus (10740)	winclient	/opt/MicroWorld/Http://192.168.0.135-222/WinC/WinC	eSc		
7/3/2021	12:52:34	root	File Anti-Virus (10154)	update	New virus database taken and applied [2021/07/03 07:02] [7.89103]	Upd		
7/3/2021	12:52:34	root	File Anti-Virus (10740)	winclient	/opt/MicroWorld/Http://192.168.0.135-222/WinC/WinC	eSc		
7/3/2021	11:30:18	root	File Anti-Virus (10154)	update	New virus database taken and applied [2021/07/03 05:05] [7.89103]	Upd		
7/3/2021	11:30:18	root	File Anti-Virus (10740)	winclient	/opt/MicroWorld/Http://192.168.0.135-222/WinC/WinC	eSc		
7/3/2021	11:30:18	root	File Anti-Virus (10740)	winclient	/opt/MicroWorld/Http://192.168.0.135-222/WinC/WinC	eSc		
7/3/2021	11:30:18	root	File Anti-Virus (10154)	update	New virus database taken and applied [2021/07/03 05:05] [7.89103]	Upd		
7/3/2021	10:30:14	root	File Anti-Virus (10740)	winclient	/opt/MicroWorld/Http://192.168.0.135-222/WinC/WinC	eSc		
7/3/2021	10:30:14	root	File Anti-Virus (10154)	update	New virus database taken and applied [2021/07/03 05:05] [7.89103]	Upd		

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



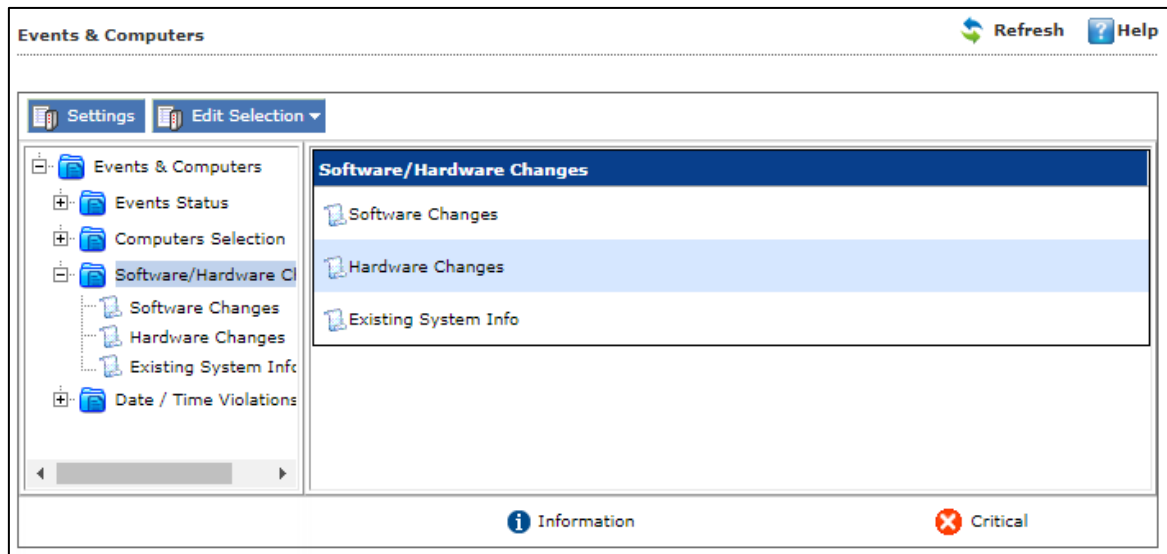
- **Remove from Group:** To learn about this option, [click here](#).
- **Connect to Client (RMM):** To learn about this option, [click here](#).
- **Force Download:** To learn about this option, [click here](#).

- **Send Message:** To learn about this option, [click here](#).
- **Check escan Port(s):** To learn about this option, [click here](#).
- **Properties:** To learn about this option, [click here](#).

## Software/Hardware Changes

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

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



### Software Changes

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

### Hardware changes

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

### Existing System Info

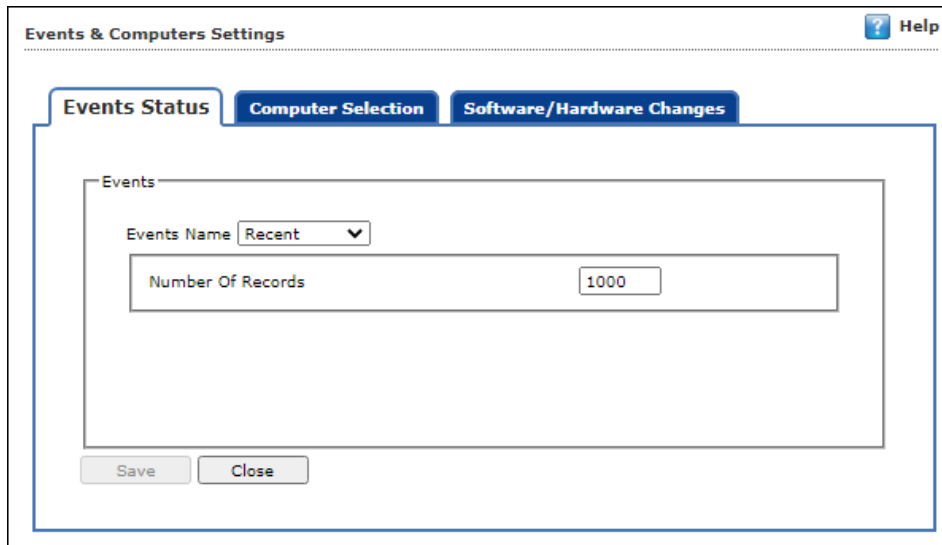
This section displays a computer's existing hardware information.

## Settings

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

## Event Status

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.
- **Information:** It displays all informative types of events, such as virus database update, status, and so on.

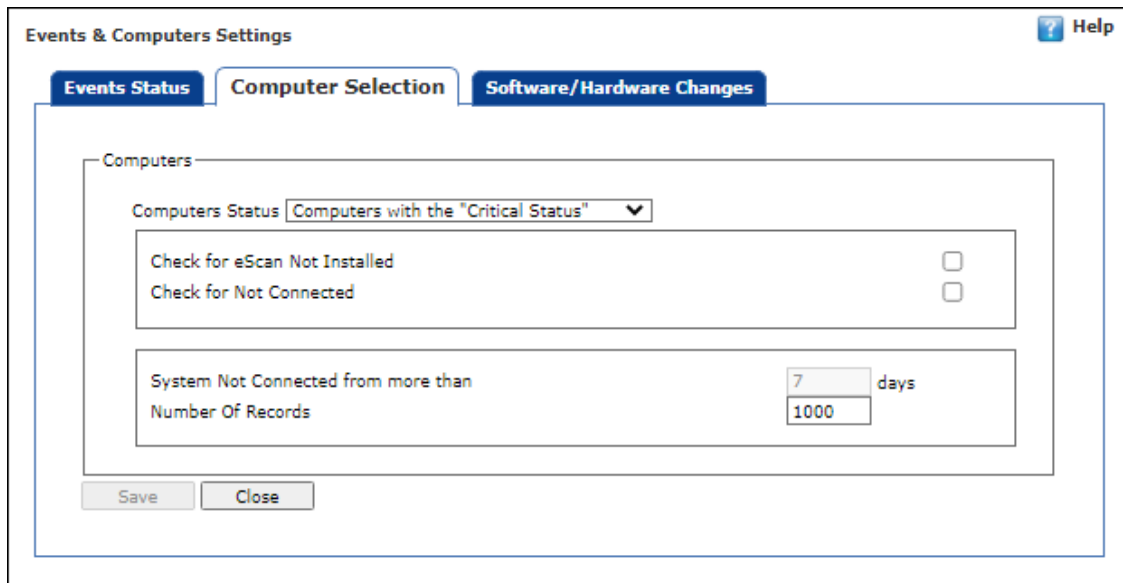
### Steps to define event status settings:

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 Not Connected:** Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **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.

### Secondary Server Status (Not Updated)

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

### Live Status

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

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

- **Check for Not Connected:** Select this checkbox to view the list of eScan client systems that have not been communicated with eScan server.
- **System Not Connected 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.

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

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

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

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

## 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 screenshot shows a web application window titled "Events & Computers Settings" with a "Help" icon in the top right. There are three tabs: "Events Status", "Computer Selection", and "Software/Hardware Changes". The "Software/Hardware Changes" tab is active. Inside this tab, there is a section labeled "Updates". Under "Updates", there is a label "Software/Hardware Changes" followed by a dropdown menu currently showing "Software Changes". Below this, there are two input fields: "Number Of Days" with a value of "1" and the unit "days", and "Number Of Records" with a value of "1000". At the bottom of the window, there are two buttons: "Save" and "Close".

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

Type of Software/Hardware Changes

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

To Change software/hardware settings, follow the steps given below:

1. Click the **Software/Hardware Changes** tab.
2. Specify the following field details.
  - **Software/Hardware Changes:** Click the drop-down and select the changes made.

- **Number of Days:** Enter the number of days, to view changes made within the specified days.
  - **Number of Records:** Enter the number of client systems that you want to view in the list.
3. Click **Save**.  
The settings get saved.

**Existing system info:** It displays the list of existing systems on which software/hardware changes made for any module, as per the protection criteria's selected in computer settings. Specify the following field details.

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

## Performing an action for computer

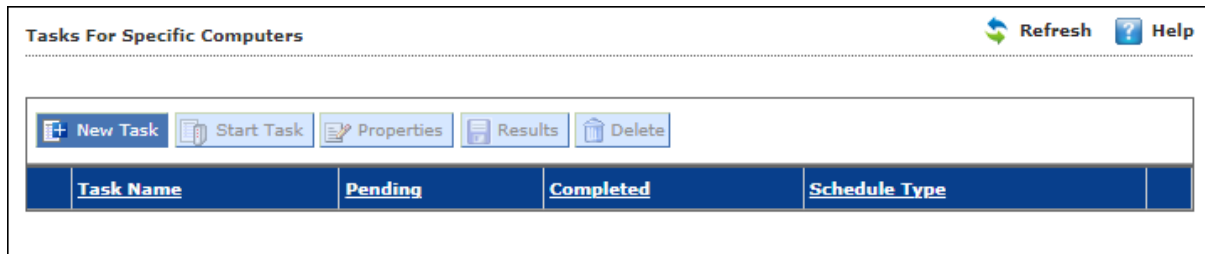
To perform an action for a computer, follow the steps given below:

1. Select a computer.
2. Click **Edit Selection** drop-down. To learn more [click here](#).
3. Click the preferred action.



# Tasks for Specific Computers

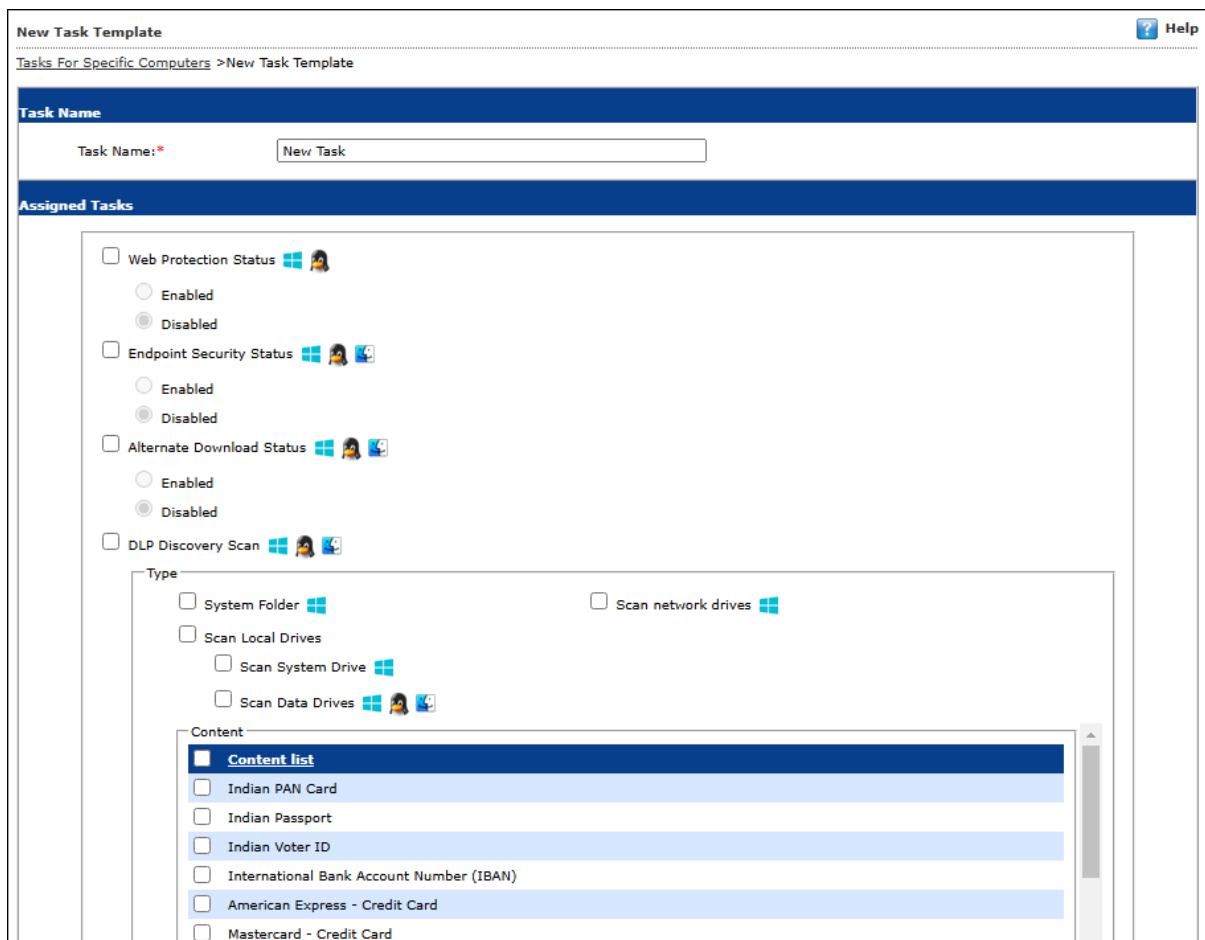
The Tasks for Specific Computers module lets you create a new task for computer(s) according to your preferences.



## Creating a task for specific computers

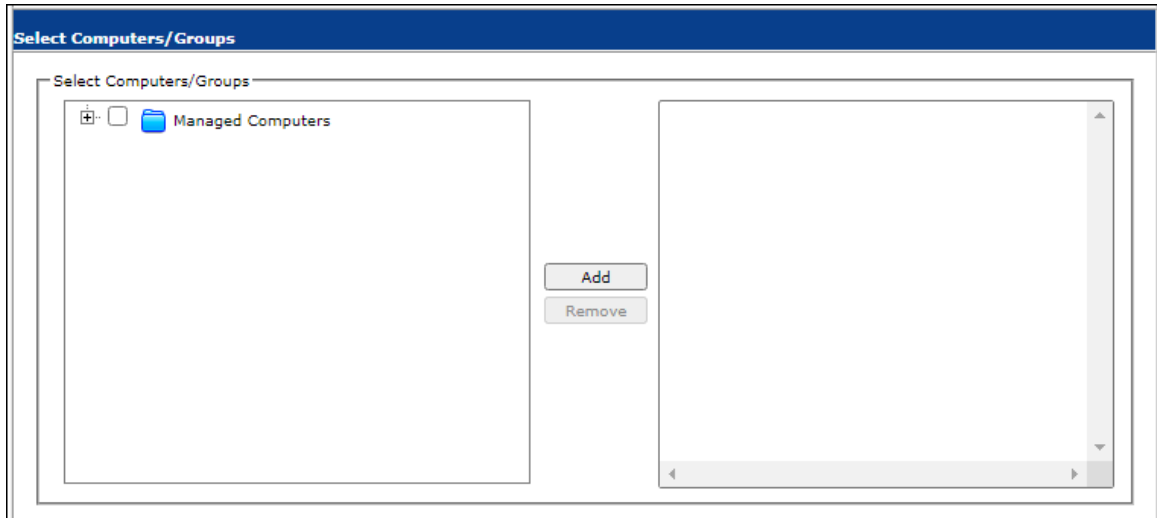
To create a task for specific computer(s), follow the steps given below:

1. In the navigation panel, click **Tasks for Specific Computers**.
2. Click **New Task**.  
New Task Template form appears.

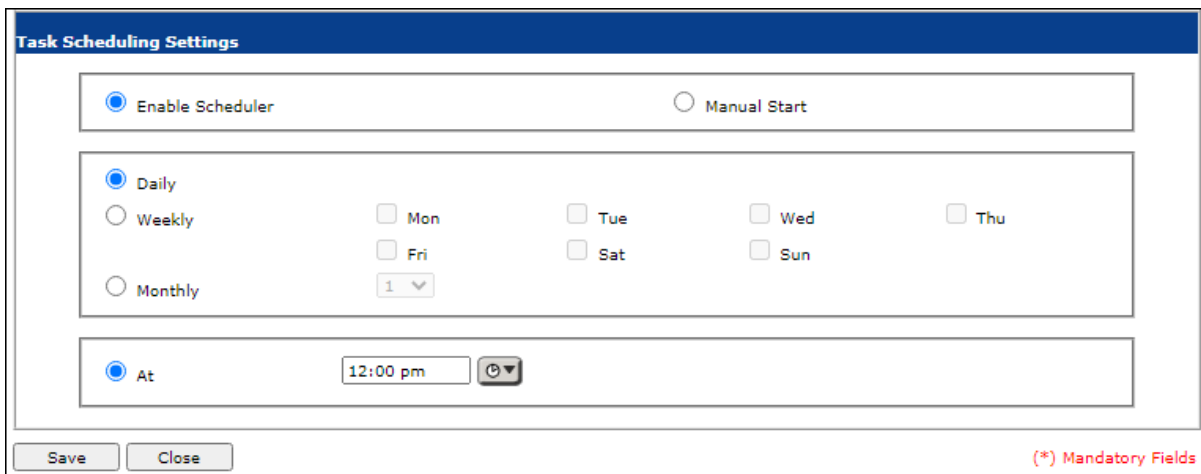


3. Enter a name for task.
4. In the **Assigned Tasks** section, select the modules to be run.

5. For example, select **DLP Discovery Scan** module.
6. And then select target drives and content types for the scan.
7. In the **Select Computers/Groups** section, select the computers/groups on which the tasks should be run and then click **Add**.



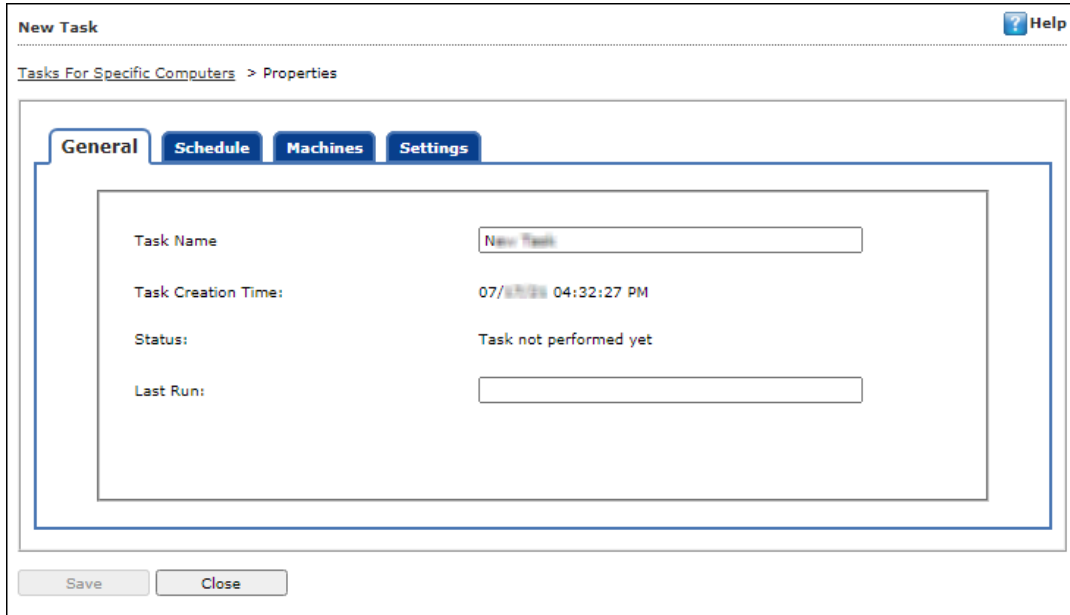
8. In the **Tasks Scheduling Settings** section, configure the schedule settings.



9. 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**.



This section will have following tabs to configure:

- **General:** This tab will display details of the task created and provides details about the task name, task creation time, 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 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**.

Client Computers	Group	Status	Date/Time
ANUP-2-336	Managed Computers\Users / Mac	Not Performed Yet	
ESR_CLIENT	Managed Computers\jrk	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

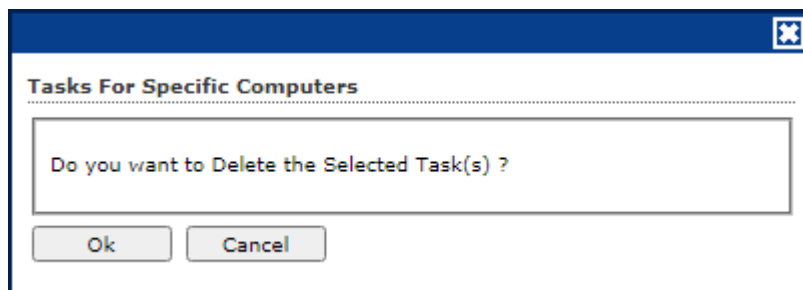
To delete a task, follow the steps given below:

1. In the Tasks for Specific Computers screen, select the task you want to delete.



	Task Name	Pending	Completed	Schedule Type	Task Status
<input checked="" type="checkbox"/>	New Task	2	0	Automatic Scheduler	

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.

The screenshot shows the 'Asset Management' interface with the 'Hardware Report' tab selected. The table displays the following data:

Computer Name	Group	IP Address	User's name	Operating System	Service Pack	OS Version	OS Installed Date	Internet Explorer	Processor
DESKTOP-LR63AH4	QA	192.168.0.199	DESKTOP-LR63AH4\Administrator	Windows 10 Home Edition 64-bit	Build 10586.164	Client:10.0	28 Aug 2020 13:09:26	IE:11.162.10586.0	Intel(R) Core(TM) i7-7700 C
QA-BHUSHAN	Managed Computers	192.168.0.151	QA-BHUSHAN\QARAO	Windows 7 Professional 64-bit	Build 7600.0	Client:6.1	30 May 2019 14:07:31	IE:8.0.7600.16385	Intel(R) Core(TM) i3 CPU 53

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
- Wifi MAC [Adapter]
- USB MAC [Adapter]
- PC Identifying Number
- Motherboard Serial No
- Network Speed
- Disk Free Space
- PC Manufacturer
- PC Model
- MB Manufacturer
- Graphic Card Details
- Machine Type
- BitLocker Status

- Software

To view the list of Software along with the installation dates, click **View** in **Software** column.

## Filtering Hardware Report

To filter the Hardware Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

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

### Include/Exclude

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

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

The Hardware Report will be filtered according to your preferences.

Reset all filter criteria in all field, click **Reset**.

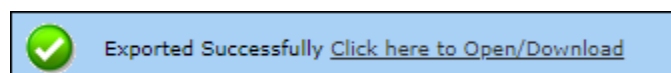
## Exporting Hardware Report

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

Export Option field expands.

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.

Software Name	Computer Count
Brave	1
Client Authentication Agent	1
Dropbox	1
eScan Corporate - 360	1
eScan Corporate for Windows	2
Google Chrome	3
Microsoft SQL Server 2008 R2	1
Microsoft SQL Server 2008 R2 Native Client	1
Microsoft SQL Server 2008 R2 Setup (English)	1
Microsoft SQL Server 2008 Setup Support Files	1

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

Computer list window appears displaying following details:

- Computer Name
- Group
- IP Address
- Operating System
- Software Version
- Installed Date

## Filtering Software Report

To filter Software Report, click **Filter Criteria** field.

Filter Criteria field expands.

### Software Name

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

### Computer Name

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

### OS Type

Enter the OS type.

### Include/Exclude

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

### Group By

The results can be grouped by Software name, Computer name or Group. If Group option is selected, the report can be filtered for a specific group.

After entering data in all fields, click **Search**.

The Software Report will be filtered according to your preferences.

Reset all filter criteria in all field, click **Reset**.

## Exporting Software Report

To export the Software Report, click **Export Option**.

Export Option field expands.

The screenshot shows a dropdown menu titled "Export Option" with three radio button options: "Excel", "PDF", and "HTML". The "HTML" option is selected. Below the radio buttons are two buttons: "Export" and "Export Detailed Report".

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



Click the link to open/download the file.

## Software License

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

The screenshot shows the "Software License" tab in the "Asset Management" interface. It displays a table with the following data:

License Key	Software Name	Computer Count
BB	Microsoft Office Professional Plus 2010	1
YT	Windows 10 Home Edition 64-bit	1
Z4	Windows 7 Professional 64-bit	1

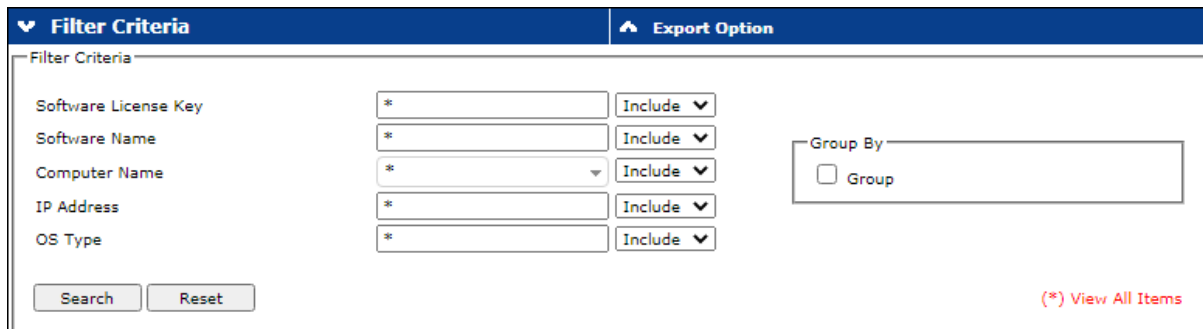
The log displays License Key, Software Name, and Computer Count.



To see more details of the computer's license key installed, click the numerical value in License Key or Computer Count column.

## Filtering Software License Report

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



Filter Criteria	Export Option
Filter Criteria	
Software License Key	* <input type="text"/> Include ▼
Software Name	* <input type="text"/> Include ▼
Computer Name	* <input type="text"/> Include ▼
IP Address	* <input type="text"/> Include ▼
OS Type	* <input type="text"/> Include ▼
Group By <input type="text"/>	
<input type="checkbox"/> Group	
Search Reset	
(*) View All Items	

### Software License Key

Entering the license key displays suggestions. Select the appropriate key.

### Software Name

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

### Computer Name

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

### 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.

### 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 License Report will be filtered according to your preferences.

Reset all filter criteria in all the fields, click **Reset**.

## Exporting Software License Report

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

Filter Criteria	Export Option					
Export Option						
<input type="radio"/> Excel	<input type="radio"/> PDF	<input checked="" type="radio"/> HTML	<input type="button" value="Export"/>	<input type="button" value="Export Detailed Report"/>	<input checked="" type="checkbox"/> Windows OS	<input checked="" type="checkbox"/> Microsoft Office

Select whether you want report for **Windows OS** and **Microsoft Office**.  
Select the preferred option and then click **Export**.

OR

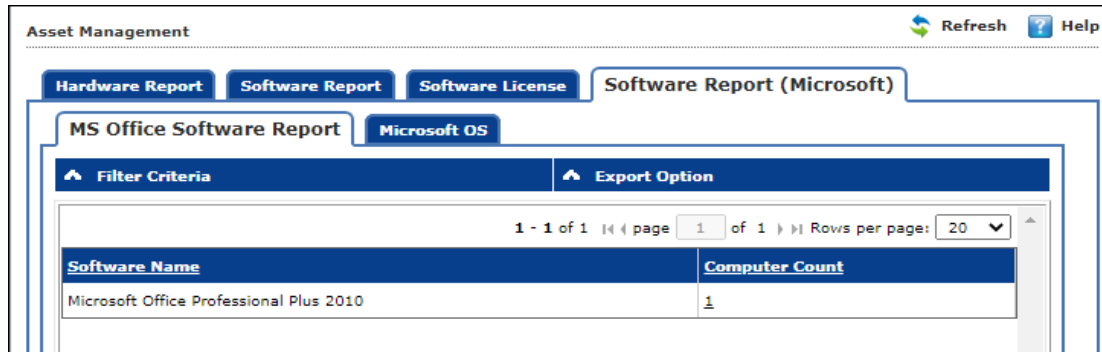
To export a detailed report, select the preferred option and then click **Export Detailed Report**.  
A success message appears.



Click the link to open/download the file.

# Software Report (Microsoft)

The Software Report (Microsoft) displays details of the Microsoft Software installed on the computers.



The tab consists following subtabs:

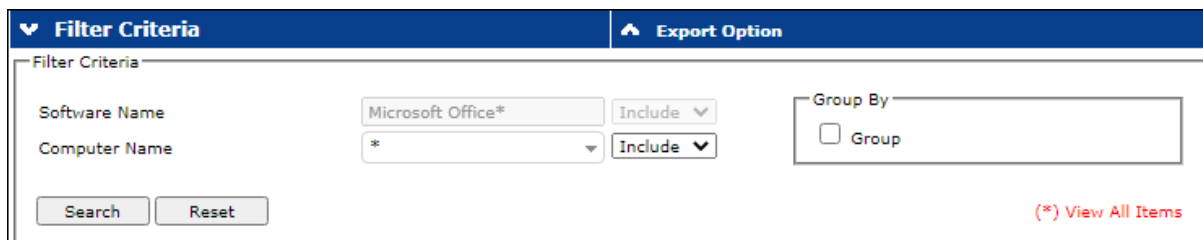
**MS Office Software Report** – It displays Microsoft software name and computer count.

**Microsoft OS** – It displays Operating System, Service Pack, OS version and computer count.

## Filtering MS Office Software Report

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

Filter Criteria field expands.



### Software Name

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

### Computer Name

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

### Include/Exclude

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

### Group By

If this 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.

Reset all filter criteria in all the fields, click **Reset**.

## Exporting MS Office Software Report

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

Filter Criteria	Export Option	
Export Option		
<input type="radio"/> Excel	<input type="radio"/> PDF	<input checked="" type="radio"/> HTML
<input type="button" value="Export"/> <input type="button" value="Export Detailed Report"/>		

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.  
A success message appears.



Click the link to open/download the file.

## Filtering Microsoft OS Report

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

Filter Criteria	Export Option
Filter Criteria	
Operating System	* <input type="text"/> Include ▼
Computer Name	* <input type="text"/> Include ▼
Service Pack	* <input type="text"/> Include ▼
OS Version	* <input type="text"/> Include ▼
Group By	
<input type="checkbox"/> Group	
<input type="button" value="Search"/> <input type="button" value="Reset"/>	
(*) <a href="#">View All Items</a>	

### Operating System

Entering the operating system name displays list of suggestions. Select the appropriate OS.

### Computer Name

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

### Service Pack

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

### OS Version

Entering the OS version displays list of suggestions. Select the appropriate OS version.

### Include/Exclude

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

### Group By

If **Group** option is selected, the report can be filtered for a specific group.

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

The Microsoft OS report will be filtered according to your preferences.

Reset all filter criteria in all the fields, click **Reset**.

## Exporting Microsoft OS Report

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

Export Option field expands.



The screenshot shows a form titled "Export Options" with three radio button options: "Excel", "PDF", and "HTML". The "HTML" option is selected. To the right of the radio buttons are two buttons: "Export" and "Export Detailed Report".

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



Click the link to open/download the file.

# User Activity

The User Activity module lets you monitor Print, Session and File activities occurring on the client computers. It also provides the reports of the running applications. It consists following sub modules:

- **Print Activity**
- **Session Activity Report**
- **File Activity Report**
- **Application Access Report**

## Print Activity

The Print Activity sub module monitors and logs print commands sent by all computers. It also lets you filter the logs on the basis of Computer name, Printer and Username. Furthermore, the module lets you export a detailed print activity report in XLS, PDF, and HTML formats. The log report generated consist information such as Print Date, Machine Name, IP Address, Username, Printer Name, Document Name along with number of Copies and Pages.

Printer Name	Copies	Pages
NFIBBAC2B (HP LaserJet 400 M121n)	5	5

## Viewing Print Activity Log

To view the Print log of a Printer, click its numerical value under **Copies** or **Pages** column. Print Activity window appears displaying details.

Client Date	Machine Name	IP Address	User name	Printer Name	Document Name	Copies
05/08/21 4:23:03 PM	QA-EER	192.168.0.117	QA-EER Administrator	NFIBBAC2B (HP LaserJet 400 M121n)	Untitled - Notepad	1
05/08/21 4:22:40 PM	QA-EER	192.168.0.117	QA-EER Administrator	NFIBBAC2B (HP LaserJet 400 M121n)	Untitled - Notepad	1
05/08/21 4:22:09 PM	QA-EER	192.168.0.117	QA-EER Administrator	NFIBBAC2B (HP LaserJet 400 M121n)	Untitled - Notepad	1
05/08/21 4:21:42 PM	QA-EER	192.168.0.117	QA-EER Administrator	NFIBBAC2B (HP LaserJet 400 M121n)	Untitled - Notepad	1
05/08/21 4:21:31 PM	QA-EER	192.168.0.117	QA-EER Administrator	NFIBBAC2B (HP LaserJet 400 M121n)	Untitled - Notepad	1

## Exporting Print Activity Log

To export this generated log,

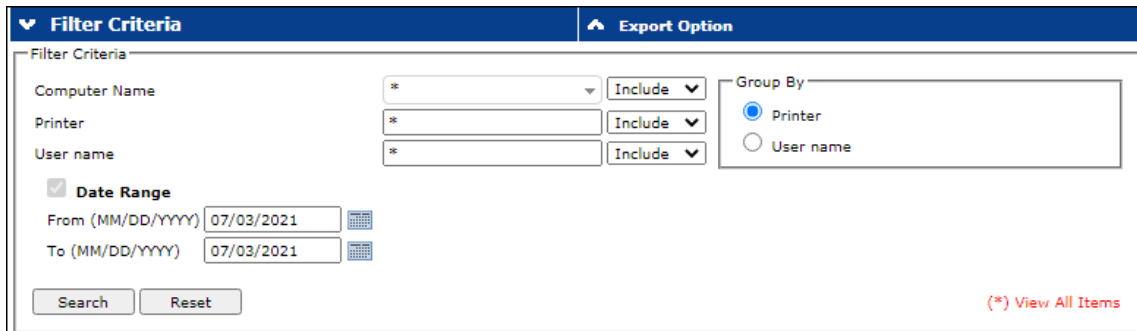
1. Click the Export to drop-down.
2. Select a preferred format.
3. Click **Export**.  
A success message appears.

 Exported Successfully [Click here to Open/Download](#)

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** checkbox. Afterwards, click the **calendar** icon and select **From** and **To** dates.

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

The Print activity log will be filtered and generated according to your preferences.

Reset all filter criteria fields, click **Reset**.

### Group By

To view results by specific printer, select **Printer**, Date Range and then click **Search**.

To view results by specific user name, select **User name**, Date Range and then click **Search**.

## Exporting Print Activity Report

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

Export Option field expands.

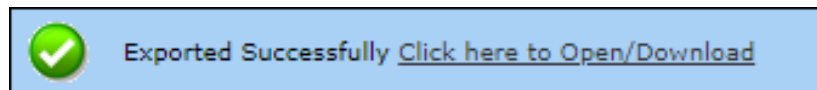
The dialog box has two tabs: 'Filter Criteria' and 'Export Option'. Under 'Export Option', there are three radio buttons: 'Excel', 'PDF', and 'HTML'. The 'HTML' radio button is selected. To the right of the radio buttons are two buttons: 'Export' and 'Export Detailed Report'.

Select the preferred option and then click **Export**.

OR

To export a detailed report, select the preferred option and then click **Export Detailed Report**.

A success message appears.



Click the link to open/download the file.

## Print Activity Settings

The Print Activity Settings lets you keep track of printers by adding them in a group and assigning it an alias name. The printers can be added or removed from this alias group.

To configure Print Activity Settings,

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

The dialog box is titled "Printer Merge Setting". It contains an "Alias Name" text field with an "Add" button to its right. Below this are three list boxes: "Alias List", "Printer List", and "Printer List". The "Alias List" box contains one entry: "Canon i4920". The "Printer List" box is empty. Each list box has a "Remove" button above it. At the bottom of the dialog is a "Save" button.

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



# Session Activity Report

This sub module monitors and logs the session activity of the managed computers. It displays a report of the Operation type, Date, Computer name, Group, IP address and event description. With this report the administrator can trace the user Logon and Logoff activity along with remote sessions that took place on all managed computers.

## Viewing Session Activity Log

In the navigation panel, click **User Activity > Session Activity Report**.

The log displays list of session activities and type of operation performed. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

Operation Type	Client Date	Computer Name/Ip	Group	IP Address	Description
Session LogOn	03/07/21 12:50:17 PM	WI\IQAD07	QA_TENM	192.168.0.85	User LogOn User's name: WI\IQAD07
Session LogOff	03/07/21 10:55:49 AM	WI\IQAD07	QA_TENM	192.168.0.85	User LogOff User's name: WI\IQAD07
Remote Session Disconnect	03/07/21 10:55:48 AM	WI\IQAD07	QA_TENM	192.168.0.85	Remote Session Connect User's name: WI\IQAD07 Name of Remote PC: WI\ESCANSERVER IP of Remote PC: 192.168.0.135
Remote Session Connect	03/07/21 10:55:47 AM	WI\IQAD07	QA_TENM	192.168.0.85	Remote Session Connect User's name: WI\IQAD07 Name of Remote PC: WI\ESCANSERVER IP of Remote PC: 192.168.0.135
Remote Session Disconnect	03/07/21 10:55:34 AM	WI\IQAD07	QA_TENM	192.168.0.85	Remote Session Connect User's name: WI\IQAD07 Name of Remote PC: WI\ESCANSERVER IP of Remote PC: 192.168.0.135
Remote Session Connect	03/07/21 10:55:33 AM	WI\IQAD07	QA_TENM	192.168.0.85	Remote Session Connect User's name: WI\IQAD07 Name of Remote PC: WI\ESCANSERVER IP of Remote PC: 192.168.0.135
Start up	03/07/21 10:43:23 AM	WI\ESCANSERVER	Managed Computers	192.168.0.135	User LogOn User's name: WI\ESCANSERVER\Administrator
Session LogOn	03/07/21 10:43:09 AM	WI\ESCANSERVER	Managed Computers	192.168.0.135	
Start up	03/07/21 10:42:13 AM	WI\IQAD07	QA_TENM	192.168.0.85	
Shut Down	03/07/21 10:37:44 AM	WI\ESCANSERVER	Managed Computers	192.168.0.135	

## Filtering Session Activity Log

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

Filter Criteria field expands.

Filter Criteria
Export Option

Filter Criteria

Computer Name

Operation Type

Description

Date Range  
 From (MM/DD/YYYY)    
 To (MM/DD/YYYY)

IP Address

Group

(\*) View All Items

Filter Criteria lets you filter and generate the log according to your preferences. The checkbox selected will be added as a column in the report.

### Computer Name

Click the drop-down and select the preferred computers.

### Operation Type

Click the drop-down and select the preferred activities.

### Include/Exclude

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


### Description

Select this checkbox to display the description of the session in the report.

### IP Address

Enter the IP address in this field.

### Group

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

### Date Range

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

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

Reset all filter criteria fields, click **Reset**.

## Exporting Session Activity Report

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

Export Option field expands.



The screenshot shows a user interface with two tabs: "Filter Criteria" and "Export Option". The "Export Option" tab is active and expanded, showing three radio button options: "Excel", "PDF", and "HTML". The "HTML" option is selected. To the right of these options is an "Export" button.

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 sub module displays a report of the files created, copied, modified, and deleted on managed computers. The File Activity report will be generated when Record files copied is enabled in endpoint security. Additionally in case of a misuse of any official files can be tracked down to the user through the details captured in the report. Select and filter the report based on any of the details captured.

## Viewing File Activity Log

In the navigation panel, click **User Activity > File Activity Report**.

The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

Client Date	Computer Name/Ip	Group	IP Address	User's name	File Action Type	Drive Type	Source File	D
6/19/2021 6:11:04 PM	PRASHANT-QA	QA_TEAM	192.168.0.102	PRASHANT-QA Administrator	Copy	Fixed Drive	C:\Users\Administrator\Downloads\unconfirmed_813948.unconfirmed	C:
6/19/2021 6:11:13 PM	PRASHANT-QA	QA_TEAM	192.168.0.102	PRASHANT-QA Administrator	Modify	Fixed Drive		C:
6/19/2021 6:11:18 PM	PRASHANT-QA	QA_TEAM	192.168.0.102	PRASHANT-QA Administrator	Delete	Fixed Drive		C:
6/21/2021 11:17:06 AM	Wih-QA007	QA_TEAM	192.168.0.85	Wih-QA007 user	Modify	Fixed Drive		C:
6/22/2021 11:04:10 AM	Wih-QA007	QA_TEAM	192.168.0.85	Wih-QA007 user	Delete	Network Drive		\\
6/22/2021 11:04:10 AM	Wih-QA007	QA_TEAM	192.168.0.85	Wih-QA007 user	Delete	Network Drive		\\
6/22/2021 11:04:10 AM	Wih-QA007	QA_TEAM	192.168.0.85	Wih-QA007 user	Delete	Network Drive		\\
6/22/2021 11:05:11 AM	Wih-QA007	QA_TEAM	192.168.0.85	Wih-QA007 user	Delete	Network Drive		\\
6/23/2021 11:29:58 AM	Wih-QA007	QA_TEAM	192.168.0.85	Wih-QA007 user	Create	Fixed Drive	NavFile	C:
6/23/2021 11:33:55 AM	Wih-QA007	QA_TEAM	192.168.0.85	Wih-QA007 user	Modify	Fixed Drive		C:

## Filtering File Activity Log

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

Filter Criteria field expands.

**Filter Criteria**

Filter Criteria

- Computer Name  Include ▼
- User's name  Include ▼
- File Action Type  Include ▼
- Source File  Include ▼
- Application  Include ▼
- Date Range
 

From (MM/DD/YYYY) 
 To (MM/DD/YYYY)

Enable search by typing keywords on above fields ( Note: By enabling this option page loading can get delayed )

**Export Option**

- IP Address  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 checkbox selected will be added as a column in the report.

### Computer Name

Click the drop-down and select the preferred computers.

### Username

Enter the username of the computer.

### File Action type

Click the drop-down and select a preferred file action.

### Source File

Enter the source file's name.

### Application

Enter an application's name.


### Include/Exclude

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

### IP Address

Enter an IP address.

### Group

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

### Drive Type

Click the drop-down and select the drive type.

### Destination File

Enter the file path.


### Date Range

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

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

Reset all filter criteria fields, click **Reset**.

This checkbox **Enable search by typing keywords on above fields** allows you to search by typing keywords.

 <b>NOTE</b>	Select “ <b>Enable search by typing keywords on above fields</b> ” option page loading can get delayed.
--	---

## Exporting File activity Report


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

Export Option field expands.

Filter Criteria	Export Option		
Export Option			
<input type="radio"/> Excel	<input type="radio"/> PDF	<input checked="" type="radio"/> HTML	<input type="button" value="Export"/>

Select the preferred option and then click **Export**.

A success message appears.

 Exported Successfully <a href="#">Click here to Open/Download</a>
---

Click the link to open/download the file.

# Application Access Report

The Application Access Report sub module gives the detailed view of all the applications accessed by the computers in the Managed Computers.

## Viewing Application Access Report

In the navigation panel, click **User Activity > Application Access Report**.

The log displays list of files and the type of operation performed on them. Options for Filtering or Exporting the log in desired formats are also present on the same interface.

Application Name	Total Duration (DD:HH:MM:SS)
Dropbox	00:00:06:10
Google Chrome	00:04:04:12
Internet Explorer	00:04:20:22
Notepad	00:00:00:23
Qt Qtwebengineprocess	00:00:03:47
Remote Desktop Connection	00:00:00:44
Secunia PSI Tray	00:02:22:45
Windows Command Processor	00:00:21:22
WordWeb	00:02:30:56

By clicking on the duration present under **Total Duration (DD:HH:MM:SS)** column, you will get the details of the computer name accessed the app and duration.

Computer Name	Total Duration (DD:HH:MM:SS)
WI-E-SCAN-SERVE R	00:13:50:41

Again, if you click on the duration, you will get detailed view of the app accessed by the computer along with the date, time, and application path.

Application Name	Start Time	End Time	Total Duration (DD:HH:MM:SS)	Application Path
AnyDesk.exe	09/07/21 11:51:05 AM	09/07/21 12:05:14 PM	00:00:14:08	C:\Program Files\AnyDesk\AnyDesk.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 checkbox selected will be added as a column in the report.

### Application Name

Entering the Application name displays suggestions. Select the appropriate application.

### Computer Name

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

### IP Address

Enter the IP address in this field.

### Include/Exclude

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

### Group By

The results can be grouped by Application name or Computer name.

### Date Range

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

After entering data in all fields, click **Search**.

The Application Access Report will be filtered according to your preferences.

Reset all filter criteria fields, click **Reset**.

## Exporting Application Access Report

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

Export Option field expands.

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



Click the link to open/download the file.

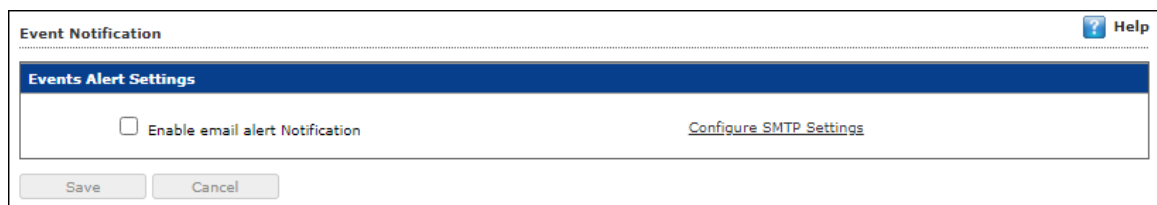
# Notifications

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

- **Event Alert**
- **Unlicensed Move Alert**
- **New Computer Alert**
- **SMTP Settings**

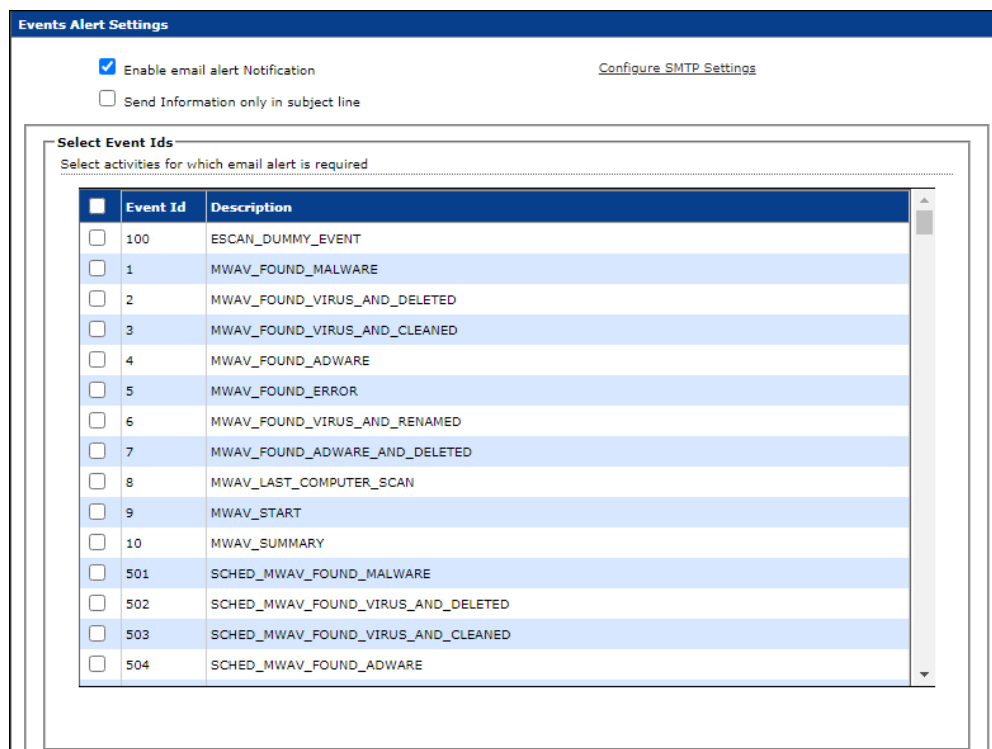
## Event Alert

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



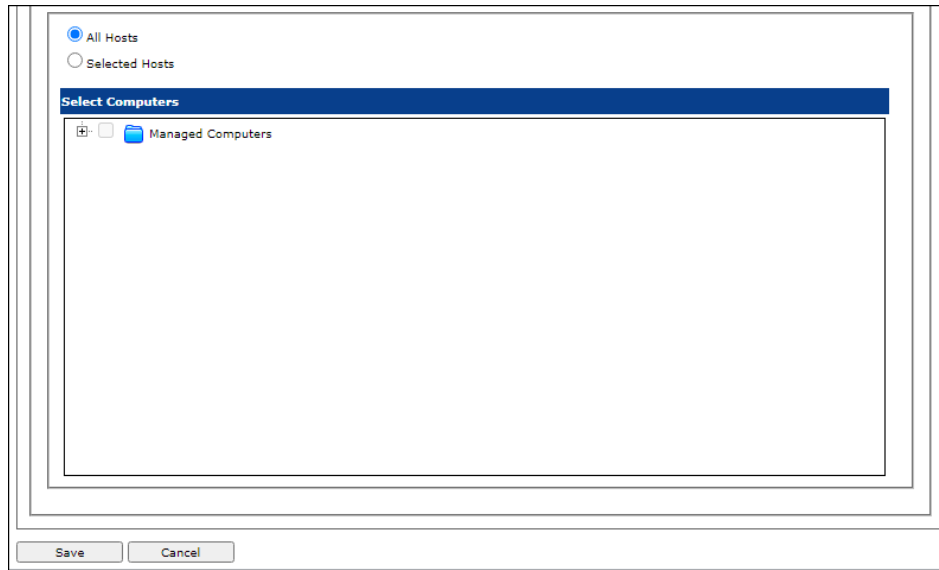
To enable the event alert,

1. In the navigation panel, click **Notifications > Event Alert**.
2. Select the checkbox **Enable email alert Notification**.
3. Select the checkbox **Send Information only in subject line**.  
This checkbox enable after selecting enable email alert notification.
4. Select the events from the list for which you prefer an alert.





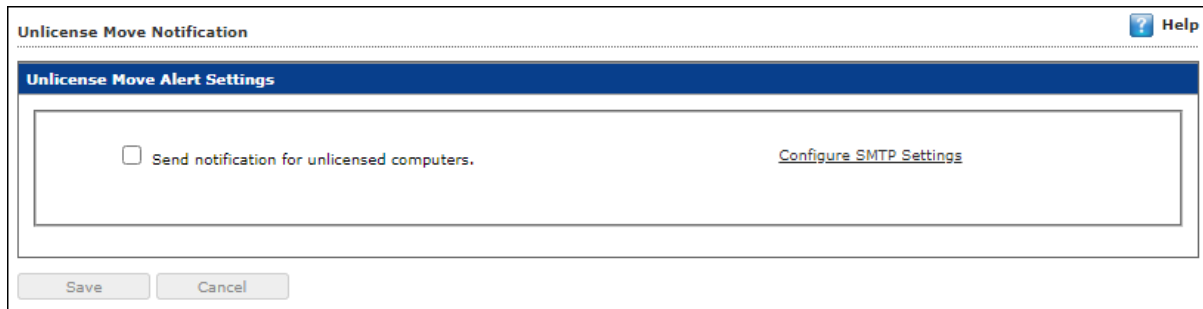
5. Select the required hosts or group.



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

## Unlicensed Move Alert

This sub module lets you enable notification alert when a computer automatically moves to Unlicensed Computers category based on the setting done (under events and computers) for the computer which is not connected to the server for a long time.



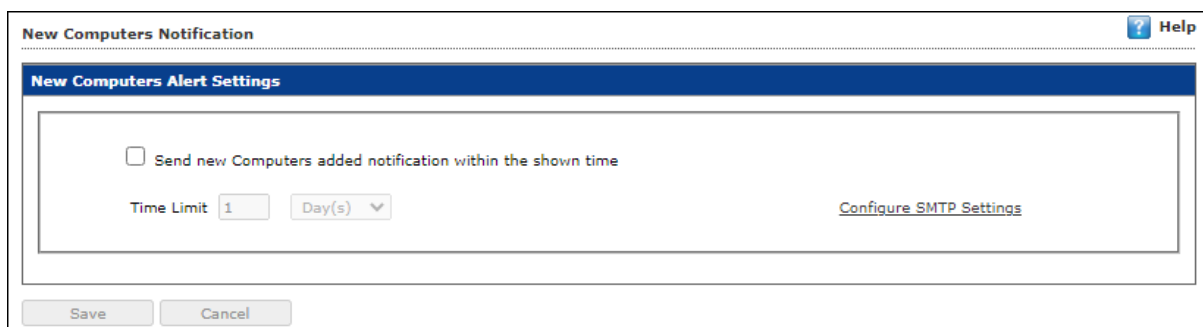
To enable the unlicensed move alert,

1. In the navigation panel, click **Notifications > Unlicensed Move Alert**.
2. Select the checkbox **Send notification for unlicensed computers**.
3. Click **Save**.

The Unlicensed Move Alert Settings will be saved.

## New Computer Alert

This sub module 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.



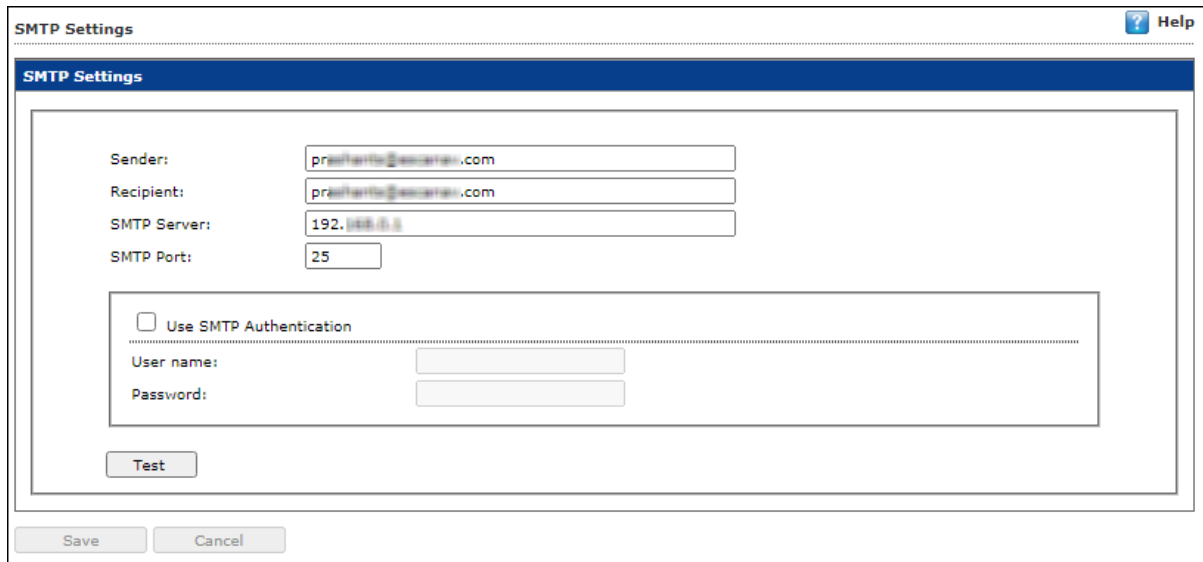
To enable the new computer alert, follow the steps given below:

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.

# SMTP Settings

This sub module lets you configure the SMTP settings for all the email notifications.



The screenshot shows a web-based configuration window titled "SMTP Settings". At the top right, there is a "Help" icon. The main content area contains the following fields:

- Sender:
- Recipient:
- SMTP Server:
- SMTP Port:

Below these fields is a section for authentication:

- Use SMTP Authentication
- User name:
- Password:

At the bottom of the main content area is a "Test" button. Below the entire configuration area are "Save" and "Cancel" buttons.

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

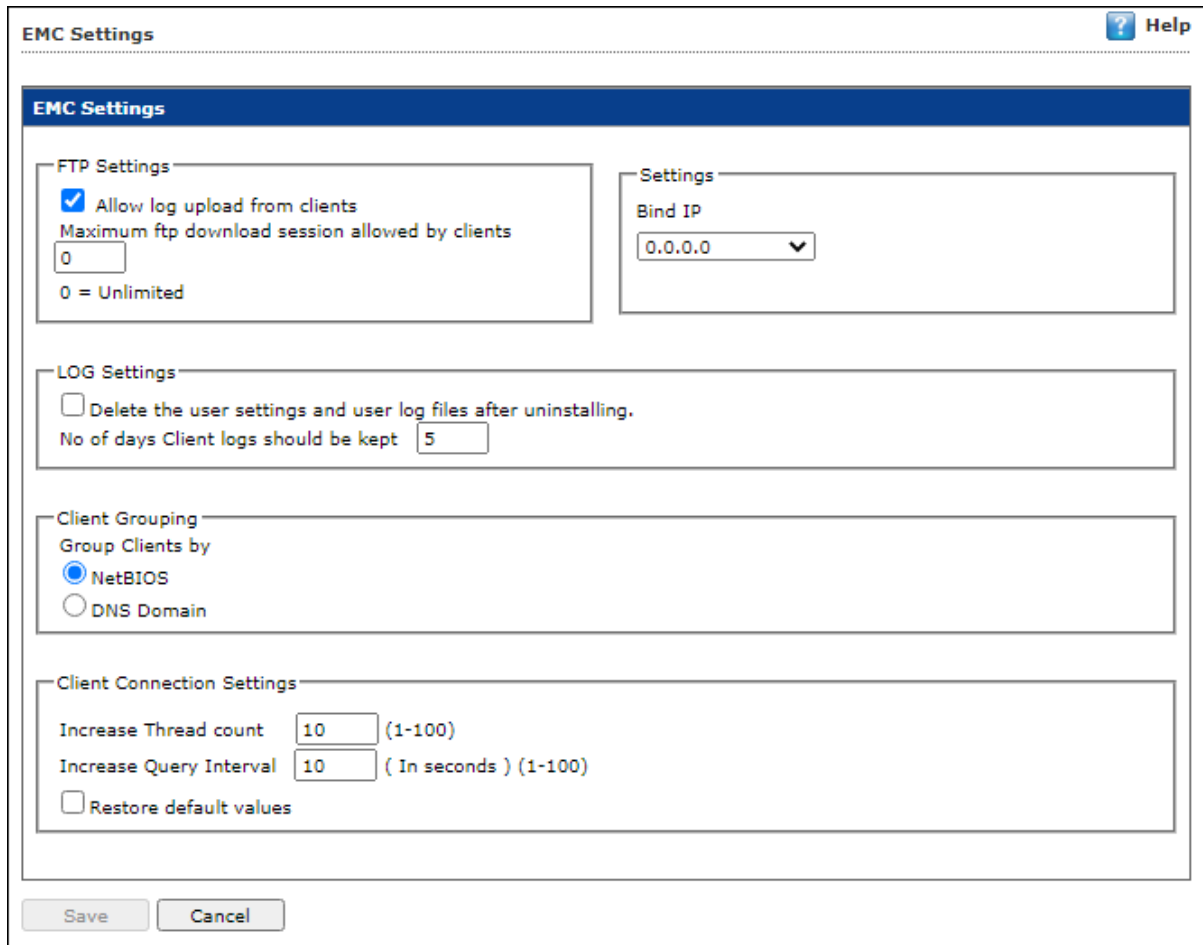
The Settings module lets you configure general settings. It contains following sub modules.

- **EMC Settings:** This sub module lets you define settings for FTP sessions, Log Settings, Client Grouping and Client connection settings.
- **Web Console Settings:** This sub module lets you define settings for web console timeout, Dashboard Settings, Login Page settings, SQL Server Connection settings, SQL Database compression settings.
- **Update Settings:** This sub module lets you define settings for General Configuration, Update Notifications, and Scheduling.
- **Auto-Grouping:** This sub module lets you define settings for Grouping of computers after installation of eScan client is carried out.
- **Two-Factor Authentication:** This sub module 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 dialog box with the following sections:

- FTP Settings:** Includes a checked checkbox for "Allow log upload from clients" and a text input for "Maximum ftp download session allowed by clients" set to 0. A note below states "0 = Unlimited".
- Settings:** A dropdown menu for "Bind IP" currently showing "0.0.0.0".
- LOG Settings:** Includes an unchecked checkbox for "Delete the user settings and user log files after uninstalling." and a text input for "No of days Client logs should be kept" set to 5.
- Client Grouping:** Radio buttons for "Group Clients by", with "NetBIOS" selected and "DNS Domain" unselected.
- Client Connection Settings:** Includes text inputs for "Increase Thread count" (10) and "Increase Query Interval" (10), both with "(1-100)" ranges. A checkbox for "Restore default values" is unchecked.

Buttons for "Save" and "Cancel" are located at the bottom of the dialog.

## 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 sub module lets you configure web console Timeout, Dashboard, Login Page, SQL Server Connection, SQL Database compression and Password Policy Setting.

Web Console Settings
Help

---

**Web Console Timeout Setting**

Enable Timeout Setting  
Automatically log out the Web Console after  minutes

**Dashboard Setting**

Show Status for Last  days (1 - 365)

**Login Page Setting**

Show Client Setup Link

**Logo Settings**

Logo :   
The logo needs to have the size 300 x 100px, and needs to be in .png or .jpg (RGB Color) format.

**Sql Server Connection Setting**

Microsoft Windows Authentication Mode  
 SQL Server Authentication Mode  
timeout is met

**RMM Settings**

Activate View Only  
 De-Activate View Only  
Screen Quality   
Screen Ratio

**Password Policy Settings**

Password Age :  days (30-180 days)      0 = Password Never Expires  
Password History :  (2-10 Passwords)      0 = No password history is maintained  
Maximum Failed login attempts :  (2-10 times)      0 = Unlimited failed attempts allowed

Note: The above restrictions are not applicable to "Root" login.

**Delete log settings**

Delete Uploaded log files (Forensics\Debug\Screenshots) after  days (1 - 365)

## Web Console Timeout Settings

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

## Dashboard Setting

This setting lets you set number of days for which you wish to View the Status, Statistics and Protection Status Charts in the Dashboard. Enter the preferred number of days.

### Login Page Setting

This setting lets you show or hide the download links shared for eScan Client setup and Agent setup. To show the download links on login page, select the checkboxes of respective links.

### Logo Settings

This setting allows you to add the organization logo in PNG or JPEG format. So the console and reports will have the uploaded logo for customization. To have the default eScan logo, click **Default**. To have customized logo, click **Change**.

### SQL Server Connection settings

This setting lets you select an authentication mode either Microsoft Windows Authentication Mode or 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 ▾ Medium High	80% ▾



- **Screen Ratio** can be set to anywhere from **20%** to **100%**.

Screen Quality	Screen Ratio
Medium ▾	80% ▾
	100%
	90%
	80%
	70%
	60%
	50%
	40%
	30%
	20%

	<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.
--	--

### Password Policy Settings

This setting allows the admin to configure the password settings for other users.

- **Password Age:** Enter the preferred value (between 30-180); this will prompt user to reset the password after specified number of days. Here, 0 indicates that password never expires.
- **Password History:** Enter the preferred value (between 3-10); this maintains the password history for specified count. Here, 0 indicates, no password history is maintained.
- **Maximum Failed login attempts:** Enter the preferred value (between 3-10); this will restrict the user from logging after specified attempts. Here, 0 indicates unlimited login attempts.

To restore the changes made, click **Default**.

	<b>NOTE</b> This setting will not be applicable for the root login
--	--

### Delete log Settings

Enter the number of days in Days field to delete the uploaded log files such as forensic, debug, and screenshot after specified number of days.

After making the necessary changes, click **Save**.

The web console Settings will be updated.

# Update Settings

The Update Settings sub module keeps your virus definitions up-to-date and protects your computer from emerging species of viruses and other malicious programs. This sub module 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.

### 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 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

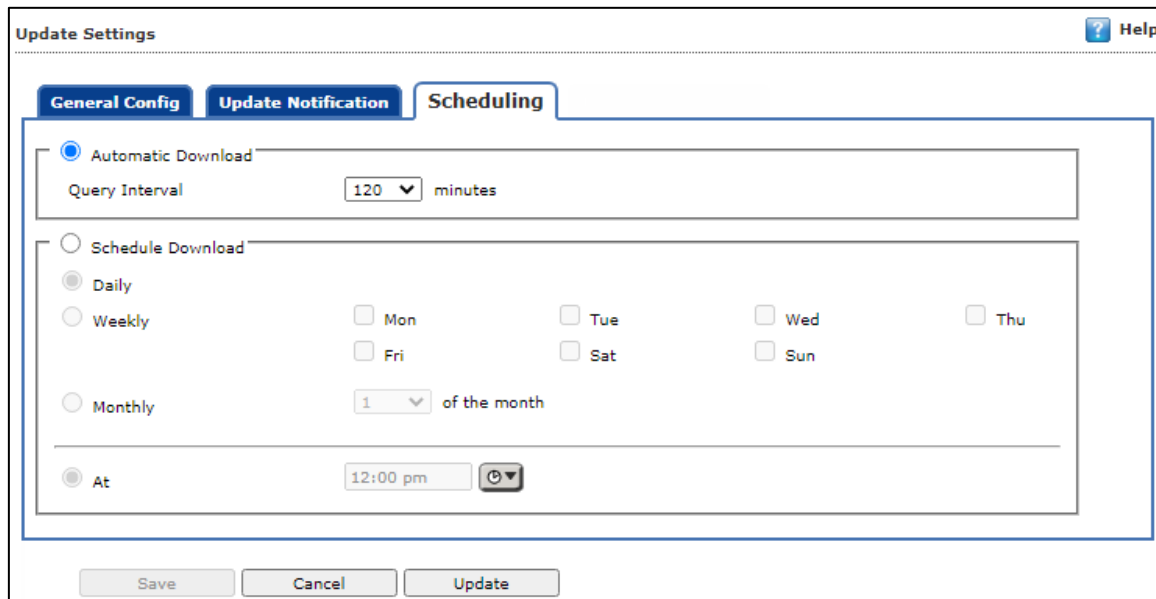
If the SMTP server requires authentication, select this checkbox and enter the login credentials in the **Username** and **Password** fields.

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.



The screenshot shows the 'Update Settings' dialog box with the 'Scheduling' tab selected. The 'Automatic Download' option is chosen. The 'Query Interval' is set to 120 minutes. Under 'Schedule Download', the 'At' option is selected with a time of 12:00 pm. The 'Save', 'Cancel', and 'Update' buttons are visible at the bottom.

### 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.

# Auto-Grouping

The Auto grouping sub module 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 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).

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.

To remove the clients from the excluded list,

1. Select the computer you want to remove.

2. Click **Remove**.  
The client computer will be removed from the list.

### 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.

### 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.

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.

<p><b>NOTE</b></p>	To browse through the list of groups, click <b>Up</b> or <b>Down</b> .
--------------------	--

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**.

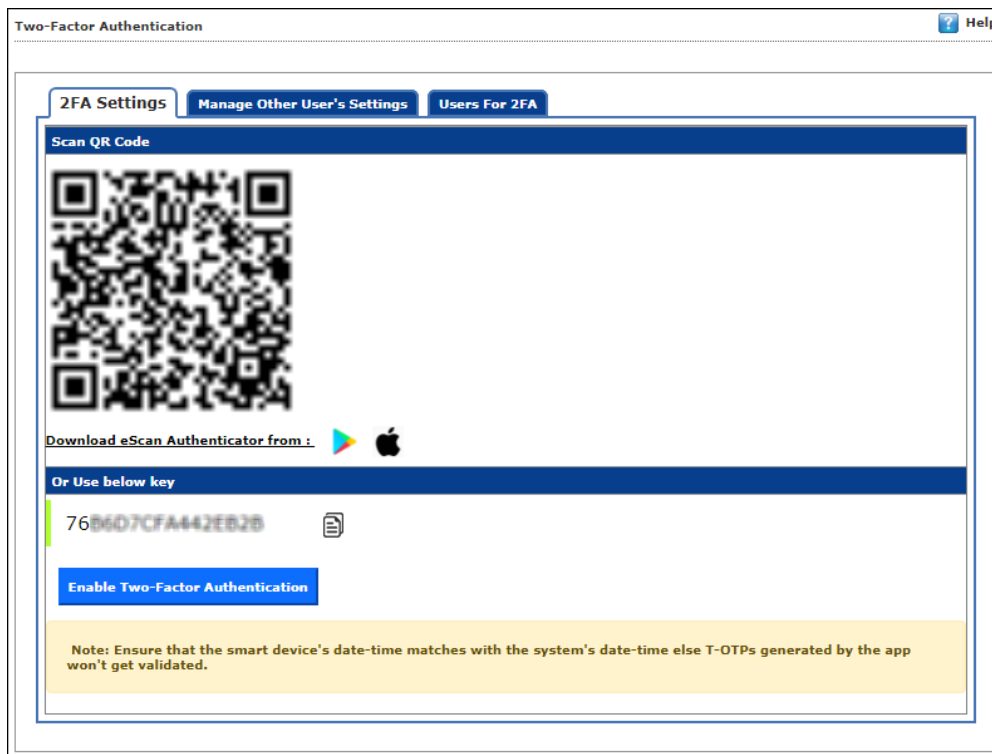
## Two-Factor Authentication (2FA)


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 from [Play Store](#) for Android devices or from [App Store](#) for iOS devices. The Authenticator app needs camera access for scanning a QR code, so ensure you get an appropriate approval to use device camera in your organization. If a COD or BYOD policy restricts you from using device camera in your organization, enter the **Account Key** in the Authenticator app.



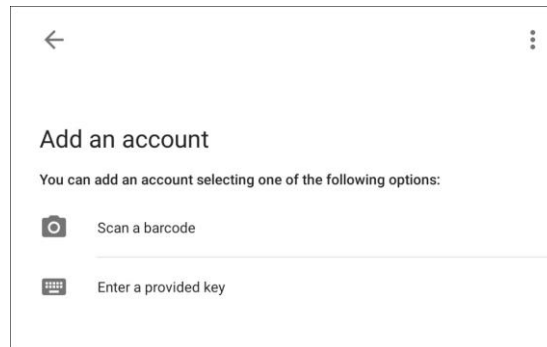
 <b>NOTE</b>	Ensure that the smart device's date and time matches with the system's date and time, else T-OTPs generated by app won't get validated.
--	---

 <b>IMPORTANT</b>	We recommend that you save/store the <b>Account Key</b> in offline storage or a paperback copy, in case you lose the account access.
---	--

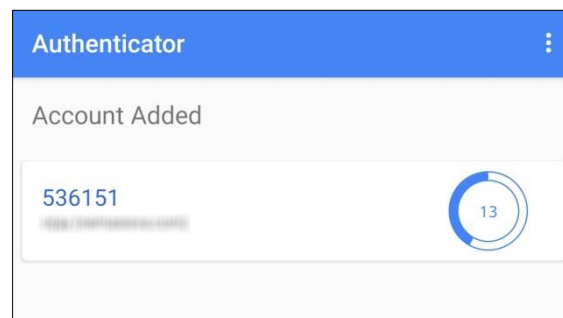
## Enabling 2FA login

To enable 2FA login,

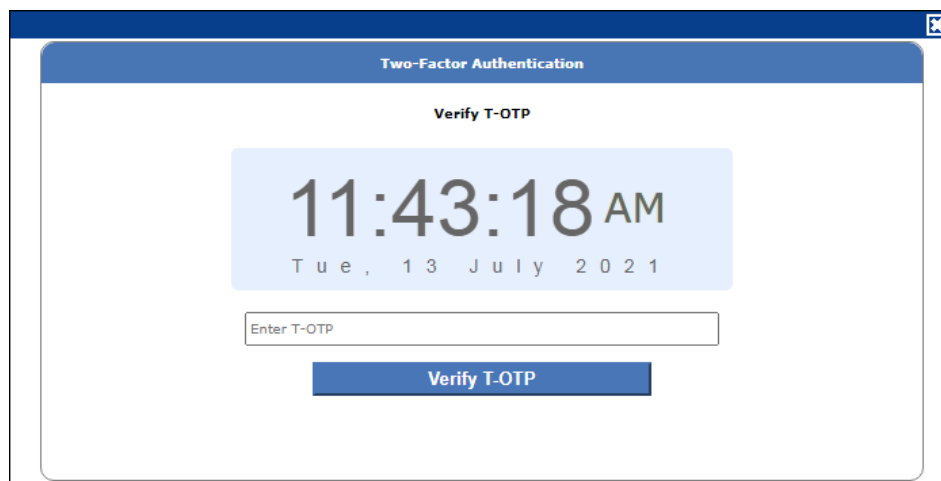
1. Go to **Settings > Two-Factor Authentication**.
2. Open the Authenticator app.  
After basic configuration following screen appears on smart device.



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.





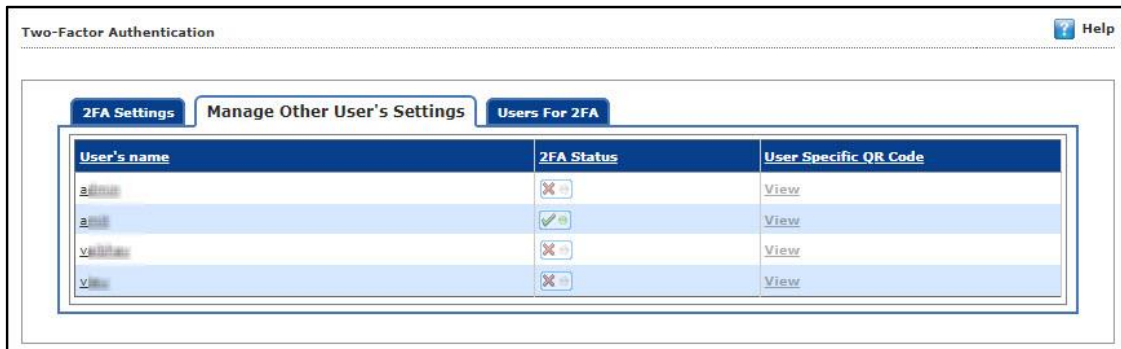
5. Enter the TOTP displayed on smart device and then click **Verify TOTP**.  
The 2FA login feature gets enabled.
6. To apply the login feature for specific users, click **Manage Other User Settings** tab. The tab displays list of added users and whether 2FA status is enabled or disabled.



- 2FA Disabled



- 2FA Enabled



7. To enable 2FA login for an added user, click the button to check icon.  
The 2FA login for added users gets enabled. After enabling the 2FA login for users, whenever they log in to eScan web console Verify TOTP window appears.
8. To view the QR Code of specific user, click **View** option in the User Specified QR Code column.

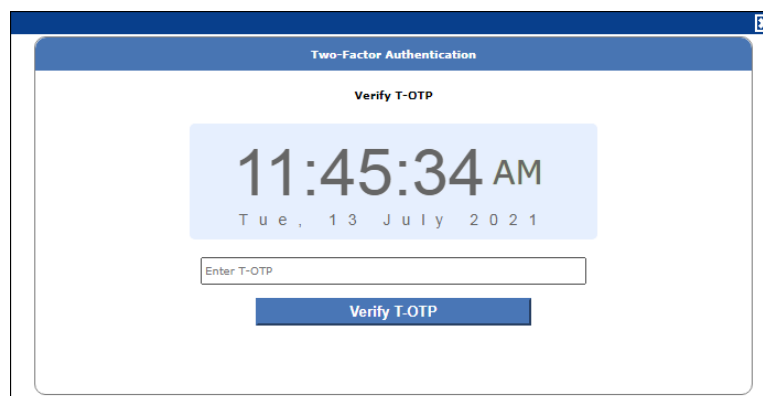
## Disabling 2FA login

To disable 2FA login,

1. Go to **Settings > Two Factor Authentication**.
2. Click **Disable Two-Factor Authentication**.



Verify TOTP window appears.



3. Enter the **TOTP** and then click **Verify TOTP**.

The 2FA feature gets disabled.



After disabling the 2FA feature and enabling it again, the 2FA login status will be reinstated for added users.

## Users For 2FA

This tab helps to add the users and apply 2FA to the endpoints via policy template. The users can be added directly or from Active directory.



## Adding the User

To add users for the same, follow the below steps:

1. Go to **Settings > Two-Factor Authentication > Users For 2FA**.
2. Click **Add User**.

Add User window appears.

**Add User**

Username

Description

3. Enter the **Username** and **Description**.
4. Click **OK**.

The user will be added for 2FA.

## Adding User from Active Directory

To add users from Active Directory, follow the below steps:

1. Go to **Settings > Two-Factor Authentication > Users For 2FA**.
2. Click **Add from Active Directory**.

Add Active Directory Users window appears.

**Add Active Directory Users** Help

> Add Active Directory Users

**Search Criteria**

User's name\*:   
For Example: user or user\*

Domain\*:

AD IP Address\*:

AD Admin User name\*:   
For Active Directory account: domain\username

AD Admin Password\*:

Use SSL Auth.:

AdsPort\*:

**Search Results**

Users

Selected Users

(\*) Mandatory Fields

3. Enter the required information.
4. Click **Ok**.  
The Active Directory Users will be added.

## Importing Users

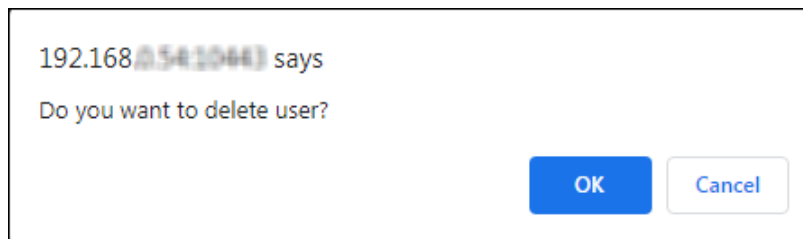
To import the users, follow the below steps:

1. Go to **Settings > Two-Factor Authentication > Users For 2FA**.
2. Click **Import Users**.  
Import Users window appears.

## Deleting Users

To delete the users, follow the below steps:

1. Go to **Settings > Two-Factor Authentication > Users For 2FA**.
2. Click **Delete**.  
The Confirmation prompt appears.



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

# Administration

The Administration module lets you create User Accounts and allocate them Admin rights for using eScan Management Console. In a large organization, installing eScan client on all computers may consume lot of time and efforts. With this option, you can allocate rights to the other employees and allow them to install eScan Client, implement Policies and Tasks.

The Administration module consists following sub modules:

- User Accounts
- User Roles
- Export & Import
- Customize Setup
- Audit Trail

## User Accounts

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

User's name	Full Name	Domain	Role	Session Log	Status
dlp	DLP		DLP	View	✓
root	Administrator account created during installation		Administrator	View	✓

## Create New Account

To create a User Account,

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

**Create User**

User Accounts > Create User

**Account Type and Information**

User's name\*:

Full Name\*:

Password\*:

Confirm Password\*:

Email Address\*:

For Example: user@yourcompany.com

**Account Role**

Role\*:



Save Cancel (\*) Mandatory Fields

2. From **Account Role** field, click drop-down and assign the role to the account.
3. After filling all the details, click **Save**.  
The user will be added to the User Accounts list.

## Adding a User from Active Directory

To create a User from Active Directory,

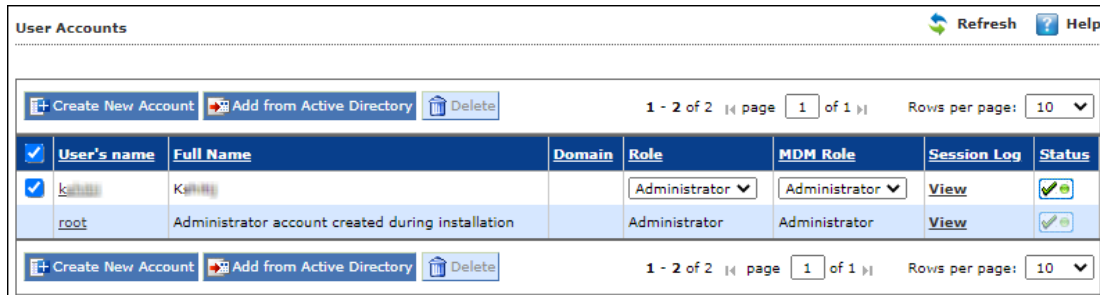
1. In the User Accounts screen, click **Add from Active Directory**.  
Add Active Directory Users form appears.

2. After filling **Search Criteria** section details, click **Search**.
3. A list of users will be displayed in the **Users** section.
4. Select a user and then click  button to add the user to **Selected Users** section.
5. Vice versa the added user can be moved from **Selected Users to Users** by clicking .
6. Click **Save**.  
The user will be added to the User Accounts list.

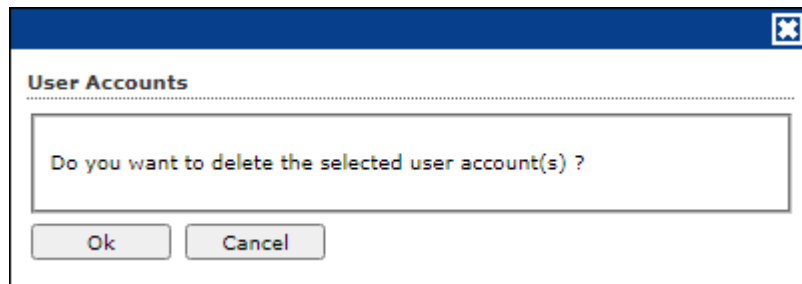
# Delete a User Account

To delete a user account,

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



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

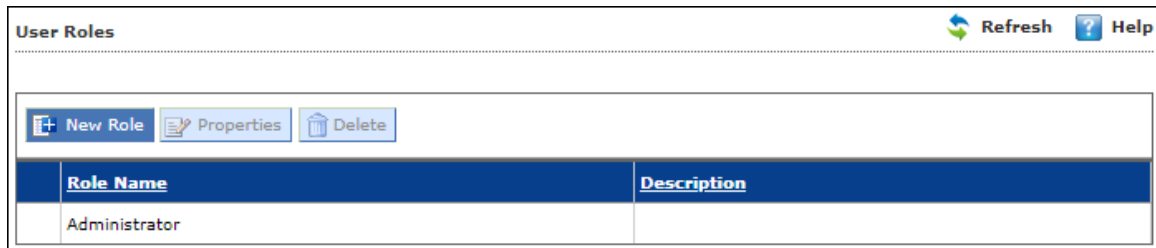


3. Click **OK**.  
The User Account will be deleted.



# User Roles

The User Roles sub module lets you create a role and assign it to the User Accounts with variable permissions and rights as defined in the role being assigned to them. It can be an Administrator role with set of permissions and rights Group Admin Role or a Read only Role.

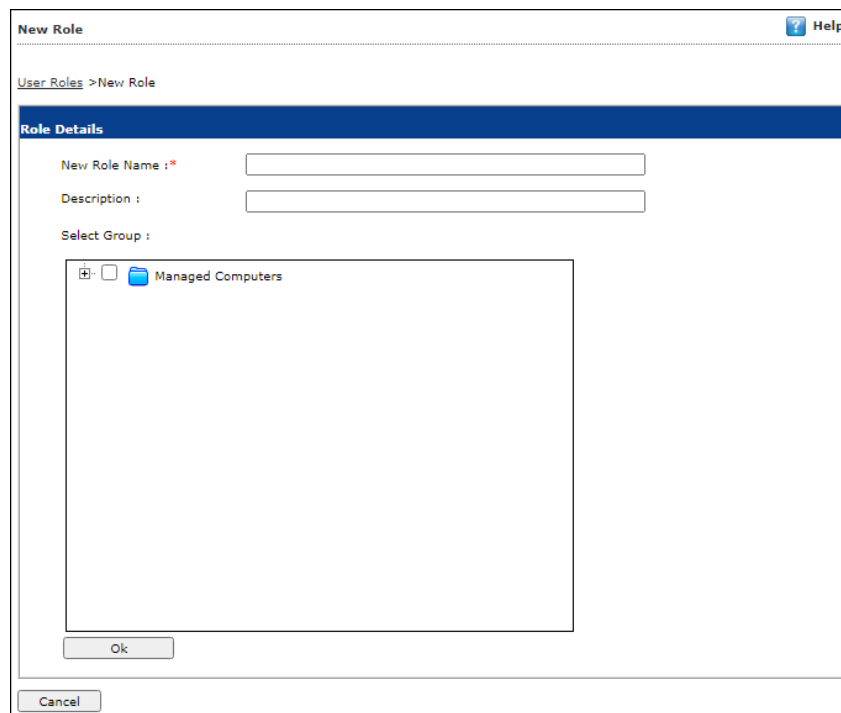


You can re-define the Properties of the created role for configuring access to various section of eScan Management Console and the networked Computers. It also lets you delete any existing role after the task is completed by them. It allows the administrator to give permission to sub administrators to access defined modules of eScan and perform installation/uninstallation of eScan Client on network computers or define policies and tasks for the computers allocated to them.

## New Role

To add a user role,

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



2. Enter name and description for the role.
3. Click **Managed Computers** and select the specific group to assign the role.  
The added role will be able to manage and monitor only the selected group's activities.

- Click **OK**.  
Permissions section appears displaying Main Tree Menu and Client Tree Menu tabs. The Main Tree Menu consists of Navigation Panel Access permissions while the Client Tree Menu consists of selected groups on which permissions the user is allowed to take further.

Menu	View	Configure
DashBoard	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Managed Computers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unmanaged Computers	<input type="checkbox"/>	<input type="checkbox"/>
Network Computers	<input type="checkbox"/>	<input type="checkbox"/>
IP Range	<input type="checkbox"/>	<input type="checkbox"/>
Active Directory	<input type="checkbox"/>	<input type="checkbox"/>
Report Templates	<input type="checkbox"/>	<input type="checkbox"/>
Report Scheduler	<input type="checkbox"/>	<input type="checkbox"/>
Events & Computers	<input type="checkbox"/>	<input type="checkbox"/>
System Action List	<input type="checkbox"/>	<input type="checkbox"/>
Tasks For Specific Computers	<input type="checkbox"/>	<input type="checkbox"/>
Asset Management	<input type="checkbox"/>	<input type="checkbox"/>
User Activity	<input type="checkbox"/>	<input type="checkbox"/>
Print Activity	<input type="checkbox"/>	<input type="checkbox"/>
Session Activity Report	<input type="checkbox"/>	<input type="checkbox"/>
File Activity Report	<input type="checkbox"/>	<input type="checkbox"/>
Application Access Report	<input type="checkbox"/>	<input type="checkbox"/>
Patch Report	<input type="checkbox"/>	<input type="checkbox"/>
Notifications	<input type="checkbox"/>	<input type="checkbox"/>
Outbreak Alert	<input type="checkbox"/>	<input type="checkbox"/>
Event Alert	<input type="checkbox"/>	<input type="checkbox"/>

- Select the checkboxes that will allow the role to view/configure the module.
- After selecting the necessary checkboxes, click **Save**.  
The role will be added to the User Roles list.

## View Role Properties

To view the properties of a role,

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

Role Name	Description
Administrator	
<input checked="" type="checkbox"/> Kali	

- Click **Properties**.  
Properties screen appears. It lets you modify role description, permissions for accessing and configuring modules and assign the role to other groups by clicking **Select Group Tree**.

Permissions		
Main Tree Menu		Client Tree Menu
Menu	View	Configure
Dashboard	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Managed Computers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unmanaged Computers	<input type="checkbox"/>	<input type="checkbox"/>
Network Computers	<input type="checkbox"/>	<input type="checkbox"/>
IP Range	<input type="checkbox"/>	<input type="checkbox"/>
Active Directory	<input type="checkbox"/>	<input type="checkbox"/>
Report Templates	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Report Scheduler	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Events & Computers	<input type="checkbox"/>	<input type="checkbox"/>
System Action List	<input type="checkbox"/>	<input type="checkbox"/>
Tasks For Specific Computers	<input type="checkbox"/>	<input type="checkbox"/>
Asset Management	<input type="checkbox"/>	<input type="checkbox"/>
User Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Print Activity	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Session Activity Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>
File Activity Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Application Access Report	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Patch Report	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Notifications	<input type="checkbox"/>	<input type="checkbox"/>

- 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.

Permissions																																																																				
Main Tree Menu		Client Tree Menu																																																																		
<ul style="list-style-type: none"> <li>Managed Computers</li> <li>Roaming Users</li> <li>Linux / Mac</li> <li>Managed Team</li> </ul>		<table border="1"> <thead> <tr> <th colspan="2">[ Managed Computers/Samples_Team ]</th> <th>Configure</th> </tr> <tr> <th>Menu</th> <th></th> <th><input type="checkbox"/></th> </tr> </thead> <tbody> <tr><td colspan="3">Action List</td></tr> <tr><td>  New Sub Group</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Set Group Configuration</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Deploy / Upgrade Client</td><td></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>  Uninstall eScan Client</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Remove Group</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Synchronize with Active Directory</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Outbreak Prevention</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Create Client Setup</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Properties</td><td></td><td><input checked="" type="checkbox"/></td></tr> <tr><td colspan="3">Client Action List</td></tr> <tr><td>  Set Host Configuration</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Deploy / Upgrade Client</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Uninstall eScan Client</td><td></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>  Move to Group</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Remove from Group</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Refresh Client</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Show Critical Events</td><td></td><td><input type="checkbox"/></td></tr> <tr><td>  Export</td><td></td><td><input checked="" type="checkbox"/></td></tr> <tr><td>  Show Installed Softwares</td><td></td><td><input type="checkbox"/></td></tr> </tbody> </table>	[ Managed Computers/Samples_Team ]		Configure	Menu		<input type="checkbox"/>	Action List			New Sub Group		<input type="checkbox"/>	Set Group Configuration		<input type="checkbox"/>	Deploy / Upgrade Client		<input checked="" type="checkbox"/>	Uninstall eScan Client		<input type="checkbox"/>	Remove Group		<input type="checkbox"/>	Synchronize with Active Directory		<input type="checkbox"/>	Outbreak Prevention		<input type="checkbox"/>	Create Client Setup		<input type="checkbox"/>	Properties		<input checked="" type="checkbox"/>	Client Action List			Set Host Configuration		<input type="checkbox"/>	Deploy / Upgrade Client		<input type="checkbox"/>	Uninstall eScan Client		<input checked="" type="checkbox"/>	Move to Group		<input type="checkbox"/>	Remove from Group		<input type="checkbox"/>	Refresh Client		<input type="checkbox"/>	Show Critical Events		<input type="checkbox"/>	Export		<input checked="" type="checkbox"/>	Show Installed Softwares		<input type="checkbox"/>
[ Managed Computers/Samples_Team ]		Configure																																																																		
Menu		<input type="checkbox"/>																																																																		
Action List																																																																				
New Sub Group		<input type="checkbox"/>																																																																		
Set Group Configuration		<input type="checkbox"/>																																																																		
Deploy / Upgrade Client		<input checked="" type="checkbox"/>																																																																		
Uninstall eScan Client		<input type="checkbox"/>																																																																		
Remove Group		<input type="checkbox"/>																																																																		
Synchronize with Active Directory		<input type="checkbox"/>																																																																		
Outbreak Prevention		<input type="checkbox"/>																																																																		
Create Client Setup		<input type="checkbox"/>																																																																		
Properties		<input checked="" type="checkbox"/>																																																																		
Client Action List																																																																				
Set Host Configuration		<input type="checkbox"/>																																																																		
Deploy / Upgrade Client		<input type="checkbox"/>																																																																		
Uninstall eScan Client		<input checked="" type="checkbox"/>																																																																		
Move to Group		<input type="checkbox"/>																																																																		
Remove from Group		<input type="checkbox"/>																																																																		
Refresh Client		<input type="checkbox"/>																																																																		
Show Critical Events		<input type="checkbox"/>																																																																		
Export		<input checked="" type="checkbox"/>																																																																		
Show Installed Softwares		<input type="checkbox"/>																																																																		

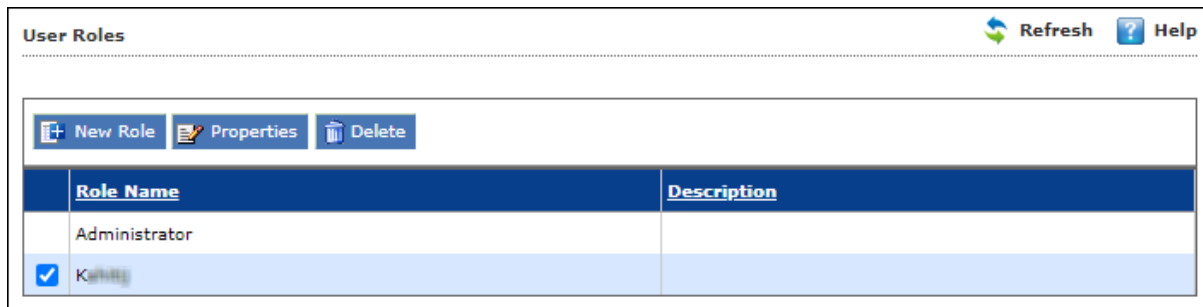
- To let the role configure these actions, under the Configure column select the checkboxes of corresponding actions.

6. Click **Save**.  
The Role Properties will be updated accordingly.

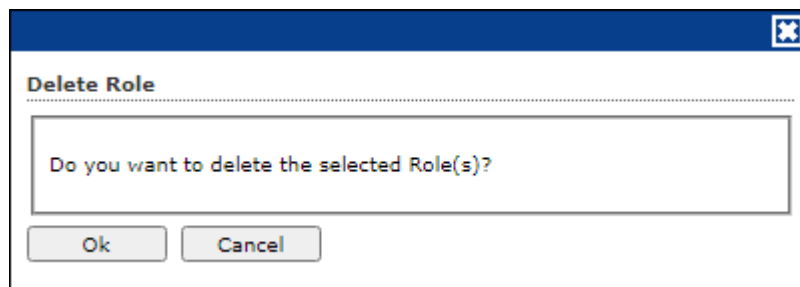
## Delete a User Role

To delete a user role,

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



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



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

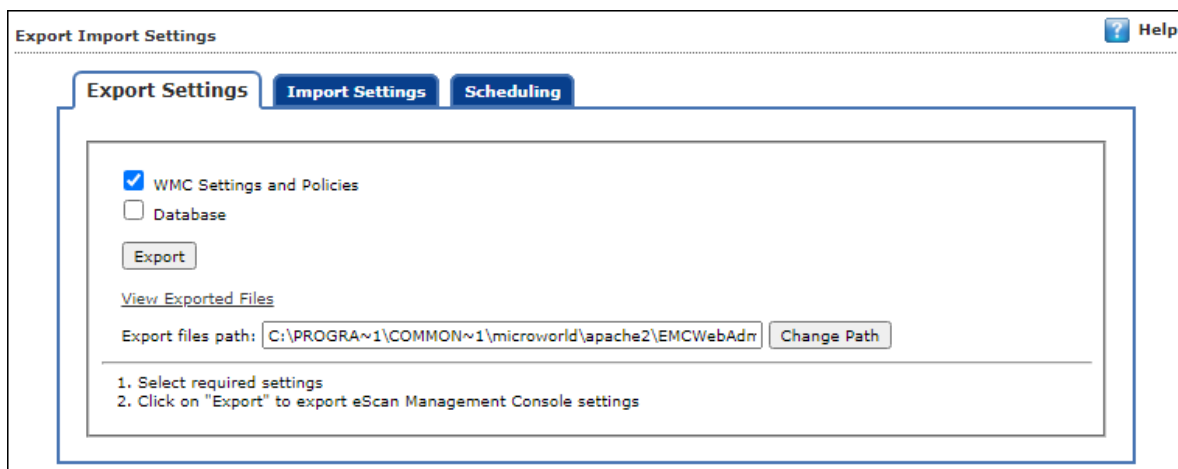
## Export & Import

The Export & Import sub module 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

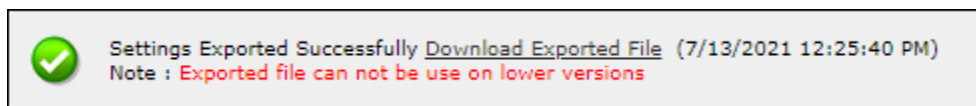
This tab lets you export the eScan Server Settings, Policies, and Database. To export the eScan Server settings, follow the steps given below:

1. In the Export Import Settings screen, click **Export Settings** tab.



The screenshot shows the 'Export Import Settings' window with three tabs: 'Export Settings', 'Import Settings', and 'Scheduling'. The 'Export Settings' tab is active. It contains two checkboxes: 'WMC Settings and Policies' (checked) and 'Database' (unchecked). Below the checkboxes is an 'Export' button. Underneath is a link 'View Exported Files'. The 'Export files path' is set to 'C:\PROGRA~1\COMMON~1\microworld\apache2\EMCWebAdn' with a 'Change Path' button. At the bottom, there are two numbered instructions: '1. Select required settings' and '2. Click on "Export" to export eScan Management Console settings'.

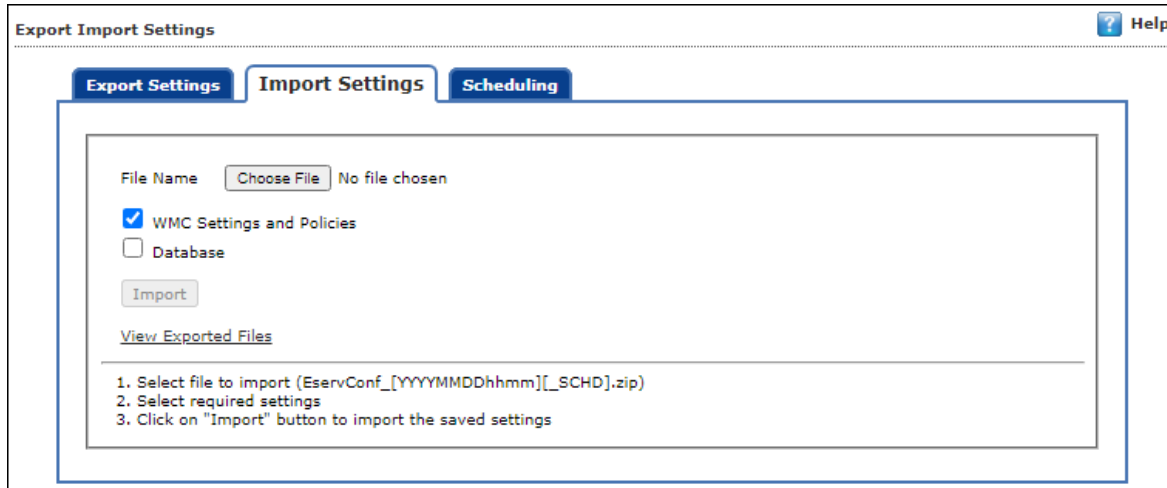
2. To backup **WMC Settings and Policies** and **Database**, select both the checkboxes. The backup file will be exported to the path shown in **Export files path** field. To change the file path, click **Change Path**. Enter the file path and click **Add**.
3. To view the exported files, click **View Exported Files**.
4. 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.



The screenshot shows the 'Export Import Settings' window with three tabs: 'Export Settings', 'Import Settings', and 'Scheduling'. The 'Import Settings' tab is active. It contains a 'File Name' field with a 'Choose File' button and the text 'No file chosen'. Below this are two checkboxes: 'WMC Settings and Policies' (checked) and 'Database' (unchecked). An 'Import' button is located below the checkboxes. A link 'View Exported Files' is also present. At the bottom, there are three numbered instructions: 1. Select file to import (EservConf\_[YYYYMMDDhhmm]\_[\_SCHD].zip), 2. Select required settings, and 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 **WMC Settings and Policies** and **Database**, select both the checkboxes.
4. To view the exported files, click **View Exported Files**.
5. Click **Import**.  
The backup file will be imported.  
A success message is displayed after complete import.



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.

To create a Schedule for export, follow the steps given below:

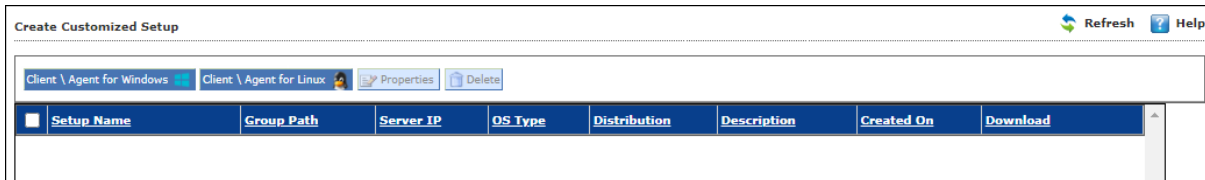
1. Select **Enable Export Scheduler** checkbox.
2. Select the checkboxes whether to back up both **WMC Settings and Policies** and **Database**.
3. Schedule the backup for a **Daily**, **Weekly** (Select a day) or **Monthly** (Select a date) basis.
4. For the **At** field, click the drop-down and select 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.
5. If the SMTP server requires authentication, select the **Use SMTP Authentication** checkbox and enter the credentials.
6. To check if the SMTP settings are correct, click **Test**.  
A test email will be sent to recipient email ID.

7. To configure additional settings for backup file, select the **Enable Optional Settings**, and make the necessary changes.
8. To restore the changes made, click **Default**.
9. To view the exported files, click **View Exported Files**.
10. After performing all the necessary steps, click **Save**.  
The export schedule will be saved.



# Customize Setup

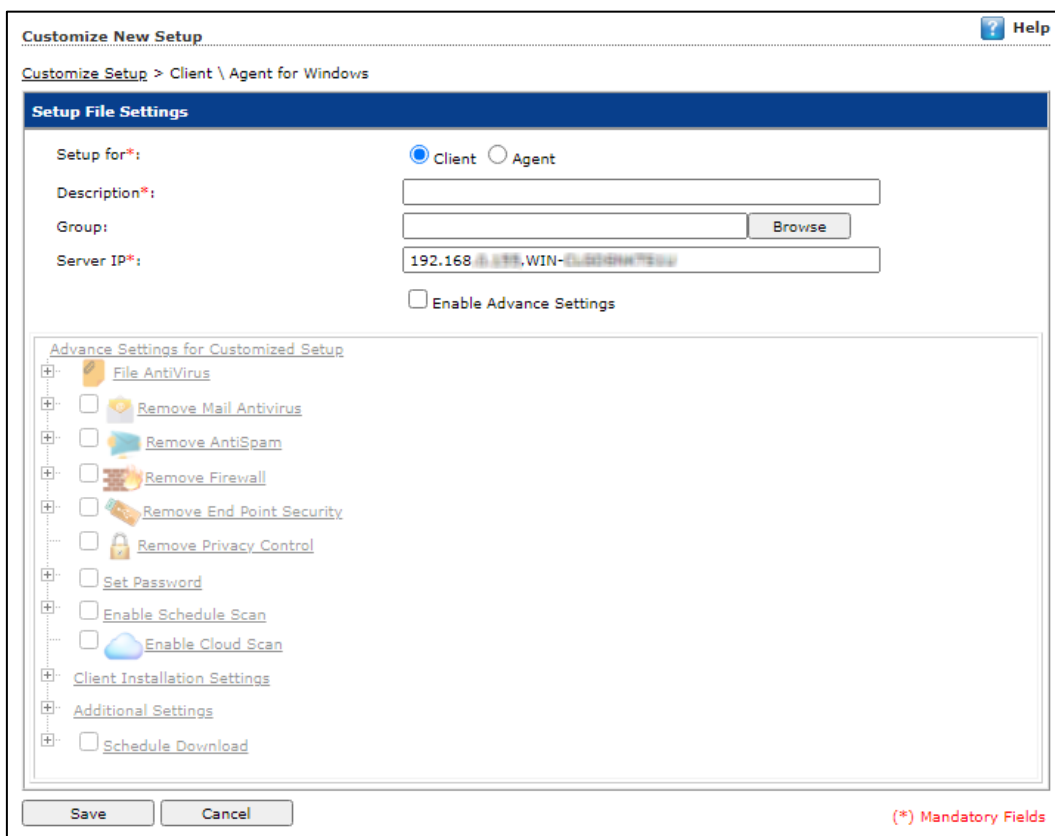
This sub module lets you create a customized setup for a Client or an Agent with fewer modules and deploy it to various locations. This can be very useful, if there are locations to which a server is unable to push the setup or locations that are unable to connect to the server directly. The custom setup 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**.

- 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.
- Click **Save**.  
The customized setup for Windows will be created.

## Editing Setup Properties

The properties can be edited only for customized Windows setup. To edit the customized Windows setup's properties, follow the steps given below:

Client \ Agent for Windows			Client \ Agent for Linux			Properties	Delete
Setup Name	Group Path	Server IP					
Set	Ma	st					

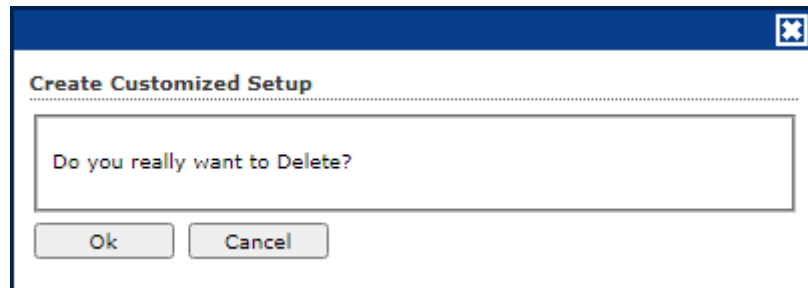
- In the Create Customized Setup screen, select the Windows setup you want to edit.
- Click **Properties**.  
Edit Customized Setup screen appears.

- 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:

1. In the Create Customized Setup screen, select the setup you want to delete.
2. Click **Delete**.

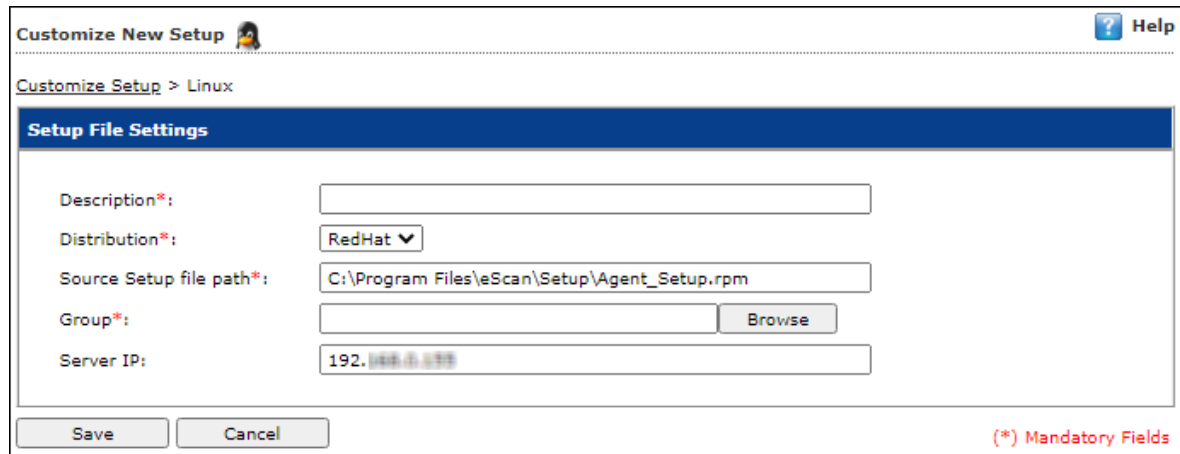


4. Click **Ok**.  
The setup will be deleted.

## 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.



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.

# Audit Trail

The Audit Trail sub module let you record the security relevant data, operation, event, Action, policy updates. Audit logs are used to track the date, time and activity of each user, including the policy/criteria that have been changed. A record of the changes that have been made to a database. You can get audit trail of user activity across all these systems.

User Name	Session Id	IP Address	Client Date	Client Time	Audit Type	Policy/Criteria Name	Module Name	Action	View Action
meat	[E5H0-283A378-088436]	192.168.1.101	09/09/21	12:38:56	Log Off	---	---	Console LogOut	---
meat	[DCMC-287D42C-080338]	192.168.1.101	09/09/21	12:39:53	Login	---	---	Console Login	---
meat	[6CIP-2849F77-0C1035]	192.168.1.101	09/09/21	12:40:26	Login	---	---	Console Login	---
meat	[6CIP-2849F77-0C1035]	192.168.1.101	09/09/21	12:40:47	Log Off	---	---	Console LogOut	---

## Filter all Audit Trail report

To filter the Audit Trail Report as per your requirements, click **Filter Criteria** field. Filter Criteria field expands.

**Filter Criteria** | **Export Options**

Filter Criteria

User Name    \*    Include

Audit Type    \*    Include

Module Name    \*    Include

Date Range

From (MM/DD/YYYY)    09/09/2021

To (MM/DD/YYYY)    09/09/2021

IP Address    \*    Include

Policy/Criteria Name    \*    Include

(\*) View All Items

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

### Include/Exclude

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

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

The Audit Trail Report will be filtered according to your preferences.

## Exporting Audit Trail

To export the Audit Trail Report, click **Export Option**.

Export Option field expands.

**Filter Criteria** | **Export Option**

Export Option

Excel     PDF     HTML

Select the preferred option and then click **Export**.

A success message appears.



# License

The License module lets you manage user licenses. You can add, activate, and view the total number of licenses available for deployment, previously deployed, and licenses remaining with their corresponding values. The module also lets you move the licensed computers to non-licensed computers and vice versa. Here you can also view the number of add-on license along with the name of it. For example, as you can see here there are 15 add-on licenses for eBackup feature. The add-on license is available for RMM, 2FA, and DLP features.

Refresh Help

**License**

**Register Information**

License Key(30 char)	Activation Code(60 char)	Registration Status	Contract Period Ends on	No. of Users	Add On License
ABC-DEF-GHI-JKL-MNO-PQR-STU-VWX-YZ-ABC-DEF-GHI	12345-67890-ABDEF-GHIJK-LMNOP-QRSTU-VWXYZ-12345-67890-ABDEF-GHIJK-LMNOP-QRSTU-VWXYZ	Activated	05-Sep-2021	10	RMM+ DLP+2FA+ Anti-Theft

To Add License [Click Here](#)

**License**

70.0%      30.0%

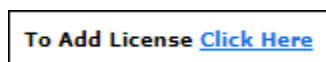
● License In Use - 3    ● Remaining License - 7

[\[Manage License\]](#)

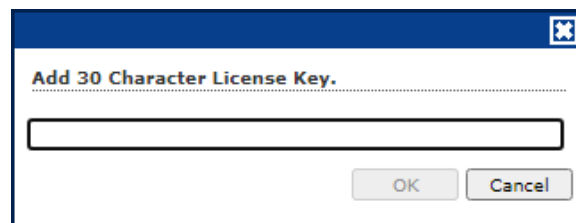
## Adding and Activating a License

To add and activate a license,

1. In the License screen, click on **Click Here** link.



Add License Key dialog box appears.



2. Enter the license key and then click **OK**.  
The license key will be added and displayed in the **Register Information** table.
3. To activate the added license, click **Activate Now**.
4. Click **Activate now** link displayed in Activation Code column to activate the license key on eScan server system.  
Online Registration Information form appears.

Online Registration Information Privacy Policy Refresh Help

License > Online Registration Information

License Key : **8PCK-8PQD-8QAK-8KLD-8QDQ-8ZSB-8VKB-8E**

I have Activation Code  
Enter Activation Code

Activate Now

Personal Information

Name:  Company Name:

Country:  Email Id:

State:  Customer Mobile No. \*:

**Note:** Enter valid email id in order to receive backup copy of your license details.

Email Subscription

Yes  No

Dealer Mobile No.:

(\*)Mandatory Field

5. Select a desired option for activation.
6. Enter details in **Personal Information** section.

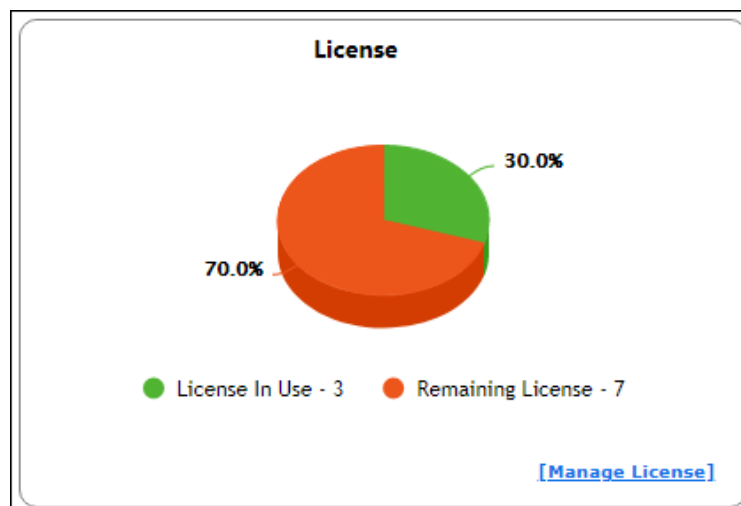
<b>NOTE</b>	Enter valid email id in order to receive backup copy of your license details.
-------------	---

7. Select a desired option for **Email Subscription**.
8. Enter the **Dealer Mobile Number**.
9. Click **Activate**. (Ensure that the Internet connection is Active.)

## Moving Licensed Computers to Non-Licensed Computers

To move licensed computers to non-licensed computers,

1. In the License statistics box, click **Manage License**.



Manage License window appears.

The screenshot shows the 'Manage License' window with the following data:

Licensed Computers / Devices (3)		Filter License	Move to Non-License
Machine Name	Group	All	
<input type="checkbox"/> UBUNTU	Managed Computers\Linux / Mac		
<input type="checkbox"/> QNAP	Managed Computers\QNAP		
<input type="checkbox"/> WIN-CQAC27R047	Managed Computers		

Non-Licensed Computers / Devices (0)		Filter License	Move to License
No Record Found			
No Record Found			

Close

- Under the **Licensed Computers** section, select the computer(s) that you want to move to Non-Licensed Computers section.
- Click **Move to Non-License**.  
The selected computer(s) will be moved to Non-Licensed computers section.

The screenshot shows the 'Manage License' window after one computer has been moved. The data is as follows:

Licensed Computers / Devices (2)		Filter License	Move to Non-License
Machine Name	Group	All	
<input type="checkbox"/> UBUNTU	Managed Computers\Linux / Mac		
<input type="checkbox"/> WIN-CQAC27R047	Managed Computers		

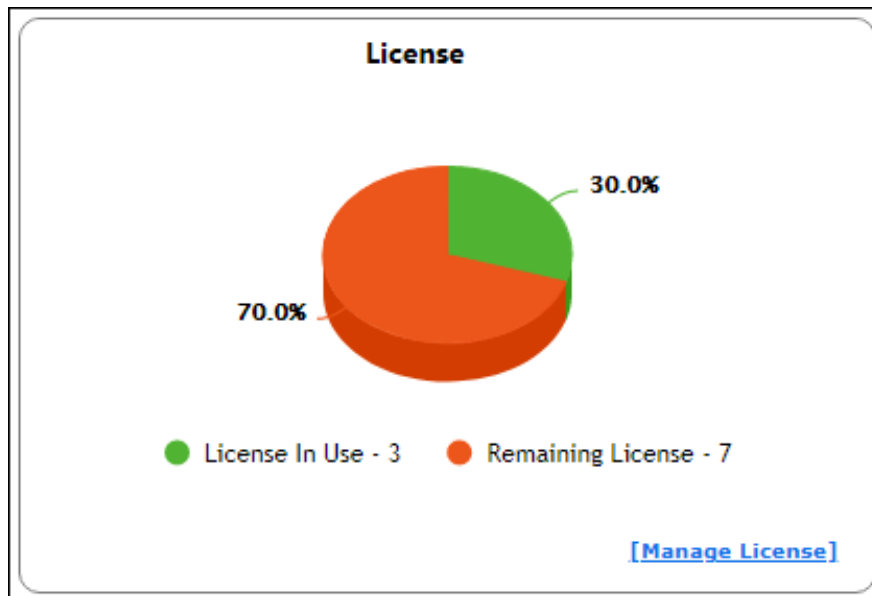
Non-Licensed Computers / Devices (1)				Filter License	Move to License
Machine Name	Group	Unlicense Date Time	Description	All	
<input type="checkbox"/> QNAP	Managed Computers\QNAP	05/08/2021 16:43:00			

Close

# Moving Non-Licensed Computers to Licensed Computers

To move licensed computers to non-licensed computers, follow the steps given below:

1. In the License statistics box, click **Manage License**.



Manage License window appears.

Manage License ? Help

---

Licensed Computers / Devices (2) Filter License: All

<input type="checkbox"/>	Machine Name	Group
<input type="checkbox"/>	UBUNTU	Managed Computers\Ubuntu / Mac
<input type="checkbox"/>	WIN-0268222007	Managed Computers

---

Non-Licensed Computers / Devices (1) Filter License: All

<input type="checkbox"/>	Machine Name	Group	Unlicense Date Time	Description
<input type="checkbox"/>	Q6-638	Managed Computers\Q638	05/08/2021 16:43:00	

2. Under the **Non-Licensed Computers** section, select the computer(s) that you want to move to Licensed Computers section.



3. Click **Move to License**.  
The selected computer(s) will be moved to Licensed Computers section.

The screenshot shows the 'Manage License' window with a 'Help' icon in the top right. It is divided into two main sections:

- Licensed Computers / Devices (3)**: This section has a 'Filter License' dropdown set to 'All' and a 'Move to Non-License' button. It contains a table with the following data:

<input type="checkbox"/>	Machine Name	Group
<input type="checkbox"/>	UBUNTU	Managed Computers\linux / Mac
<input type="checkbox"/>	QAKESK	Managed Computers\QAKESK
<input type="checkbox"/>	WIN-CGAC2TMAU7	Managed Computers
- Non-Licensed Computers / Devices (0)**: This section has a 'Filter License' dropdown set to 'All' and a 'Move to License' button. It displays 'No Record Found'.

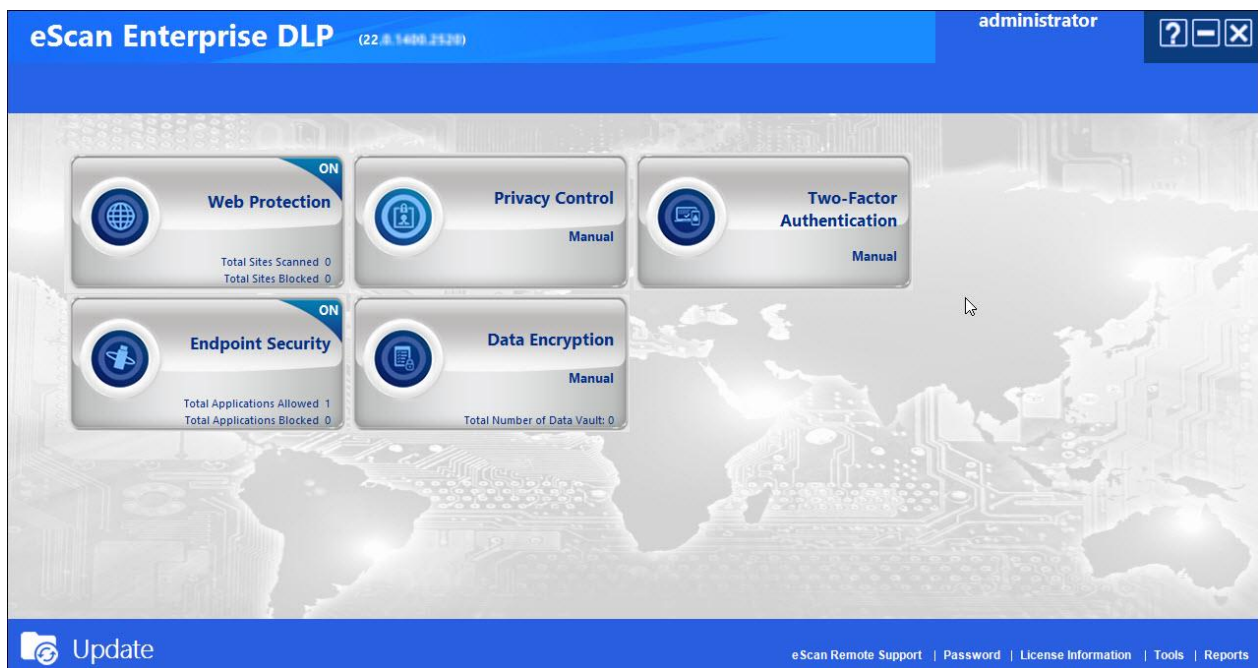
A 'Close' button is located at the bottom left of the window.

# Getting Started

The following sections will be give you the detailed description and configuration procedure of all the eScan GUI and Modules presents in the eScan Enterprise DLP:

## Graphical User Interface (GUI)

eScan V22 is not only equipped with the latest innovative technology but also has very simple yet trendy GUI. eScan displays additional options buttons and quick access links.



## Data Encryption

The Data Encryption module allows you to protect confidential data from unauthorized access and data leak. With this module, user can create a Vault that stores data in an 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.

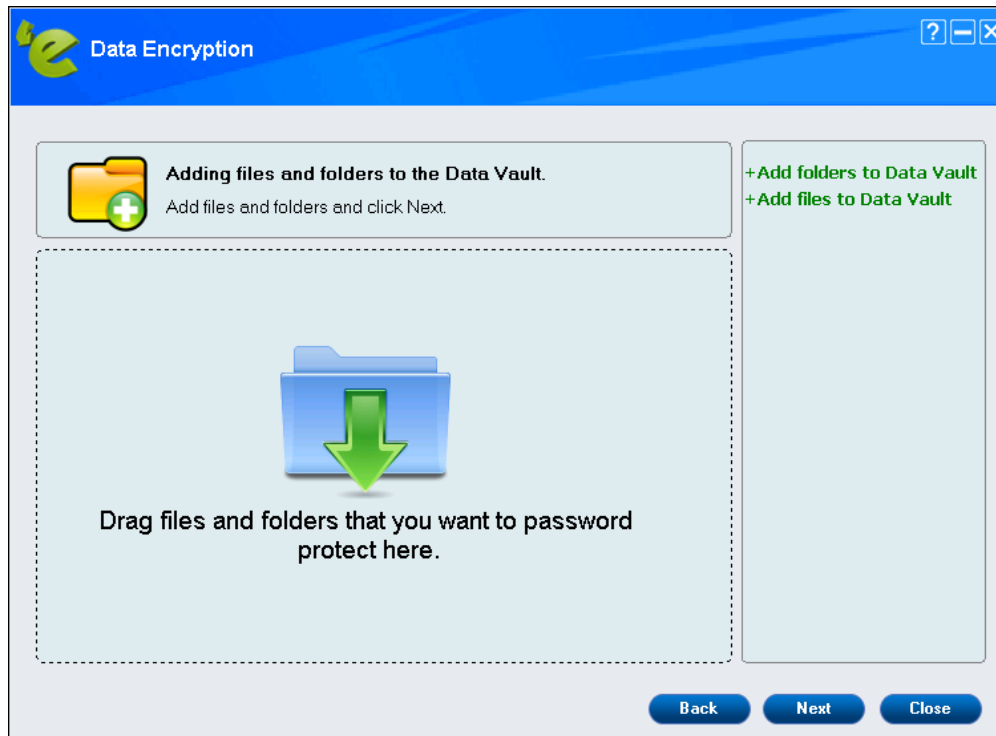
## How to Create a Vault?

To create a vault, follow the steps given below:

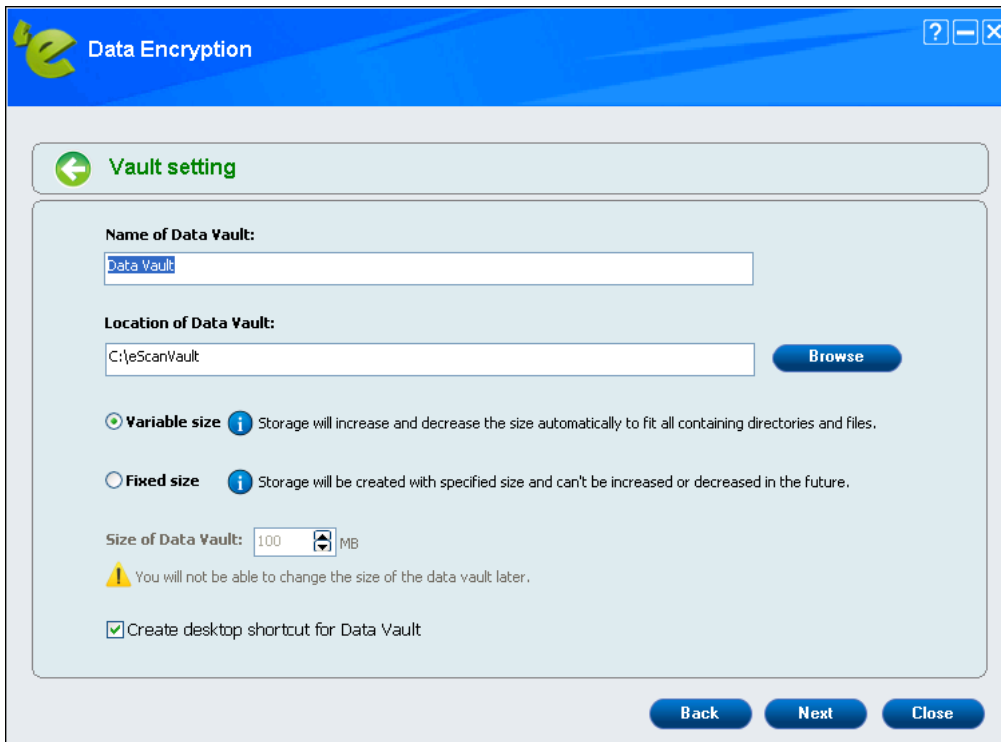
1. Launch eScan.
2. Click **data encryption**.  
Data Vault window appears.
3. Click **Create new Data Vault**.



- To add files or folders in Data Vault, click **Add folders to Data Vault** or **Add files to Data Vault**. You can add files and folders by drag files and folders to vault.



- After adding required files and folder, click **Next**.
- 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**.



7. After filling all the details, click **Next**.
8. Read the **Password Hint** and then enter the password.

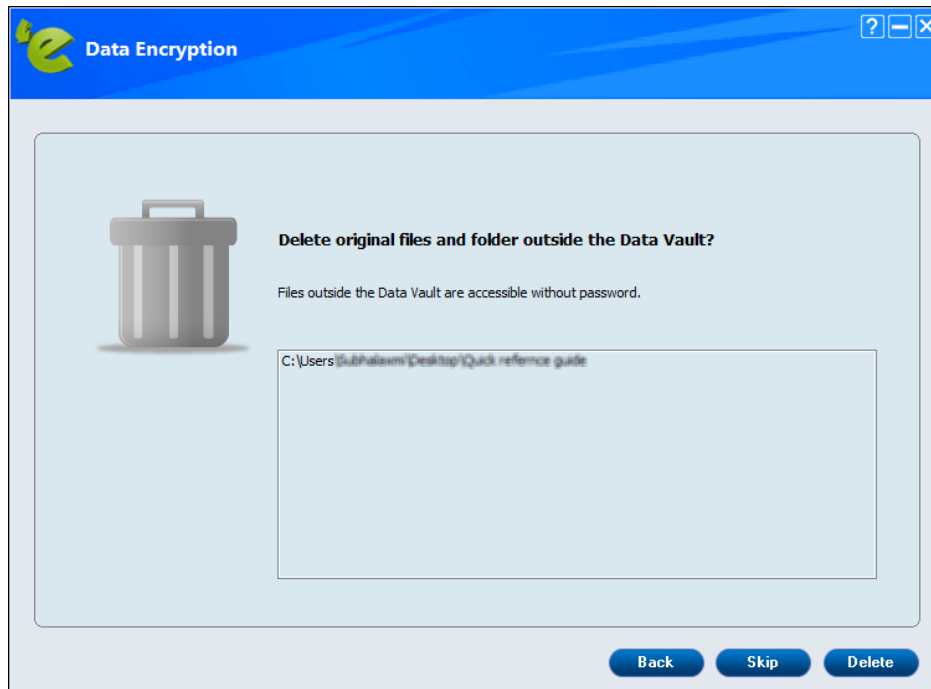
**NOTE**

In case, if you forget your password, it can be recovered with the help of eScan Team.

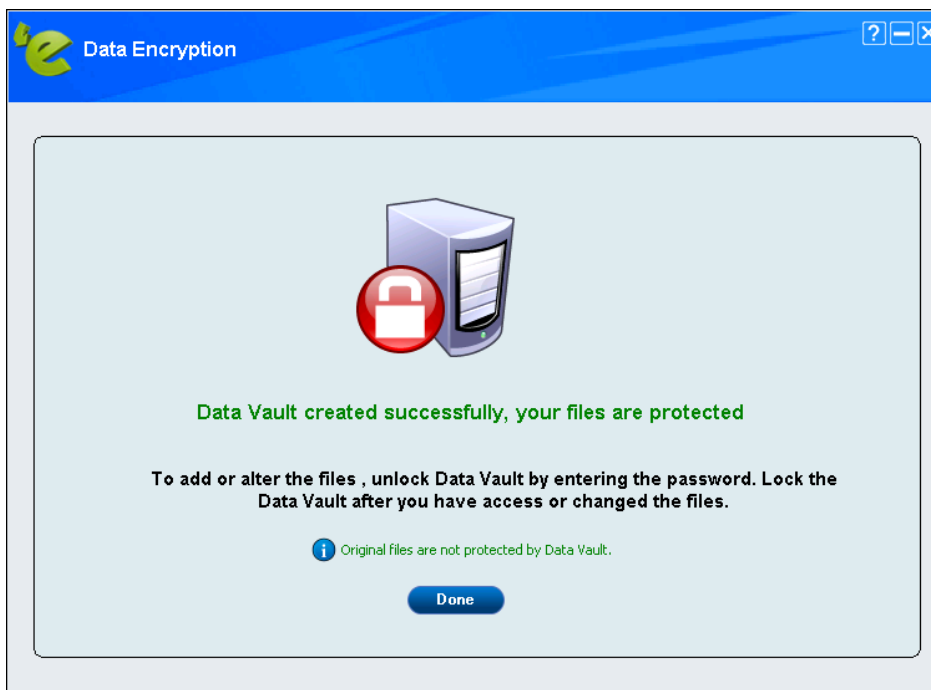


9. Click **Next**.

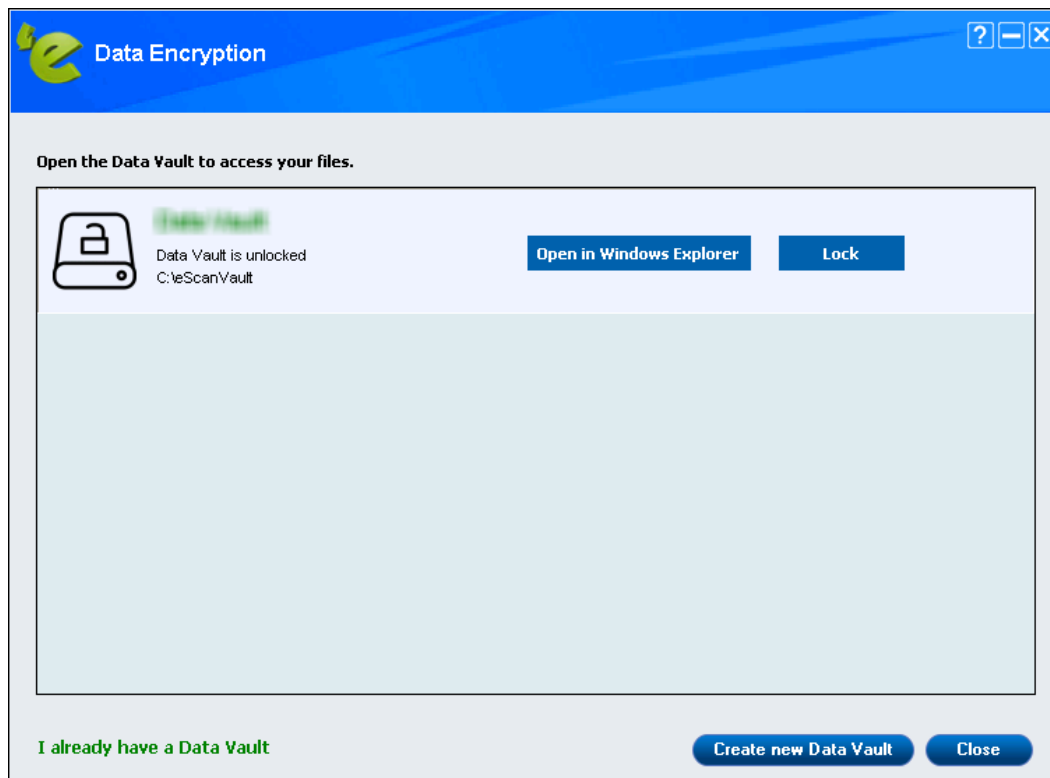
10. Data will be copied to the Data Vault. If you wish to delete the original files and folders outside the data vault by clicking **Delete** or else click **Skip**.



11. Click **Finish**.
12. Data Encryption window appears, click **Done**.

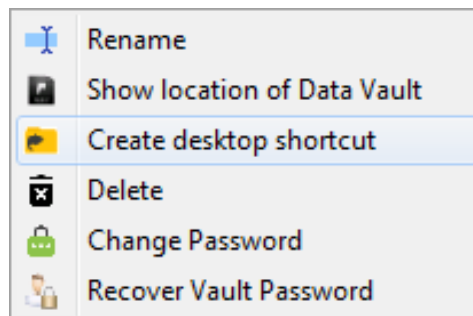


13. The Data Vault will be created and get displayed on the data encryption list. To encrypt your data, click **Lock**.



14. 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, Rename window appears, change the name and click **Save**.

### **Show location of Data Vault**

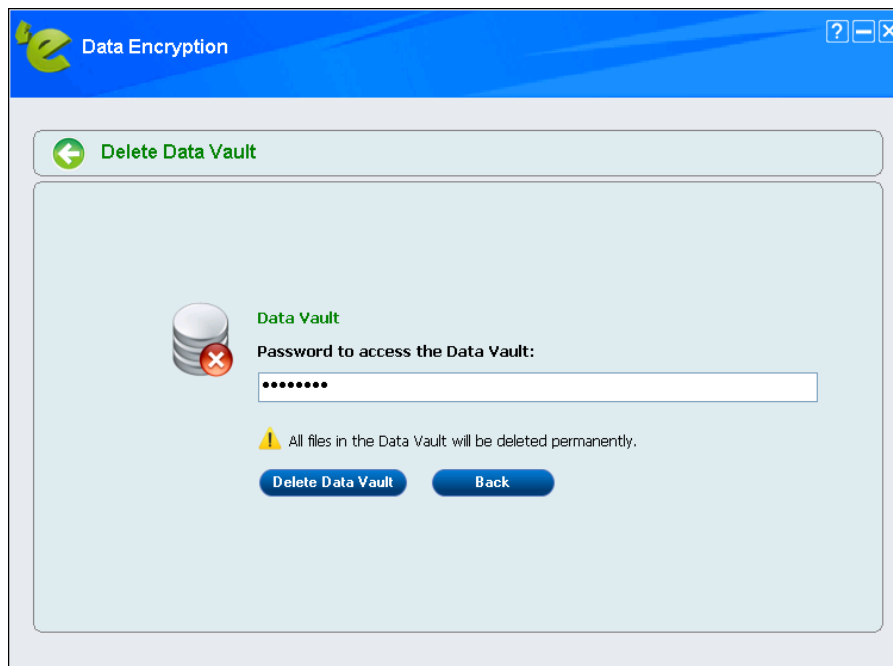
This option will open the location where data vault is created.

### **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, the screen will 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 be forwarded to the Data Encryption window.



Enter the **Old Password**, **New Password**, and **Confirm New Password**.  
Click **Save**.  
This will change the password of the data vault.




### Recover Password

This option is used to recover password, this will generate the password in an encrypted format.



  
**NOTE**

If you selected **Create desktop shortcut for Data Vault** checkbox, it will create a shortcut  of data vault to the Desktop.

## Two-Factor Authentication

The system login password is Single-Factor Authentication which is considered unsecure as it may put your system'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 computer.

The 2FA feature mandates you to enter a Time-based One-Time Password (TOTP) after entering Windows login credentials. So, even if somebody knows your login credentials, the 2FA feature secures data against unauthorized logins.

You can use various options to set password for the 2FA. You can set password or you can use the eScan administrator password in case the system is offline (without internet access). To use 2FA online authentication, 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 in the Authenticator app.



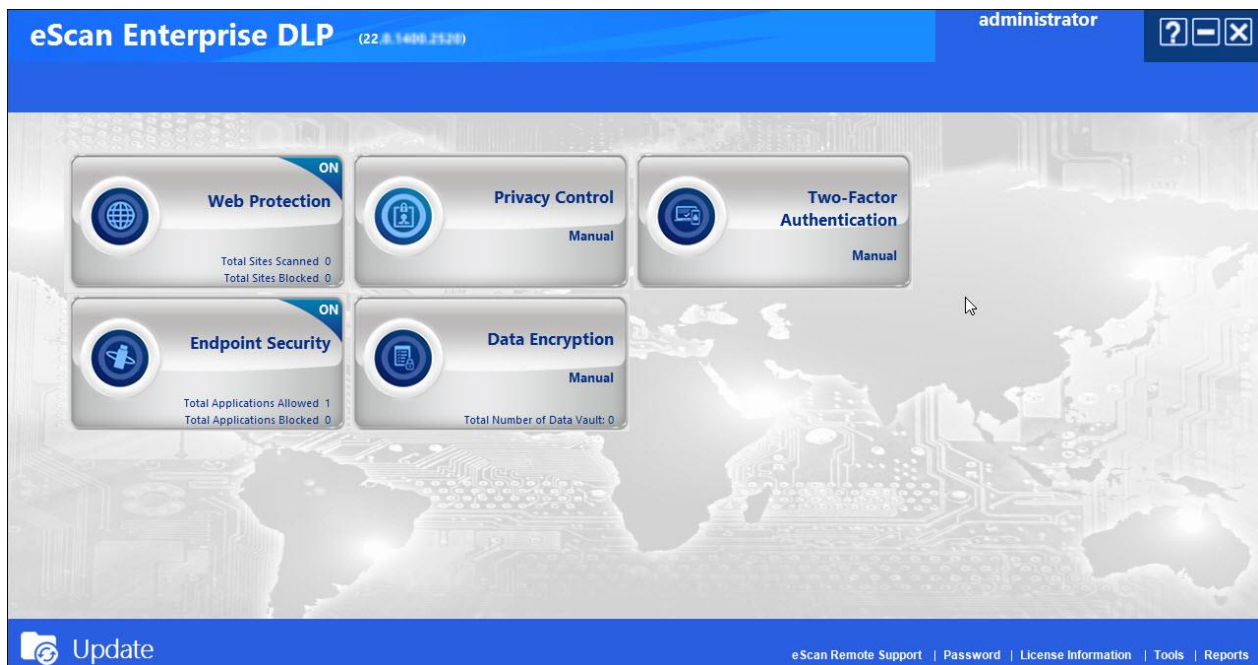
### NOTE

Ensure that the smart device's date and time matches with the system's date and time or else T-OTPs generated by app won't get validated.

## Enabling 2FA login

To enable 2FA login, follow the below steps:


1. Open eScan Protection Center,
  - From Desktop, double-click the  icon.
  - From Taskbar, right-click the  icon and click **Open eScan Protection Center**.



2. Click **Two-Factor Authentication**.



3. Select **Enable Two-Factor Authentication**. This will enable the other configuration settings.

 <b>NOTE</b>	<b>Unlock</b> option will be enabled only after selecting <b>User Logon</b> option.
--	---

4. You can configure it according to your requirement and click **Save**.  
The 2FA will work according to the configuration.

## Login Scenarios

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

### RDP

RDP stands for Remote Desktop Protocol. Whenever someone takes remote control of your system, the personnel will have to enter system login credentials and 2FA passcode to access the system.

### Safe Mode

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

### User Logon

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

### Unlock

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

## Password Types

You can use following password types to log in:

### Use eScan Administrator Password

You can use the existing eScan Administrator password for 2FA login.

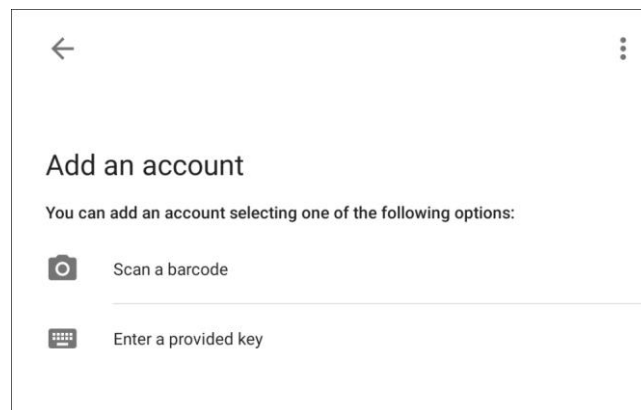
### Use Other Password

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

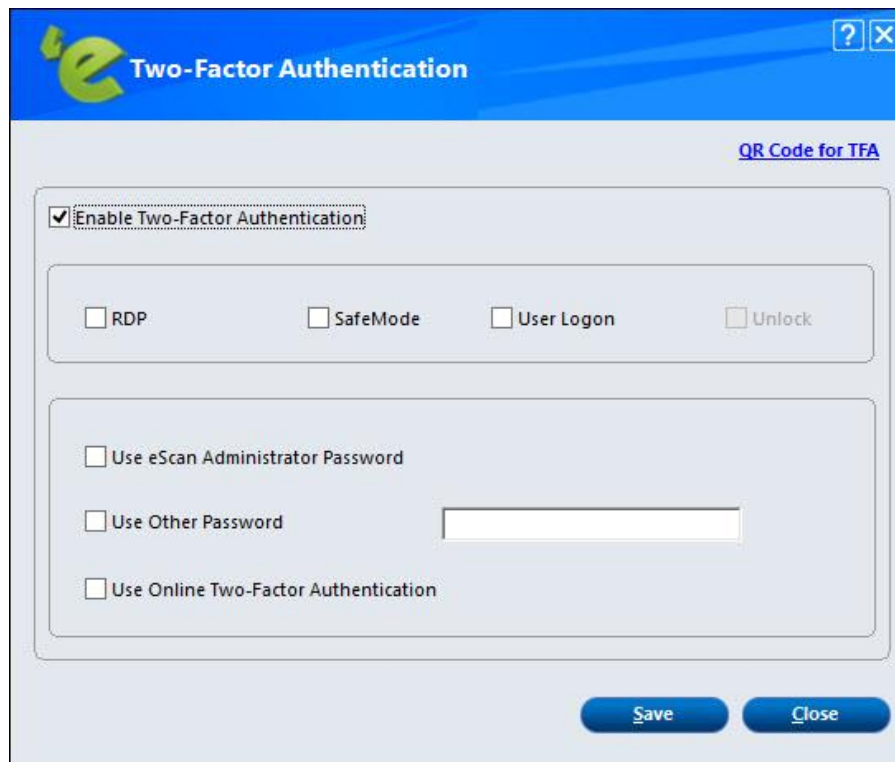
### Use Online Two-Factor Authentication

To use Online 2FA authentication, follow the steps given below:

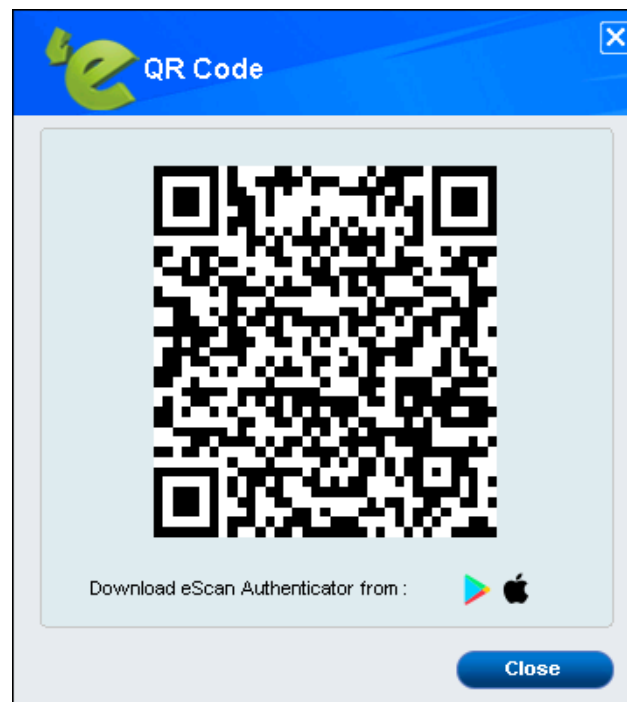
1. Install the **Authenticator** app from Play Store for Android devices or App Store for iOS devices.
2. Open the Authenticator app and tap **Scan a barcode**.



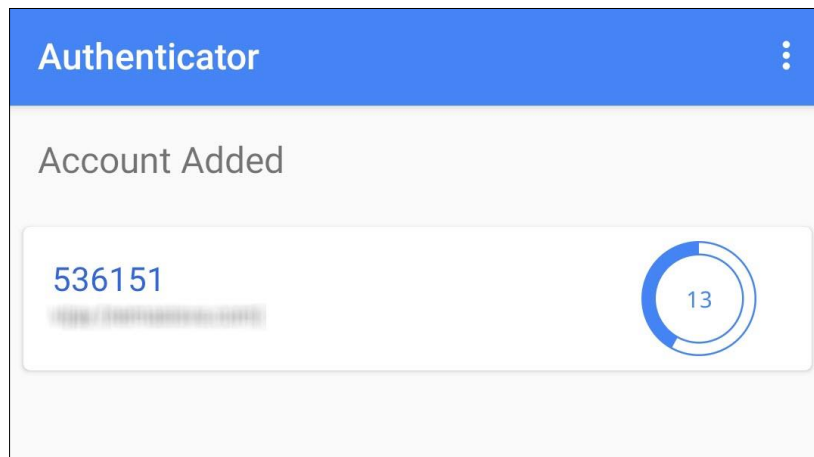
3. Now, open **eScan Protection Center** on your system and click **two-factor authentication**.
4. Select **Enable Two-Factor Authentication**.



5. Configure the login scenarios according to your need and select **Use Online Two-Factor Authentication**.
6. On the top right corner, click **QR code for TFA**.  
A QR code appears.



7. Scan the onscreen QR code via the Authenticator app.  
A Time-based One-Time Password (TOTP) appears on smart device.



8. You can use this TOTP for login.  
This TOTP will get updated after every 30 seconds.

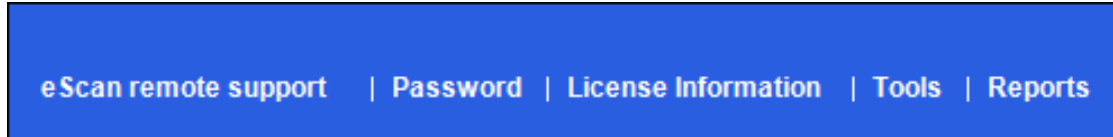
## Disabling 2FA login

To disable the 2FA login, follow the below steps:

1. Open **eScan Protection Center** > **two-factor authentication**.
2. Uncheck the **Enable Two-Factor Authentication** option.
3. Click **Save**.  
The 2FA feature gets disabled.

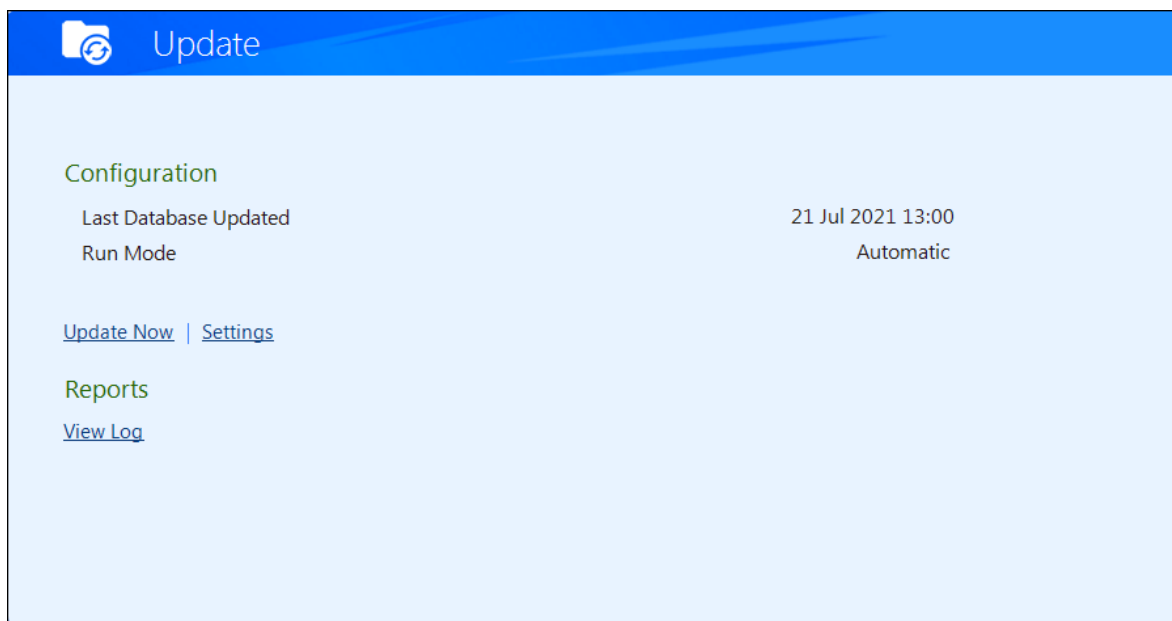
## Quick Access Links

On lower-right corner of the screen, you can view the following quick access links:



## Update

The Update module automatically keeps your virus definitions up-to-date and protects your computer from emerging species of viruses and other malicious programs.



You can access tabbed page for the Update module by clicking the **Update** button. The update tabbed page provides you with information regarding the type of update mode on which the database was last updated.

## Configuration

This section displays the following information:

- **Run Mode:** It displays the type of update mode used by eScan.
- **Update Now:** This button updates the Anti-Virus and Anti-Spam definitions through HTTP or FTP.

Update via HTTP    Anti-Virus    (100%)
[-] [X]

Regular updates of eScan Anti-Virus databases and program modules ensures effective protection.
Last Update: 24 Feb 2021 11:30

Connecting to proxy server 192.168.0.10  
 Requested file name and size  
 eScan Anti-virus Database is Updated. No need to Download.  
 Requested file name and size  
 Starting Anti-Virus Download...  
 Requested file name and size  
eScan Anti-virus Database is Updated. No need to Download.

Time	Result	Object	Size
✓ 3/1/2021 10:34:53 AM	File Downloaded	exploits.avc3	51 Bytes
✓ 3/1/2021 10:34:53 AM	File Downloaded	settings.avc3	64 Bytes
✓ 3/1/2021 10:34:53 AM	File Downloaded	avc3.gx	1525 Bytes
✓ 3/1/2021 10:34:54 AM	File Downloaded	configuration.avc3	210 Bytes
✓ 3/1/2021 10:34:54 AM	File Downloaded	update.bin	35 Bytes

Downloading File    update.bin

<b>Total Downloaded</b>	1.8 KB / 1.8 KB	<b>Duration</b>	00:00:11
<b>Anti-Virus Status</b>	<div style="width: 100%; height: 15px; background-color: #ccc;"></div>	<b>Time Left</b>	00:00:00
<b>Anti-Spam Status</b>	<div style="width: 100%; height: 15px; background-color: #ccc;"></div>	<b>Time Left</b>	00:00:00

Hide
Stop Update



## Reports

This section displays the following information:

- **View Log:** When you click this button, the Update Log window is displayed. This window displays the latest activity report for the Update module.

The screenshot shows the 'Update Log' window with the following data:

Date/Time	Session	Ip Address/Host Name
2/23/2021 4:24:08 PM	Starting Automatic HTTP session to host	http://www.microworldsystems.com/pub/upd...
2/23/2021 5:29:11 PM	Starting Automatic HTTP session to host	http://www.microworldsystems.com/pub/upd...
2/24/2021 1:13:48 AM	Starting Automatic HTTP session to host	http://www.microworldsystems.com/pub/upd...
2/24/2021 8:58:48 AM	Starting Automatic HTTP session to host	http://www.microworldsystems.com/pub/upd...

Result	Object	Size
Successfully Downloaded File	aitok.cvd	7850
Successfully Downloaded File	auto.cvd	30043
Successfully Downloaded File	cevakrnl.rv2	277382
Successfully Downloaded File	cevakrnl.rv8	68016
Successfully Downloaded File	e_spyw.i00	1062

Event Description:

```
Automatic HTTP Downloader Ver 4.0.2.389.
-----
Check eUpdate.ini Settings.
24-Feb-2021 08:58:49 Connection Successful with Ini Settings.
Connecting to proxy server 192.168.1.100
Requested file name and size
[BDUpdCallBck]Update started
Starting Anti-Virus Download...
Total number of Anti-virus files downloaded is 48
```

This report includes the following information:

- The timestamp, session description, and host name or IP address.
- The description of file, such as result of the download, name of the object, and its size.
- The description of event, such as the number of files downloaded, time at which the connection was established or terminated, and the errors, if any.

This window has 2 buttons:

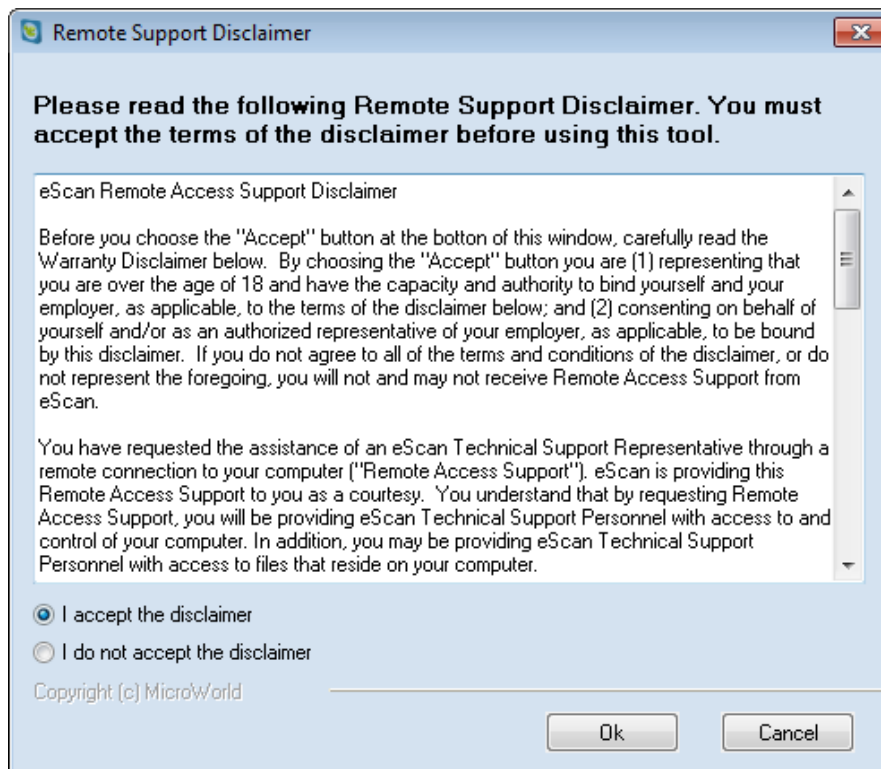
- **Refresh:** This button refreshes the window.
- **Close:** This button closes the popup window.

## eScan Remote Support

eScan Remote Support is the option to get remote help from our Support Center; the Technical Support Executive will take control of your system for resolving the reported issue. It requires an active internet connection.

Steps for availing remote support:

1. Click on **eScan Remote Support** link at the bottom of the interface.  
The Remote Support Disclaimer window will be opened.



2. Read and accept the disclaimer and click **Ok**.  
eScan Remote Support tool will open.
3. It will generate a user ID and password. Send this user id and password to the technical support executive.  
The executive will take remote support of your system.

## Password

Password will secure your system from making any unauthorized changes to the settings and configurations defined by you.

### Using Password Protection for opening eScan

You can define a password for accessing eScan. Use the following steps for defining a password:

1. Open eScan Window.
2. Click **Password** link at the bottom of the interface.
3. Type a Password in the **Enter New Password** field. It is recommended to enter alphanumeric password.
4. Re-enter the Password in **Confirm New Password** field and click **OK**. You will have to enter this password to change any settings and also to open eScan.



  
**NOTE**

For removing the password, Click the password link and Enter old **Password**, leave **Enter New Password** and **Confirm New Password** fields as blank. Now click **OK**. The defined password will be removed and you will not be prompted to enter password to open eScan.

## License Information

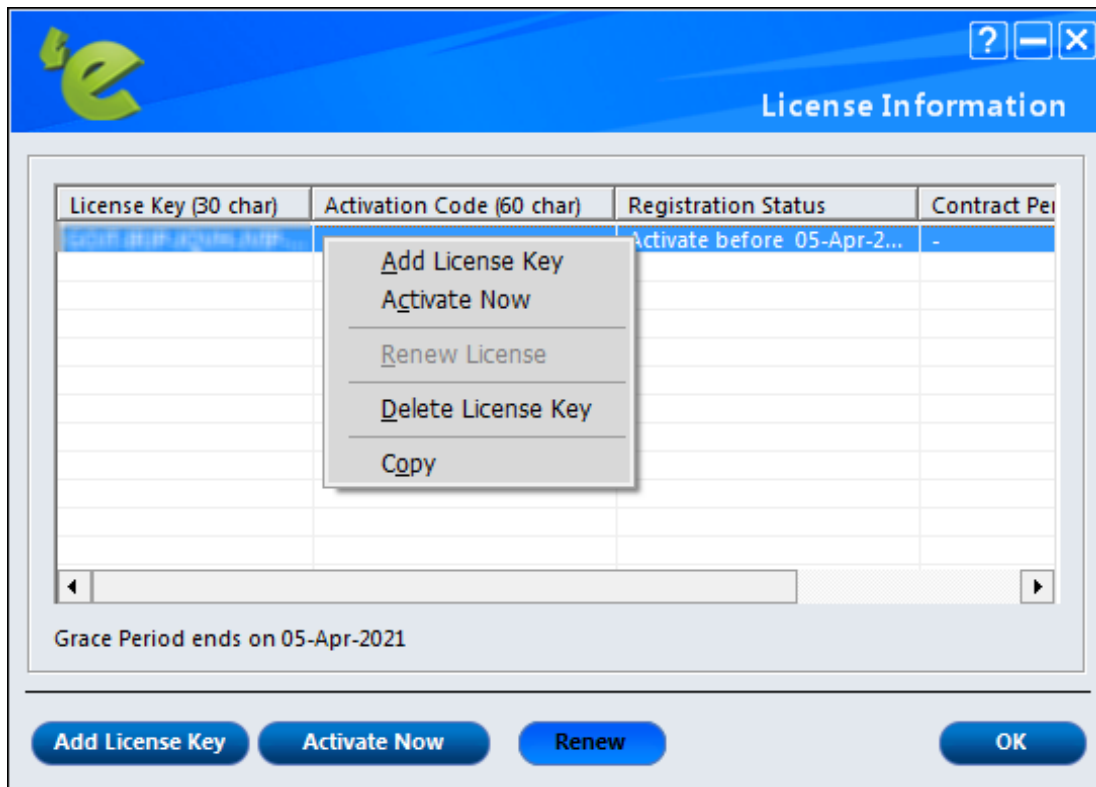
Click License Information link present in Quick access links at the bottom of eScan Protection Center. You will be forwarded to License information window, it displays following important information.

License Key (30 char)	Activation Code (60 char)	Registration Status	Contract Period
XXXXXXXXXXXXXXXXXXXX	XX	Activated	06-Mar-2022

Contract Period Ends on 06-Mar-2022

- **License Key:** Displays the License Key of the product.
- **Activation Code:** Displays the Activation Code of the product.
- **Registration Status:** Displays the registration status of the product namely, Active, Trail, or Expired.
- **Contract Period Ends on:** Displays the expiry date of the product activation.
- **Version:** Displays the version number of the antivirus software.

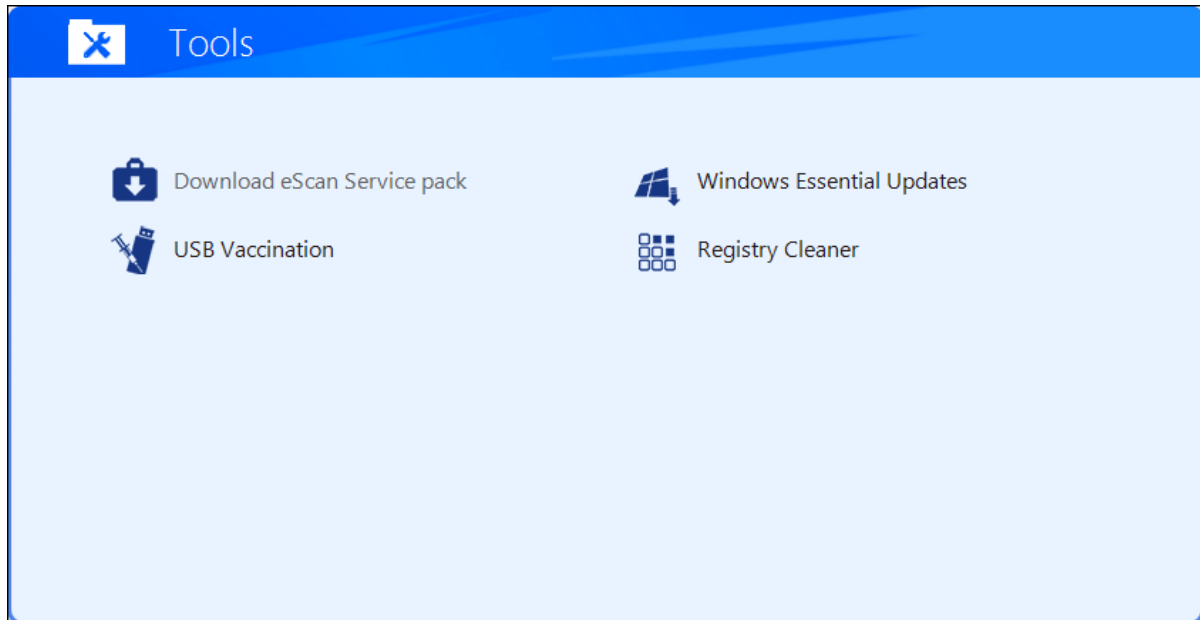
Additionally, it also allows you to perform following actions on right click.



- **Add License Key:** Click on this button to add license key.
- **Activate Now:** Click on this button to activate the license key.
- **Renew License:** Click on this button to renew the license key.
- **Delete License Key:** Click on this button to delete the added license key.
- **Copy:** This option will copy license key.

## Tools

The Tools link provides you with the options for easy and quick access to various tools for eScan and each tool will have its own functions.



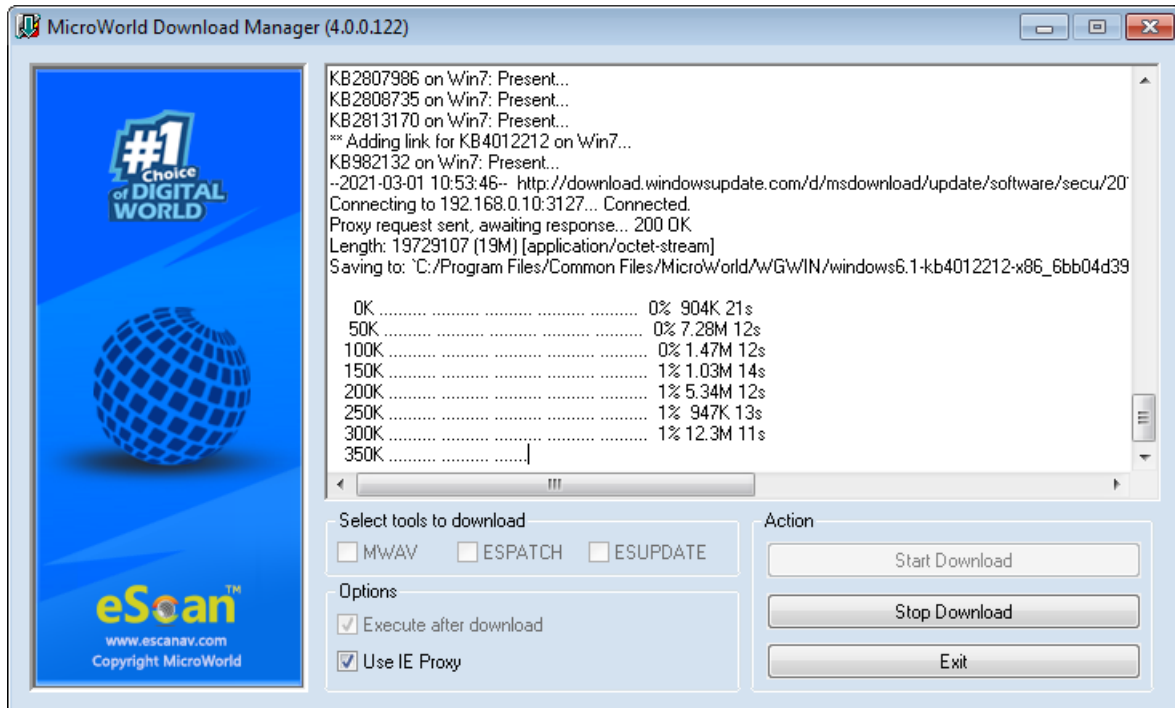
It gives you access to the various eScan tools and it performs the following actions.

### Download eScan service pack

You can download the latest eScan service pack directly from here. This will include all the latest updates.

## Windows Essential Updates

It will update your system with the latest windows patch updates. eScan maintains a list of critical Windows Update patches on every computer that are available for free, whenever the user clicks on **Download Latest Hotfix (Microsoft Windows OS)** option, it checks the computer for missing patches on the OS by matching the installed patches with the released patch list in the database. The missing critical Windows update patches are then downloaded and installed on the computer where eScan is running. The database list is categorized on the basis of the operating system.

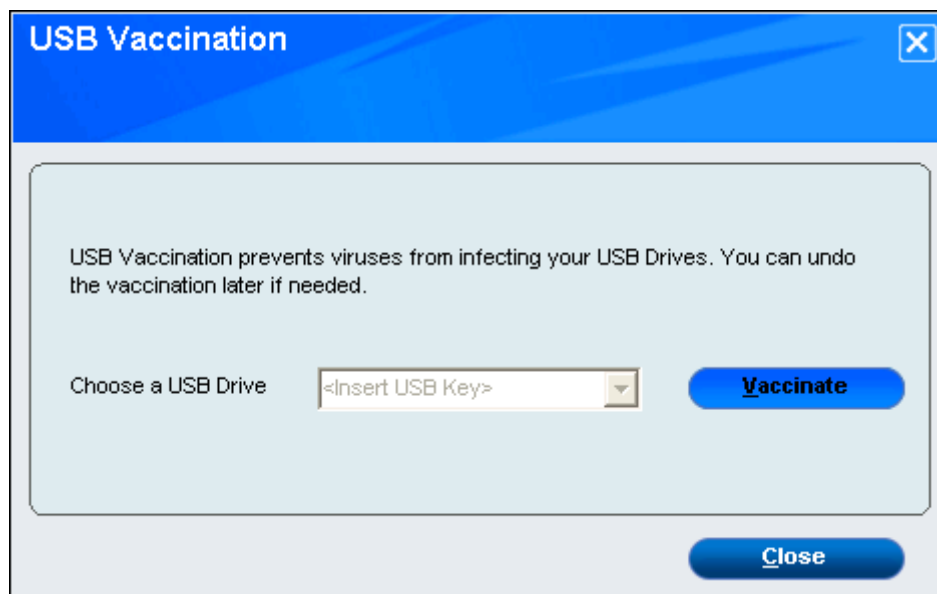


## USB Vaccination

The USB devices are used for various purposes, but while using them you may not be aware that the system to which you are connecting is virus infected. When connected to such machines the USB devices also tend to get infected. So, to prevent such cases, eScan has introduced a feature wherein you can vaccinate USB device, whenever needed. Once vaccinated it stays protected even if you connect the flash drive to an infected system, it doesn't become a carrier to infection.

By default, the **Choose a USB Drive** drop-down list and **Vaccinate** button appears dimmed. It is available only when you connect any USB device to your system.

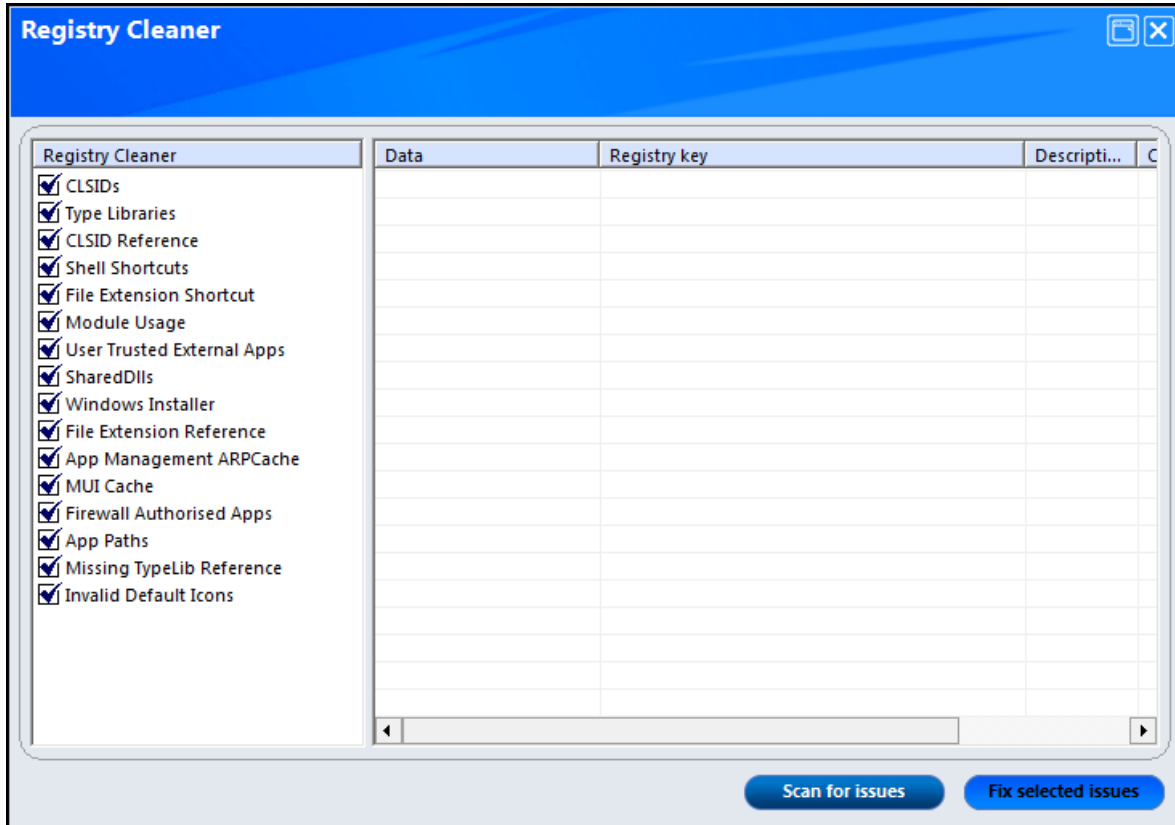
To vaccinate, select an appropriate USB drive, which you want to vaccinate from the **Choose a USB Drive** drop-down list, and click the **Vaccinate** button.





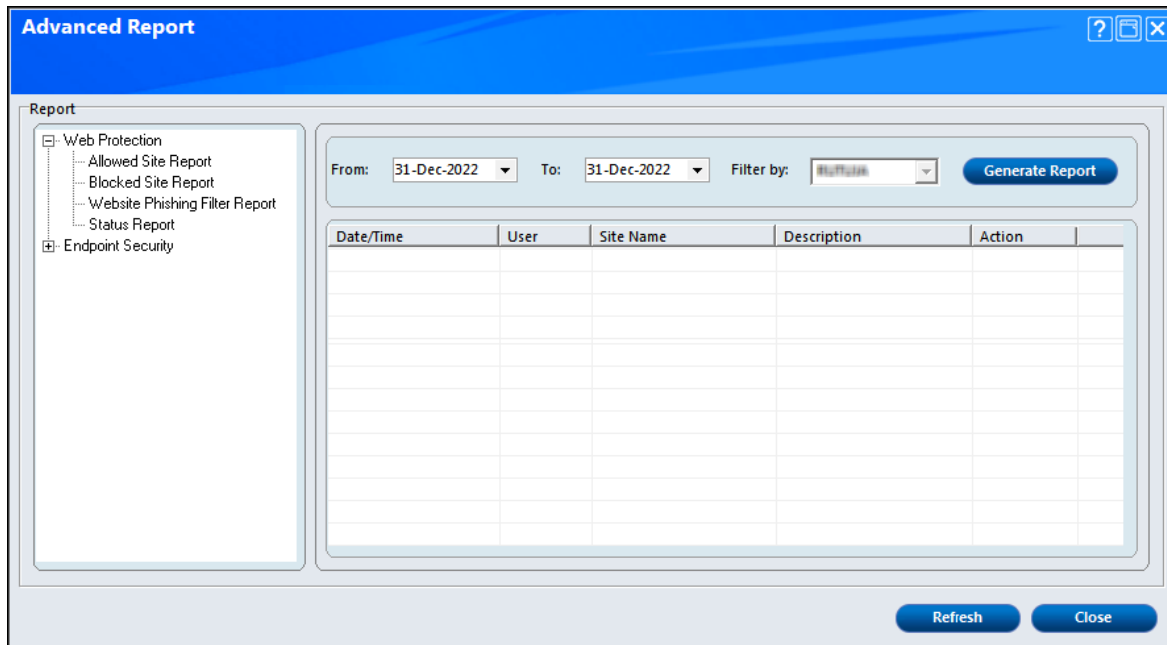
## Registry Cleaner

eScan will scan for issues in the selected registry entries, all issues found will be displayed in the Panel on the right. You can select / unselect the issues found by eScan and fix selected issues button to fix the issues. eScan will fix the selected issues instantly.

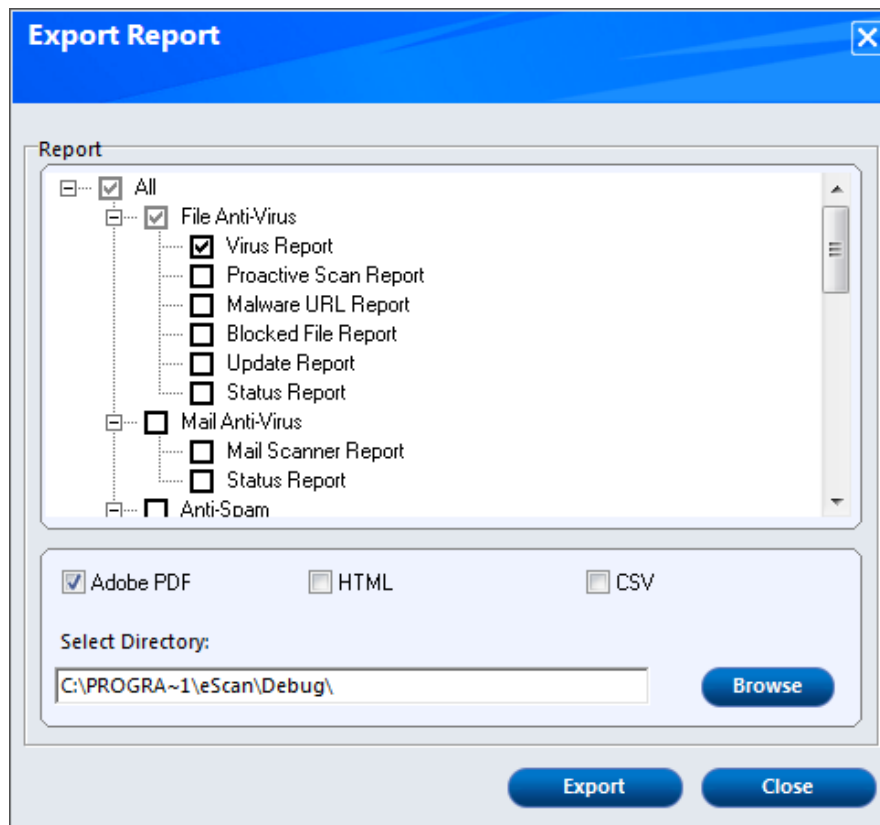


## Reports

eScan generate reports for Web Protection and Endpoint Security modules. Click **Reports** link present in Quick access links at the bottom of eScan Protection Center. You will be forwarded to Advance Report window; it displays the report for all the modules of eScan Enterprise DLP.



- eScan generates reports of all its modules; you can View/Generate a report of any module through Reports link present in every module.
- eScan maintains a log of all the recent activities; it includes the date and timestamp, the user details, description and the action taken.
- It will also allow you to export the particular report as per your requirement or all the existing reports in PDF/ HTML/CSV format; it will also allow you to choose the path to save these reports on to your computer.



## Procedure to export the report files

1. Select the particular files that you want to export or select the checkbox next to **All** option to select all the report.
2. Select the particular format of the file that you want to export; you can select from PDF/HTML/CSV file formats.
3. Click **Browse** and select the path where the file has to be saved.
4. Click **Export** to export the report files, or click **Close** to exit the window.

## 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**